6. Авторизация пользователей и система защиты OpenVMS

Содержание

6.1. Введение

Защита данных от неавторизованного (несанкционированного) доступа или случайного удаления - это одна из наиболее важных вещей, которые должен изучить пользователь.

Эта глава описывает, как просматривать защиту файлов и управлять ею, как уничтожать информацию при удалении ненужных файлов и объясняет причины, по которым файлы нужно регулярно архивировать или резервировать.

Важной функцией управления системой является управление пользователями. Системный администратор отвечает за выполнение таких задач, как:

- Управление доступом к системе
- Поддержка безопасности системы
- Определение времени доступа пользователей к системе
- Управление процессами пользователей

В этой главе даётся введение в основные задачи управления пользователями в системе OpenVMS.

6.2. Литература

OpenVMS DCL Dictionary

OpenVMS Backup Utility Manual

OpenVMS System Management Utilities Reference Manual

OpenVMS System Manager's Manual

6.3. Защита Ваших файлов

Защита файлов определяет, кто имеет доступ к данному файлу, и тип разрешенного доступа.

Операционная система VMS предоставляет два метода защиты файлов:

- Защита по коду идентификации пользователя (UIC)
- Списки управления доступом (ACL)

Изменяйте защиту файлов, чтобы:

- Ограничить доступ к Вашим файлам
- Предотвратить неавторизованное перемещение или удаление файлов
- Назначить специальный код защиты для всех файлов, созданных в данном каталоге
- Удалить подкаталог

6.3.1. Защита файлов по UIC

Каждый пользователь в системе VMS имеет код идентификации пользователя (UIC).

Формат UIC - это два числа в квадратных скобках, как показано ниже:

[группа,член]

- Номер группы может лежать в диапазоне от 0 до 37777 (восьмеричное).
- В каждой группе может быть от 0 до 177777 (восьмеричное) членов.

- Пример цифрового UIC:

  [100,30]

- UIC может быть также в алфавитно-цифровом формате, например:

  [GROUP11,SMITH] или [SMITH]

Операционная система VMS назначает каждому файлу при создании UIC и код защиты.

Система использует UIC и код защиты, чтобы определить, кто может:

- Читать файл
- Писать в файл
- Выполнять файл
- Удалять файл

6.3.1.1. Коды защиты

Код защиты описывает вид доступа, разрешенный каждой категории пользователей.

Категория пользователя по отношению к обработке файлов определяется пользовательским UIC

Таблица 6-1 показывает, как определяется эта категория.

Таблица 6-1. Категории пользователей на основе UIC

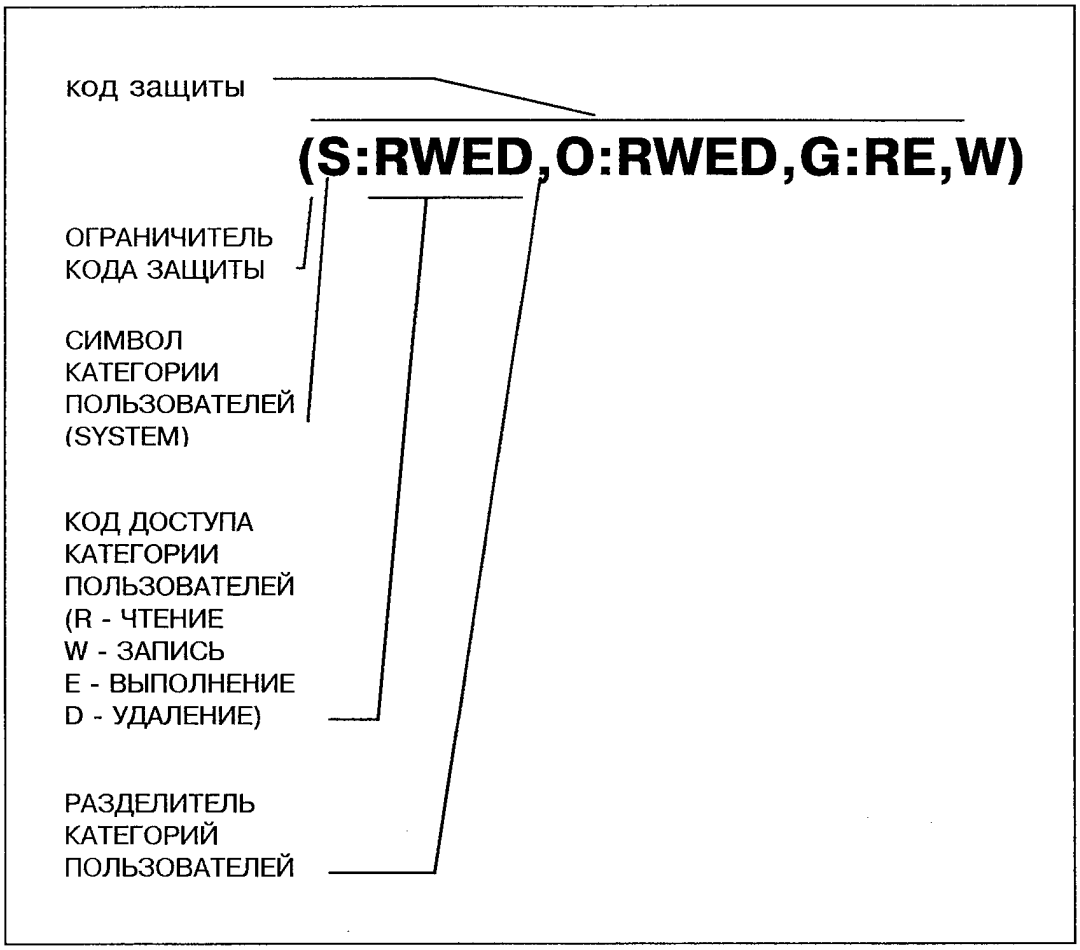
Категория	*Номер группы*	*Номер члена*
SYSTEM (система)	0-10[1] (восьмеричное)	Не имеет значения
OWNER (владелец)	Соответствует номеру группы в UIC файла	Соответствует номеру члена в UIC файла
GROUP (группа)	Соответствует номеру группы в UIC файла	Не имеет значения
WORLD (все)	Не имеет значения	Не имеет значения

Категория, к которой принадлежит пользователь, имеет отношение к коду защиты файла, к которому осуществляется доступ

Рис. 6-1 показывает элементы кода защиты, как он был бы указан в команде SET PROTECTION.

[1] Это число определяется администратором системы, по умолчанию 10_8.

Рис. 6-1. Элементы кода защиты



6.3.1.2. Манипулирование кодами защиты

Таблица 6-2 описывает команды DCL, используемые для просмотра и изменения кодов защиты файлов.

Таблица 6-2. Команды для просмотра и изменения защиты файлов

Операция	*Комментарий и пример команды*

Просмотр защиты, назначаемой новым файлам по умолчанию	Защита по умолчанию применяется ко всем вновь создаваемым файлам в текущем каталоге.
	`$ SHOW PROTECTION`
	`SYSTEM=RWED, OWNER=RWED, GROUP=RE, WORLD=NO ACCESS`

Получение кода защиты данного файла	Показывает текущую защиту данного файла
	`$ DIRECTORY/PROTECTION LOGIN.COM`
	`Directory WORK3:[PICCADACI]`
	`LOGIN.COM;18 (RWED,RWED,RE,)`
	`Total of 1 file.`

Операция	*Комментарий и пример команды*
Изменение защиты, назначаемой новым файлам по умолчанию	Защита по умолчанию после изменения действует на все файлы, создаваемые в будущем в этом конкретном каталоге. Файлы, созданные перед изменением защиты по умолчанию, будут сохранять прежнюю защиту. `$ SET PROTECTION=(S:RWED,O:RWED,G:RWE,W:RWE)/DEFAULT`
Изменение кода защиты существующего файла	Код защиты может быть изменен для разрешения большего или меньшего доступа к конкретному файлу. `$ SET PROTECTION=(S:RWE,O:RWE,G:RE,W) LOGIN.COM`

Пример 6-1 показывает, как посмотреть и изменить код защиты файла.

Пример 6-1. Изменение защиты файла

```
❶ $ DIRECTORY/PROTECTION LOGIN.COM

   Directory WORK3:[PICCADACI]

   LOGIN.COM;18          (RWED,RWED,RE,)

   Total of 1 file.
   $
❷ $ SET PROTECTION=W:R LOGIN.COM
   $
❸ $ DIRECTORY/PROTECTION LOGIN.COM

   Directory WORK3:[PICCADACI]

   LOGIN.COM;18          (RWED,RWED,RE,R)

   Total of 1 file.
   $
```

Пример 6-1, замечания

❶ Посмотрите защиту файла LOGIN.COM.

Система (System) и Владелец (Owner) имеют полный доступ к файлу, Группа (Group) может читать и выполнять файл, Все (World) не имеют никакого доступа.

❷ Измените защиту LOGIN.COM так, чтобы все пользователи имели доступ по чтению.

❸ Снова посмотрите защиту файла LOGIN.COM.

Права доступа не изменились для Системы, Владельца и Группы, но Все теперь имеют доступ по чтению.

Ваш код защиты по умолчанию применяется к вновь создаваемым Вами файлам, если Вы не укажете, что они должны получить другой код защиты. Пример 6-2 показывает, как посмотреть и модифицировать Ваш код защиты по умолчанию.

Пример 6-2. Изменение Вашего кода защиты по умолчанию

```
   $ SET DEFAULT [SMITH.DOC]

❶ $ SHOW PROTECTION
     SYSTEM=RWED, OWNER=RWED, GROUP=RE, WORLD=NO ACCESS

❷ $ DIRECTORY/OUTPUT=DIRECTORY1.LIS
```

```
❸  $ DIRECTORY/PROTECTION

   Directory DISK:[SMITH.DOC]

❹  DIRECTORY1.LIS;1       (RWED,RWED,RE,)

   Total of 1 file.

❺  $ SET PROTECTION=(S:R,G:R)/DEFAULT

❻  $ SHOW PROTECTION
     SYSTEM=R, OWNER=RWED, GROUP=R, WORLD=NO ACCESS

❼  $ DIRECTORY/OUTPUT=DIRECTORY2.LIS
❽  $ DIRECTORY/PROTECTION

   Directory DISK:[SMITH.DOC]

   DIRECTORY1.LIS;1       (RWED,RWED,RE,)
❾  DIRECTORY2.LIS;1       (R,RWED,R,)

   Total of 2 files.
```

Пример 6-2, замечания:

❶ Посмотрите текущую защиту файлов по умолчанию.

❷ Создайте новый файл.

❸ Посмотрите защиту файлов в текущем каталоге.

❹ Новый файл имеет защиту по умолчанию.

❺ Измените защиту файлов по умолчанию так, чтобы Система и Группа имели только доступ по чтению.

❻ Посмотрите новую защиту файлов по умолчанию.

❼ Создайте еще один файл.

❽ Посмотрите защиту файлов.

❾ Второй файл был создан с новой защитой.

6.3.2. Просмотр защиты файлов

Пример 6-3 показывает информацию о защите, которую Вы можете получить, используя команду DIRECTORY.

Пример 6-3. Просмотр защиты файла

```
❶  $ DIRECTORY/FULL LOGIN.COM

   Directory WORK3:[ROUNDS]

   LOGIN.COM;15                  File ID:  (15354,4,0)
   Size:            2/3          Owner:    [GROUP11,ROUNDS]
   Created:  13-SEP-1990 14:57:43.12
   Revised:  13-SEP-1990 14:57:43.75 (2)
   Expires:   <None specified>
   Backup:   30-OCT-1990 19:31:50.53
   File organization:  Sequential
   File attributes:    Allocation: 3, Extend: 0, Global buffer count: 0, No
   version limit
   Record format:      Variable length, maximum 58 bytes
   Record attributes:  Carriage return carriage control
   RMS attributes:     None
   Journaling enabled: None
```

```
❷ File protection:     System:RWED, Owner:RWED, Group:RE, World:
  Access Cntrl List:   None

  Total of 1 file, 2/3 blocks.

❸ $ DIRECTORY/PROTECTION LOGIN.COM

  Directory WORK3:[ROUNDS]

❹ LOGIN.COM;15           (RWED,RWED,RE,)

  Total of 1 file.
```

Пример 6-3, замечания:

❶ Запросите полную каталоговую информацию о LOGIN.COM.

❷ Это защита файла по UIC: Система и Владелец имеют полный доступ к файлу, Группа имеет доступ для чтения и выполнения, а Все не имеют никакого доступа.

❸ Запросите информацию о защите файла LOGIN.COM.

❹ Показан код защиты файла по UIC.

6.3.3. Защита файлов каталогов

Файлы каталогов создаются с защитой, отличной от защиты "обычных" файлов, чтобы уберечься от случайного удаления. Пример 6-4 показывает эту защиту.

Пример 6-4. Защита файлов каталогов

```
$ DIRECTORY/PROTECTION COMMANDS.DIR

Directory $1$DUA1:[ROUNDS]

Total of 1 file.
```

6.3.3.1. Удаление файла каталога

Так как каталоги защищены от удаления, то для удаления файла каталога должны быть предприняты специальные действия.

Для удаления каталога или подкаталога выполните следующие шаги:

1. Уберите все файлы из каталога, либо удаляя их, либо переименовывая в другой каталог.
2. Измените защиту файла каталога так, чтобы Вы (Владелец) могли удалить его.
3. Удалите файл каталога.

