

Закрывое акционерное общество

"АСТРА СТ"

ТЕРМИНАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ

СИСТЕМА «MIRAGE»

Руководство по КСЗ

АСТР.51240-01 90 01

Листов 56

## АННОТАЦИЯ

Документ предназначен для сотрудников, выполняющих функции системного администратора или администратора безопасности в TBC Mirage.

Данный документ содержит инструкции, необходимые администратору для установки и конфигурирования системы. Приводится описание параметров системы, влияющих на её функционирование. Описывается порядок и технические средства для регистрации отпечатков пальцев пользователей. Приводится описание программных средств архивирования журнала событий, средств архивного копирования и восстановления системы в случае сбоев.

## СОДЕРЖАНИЕ

1. ФУНКЦИИ АДМИНИСТРАТОРА В MIRAGE.....	5
1.1 Функции системного администратора в системе.....	5
1.2 Функции администратора безопасности в системе.....	5
2. УСТАНОВКА СИСТЕМЫ.....	7
2.1 Требования к программному и аппаратному обеспечению сервера.....	7
2.2 Перечень установочных пакетов.....	7
2.3 Порядок действий по установке системы.....	8
2.4 Режимы работы серверов Mirage.....	9
2.4.1 Нормальный режим.....	9
2.4.2 Режим конфигурирования.....	9
2.4.3 Выбор режима работы.....	10
2.5 Первоначальное конфигурирование системы.....	11
2.5.1 Подключение к служебной базе данных.....	12
2.5.2 Сервис загрузки терминалов.....	13
2.5.3 Сервис печати.....	14
2.5.4 Терминал администратора.....	15
2.5.5 Параметры системы.....	17
2.5.6 Регистрационный номер.....	18
2.5.7 Восстановление.....	18
2.5.8 Перезагрузка.....	19
3. КОНФИГУРИРОВАНИЕ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА.....	20
3.1 Конфигурирование учётных записей.....	20
3.1.2 Создание учётных записей.....	20
3.1.3 Редактирование учётных записей.....	25
3.1.4 Удаление учётных записей.....	25
3.1.5 Блокирование и разблокирование учётных записей пользователей.....	26
3.2 Предусмотренные пользователи и группы пользователей.....	27
3.3 Отпечатки пальцев пользователей.....	28
3.3.1 Регистрация образцов.....	29
3.3.2 Удаление образцов.....	30
3.3 Конфигурирование дискреционных прав доступа.....	30

3.4.1	Обозначения связей.....	31
3.4.2	Создание связей.....	33
3.4.2	Изменение дискреционных прав доступа.....	35
3.4.3	Удаление связей.....	35
3.4	Пользователи и группы пользователей.....	36
3.5	Конфигурирование мандатных прав доступа.....	36
3.6	Конфигурирование шаблонов документов.....	38
3.6.1	Создание шаблона документа.....	39
3.6.2	Редактирование шаблона документа.....	39
3.6.3	Удаление шаблона документа.....	39
3.6.4	Предустановленные шаблоны документов.....	40
3.7	Отчёты по конфигурации.....	40
4.	МОНИТОРИНГ СИСТЕМЫ.....	42
4.1	Мониторинг сеансов.....	42
4.2	Мониторинг принтеров.....	43
4.3	Мониторинг серверов.....	44
4.4	Мониторинг критических событий.....	45
5.	РАБОТА С ЖУРНАЛОМ СОБЫТИЙ.....	48
5.1	Просмотр событий в журнале.....	48
5.2	Поиск событий по условию (фильтрация).....	48
5.3	Архивирование и удаление событий.....	49
6.	СРЕДСТВА НАДЁЖНОГО ВОССТАНОВЛЕНИЯ.....	51
6.1	Резервное копирование.....	51
6.2	Восстановление.....	52
7.	ВВОД И ВЫВОД ИНФОРМАЦИИ НА ВНЕШНИЕ НОСИТЕЛИ.....	54
7.1	Вывод на внешний носитель.....	54
7.2	Ввод с внешнего носителя.....	55

## 1. ФУНКЦИИ АДМИНИСТРАТОРА В MIRAGE

В TBC Mirage (далее по тексту "система") различают системных администраторов и администраторов безопасности.

### 1.1 Функции системного администратора в системе

В функции системного администратора входит:

1. Установка программного обеспечения TBC Mirage на серверах системы;
2. Первоначальное конфигурирование и установка параметров системы;
3. Создание учётных записей пользователей (в том числе администраторов безопасности), терминалов, принтеров и защищаемых файлов;
4. Контроль и мониторинг функционирования системы;
5. Создание архивных копий системы;
6. Восстановление системы в случае сбоя;
7. Установка и настройка стороннего программного обеспечения, функционирующего в системе.

### 1.2 Функции администратора безопасности в системе

В функции администратора безопасности в системе входит:

1. Конфигурирование правил разграничения доступа;
2. Контроль и мониторинг пользователей, их сеансов и запущенных ими приложений, печатаемых на твердую копию документов;
3. Реагирование на сигналы о попытках несанкционированного доступа;
4. Блокирование при необходимости учётных записей пользователей, принтеров, блокирование и завершение работающих сеансов и отдельных приложений;
5. Контроль действий системного администратора (в особенности в режиме конфигурирования системы);
6. Ввод/вывод информации на внешние носители.



## 2. УСТАНОВКА СИСТЕМЫ

Установка системы предполагает наличие знаний и навыков администратора UNIX-систем, выполнение требований к программному и аппаратному обеспечению сервера.

### 2.1 Требования к программному и аппаратному обеспечению сервера

Для установки и использования системы требуется следующее оборудование и ресурсы.

- Процессор: x86-совместимый с тактовой частотой не менее 733 МГц.
- Оперативная память: не менее 512 Мб. Объем необходимой памяти зависит от числа одновременно работающих активных сеансов и может быть приблизительно оценен по формуле:  $M = 128 \text{ Мб} + 40 \text{ Мб} * S$ . Где  $S$  – число одновременно работающих активных сеансов;
- Видеоадаптер: не менее 1 Мб видеопамяти;
- Жесткие диски: IDE или SCSI, RAID-массивы;
- Сетевые интерфейсы: любые сетевые ethernet контроллеры, работающие на скорости передачи 100/1000 Мбит/сек и поддерживаемые операционной системой;
- Операционная система: GNU/Linux (далее по тексту просто "Linux"). Рекомендуемый дистрибутив: ASP Linux 9.2;
- Программное обеспечение: XWindows, Xvnc, GNOME, грт;

### 2.2 Перечень установочных пакетов

Mirage поставляется в виде трех грт-пакетов, каждый из которых содержит законченную функциональную часть. "xxx" в названии пакета – обозначение версии:

- mirage-ts-xxx-1.i386.грт – терминальный сервер;

Главный пакет системы Mirage. Устанавливается на сервер терминального доступа и обеспечивает базовую функциональность системы Mirage.

- mirage-dbc-xxx-1.386.грт – сервер служебной базы данных;

Хранит информацию об объектах доступа, субъектах доступа, ПРД, настройках

системы, журнал регистрации. Эта база данных недоступна конечному пользователю и обрабатывается служебными программами системы Mirage.

– mirage-ps-xxx-1.386.rpm – сервер печати.

Наличие этого пакета обеспечивает дополнительную функциональность – возможность контролируемого вывода документов на твёрдую копию.

## 2.3 Порядок действий по установке системы

Установка системы требует привилегии администратора (root) Linux. Для установки с CD выполните следующую последовательность действий:

- 1) Поместите диск с дистрибутивом в привод CDROM.
- 2) В командной строке выполните последовательность команд:

```
# mkdir -p /mnt/cdrom
# mount /dev/cdrom /mnt/cdrom
# cd /mnt/cdrom/RPM
# rpm -vih mirage-*.rpm
```

Экранная форма процесса установки системы представлена на рисунке 2.1.

```
[root@mirage / # mkdir -p /mnt/cdrom
[root@mirage /]# mount /dev/cdrom /mnt/cdrom
[root@mirage /]# cd /mnt/cdrom/RPM
[root@mirage /mnt/cdrom/RPM]# rpm -vih mirage-*.rpm
Подготовка...
mirage-ts
Подсистема контроля целостности: подсчёт контрольных сумм...
Подсистема контроля целостности: подсчёт завершён.
mirage-dbs
Производится установка СУБД. Пожалуйста подождите...
Успешно установлено
Подсистема контроля целостности: подсчёт контрольных сумм...
Подсистема контроля целостности: подсчёт завершён.
mirage-ps
Подсистема контроля целостности: подсчёт контрольных сумм...
Подсистема контроля целостности: подсчёт завершён.
[root@mirage /mnt/cdrom/RPM]#
```

Рисунок 2.1 – Процесс установки системы. Пример

- 3) В случае, если в составе операционной системы не хватает каких-либо пакетов – об этом будет сообщено (рисунок 2.2). Установите недостающие пакеты и повторите установку Mirage.

```
ошибка: Неудовлетворенные зависимости:  
vnc-server >= 4.0 нужен для mirage-ts-0.2.50-0
```

*Рисунок 2.2 – Экранная форма сообщения об ошибке*

- 4) После успешной установки перезагрузите компьютер.
- 5) Произведите первоначальное конфигурирование системы с помощью системного конфигуратора (подразделы 2.4 и 2.5).

## 2.4 Режимы работы серверов Mirage

Функционирование сервера возможно в одном из двух режимов: нормальном режиме или режиме конфигурирования.

### 2.4.1 Нормальный режим

Это режим эксплуатации, нормального функционирования системы. В этом режиме доступны все основные функции системы:

- загрузка терминалов;
- авторизация пользователей;
- работа пользователей в терминальном режиме;
- печать документов на серверах печати;
- администрирование системы;
- мониторинг системы;
- и т.д.

В нормальном режиме у администратора нет доступа к командной строке, нельзя войти в систему, используя учётную запись пользователя Linux.

### 2.4.2 Режим конфигурирования

В этом режиме производится конфигурирование системы. Ядро защиты в это время не

функционирует. Настройка должна производиться локально с консоли сервера. После установки системы и перезагрузки сервер автоматически загрузится в этом режиме для осуществления первоначального конфигурирования системы.

Режим конфигурирования предназначен для случаев:

- первоначального конфигурирования;
- установки прикладного ПО;
- обновления прикладного ПО;
- удаления прикладного ПО;
- настройки операционной системы;
- восстановления системы;
- и т.п.

В этом режиме большинство функций системы Mirage недоступно. Например:

- пользователи не могут войти в систему;
- функции администрирования и мониторинга недоступны.

Но, в отличие от нормального режима, администратор может получить доступ к командной строке сервера. Для этого ему необходимо переключиться в консоль Linux (нажатием клавиш Alt+F2) и пройти авторизацию Linux, используя учётную запись root.

Внимание! Поскольку супер-пользователь root операционной системы Linux имеет неограниченные возможности, важно, по крайней мере, административными мерами контролировать действия администратора, пока сервер находится в режиме конфигурирования!

### 2.4.3 Выбор режима работы

Выбор режима работы производится при загрузке операционной системы путём выбора соответствующего пункта меню. Если выбор не был произведён пользователем в течение 10 секунд – система автоматически перейдёт в нормальный режим.

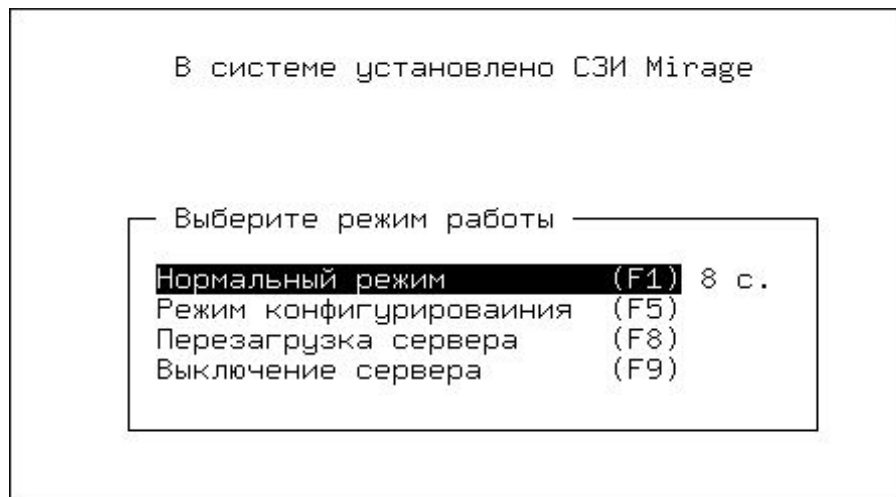


Рисунок 2.3 – Выбор режима работы

## 2.5 Первоначальное конфигурирование системы

В ходе первой загрузки сервера после установки системы будет автоматически запущен конфигуратор системы (рисунок 2.5), в котором необходимо произвести первоначальное конфигурирование. Выбор пункта главного меню конфигуратора приводит к переходу к соответствующему разделу конфигурации.

Перечень пунктов главного меню:

- подключение к серверу СУБД;
- сервис загрузки терминалов;
- сервис печати;
- конфигурация терминала администратора;
- параметры системы;
- регистрационный номер;
- восстановление.

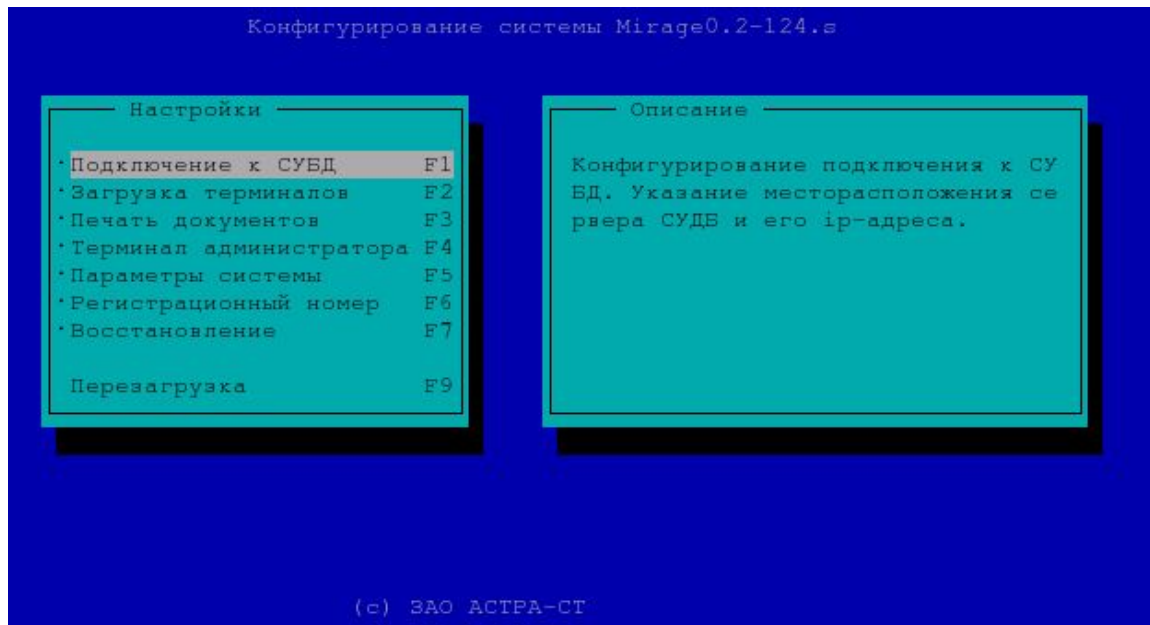


Рисунок 2.5 – Конфигуратор системы

Недоступные для конфигурирования разделы отмечаются отличительным серым цветом и не могут быть выбраны. Разделы, успешно прошедшие конфигурирование, отмечаются символом точки слева от названия соответствующего пункта меню.

