Политики безопасности (теоретические основы)

- Интегральная характеристика системы, Политика Безопасности (ПБ) – *качественно-количественное выражение свойств защищенности в терминах, представляющих систему*.
- ПБ может включать свойства злоумышленника и объекта атаки.
- ПБ включает
  - множество всех возможных операций над объектами C
  - для каждой пары «субъект-объект» (S_i, O_j) множество разрешенных операций L:

$$L \ni L \subset C$$

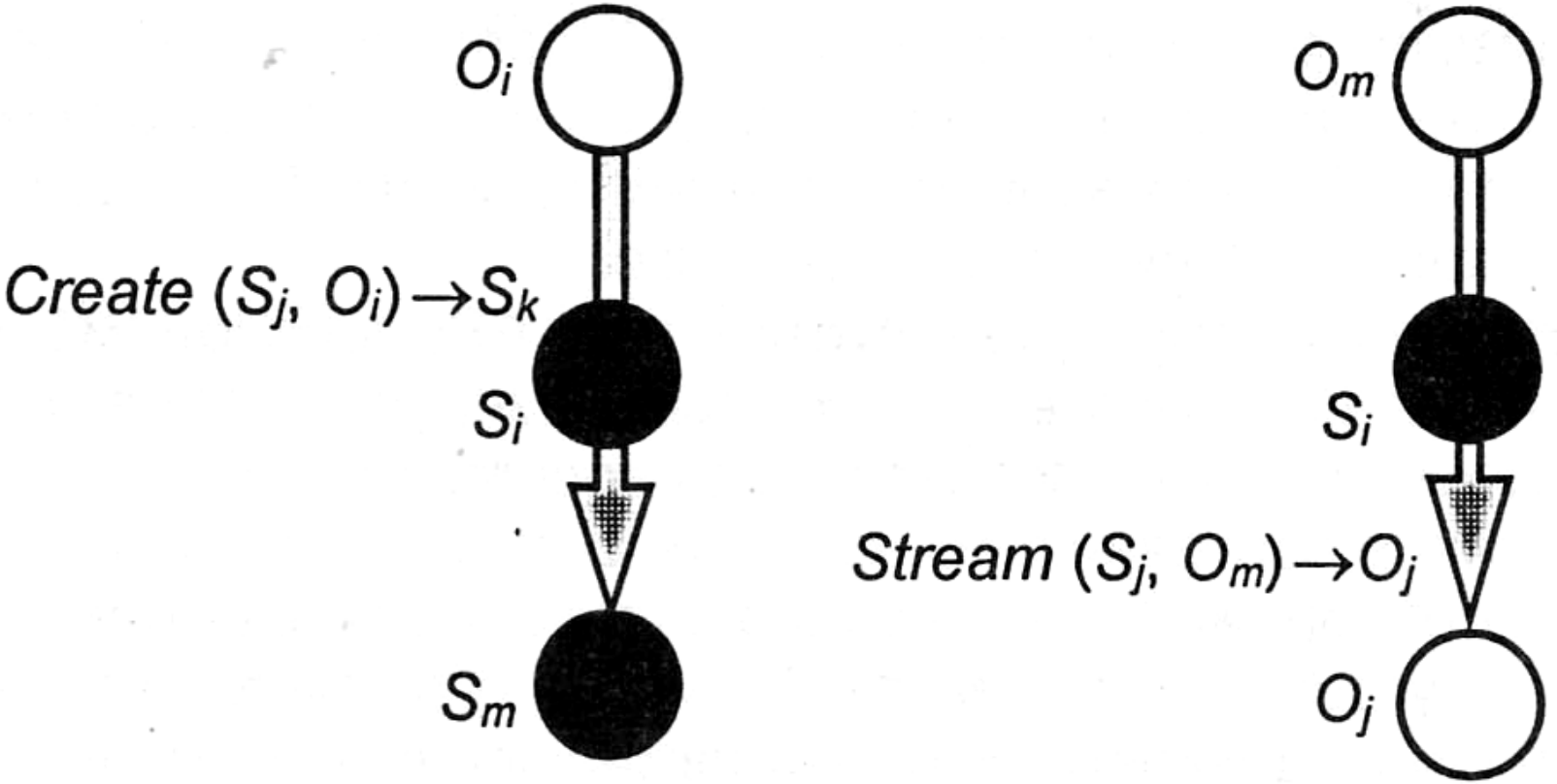
Проблемы создания безопасных АС в современном мире

- Недостаток коммерческих решений, выполненных по общим стандартам.
- Проблемы безопасности АС, набранной из разнородных компонентов, построенных в рамках различных моделей безопасности
- Сложность и большая длительность тестирования АС, приводящая к недопустимым в современном бизнесе задержкам выпуска в продажу
- Перечисленные выше проблемы приводят к повсеместному использованию систем с низким уровнем безопасности для хранения и обработки данных высокого уровня секретности и, следовательно, недопустимым рискам.