Пример 6-5. Удаление подкаталога

```
❶ $ SET DEFAULT [SMITH.DOC]
  $
❷ $ DIRECTORY

  Directory DISK:[SMITH.DOC]

  CLASS.LIST;4          CLOCK.EXE;1          COLOR.COM;4          DEG.EXE;1
  JOE_EVE.TPU$SECTION;1                      MYFILE.TXT;1         NOTE.COM;4
  REMIND.EXE;1          REMLOG.EXE;1         TRNG.PLAN;6          VT100.CLR;1

  Total of 11 files.
  $
❸ $ DELETE *.*;*
  $
```

```
❹ $ DIRECTORY
  %DIRECT-W-NOFILES, no files found
  $
❺ $ SET DEFAULT [SMITH]
  $
❻ $ SET PROTECTION=O:RWED DOC.DIR
  $
❼ $ DELETE DOC.DIR
  $
❽ $ DIRECTORY DOC.DIR
  %DIRECT-W-NOFILES, no files found
  $
❾ $ DIR [.DOC]
  %DIRECT-E-OPENIN, error opening DISK:[SMITH.DOC]*.*;* as input
  -RMS-E-DNF, directory not found
  -SYSTEM-W-NOSUCHFILE, no such file
```

Пример 6-5, замечания:

❶ Сделайте подкаталог, который хотитке удалить, своим подкаталогом по умолчанию.

❷ Получите список имен всех файлов в подкаталоге.

❸ Удалите файлы, находящиеся в подкаталоге. (Вы могли бы предпочесть переименовать их в другой каталог вместо их удаления.)

❹ Проверьте, что в подкаталоге не осталось файлов.

❺ Сделайте своим каталогом по умолчанию каталог, содержащий файл подкаталога, который Вы хотите удалить.

❻ Предполагая, что Вы являетесь владельцем файла, дайте себе доступ по удалению к файлу подкаталога.

❼ Удалите файл каталога.

❽ Файл каталога больше не существует.

❾ Подкаталог больше не является частью Вашей структуры каталогов.

6.3.3.2. Типичные ошибки при удалении файлов каталогов

Пример 6-6 показывает некоторые ошибки, обычно встречающиеся, когда пользователь пытается удалить файл каталога.

Пример 6-6. Типичные ошибки при удалении файлов каталогов

```
❶ $ DELETE TRAVEL.DIR;1
  %DELETE-W-FILNOTDEL, error deleting $1$DUA1:[ROUNDS]TRAVEL.DIR;1
  -RMS-E-MKD, ACP could not mark file for deletion
  -SYSTEM-F-NOPRIV, no privilege for attempted operation
  $
  $ SET PROTECTION=O:RWED TRAVEL.DIR;1
  $
❷ $ DELETE TRAVEL.DIR
  %DELETE-E-DELVER, explicit version number or wild card required
  $
❸ $ DELETE TRAVEL.DIR;1
  %DELETE-W-FILNOTDEL, error deleting $1$DUA1:[ROUNDS]TRAVEL.DIR;1
  -RMS-E-MKD, ACP could not mark file for deletion
  -SYSTEM-F-DIRNOTEMPTY, directory file is not empty
  $
```

Пример 6-6, замечания:

❶ Файл каталога защищен от удаления. Это типичная ошибка, встречающаяся при попытке удалить файл подкаталога.

Установите код защиты файла таким образом, чтобы Вы имели доступ по удалению.

❷ При удалении файла Вы должны указать версию.

Любая из следующих команд была бы верной:

`$ DELETE TRAVEL.DIR;1`	Удалить определенную версию
`$ DELETE TRAVEL.DIR;`	Удалить наивысшую версию
`$ DELETE TRAVEL.DIR;*`	Удалить все версии

У файла каталога должна быть только одна версия - версия 1.

❸ Вы не можете удалить каталог, если в нем содержатся другие файлы. Используйте команду DELETE или RENAME, чтобы убрать файлы из каталога:

`$ DELETE [.TRAVEL]*.*;*`	Удалить все файлы из подкаталога
`$ RENAME [.TRAVEL]*.*;* -` `_$ [.TRIPS]*.*;*`	Переименовать все файлы в другой каталог

6.4. Удаление файлов с уничтожением информации

При удалении файла, содержащего конфиденциальную информацию, Вы должны обеспечить действительное уничтожение этой информации.

- Когда Вы удаляете файл, область, на которой он хранился, возвращается системе для дальнейшего использования.
- Информация, которая хранилась в этом месте, еще существует в системе, пока поверх нее не запишется новая информация.
- Когда Вы указываете квалификатор /ERASE, место хранения перезаписывается с помощью системно-определенного шаблона таким образом, что предыдущая информация более не существует.

  Формат:

  $ DELETE спецификация-файла/ERASE

  $ PURGE спецификация-файла/ERASE

6.5. Защита Ваших файлов и данных от потери

Файлы и данные могут быть потеряны или испорчены разными способами.

- Может быть поврежден диск.
- Пользователь может случайно удалить файл.
- Вычислительный центр может быть разрушен пожаром или наводнением.

6.5.1. Резервное копирование данных

Администратор системы должен завести такой порядок, чтобы делать резервные копии всех файлов в соответствии с опубликованным расписанием.

- Резервные копии должны храниться подальше от места работы системы в целях полной защиты данных.
- Пользователи должны знать о расписании резервного копирования.

Поле *"backup"* в выходной информации команды DIRECTORY/FULL скажет Вам о том, когда последний раз была сделана резервная копия файла.

Пример 6-7. Просмотр даты резервного копирования файла

```
$ DIRECTORY/FULL LOGIN.COM

Directory WORK3:[ROUNDS]

LOGIN.COM;18                File ID:   (714,84,0)
Size:            2/3        Owner:     [GROUP11,ROUNDS]
Created:  17-APR-1991 15:46:48.04
Revised:  17-APR-1991 15:46:48.67 (2)
Expires:   <None specified>
Backup:   17-APR-1991 19:47:12.10
File organization:  Sequential
File attributes:    Allocation: 3, Extend: 0, Global buffer count: 0, No
version limit
Record format:      Variable length, maximum 51 bytes
Record attributes:  Carriage return carriage control
RMS attributes:     None
Journaling enabled: None
File protection:    System:RWED, Owner:RWED, Group:RE, World:
Access Cntrl List:  None

Total of 1 file, 2/3 blocks.
```

6.5.2. Архивирование данных

Правительственные, юридические или аудиторские процедуры могут требовать, чтобы определенный период времени хранились исторические копии файла.

- Это служит "снимком" данных.
- Архивные копии должны храниться в надежном месте.
- Примеры:
  - Копия файла цен компании в конце каждого квартала.
  - Копия счетов клиентов в конце каждого дня.

6.6. Управление пользователями системы

6.6.1. Использование утилиты AUTHORIZE

Утилита AUTHORIZE используется для манипулирования файлом авторизации пользователе UAF (User Authorization File), который определяет системных пользователей.

В этом разделе рассматриваются следующие темы:

- Файл авторизации пользователей (UAF)
- Работа утилиты авторизации AUTHORIZE
- Получение вспомогательной информации из утилиты авторизации
- Просмотр записей в UAF

6.6.1.1. Файл авторизации пользователей

Администратор системы определяет имена пользователей в файле авторизации пользователей UAF.

- UAF содержит одну запись для каждого пользователя, авторизованного для работы в системе.

- В любой системе OpenVMS пользователи идентифицируются по своему имени пользователя.

Каждая запись UAF состоит из имени пользователя, закодированного пароля и некоторых других полей.

- Каждый раз, когда Вы входите в систему, система читает запись UAF, соответствующую Вашему имени пользователя.
- Система создает для Вас процесс (если Вы ввели правильный пароль) с лимитами и ограничениями, найденными в различных полях Вашей записи в UAF.
- Администратор системы может модифицировать любое поле в записи UAF.

6.6.1.2. Запуск утилиты AUTHORIZE

Утилита AUTHORIZE используется для манипулирования файлом авторизации пользоателей UAF. Для запуска этой утилиты Вы должны войти в систему как пользователь SYSTEM или как пользователь с привилегией SYSPRV.

Чтобы запустить утилиту AUTHORIZE:

1. Сделайте своим каталогом по умолчанию каталог SYS$SYSTEM.
2. Для запуска утилиты наберите RUN AUTHORIZE.
3. Для выхода из утилиты наберите EXIT или нажмите CTRL/Z.

Пример 6-8. Запуск утилиты AUTHORIZE

```
$ SET DEFAULT SYS$SYSTEM
$ RUN AUTHORIZE
UAF>
        .
        .
        .
UAF> EXIT
$
```

Использование утилиты AUTHORIZE требует доступа по записи к одному (или всем) из нижеперечисленных файлов:

- SYSUAF.DAT
- NETPROXY.DAT
- RIGHTSLIST.DAT

6.6.1.3. Получение вспомогательной информации из утилиты AUTHORIZE

Для получения информации о командах и квалификаторах утилиты AUTHORIZE используйте команду HELP.

Пример 6-9. Получение вспомогательной информации из утилиты AUTHORIZE

```
$ SET DEF SYS$SYSTEM
$ RUN AUTHORIZE
UAF> HELP

  Information available:

  ADD           Command_Summary       COPY        CREATE      DEFAULT     EXIT
  GRANT         HELP          LIST    MODIFY      REMOVE      RENAME      REVOKE
  SHOW          Usage_Summary
```

```
Topic?
.
.
.
UAF>
```

6.6.1.4. Просмотр записи UAF

Для просмотра отдельных записей UAF используйте команду SHOW утилиты AUTHORIZE.

Для просмотра отдельной записи UAF:

1. Сделайте своим каталогом по умолчанию каталог SYS$SYSTEM.
2. Для запуска утилиты наберите RUN AUTHORIZE.
3. Используйте команду SHOW для просмотра записи.

Пример 6-10. Как посмотреть запись в файле UAF

```
$ SET DEFAULT SYS$SYSTEM
$ RUN AUTHORIZE
UAF> SHOW имя-пользователя
UAF>
```

- Некоторые из полей UAF содержат информацию, уникальную для каждого пользователя, например, поля OWNER, UIC и DEFAULT.
- Другие поля содержат информацию, общую для пользователей одной группы, например, поля ACCOUNT и LGICMD.

Следующий пример использует команду SHOW утилиты AUTHORIZE для просмотра записи UAF для пользователя с именем USER1.

Пример 6-11. Просмотр записи UAF

```
    $ SET DEFAULT SYS$SYSTEM
    $ RUN AUTHORIZE
    UAF> SHOW USER1
❶   Username: USER1                          ❷Owner:  Вова Сидоров
❸   Account:  GRP11                          ❹UIC:    [11,2] ([GRP11,USER1])
    CLI:      DCL                             Tables: DCLTABLES
❺   Default:  DISK$USER:[USER1]
❻   LGICMD:   SYS$MANAGER:GRP11LOGIN
❼   Flags:    Diswelcome Disnewmail
    Primary days:   Mon Tue Wed Thu Fri
    Secondary days:                      Sat Sun
    Primary   000000000011111111112222  Secondary  000000000011111111112222
    Day Hours 012345678901234567890123  Day Hours  012345678901234567890123
    Network:  --------##########------             -----  No access  ------
    Batch:    --------##########------             -----  No access  ------
    Local:    ##### Full access ######             ##### Full access ######
    Dialup:   --------##########------             -----  No access  ------
    Remote:   --------##########------             -----  No access  ------
    Expiration:            (none)    Pwdminimum:  6   Login Fails:     0
    Pwdlifetime:        180 00:00    Pwdchange:       (pre-expired)
    Last Login:            (none) (interactive),   (none) (non-interactive)
❽   Maxjobs:         0  Fillm:       300  Bytlm:        60000
    Maxacctjobs:      0  Shrfillm:      0  Pbytlm:           0
    Maxdetach:        0  BIOlm:        40  JTquota:       4096
    Prclm:          100  DIOlm:        40  WSdef:         3072
    Prio:             4  ASTlm:       100  WSquo:         6144
    Queprio:          0  TQElm:        40  WSextent:     16384
    CPU:         (none)  Enqlm:      2000  Pgflquo:      65536
```

```
❾ Authorized Privileges:
    NETMBX      TMPMBX
  Default Privileges:
    NETMBX      TMPMBX
  UAF>
```

Пример 6-11, замечания:

❶ Это имя пользователя, которое он набирает в ответ на подсказку *Username:* при входе в систему.

❷ Поле владельца не используется системой. Для включения пробелов в имя владельца, заключите его в кавычки (" ").

❸ Используется утилитой учета использования системных ресурсов ACCOUNTING для идентификации процессов, чья активность учитывается вместе.

❹ Код идентификации пользователя (UIC) используется для усиления защиты устройств, томов и файлов. Он также используется для регулирования способности процесса общаться с другими процессами и воздействовать на них. UIC может быть показан в числовой форме и в форме строки символов. Числовая форма - это *[группа,член]* (*[group,member]*). Символьная форма - это *[учетное_имя,имя_пользователя]* (*[account,username]*).

❺ Используется операционной системой для устоновления имени устройства и каталога по умолчанию при входе в систему. Предпочтительнее указывать устройство по умолчанию с помощью логического имени, основанного на метке тома (например, DISK$USER), а не с помощью имени физического устройства (например, DUA1:).

❻ Указывает общий для всей системы или для группы пользователей командный файл, выполняемый при входе в систему. Команды этого файла выполняются перед тем, как пользовател сможет вводить команды интерактивно или посредством пакетного командного файла. Если это поле пустое, система выполняет файл LOGIN.COM в пользовательском каталоге по умолчанию перед выполнением команд ползователя.

❼ Специальные ограничения во время и после входа в систему. Эти флаги также включают флаг DISUSER, используемый для запрещения работы пользователя.

❽ Лимиты используются для ограничения использования процессом различных ресурсов. Лимиты также называют квотами, что не следует путать с дисковыми квотами.

❾ Привилегии, присвоенные данному пользователю. Привелегии по умолчанию (default privileges) даются пользователю при входе в систему. Авторизованные привилегии (authorized privileges) даются при вводе пользователем команды SET PROCESS/PRIVILEGE.

