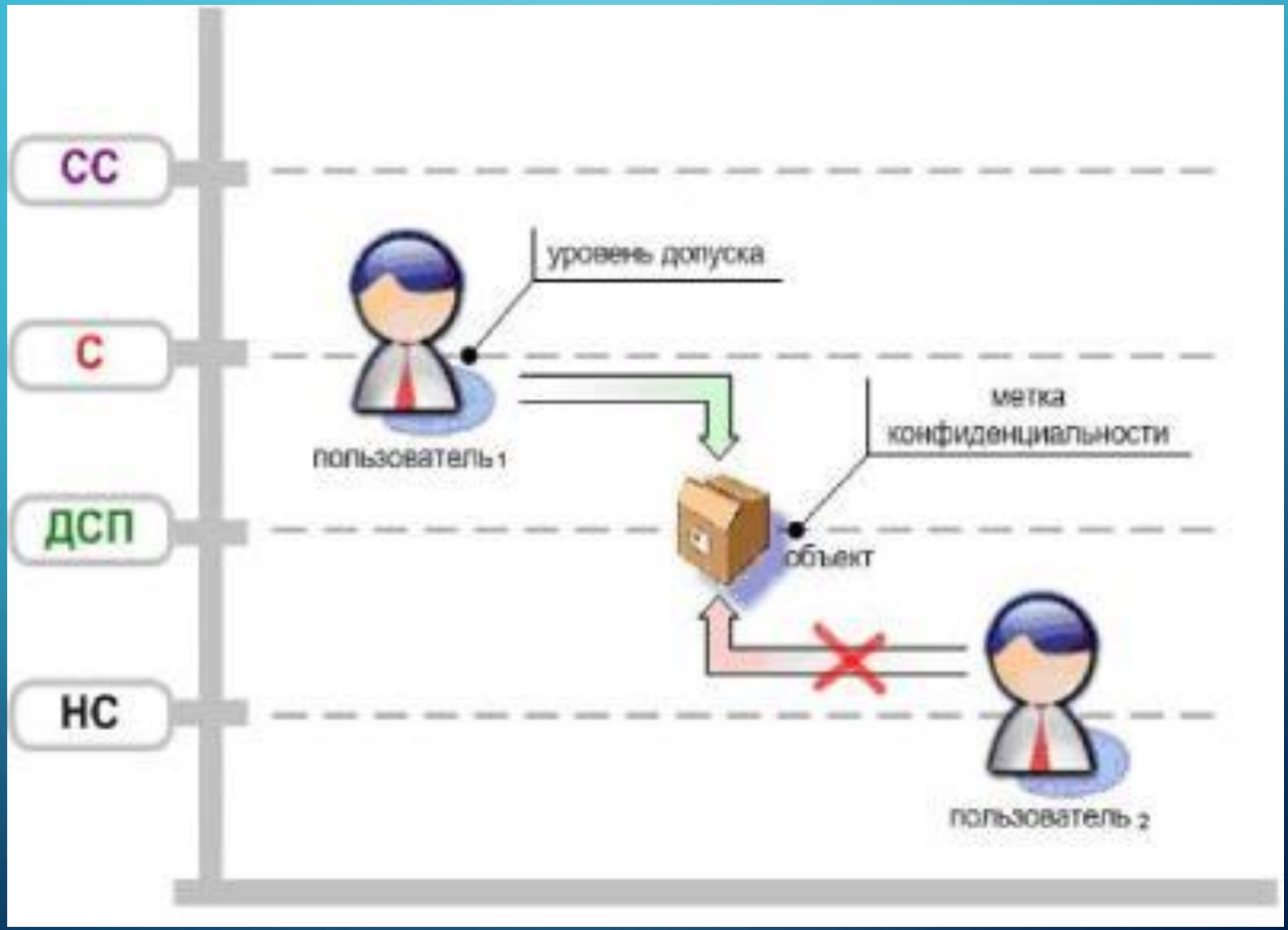
Презентация к выпускной квалификационной работе учащегося: Малинников Сергей Алексеевич ГРУППА 34 НК

На тему: Анализ дискреционного принципа контроля доступа к информации

Показатели защищенности(ГОСТ Р 50739-95)

- **Дискреционный принцип контроля доступа**
- **Мандатный принцип контроля доступа**
- Идентификация и Аутентификация
- Очистка памяти
- Изоляция модулей
- И т.д.


