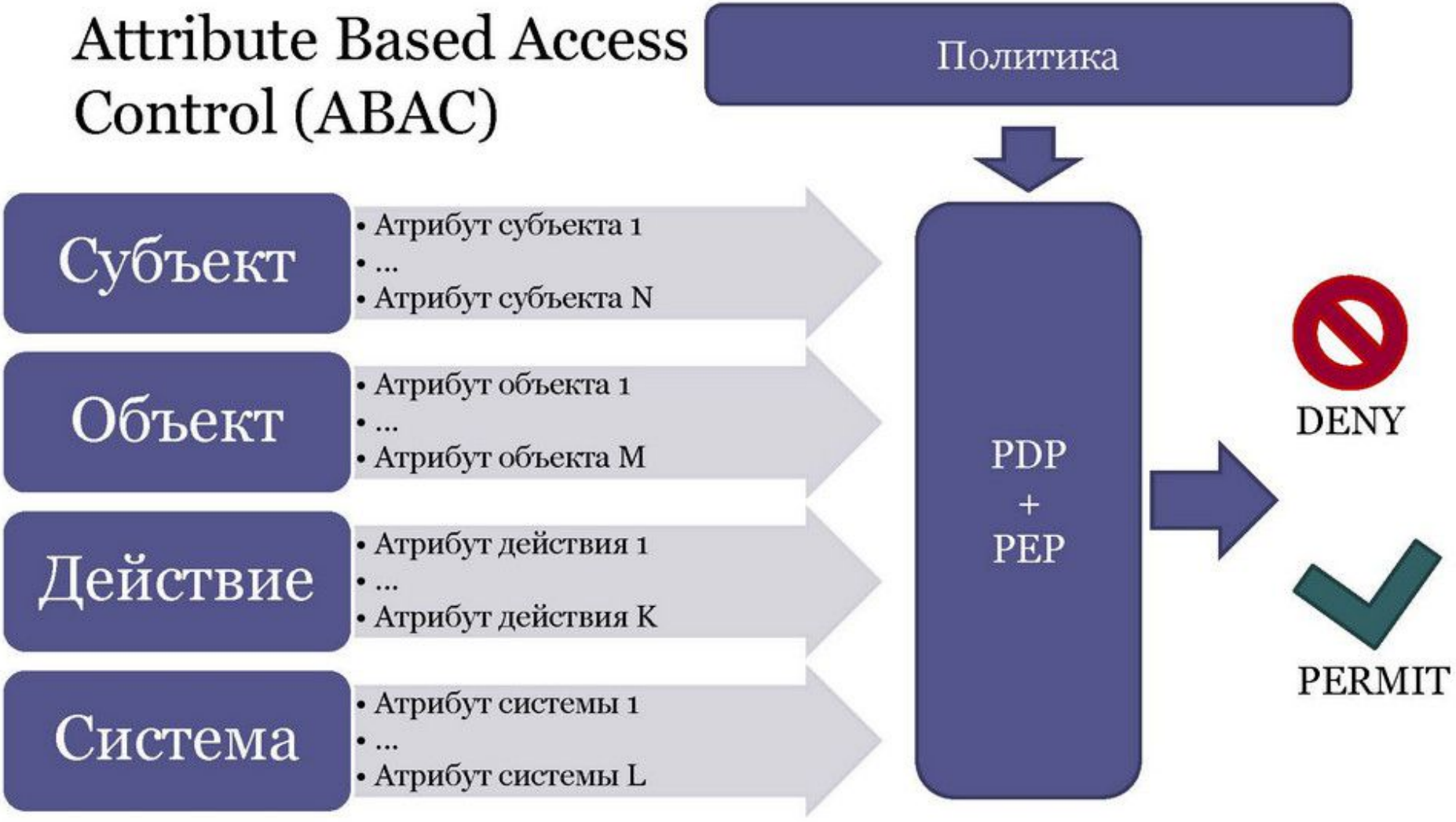
Использование атрибутной модели контроля доступа в задаче контроля целостности конфигурации

