Смоленский колледж телекоммуникаций (филиал) СПбГУТ
ФГОБУ ВПО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Дипломный проект на тему: «Модернизация существующей системы защиты информации предприятия связи»

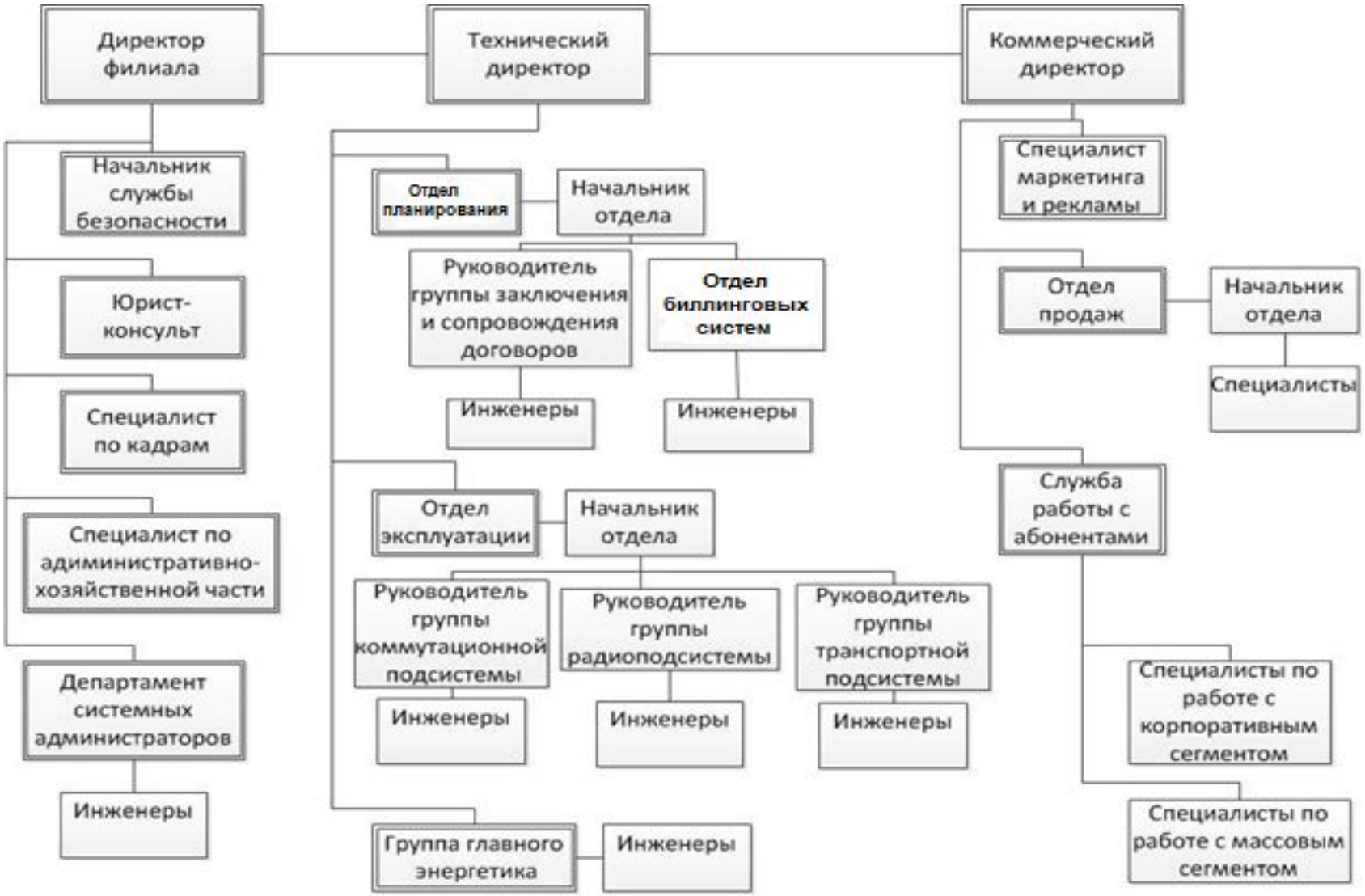
Студента группы СП 9316
Кривченков Д.В.

Руководитель: Грубник Е.М.

Цель проекта - повышение уровня защищенности системы информационной безопасности предприятия связи

Задачи:
- определение требуемого класса защищенности **автоматизированной системы обработки данных** (**АСОД**) предприятия связи;
- определение требований по защите информации от несанкционированного доступа для (**АСОД**) предприятия связи;
- классификация современных средств защиты информации, используемых в **системе защиты информации** (СЗИ) предприятия связи;
- разработка и систематизация настройки подсистемы разграничения доступа;
- расчет основных экономических показателей модернизации системы;

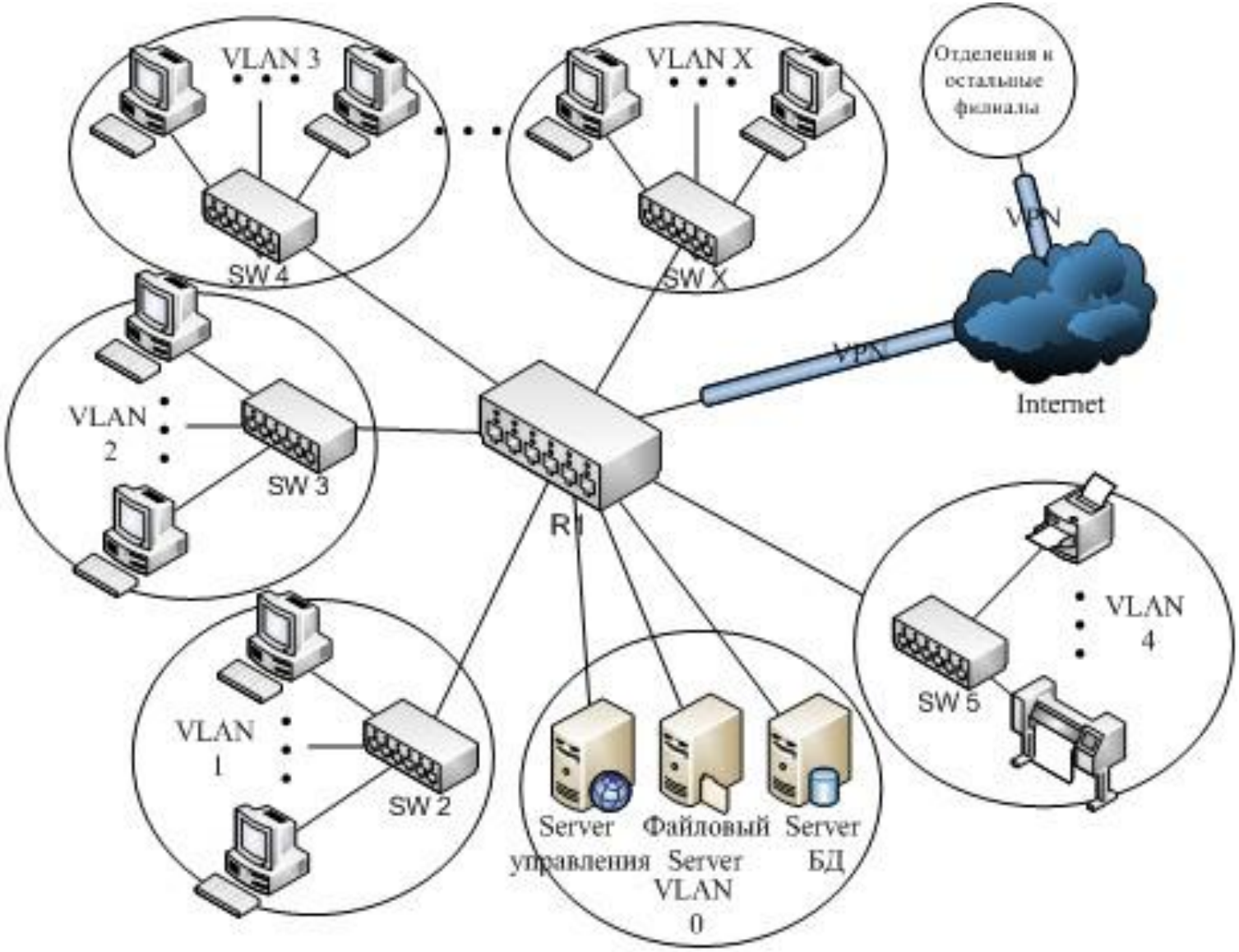
Организационная структура предприятия связи