6.6.2. Использование утилиты AUTHORIZE для просмотра списка пользователей

Администратору системы может понадобиться получить спсиок пользователей системы. Возможные причины:

- Перед добавлением нового пользователя важно выбрать UIC и имя пользователя, еще не присвоенные другому пользователю.
- Список существующих записей о пользователях позволяет системному администратору присвоить новому пользователю подходящий номер группы в коде UIC.
- Полезно иметь под рукой текущий список пользователей системы для справки.

6.6.2.1. Получение списка пользователей

Для получения списка пользователей на своём терминале или в файле используйте утилиту AUTHORIZE.

- Команда LIST создаст файл SYSUAF.LIS, содержащий список пользовательских записей.
- Команда SHOW/BRIEF покажет список пользовательских записей на терминале.

Следующая таблица показывает широко используемые команды LIST и COPY утилиты AUTHORIZE.

Таблица 6-3. Образцы команд для получения списка пользователей

Если Вы хотите получить список записей UAF для...	*Используйте эту команду для записи списка в файл:*	*Используйте эту команду для получения списка на экране терминала:*
всех пользователей	LIST	SHOW/BRIEF *
определённой группы UIC	LIST [*группа*,*]	SHOW/BRIEF [*группа*,*]
определённого пользователя	LIST *имя_пользователя*	SHOW/BRIEF *имя_пользователя*

Пароли в списке никогда не показываются.

Краткий список записей UAF содержит следующую информацию:

- Владелец записи (счёта)
- Имя пользователя
- UIC
- Учетное имя (account name)
- Привилегии
- Приоритет процесса
- Диск и каталог по умолчанию

Следующий пример показывает использование команды SHOW/BRIEF и команды LIST.

Пример 6-12. Краткий список записей UAF

```
❶ UAF> SHOW/BRIEF [400,*]
        Owner    Username       UIC  Account Privs Pri Directory
   Group leader  PER_USER1   [400,1] PER     All     4 $1$DUA1:[PER_USER1]
   Jerry D.      PER_USER2   [400,2] PER     Normal  4 $1$DUA1:[PER_USER2]
   Krystle R.    PER_USER3   [400,3] PER     Normal  4 $1$DUA1:[PER_USER3]
   Dave L.       PER_USER4   [400,4] PER     Normal  4 $1$DUA1:[PER_USER4]
   Min R.        PER_USER5   [400,5] PER     Normal  4 $1$DUA1:[PER_USER5]
       .
       .
       .
❷ UAF> LIST [400,*]
   %UAF-I-LSTMSG1, writing listing file
   %UAF-I-LSTMSG2, listing file SYSUAF.LIS complete
   UAF>
```

Пример 6-12, замечания:

❶ Используя утилиту AUTHORIZE, просмотрите краткий список всех пользователей с номером группы 400 в коде UIC.

❷ Создайте файл, содержащий ту же информацию

Привилегии делятся на семь категорий в соответствии с вредом, который может нанести системе обладающий этими привилегиями пользователь. Эти категории показывает Таблица 6-4.

Таблица 6-4. Категории привилегий пользователей системы

Категория	*Описание*
None	Никаких привилегий
Normal	Минимальные привилегии для эффективного использования системы
Group	Возможность мешать членам своей группы
Devour	Возможность потребления некритичных общесистемных ресурсов
System	Возможность мешать нормальной работе системы
Objects	Возможность нарушения защиты объектов
All	Возможность управлять системой

6.6.3. Добавление нового пользователя системы

Процедура добавления нового пользователя системы может сильно изменяться от одного места установки системы к другому в зависимости от проводимой в данном месте политики в области безопасности. Однако, все процедуры обычно включают в себя следующие общие шаги:

1. Планирование счёта (записи в UAF) пользователя
2. Добавление записи в UAF
3. Установление дисковой квоты
4. Создание каталога по умолчанию
5. Проверка нового счёта (необязательно, но настоятельно рекомендуется)

6.6.3.1. Планирование пользовательского счёта

Планирование пользовательского счёта

Перед добавлением пользователя в систему определите:

- Имя пользователя
- Пароль
- Код идентификации пользователя (UIC)
- Устройство по умолчанию
- Каталог по умолчанию
- Учетное имя

Требования в каждом отдельном месте установки системы могут предусматривать необходимость установки других параметров при добавлении пользователя.

Назначение имени пользователя

Имя пользователя идентифицирует данного пользователя при входе (регистрации) в операционную систему.

- Имя пользователя обычно соответствует фамилии пользователя или некоторой комбинации его имени и фамилии. При повышенных требованиях к безопасности может возникнуть

необходимость в назначении более таинственных имен пользователей.

- Имя пользователя - это строка от 1 до 12 символов, включая буквы, цифры и знаки подчёркивания (_). Знаки доллара ($) разрешены, но обычно зарезервированы для системных имён. Не следует назначать полностью цифровых имён пользователей.

Хотя полностью цифровые имена пользователей и разрешены, полностью цифровые идентификаторы - нет. Цифровые имена пользователей следует избегать, так как они не получат соответствующих идентификаторов.

Назначение пароля

Пароль служит удостоверением, которое должно быть известно только пользователю и операционной системе.

- По умолчанию пароли, назначаемые системным администратором с использованием утилиты AUTHORIZE, являются заранее просроченными, и пользователь должен выбрать новый пароль при первом входе в систему.
- Пароли могут быть длиной от 0 до 31 символа и содержатьбуквы, цифры, знаки доллара ($) и знаки подчёркивания (_).
- Короткие и очевидные пароли представляют потенциальную проблему для безопасности, облегчая неавторизованным личностям возможность входить в систему. Системный администратор должен обсудить этот вопрос с новым пользователем.
- Минимальная длина для пароля, устанавливаемого пользователем, 6 символов. В некоторых местах могут потребоваться более длинные пароли.

Системный администратор может с помощью утилиты AUTHORIZE назначить пароль, который короче минимальной требуемой длины. Соблюдение длины пароля требуется только для команды SET PASSWORD языка DCL.

Минимальная длина пароля

Используйте утилиту AUTHORIZE для указания минимальной длины пароля с помощью квалификатора PWDMINIMUM во время добавления или модификации записи о пользователе.

Например:

```
UAF> MODIFY USER1/PWDMINIMUM=12
```

Назначение кода идентификации пользователя

Код идентификации пользователя (UIC) указывает на принадлежность пользователя к группе, имеющей отношение к департаменту, проекту или функции данного пользователя.

- Этот код представляет собой восьмеричные номер группы и номер члена группы, разделённые запятой и заключённые в квадратные скобки. Пример: [11,2]
  - Номер группы должен лежать в диапазоне от 1 до 37776_8. Номера групп 10 и меньше должны быть зарезервированы для системных пользователей.
  - Номер члена группы должен лежать в диапазоне от 1 до 177776_8.
- Код UIC должен быть уникальным в системе, так как он

используется для определения принадлежности файлов пользователей.

Назначение устройства по умолчанию

Выберите устройство, имеющее достаточно свободного места для такого количества файлов, которе пользователь, вероятно, будет иметь. Полезно (но не обязательно) использовать в качестве устройства по умолчанию один и тот же диск для всех членов одной группы.

Назначение каталога по умолчанию

Каталог пользователя верхнего уровня (каталог по умолчанию) будет расположен на устройстве по умолчанию.

- Обычно, но не обязательно, имя каталога по умолчанию совпадает с именем пользователя.
- Имя каталога по умолчанию не должно совпадать с именем каталога верхнего уровня на том же устройстве.

Назначение учётного имени

Учётное имя - это строка от 1 до 8 символов.

- Это имя может быть использовано как учётное имя или номер утилитой ACCOUNTING.
- Учётное имя используется в качестве первой (групповой) части алфавитно-цифрового UIC пользователя и должно соответствовать учетному имени других членов группы UIC данного пользователя.

6.6.3.2. Добавление новой записи в UAF

Добавление новой записи в UAF

Для добавления записи в UAF используйте команду ADD утилиты AUTHORIZE.

- Код UIC должен быть уникальным в системе. Утилита AUTHORIZE возвратит сообщение об ошибке при вводе неуникального значения.
- Неуказанные параметры примут значения по умолчанию.
- Если запись о пользователе DEFAULT (запись, хранящая значения по умродчанию) имеет установленный флаг DISUSER, используйте квалификатор /FLAG=NODISUSER для указания, что данный счёт пользователя не является недействительным.

При вводе неуникального значения UIC утилита AUTHORIZE выдаст сообщение об ошибке.

- Запись о пользователе будет всё же добавлена в файл UAF.
- В базу данных прав не будет добавлен соответствующий идентификатор.

Указание учётного имени при добавлении пользователя

Если это первый пользователь в данной группе UIC, то укажите учётное имя (account) в командной строке ADD, чтобы был должным образом создан соответствующий идентификатор.

Разрешение на использование счёта

Пользовательская запись унаследует флаг DISUSER у счёта DEFAULT, если в записи DEFAULT в файле UAF этот флаг не был сброшен

Запись DEFAULT в файле UAF

Если для какого-либо поля новой записи UAF не было указано значение, значение для этого поля будет взято из записи DEFAULT файла UAF.

Пример 6-13 показывает использование утилиты AUTHORIZE для добавления записи в файл UAF для пользователя USER1.

Пример 6-13. Добавление записи о пользователе вручную

```
   $ SET DEFAULT SYS$SYSTEM
   $ RUN AUTHORIZE
❶  UAF> ADD USER1/UIC=[11,2]/ACCOUNT=GRP11-
❷  _UAF> /DEVICE=DISK$USER/DIRECTORY=[USER1]-
   _UAF> /PASSWORD=ENIGMA/OWNER="Вова Сидоров"-
   _UAF> /FLAG=NODISUSER
❸  %UAF-I-ADDMSG, user record successfully added
❹  %UAF-I-RDBADDMSGU, identifier USER1 value: [000011,000002] added to
   rights database
   UAF> EXIT
❺  %UAF-I-DONEMSG, system authorization file modified
   %UAF-I-NAFNOMODS, no modifications made to network proxy data base
   %UAF-I-RDBDONEMSG, right data base modified
   $
```

Пример 6-13, замечания:

❶ Заметьте, что для продолжения команды на следующей строке использован символ переноса (-).

❷ Утилита AUTHORIZE даёт подсказку _UAF> для указания на то, что команда не окончена.

❸ Информационное сообщение утилиты AUTHORIZE.

❹ Пользователь получает уникальный идентификатор в базе данных прав системы.

❺ Когда Вы выходите из утилиты AUTHORIZE, эти сообщения показывают, какие изменения были (если были) внесены в системные файлы.

6.6.3.3. Установление дисковой квоты

Дисковая квота

Системный администратор может использовать дисковые квоты для ограничения размера дискового пространства, которое пользователь может израсходовать на данном дисковом томе. Если на дисковом томе, который пользователь будет использовать, разрешены дисковые квоты, то для кода UIC данного пользователя должна быть установлена дисковая квота на этом томе.

Использование утилиты SYSMAN для установления дисковой квоты

Утилита управления системой (SYSMAN) централизует управление системой, так что узлы или кластеры могут управляться из одного места.

Запустите утилиту SYSMAN для добавления UIC пользователя к файлу квот на каждом томе, где разрешены квоты и где пользователь будет создавать или модифицировать файлы.

SYSMAN требует следующие привилегии:

- OPER на локальном узле
- Авторизованные привилегии OPER или SETPRV на тех удалённых узлах, доступ к которым будет осуществляться
- Привилегии, необходимые для отдельных исполняемых команд

Пример 6-14 показывает, как коду UIC [11,2] назначается постоянная квота в 500 блоков и перерасход в 100 блоков на томе DISK$USER.

Пример 6-14. Использование утилиты SYSMAN для установления дисковой квоты

```
$ SET PROCESS/PRIVILIGE=OPER
$ RUN SYS$SYSTEM:SYSMAN
SYSMAN> DISKQUOTA ADD [11,2]/DEVICE=DISK$USER-
_SYSMAN> /PERMQUOTA=500/OVERDRAFT=100
SYSMAN> EXIT
$
```

Значения по умолчанию для постоянной квоты и перерасхода берутся из записи для UIC=[0,0]

Пример 6-15. Величины дисковых квот по умолчанию

```
$ RUN SYS$SYSTEM:SYSMAN
SYSMAN> DISKQUOTA SHOW [0,0]/DEVICE=WORK12:

%SYSMAN-I-QUOTA, disk quota statistics on device WORK12: -- Node TIDY
     UIC                  Usage        Permanent Quota   Overdraft Limit
[0,0]                     0            1000              100
SYSMAN>
```

Сверх-распределение дискового пространства[2]

Дисковое пространство может быть сверхраспределено, то есть сумма всех дисковых квот может превышать количество блоков на диске. Чтобы определить степень возможного сверхраспределения диска, следите за процентным соотношением использованного дискового пространства и пространства, распределенного в виде квот.

Дисковое пространство не должно быть сверхраспределено, если выполняются оба следующих условия:

- Пользователи не имеют достаточно дискового пространства и всё время используют почти всю свою квоту
- Диски используются более чем на девяносто процентов своей ёмкости

6.6.3.4. Создание каталога по умолчанию

Каталог по умолчанию

Когда пользователь входит в систему, операционная система ищет запись в UAF, чтобы определить, какие устройство и каталог должны быть использованы как устройство и каталог по умолчанию для данного пользователя.

Дисковый каталог может быть создан до или после того, как создана запись в UAF

Установление каталога по умолчанию

При добавлении пользователя в систему, создайте каталог, соотвтествующий полю DEFAULT в записи UAF.

- Создайте каталог пользователя по умолчанию на томе, где пользователь сможет создавать и модифицировать файлы. (Это может быть также и том, на котором запрещено использование дисковых квот.)
- Это должен быть именно тот каталог, который указан в UAF с помощью квалификаторов /DEVICE и /DIRECTORY.
- Используйте команду CREATE/DIRECTORY языка DCL, указав UIC владельца каталога.