СС
С
ДСП
НС
уровень допуска
пользователь 1
метка конфиденциальности
объект
пользователь 2

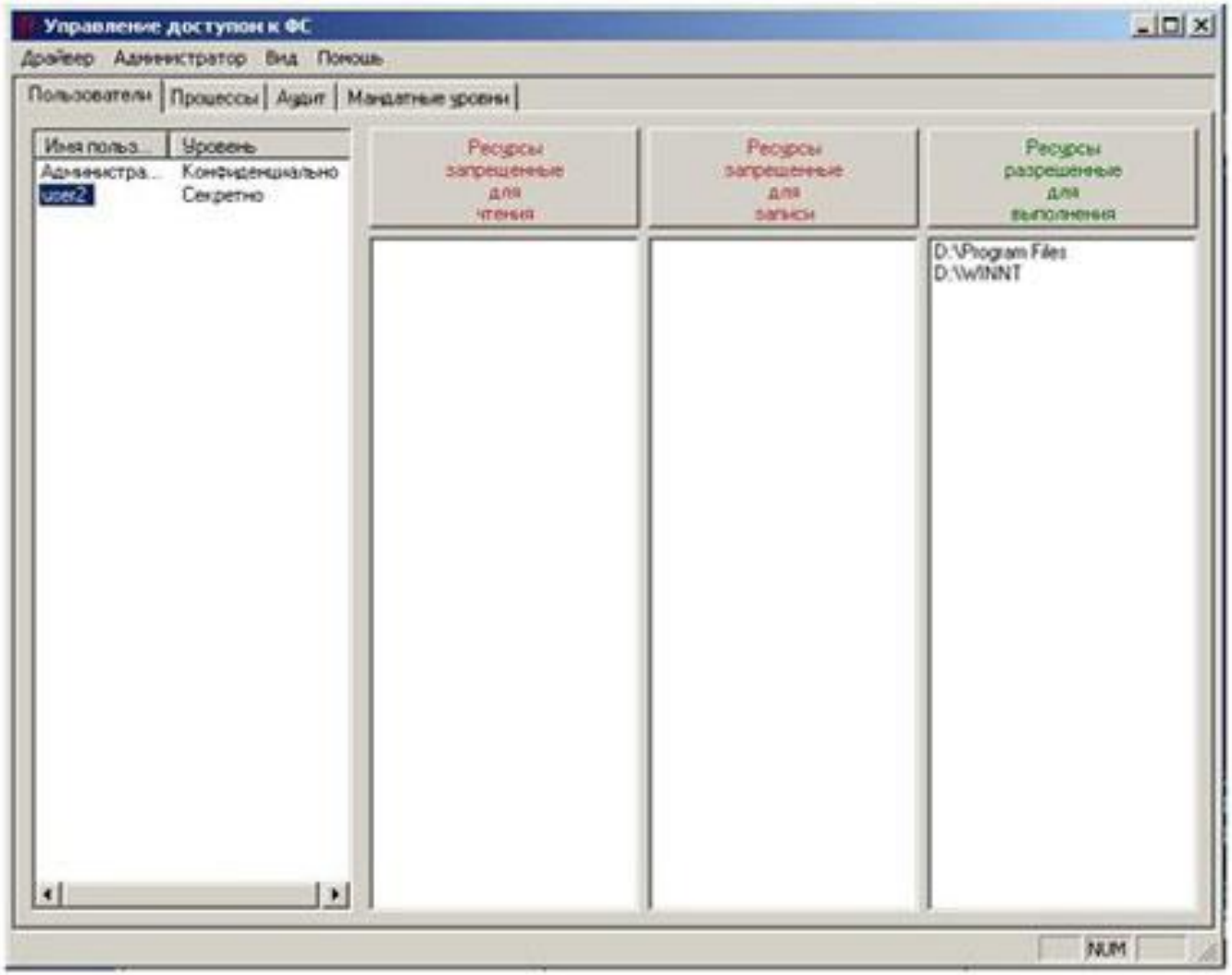
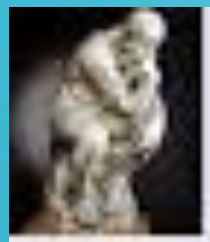


Рис.5.2 Интерфейс настройки дискреционного механизма контроля доступа

Дискреционная модель

- Явная выдача разрешений для каждого объекта системы.
- Пример – большинство операционных систем.
- Модель Харрисона-Руззо-Ульмана – матрица доступа.
- Гибче мандатного, но сложен в управлении.
- Улучшения:
  - Группировка пользователей.
  - Типы объектов.