Минимально, требуется произвести конфигурирование следующих разделов:

- подключение к СУБД;
- загрузка терминалов;
- терминал администратора;
- регистрационный номер.

### 2.5.1 Подключение к служебной базе данных

Для нормального функционирования системы ей необходим доступ к служебной базе данных, в которой будут храниться учётные записи, ПРД, документы и прочая служебная информация.

Для конфигурирования подключения к служебной базе данных выберите пункт меню "Подключение к СУБД" или нажмите <F1>. В открывшемся диалоге (рисунок 2.6) укажите местоположение базы данных.

Если сервер СУБД установлен совместно с терминальным сервером, то на вопрос "СУБД установлена на этом же сервере?" следует ответить "Да", в противном случае нужно ответить "Нет" и ввести IP-адрес сервера СУБД.

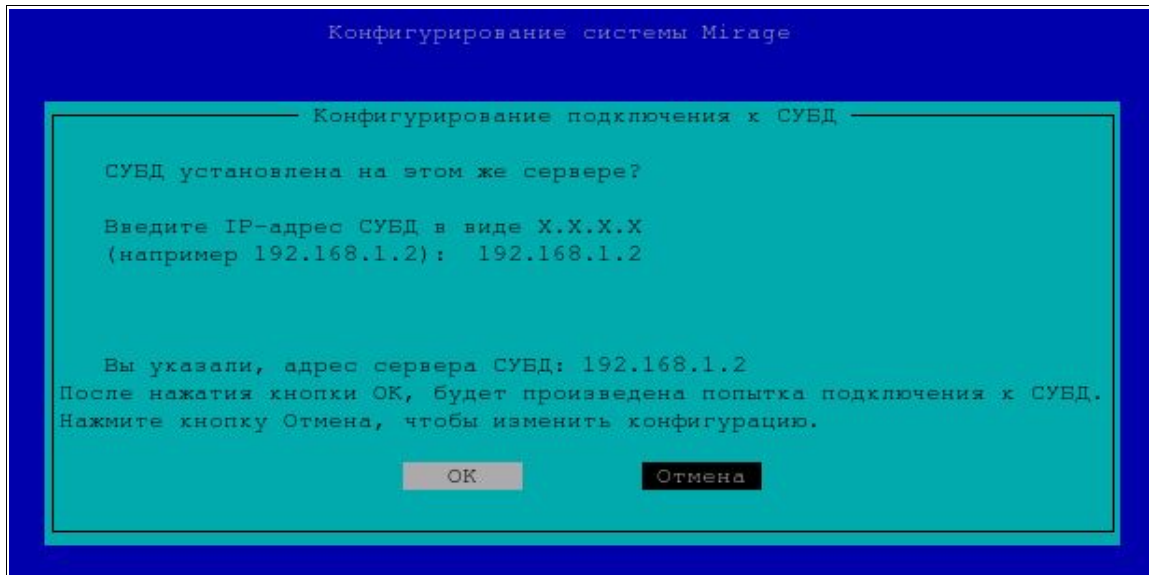


Рисунок 2.6 – Конфигурирование подключения к СУБД

Конфигуратор попытается произвести подключение к СУБД. При возникновении ошибок в ходе подключения о них будет сообщено. После успешной связи с СУБД пользователь снова попадет в главное меню программы.

## 2.5.2 Сервис загрузки терминалов

Выберите пункт меню "Загрузка терминалов" или нажмите <F2>. В открывшемся диалоге (рисунок 2.7) выберите сетевой интерфейс, на котором должен ждать подключений сервис загрузки терминалов. Выбранный сетевой интерфейс должен быть подключен к тому же сегменту сети, к которому подключены терминалы.

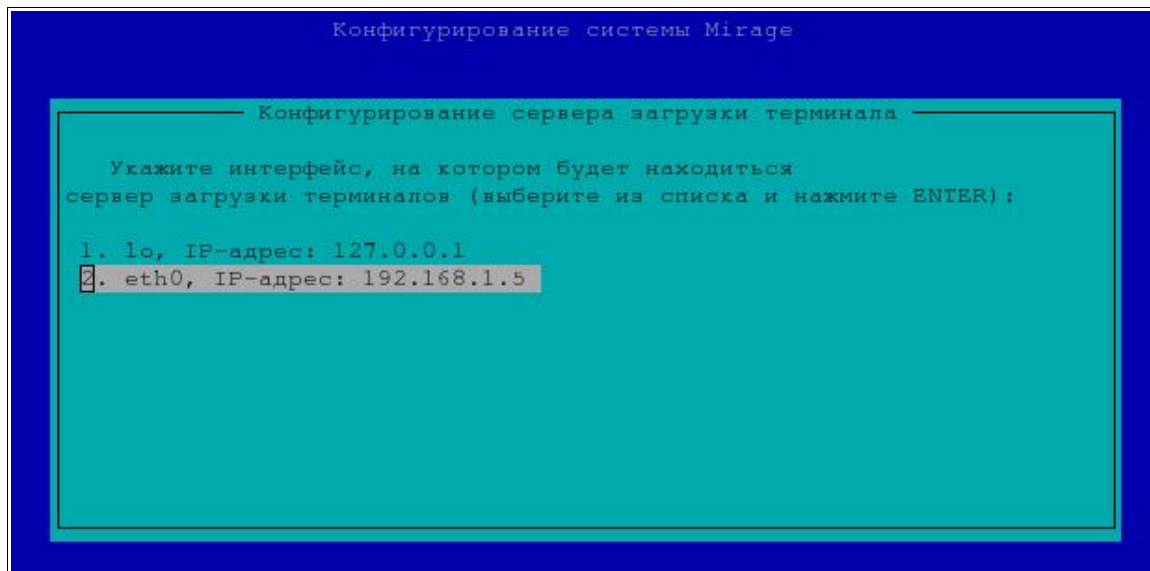


Рисунок 2.7 – Конфигурирование загрузки терминалов

### 2.5.3 Сервис печати

Конфигурирование сервиса печати нужно производить на сервере печати (если таковой имеется). Конфигурирование заключается в указании сетевого интерфейса, через который сервер печати связан с терминальным сервером. В случае если сервер печати и сервер терминального доступа функционируют на одном аппаратном сервере в качестве интерфейса сервера печати, следует указать интерфейс сервера загрузки терминалов.

Для перехода к конфигурированию сервиса печати выберите пункт меню "Печать документов" или нажмите <F3>. В открывшемся диалоге (рисунок 2.8) выберите сетевой интерфейс, на котором должен ждать подключений сервис печати документов.

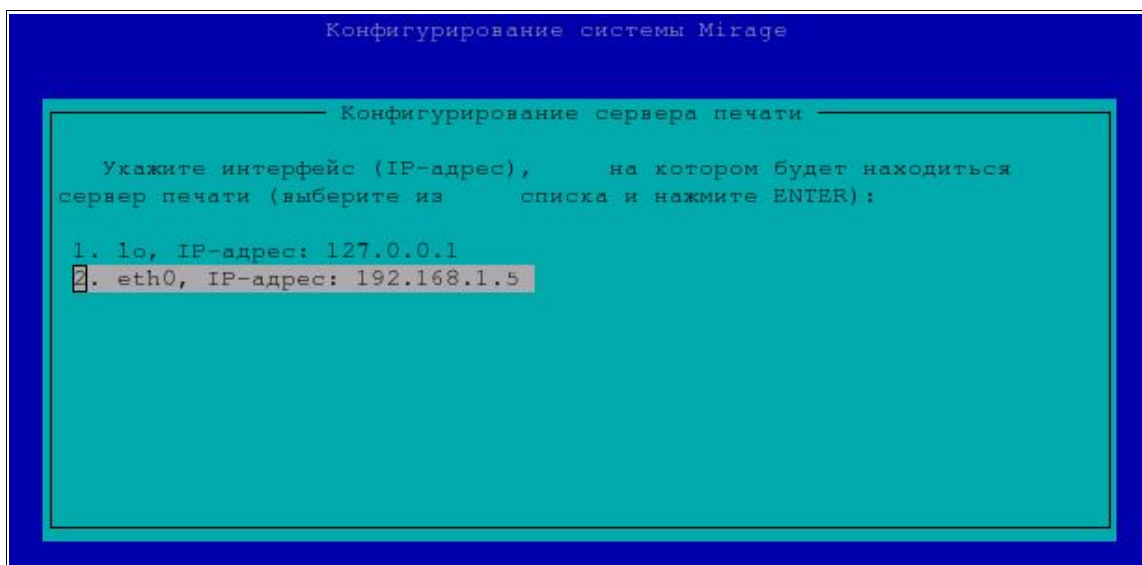


Рисунок 2.8 – Конфигурирование подсистемы печати

#### 2.5.4 Терминал администратора

Терминал администратора – первый регистрируемый в системе терминал, загрузка с которого разрешается учётной записи admin. С этого терминала должен загружаться администратор системы для создания учётных записей субъектов и объектов доступа.

Для перехода в раздел конфигурирования терминала администратора выберите пункт меню "Терминал администратора" или нажмите <F4>. В открывшемся диалоге укажите идентификатор терминала (его можно увидеть в правом верхнем углу экрана при включении терминала), IP адрес, который будет ему назначен в ходе загрузки, файл образа ОС, который будет загружен на терминал. Файлы образов ОС, используемые при загрузке терминалов, расположены в директории /mirage/boot/.

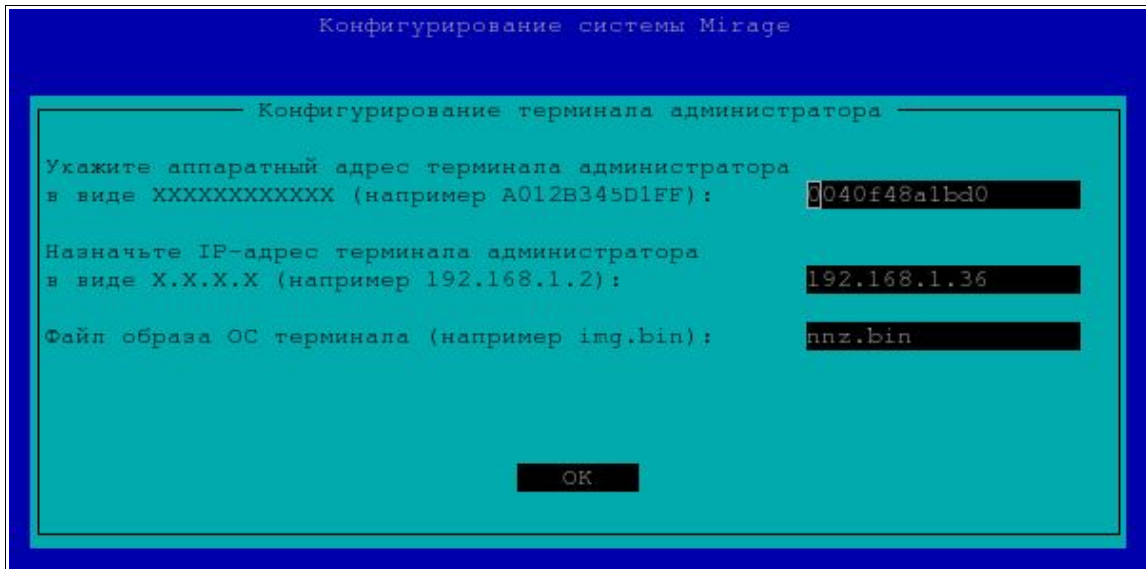


Рисунок 2.9 – Конфигурирование терминала администратора

Каждый такой файл соответствует определённой модели или семейству моделей терминалов (таблица 2.1).

Примечание. IP адрес терминала не должен совпадать ни с одним из IP адресов, установленных в сети устройств, в том числе серверов и других терминалов.

Таблица 2.1 – Перечень доступных для загрузки терминалов образов ОС

<i>Название файла образа ОС</i>	<i>Поддерживаемые модели терминалов</i>
sis.bin	XTerm500, XTerm2000, XTerm2200
nuz.bin	Нуеншанц Favourite TC uni 2

## 2.5.5 Параметры системы

Описание назначения параметров системы указано в таблице 2.2.

Таблица 2.2 – Параметры системы

<i>Параметр системы</i>	<i>Значение по умолчанию</i>	<i>Описание назначения</i>
Код используемой схемы авторизации	2	Определяет, какую схему авторизации использовать. Коды схем аутентификации приведены в документе "Описание КСЗ" (таблица 6.1.2)
Макс. число ошибок при вводе пароля	5	Если число последовательных ошибок при вводе пароля пользователем превышает значение данного параметра, учётная запись пользователя блокируется системой автоматически.
Минимальная длина пароля	8	Минимальная длина пароля пользователя Mirage в символах.
Требуемая схожесть отпечатков пальцев (%).	70	Минимальная степень схожести отпечатка пальца пользователя и образца отпечатка из служебной базы данных, требуемая для прохождения пользователем идентификации и / или аутентификации.
Время бездействия для блокировки сеанса (минуты)	30	Количество времени бездействия пользователя в минутах, по прошествии которого сеанс пользователя будет автоматически заблокирован.
Время хранения событий (в днях)	14	Количество дней с момента регистрации события, по истечении которого событие удаляется.
Устройство ввода-вывода USB	/dev/sda1	Файл устройства USB, используемого для ввода-вывода.

<i>Параметр системы</i>	<i>Значение по умолчанию</i>	<i>Описание назначения</i>
Устройство флоппи дисковода	/dev/fd0	Файл устройства флоппи дисковода, используемого для ввода-вывода.

### 2.5.6 Регистрационный номер

Регистрационный номер используется для активации программного обеспечения системы и служит подтверждением того, что используемая версия программного продукта легальна и приобретена в соответствии с лицензионным соглашением. Регистрационный номер можно получить у поставщика системы по предъявлению идентификационного номера.