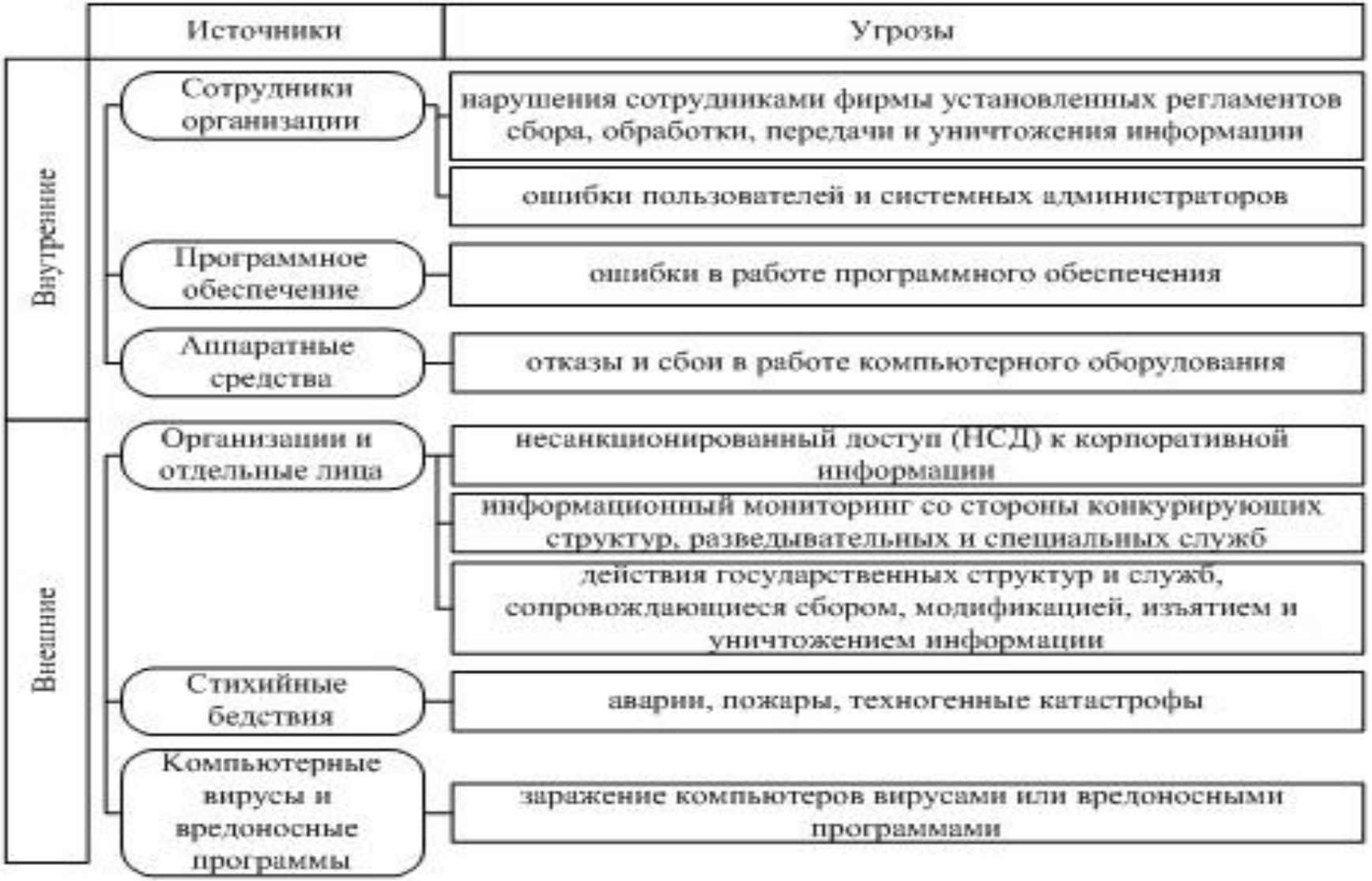
Характеристика исследуемых отделов предприятия связи

Наименование отдела	Основные функции отдела
Отдел биллинговых систем	- начисление платы клиентам за пользование предоставляемыми услугами связи, путем ведения учета использованного объема сервисов и применения соответствующей тарификации на каждый тип услуги. - осуществляет привязку паспортных данных клиентов к персональному номеру в системе; - операции внесения денежных средств на персональный счет клиента; - учет использованного объема предоставляемых сервисов; - управление персональными системами тарификации (тарифными планами); - операции по расчету и списанию необходимого количества денежных средств с персонального счета клиента, исходя из закрепленной индивидуальной системы тарификации; - начисление и списание неоплачиваемых объемов пользования услугами в рамках программ лояльности.
Отдел кадров	Учет, обработка информации о сотрудниках, непосредственными контактами с персоналом. - сектор учета кадров - занимается приемом и увольнением работником, ведением соответствующей документации о всех изменениях среди штата, ведет учет рабочего времени. - сектор обучения и подготовки кадров - проводит предварительный узкоспециализированный курс дополнительного обучения новых сотрудников.
Отдел планирования	Разработка долгосрочной модели поведения компании, определяя, таким образом, вектор ее развития в перспективе.

Структурная схема информационной системы предприятия



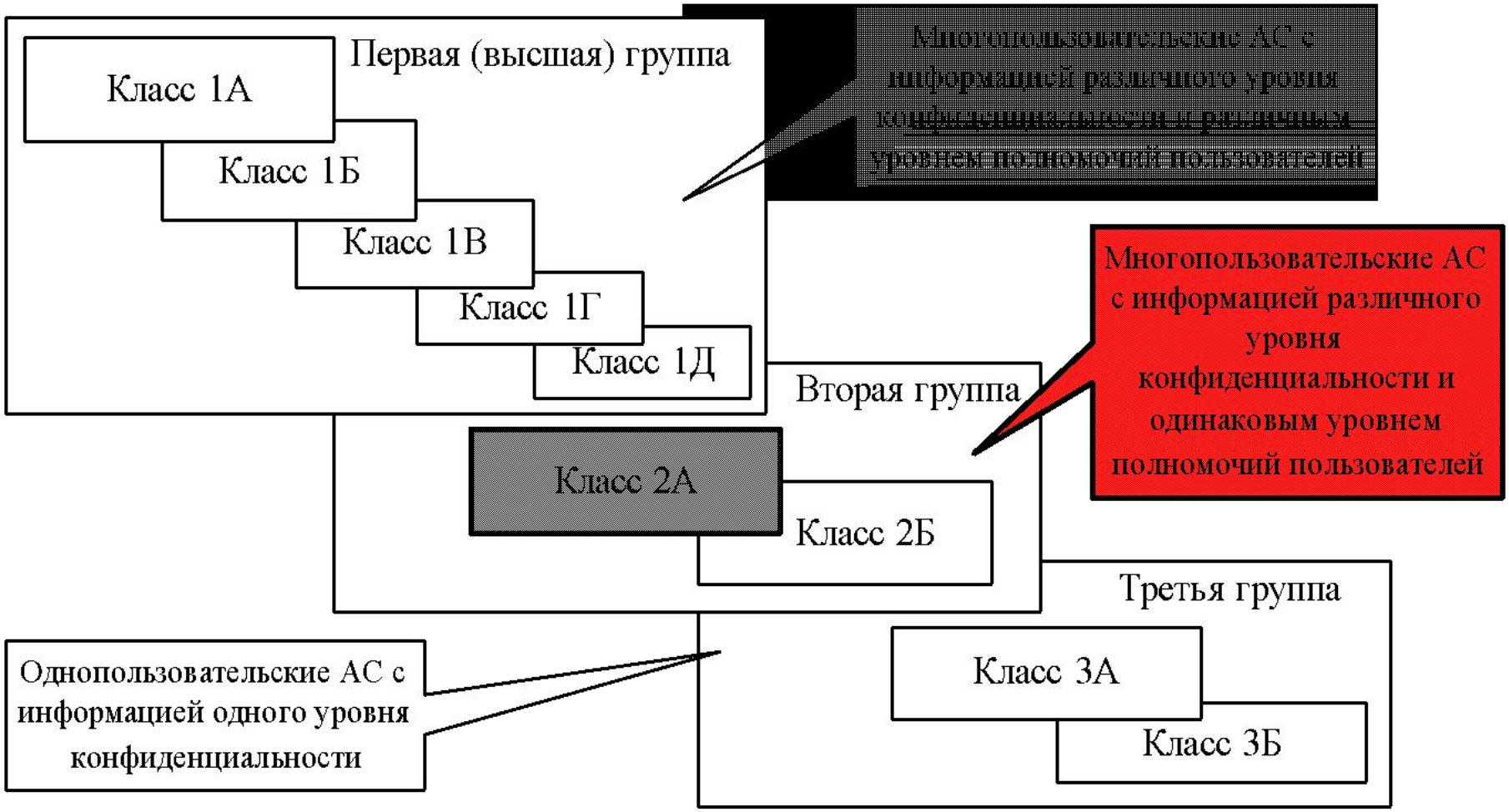
Классификация угроз на предприятии связи