MyShared



Основные методы управления доступом

Дискреционное управление доступом
(*Discretionary access control, DAC*. Также: контролируемое, разграничительное)

Ролевое управление доступом
(*Role Based Access Control, RBAC*. Дословно: управление доступом на основе ролей)

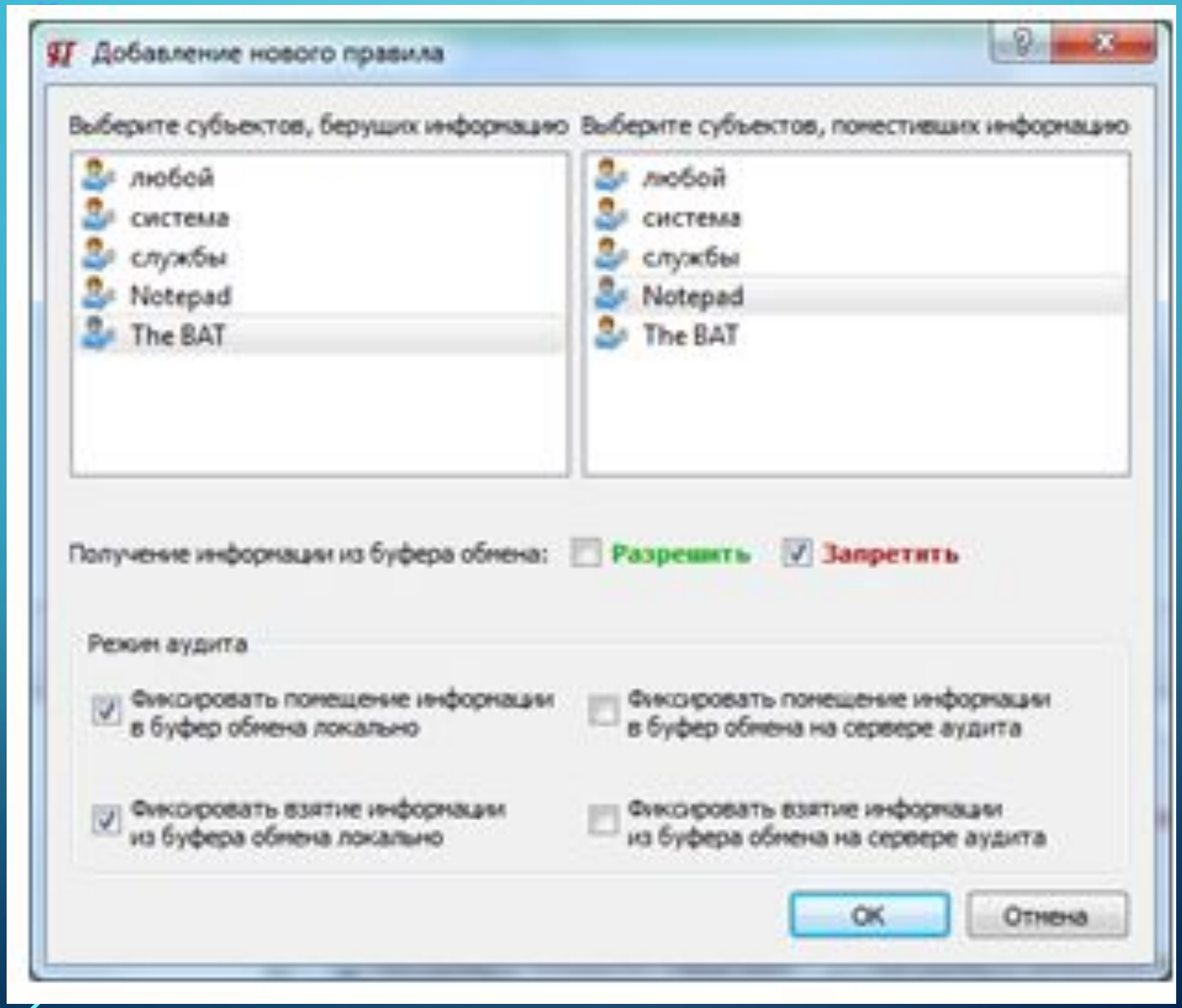
Мандатное управление доступом
(*Mandatory access control, MAC*. Также: обязательное, принудительное)