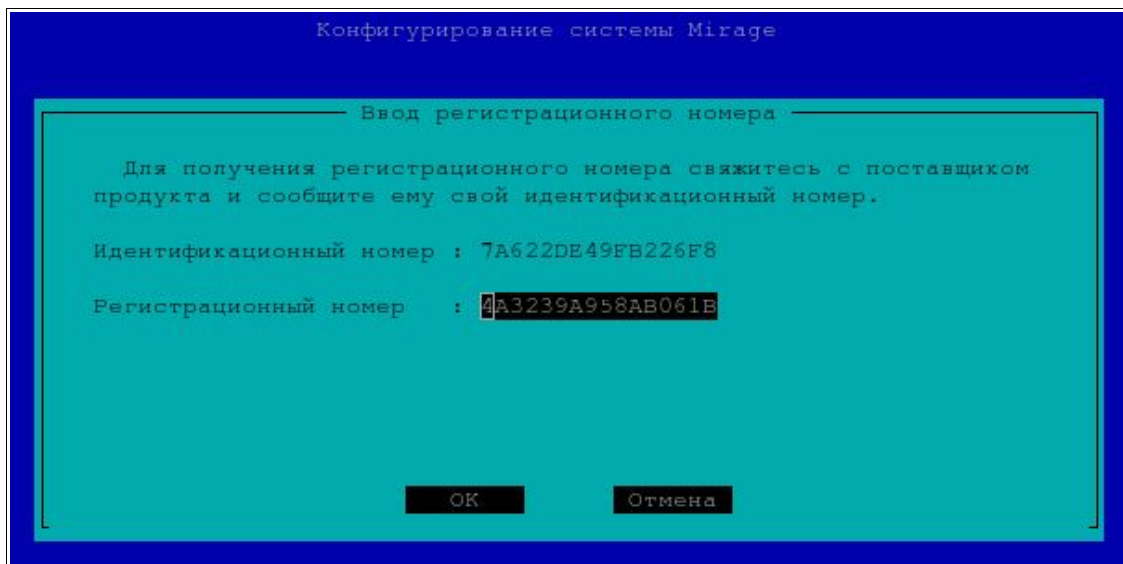


Рисунок 2.10 – Ввод регистрационного номера

Для перехода к вводу регистрационного номера выберите пункт меню “Регистрационный номер” или нажмите <F6>. В открывшемся диалоге (рисунок 2.10) введите регистрационный номер, соответствующий идентификационному номеру установленной системы.

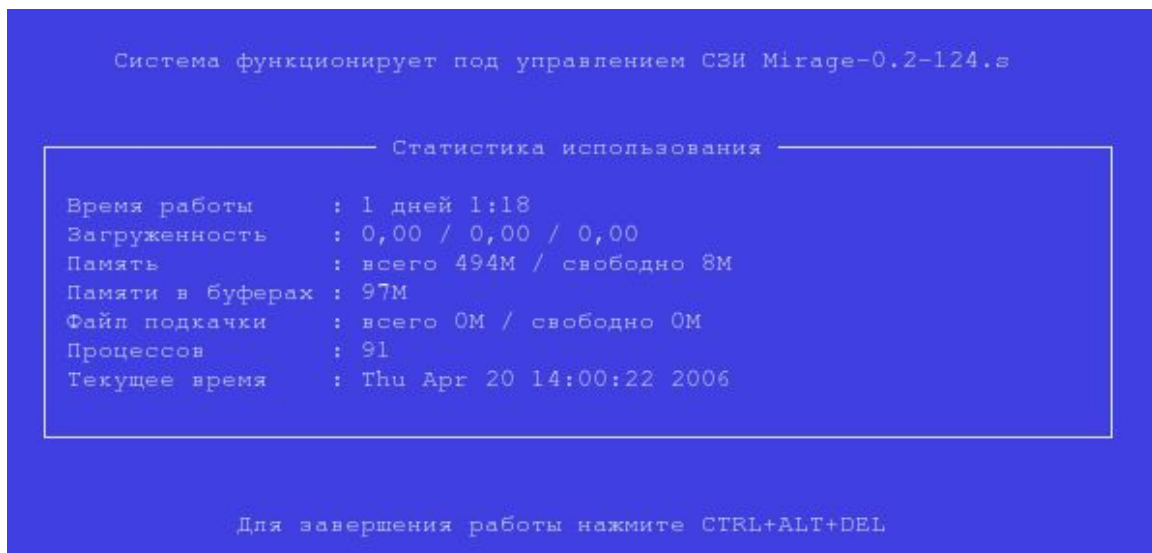
### 2.5.7 Восстановление

Система включает в себя средства, позволяющие восстановить служебное хранилище (учётные записи, настройки ПРД, параметры системы) из резервной копии. Подробнее

механизм резервного копирования и восстановления описан в пункте 6.

### 2.5.8 Перезагрузка

После завершения первоначального конфигурирования необходимо проверить работоспособность системы. Для этого перезагрузите сервер (выбрав пункт "Перезагрузка" в конфигураторе), выберите нормальный режим работы. По окончании загрузки сервера запустится программа – заставка нормального режима работы, снимок экрана которой приведён на рисунке 2.11. После этого можно входить в систему с терминала администратора под учётной записью пользователя admin (с паролем "admin").



```
Система функционирует под управлением СЗИ Mirage-0.2-124.в

----- Статистика использования -----
Время работы      : 1 дней 1:18
Загруженность     : 0,00 / 0,00 / 0,00
Память            : всего 494М / свободно 8М
Памяти в буферах  : 97М
Файл подкачки     : всего 0М / свободно 0М
Процессов         : 91
Текущее время     : Thu Apr 20 14:00:22 2006

Для завершения работы нажмите CTRL+ALT+DEL
```

Рисунок 2.11 – Заставка нормального режима работы сервера

## 3. КОНФИГУРИРОВАНИЕ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА

Для конфигурирования ПРД используется программа “Центр управления”, запускаемая терминально на рабочем месте администратора. Конфигурирование производится поэтапно:

1. Конфигурирование учётных записей групп, пользователей, принтеров, защищаемых файлов и приложений;
2. Конфигурирование дискреционных прав доступа;
3. Конфигурирование мандатных прав доступа;
4. Конфигурирование шаблонов документов;
5. Отчёты по конфигурации.

### 3.1 Конфигурирование учётных записей

Каждый контролируемый перманентный субъект доступа и объект доступа описывается в системе учётной записью, содержащей основные сведения об объекте: его идентификатор, уровень доступа или метку конфиденциальности, параметры. В системе можно создавать учетные записи для:

- групп пользователей;
- пользователей;
- принтеров;
- терминалов;
- файлов или приложений.

#### 3.1.2 Создание учётных записей

##### *3.1.2.1 Создание учётных записей групп пользователей*

Группы пользователей выполняют функцию ролей. Задав набор правил разграничения доступа группе пользователей, можно легко назначать эти правила отдельным пользователям, просто включая их в эту группу. Поэтому группы рекомендуется назначать

в соответствии с реальным разделением ролей в рабочей группе (например, по должностным обязанностям).

Для создания новой группы выберите пункт главного меню "Правка -> Новая группа пользователей". Заполните открывшееся диалоговое окно и нажмите кнопку "ОК". Название группы не может превышать 19 символов и может состоять из любых печатных символов.

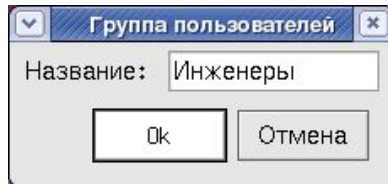


Рисунок 3.1 – Регистрация группы пользователей.

### 3.1.2.2 Создание учётных записей пользователей

Для создания учётной записи пользователя выберите пункт главного меню "Правка->Новый пользователь". Заполните открывшееся диалоговое окно (рисунок 3.2) и нажмите кнопку "ОК".

Рисунок 3.2 – Регистрация пользователя

Логин пользователя является основным идентификатором пользователя и не может превышать 19 символов. Он должен состоять только из допустимых символов: буквы латинского алфавита в нижнем регистре, арабские цифры, знак "минус" ("-").

Внимание! Логин пользователя должен быть уникален. И после создания учётной записи пользователя его нельзя будет изменить.

Минимальная длина задаваемого пароля определяется параметром системы "Минимальная длина пароля" (п. 2.5.5, "Параметры системы"). По умолчанию этот параметр равен 8.

### 3.1.2.3 Создание учётных записей терминалов

Для создания учётной записи терминала выберите пункт главного меню "Правка -> Новый Терминал". Заполните открывшееся диалоговое окно и нажмите кнопку "OK".

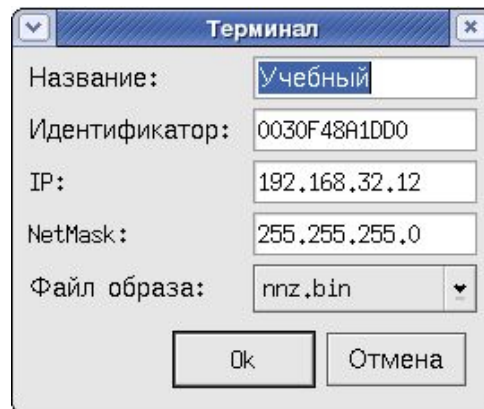


Рисунок 3.3 – Регистрация терминала

На рисунке 3.3:

"Идентификатор" – уникальный идентификатор терминала. Отображается при загрузке на терминале в верхнем правом углу экрана.

"IP" – Адрес IPv4, назначаемый терминалу. Записывается в виде чисел и точек в формате : ppp.ppp.ppp.ppp.

"NetMask" – Сетевая маска. Записывается в том же виде, что и IP. Для сетей класса "С" должна быть равна "255.255.255.0".

"Файл образа" – файл, содержащий образ операционной и файловой систем терминала. Выбор конкретного файла образа зависит от типа добавляемого терминала (его

аппаратуры: видео- и сетевой карт).

#### 3.1.2.4 Создание учётных записей принтеров

Для регистрации нового принтера выберите пункт главного меню "Правка -> Новый Принтер". Заполните открывшееся диалоговое окно и нажмите кнопку "ОК".

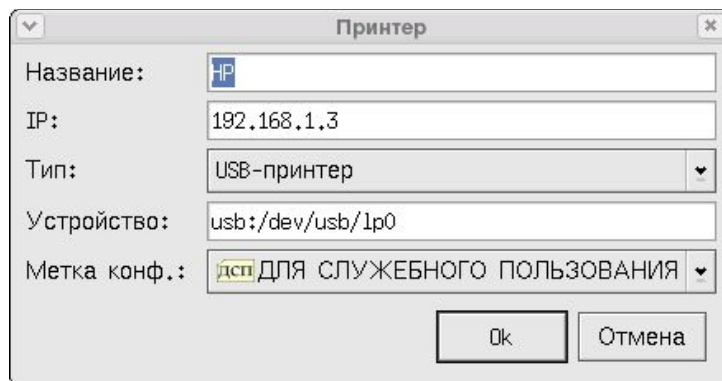


Рисунок 3.4 – Регистрация принтера

В поле IP адреса необходимо указать сетевой адрес сервера печати, к которому подключен данный принтер. Система поддерживает работу нескольких серверов печати одновременно. Поэтому для корректной работы нужно указать тот IP-адрес сервера печати, по которому он доступен для терминального сервера.

Тип принтера определяет его способ подключения к серверу печати. Поддерживаемые типы принтеров:

- "USB-принтер" – для принтеров, поддерживающих протокол Postscript и подключаемых через USB;
- "Печать в файл" – для эмуляции принтера (печать будет производиться в файл);
- "Сетевой принтер PCL" – для сетевого принтера, поддерживающего протокол PCL;
- "Сетевой Windows принтер PCL" – для принтеров поддерживающих протокол PCL, подключенных к рабочей станции Windows;

Устройство определяет файл устройства (для локального принтера) или сетевой адрес (для сетевого принтера), через который будет осуществляться взаимодействие системы с принтером. Примеры устройств:

- "usb:/dev/usb/lp0" – первое устройство USB;
- "/home/printer-output" – для эмуляции печати записью в файл printer-output домашней

директории пользователя;

- "socket://192.168.1.3/" – адрес сетевого PCL-принтера;
- "smb://user:pass@workgroup/server/sharename" – адрес windows PCL-принтера, где user – имя пользователя, pass – пароль, workgroup – рабочая группа, server – имя или IP-адрес сервера, sharename – название ресурса.

Метка конфиденциальности задает максимальный гриф документов, которые можно будет распечатывать на этом принтере. Т.е. если указана метка "С", то печатать можно будет документы с меткой "НС", "ДСП" и "С". А если указана метка "НС" – то разрешается печать только документов с меткой "НС".

### 3.1.2.5 Создание учётных записей защищаемых файлов и приложений

Для создания учётной записи защищаемого файла или приложения выберите пункт главного меню "Правка -> Новый защищаемый файл". Заполните открывшееся диалоговое окно и нажмите кнопку "ОК".

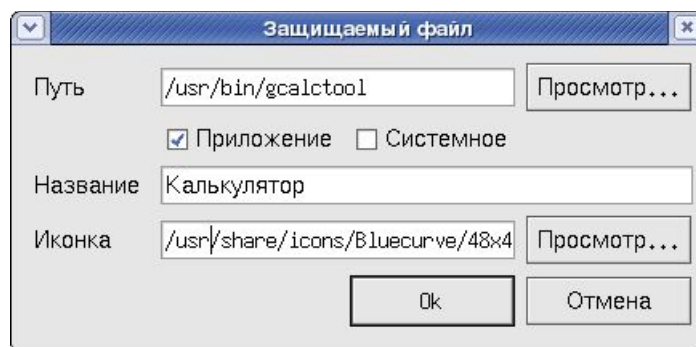


Рисунок 3.5 – Регистрация защищаемого приложения или файла

Название приложения и его иконка используются для формирования главного меню рабочего стола пользователей. Включение флажка "Приложение" означает, что выбранный файл является исполняемой программой. Включение флажка "Системное" означает, что выбранное приложение является системным и не должно отображаться в меню рабочего стола пользователя.

Примечание. Некоторые системные утилиты используются другими прикладными приложениями, однако пользователи не работают с ними

непосредственно. Например: /bin/cut, /bin/pwd и пр. Для таких программ рекомендуется устанавливать флаг "системное", чтобы не загромождать меню программ пользователя.

### 3.1.3 Редактирование учётных записей

Для редактирования любой учётной записи: группы, пользователя, принтера, терминала или файла – необходимо вызвать контекстное меню на редактируемом элементе и выбрать в меню пункт "Свойства..." (рисунке 3.6). Появится диалог параметров, аналогичный тому, что появляется при регистрации новых учётных записей. В нем можно отредактировать необходимые свойства объекта. Изменения вступят в силу сразу после нажатия кнопки "ОК".