Угрозы ИБ каждого из объектов АСОД

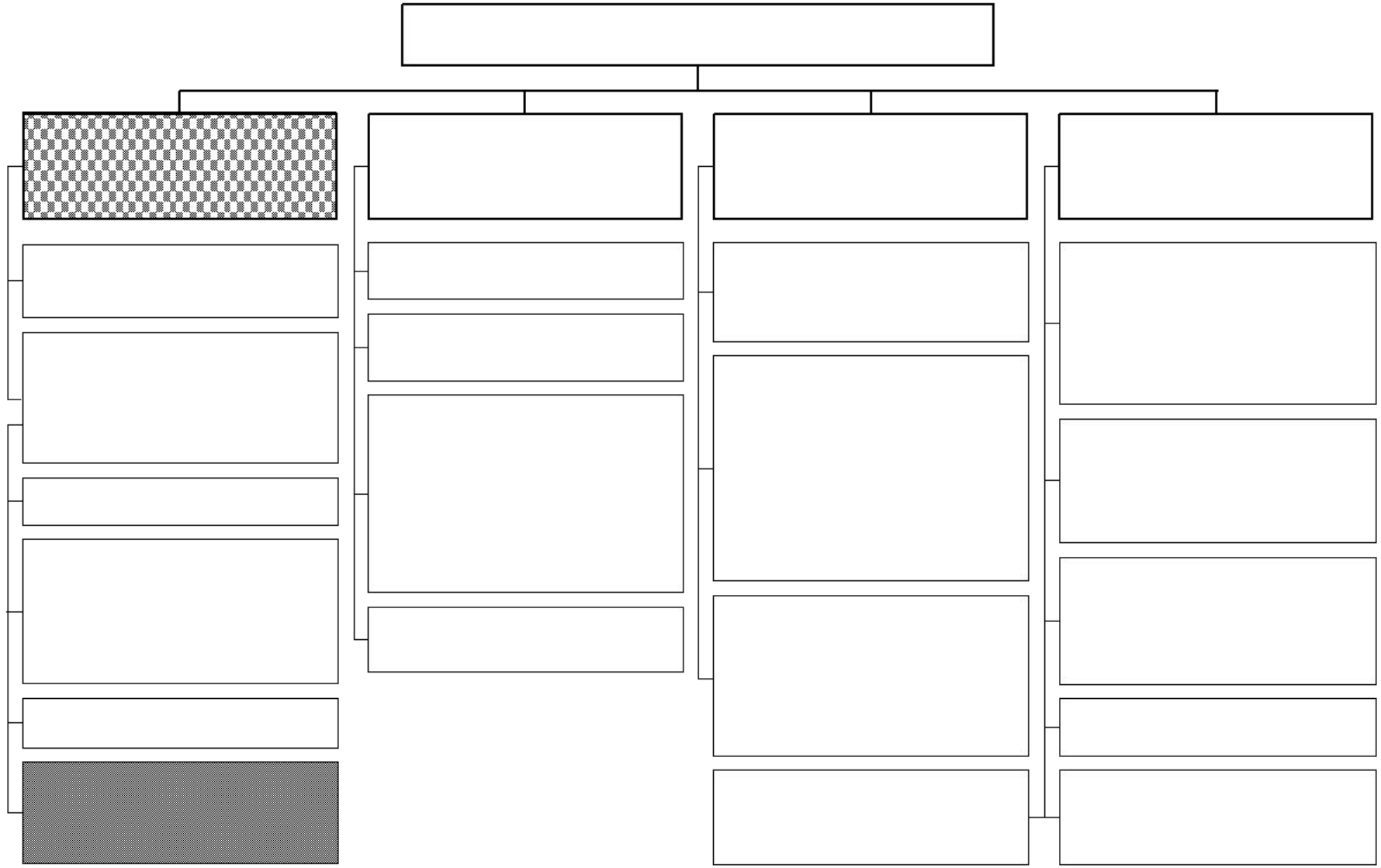
Объект АСОД	Угрозы ИБ
АРМ сотрудника	Копирование информации на носители
	Установка и использование «левого» ПО
	Заражение компьютера вирусами
	Ошибки оператора при эксплуатации СВТ
	Ошибки оператора при эксплуатации программных средств
	Несанкционированный доступ к ресурсам АС и дальнейшего его использования (копирование, модификации, удаления)
Сервер БД	Копирование информации
	Доступ к информации, путем нарушения функционирования
	Ошибки пользователей при эксплуатации программных средств
Файловый сервер	Изменение информации
	Копирование информации
	Удаление информации
	Разглашение защищаемой информации путем передачи носителей информации, лицам не имеющих права доступа
Сервер управления	Незаконное получение паролей и др. реквизитов разграничения доступа.
	Блокировка доступа зарегистрированных пользователей

Определение требуемого класса защищенности АСОД (в соответствии с Руководящем Документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации)

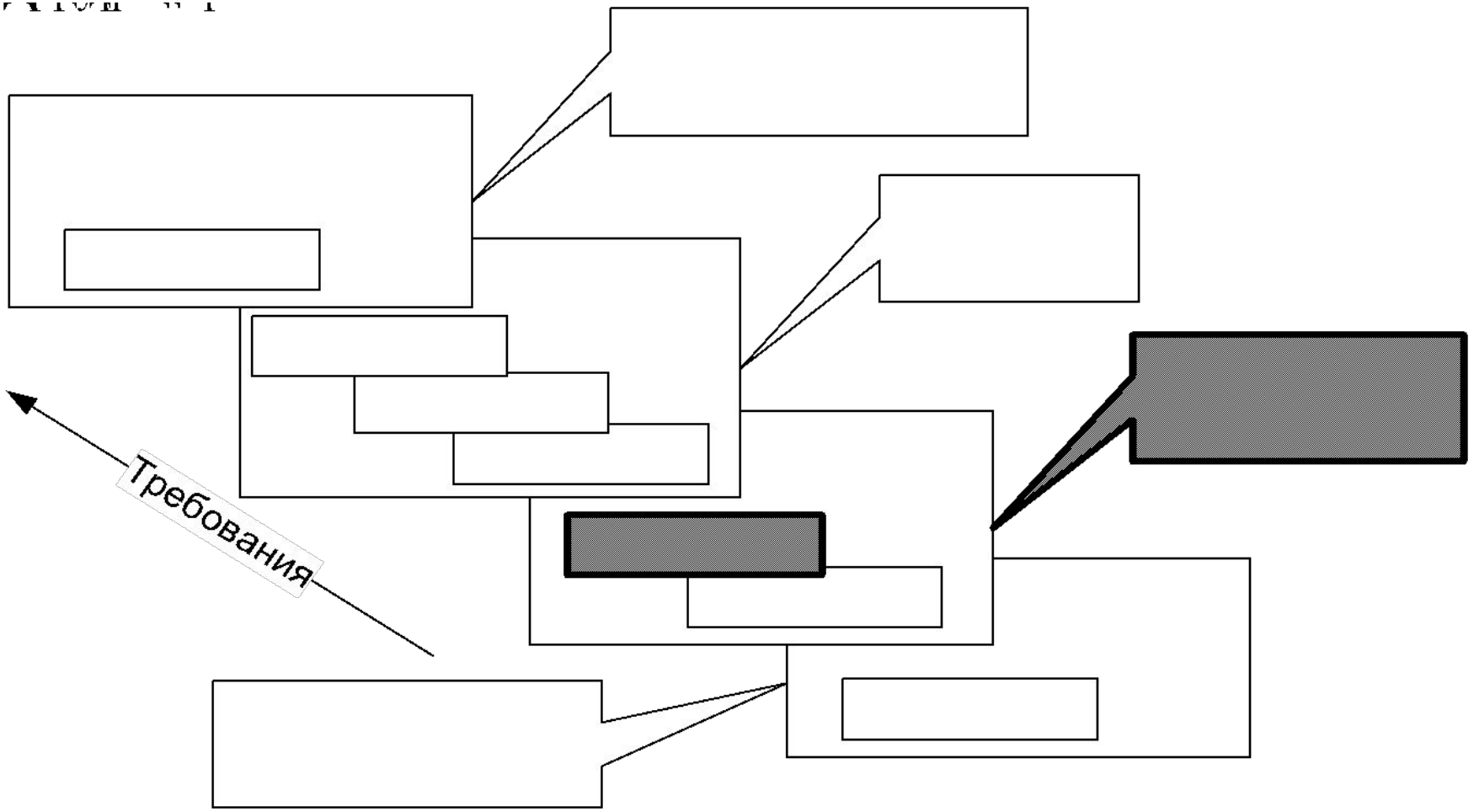


Для рассматриваемой АСОД характерен 2А класс защищенности.