---

[2] Дословно *overbooking* переводится с английского как продажа большего количества билетов, чем имеется посадочных мест.

Пример указания цифрового UIC владельца:

```
$ CREATE/DIRECTORY DISK$USER:[USER1]/OWNER=[11,2]
$
```

Пример указания идентификатора владельца:

```
$ CREATE/DIRECTORY DISK$USER:[USER1]/OWNER=USER1
$
```

6.6.3.5. Проверка нового счёта пользователя

Проверка нового счёта

Когда пользователь добавлен в систему, системный администратор должен проверить его счёт, чтобы убедиться, что все флаги и поля в UAF установлены правильно, а также установлены соответствующие дисковые квоты (если они необходимы).

Пример 6-16 показывает, как администратор системы проверяет новый счёт, созданный для пользователя USER1.

Пример 6-16. Проверка нового пользовательского счёта

```
❶ Username: USER1
❷ Password:
        Добро пожаловать в Московский учебный центр DIGITAL

❸ Your password has expired; you must set a new password to log in

❹ New password:
  Verification:

❺ $ SHOW PROCESS

  25-JUN-1994 11:44:12.96    User: USER1          Process ID:     20200718
                             Node: TIDY           Process name:   "USER1"

  Terminal:                TTC1: (TIDY::SYSTEM)
  User Identifier:         [GRP11,USER1]
  Base Priority:           4
  Default file spec:       DISK$USER:[USER1]

  Devices allocated:       TIDY$TTC1:
❻ $ SHOW DEFAULT
    DISK$USER:[USER1]
❼ $ SHOW QUOTA
    User [USER1] has 6 blocks used, 494 available,
    of 500 authorized and permitted overdraft of 100 blocks on DISK$USER
  $ LOGOUT
    USER1         logged out at 25-JUN-1994 11:53:24.50
```

Пример 6-16, замечания:

❶ Войдите в систему с использованием имени пользователя, которое можно посмотреть в UAF.

❷ Пароль не появляется на экране, его также нельзя увидеть при просмотре UAF.

❸ По умолчанию, счёт имеет заранее просроченный пароль. Это принуждает пользователя выбрать новый пароль при первом входе в систему.

❹ Новый пароль подвергается системой проверкам на минимальную длину, предысторию пароля и на наличие в системном словаре.

❺ Для проверки кода UIC используйте команду SHOW PROCESS

❻ Для проверки входного каталога по умолчанию используйте команду SHOW DEFAULT

❼ Для проверки записи в файле дисковых квот используйте команду SHOW QUOTA

Переустановка пользовательского пароля

При входе в систему для тестирования счёта, имеющего заранее просроченный пароль, системный администратор должен установить новый пароль для данного счёта.

Этот новый пароль не является заранее просроченным. Он должен быть переустановлен с помощью утилиты AUTHORIZE, чтобы пользователь был принужден изменить его при первом входе в систему.

Пароли, установленные с помощью утилиты AUTHORIZE, не подвергаются тем проверкам, которые установлены для команды SET PASSWORD.

Системный администратор не обязан переустанавливать пароль, но переустановка пароля с помощью утилиты AUTHORIZE принуждает пользователя к изменению пароля.

Пример 6-17 показывает, как системный администратор входит в

систему под именем нового пользователя, а затем переустанавливает его пароль.

Пример 6-17. Переустановка пользовательского пароля

```
❶  $ SET HOST 0

❷  Username: USER1
   Password:
          Добро пожаловать в Московский учебный центр DIGITAL

❸  Your password has expired; you must set a new password to log in

❹  New password:
   Verification:

❺  $ LOGOUT
     USER1         logged out at 25-JUN-1994 12:38:56.01
   %REM-S-END, contril returned to node _NEAT::
   $ SET DEFAULT SYS$SYSTEM
❻  $ RUN AUTHORIZE
❼  UAF> MODIFY USER1/PASSWORD=ENIGMA
   %UAF-I-MDFYMSG, user record(s) updated
   UAF>
```

Пример 6-17, замечания:

❶ Используйте команду SET HOST для входа в систему при тестировании пользовательского счёта. Если команда SET HOST недоступна на Вашей системе, выйдите из системы и войдите вновь для тестирования нового счёта.

❷ Введите имя пользователя и пароль нового пользователя.

❸ Если счёт имеет заранее просроченный пароль, при первом входе в систему должен быть выбран новый пароль.

❹ Новый пароль является субъектом системных ограничений на длину пароля, предысторию и наличие в сисемном словаре.

❺ Выйдите из системы как новый пользователь и верните управление процессу системного администратора.

❻ Запустите утилиту AUTHORIZE для переустановки пользовательского пароля.

❼ Новый пароль может быть таким же, как и назначенный первоначально. Пароли, установленные с помощью утилиты AUTHORIZE, не подвергаются системным ограничениям.

6.6.3.6. Использование автоматизированной процедуры добавления пользователя

ADDUSER.COM

ADDUSER.COM - это командная процедура, поставляемая с операционной системой OpenVMS, чтобы помочь системному администратору добавлять новых пользователей в систему.

Пример 6-18 показывает использование командной процедуры ADDUSER.COM для добавления пользователя в систему.

Пример 6-18. Работа с командной процедурой ADDUSER.COM

```
$ @SYS$EXAMPLES:ADDUSER ❶
************************************************************************
*  Creating a NEW user account... If at ANY TIME you need help about a    *
*  prompt, just type "?".                                                 *
************************************************************************
```

```
Username(s) - separate by commas: USER1 ❷

 *** Processing USER1's account ***

Full name for USER1: Admin User ❸
Password (password is not echoed to terminal) [USER1]: ❹

UIC Group number [200]: 11 ❺
UIC Member number: 2 ❻
Account name: ? ❼

You must enter the account name to be used for the user. This is generally
used for billing purposes.

Account name: GRP11 ❽
Privileges [TMPMBX,NETMBX]: TMPMBX,NETMBX,OPER ❾

Login directory [USER1]: ❿
Login device [SYS$SYSDEVICE:]: UD01: ①

Disk quota [1000]:
Overdraft quota [100]:

%CREATE-I-CREATED, UD01:[USER1] created
%UAF-I-ADDMSG, user record successfully added
%UAF-I-RDBADDMSGU, identifier USER1 value: [000011,000002] added to rights
data base
%UAF-I-RDBADDMSGU, identifier GRP11 value: [000011,177777] added to rights
data base
%UAF-I-DONEMSG, system authorization file modified
%UAF-I-NAFNOMODS, no modifications made to network proxy data base
%UAF-I-RDBDONEMSG, rights data base modified

Check newly created account:


Username: USER1                                  Owner:  ADMIN USER
Account:  GRP11                                  UIC:    [11,2] ([GRP11,USER1])
CLI:      DCL                                    Tables: DCLTABLES
Default:  UD01:[USER1]
LGICMD:   LOGIN
Flags:  DisUser
Primary days:   Mon Tue Wed Thu Fri
Secondary days:                      Sat Sun
No access restrictions
Expiration:            (none)     Pwdminimum:  6   Login Fails:     0
Pwdlifetime:         90 00:00     Pwdchange:       (pre-expired)
Last Login:            (none) (interactive),             (none) (non-
interactive)
Maxjobs:          0  Fillm:       100  Bytlm:        32768
Maxacctjobs:      0  Shrfillm:      0  Pbytlm:           0
Maxdetach:        0  BIOlm:        18  JTquota:       1024
Prclm:           10  DIOlm:        18  WSdef:          256
Prio:             4  ASTlm:        24  WSquo:          512
Queprio:          0  TQElm:        20  WSextent:      2048
CPU:         (none)  Enqlm:      2000  Pgflquo:      20480
Authorized Privileges:
  TMPMBX OPER NETMBX
Default Privileges:
  TMPMBX NETMBX
%UAF-I-NOMODS, no modifications made to system authorization file
%UAF-I-NAFNOMODS, no modifications made to network proxy data base
%UAF-I-RDBNOMODS, no modifications made to rights data base

Is everything satisfactory with the account [YES]: ②
```

```
$
```

Пример 6-18, замечания:

❶ Выполните командную процедуру ADDUSER.

❷ Введите имя пользователя (или несколько имён). Это будет то имя, под которым пользователь может войти в систему.

❸ Не используется системой, но включено для удобства системного администратора.

❹ Вы не видите пароль, когда набираете.

❺ Номер группы должен быть восьмеричным.

❻ Номер члена группы должен быть восьмеричным и уникальным внутри данной группы.

❼ Здесь введён знак вопроса, чтобы увидеть вспомогательную информацию по учётным именам.

❽ Это имя используется программами учёта для отслеживания использования ресурсов.

❾ Этот пользователь бкдет иметь привилегию OPER вместе с привилегиями TMPMBX и NETMBX. Это авторизованная привилегия, а не привилегия по умолчанию. Чтобы активизировать привилегию OPER, USER1 должениспользовать команду SET PROCESS/PRIVILEGE.

❿ Также известен как "домашний каталог" (home directory).

① Для входного устройства по умолчанию используйте логическое имя, а не имя физического устройства. Это сохранит Вам время впоследствии, если понадобится перевести пользователей на другое физическое устройство.

② Если что-то в счёте не так или чего-то не хватает, ответьте NO, чтобы повторить процесс.

6.6.3.7. *Типичные ошибки при добавлении пользователей*

Типичные ошибки

Существует несколько типичных ошибок, которые легко допустить при добавлении пользователя к системе. Они включают:

- Отсутствие достаточных привилегия для запуска AUTHORIZE.
- Неправильный запуск AUTHORIZE.
- Назначение дублирующихся кодов UIC.
- Неуказание учётного имени для новой группы UIC.
- Неснятие флага DISUSER (недействительный пользователь) со счёта пользователя.
- Неуказание устройства и каталога по умолчанию.
- Неуказание владельца каталога.
- Неверное расположение каталога пользователя.
- Неустановка дисковой квоты.

Ошибка: отсутствие достаточных привилегий для запуска AUTHORIZE

Для получения доступа к системному файлу UAF системный администратор должен иметь либо привилегию SYSPRV, либо системный UIC.

Пример ошибки:

```
$ SET DEF SYS$SYSTEM
$ RUN AUTHORIZE
%UAF-E-NAOFIL, unable to open system authorization file
```

```
(SYSUAF.DAT)
-RMS-E-PRV, insufficient privilege or file protection
violation
$
```

Для исправления этой ошибки:

```
$ SET PROCESS/PRIVILEGE=SYSPRV
$ RUN AUTHORIZE
        .
        .
        .
```

Если администратор системы имеет привилегию SYSPRV, то она может быть включена.

Ошибка: неправильный запуск AUTHORIZE

Утилита AUTHORIZE ищет в текущем каталоге по умолчанию файл SYSUAF.DAT, файл авторизации пользователей.

- Если системный администратор не сделал своим каталогом по умолчанию SYS$SYSTEM перед запуском AUTHORIZE, системный UAF не будет найден.
- AUTHORIZE предлагает возможность создания UAF в каталоге по умолчанию, если не нашёл его там. Хотя этот файл и полезен для тренировки, системный администратор может по ошибке создать в нём запись о реальном пользователе.

Пример создания тренировочного UAF:

```
$ RUN SYS$SYSTEM:AUTHORIZE
%UAF-E-NAOFIL, unable to open system authorization file
(SYSUAF.DAT)
-RMS-E-FNF, file not found
Do you want to create a new file? Y
UAF>
```

Если пользовательская запись была добавлена в этот "тренировочный" файл, имя этого пользователя не будет найдено в системном UAF при попытке пользователя войти в систему.

```
  Personnel System - Unauthorized Access Prohibited

Username: USER1
Password:
User authorization failure
```

Чтобы исправить это упущение:

1. Сделайте своим каталогом по умолчанию SYS$SYSTEM.
2. Снова запустите AUTHORIZE.
3. Добавьте пользовательскую запись.

Может существовать системное логическое имя

SYSUAF, которое указывает на системный файл UAF.

- Если логическое имя назначено, файл авторизации пользователей юудет найден, даже если каталог по умолчанию не SYS$SYSTEM.
- Для создания тренировочного файла UAF системный администратор должен создать логическое имя процесса для отказа от системного логического имени.

Ошибка:

Дублирующиеся коды UIC могут быть назначены несколькими

назначение дублирующихся кодов UIC

путями.

- Назначение UIC без проверки списка существующих UIC.
- Добавление пользователя путём копирования другой пользовательской записи UAF без указания другого UIC.
- Добавление пользователя без указания UAF, значение для которого будет взято из записи о пользователе DEFAULT.

Пример добавления пользователя без указания UIC:

```
$ SET DEFAULT SYS$SYSTEM
$ RUN AUTHORIZE
UAF> ADD PER_USER7/PASSWORD=TESTING
%UAF-I-ADDMSG, user record successfully added
%UAF-E-RDBADDERRU, unable to add PER_USER7 value: [000200,000200] to rights
data base
-SYSTEM-F-DUPIDENT, duplicate identifier
UAF> SHOW PER_USER7

Username: PER_USER7                          Owner:
Account:                                     UIC:    [200,200] ([200,200])
CLI:      DCL                                Tables: DCLTABLES
Default:  $1$DUA2:[USER]
        .
        .
        .
UAF> EXIT
%UAF-I-DONEMSG, system authorization file modified
%UAF-I-NAFNOMODS, no modifications to network proxy data base
%UAF-I-RDBNOMODS, no modifications made to rights data base
$
```

Для исправления ошибки запустите AUTHORIZE:

1. Удалите пользовательскую запись.
2. Создайте новую запись для пользователя, указав уникальный UIC.