Мозолина Надежда,
МФТИ

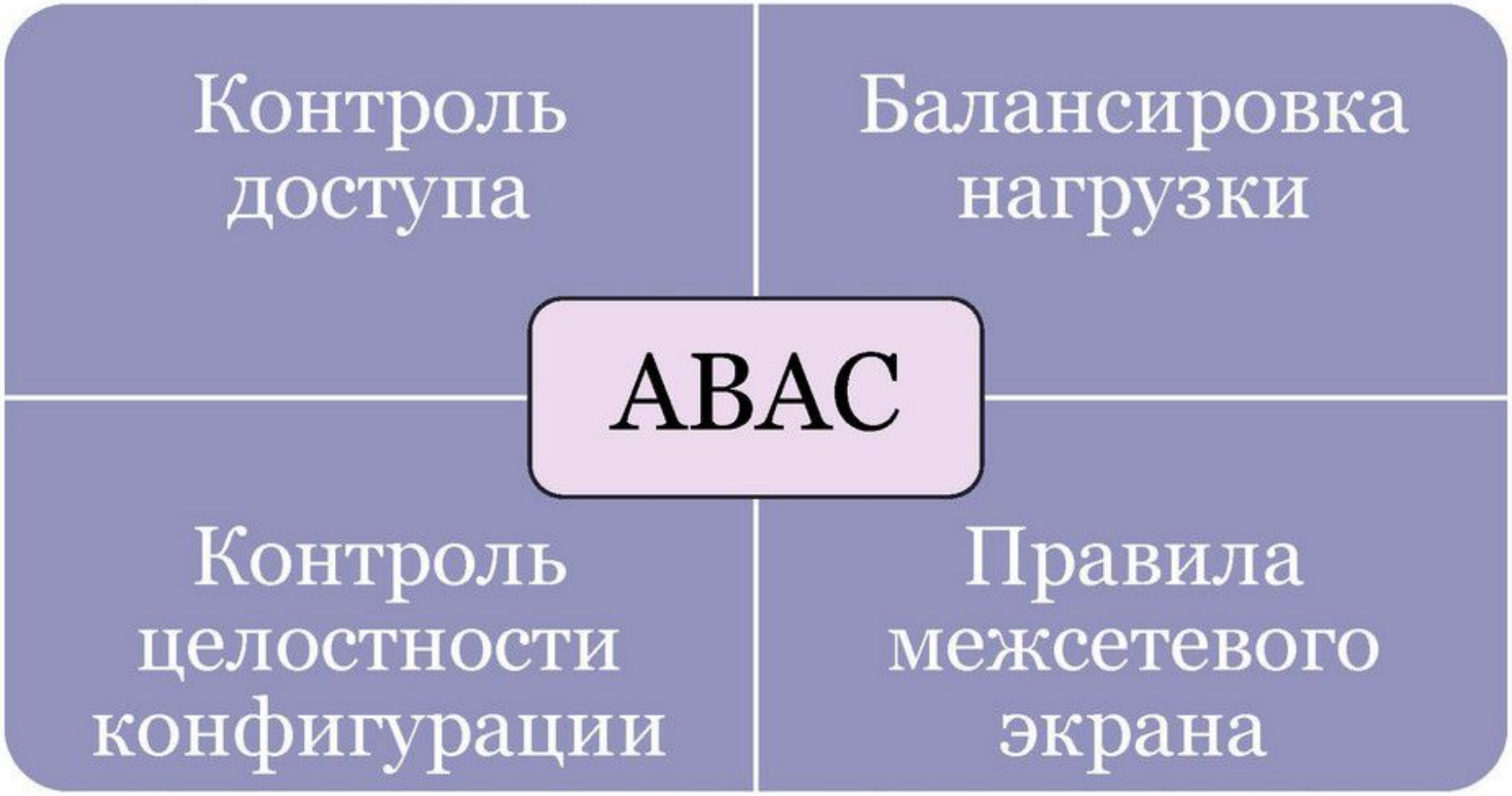
КЗИ, Полоцк, 2017

Атрибутная модель контроля доступа

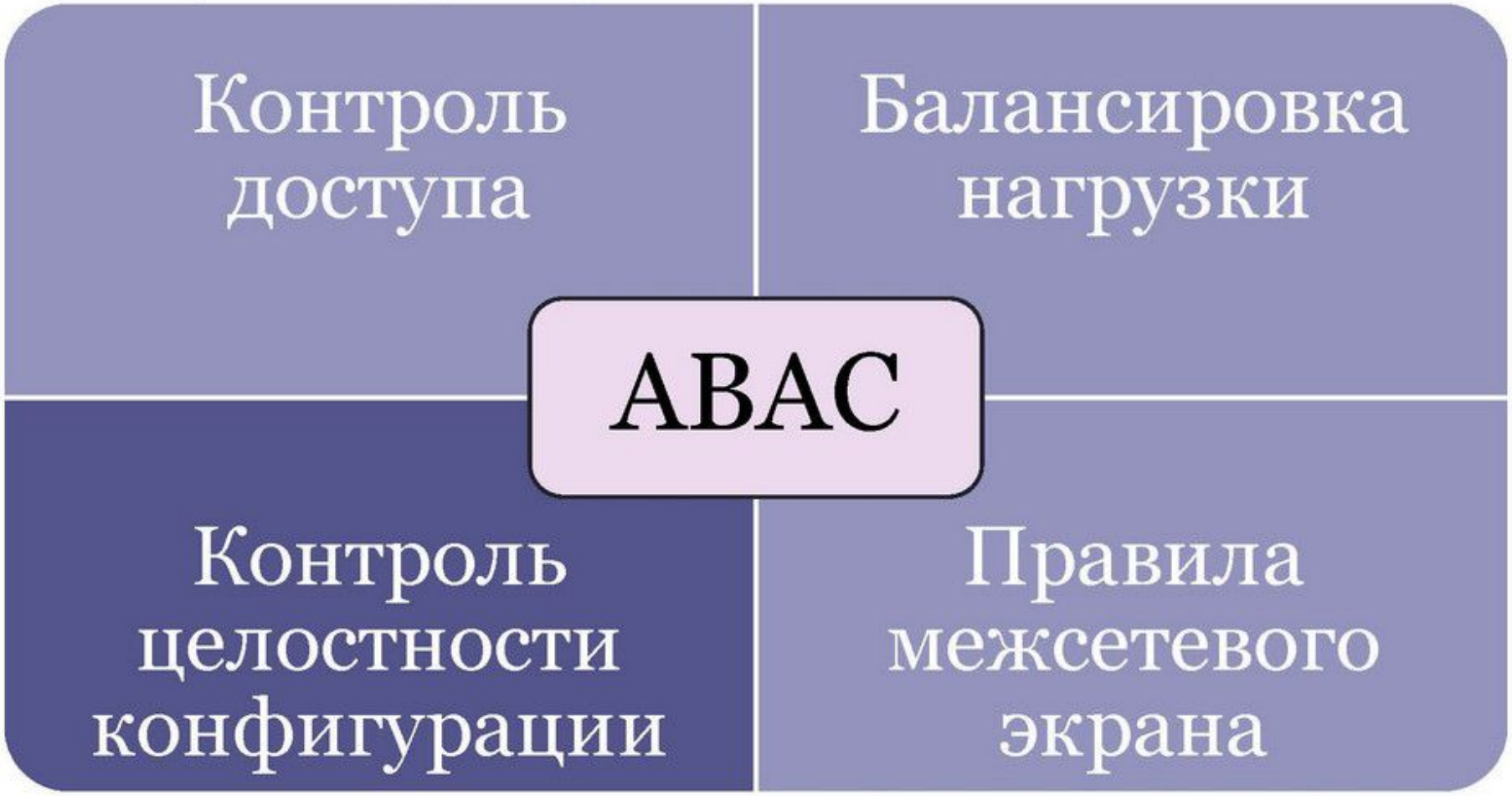
Attribute Based Access Control (ABAC)



