



**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

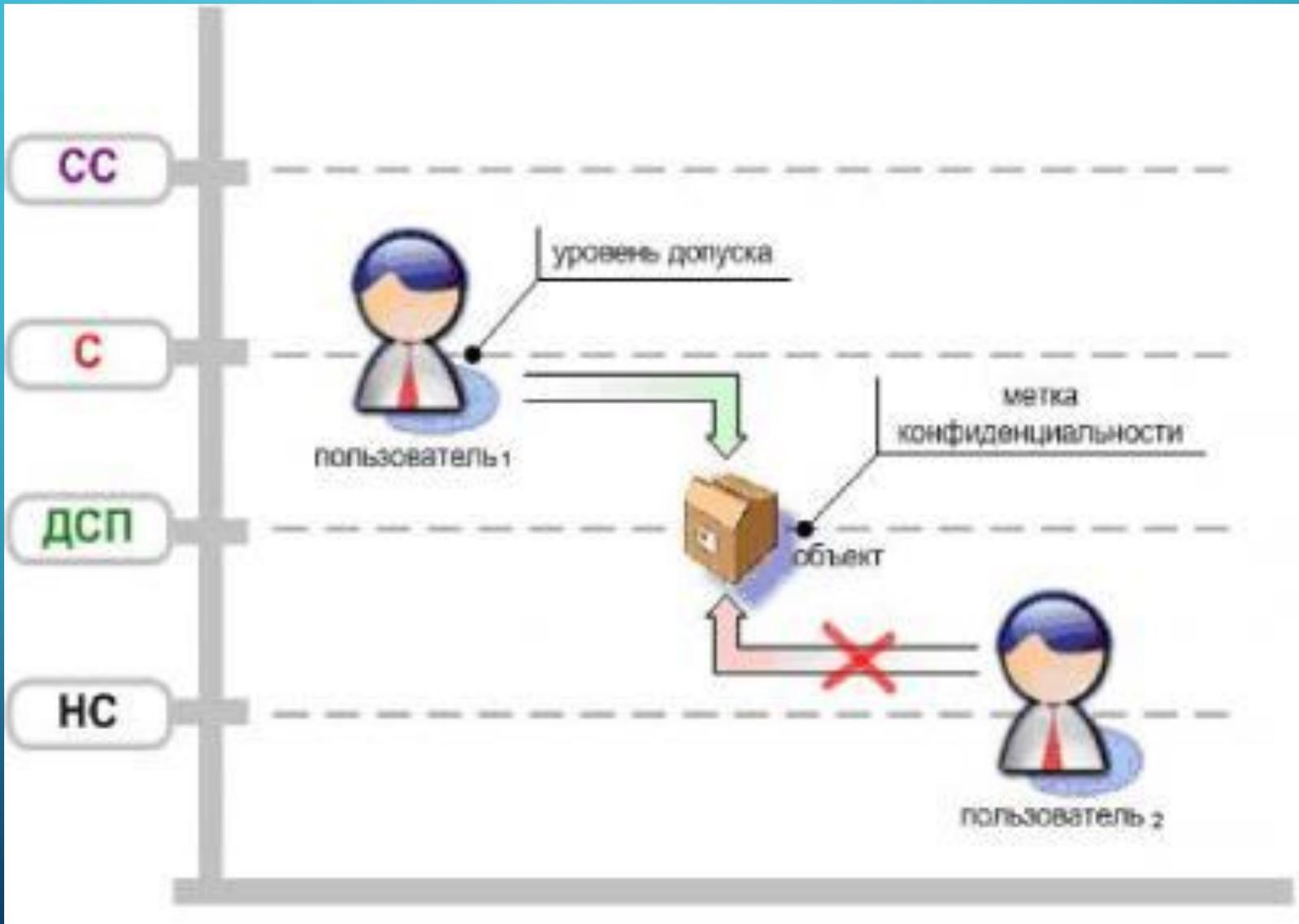
Мандатный принцип контроля доступа

→ Идентификация и Аутентификация

→ Очистка памяти

→ Изоляция модулей

→ И т.д.