Служебные утилиты администрирования
Блок аудита
Блок идентификации и аутентификации
Реализация режима паузы неактивности
Аппаратные средства защиты
БД полномочий
Блок разграничения доступа к процедурам
Блок управления
Драйвер разграничения доступа
Драйвер фильтрации USB-устройств
Обеспечение непрерывности загрузки ОС

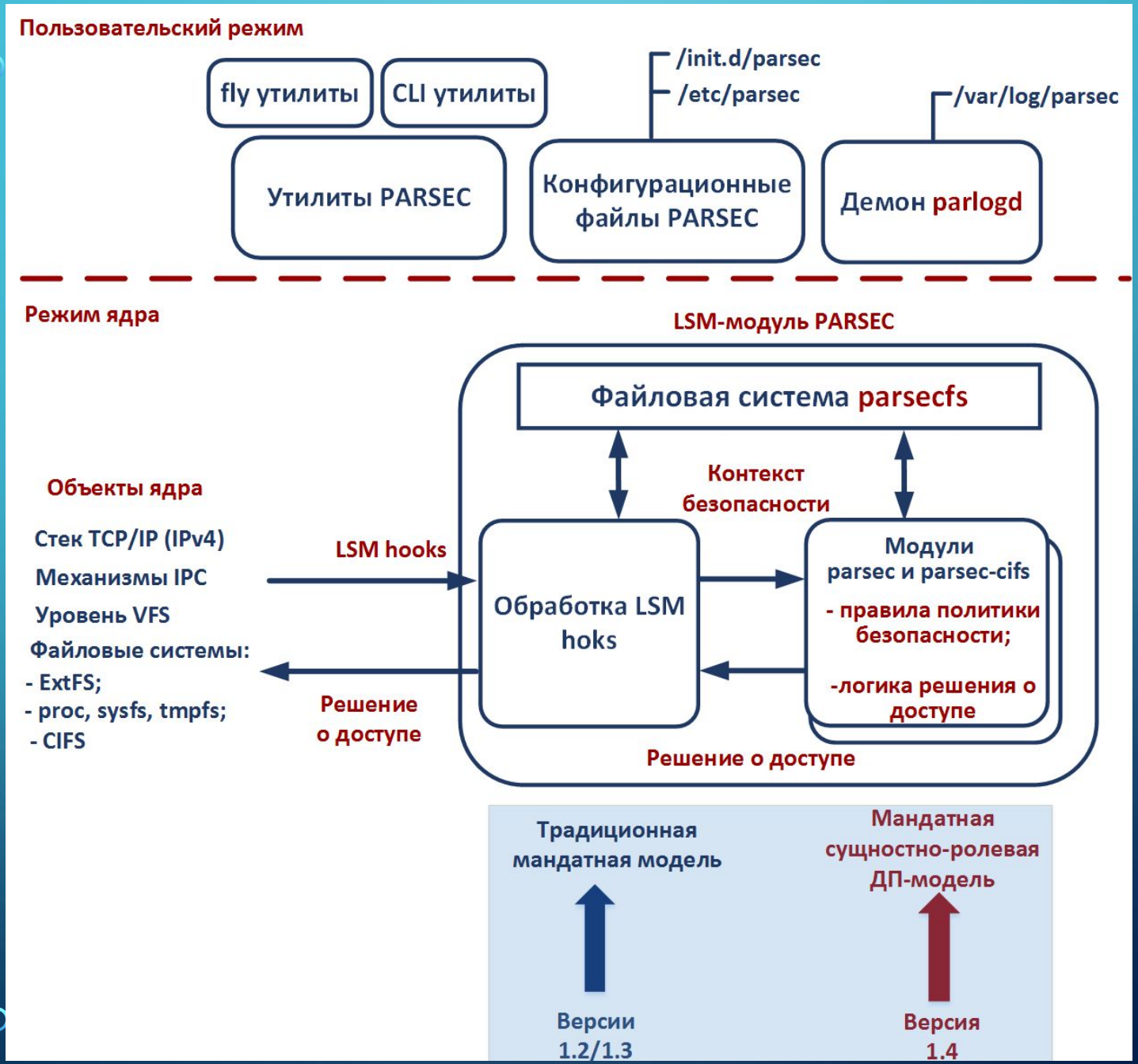
Пример дискреционной модели