Определение требуемого класса защищенности АСОД



Определение требуемого класса защищенности СВТ в АСОД (в соответствии с Руководящем Документом «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации»)



Для класса защищенности АС 2А характерна 2-я группа классов защищенности СВТ, и класс 5 или 6 в зависимости от секретности используемой информации.
Для нас характерен **5 класс**

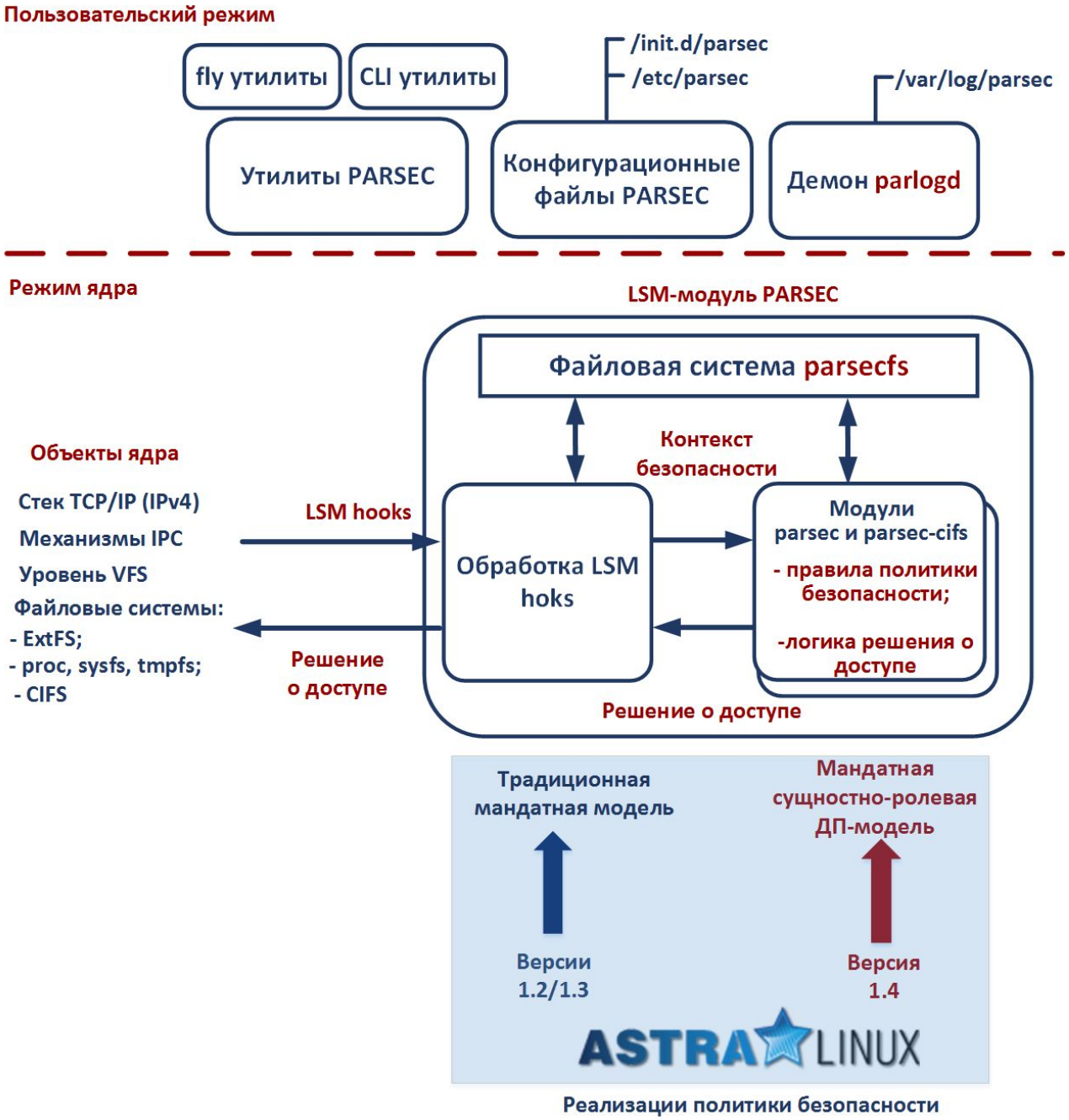
Определение подхода к выбору методов и средств защиты АСОД

Подсистема управления доступом

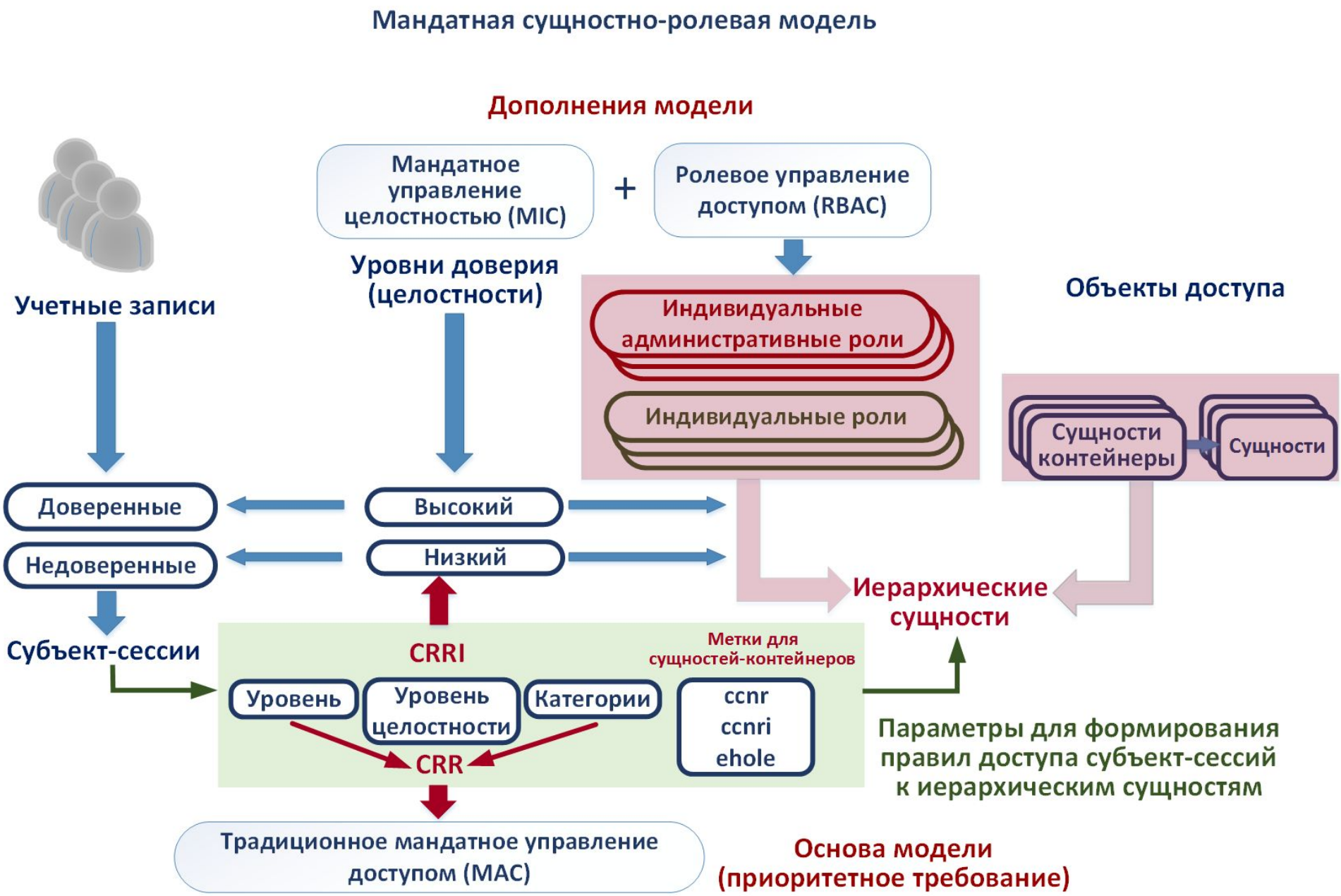
Требования	СЗИ	Компетентность
1 Идентификация, проверка подлинности и контроль доступа субъектов	AD, Firewall, Брандмауэр, Электронные ключи	Присутствуют недостатки
В систему	AD	Удовлетворяет в полной мере
К терминалам, ЭВМ, каналам связи, внешним устройствам ЭВМ	AD, Firewall, Брандмауэр	Удовлетворяет в полной мере
К программам	AD, Электронные ключи	Удовлетворяет в полной мере
К томам, каталогам, файлам, записям, полям записей	**AD**	**Проблемы с наследованием прав доступа**
2 Управление потоками информации	VPN, VLAN, Firewall, Брандмауэр	Удовлетворяет в полной мере