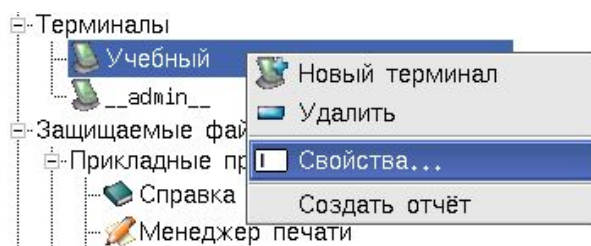


Рисунок 3.6 – Контекстное меню редактируемого элемента

### 3.1.4 Удаление учётных записей

Для удаления любой учётной записи: группы, пользователя, принтера, терминала или файла – необходимо в центре управления вызвать контекстное меню на удаляемом элементе и выбрать в меню пункт "Удалить" (рисунок 3.7). После подтверждения удаления в появившемся диалоге будет удалена учётная запись об объекте и все существовавшие с ним на момент удаления связи.

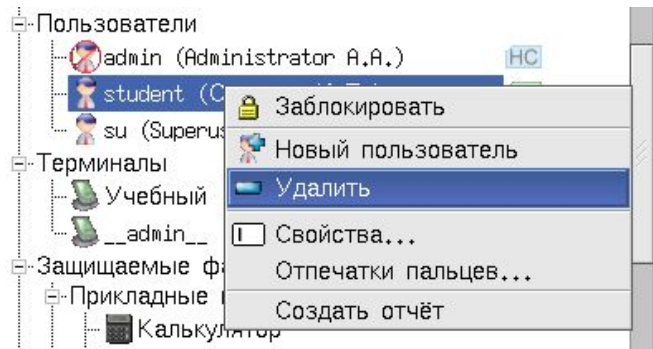


Рисунок 3.7 – Фрагмент главного окна центра управления. Удаление учётной записи пользователя student.

### 3.1.5 Блокирование и разблокирование учётных записей пользователей

Для блокирования или разблокирования учётных записей пользователей необходимо выбрать соответствующий пункт контекстного меню пользователя (рисунок 3.8).

Внимание! Пользователь, учётная запись которого заблокирована, не сможет войти в систему.

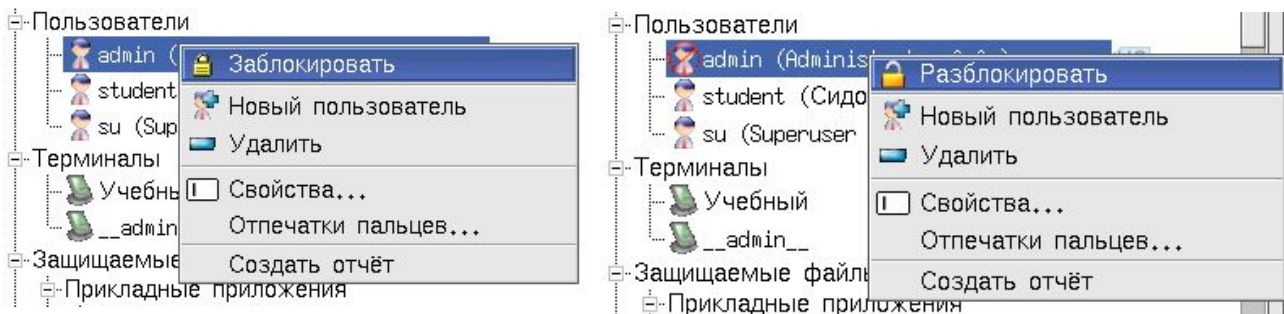


Рисунок 3.8 – Фрагменты главного окна центра управления. Блокирование, разблокирование учётной записи пользователя.

Учётная запись пользователя может быть заблокирована автоматически при превышении числа неудачных попыток авторизации при входе пользователя.

Учётная запись администратора безопасности не может быть автоматически заблокирована.

## 3.2 Предусстановленные пользователи и группы пользователей

При установке системы в ней автоматически создаются пользователи и группы пользователей специального назначения. Их перечень приведён в таблице 3.1

Таблица 3.1 – Перечень групп и пользователей специального назначения

<i>Название</i>	<i>Описание</i>
Группа "Администраторы"	<p>В эту группу следует включать всех системных администраторов. По умолчанию в неё включены: группа "Администраторы безопасности", пользователь "admin".</p> <p>Группа "Администраторы" входит в группы: "Пользователи", "Сигнализация".</p> <p>Этой группе разрешён запуск интерактивных приложений системы, а также приложений, доступных для запуска родительским группам.</p>
Группа "Служба безопасности"	<p>В эту группу следует включать всех сотрудников службы безопасности. Пользователи этой группы обладают всеми правами группы "Администраторы", плюс некоторыми дополнительными возможностями.</p> <p>Группа "Служба безопасности" входит в группы: "Администраторы", "Пользователи", "Сигнализация".</p>
Группа "Пользователи"	<p>Этой группе по умолчанию разрешён запуск стандартных утилит командной строки linux, требующихся для функционирования многих графических прикладных приложений.</p> <p>В эту группу рекомендуется включать все вновь создаваемые группы.</p>
Группа "Сигнализация"	<p>Этой группе установлен в автозапуск сигнализатор событий, визуально уведомляющий о значимых событиях, происходящих в системе.</p>

<i>Название</i>	<i>Описание</i>
Пользователь "admin"	Системный администратор по-умолчанию. Обладает правами доступа группы "Администраторы". После первоначального конфигурирования имеет разрешение на загрузку с терминала администратора ("__admin__"). После установки имеет пароль: "admin".
Пользователь "su"	Администратор безопасности по-умолчанию. Обладает правами доступа группы "Служба безопасности". После установки имеет пароль: "su".

Внимание! При конфигурировании модели защиты обязательно необходимо изменить пароль пользователей "admin" и "su" на новые. Учётные записи пользователей "admin" и "su" нужно использовать только при первой загрузке с терминала и в дальнейшем при диагностике неисправностей. Для нормальной работы следует использовать другие учётные записи, соответствующие реальным сотрудникам.

### 3.3 Отпечатки пальцев пользователей

В схемах авторизации FF, LF, LPF (см. документ "Описание КСЗ", таблица 6.1.2) для биометрической идентификации используются отпечатки пальцев пользователей. Для управления образцами отпечатков пальцев необходимо перейти в диалог "Образцы отпечатков пальцев". Для этого:

1. В левой части окна центра управления выделите нужного пользователя (для примера см. рисунок 3.9);
2. Вызовите контекстное меню нажатием на пользователя правой кнопки мыши;
3. Выберите пункт меню "Отпечатки пальцев" как показано на рисунке 3.9;

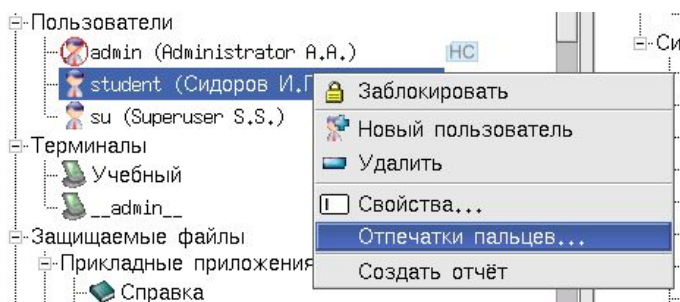


Рисунок 3.9 – Фрагмент главного окна центра управления. Переход в диалог "Образцы отпечатков пальцев".

4. Откроется диалог, изображённый на рисунке 3.10.

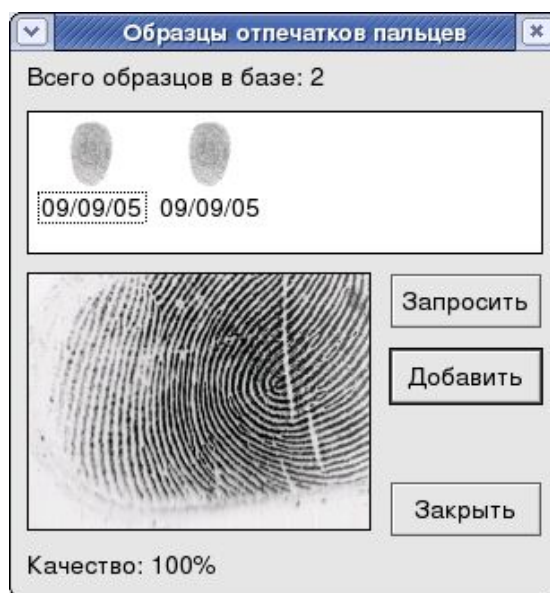


Рисунок 3.10 – Диалоговое окно с образцами отпечатков пальцев

### 3.3.1 Регистрация образцов

Для регистрации нового образца необходимо выполнить следующую последовательность операций:

- 1) Нажать кнопку "Запросить" для инициализации запроса отпечатка пальца;
- 2) Приложить палец к считывателю (это должен делать сам пользователь под контролем администратора безопасности). Палец нужно прикладывать ко считывателю на том терминале, где в данный момент производится регистрация;
- 3) По завершению чтения и анализа отпечатка убедиться, что образец имеет приемлемое качество (>90%) и нажать кнопку "Добавить" для регистрации образца;
- 4) Если качество образца неприемлемое – вернуться к шагу 1.

Примечание. Для облегчения процесса аутентификации пользователя при входе в систему рекомендуется заносить около пяти образцов отпечатков пальца приемлемого качества.

Допускается регистрировать отпечатки разных пальцев одного пользователя, т.к. это повышает надежность системы распознавания.

Примечание. Система не запоминает изображения отпечатков пальцев. Она сохраняет математическую модель отпечатка, построенную по его графическому изображению. Восстановить изображение отпечатка по его математической модели – невозможно.

### 3.3.2 Удаление образцов

Для удаления ранее зарегистрированного образца выделите условное изображение удаляемого отпечатка пальца в верхней части диалога, перейдите в контекстное меню и выберите пункт «Удалить», как показано на рисунке 3.11.



Рисунок 3.11 – Фрагмент диалогового окна с образцами отпечатков пальцев. Удаление одного образца.

## 3.3 Конфигурирование дискреционных прав доступа

Все правила дискреционного доступа обозначаются в центре управления в виде связей субъектов доступа (или их групп) с объектами доступа и отображаются в правой части главного окна. Существует возможность создания новых связей между субъектами доступа и объектами доступа, редактирования дискреционных прав доступа, задаваемых

связью, удаления существующей связи. В соответствии с возможностями системы по контролю доступа субъектов доступа к объектам доступа (п.1.1, таблица 1.1) возможно создание связей вида:

- "Пользователь - Терминал";
- "Пользователь - Защищаемый файл".

Примечание. Отсутствие зарегистрированной связи между субъектом доступа и объектом доступа эквивалентно наличию запрещающей связи между ними. Все, что не разрешено – то запрещено!

Факт принадлежности пользователя (группы пользователей) к группе пользователей также отмечается в центре управления в виде связи.

### 3.4.1 Обозначения связей

Для отображения связей в центре управления принят ряд обозначений:

- 1) Разрешение на вход субъекта в систему с терминала обозначается символом "+", запрет – символом "х";
- 2) Обозначение связей субъекта с защищаемыми файлами содержит три символа.

Возможные обозначения и пояснения к ним приведены в таблице 3.2.

Таблица 3.2 – Принятые обозначения для связей

<i>Положение</i>	<i>Комментарий</i>	<i>Символ</i>	<i>Пояснение</i>
1й символ * _ _	Право чтения.	"ч"	Чтение разрешено.
		"х"	Чтение запрещено.
		"_"	Право чтения не задано.
2й символ _ * _	Право исполнения.	"и"	Исполнение разрешено.
		"х"	Исполнение запрещено.
		"_"	Право исполнения не задано.
3й символ _ _ *	Автозапуск программы при старте сеанса	"а"	Производить автозапуск.
		"х"	Запретить автозапуск.
		"_"	Автозапуск не задан.

В таблице 3.3 приведены примеры обозначения связей с защищаемыми файлами и комментарии к ним.

Таблица 3.3 – Примеры обозначения связей с защищаемыми файлами

Пример обозначения	Комментарий
ч--	Разрешено чтение файла. Другие права не заданы.
хи-	Запрещено чтение файла. Разрешено исполнение файла. Автозапуск не задан.
-иа	Разрешено исполнение файла и установлен автозапуск. Право чтение не задано.

3) Названия объектов, доступ к которым унаследован от группы пользователей, обозначаются в списке связей отличительным серым цветом.

Например, на рисунке 3.12 разрешение входить в систему с терминала "Учебный", разрешение запуска приложения "Справка" унаследованы от группы пользователей "Студенты",

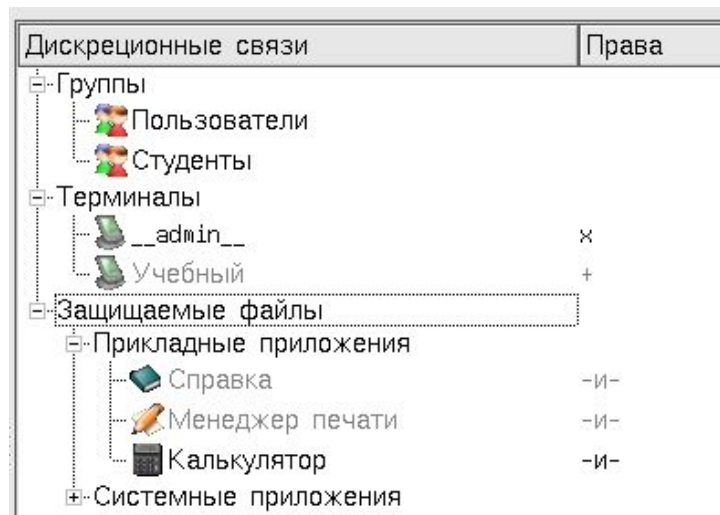


Рисунок 3.12 – Фрагмент главного окна центра управления. Дискреционные связи пользователя

На рисунке 3.12:

пользователь входит в группы: "Пользователи" и "Студенты";

пользователь может загружаться с терминала "Учебный" (это разрешение унаследовано);

пользователю явно запрещено загружаться с терминала администратора `__admin__`;

пользователю явно разрешено запускать “Калькулятор”;

пользователю разрешен запуск программ “Справка” и “Менеджер печати” (эти права унаследованы)

### 3.4.2 Создание связей

Создание связи производится путём простого перетаскивания объектов доступа в поле связей субъекта доступа.