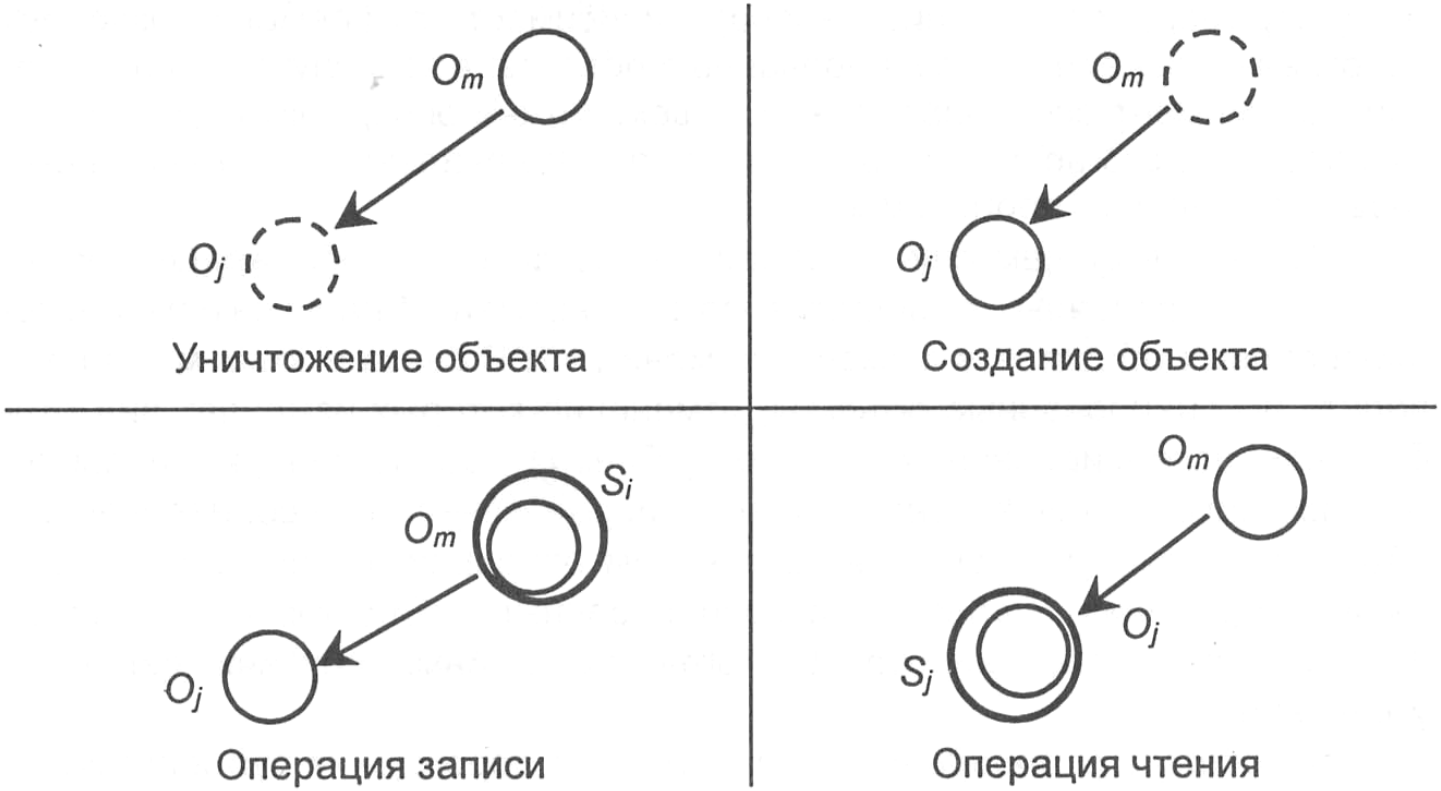
Аксиомы защищенных АС

- A1. Существования субъекта контроля операций субъектов над объектами.
- A2. Необходимости объекта содержащего информацию о запрещенных и разрешенных операций субъектов над объектами.
- A3. Все вопросы безопасности информации в АС описываются доступами субъектов к объектам
- A4. Субъекты в АС порождаются из объектов только активным компонентом (субъектами)
  - O1. Определение объекта-источника
  - O2. Определение ассоциированного объекта
  - O3. Определение потока информации