Необходимо решение проблемы с наследованием прав доступа в контроле доступа к томам, каталогам, файлам, записям, полям записи.

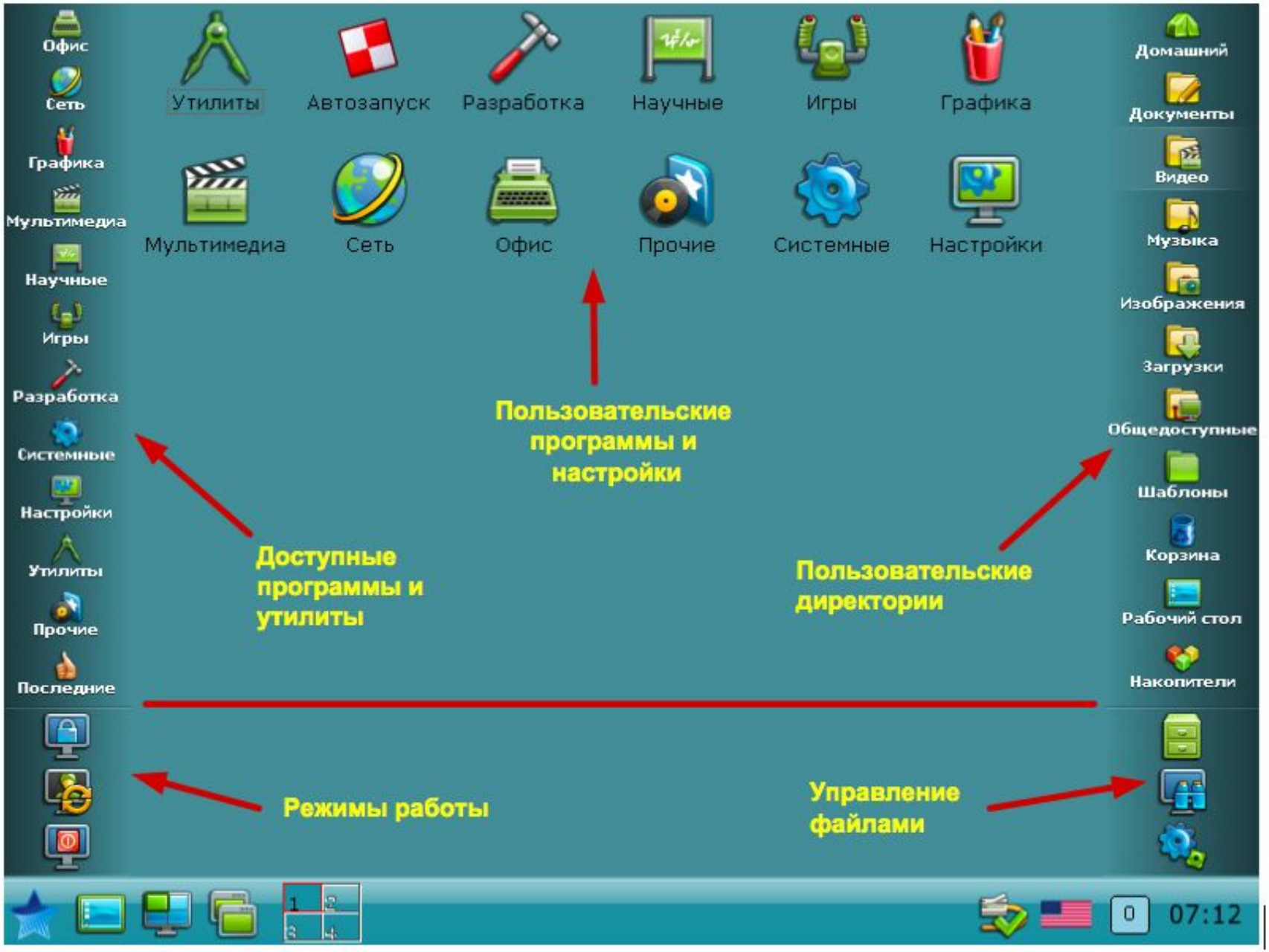
Подсистема безопасности PARSEC



МАС-модель в мандатной сущностно-ролевой ДП-модели



Использование защищенной рабочей среды Fly в AstraLinux



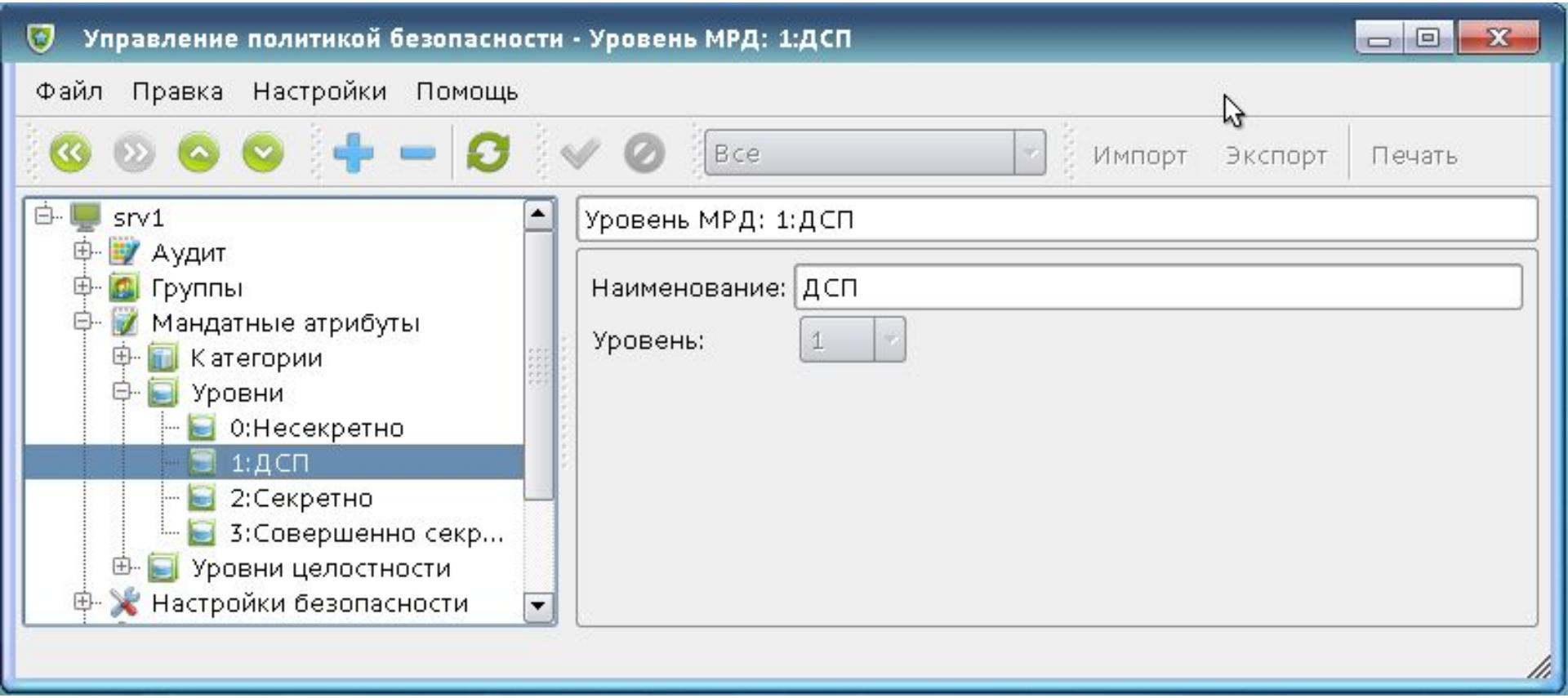
Скрипт инициализации правил разграничения доступа

```
pdp-init-fs          [----]  0 L:[  1+27  28/ 28] *(593 / 593b) <EOF>
#!/bin/bash

sysmaxlev=3
sysmaxilev=0
sysmaxcat=0xffffffffffffffff

sysmaxlbl="$sysmaxlev:0:$sysmaxcat"

pdp-flbl "$sysmaxlev:$sysmaxilev:$sysmaxcat:CCNRALL" /
pdp-flbl "$sysmaxlbl:ccnr" /dev

pdp-flbl "$sysmaxlbl:ccnr,ehole" /tmp

pdp-flbl "$sysmaxlbl:ccnr" /var/
pdp-flbl "$sysmaxlbl:ccnr" /var/private/
pdp-flbl "$sysmaxlbl:ccnr" /var/private/*
pdp-flbl "$sysmaxlbl:ccnr" /var/run/
pdp-flbl "$sysmaxlbl:ccnr" /var/spool/
pdp-flbl "$sysmaxlbl:ccnr,ehole" /var/run/shm/
pdp-flbl "$sysmaxlbl:ccnr,ehole" /var/mail/

pdp-flbl "$sysmaxlbl:ccnr" /home/
pdp-flbl "$sysmaxlbl:ccnr" /home/.pdp/
```