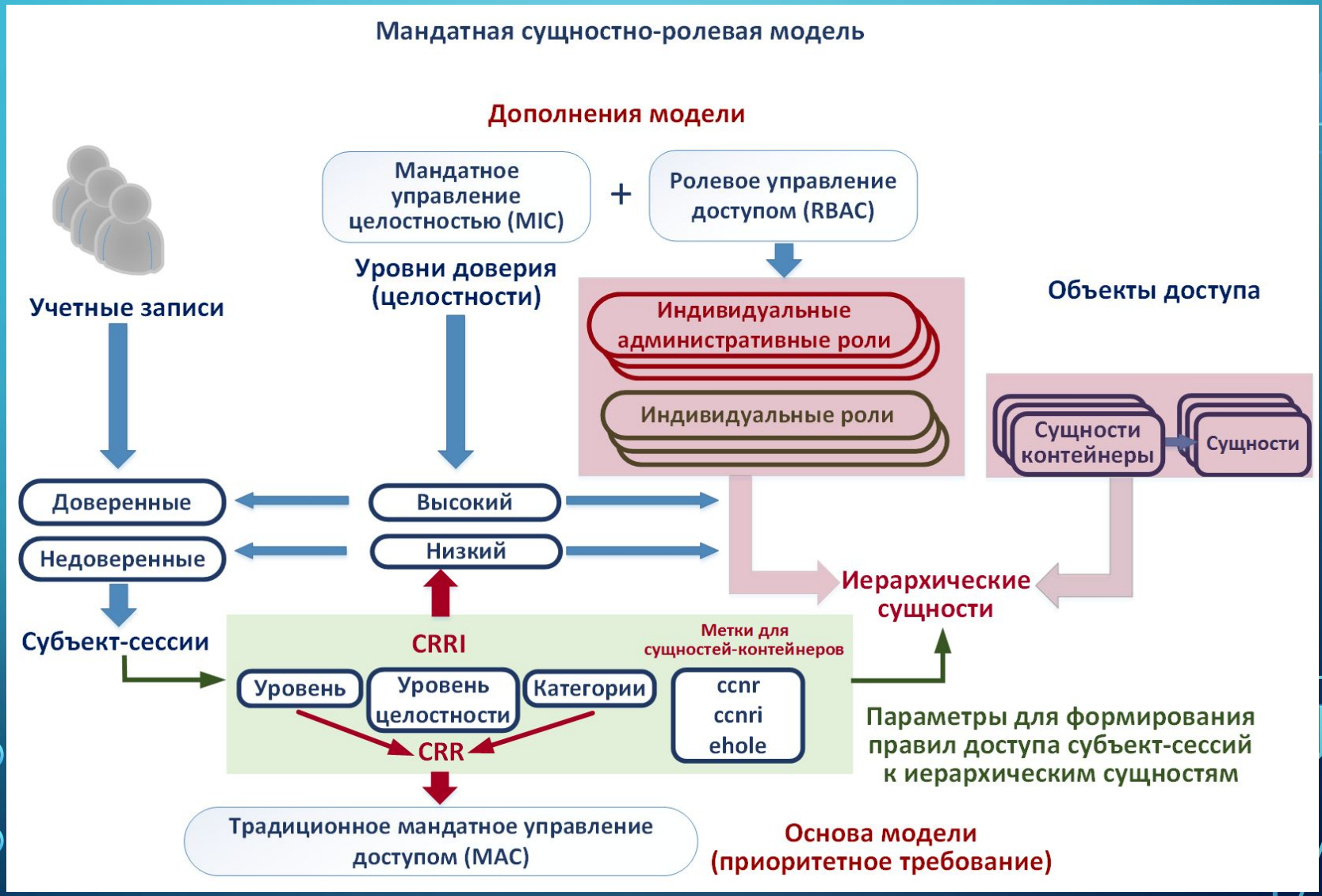
	A_1	A_2	B_1	B_2
U_1	op_{A1} - да op_{A2} - нет op_{B1} - нет	op_{A1} - да op_{A2} - нет op_{B1} - нет	op_{A1} - нет op_{A2} - нет op_{B1} - нет	op_{A1} - нет op_{A2} - нет op_{B1} - нет
U_2	op_{A1} - да op_{A2} - да op_{B1} - нет	op_{A1} - да op_{A2} - да op_{B1} - нет	op_{A1} - нет op_{A2} - нет op_{B1} - да	op_{A1} - нет op_{A2} - нет op_{B1} - да