Порождение субъекта и поток



Виды информационных потоков



Доступ

- О4. Определение доступа субъекта к объекту.
- Во множестве потоков P выделим два непересекающихся подмножества N, L:

$$P = N \cup L, \;\; N \cap L = 0$$

  - N – множество потоков, характеризующих НД
  - L – множество потоков, характеризующих легальный доступ

- О5. Определение правил разграничения доступа
- О6. Определение тождественности объектов
- О7. Определение тождественности субъектов

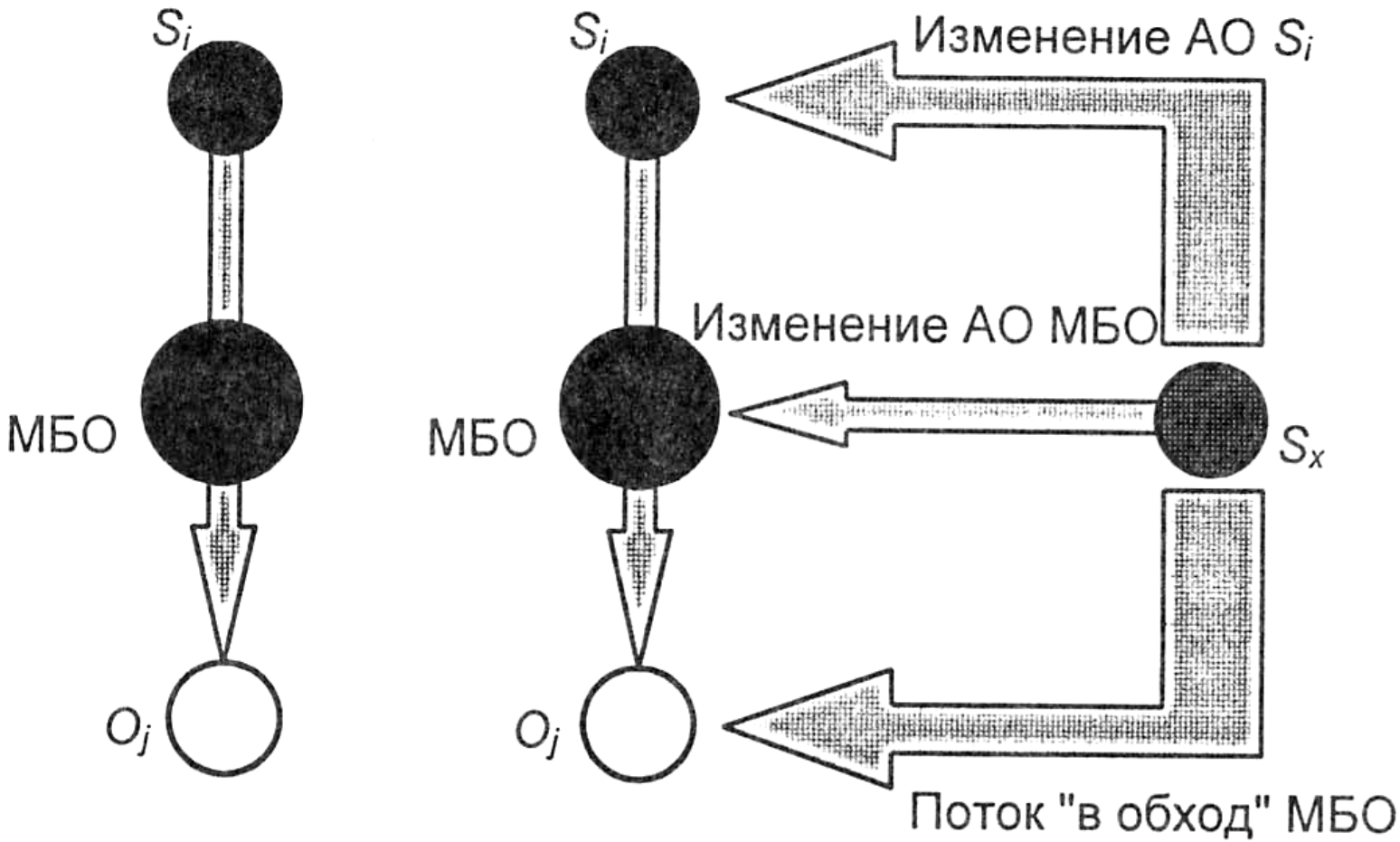
Монитор безопасности

- О8. Определение монитора обращений
- О9. Определение монитора безопасности (монитора ссылок)

Типы политик безопасности

- Типы политик безопасности (относительно методов управления доступом):
  - Дискреционная (дискретная, Discretionary Access Control -DAC)
    - Пример – модель Harrison-Ruzzo-Ullman (HRU)
    - Есть доверие к пользователям
  - Мандатная (полномочная, Mandatory Access Control MAC)
    - Пример – модель Bell-Lapadula (BL)
    - Нет доверия пользователям, действует внешнее правило

Пути нарушения ПБ



АО – ассоциированные объекты

Разработка и реализация ПБ

- О10. Определение невлияющих (корректных) субъектов
- О11. Определение абсолютно невлияющих (абсолютно корректных) объектов

- Достаточное условие N 1 гарантированного выполнения ПБ в АС
  - О12. Определение Монитора порождения субъектов (МПС)
  - О13. Определение Монитора безопасности субъектов (МБС)
  - О14. Определение замкнутой АС
  - О15. Определение изолированности (абсолютной И) АС
- Достаточное условие №2 гарантированного выполнения ПБ в АС
  - О16. Определение порождения субъекта с контролем неизменности объекта
- Теорема об изолированной программной среде (ИПС)