Рассмотрим пример. Требуется разрешить пользователю student возможность запуска приложения “Справка”. Для этого необходимо выполнить следующие шаги:

1. Выделить пользователя student в левой части окна. При этом справа отобразятся права доступа этого пользователя (рисунок 3.13);

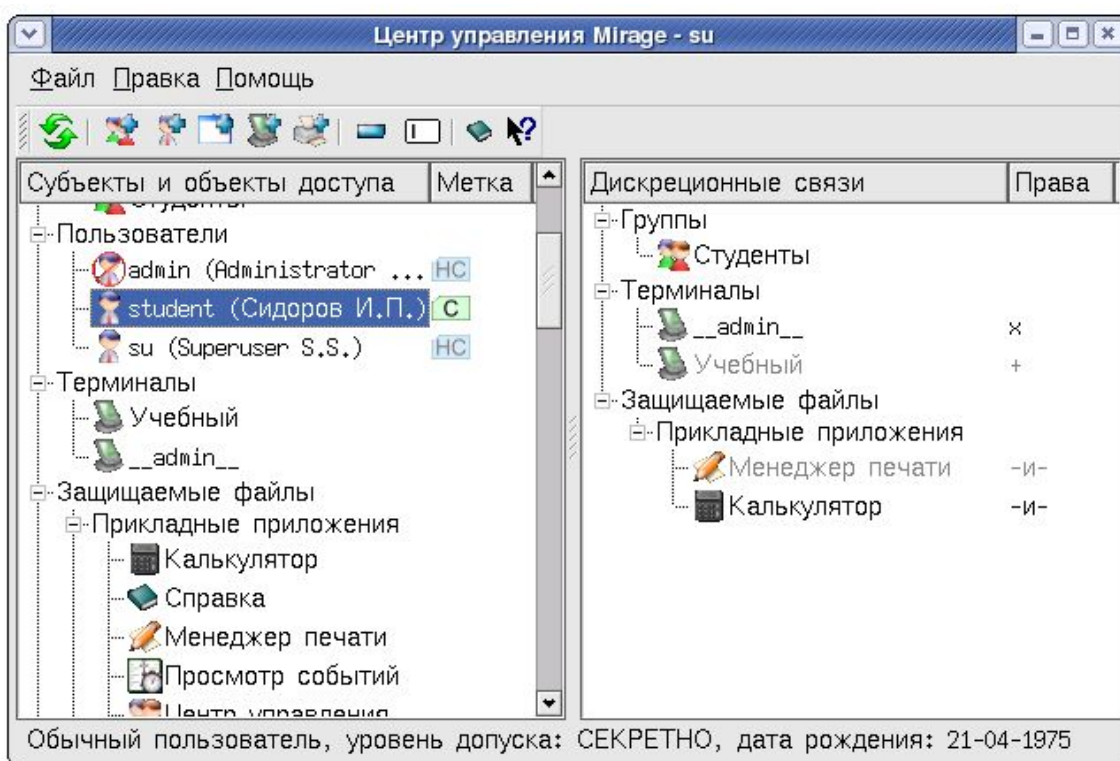


Рисунок 3.13 – Главное окно центра управления, на котором отображаются дискреционные права доступа (связи) пользователя student.

2. Перетащить из левой части окна в правую иконку приложения “Справка” (рисунок 3.14);

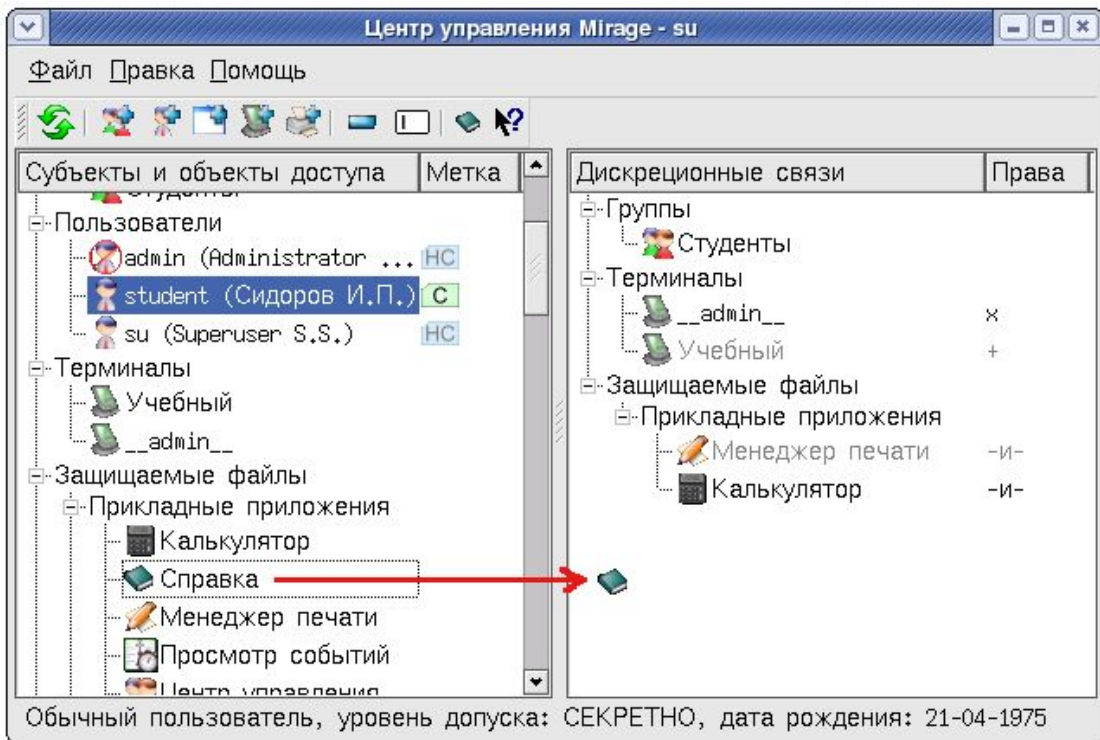


Рисунок 3.14 – Главное окно центра управления. Назначение дискреционного права доступа путём перетаскивания иконки приложения в область связей пользователя.

3. При этом откроется диалоговое окно для указания прав доступа (рисунок 3.15).

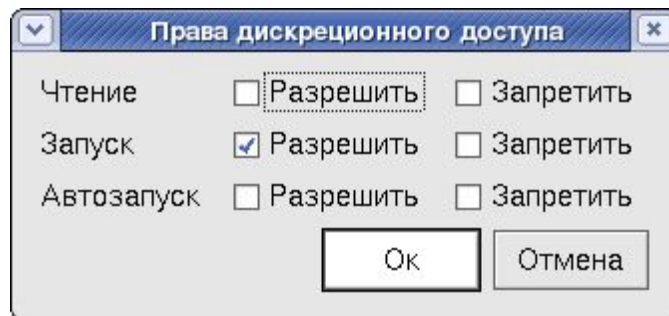


Рисунок 3.15 – Диалоговое окно указания дискреционных прав доступа к защищаемому файлу

Аналогичным образом настраиваются дискреционные права доступа пользователей или групп пользователей к терминалам и защищаемым файлам.

При указании прав доступа субъекта к терминалу появляется диалоговое окно следующего вида:

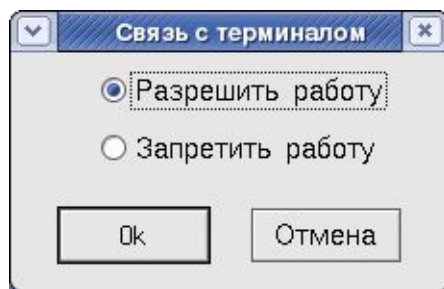


Рисунок 3.16 – Диалоговое окно указания прав дискреционного доступа к терминалу

### 3.4.2 Изменение дискреционных прав доступа

Для изменения дискреционных прав доступа необходимо выполнить следующую последовательность действий:

1. Вызвать контекстное меню на редактируемой связи;
2. Выбрать в меню пункт "Изменить права" (рисунок 3.17). Появится диалог аналогичный тому, что появляется при создании новых связей (рисунок 3.15);
3. Произвести требуемые изменения и нажать кнопку "ОК".

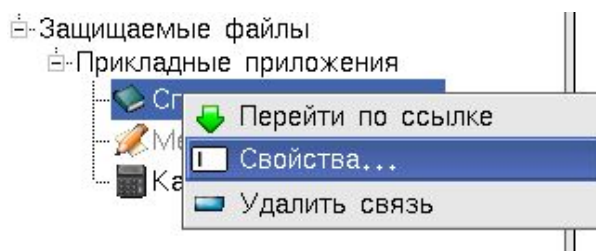


Рисунок 3.17 – Фрагмент главного окна центра управления. Изменение прав дискреционного доступа.

### 3.4.3 Удаление связей

Для удаления связи необходимо выполнить следующую последовательность действий:

1. Вызвать контекстное меню на удаляемой связи (нажав на нем правую кнопку мыши);
2. Выбрать в меню пункт "Удалить связь" (рисунок 3.18);
3. Подтвердить удаление в появившемся диалоге.

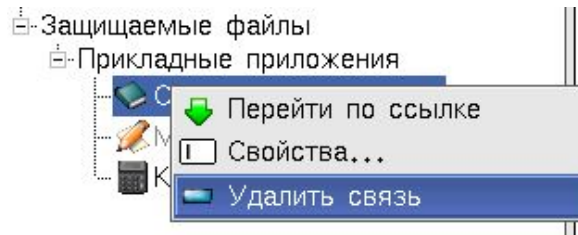


Рисунок 3.18 – Фрагмент главного окна центра управления. Удаление связи.

### 3.4 Пользователи и группы пользователей

Так как вхождение пользователя в группу представляется в центре управления в виде связи таким же образом, что и права дискреционного доступа, включение пользователей (групп пользователей) в группы пользователей производится методом создания соответствующих связей (см. п. 3.9.1). Исключение пользователей (групп пользователей) из групп пользователей производится методом удаления соответствующих связей (см. п. 3.9.2).

### 3.5 Конфигурирование мандатных прав доступа

Конфигурирование мандатных прав доступа производится в обозревателе файлов. Файлы, имеющие уровень конфиденциальности выше "НЕСЕКРЕТНО", обозначаются соответствующими изображениями (рисунок 3.19).

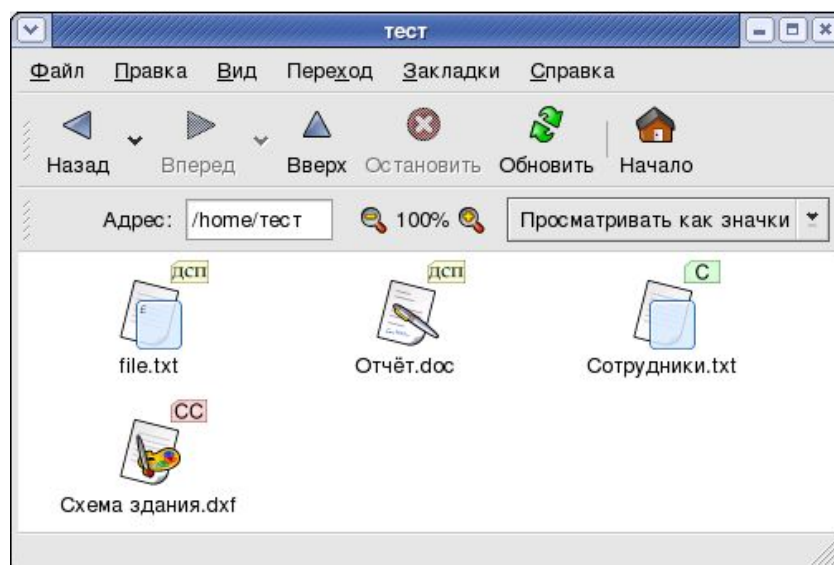


Рисунок 3.19 – Окно с файлами различных меток безопасности в директории "/home/тест"

Для назначения или изменения метки безопасности файла или директории необходимо в контекстном меню интересующего объекта выбрать пункт "Метка безопасности..." (рисунок 3.20).

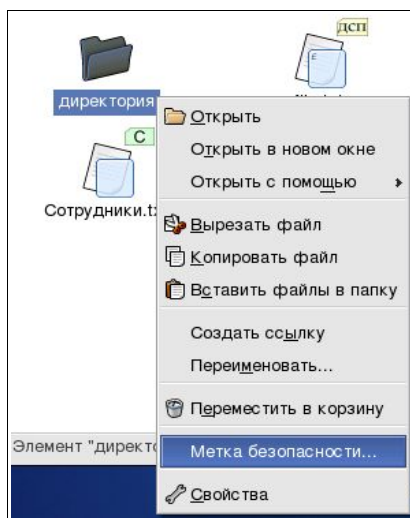


Рисунок 3.20 – Контекстное меню.  
Назначение метки безопасности.

При этом появится диалоговое окно с выбором метки безопасности (рисунок 3.21). Для директорий также доступна возможность включения режима фиктивной записи, необходимого для работы многих графических приложений в условиях строгих ПРД. (см. документ "Описание КСЗ Mirage", п. 5.3.3.3).

Примечание: Для директорий, название которых начинается с точки (например ".dconf2"), режим фиктивной записи включается автоматически при их создании. В этих директориях прикладные программы хранят конфигурационные и временные файлы, а режим фиктивной записи предотвращает запись данных в конфигурационные файлы и, следовательно, повышение их метки в случае, если приложение работает с конфиденциальными данными.

Примечание: Вновь создаваемым директориям автоматически назначается метка безопасности родительской директории и режим фиктивной записи (если таковой был назначен родителю).

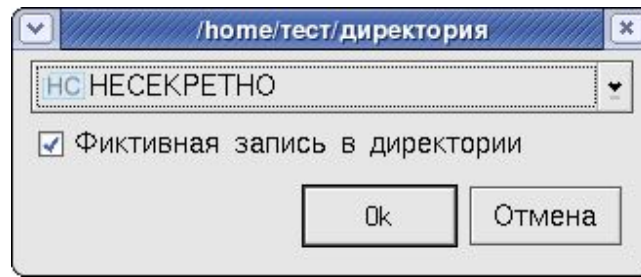


Рисунок 3.21 – Окно установки метки безопасности

Внимание! Все действия пользователей при назначении меток безопасности файлам и каталогам протоколируются в журнале событий.

### 3.6 Конфигурирование шаблонов документов

Шаблон документа – программа, написанная на языке postscript, используемая сервером печати в процессе печати документа. Шаблон документа определяет, какие именно штампы, рамки, графические элементы, реквизиты и на каких страницах будут напечатаны при выводе документов на твёрдую копию.

Шаблоны документов обладают метками конфиденциальности, позволяющие системе осуществлять контроль мандатного доступа к ним.