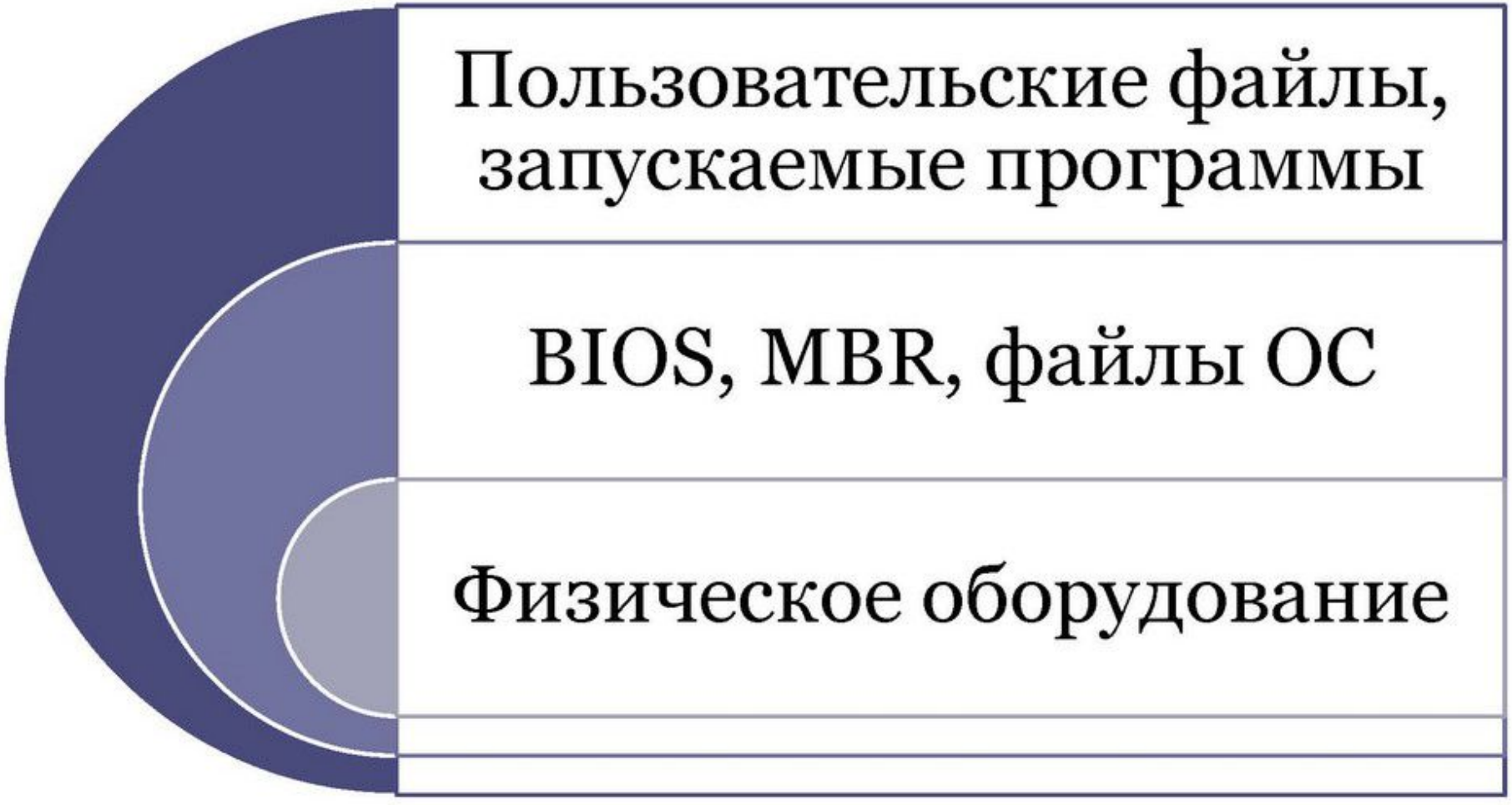
Применение атрибутной модели контроля доступа