Пример исправления ошибки:

```
UAF> REMOVE PER_USER7
%UAF-I-REMMSG, record removed from system authorization file
UAF> ADD PER_USER7/UIC=[400,7]/PASSWORD=TESTING/ACCOUNT=PER
%UAF-I-ADDMSG, user record successfully added
%UAF-I-RDBADDMSGU, identifier PER_USER7 value: [000400,000007] added to
rights data base
UAF> EXIT
%UAF-I-DONEMSG, system authorization file modified
%UAF-I-NAFNOMODS, no modifications to network proxy data base
%UAF-I-RDBDONEMSG, rights data base modified
$
```

После правильной установки UIC пользователя используйте команду MODIFY для установки других полей UAF.

Альтернативный путь решения проблемы дублирующихся UIC:

1. Запустите AUTHORIZE и добавьте новый идентификатор.
2. Модифицируйте запись пользователя для назначения ему этого нового идентификатора.

Пример[3]:

[3] В этом примере допущена другая типичная ошибка. Какая?

```
UAF> ADD/IDENTIFIER/VALUE=UIC:[400,7] PER_USER7
%UAF-I-RDBADDMSGU, identifier PER_USER7 value: [000400,000007] added to
rights data base
UAF> MODIFY PER_USER7/UIC=[400,7]
%UAF-E-RDBMDFYERR, unable to modify identifier DEFAULT
-SYSTEM-F-DUPIDENT, duplicate identifier
%UAF-I-MDFYMSG, user record(s) updated
UAF> SHOW PER_USER7

Username: PER_USER7                             Owner:
Account:                                        UIC:    [400,7] ([PER_USER7])
        .
        .
        .
UAF>
```

Ошибка: неуказание учётного имени для новой группы UIC

При добавлении пользователя с новым, ранее никому не назначенным, номером группы UIC важно указать учётное имя для этой группы для того, чтобы был правильно установлен идентификатор.

Пример неуказания учётного имени:

```
UAF> ADD FIN_USER1/UIC=[500,1]/PASSWORD=TESTING
%UAF-I-ADDMSG, user record successfully added
%UAF-I-RDBADDMSGU, identifier FIN_USER1 value: [000500,000001] added to
rights data base
UAF> SHOW FIN_USER1

Username: FIN_USER1                             Owner:
Account:                                        UIC:    [500,1] ([FIN_USER1])
        .
        .
        .
UAF>
```

В этом примере алфавитноцифровой формат UIC имеет только одну часть.

Для исправления этой ошибки запустите AUTHORIZE:

1. Удалите пользовательскую запись.
2. Создайте новую запись для пользователя, указывая учётное имя и UIC.

```
UAF> REMOVE FIN_USER1
%UAF-I-REMMSG, record removed from system authorization file
%UAF-I-RDBREMMSGU, identifier FIN_USER1 value: [000500,000001] removed from
rights data base
UAF> ADD FIN_USER/UIC=[500,1]/PASSWORD=TESTING/ACCOUNT=FINANCE
%UAF-I-ADDMSG, user record successfully added
%UAF-I-RDBADDMSGU, identifier FIN_USER1 value: [000500,000001] added to
rights data base
%UAF-I-RDBADDMSGU, identifier FINANCE value: [000500,177777] added to
rights data base
UAF> SHOW FIN_USER1

Username: FIN_USER1                             Owner:
Account:                                        UIC:    [500,1] ([FINANCE,FIN_USER1])
        .
        .
        .
UAF>
```

После того, как пользовательские идентификаторы установлены правильно, используйте команду MODIFY для установки других полей UAF, таких как устройство и каталог.

При добавлении пользователя в систему с помощью команды ADD, как минимум, должны быть указаны UIC и (если это первый пользователь в группе) учётное имя.

Хотя существуют другие способы добавления идентификатора без удаления пользователя, проще удалить и начать снова.

Пример явного добавления идентификатора:

```
UAF> ADD/IDENTIFIER/VALUE=UIC:[400,*] PER
%UAF-I-RDBADDMSGU, identifier PER value: [000400,177777] added to rights
data base
UAF>
```

Ошибка: неразрешение работы пользователя

Если в записи DEFAULT файла UAF установлен флаг DISUSER, новый пользователь унаследует этот флаг и работа нового пользователя будет запрещена.

Пример попытки войти в систему с использованием запрещённого счёта:

```
    Personnel System - Unathorized Access Prohibited

Username: USER1
Password:
User authorization failure
```

Для исправления этой ошибки запустите AUTHORIZE и удалите флаг DISUSER у пользовательской записи UAF.

```
UAF> MODIFY USER1/FLAG=NODISUSER
%UAF-I-MDFYMSG, user record(s) updated
UAF>
```

Ошибка: неуказание устройства и каталога по умолчанию

Если в записи UAF не указаны значения для устройства и каталога пользователя по умолчанию, они будут по умолчанию унаследуются из записи DEFAULT.

Пример ошибки:

```
$ DIRECTORY
%DIRECT-E-OPENIN, error opening $1$DUA0:[USER]*.*;* as
input
-RMS-E-DNF, directory not found
-SYSTEM-W-NOSUCHFILE, no such file
$
```

Для исправления этой ошибки запустите AUTHORIZE и модифицируйте пользовательскую запись, указав правильное устройство. (В утилите AUTHORIZE для устройств могут быть использованы логические имена.)

```
UAF> MODIFY
PER_USER7/DEVICE=WORK12/DIRECTORY=[PER_USER7]
%UAF-I-MDFYMSG, user record(s) updated
UAF>
```

Ошибка: неуказание владельца каталога

Если UIC пользователя не указан в качестве владельца пользовательского каталога по умолчанию, пользователь не сможет осуществлять запись в каталог из-за нарушения защиты файла каталога.

Пример ошибки администратора системы:

```
$ CREATE/DEIRCTORY WORK12:[PER_USER7]
$
```

Пример возникающей при этом у пользователя проблемы:

```
$ CREATE TEST.DAT
%CREATE-E-OPENOUT, error opening
WORK12:[PER_USER7]TEST.DAT; as output
-RMS-E-PRV, insufficient privilege or file protection
violation
$
```

Для исправления этой ошибки используйте любую из следующих команд для указания UIC пользователя в качестве владельца файла каталога.

- SET DIRECTORY/OWNER

  ```
  $ SET DIRECORY/OWNER=[400,7] WORK12:[PER_USER7]
  ```

  или

  ```
  $ SET DIRECTORY/OWNER=[PER_USER7] WORK12:[PER_USER7]
  ```

- SET FILE/OWNER

  ```
  $ SET FILE/OWNER=[400,7]
  WORK12:[000000]PER_USER7.DIR
  ```

  или

  ```
  $ SET FILE/OWNER=[PER_USER7]
  WORK12:[000000]PER_USER7.DIR
  ```

Ошибка: неверное расположение каталога пользователя

Если перед запуском AUTHORIZE системный администратор сделает каталогом по умолчанию SYS$SYSTEM и не укажет устройство при создании каталога, то каталог будет расположен под SYS$SYSROOT.

Пример ошибки системного администратора:

```
$ SET DEFAULT SYS$SYSTEM
$ RUN AUTHORIZE
        .
        .
        .
$ CREATE/DIRECTORY/OWNER=[11,2] [USER1]
$
```

Пример проблемы пользователя:

```
$ DIRECTORY
%DIRECT-E-OPENIN, error opening DISK$USER:[USER1]*.*;*
as input
-RMS-E-DNF, directory not found
-SYSTEM-W-NOSUCHFILE, no such file
$
```

Для исправления этой ошибки:

1. Удалите неправильно расположенный каталог.

   ```
   $ SET PROTECTION=S:REWD SYS$SYSROOT:[000000]USER1.DIR
   $ DELETE SYS$SYSROOT:[000000]USER1.DIR
   $
   ```

2. Создайте каталог вновь, указав верное устройство

```
$ CREATE/DIRECTORY/OWNER=[11,2] DISK$USER:[USER1]
$
```

или

```
$ CREATE/DIRE DIRECTORY/OWNER=[USER1]
DISK$USER:[USER1]
$
```

Ошибка: неустановка дисковой квоты

Если каталог нового пользователя находится на диске, на котором рарешены дисковые квоты, и для данного пользователя дисковая квота не установлена, при попытке пользователя создать файл возникнет следующая ошибка:

```
$ EDIT LOGIN.COM
%EDT-F-OPENOUT, error opening
DUSK$USER:[USER1]LOGIN.JOU; as output
-RMS-E-CRE, ACP file create failed
-SYSTEM-F-EXDISKQUOTA, disk quota exceeded
$
```

Для исправления этой ошибки запустите утилиту SYSMAN и используйте команду DISKQUOTA для установки пользовательской лисковой квоты.

6.6.4. Удаление пользователя системы

Процедура удаления пользователя в различных местах может отличаться в зависимости от политики обеспечения безопасности. Однако, все процедуры обычно имеют некоторые общие шаги:

1. Предотвращение входа пользователя в систему.
2. Удаление дисковых файлов из каталогов пользователя.
3. Удаление (если существуют) записей для UIC пользователя из файла дисковых квот.
4. Удаление (если существует) почтовой информации о пользователе.
5. Удаление записи о пользователе из UAF.

6.6.4.1. Предотвращение входа пользователя в систему.

Предотвращение входов в систему

Администратор системы должен предотвратить входы в систему с использованием пользовательского счёта перед удалением этого счёта. Таким образом, если процедура удаления пользователя будет прервана, информация о пользователе будет после этого всё ещё доступна.

Как предотвратить вход пользователя в систему

Существует два способа предотвратить вход пользователя в систему. С использованием утилиты AUTHORIZE произведите одно из следующих действий:

1. Измените пароль пользователя.

   Образец команды:

   ```
   UAF> MODIFY USER1/PASSWORD=SAYGOODBYE
   ```

2. Запретить работу пользователя.

Образец команды:

```
UAF> MODIFY USER1/FLAG=DISUSER
```

6.6.4.2. Удаление дисковых файлов из каталогов пользователя

Удаление файлов пользователя

Если пользователь удаляется из системы, системный администратор должен удалить все файлы, принадлежащие этому пользователю, по нескольким причинам:

- Дисковое пространство - Неиспользуемые файлы занимают место, которое могло бы быть использовано для активных файлов.
- Безопасность - Секретные файлы не должны оставаться в неактивном каталоге.
- Учёт - В некоторых местах назначается плата за дисковое пространство и услуги по резервному копированию.

Что делать с файлами пользователя

Решите, что делать с файлами пользователя перед тем, как Вы их удалите.

- В некоторых случаях Вы можете удалить всю структуру подкаталогов из домашнего каталога пользователя, а затем удалить и сам домашний каталог.
- Может возникнуть необходимость создать архивную копию файлов или переместить их в другой каталог системы.

Последовательность удаления файлов пользователя

Удаляйте файлы пользователя, начиная с нижнего уровня каталогов по направлению к верхнему.

1. Найдите и проверьте все подкаталоги с использованием команды DIRECTORY языка DCL.
2. Удалите все файлы в каждом подкаталоге и затем удалите сам подкаталог. Так как файлы каталогов защищены от удаления, код защиты должен быть изменён для разрешения удаления.
3. Удалите все файлы в каталоге верхнего уровня и затем удалите сам каталог.

Следующий пример показывает удаление каталога пользователя, который имеет два уровния подкаталогов.

Пример 6-19. Удаление файлов пользователя

```
❶ $ DIRECTORY DISK$USER:[USER1...]

   Directory DISK$USER:[USER1]

   LOGIN.COM;1      REPORTS.DIR;1

   Total of 2 files.

   Directory DISK$USER:[USER1.REPORTS]

   DATA.DIR;1       DECEMBER.RPT;1  NOVEMBER.RPT;1  OCTOBER.RPT;1

   Total of 4 files.

   Directory DISK$USER:[USER1.REPORTS.DATA]

   SALES.DAT;1
```

```
   Total of 1 file.

   Grand total of 3 directories, 7 files.
❷  $ DELETE/LOG DISK$USER:[USER1.REPORTS.DATA]*.*;*
   %DELETE-I-FILDEL, DISK$USER:[USER1.REPORTS.DATA]SALES.DAT;1 deleted (3
   blocks)
❸  $ SET PROTECTION=W:RWED DISK$USER:[USER1.REPORTS]DATA.DIR
❹  $ DELETE/LOG DISK$USER:[USER1.REPORTS]DATA.DIR;
   %DELETE-I-FILDEL, DISK$USER:[USER1.REPORTS]DATA.DIR;1 deleted (3 blocks)
❺  $ DELETE/LOG DISK$USER:[USER1.REPORTS]*.*;*
   %DELETE-I-FILDEL, DISK$USER:[USER1.REPORTS]DECEMBER.RPT;1 deleted (3
   blocks)
   %DELETE-I-FILDEL, DISK$USER:[USER1.REPORTS]NOVEMBER.RPT;1 deleted (3
   blocks)
   %DELETE-I-FILDEL, DISK$USER:[USER1.REPORTS]OCTOBER.RPT;1 deleted (3
   blocks)
❻  $ SET PROTECTION=W:RWED DISK$USER:[USER1]REPORTS.DIR
❼  $ DELETE/LOG DISK$USER:[USER1]REPORTS.DIR;
   %DELETE-I-FILDEL, DISK$USER:[USER1]REPORTS.DIR;1 deleted (3 blocks)
❽  $ DELETE/LOG DISK$USER:[USER1]*.*;*
   %DELETE-I-FILDEL, DISK$USER:[USER1]LOGIN.COM;1 deleted (3 blocks)
❾  $ SET PROTECTION=W:RWED DISK$USER:[000000]USER1.DIR
❿  $ DELETE/LOG DISK$USER:[000000]USER1.DIR;
   %DELETE-I-FILDEL, DISK$USER:[000000]USER1.DIR;1 deleted (3 blocks)
①  $ DIRECTORY DISK$USER:[USER1...]
   %DIRECT-E-OPENIN, error opening DISK$USER:[USER1...]*.*;* as input
   -RMS-E-DNF, directory not found
   -SYSTEM-W-NOSUCHFILE, no such file
   $
```

Пример 6-19, замечания:

❶ Найдите и проверьте все подкаталоги пользователя. В данном случае три каталога, содержащих всего семь файлов.