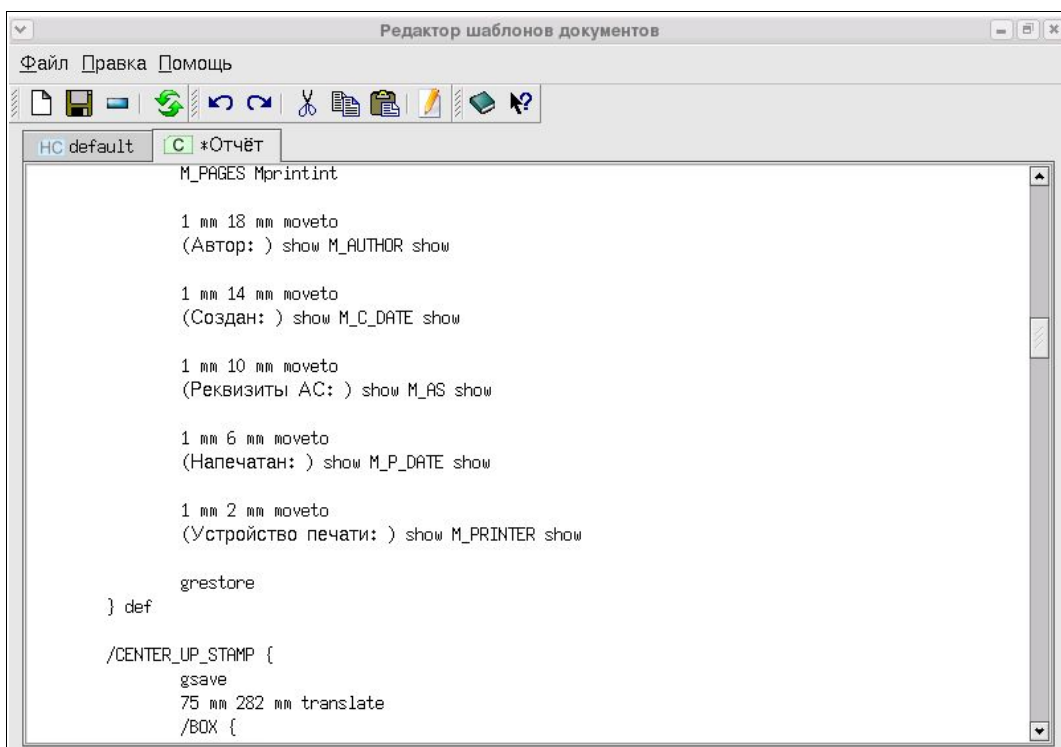


Рисунок 3.22 – Главное окно редактора шаблонов документов

Для управления шаблонами используется приложение "Редактор шаблонов документов", снимок главного окна которого представлен на рисунке 3.22.

### 3.6.1 Создание шаблона документа

Для создания нового шаблона документа необходимо выбрать в главном меню программы пункт "Файл->Новый" и в появившемся диалоговом окне (рисунок 3.23) указать параметры шаблона.

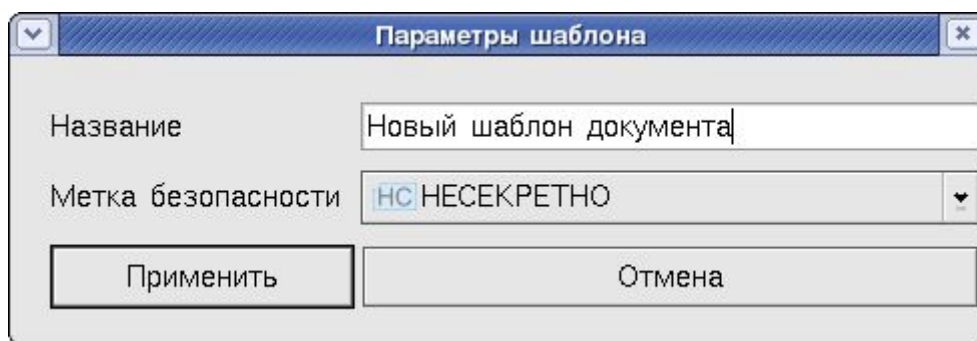


Рисунок 3.23 – Диалоговое окно параметров шаблона

### 3.6.2 Редактирование шаблона документа

Переключение между шаблонами происходит путём выбора соответствующей вкладки главного окна.

Для редактирования шаблона необходимо выбрать вкладку интересующего шаблона (например на рисунке 3.22 в программе выбрана вкладка "Отчёт"). При этом в текстовом поле отобразится содержимое шаблона. После внесения изменений шаблон нужно сохранить ("Файл->Сохранить").

Для изменения параметров шаблона выберите пункт меню "Правка->Параметры". При этом появится диалог, аналогичный изображённому на рис 3.23.

### 3.6.3 Удаление шаблона документа

Для удаления шаблона необходимо перейти в него и выбрать пункт меню "Файл->Удалить". Шаблон будет удалён после подтверждения удаления в открывшемся диалоге.

### 3.6.4 Предусстановленные шаблоны документов

При установке системы в ней автоматически создаются несколько стандартных шаблонов документов, перечисленных в таблице 3.4, которые могут использоваться как основа для создания новых шаблонов.

Таблица 3.4 – Предусстановленные шаблоны документов

<i>Наименование</i>	<i>Метка безопасности</i>	<i>Описание назначения</i>
Пустой	НС	Предназначен для печати документов с грифом "НЕСЕКРЕТНО". Шаблон не создаёт никаких штампов; документ будет напечатан без изменений. Подходит только для печати несекретных документов.
Стандартный	СС	Шаблон создаёт стандартный набор штампов, содержащий реквизиты документа, системы, фамилию автора. Подходит для печати документов с грифами: ДСП, С и СС.

### 3.7 Отчёты по конфигурации

По каждому из субъектов (объектов) в центре управления возможна генерация отчёта. Для этого в контекстном меню интересующего объекта необходимо выбрать пункт меню "Создать отчёт" (рис 3.24).

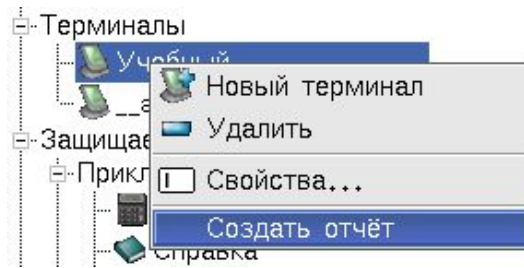


Рисунок 3.24 – Фрагмент окна центра управления. Формирование отчёта о терминале "Учебный" посредством всплывающего меню.

Краткий отчёт содержит информацию об учётной записи объекта. Подробный отчёт включает в себя описание всех связей этого объекта. На рисунке 3.25 изображён пример отчёта по терминалу.

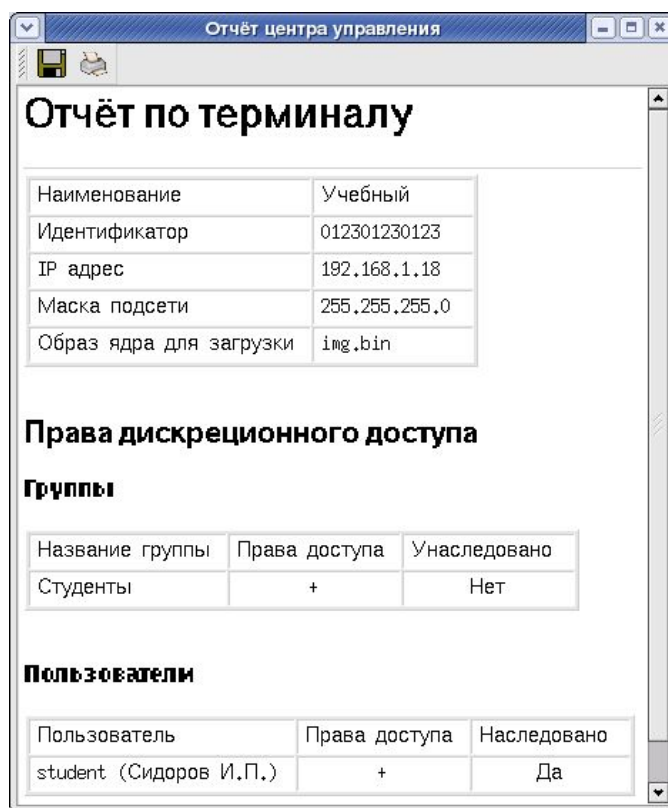


Рисунок 3.25 – Снимок окна с отчётом о терминале

Сформированный отчёт можно сохранить или напечатать, выбрав соответствующую кнопку панели управления в верхней части окна.

## 4. МОНИТОРИНГ СИСТЕМЫ

Мониторинг системы осуществляется в приложении "Центр мониторинга", которое позволяет администратору следить за состоянием сеансов пользователей, запущенными приложениями, работой принтеров и серверов системы.

Функции, выполняемые программой:

- мониторинг сеансов и запущенных приложений;
- мониторинг принтеров;
- мониторинг серверов.

Доступ ко всем функциям контроля осуществляется через контекстное меню соответствующего объекта, вызываемое нажатием правой кнопки мыши.

Внимание! Все действия администратора, влияющие на работу системы: блокирование, разблокирование принтеров и сеансов, завершение приложений и сеансов – протоколируются в журнале событий.

### 4.1 Мониторинг сеансов

В левой части окна программы отображаются все существующие сеансы, содержится информация о соответствующих пользователях и терминалах. Программа позволяет проследить динамику работы запущенных пользователями приложений, их общее количество, состояние каждого приложения, метку его конфиденциальности.

Для каждого сеанса показывается следующая информация:

- В заголовке – имя пользователя и терминала.
- Стартовое время – дата и время, когда сеанс был запущен пользователем.
- Состояние сеанса – Активен, Приостановлен или Заблокирован.
- Список приложений, работающих в сеансе. Для каждого показываются:
  - наивысший гриф документа, с которым работало приложение;
  - название приложения (или путь запуска);

– текущее состояние приложения: S – приостановлено, R – активно, Z – завершается.

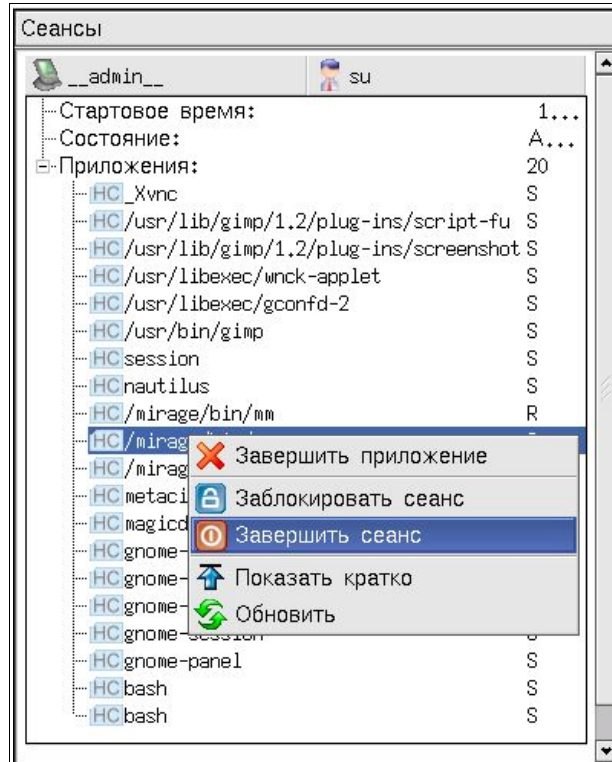


Рисунок 4.1 – Мониторинг и управление сеансами

Доступные операции:

- Блокирование сеанса;
- Разблокирование ранее заблокированных сеанса;
- Завершение сеанса;
- Принудительное завершение запущенного пользователем приложения в сеансе.

## 4.2 Мониторинг принтеров

В верхней правой части окна программы отображается список зарегистрированных на текущий момент принтеров, адреса соответствующих им серверов печати, состояние принтеров, количество поставленных заданий на печать в очередях печати.

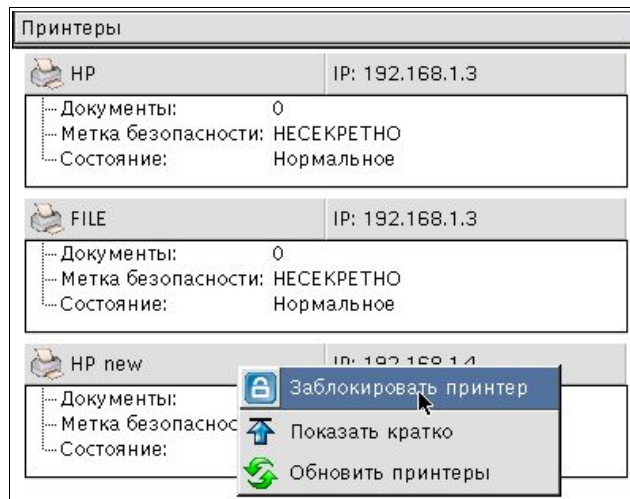


Рисунок 4.2 – Мониторинг и управление принтерами.

*Доступные операции:*

- Блокирование принтеров (сервера печати перестают отправлять документы на печать на заблокированные принтеры);
- Разблокирование заблокированных принтеров.

### 4.3 Мониторинг серверов

В нижней правой части окна программы отображается информация о серверах системы, их времени работы с последнего включения, степени их загруженности.

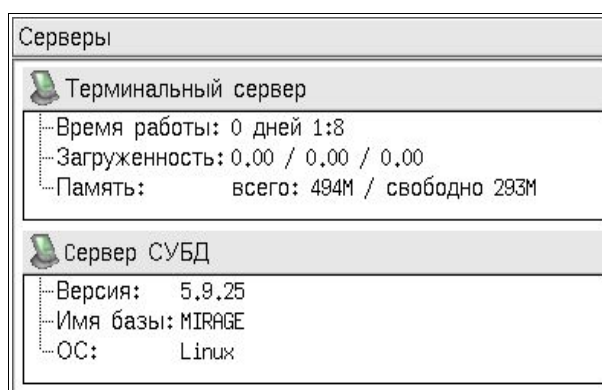


Рисунок 4.3 – Мониторинг серверов

На рисунке 4.3:

“Время работы” – время работы сервера с момента последней загрузки.

“Загруженность” – средний интегральный показатель загруженности системы за

последние одну, пять и пятнадцать минут (показатели принимают неотрицательные значения, чем больше показатель – тем выше загруженность).

“Память” – объёмы доступной оперативной памяти, свободной оперативной памяти.

“Версия” – версия СУБД ЛИНТЕР.

#### 4.4 Мониторинг критических событий

Для сигнализации о значимых событиях, происходящих в системе, используется программа – сигнализатор. По умолчанию, сигнализатор разрешён на автозапуск группе пользователей “Сигнализация” и входящей в неё группе “Администраторы”.







Сигнализатор запускается автоматически при старте сеанса администратора и уведомляет его об всех событиях, удовлетворяющих заданному критерию фильтрации.

Уведомление о новых событиях можно увидеть в системном лотке (рисунок 4.4) в виде изображения соответствующего уровня значимости (таблица 4.1).



Рисунок 4.4 – Отображение события НСД в системном лотке рабочего стола

Таблица 4.1 – Перечень изображений и соответствующих уровней значимости

Изображение	Уровень значимости
	ОТЛАДКА
	ИНФОРМАЦИЯ
	ПРЕДУПРЕЖДЕНИЕ
	ОШИБКА
	НСД
	АВАРИЯ!

Двойной клик по изображению в лотке открывает список произошедших событий (рисунок 4.5).