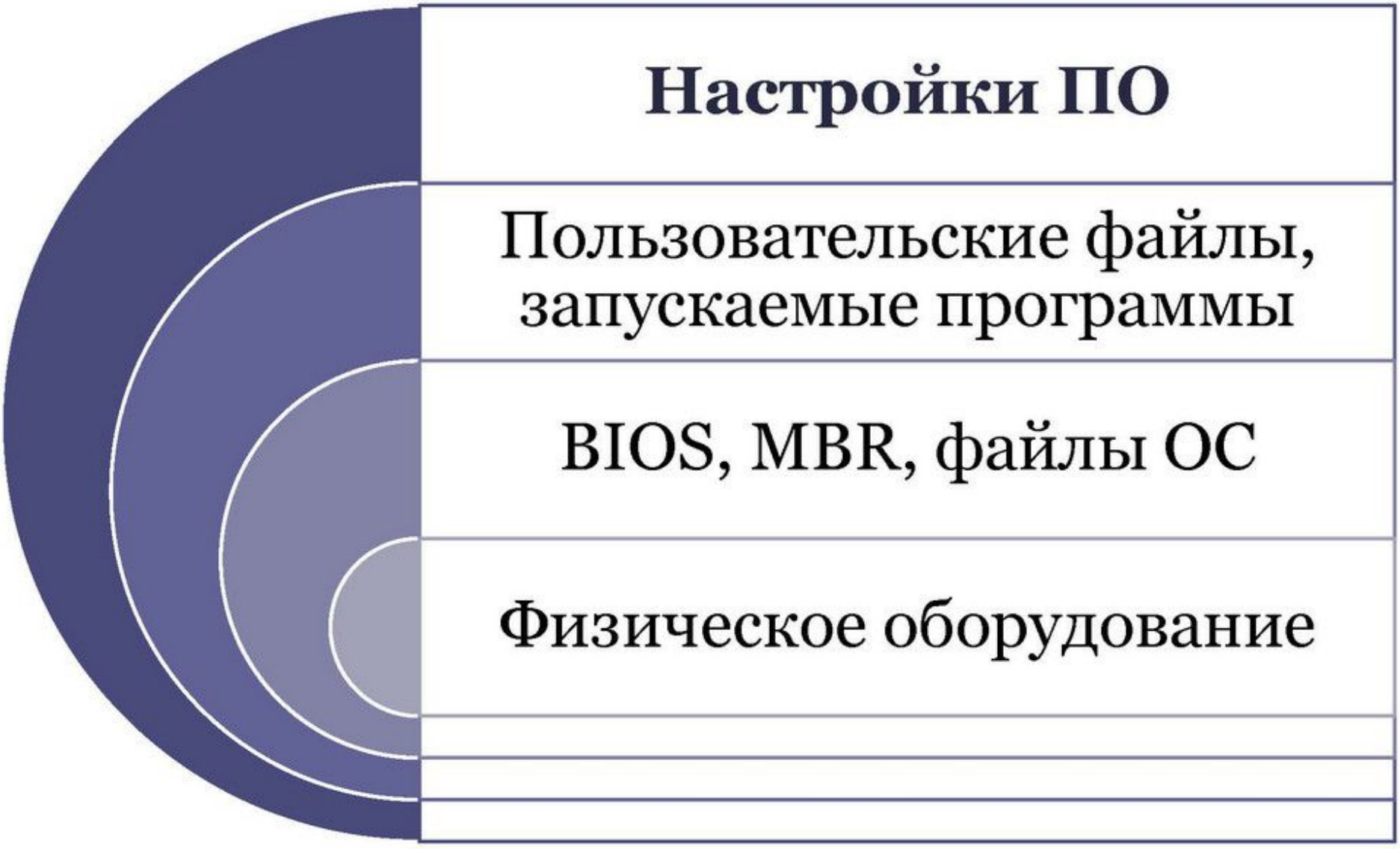


Применение атрибутной модели контроля доступа



Этапы контроля целостности




Настройки ПО
Пользовательские файлы, запускаемые программы
BIOS, MBR, файлы ОС
Физическое оборудование

Традиционный подход:

только 1 разрешённое состояние

Контроль целостности конфигурации:

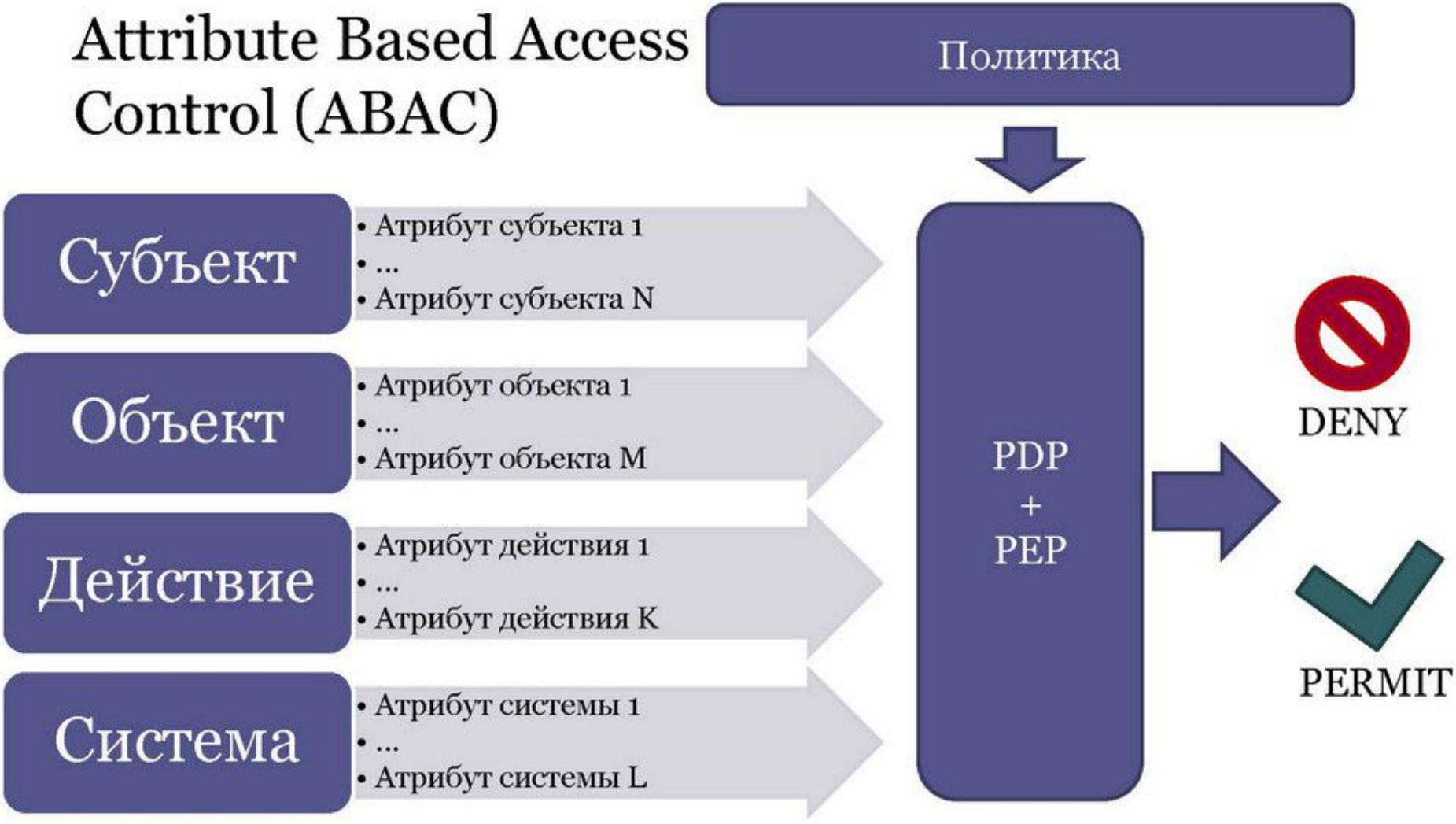
множество разрешённых состояний

Конфигурация виртуальной инфраструктуры

Объекты	Связи между объектами	Атрибуты объектов

Атрибутная модель контроля доступа

Attribute Based Access Control (ABAC)



Практическая реализация

Эталон

```
PolicySet MainPolicy { deny-
        overrides
policies:
        PolicySet Hosts {...}
        PolicySet VMs {...}
        ...
}
```

Текущее состояние

Request:{Requestvm34
(VirtualMachine/id, "vm-34")
(VirtualMachine/type, "VirtualMachine")
(VirtualMachine/name, "RHEL")
(Vir

Request:{Requestvm38
(VirtualMachine/id, "vm-38")
(VirtualMachine/type, "VirtualMachine")
(VirtualMachine/name, "WinXP SP3 - 2")
(VirtualMachine/host, "host-16") }