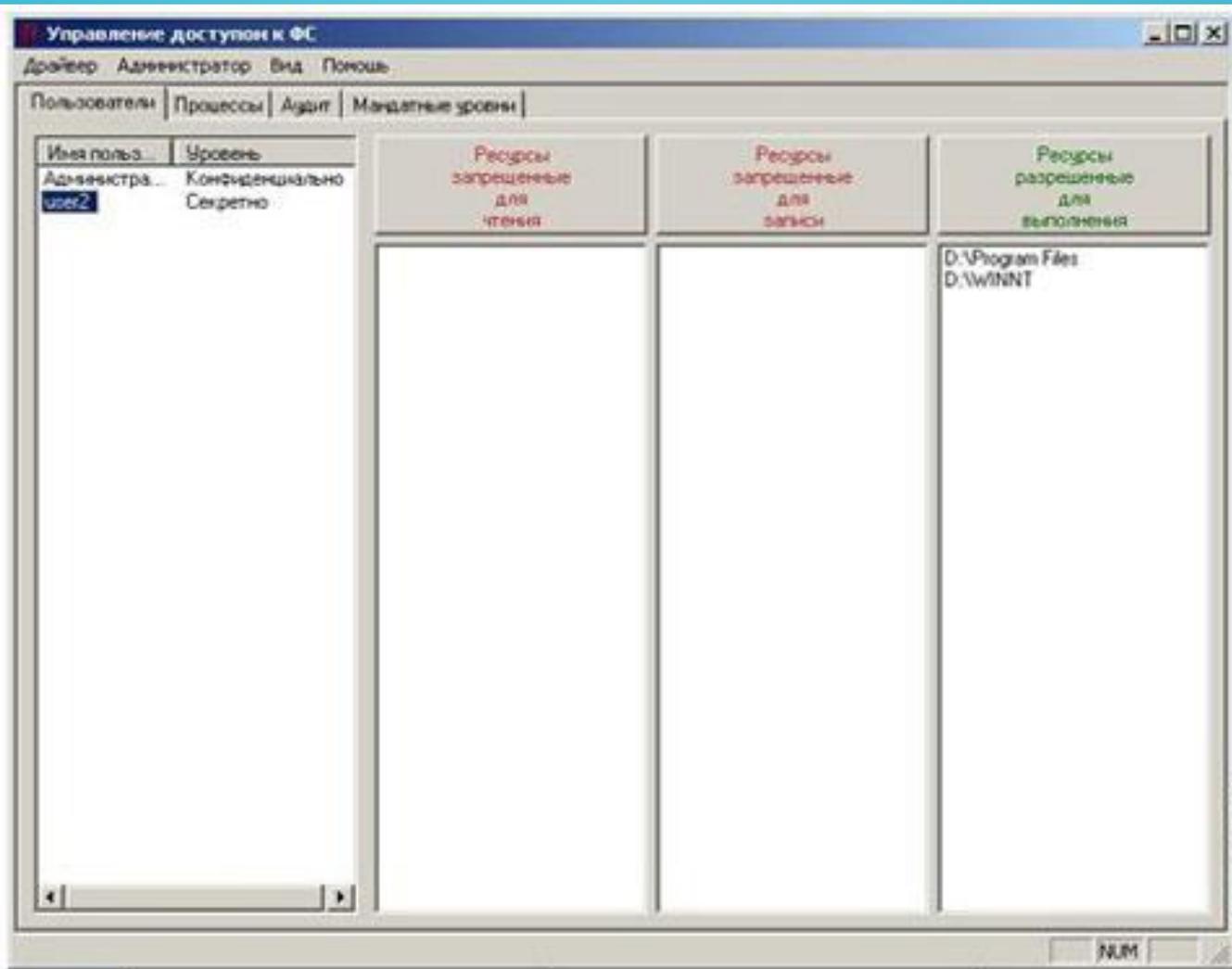


Рис. 5.2 Интерфейс настройки дискреционного механизма контроля доступа

## 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.



# 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)



## 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

## Добавление нового правила

Выберите субъектов, берущих информацию

-  любой
-  система
-  службы
-  Notepad
-  The BAT

Выберите субъектов, понесших 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



Условные обозначения

Уровни конфиденциальности		Уровни сессии	
	Неконфиденциально	<u>нк</u>	Неконфиденциально
	Для служебного пользования	<u>дсп</u>	Для служебного пользования

## Пользовательский режим



## Режим ядра

### LSM-модуль PARSEC

### Объекты ядра

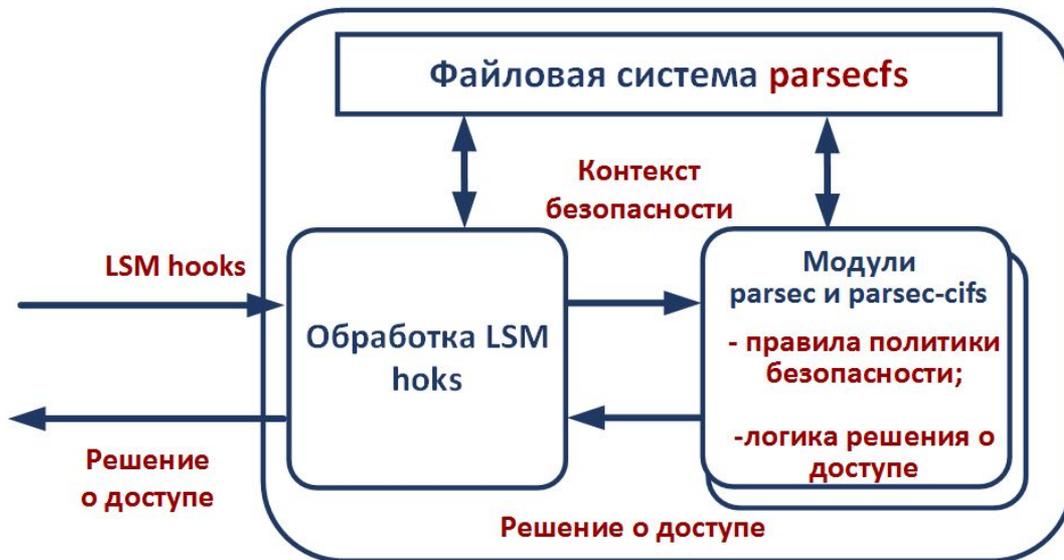
Стек TCP/IP (IPv4)

Механизмы IPC

Уровень VFS

Файловые системы:

- ExtFS;
- proc, sysfs, tmpfs;
- CIFS



Традиционная  
мандатная модель



Версии  
1.2/1.3

Мандатная  
сущностно-ролевая  
ДП-модель



Версия  
1.4

# Мандатная сущностно-ролевая модель

## Дополнения модели



## 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



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

**ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ ДОВЕРЕННОЙ СРЕДЫ**

- **Дискреционное (произвольное) управление доступом** – обращение именованных субъектов к именованным 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.