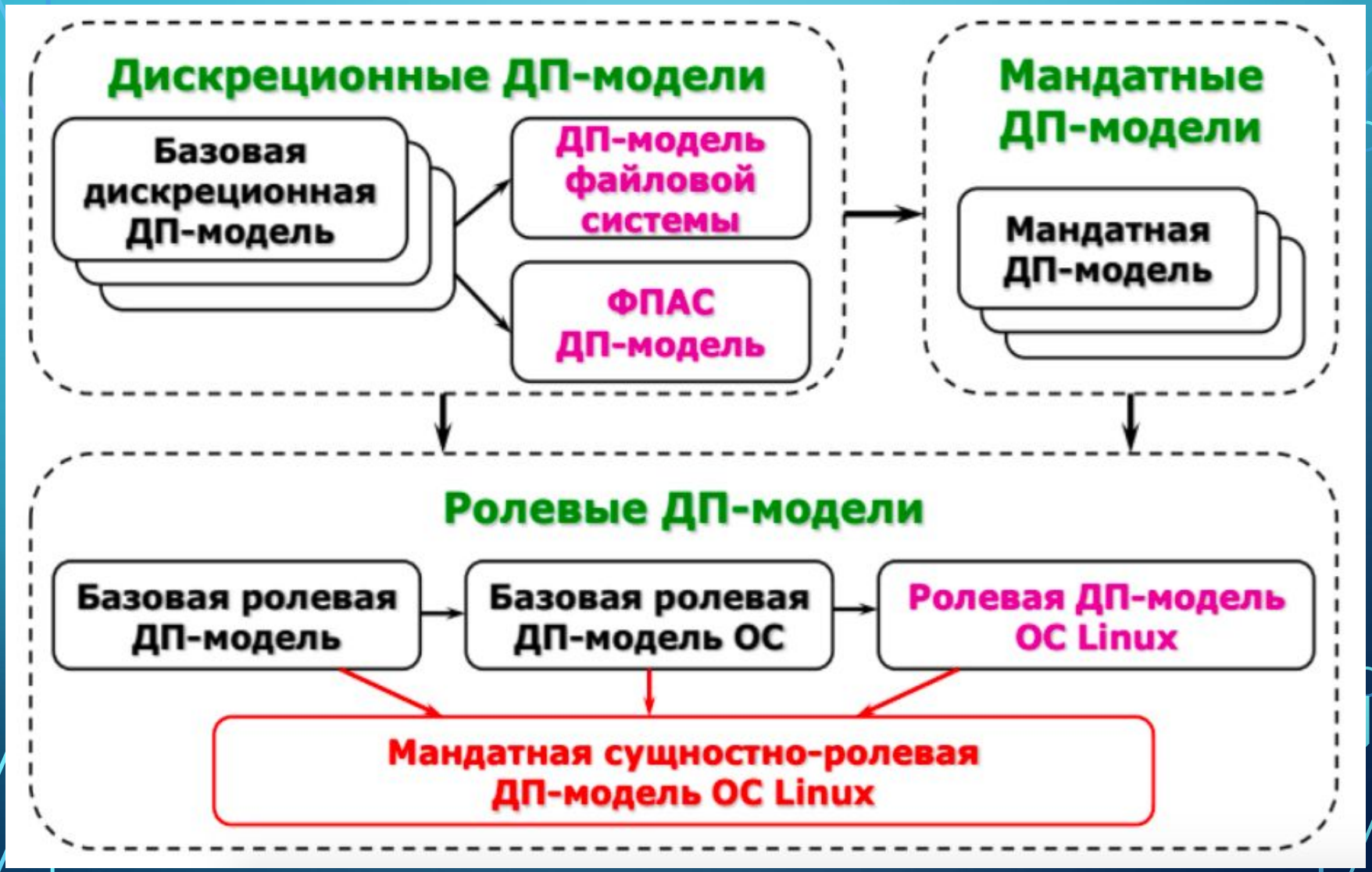
MyShared


Добавление нового правила
Выберите субъектов, берущих информацию
любой
система
службы
Notepad
The BAT
Выберите субъектов, помещающих информацию
любой
система
службы
Notepad
The BAT
Получение информации из буфера обмена:
Разрешить
Запретить
Режим аудита
Фиксировать помещение информации в буфер обмена локально
Фиксировать помещение информации в буфер обмена на сервере аудита
Фиксировать взятие информации из буфера обмена локально
Фиксировать взятие информации из буфера обмена на сервере аудита
OK
Отмена


АВИ 1
ДСП
АВИ 2
НК
ДСП
НК
НК
ДСП
ВМ 1
НК
ВМ 2
Сервер Hyper-V
ДСП
Условные обозначения
Уровни конфиденциальности
НК
Неконфиденциально
ДСП
Для служебного пользования
Уровни сессии
НК
Неконфиденциально
ДСП
Для служебного пользования


Пользовательский режим
fly утилиты
CLI утилиты
/init.d/parsec
/etc/parsec
/var/log/parsec
Утилиты PARSEC
Конфигурационные файлы PARSEC
Демон parlogd
Режим ядра
LSM-модуль PARSEC
Файловая система parsecfs
Контекст безопасности
Объекты ядра
Стек TCP/IP (IPv4)
Механизмы IPC
Уровень VFS
Файловые системы:
- ExtFS;
- proc, sysfs, tmpfs;
- CIFS
LSM hooks
Обработка LSM hoks
Модули parsec и parsec-cifs
- правила политики безопасности;
-логика решения о доступе
Решение о доступе
Решение о доступе
Традиционная мандатная модель
Мандатная сущностно-ролевая ДП-модель
Версии 1.2/1.3
Версия 1.4


Мандатная сущностно-ролевая модель
Дополнения модели
Мандатное управление целостностью (MIC)
+
Ролевое управление доступом (RBAC)
Учетные записи
Уровни доверия (целостности)
Индивидуальные административные роли