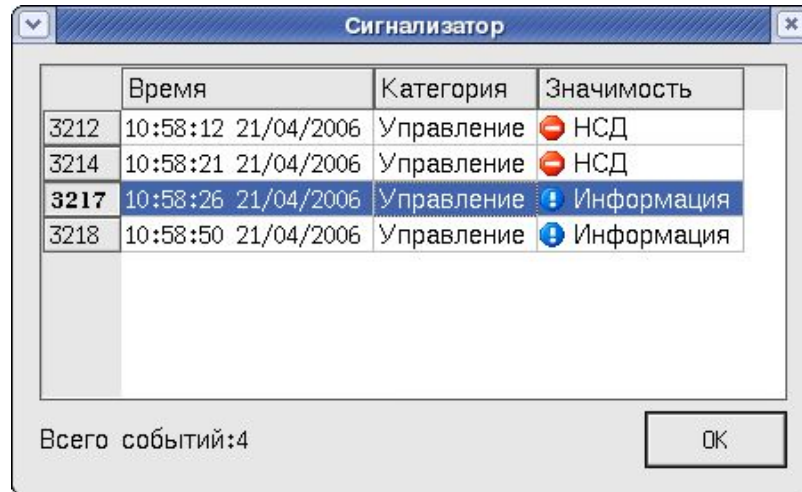


Рисунок 4.5 – Пример диалога со списком событий

Для просмотра подробной информации нужно дважды кликнуть на интересующем событии (рисунок 4.6).

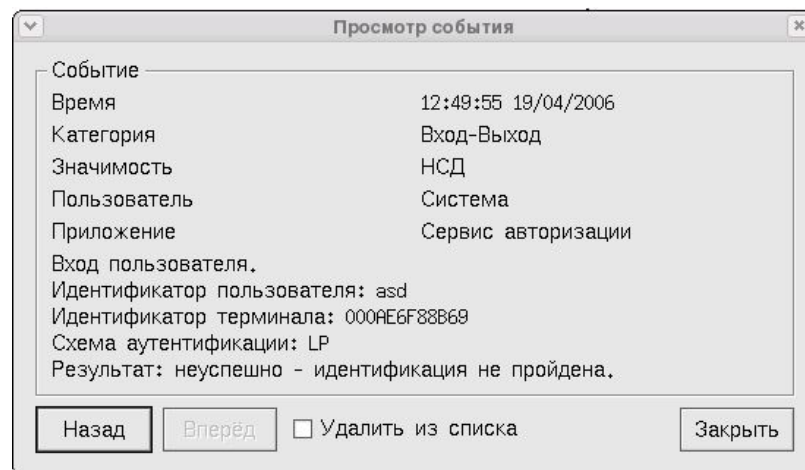


Рисунок 4.6 – Пример диалога уведомлением о событии

Окно просмотра событий содержит информацию о событии и кнопки навигации ("Назад", "Вперёд") по событиям из списка. Установка флажка "Удалить из списка" приведёт к удалению просматриваемого события из списка после закрытия окна (кнопка "Закреть") или перехода к другому событию.

Для задания критерия фильтрации необходимо в контекстном меню программы выбрать пункт "Фильтр событий..." (рисунок 4.7).

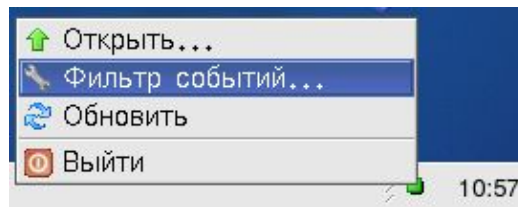


Рисунок 4.7

Критерий фильтрации включает в себя возможность выбора интересующих категорий и значимости событий (рисунок 4.8).

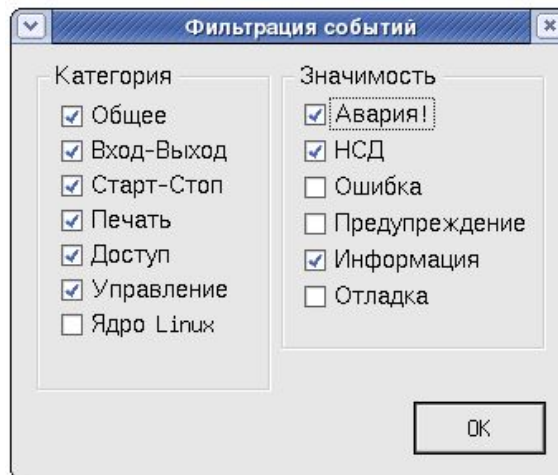


Рисунок 4.8 – Задание критерия фильтрации

## 5. РАБОТА С ЖУРНАЛОМ СОБЫТИЙ

Для просмотра зарегистрированных в системе событий используется программа просмотра событий.

### 5.1 Просмотр событий в журнале

На рисунке 5.1 приведен снимок экрана с окном просмотра событий. В левой части окна находится панель поиска (фильтрации) событий. В правой части окна – перечень событий, удовлетворяющих текущим условиям выборки. В нижней части окна отображается текст сообщения (комментарий) к текущему выделенному в перечне событию.

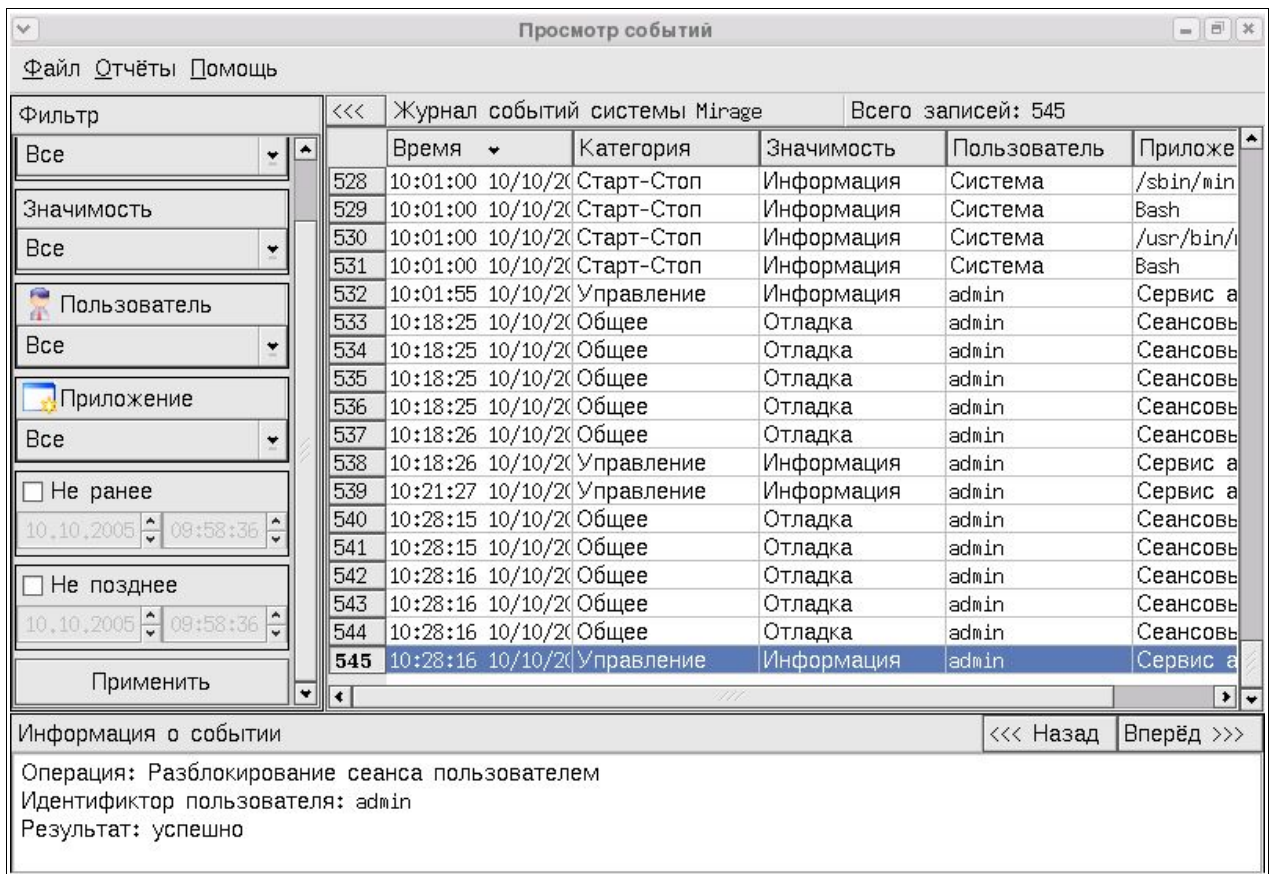


Рисунок 5.1 – Главное окно программы просмотра событий

### 5.2 Поиск событий по условию (фильтрация)

Для поиска события или группы событий по условию необходимо задать критерии фильтрации в левой панели главного окна и нажать кнопку применить. Фильтрация событий может быть осуществлена по следующим критериям:

- Категория события;
- Значимость события;
- Приложение, к которому относится событие;
- Пользователь, от имени которого было запущено приложение;
- Штмп времени события. Фильтр может ограничить перечень событий по дате как снизу так и сверху (путём использования соответствующих элементов управления “Не ранее”, “Не позднее” ) .

### 5.3 Архивирование и удаление событий

Для архивации событий выберите пункт меню “Файл->Архивация данных”. В появившемся диалоговом окне (рисунок 5.2) укажите хронологический диапазон архивируемых событий, параметры архивации.

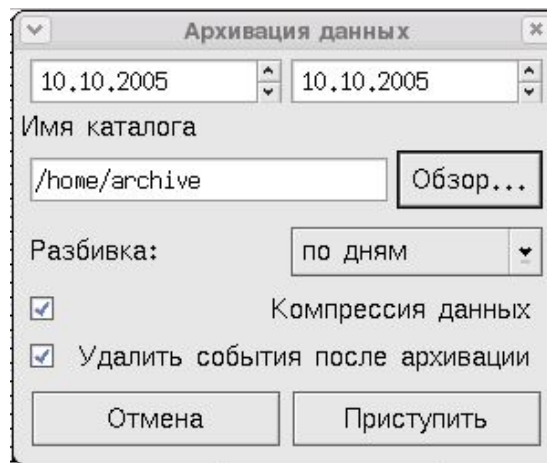


Рисунок 5.2 – Диалоговое окно архивации событий

На рисунке 5.2:

“Имя каталога” – директория, в которую будут помещаться файлы архива.

“Разбивка” – определяет способ деления всех событий на файлы. При разбивке по дням в один файл (в имени файла будет указана дата) помещаются события за соответствующий день, при разбивке по неделям в один файл помещаются события за соответствующую неделю.

“Компрессия данных” – включение этого флажка включит режим сжатия данных, при

котором каждый файл архива будет сжат компрессором gzip.

“Удалить события после архивации” – включите этот флажок, если требуется удаление событий.

## 6. СРЕДСТВА НАДЁЖНОГО ВОССТАНОВЛЕНИЯ

Система включает в себя средства, позволяющие проводить резервное копирование данных служебного хранилища (учётные записи, настройки ПРД, параметры системы) в файл для возможности последующего восстановления.

### 6.1 Резервное копирование

Резервное копирование производится в ходе нормального режима работы администратором безопасности системы с помощью программы резервного копирования (mss). При запуске программы резервного копирования от администратора требуется указать путь до файла (с расширением ".m.z"), в который будет записана архивная копия. Имеется возможность сопроводить архив комментарием (на английском языке). Получаемые архивные файлы имеют примерный размер 1 – 8 мегабайтов.

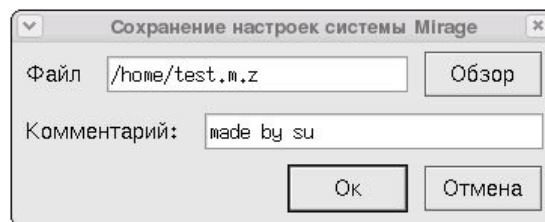


Рисунок 6.1 – Диалоговое окно сохранения служебной базы данных

По нажатию кнопки "Ок" производится резервное копирование, в журнал регистрации записываются соответствующие события. Результаты выполнения операции выводятся на экран (рисунок 6.2).

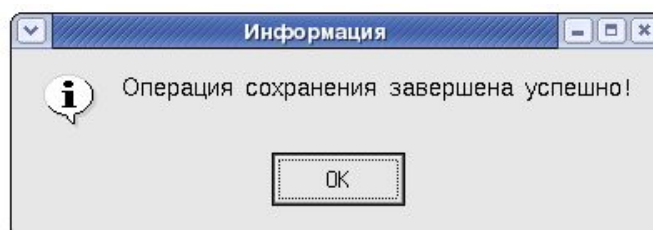


Рисунок 6.2

Примечание: при резервном копировании служебной базы данных директории и файлы пользователей – не сохраняются. Для резервного копирования файлов и файловых систем следует использовать соответствующие утилиты Linux

(Например `dump, restore`).

## 6.2 Восстановление

Восстановление системы производится в режиме конфигурирования из конфигуратора системы. При выборе пункта "Восстановление" производится рекурсивный поиск доступных архивных копий в директории `/mirage` и открывается диалог для выбора архивной копии для восстановления (рисунок 6.3).

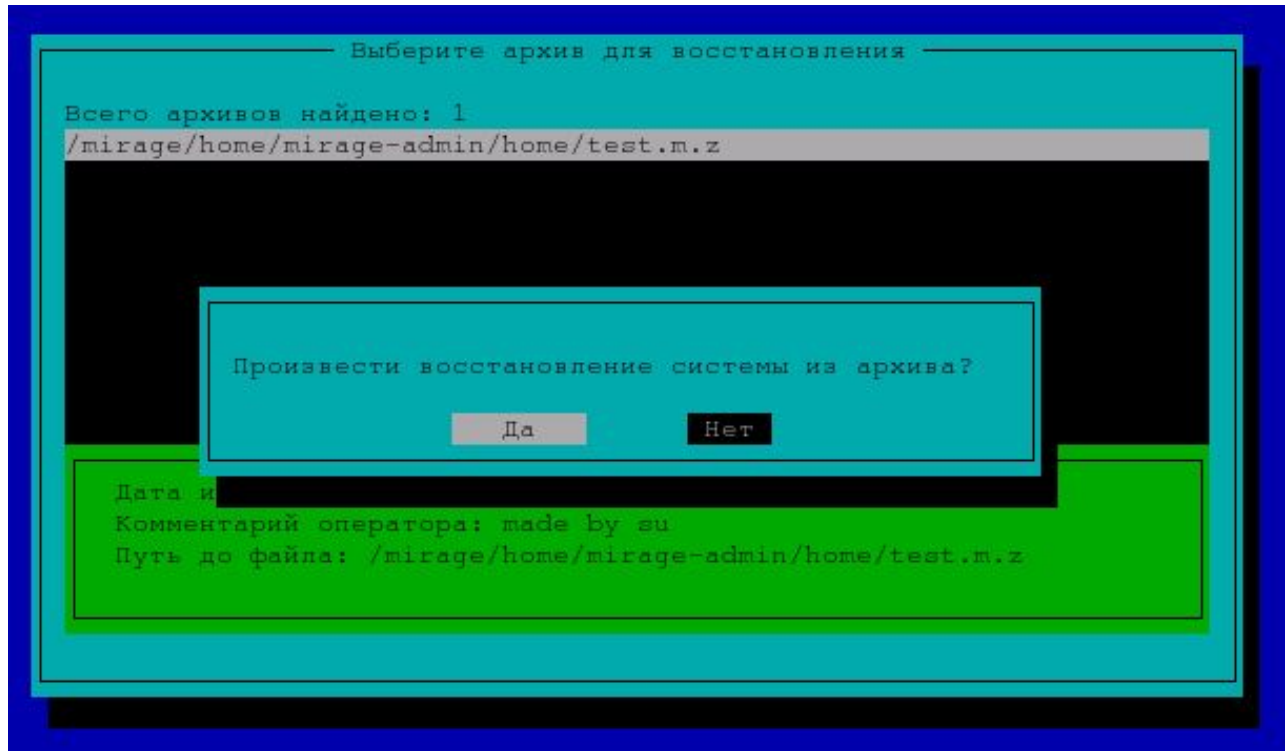


Рисунок 6.3 – Диалоговое окно выбора архива для восстановления

После подтверждения выбора производится восстановление системы, результаты операции выводятся на экран (рисунок 6.4).