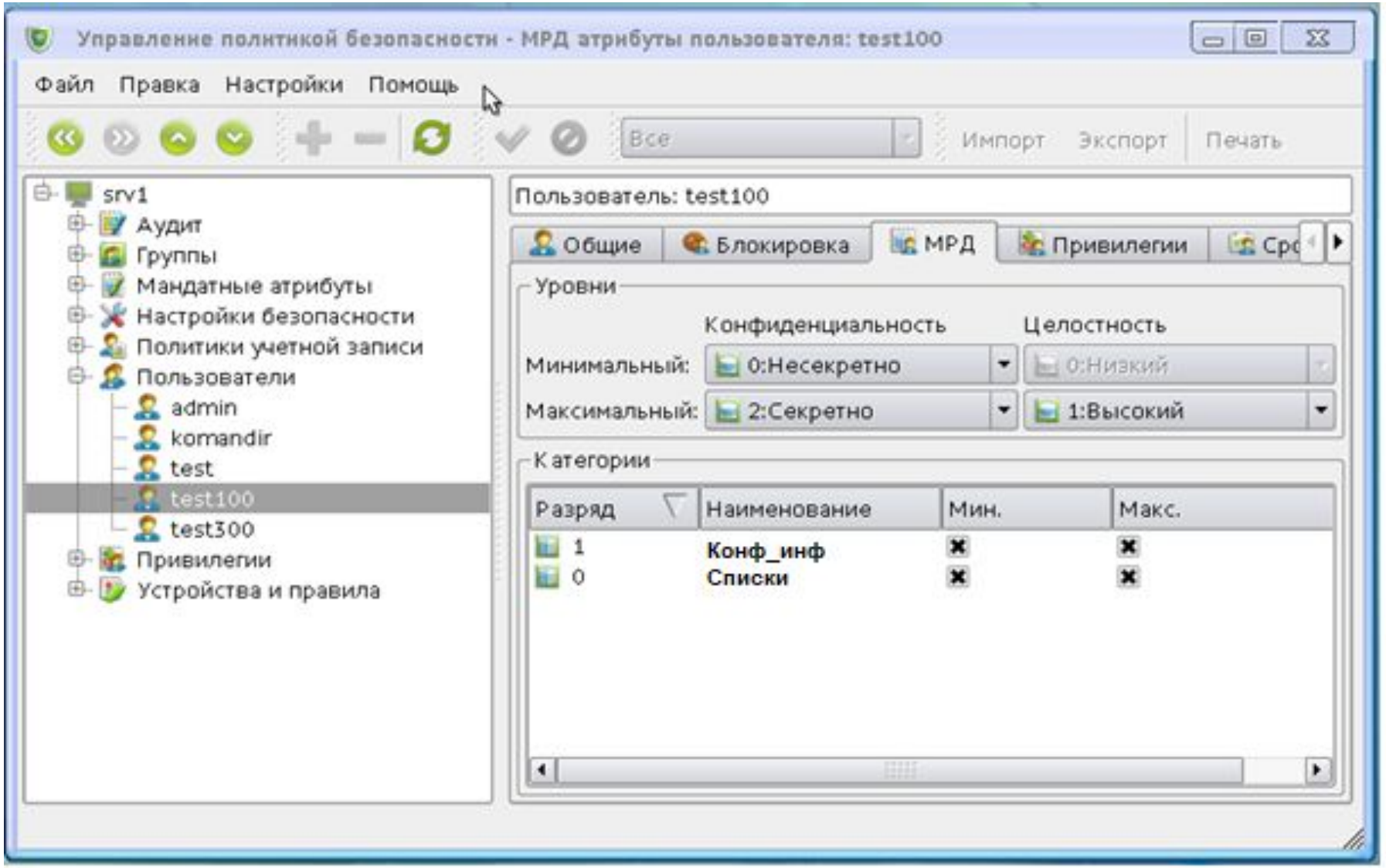
Pdp-утилиты в настройках подсистемы PARSEC

```
30 setenv                [----] 57 L:[  1+ 8   9/ 33] *(159 / 491
#!/bin/sh

. /lib/lsb/init-functions

setenv()
{
<------>CHMAC="/usr/sbin/pdp-flbl"
<------>CHMAC_EQU="$CHMAC -f :::ehole"
<------>EQU_FILES="/dev/tty /dev/dsp /dev/snd/* /run/shm"
<------>#/dev/ptmx /dev/null /dev/full
<------>for EQUF in $EQU_FILES; do
<------><------>$CHMAC_EQU $EQUF
<------>done
<------>/bin/mount --make-rshared /
<------>/usr/sbin/pdp-init-fs
<------>return $?
```