❷ Удалите все файлы из подкаталога самого нижнего уровня.

❸ Установите такую защиту на подкаталог нижнего уровня, чтобы его можно было удалить.

❹ Удалите подкаталог нижнего уровня.

❺ Удалите все файлы из подкаталога следующего снизу уровня.

❻ Установите такую защиту на подкаталог следующего снизу уровня, чтобы его можно было удалить.

❼ Удалите подкаталог следующего снизу уровня.

❽ Удалите все файлы из подкаталога самого верхнего уровня.

❾ Установите такую защиту на подкаталог верхнего уровня, чтобы его можно было удалить.

❿ Удалите подкаталог верхнего уровня.

① Проверьте, что структура каталогов пользователя удалена.

6.6.4.3. Удаление записей из файла квот

Запустите утилиту SYSMAN для удаления записей о дисковых квотах для пользовательского счёта.

Пример 6-20. Удаление записей из файла квот

```
$ SET PROCESS/PRIVILEGE=OPER
$ RUN SYS$SYSTEM:SYSMAN
SYSMAN> DISKQUOTA REMOVE [11,2] /DEVICE=DISK$USER
SYSMAN> EXIT
```

```
$
```

При работе с SYSMAN вместо UIC можно указывать идентификатор пользователя. Например:

```
SYSMAN> DISKQUOTA REMOVE [USER1] /DEVICE=DISK$USER
SYSMAN> EXIT
```

6.6.4.4. Удаление почтовой информации

Используйте команду REMOVE утилиты MAIL для удаления записи о пользовательском счёте.

Пример 6-21. Удаление почтовой информации о пользователе

```
$ MAIL
MAIL> REMOVE USER1
MAIL> EXIT
$
```

Для того, чтобы удалить запись почтового профиля, необходимо иметь привилегию SYSPRV.

Эта операция удаляет персональную информацию из файла SYS$SYSTEM:VMSMAIL_PROFILE.DATA.

6.6.4.5. Удаление записи из файла UAF

Используйте команду REMOVE утилиты AUTHORIZE для удаления записи из UAF. Это навсегда запретит вход пользователя в систему.

Пример 6-22. Удаление записи из файла UAF

```
$ SET DEFAULT SYS$SYSTEM
$ RUN AUTHORIZE
UAF> REMOVE USER1
%UAF-I-REMMSG, record removed from SYSUAF.DAT
%UAF-I-RDBREMMSGU, identifier USER1 value: [000011,000002] removed from
RIGHTSLIST.DAT
UAF> EXIT
%UAF-I-DONEMSG, system authorization file modified
%UAF-I-NAFNOMODS, no modification made to network authorization file
%UAF-I-RDBDONEMSG, rights data base modified
$
```

6.6.5. Управление процессами пользователей

Существует несколько способов, которыми системный администратор может определять, что может делать процесс пользователя.

Этот раздел рассматривает следующие темы:

- Установление пользовательских лимитов и привилегий
- Установление входных командных процедур
- Управление процессами
- Использование утилиты SYSMAN для управления процессами на других узлах.

6.6.5.1. Установление пользовательских лимитов и привилегий

Пользовательские лимиты и Пользовательские лимиты и привилегии управляются полями в пользовательской записи UAF.

привилегии

- Используйте команду ADD утилиты AUTHORIZE для указания первоначальных значений для этих полей при создании пользовательской записи в UAF.
- Используйте команду MODIFY утилиты AUTHORIZE для модифицирования этих полей у существующей пользовательской записи.
- Для получения списка всех полей, которые могут быть изменены, войдите в утилиту AUTHORIZE и наберите HELP MODIFY в ответ на подсказку.

Определяя пользовательские привилегии, системный администратор может ограничивать возможность пользователя воздействовать на операционную систему OpenVMS и на пользователей системы.

- Как правило, обычные пользователи имеют только привилегии TMPMBX и NETMBX, которые позволяют им создавать файлы и посылать почту.
- Приставка NO удаляет привилегию пользователя.
- Квалификатор /PRIVILIGES указывает, какие авторизованные привилегии имеет пользователь. Эти привилегии не обязательно включены при входе в систему.
- Квалификатор /DEFPRIVILEGES определяет, какие привилегии включены при входе в систему.
- Ключевое слово NOALL отключает все пользовательские привилегии.

Предоставление и удаление привилегий

Используйте команду MODIFY утилиты AUTHORIZE для модификации пользовательских привилегий.

- Для предоставления привилегии укажите /PRIVILIGE=*привилегия*.
- Для удаления привилегии укажите /PRIVILEGE=NO*привилегия*.

Пример 6-23 Предоставление и удаление привилегий

```
    $ SET DEFAULT SYS$SYSTEM
❶   $ RUN AUTHORIZE
❷   UAF> MODIFY USER1 /PRIVILEGE=OPER
    %UAF-I-MDFYMSG, user record(s) updated
❸   UAF> MODIFY USER2 /PRIVILEGE=NOOPER
    %UAF-I-MDFYMSG, user record(s) updated
    UAF> EXIT
    %UAF-I-DONEMSG, system authorization file modified
    %UAF-I-RDBNOMODS, no modifications made to rights
    data base
    $
```

Пример 6-23, замечания:

❶ Для предоставления и удаления привилегий используйте утилиту AUTHORIZE.

❷ Предоставьте пользователю USER1 привилегию OPER (оператор).

❸ Удалите привилегию OPER у пользователя USER2.

Установка лимитов

Определяя пользовательские лимиты, системный администратор

может ограничивать возможность пользователя использовать определённые системные ресурсы.

Используйте команду MODIFY утилиты AUTHORIZE для модификации пользовательских лимитов.

В некоторой документации лимиты называются также квотами. Не путайте лимиты с дисковыми квотами.

Пример 6-24. Установка пользовательских лимитов

```
$ SET DEFAULT SYS$SYSTEM
$ RUN AUTHORIZE
UAF> MODIFY USER1 /PRCLM=12
%UAF-I-MDFYMSG, user record(s) updated
UAF> EXIT
%UAF-I-DONEMSG, system authorization file modified
%UAF-I-RDBNOMODS, no modifications made to rights data
base
$
```

6.6.5.2. Указание входных командных процедур

Входные командные процедуры

Когда пользователь входит в систему OpenVMS, выполняется одна или несколько командных процедур.

- Системная входная командная процедура.
- Пользовательская входная командная процедура.

Системная входная командная процедура

Системная входная командная процедура устанавливает элементы вычислительной среды, которые являются общими для всех пользователей.

- Эта командная процедура выполняется для каждого интерактивного пользователя при входе его в систему.
- Системное логическое имя SYS$SYLOGIN указывает на эту командную процедуру.

Пользовательская входная командная процедура.

После завершения системной входной командной процедуры выполняется (если есть) собственная входная командная процедура пользователя.

Этот файл может быть указан полем LGICMD пользовательской записи в UAF.

По умолчанию имя файла LOGIN.COM.

По умолчанию этот файл расположен в пользовательском каталоге по умолчанию на пользовательском устройстве по умолчанию.

Системный администратор может указать другую командную процедуру для группы пользователей. Примером может служить студенческая группа или члены творческого коллектива.

В следующем примере для пользователя USER1 указана групповая входная командная процедура.

Пример 6-25. Указание входной командной процедуры

```
   $ SET DEFAULT SYS$SYSTEM
❶  $ RUN AUTHORIZE
❷  UAF> MODIFY FIN_USER1/LGICMD=WORK6:[FINANCE]GROUP_SETUP.COM
   %UAF-I-MDFYMSG, user record(s) updated
❸  UAF> SHOW FIN_USER1

   Username: FIN_USER1                Owner:
   Account:  FINANCE                  UIC:    [500,1] ([FINANCE,FIN_USER1])
   CLI:      DCL                      Tables: DCLTABLES
   Default:  WORK6:[FIN_USER1]
❹  LGICMD:   WORK6:[FINANCE]GROUP_SETUP.COM
       .
       .
       .
   UAF>
```

Пример 6-25, замечания:

❶ Используйте утилиту AUTHORIZE для определения входной командной процедуры для пользователя.

❷ Модифицируйте поле LGICMD в пользовательской записи UAF для определения входной процедуры.

❸ Выведите на экран пользовательскую запись UAF для проверки изменений.

❹ Поле LGICMD теперь указывает на определённый файл.

6.6.5.3. Управление процессами

Управление процессами

Изредка системному администратору может понадобиться манипулировать отдельными процессами в системе, когда:

- Процесс зациклился.
- Процесс использует чрезмерное количество ресурсов и должен быть остановлен.
- Пользователь породил несколько подпроцессов, которые должны разделять ресурсы и квоты, и один или несколько подпроцессов должны быть ыременно приостановлены для освобождения этих ресурсов для более важных задач.

Ограничение процессов

Есть три способа управлять процессами в системе:

- Приостановка выполнения
- Возобновление выполнения
- Удаление процесса

Привилегии, необходимые для управления процессами

Привилегии, необходимые для управления данным процессом могут быть разделены на три уровня, которые относятся на к методу защиты по коду UIC:

- Владелец (owner)
- Группа (group)
- Все (world)

Владелец — Пользователи могут всегда управлять своими собственными процессами и подпроцессами. Они могут быть созданы командами SPAWN или

RUN/DETACH.

Группа	Пользователи с привилегией GROUP могут управлять любыми процессами, которые несут на себе тот же групповой идентификатор UIC, что и их собственный процесс.
Все	Пользователи с првилегией WORLD могут управлять всеми процессами в системе. Обычно такая привилегия есть только у администратора системы.

Приостановка процесса

Используйте команду SET PROCESS/SUSPEND для приостановки процесса. Это на время приостановит активность процесса. Процесс остаётся приостановленным, пока другой процесс не возобновит его выполнение или не удалит его.

Формат:

SET PROCESS/SUSPEND/ID=*pid*

- PID - это идентификационный номер процесса, который должен быть приостановлен.
- Привилегия GROUP необходима для приостановки другого процесса в той же группе UIC.
- Привилегия WORLD необходима для приостановки процесса за пределами Вашей группы UIC.

Если процесс находится в одной с Вами группе UIC, можно использовать следующую команду:

SET PROCESS/SUSPEND *имя_процесса*

В следующем примере приостанавливается процесс, принадлежащий пользователю USER13.

Пример 6-26. Приостановка выполнения процесса

```
❶  $ SHOW SYSTEM
   VAX/VMS V6.0 on node NEAT  25-jun-1993 09:39:45.11   Uptime  12 21:16:05
     Pid    Process Name  State  Pri   I/O     CPU        Page flts Ph.mem
❷  2020071E USER13        COM      4  1942  0 00:00:56.48      6196    346
       .
       .
       .
❸  $ SET PROCESS/SUSPEND/ID=2020071E
❹  $ SHOW SYSTEM
   VAX/VMS V6.0 on node NEAT  25-jun-1993 09:39:45.11   Uptime  12 21:16:05
     Pid    Process Name  State  Pri   I/O     CPU        Page flts Ph.mem
❺  2020071E USER13        SUSP     7  3010  0 00:01:15.81      7291    345
       .
       .
       .
   $
```

Пример 6-26, замечания:

❶ Используйте команду SHOW SYSTEM для вывода на экран кода идентификации (PID) процесса, который должен быть приостановлен.

❷ Обратите внимание на PID процесса.

❸ Используйте команду SET PROCESS/SUSPEND, указывая PID, для приостановки процесса.

❹ Используйте команду SHOW SYSTEM для проверки того, что процесс приостановлен.

❺ Состояние процесса в списке - SUSP, это показывает, что процесс приостановлен.

Возобновление выполнения процесса

Используйте команду SET PROCESS/RESUME для возобновления выполнения процесса.

Формат:

SET PROCESS/RESUME/ID=*pid*

- PID - это идентификационный номер процесса, выполнение которого должно быть возобновлено.
- Привилегия GROUP необходима для возобновления выполнения другого процесса в той же группе UIC.
- Привилегия WORLD необходима для возобновления выполнения процесса за пределами Вашей группы UIC.

Если процесс находится в одной с Вами группе UIC, можно использовать следующую команду:

SET PROCESS/RESUME *имя_процесса*

В следующем примере возобновляется выполнение процесса, принадлежащего пользователю USER13.

Пример 6-27. Возобновление выполнения процесса.

```
❶  $ SHOW SYSTEM
   VAX/VMS V6.0 on node NEAT  25-JUN-1993 09:39:45.11   Uptime  12 21:16:05
     Pid    Process Name  State  Pri   I/O     CPU         Page flts Ph.mem
❷  2020071E USER13        SUSP     4  1942  0 00:00:56.48      6196    346
        .
        .
        .
❸  $ SET PROCESS/RESUME/ID=2020071E
❹  $ SHOW SYSTEM
   VAX/VMS V6.0 on node NEAT  25-jun-1993 09:39:45.11   Uptime  12 21:16:05
     Pid    Process Name  State  Pri   I/O     CPU         Page flts Ph.mem
❺  2020071E USER13        COM      7  3010  0 00:01:15.81      7291    345
        .
        .
        .
   $
```

Пример 6-27, замечания:

❶ Используйте команду SHOW SYSTEM для вывода на экран кода идентификации (PID) процесса, выполнение которого должно быть возобновлено.

❷ Состояние процесса SUSP. Обратите внимание на PID процесса.

❸ Используйте команду SET PROCESS/RESUME, указывая PID, для возобновления выполнения процесса.

❹ Используйте команду SHOW SYSTEM для проверки того, что выполнение процесса взобновлено.