(VirtualMachine/host, "host-13") }

Схема работы

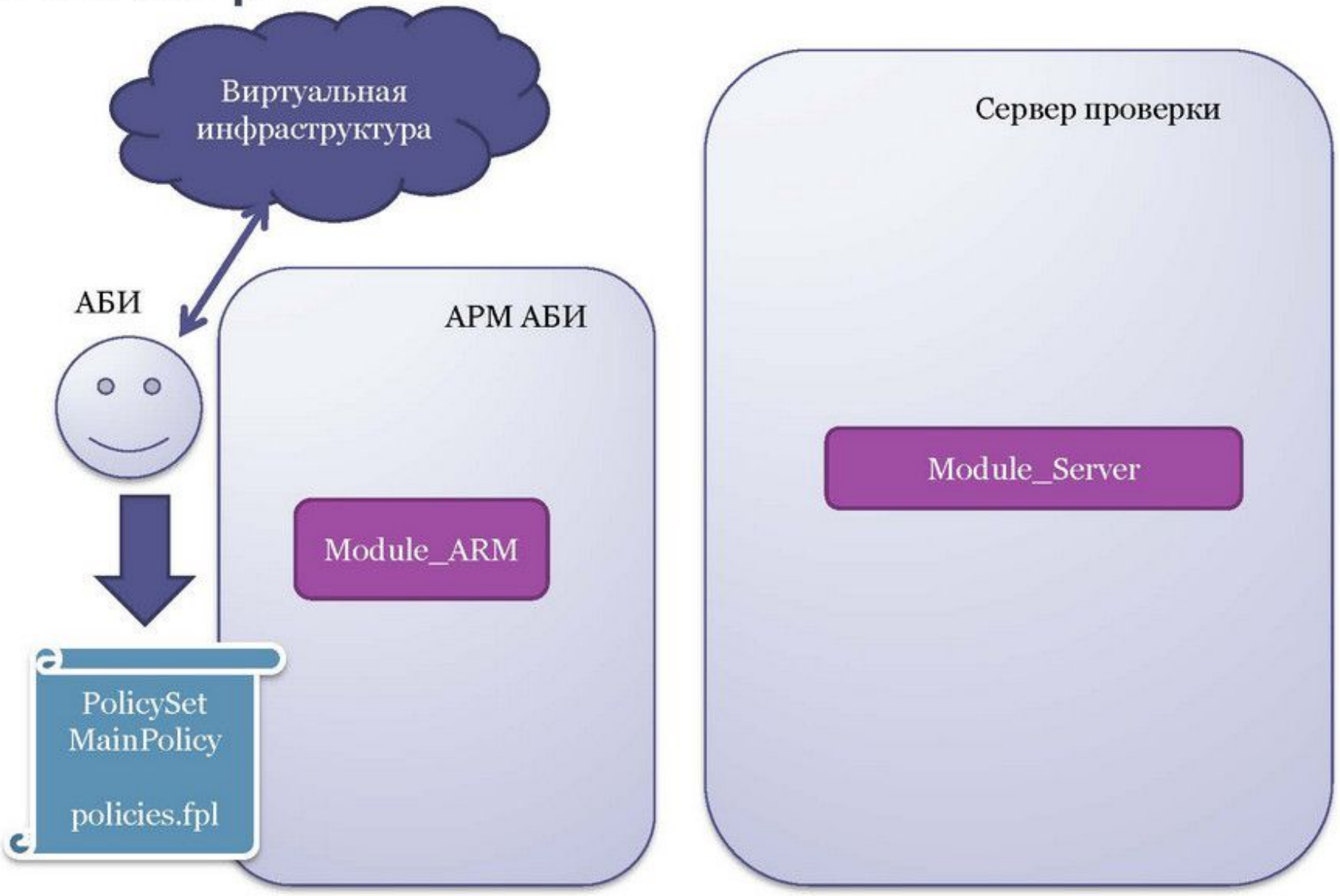


Схема работы

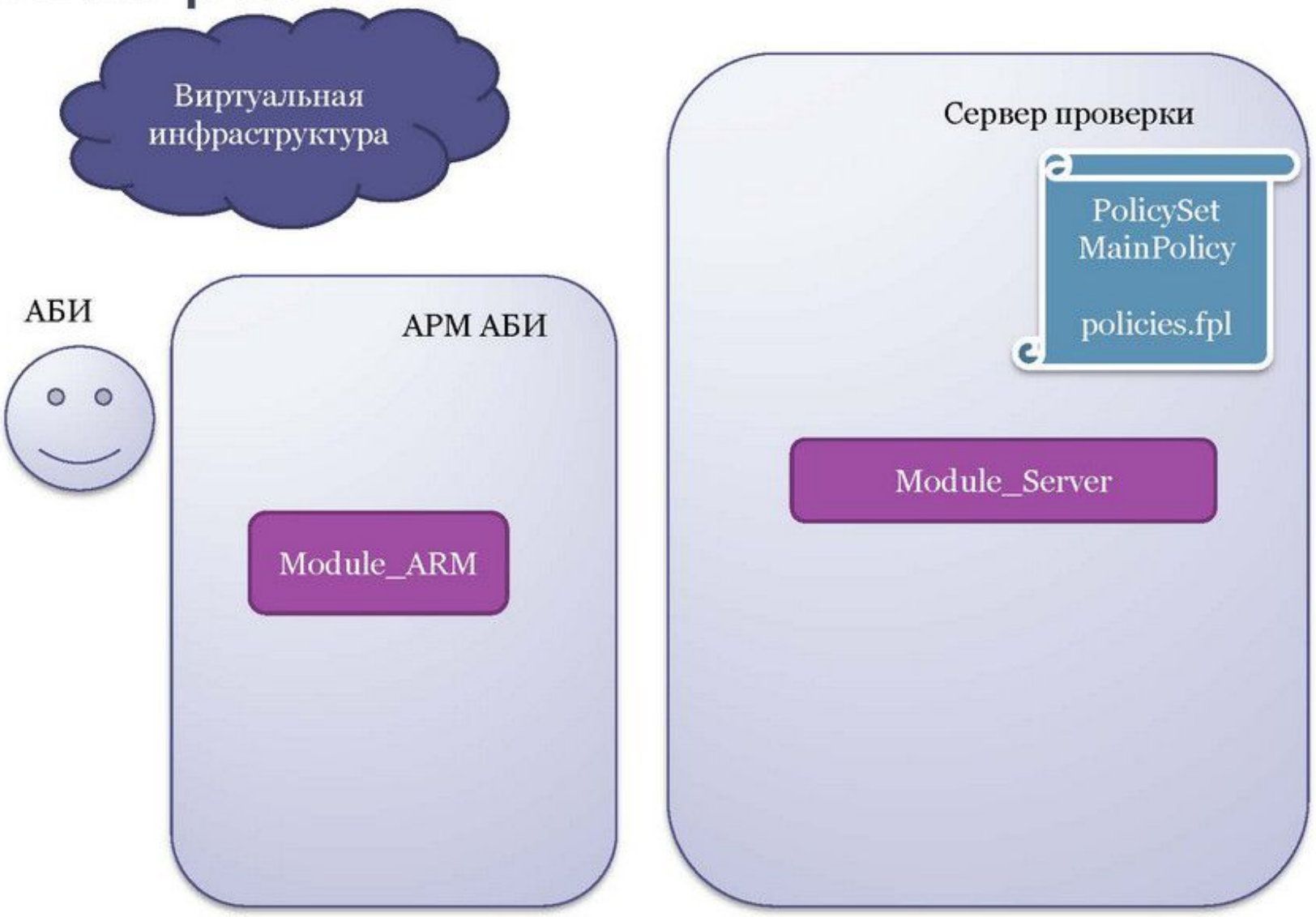


Схема работы