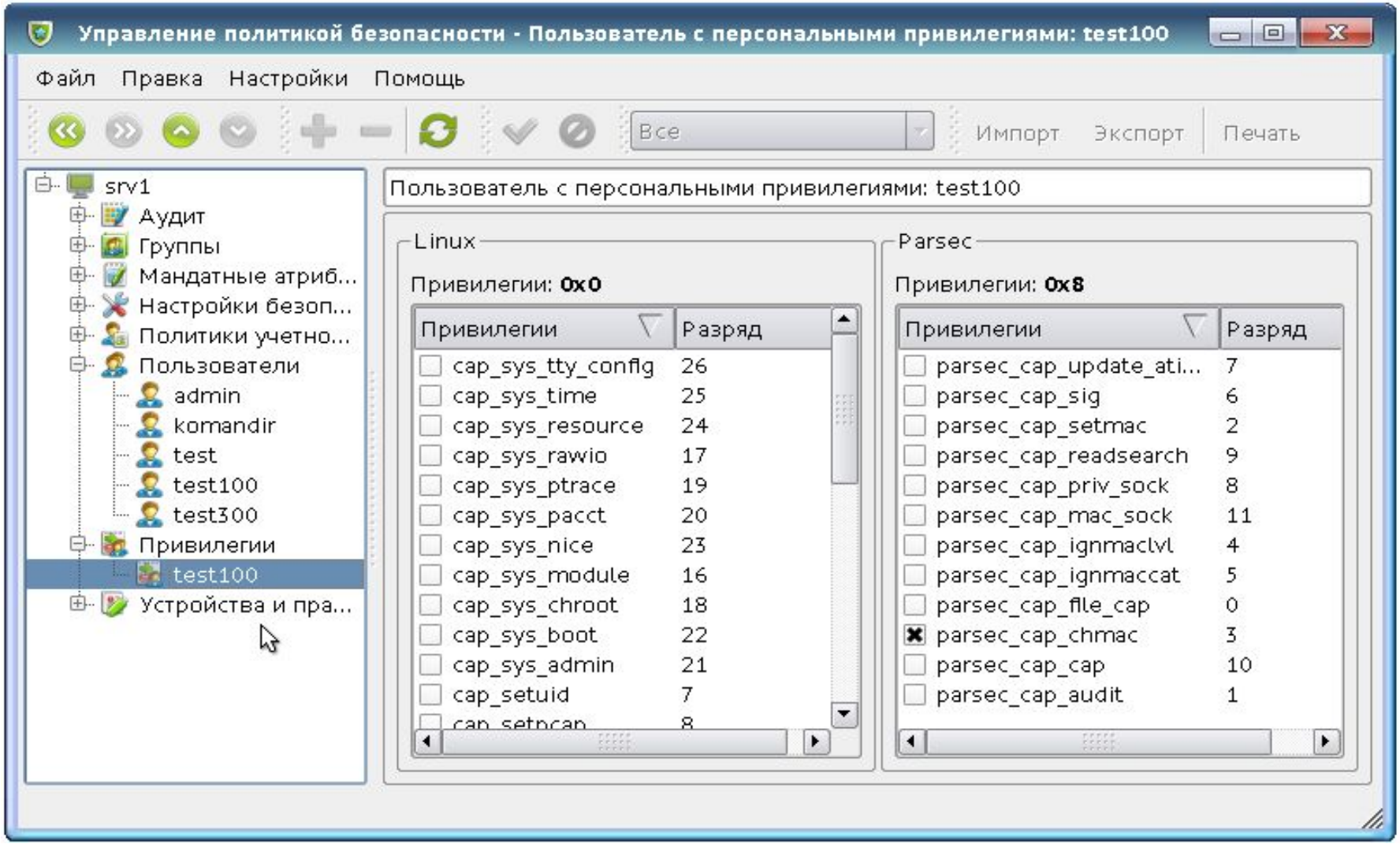
Задание уровней доступа и конфиденциальности для ОССН



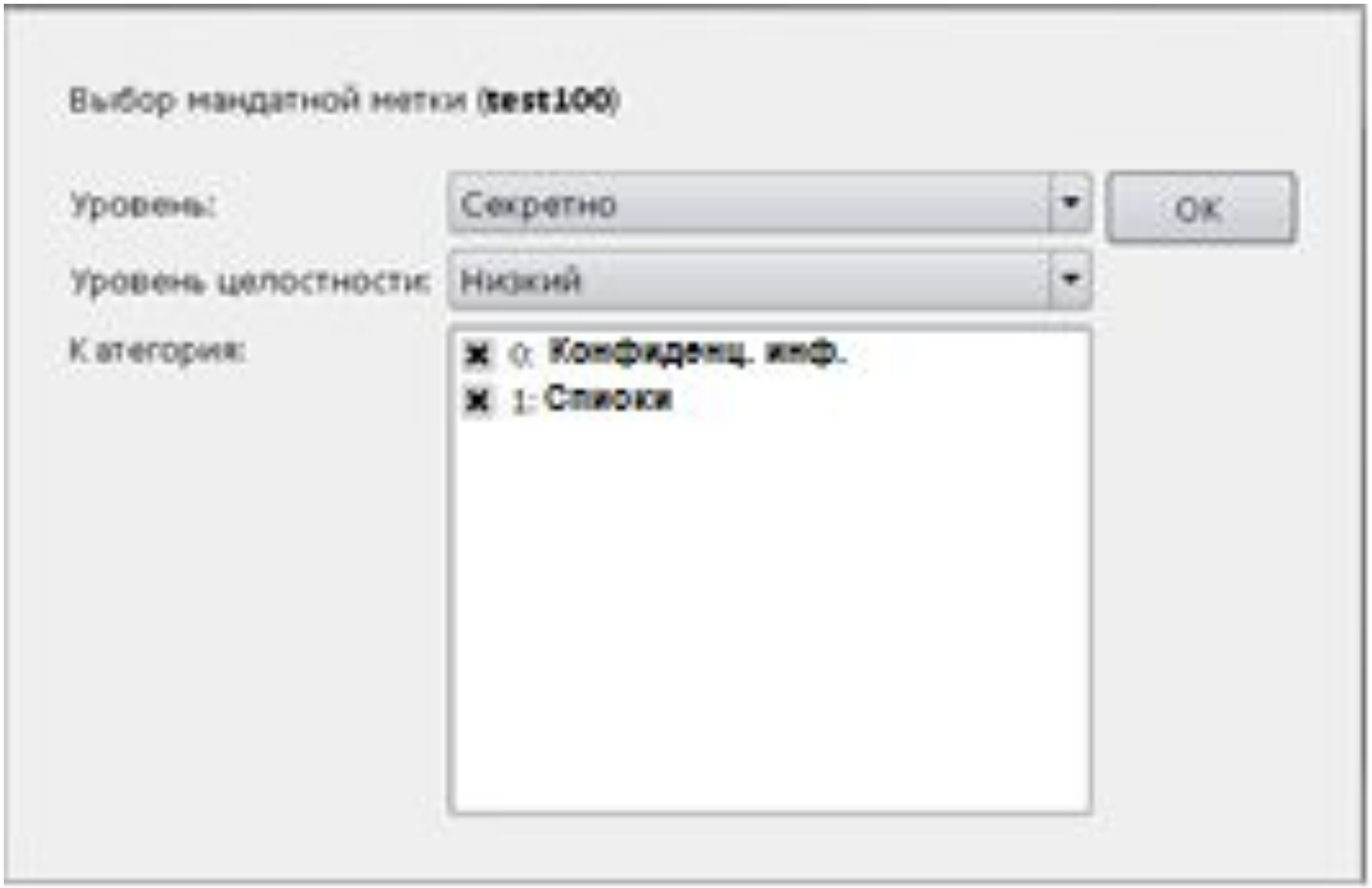
Назначение учётной записи пользователя уровня доступа и набора неиерархических категорий



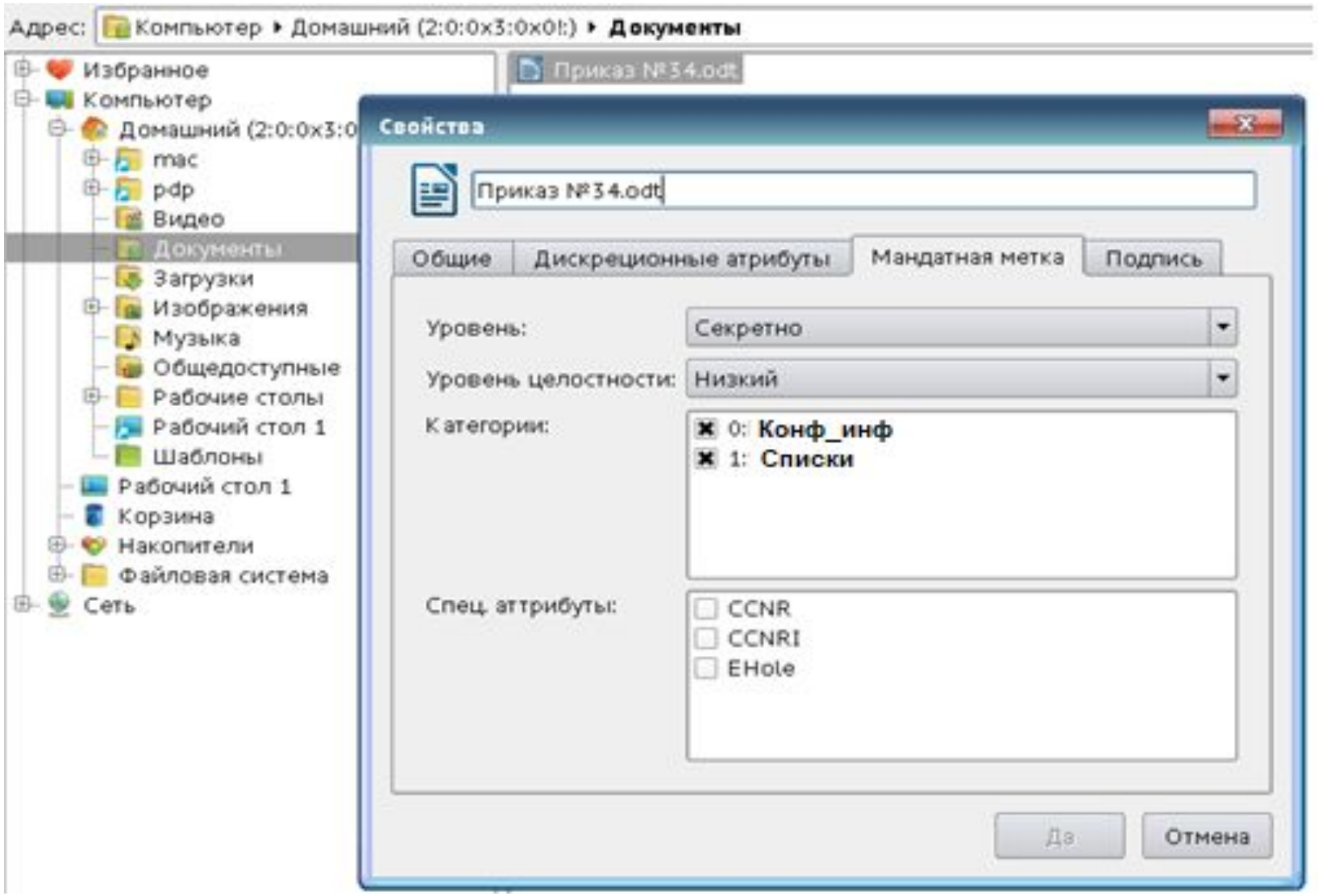
Задание привилегий для администрирования мандатного управления доступом