❺ Состояние процесса в списке - COM, это показывает, что процесс больше не приостановлен.

Удаление процесса

Используйте команду STOP для удаления процесса.

Формат:

STOP/ID=*pid*

- PID - это идентификационный номер процесса, который должен быть удалён.
- Привилегия GROUP необходима для удаления другого процесса в той же группе UIC.
- Привилегия WORLD необходима для удаления процесса за пределами Вашей группы UIC.

Если процесс находится в одной с Вами группе UIC, можно использовать следующую команду:

STOP *имя_процесса*

В следующем примере удаляется процесс, принадлежащий пользователю USER13.

Пример 6-28. Удаление процесса

```
❶  $ SHOW SYSTEM
   VAX/VMS V6.0 on node NEAT  25-JUN-1993 09:39:45.11   Uptime  12 21:16:05
     Pid    Process Name  State  Pri   I/O     CPU        Page flts Ph.mem
❷  2020071E USER13        COM      4  1942  0 00:00:56.48      6196    346
        .
        .
        .
❸  $ STOP/ID=2020071E
❹  $ SHOW SYSTEM
   VAX/VMS V6.0 on node NEAT  25-jun-1993 09:39:45.11   Uptime  12 21:16:05
❺    Pid    Process Name  State  Pri   I/O     CPU        Page flts Ph.mem
        .
        .
        .
   $
```

Пример 6-28, замечания:

❶ Используйте команду SHOW SYSTEM для вывода на экран кода идентификации (PID) процесса, который должен быть удалён.

❷ Обратите внимание на PID процесса.

❸ Используйте команду STOP, указывая PID, для удаления процесса.

❹ Используйте команду SHOW SYSTEM для проверки того, что процесс удалён.

❺ Процесс не показан в списке, выданном по команде SHOW SYSTEM.

6.6.5.4. Использование утилиты SYSMAN для управления процессами на других узлах

Утилита SYSMAN

Утилита управления системой SYSMAN (System Management Utility) позволяет с локального узла выполнять задачи управления системой на разных узлах и кластерах. Системный администратор может определять среду управления (любой узел или кластер, доступный через программное обеспечение DECnet) и выполнять в этой среде задачи системного управления.

Запуск утилиты SYSMAN

Для запуска утилиты SYSMAN введите следующую команду:

RUN SYS$SYSTEM:SYSMAN

Для запуска утилиты SYSMAN Вы должны иметь привилегию OPER на локальном узле и авторизованную привилегию OPER или SYSPRV на удалённом узле.

Для выхода из утилиты SYSMAN наберите EXIT или нажмите CTRL/Z.

Установка среды утилиты SYSMAN

Используйте команду SET ENVIRONMENT утилиты SYSMAN для установки среды применения последующих команд. Среда может быть:

- Любой другой узел в кластере
- Весь кластер
- Любой узел или кластер в сети

Эта команда требует привилегию OPER или SETPRV на всех узлах желаемой среды.

Формат:

SET ENVIRONMENT/*квалификатор(ы)*

Действующие квалификаторы:

I. /CLUSTER

A. Среда управления по умолчанию - локальный кластер. Указавайте нелокальный кластер, называя один член этого кластера с помощью квалификатора /NODE.

II. /NODE=(*узел1,узел2,...*)

A. Именем узла может быть или имя системы, или кластерный псевдоним (cluster alias).

III. /USERNAME=*имя_пользователя*

A. Указывает имя пользователя, которое должно использоваться для доступа к удалённому узлу. Если не указано, используется текущее имя пользователя.

Используйте команду SHOW ENVIRONMENT для просмотра текущей среды.

Некоторые команды DCL (такие как MOUNT/CLUSTER, SET QUORUM/CLUSTER) действуют на весь кластер по своему назначению. Во избежание чрезмерного выполнения таких команд в утилите SYSMAN определите в качестве среды один узел внутри кластера.

Установка профиля SYSMAN

Используйте команду SET PROFILE для временного изменения текущих привилегий, устройства по умолчанию и каталога по умолчанию в текущей среде SYSMAN. Профиль действует, пока Вы его не измените, переустановите среду или выйдете из утилиты SYSMAN.

Формат:

SET PROFILE/*квалификатор(ы)*

Действующие квалификаторы:

- /DEFAULT=*устройство*:[*каталог*]

  Указывает диск и каталог по умолчанию для использования в текущей среде.

- /PRIVILEGES=(*прив1,прив2,...*)

  Указывает привилегии, которые должны быть добавлены к текущим привилегиям. Любые дополнительные привилегии должны быть авторизованы.

Используйте команду SHOW PROFILE для просмотра текущего профиля.

Первоначальная реализация SYSMAN была создана для кластеров. В кластере Вам необязательно устанавливать профиль для себя.

Выполнение команд DCL в среде кластера

Используйте команду DO утилиты SYSMAN для выполнения команды DCL или командной процедуры на всех узлах текущей среды.

Формат:

DO[/OUTPUT[=*спецификация_файла*]] *командная_строка*

- Необязательный квалификатор /OUTPUT используется для записи выходной информации команды в файл. По умолчанию,

спецификация_файла SYSMAN.LIS в текущем каталоге на текущем устройстве по умолчанию.

- Параметр *командная_строка* указывает командную строку, которую должен выполнить DCL.

Эта команда требует привилегий той команды DCL, которая должна быть выполнена.

Следующий пример демонстрирует команды SYSMAN, используемые для выполнения различных задач на других узлах.

Пример 6-29. Выполнение команд на других узлах

```
❶  $ SET PROCESS/PRIVILEGE=OPER
❷  $ RUN SYS$SYSTEM:SYSMAN

❸  SYSMAN> SET ENVIRONMENT/CLUSTER/NODE=NEAT
   Remote password:
   %SYSMAN-I-ENV, current command environment:
    Clusterwide on remote cluster NEAT
    Username MGR1         will be used on nonlocal nodes

❹  SYSMAN> SHOW ENVIRONMENT
   %SYSMAN-I-ENV, current command environment:
    Clusterwide on remote cluster NEAT
    Username MGR1         will be used on nonlocal nodes

❺  SYSMAN> SET PROFILE/PRIVILEGE=SYSPRV

❻  SYSMAN> SHOW PROFILE
   %SYSMAN-I-DEFDIR, default directory on node NEAT -- $1$DUA1:[MGR1]
   %SYSMAN-I-DEFPRIV, process privileges on node NEAT --
   SETPRV
   TMPMBX
   NETMBX
   SYSPRV
   %SYSMAN-I-DEFDIR, default directory on node TIDY -- $1$DUA1:[MGR1]
   %SYSMAN-I-DEFPRIV, process privileges on node TIDY --
   SETPRV
   TMPMBX
   NETMBX
   SYSPRV
      .
      .
      .
❼  SYSMAN> DO SHOW SYSTEM
   %SYSMAN-I-OUTPUT, command execution on node NEAT
   VAX/VMS V6.0 on node NEAT  25-JUN-1993 15:00:20.57   Uptime   3 14:04:12
     Pid    Process Name  State  Pri   I/O     CPU        Page flts Ph.mem
   20200081 SWAPPER       HIB     16     0  0 00:00:29.76         0      0
      .
      .
      .
   %SYSMAN-I-OUTPUT, command execution on node TIDY
   VAX/VMS V6.0 on node TIDY  25-JUN-1993 15:00:08.76   Uptime   3 12:49:29
     Pid    Process Name  State  Pri   I/O     CPU        Page flts Ph.mem
   40600041 SWAPPER       HIB     16     0  0 00:00:10.97         0      0
      .
      .
      .
❽  SYSMAN> EXIT
   $
```

Пример 6-29, замечания:

❶ Для запуска утилиты SYSMAN требуется привилегия OPER.

❷ Запустите утилиту SYSMAN.

❸ Установите текущую среду как кластер. содержащий узел NEAT. Так как это не локальный кластер, требуется пароль.

❹ Посмотрите текущую среду.

❺ Добавьте привилегию к текущему профилю.

❻ Посмотрите текущий профиль. Информация будет показана отдельно для каждого узла среды.

❼ Используйте команду DO для выполнения команды DCL на каждом узле среды. Каждая команда полностью выполняется перед тем, как SYSMAN пошлёт команду на следующий узел.

❽ Выйдите из утилиты SYSMAN.

Каждая команда DO выполняется как независимый процесс, поэтому никакой контекст процесса не сохраняется между командами DO. По этой причине Вы должны выразить все команды DCL в одной командной строке и не должны запускать программы, ожидающие ввод информации.

6.6.6. Управление использованием дискового пространства

Эффективное использование дискового пространства - одна из задач системного администратора. Она включает в себя:

- Удаление старых версий файлов
- Установка лимитов версий для каталогов
- Наблюдение за использованием дискового пространства (мониторинг)
- Управление дисковыми квотами

6.6.6.1. Удаление старых версий файлов

Старые версии файлов

Устаревшие версии системных протокольных файлов должны периодически вычищаться.

Системные файлы, подлежащие чистке

Файл протокола оператора SYS$MANAGER:OPERATOR.LOG

- Новая версия этого файла создаётся каждый раз при перезагрузке системы. Устаревшие версии должны удаляться после создания резервных копий.
- Если файл протокола оператора очень разросся, используйте команду REPLY/LOG для создания новой версии, чтобы старую можно было скопировать и удалить.

Файл протокола ошибок SYS$ERRORLOG:ERRLOG.SYS

- Этот файл остаётся на диске до тех пор, пока не будет явно удалён или переименован.
- Для освобождения места на системном диске этот файл должен каждый день переименовываться, с него должна делаться резервная копия на другой том, а затем он должен быть удалён.

Файл учёта использования системных ресурсов SYS$MANAGER:ACCOUNTNG.DAT

- Этот файл всё время растёт, если разрешён учёт ресурсов.
- Создайте новый учётной файл с помощью команды SET ACCOUNTING/NEW_FILE языка DCL. Затем сделайте резервную копию и удалите старый файл.

6.6.6.2. Установка лимита версий для каталогов

Лимиты версий в каталогах

Для ограничения количества версий файлов, которые могут быть созданы в каталоге пользователя, установите для каталога лимит версий.

- Это может быть сделано при создании каталога или для уже

существующего каталога.

- Лимит версий для каталога указывает общее количество версий, которые может иметь файл в этом каталоге.
- Когда лимит версий израсходован, наиболее ранняя версия файла удаляется из каталога без уведомления пользователя.

Установка лимита версий при создании каталога

Используйте команду CREATE/DIRECTORY для установке лимита версий на каталог при его создании. Этот лимит становится лимитом по умолчанию для всех подкаталогов, создаваемых ниже этого каталога.

Формат:

CREATE/DIRECTORY/VERSION_LIMIT=*n спец_каталога*

- Значение *n* - это общее количество версий, которое может иметь файл в указанном каталоге. Значение 0 (по умолчанию) указывает, что количество версий ограничено архитектурным пределом 32767.
- *Спец_каталога* - спецификация каталога, который должен быть создан. Шаблонные символы в спецификации не разрешены.

Для указания владельца каталога может быть использован идентификатор:

```
$ CREATE/DIRECTORY/VERSION_LIMIT=3/OWNER=[USER1] -
_$ WORK6:[USER1]
```

Пример 6-30 показывает создание каталога с лимитом версий 3

Пример 6-30. Установка лимита версий при создании каталога

```
❶  $ CREATE/DIRECTORY/VERSION_LIMIT=3/OWNER=[500,1] WORK6:[FIN_USER1]
❷  $ DIRECTORY/FULL WORK6:[000000]FIN_USER1.DIR

   Directory WORK6:[000000]

   FIN_USER1.DIR;1                File ID:  (3696,14,0)
   Size:          1/3             Owner:    [FINANCE,FIN_USER1]
   Created:  25-JUN-1993 16:49:46.93
   Revised:  25-JUN-1993 16:49:47.17 (1)
   Expires:   <None specified>
   Backup:    <No backup recorded>
   File organization:  Sequential
   File attributes:    Allocation: 3, Extend: 0, Global buffer count: 0
❸                      Default version limit: 3, Contiguous, Directory file
       .
       .
       .
   $
```

Пример 6-30, замечания:

❶ Создайте каталог с лимитом версий, равном 3. Не забудьте указать владельца каталога.

❷ Используйте команду DIRECTORY/FULL, чтобы увидеть детальную информацию о каталоге.

❸ Каталог имеет лимит версий, равный 3. Этот лимит версий будет лимитом по умолчанию для всех подкаталогов, создаваемых ниже этого каталога.

Установка лимита версий для существующего

Используйте команду SET DIRECTORY для установки лимита версмй на уже существующий каталог. Если Вы измените лимит версий для каталога, новое значение подействует толко на файлы, созданные

каталога

после совершения этого изменения.

Формат:

SET DIRECTORY/VERSION_LIMIT=*n спец_каталога*

- Величина *n* - это общее количество версий, которое может иметь файл в указанном каталоге. Значение 0 (по умолчанию) указывает, что количество версий ограничено архитектурным пределом 32767.
- *Спец_каталога* - спецификация каталога, который должен быть модифицирован. Шаблонные символы в спецификации разрешены.

Пример 6-31 устанавливает лимит версий 3 на существующий каталог.