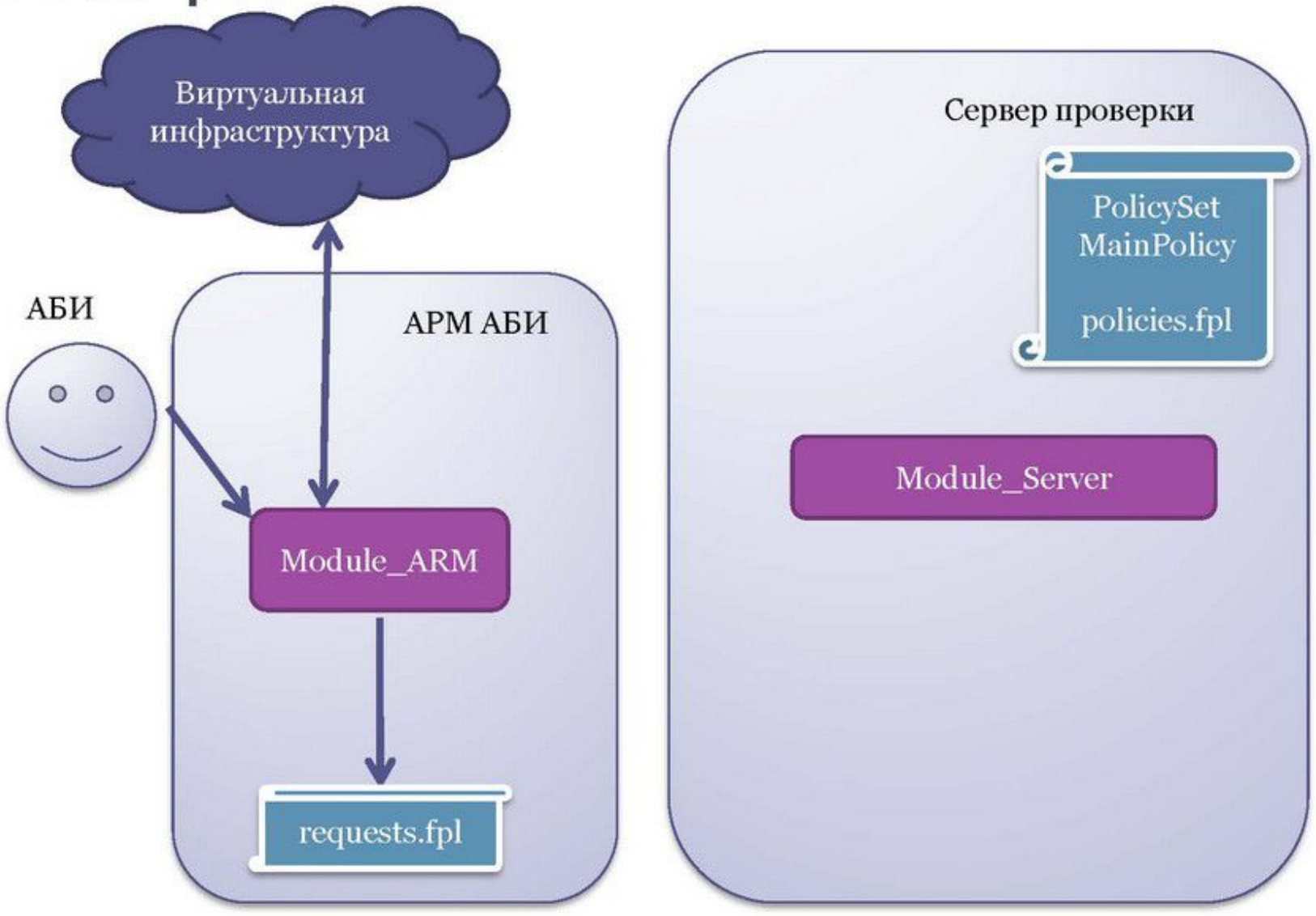


Схема работы

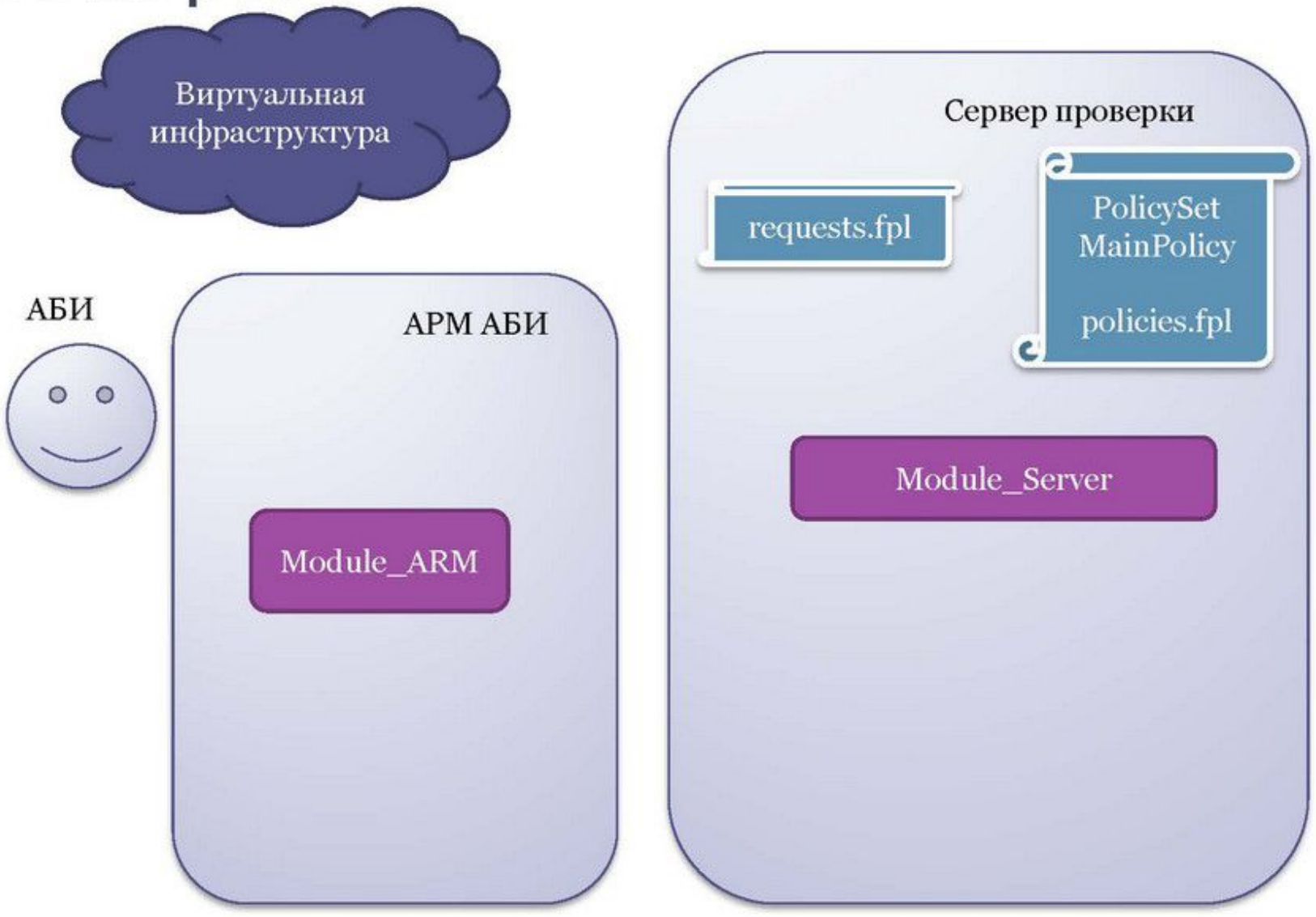
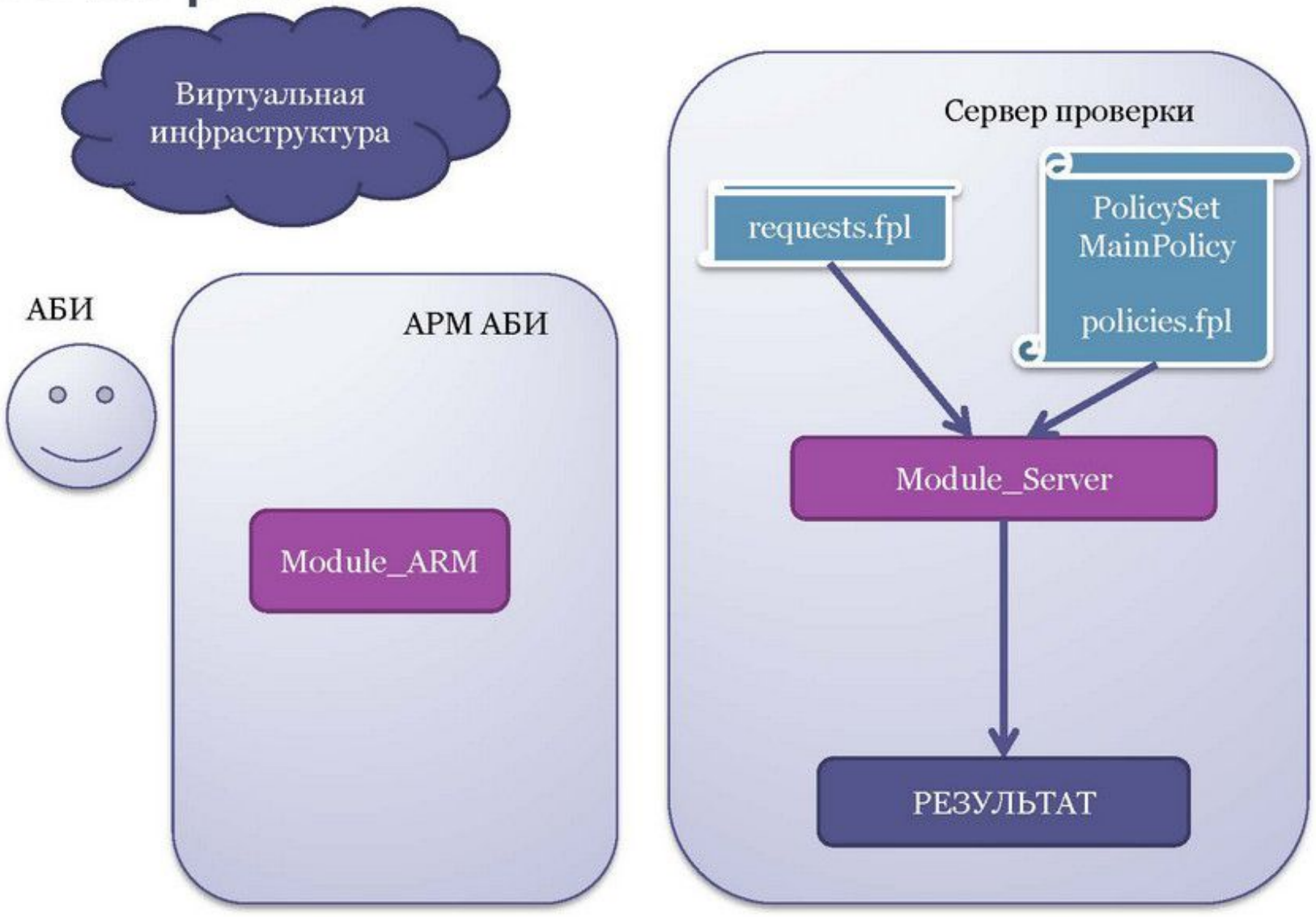


Схема работы



Заключение

Применение атрибутной модели контроля доступа позволяет учесть, что разрешёнными (не нарушающими целостность) могут быть **несколько** конфигураций