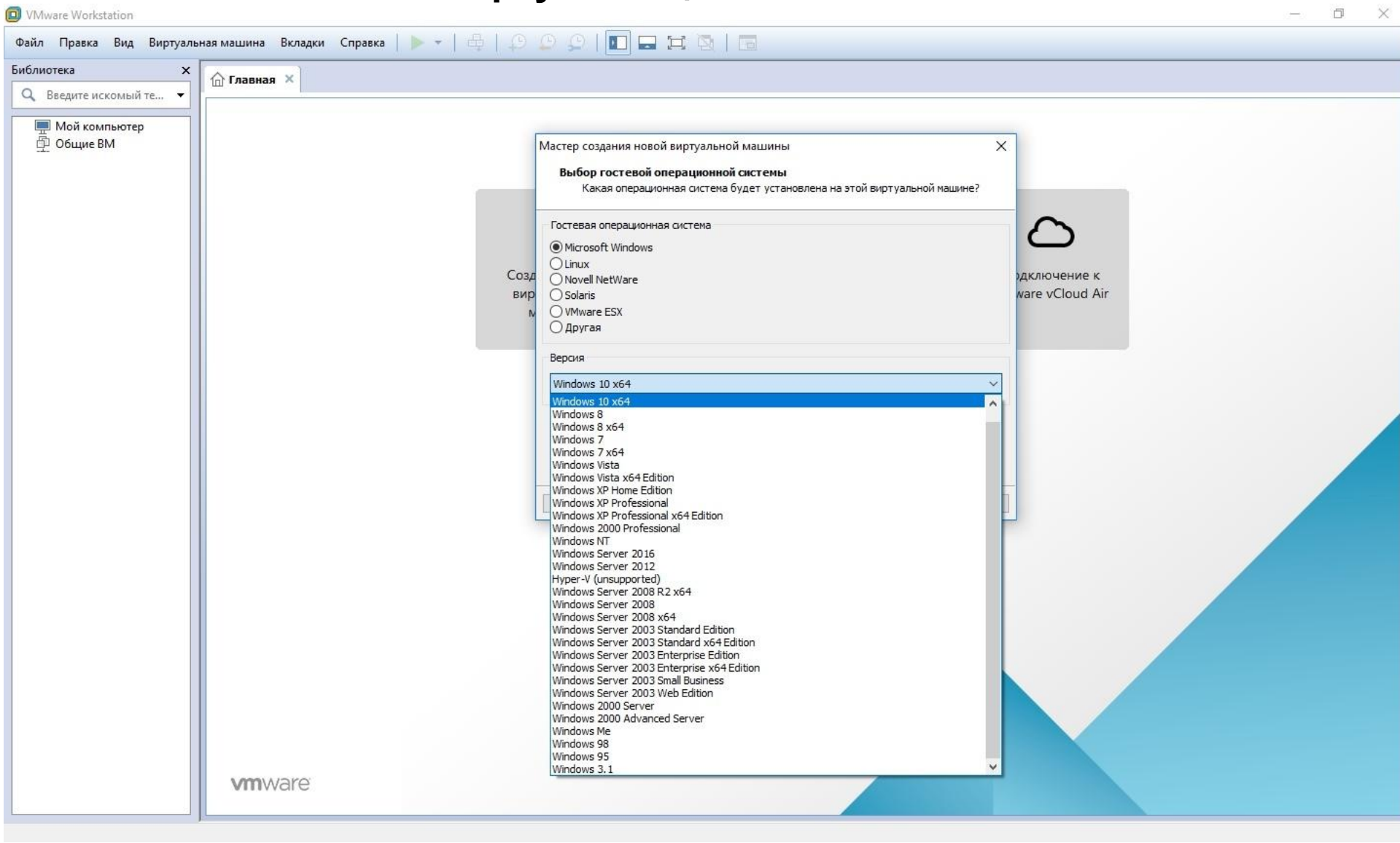
Ввода параметров мандатного управления доступом при входе пользователя в ОССН



Администрирование параметров мандатного управления доступом к файлу



Настройка среды виртуализации



Результаты тестирования

```
---[rwx.sh]: start test
# Проверка механизма файловой системы RWX
Проверка чтения файла владельцем...УСПЕШНО
Проверка записи для владельца...УСПЕШНО
Проверка чтения для группы владельца...УСПЕШНО
Проверка записи для группы владельца...УСПЕШНО
Проверка чтения для других...УСПЕШНО
Проверка записи для других...УСПЕШНО
Test PASS
---[rwx.sh]: stop test
---[acl.sh]: start test
# Testing correct Acl RWX mechanism
Выставление ACL для владельца...проверка битовой маски УСПЕШНО
Выставление битовой маски для владельца...проверка ACL УСПЕШНО
Выставление ACL для группы...проверка битовой маски УСПЕШНО
Выставление битовой маски для группы...проверка ACL УСПЕШНО
Выставление ACL для прочих...проверка битовой маски УСПЕШНО
Выставление битовой маски для прочих...проверка ACL УСПЕШНО
Test PASS
---[acl.sh]: stop test
---[ipc_dac]: start test
PARSEC IPC/SIGNAL TEST: INFO: start...
progname = /usr/lib/parsec/tests/ipc_dac
DAC IPC test: INFO: Начинаем тест: PARSEC IPC/SIGNAL TEST...
DAC IPC test: INFO: Итерация 0.
DAC IPC test: INFO: Итерация 1.
DAC IPC test: INFO: Итерация 2.
DAC IPC test: INFO: Итерация 3.
DAC IPC test: INFO: Итерация 4.
DAC IPC test: INFO: Итерация 5.
DAC IPC test: INFO: Итерация 6.
DAC IPC test: INFO: Итерация 7.
DAC IPC test: INFO: Итерация 8.
DAC IPC test: INFO: Итерация 9.
DAC IPC test: INFO: DAC IPC test прошел успешно
DAC Signals test: INFO: Начинаем тест: PARSEC IPC/SIGNAL TEST...
DAC Signals test: INFO: Итерация 0.
DAC Signals test: INFO: Итерация 1.
DAC Signals test: INFO: Итерация 2.
DAC Signals test: INFO: Итерация 3.
DAC Signals test: INFO: Итерация 4.
DAC Signals test: INFO: Итерация 5.
DAC Signals test: INFO: Итерация 6.
DAC Signals test: INFO: Итерация 7.
DAC Signals test: INFO: Итерация 8.
DAC Signals test: INFO: Итерация 9.
DAC Signals test: INFO: DAC Signals test прошел успешно
PARSEC IPC/SIGNAL TEST: INFO: ТЕСТ УСПЕШЕН! ОБЩИЙ СТАТУС = 0
Test PASS
---[ipc_dac]: stop test
```