Индивидуальные роли
Объекты доступа
Сущности контейнеры
Сущности
Доверенные
Недоверенные
Высокий
Низкий
Иерархические сущности
Субъект-сессии
CRRI
Метки для сущностей-контейнеров
Уровень
Уровень целостности
Категории
ccnr
ccnri
ehole
CRR
Параметры для формирования правил доступа субъект-сессий к иерархическим сущностям
Традиционное мандатное управление доступом (MAC)
Основа модели (приоритетное требование)


Дискреционные ДП-модели
Базовая дискреционная ДП-модель
ДП-модель файловой системы
ФПАС ДП-модель
Мандатные ДП-модели
Мандатная ДП-модель
Ролевые ДП-модели
Базовая ролевая ДП-модель
Базовая ролевая ДП-модель ОС
Ролевая ДП-модель ОС Linux
Мандатная сущностно-ролевая ДП-модель ОС Linux


СТРУКТУРА РАЗРАБОТКИ МОДЕЛИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОТТЕДЖНОГО ПОСЕЛКА
РИСКИ И УГРОЗЫ
ОБЪЕКТЫ ЗАЩИТЫ
МОДЕЛЬ НАРУШИТЕЛЯ
СЦЕНАРИИ РАЗВИТИЯ СОБЫТИЙ
СПОСОБЫ НЕЙТРАЛИЗАЦИИ
СРЕДСТВА НЕЙТРАЛИЗАЦИИ
Служба охраны
Комплекс ТСО
Профилактические мероприятия
МОДЕЛЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КП

«ОРАНЖЕВАЯ КНИГА»
(Trusted Computer System Evaluation Criteria, TCSEC)

ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ ДОВЕРЕННОЙ СРЕДЫ

- **Дискреционное (произвольное) управление доступом** – *обращение именованных субъектов к именованных объектам. Уполномоченный субъект может предоставлять или отбирать права на доступ к объектам.*

- **Мандатное управление доступом** – *доступ к объектам осуществляется на основе сопоставления метки безопасности объекта и уровня доверия к субъекту по некоторому формально заданному правилу.*

MyShared