Классическая схема ядра безопасности

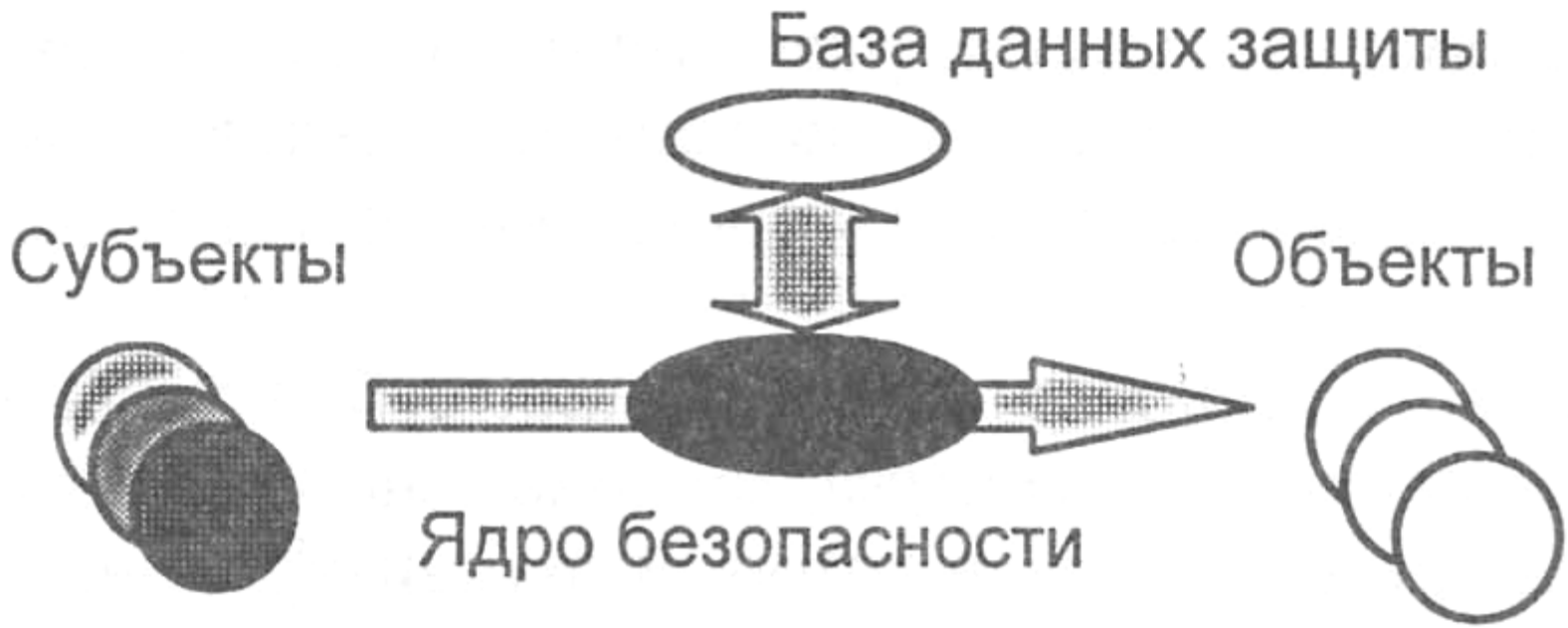
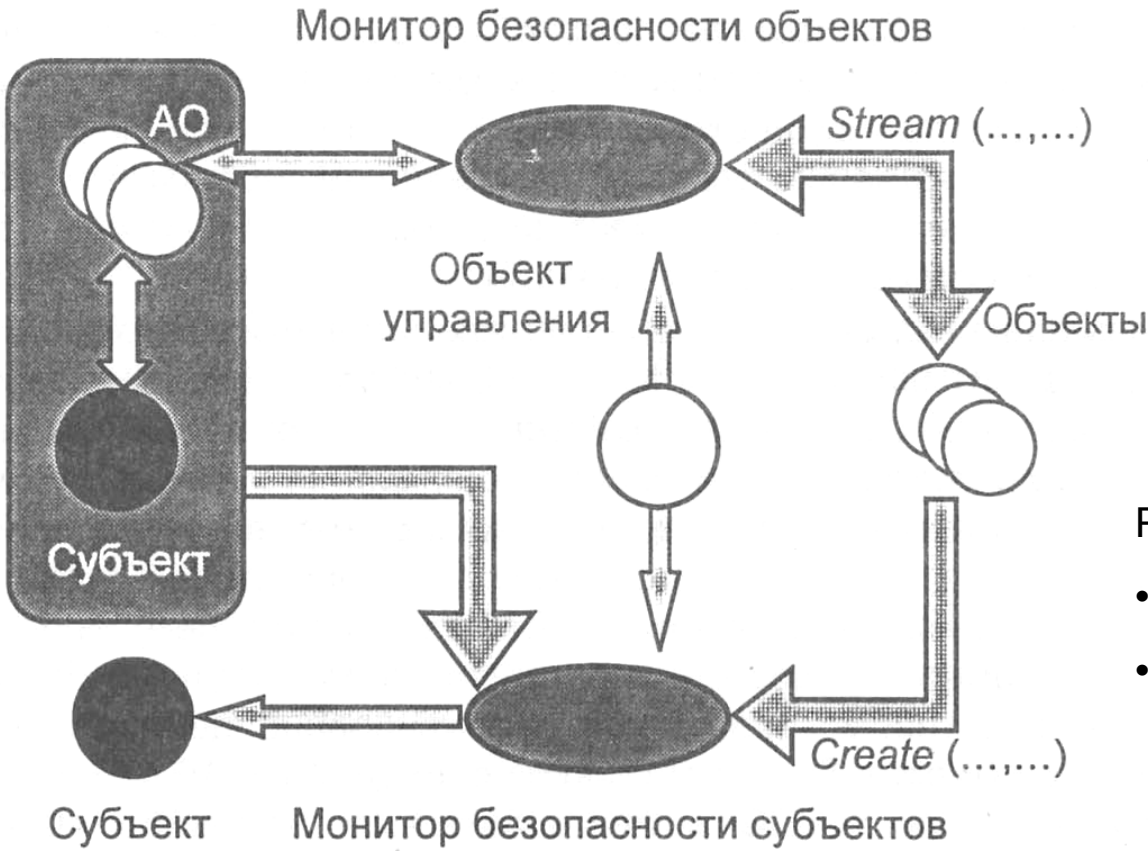


Схема ядра безопасности с учетом контроля порождения объектов

Для учета влияния субъектов в АС необходимо рассматривать расширенную схему взаимодействия элементов системы реализации и гарантирования политики безопасности.