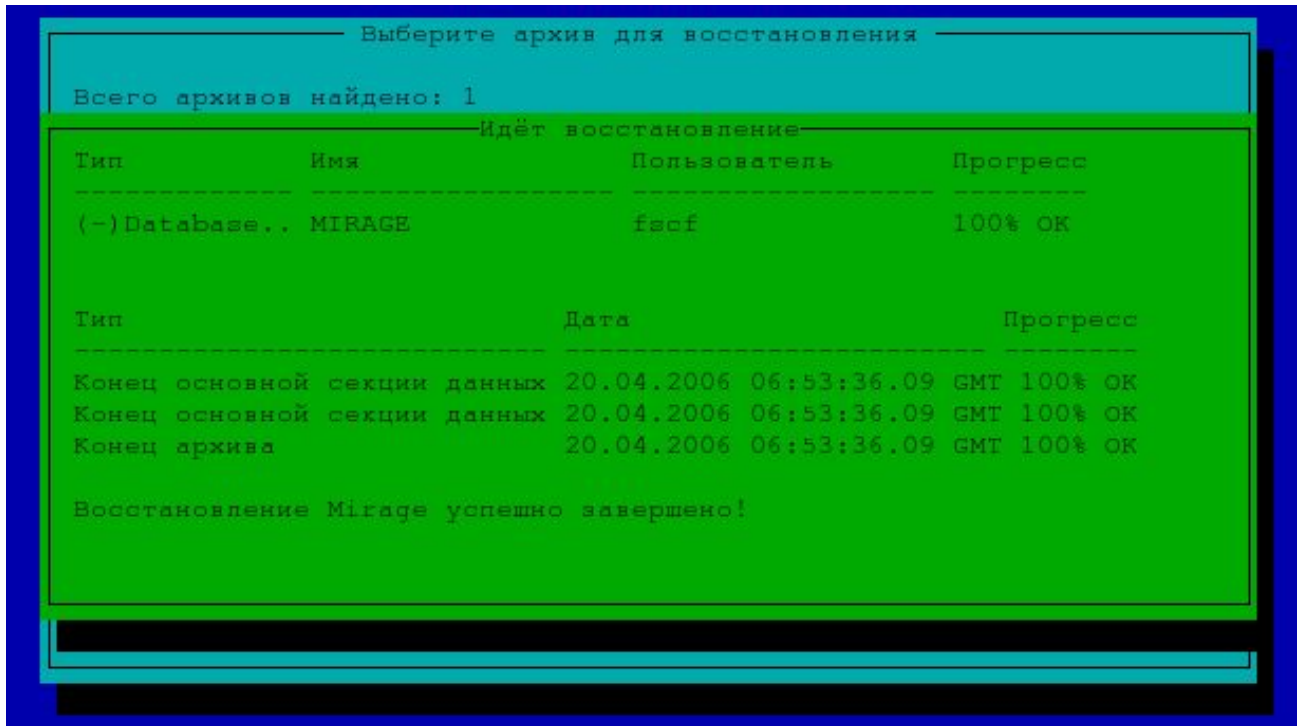


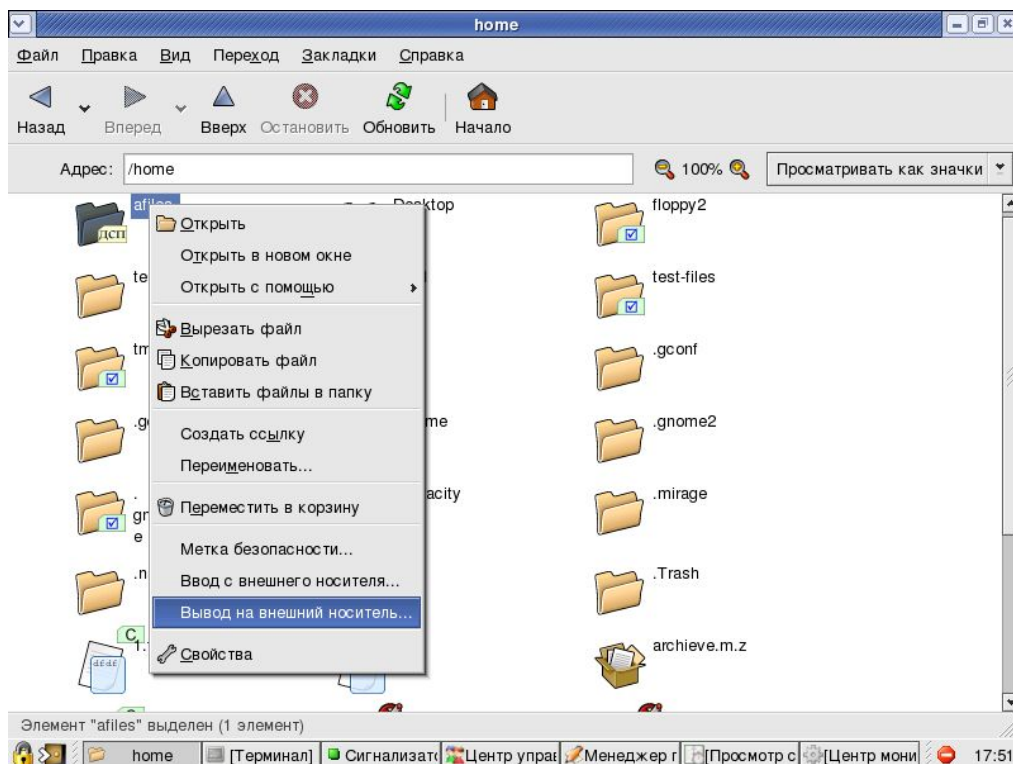
Рисунок 6.4 – Результаты восстановления

## 7. ВВОД И ВЫВОД ИНФОРМАЦИИ НА ВНЕШНИЕ НОСИТЕЛИ

Ввод/вывод информации (файлов) на внешние носители (дискеты, USB-диски) производится администратором безопасности на терминальном сервере. Ввод/вывод информации непосредственно с терминала запрещён.

### 7.1 Вывод на внешний носитель

Для вывода файла, группы файлов или каталогов, необходимо выделить необходимые файлы/каталоги и, нажав правую кнопку мыши, вызвать контекстное меню. В контекстном меню следует выбрать пункт "Вывод на внешний носитель" (рисунок 7.1). В появившемся диалоговом окне (рисунок 7.2) следует выбрать устройство для вывода и указать его идентификатор. После нажатия кнопки "Ок" необходимо вставить дискету в дисковод или USB-устройство в разъём USB-интерфейса сервера. После нажатия кнопки "Ок" будет произведено копирование файлов на устройство. Результат выполнения операции будет показан на экране (рисунок 7.3).



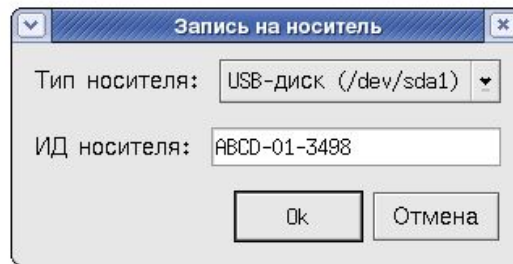


Рисунок 7.2 – Выбор устройства для ввода-вывода

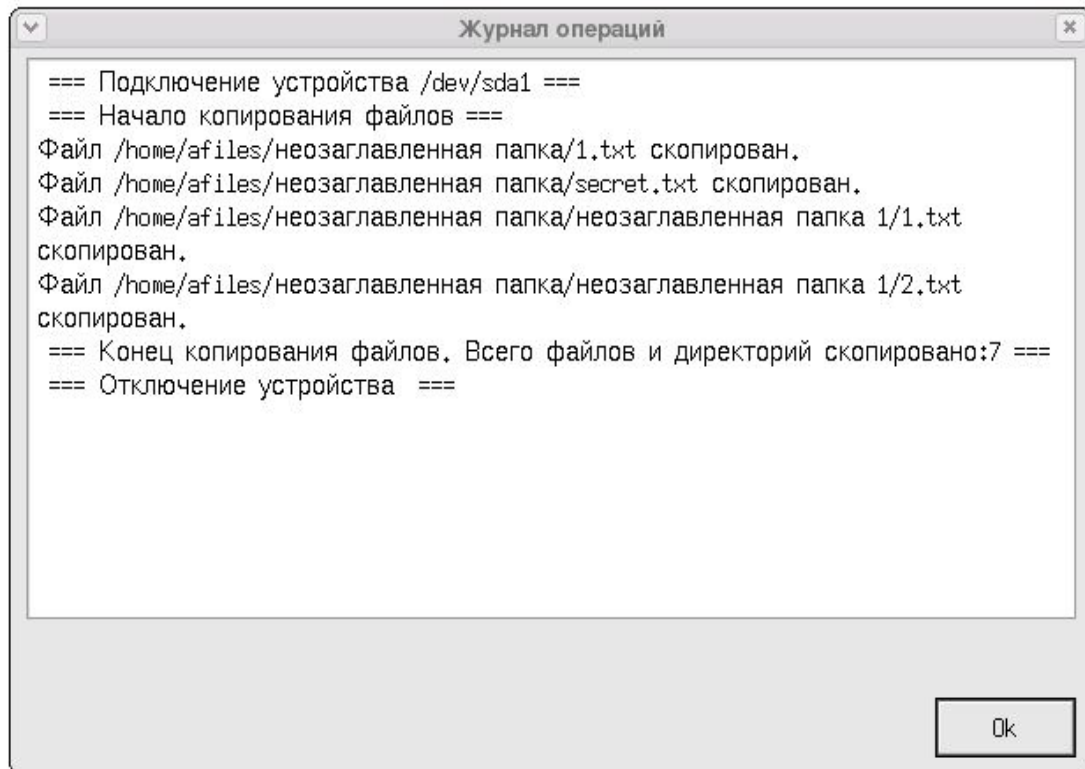


Рисунок 7.3 – Журнал операций ввода-вывода

Примечание: если на устройстве файлы с таким именем существуют, то они будут перезаписаны.

## 7.2 Ввод с внешнего носителя

Для ввода информации с внешнего носителя необходимо выделить каталог, в который будут копироваться вводимые файлы и, нажав правую кнопку мыши, вызвать контекстное меню. В контекстном меню следует выбрать пункт "Ввод с внешнего носителя" (рисунок 7.4). В появившемся диалоговом окне (рисунок 7.2) следует выбрать устройство для вывода, и указать его идентификатор. После нажатия кнопки "Ок" необходимо вставить дискету в дисковод или USB-устройство в разъем USB-интерфейса сервера. После нажатия кнопки "Ок" будет произведено копирование всех файлов с устройства. Результат выполнения операции

будет показан на экране (рисунок 7.3).

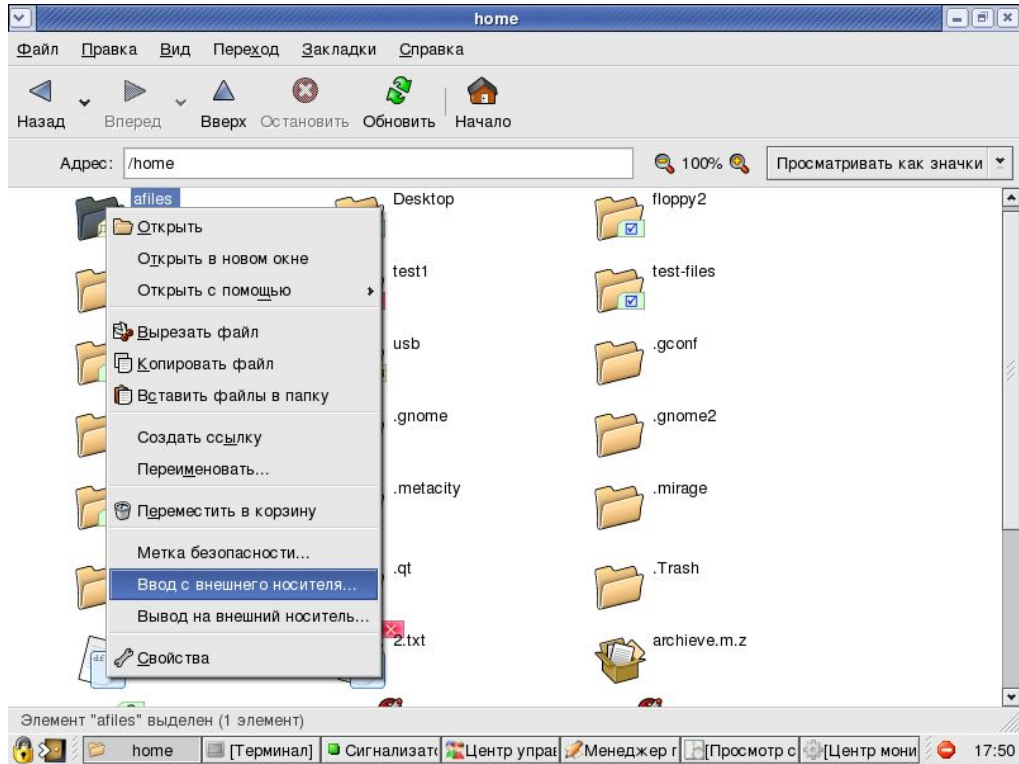


Рисунок 7.4 – Контекстное меню. Выбор операции “Ввод с внешнего носителя”

Примечание: если в папке файлы с таким именем существуют, то они будут перезаписаны.