Пример 6-31. Установка лимита версий на существующий каталог

```
❶  $ DIRECTORY/FULL DISK$USER:[000000]USER1.DIR

   Directory DISK$USER:[000000]

   USER1.DIR;1                        File ID:   (260,15,0)
   Size:           1/3                Owner:     [GRP11,USER1]
   Created:  24-JUN-1993 14:26:11.82
   Revised:  24-JUN-1993 14:54:53.91 (3)
   Expires:   <None specified>
   Backup:   25-JUN-1993 17:57:32.02
   File organization:  Sequential
   File attributes:    Allocation: 3, Extend: 0, Global buffer count: 0
❷                      No default version limit, Contiguous, Directory file
      .
      .
      .
❸  $ SET DIRECTORY/VERSION_LIMIT=3 DISK$USER:[USER1]
❹  $ DIRECTORY/FULL DISK$USER:[000000]USER1.DIR

   Directory DISK$USER:[000000]

   USER1.DIR;1                        File ID:   (260,15,0)
   Size:           1/3                Owner:     [GRP11,USER1]
   Created:  24-JUN-1993 14:26:11.82
   Revised:  24-JUN-1993 16:35:26.18 (4)
   Expires:   <None specified>
   Backup:   25-JUN-1993 17:57:32.02
   File organization:  Sequential
   File attributes:    Allocation: 3, Extend: 0, Global buffer count: 0
❺                      Default version limit: 3, Contiguous, Directory file
      .
      .
      .
   $
```

Пример 6-31, замечания:

❶ Используйте команду DIRECTORY/FULL, для того, чтобы увидеть детальную информацию о каталоге пользователя.

❷ У каталога не установлен лимит версий.

❸ Установите каталогу лимит версий, равный 3.

❹ Выведите на экран информацию о каталоге.

❺ Каталог теперь имеет лимит версий, равный 3.

Заметьте, что этот лимит версий не влияет на файлы, уже существующие в каталоге. Он будет действовать только на файлы, созданные после назначения лимита версий.

6.6.6.3. Наблюдение за использованием дискового пространства

Наблюдение за дисковым пространством

Системный администратор должен наблюдать за дисками, чтобы отслеживать количество доступного дискового пространства в системе. Используйте команду SHOW DEVICE языка DCL для просмотра количества свободных блоков на одном или нескольких дисках.

Следующий пример показывает информацию об устройстве DUA2:.

Пример 6-32. Вывод информации об определённом дисковом устройстве

```
$ SHOW DEVICE DUA2

Device                  Device      Error     Volume         Free   Trans Mnt
 Name                   Status      Count      Label        Blocks  Count Cnt
$1$DUA2:    (TIDY)     Mounted         0   USER2           478797      1  11
$
```

Следующий пример показывает информацию об устройствах класса DU.

Пример 6-33. Вывод информации о группе дисковых устройств

```
$ SHOW DEVICE DU

Device                  Device      Error     Volume         Free   Trans Mnt
 Name                   Status      Count      Label        Blocks  Count Cnt
NEAT$DUA0:              Mounted         0   (remote mount)                  1
$1$DUA0:    (TIDY)     Mounted         0   VAXVMSRL055     120876    260  11
$1$DUA1:    (TIDY)     Mounted         0   TESTSPACE       475365      1  11
$1$DUA2:    (TIDY)     Mounted         0   USER2           478797      1  11
$1$DUB0:    (TIDY)     Online          0
$
```

Действия при нехватке дискового пространства

Если количество свободных блоков на диске недостаточно, можно предпринять следующие действия:

- Почистите файлы. Это может привести к удалению старых версмй файлов, которые пользователь не хотел бы терять.
- Переместите некоторые пользовательские каталоги на другой диск. Не забудьте модифицировать соответсвующие пользовательские записи в UAF для указания нового устройства по умолчанию.
- Заархивируйте старые файлы, к которым определённое время никто не обращался.
- Замените дисковод на устройство большей ёмкости.

Важно ежедневно следить за дисками, чтобы быть уверенным , что они не слишком заполнены. Если диск не содержит очень нестабильное количество информации, он обычно не должен быть заполнен больше чем на 80%.

Обучение пользователей грамотному использованию дискового пространства

Системный администратор должен обучать пользователей правильно использовать дисковое пространство.

- Информируйте пользователей о расписании резервного копирования. Осознание того, что файл может быть при необходимости восстановлен, побудит пользователей к удалению ненужных файлов.
- Учите пользователей регулярно чистить свои каталоги.
- Учите пользователей удалять ненужные файлы, такие как файлы протоколов пакетных заданий и старые листнги компиляторов.

6.6.6.4. Управление дисковыми квотами

Управление дисковыми квотами

Для установки и управления дисковыми квотами системный администратор должен делать следующее:

- Создать файл квот на диске, не имеющем квот
- Разрешить использование файла квот (это делается автоматически при создании файла квот)
- Установить дисковую квоту для каждого UIC, использующего этот диск.

Создание и модификация файла дисковых квот

Файл квот, [000000]QUOTA.SYS, управляет дисковыми квтами того тома, на котором он расположен.

Используйте команду DISKQOUTA утилиты SYSMAN для создания и модификации файла QUOTA.SYS.

Для того,чтобы...	*Используйте команду утилиты SYSMAN:*
Создать файл квот и разрешить его использование	`DISKQUOTA CREATE`
Посмотреть запись о квоте	`DISKQUOTA SHOW`
Добавить запись о квоте	`DISKQUOTA ADD`
Модифицировать запись о квоте	`DISKQUOTA MODIFY`
Удалить запись о квоте	`DISKQUOTA DELETE`
Приостановить проверку соблюдения дисковых квот	`DISKQUOTA DISABLE`
Возобновить проверку соблюдения дисковых квот	`DISKQUOTA ENABLE`
Обновить данные в файле квот на диске, уже имеющем файлы	`DISKQUOTA REBUILD`

Digital рекомендует не использовать и не создавать файл квот на системном диске.

Дисковые квоты по умолчанию

Установите значения по умолчанию для квот и перерасходов путём модификации записи квот для UIC [0,0]. Эти значения будут использованы для пользовательских записей, если не указаны другие значения.

В следующем примере системный администратор создаёт файл дисковых квот, устанавливает значения по умолчанию путём модификации записи для UIC [0,0] и добавляет запись о квоте.

Пример 6-34. Управление дисковыми квотами

```
❶ SYSMAN> DISKQUOTA CREATE /DEVICE=$1$DUA1:
❷ SYSMAN> DISKQUOTA MODIFY [0,0] /DEVICE=$1$DUA1: -
  _SYSMAN> /PERMQUOTA=2000 /OVERDRAFT=200
❸ SYSMAN> DISKQUOTA ADD [11,7] /DEVICE=$1$DUA1:
❹ SYSMAN> DISKQUOTA SHOW [11,7] /DEVICE=$1$DUA1:

  %SYSMAN-I-QUOTA, disk quota statistics on device $1$DUA1: -- Node TIDY
       UIC                  Usage        Permanent Quota   Overdraft Limit
  [11,7]                    0            2000              200

  SYSMAN>
```

Пример 6-34, замечания:

❶ Создайте файл квот на диске 1DUA1:.

❷ Модифицируйте запись квот для [0,0], чтобы установить новые значения по умолчанию для 1DUA1:.

❸ Добавьте запись квот для [11,7]. Так как при этом не указаны значения квот, использованы значения по умолчанию.

❹ Посмотрите запись квот для [11,7]. Использованы значения для [0,0].

6.7. Выводы

Защита Ваших данных

- Каждый из Ваших файлов имеет код идентификации пользователя (UIC) и код защиты, которые вместе служат для определения разрешённого типа доступа.
- Вы можете использовать команды DCL для просмотра и изменения защиты Ваших файлов.
- Для уничтожения информации файла после его удаления используйте команду DELETE/ERASE или PURGE/ERASE.
- Архивирование и регулярное резервирование файлов поможет защитить данные от потери или порчи.

Использование утилиты AUTHORIZE

- Файл авторизации пользователей (UAF) определяет характеристики каждого пользовательского процесса, включая устройство и каталог по умолчанию, UIC и лимиты.
- Для работы с UAF используйте утилиту AUTHORIZE.
- Используйте команду HELP утилиты AUTHORIZE для получения информации о командах и квалификаторах этой утилиты.
- Для просмотра отдельных записей UAF используйте команду SHOW утилиты AUTHORIZE.
- Утилита AUTHORIZE используется для получения списка счтов пользователей как на экране терминала, так и в файле.

Добавление пользователя к системе

- Перед добавлением пользователя к системе выберите:
  - Имя пользователя
  - Пароль
  - Код идентификации пользователя (UIC)
  - Устройство по умолчанию
  - Каталог по умолчанию
  - Учётное имя.
- Для добавления записи к файлу авторизации пользователей используйте утилиту AUTHORIZE.
- Для установки дисковой квоты для пользователя используйте утилиту SYSMAN.
- При добавлении пользователя к системе используйте команду CREATE/DIRECTORY для создания каталога, соответствующего полю DEFAULT записи UAF.
- Рекомендуется, чтобы администратор системы проверил пользовательский счёт прежде, чем позволит пользователю получить к нему доступ.
- Для добавления пользователей к системе можно использовать командную процедуру ADDUSER.COM.

Удаление пользовательского счёта

- Для предотвращения входа пользователя в систему используйте утилиту AUTHORIZE и:
  - Измените пароль пользователя

    или
  - Запретите работу пользователя
- Если пользователь удаляется из системы, системный администратор должен удалить все файлы, остающиеся на его счету.
- Используйте утилиту SYSMAN для удаления записей о дисковых квотах для данного пользователя.
- Используйте команду REMOVE утилиты MAIL для удаления записи о пользователе.
- Используйте команду REMOVE утилиты AUTHORIZE для удаления записи из UAF.

Управление процессами пользователей

- Лимиты, квоты и значения по умолчанию, которые записаны в UAF, можно изменить с помощью утилиты AUTHORIZE.
- Операционная система OpenVMS выполняет до двух командных процедур при входе пользователя в систему. Первая из них - обычно общесистемная процедура, выполняемая для всех рлдьзователей.
- Отдельные процессы могут быть приостановлены, возобновлены или удалены администратором системы.
- Задачи управления системой, такие, как управление процессами пользователей, могут выполняться на других узлах вычислительной сети с помощью утилиты SYSMAN.

Управление использованием дискового пространства

- Устаревшие версии системных протокольных файлов должны периодически подвергаться чистке.
- Для ограничения количества версий файлов, которые могут быть созданы в каталоге пользователя, наложите на каталог лимит версий.
- Лимит версий каталога определяет общее количество версий, которое может иметь файл в этом каталоге.
- Когда лимит версий истекает, самая ранняя версия файла удаляется из каталога без уведомления пользователя.
- Системный администратор должен следить за дисковым пространством, чтобы знать количество дискового пространства, доступного системе.
- Для установки и управления дисковыми квотами, проделайте следующее:
  - Создайте файл квот на диске, на котором должны действовать квоты.
  - Разрешите использование файла квот (выполняется автоматически при создании файла квот).
  - Установите дисковую квоту для каждого UIC, который использует этот диск.
- Файл квот [000000]QUOTA.SYS управляет дисковыми квотами того тома, на котором он расположен.
- Используйте команду DISKQUOTA утилиты SYSMAN для создания и модифицирования QUOTA.SYS.

6.8. Письменные упражнения

6.8.1. Защита каталогов

Рядом с каждой операцией, относящейся к каталогам, поставьте букву, соответствующую команде VMS, наилучшим образом подходящей для выполнения задания. Вы можете некоторые команды использовать несколько раз, а другие - ни разу.

Операции	*Команды*
___ Изменить код защиты файла каталога	a. DELETE
___ Переместить файлы из одного каталога в другой	b. DIRECTORY
___ Удалить каталог из иерархии каталогов	c. RENAME
	d. SET PROTECTION
	e. SHOW PROTECTION

6.8.2. Коды защиты

Представьте, что Вы хотите получить доступ к файлу, код защиты которого приведен ниже:

S:RWE,O:RWED,G:RE,W:R

Допустим, что файл не имеет защиты по ACL. Завершите следующую таблицу, показывающую тип доступа, который Вы можете получить к этому файлу, если Ваш UIC совпадает с указанным. Для Вас заполнены первые три строки.

UIC файла	*Ваш UIC*	*Тип доступа, который Вы можете получить*
[132,10]	[2,25]	Read, Write, Execute (Вы "System")
[5,15]	[100,10]	Read (Вы "World")
[150,10]	[150,11]	Read, Execute (Вы "Group")
[200,5]	[100,5]	_____
[300,5]	[300,10]	_____
[105,6]	[5,16]	_____
[10,5]	[105,6]	_____
[202,15]	[202,15]	_____
[307,5]	[2,25]	_____

6.9. Решения к письменным упражнениям

6.9.1. Защита каталогов

Рядом с каждой операцией, относящейся к каталогам, поставьте букву, соответствующую команде VMS, наилучшим образом подходящей для выполнения задания. Вы можете некоторые команды использовать несколько раз, а другие - ни разу.

Операции		*Команды*
d	Изменить код защиты файла каталога	a. DELETE
c	Переместить файлы из одного каталога в другой	b. DIRECTORY
a	Удалить каталог из иерархии каталогов	c. RENAME
		d. SET PROTECTION
		e. SHOW PROTECTION

6.9.2. Коды защиты

Представьте, что Вы хотите получить доступ к файлу, код защиты которого приведен ниже:

S:RWE,O:RWED,G:RE,W:R

Допустим, что файл не имеет защиты по ACL. Завершите следующую таблицу, показывающую тип доступа, который Вы можете получить к этому файлу, если Ваш UIC совпадает с указанным. Для Вас заполнены первые три строки.

UIC файла	*Ваш UIC*	*Тип доступа, который Вы можете получить*
[132,10]	[2,25]	Read, Write, Execute (Вы "System")
[5,15]	[100,10]	Read (Вы "World")
[150,10]	[150,11]	Read, Execute (Вы "Group")
[200,5]	[100,5]	Read (Вы "World")
[300,5]	[300,10]	Read, Execute (Вы "Group")
[105,6]	[5,16]	Read, Write, Execute (Вы "System")
[10,5]	[105,6]	Read (Вы "World")

[202,15]	[202,15]	Read, Write, Execute, Delete (Вы “Owner”)
[307,5]	[2,25]	Read, Write, Execute (Вы “System”)