Реализация ИПС:

- этап загрузки
- стационарная фаза

Проектирование ИПС

- Доказательство корректности субъектов программно-аппаратного уровня
- Доказательство корректности субъектов базового набора ПС
- Проектирование и разработка в в заданном множестве субъектов МБО, МБС
- «Замыкание» всех ПС в ИПС

Модели безопасности

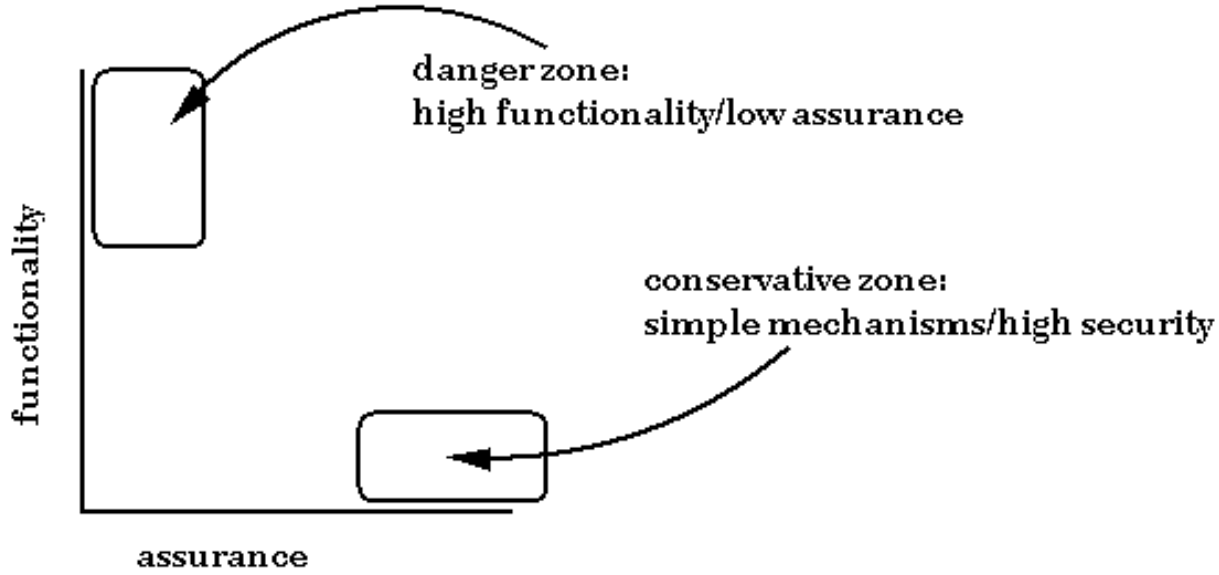
- Модель HRU используется для анализа систем защиты DAC, 1971
  - Функционирование системы рассматривается с т.з. изменений в матрице доступа: создать/удалить право, объект, субъект – шесть примитивов.
  - Теорема: задача проверки DAC систем алгоритмически неразрешима. Доказательство основывается на представлении элементов и команд HRU в виде элементов и команд МТ. При определенных ограничениях задача все же разрешима.
- Модель распространения прав Take-Grant, 1976
  - Основные элементы модели – граф доступов и правила его преобразования.
- Модель Белла-Лападула – для MAC систем, 1975
  - Даны конечные множества объектов, субъектов и 4 вида доступа: read-only, read-write, append, execute.
  - Две аксиомы безопасности: ss-свойство (запрет чтения вверх), свойство «звезда» (запрет записи вниз)
  - Три функции уровней: секретности объекта, допуска субъекта, текущий уровень допуска суббъекта.
  - Основная теорема безопасности утверждает, что система остается безопасной при выполнении ряда ограничений (см. выше), если ее исходное состояние безопасно.

Оценка защищенности

- Оценка защищенности, доказательное гарантирование защищенности АС :
  - Оценка заданного состояния защищенности АС на соответствие критериям безопасности.
  - Доказательство соответствия реализованного в АС механизма контроля доступа правилам контроля доступа.
  - Оценить защищенность множества достижимых состояний из заданного состояния АС.

Практика определения и повышения гарантий безопасности информации

- Два основных способа:
  - математическое доказательство безопасности
  - интенсивное тестирование независимой третьей стороной



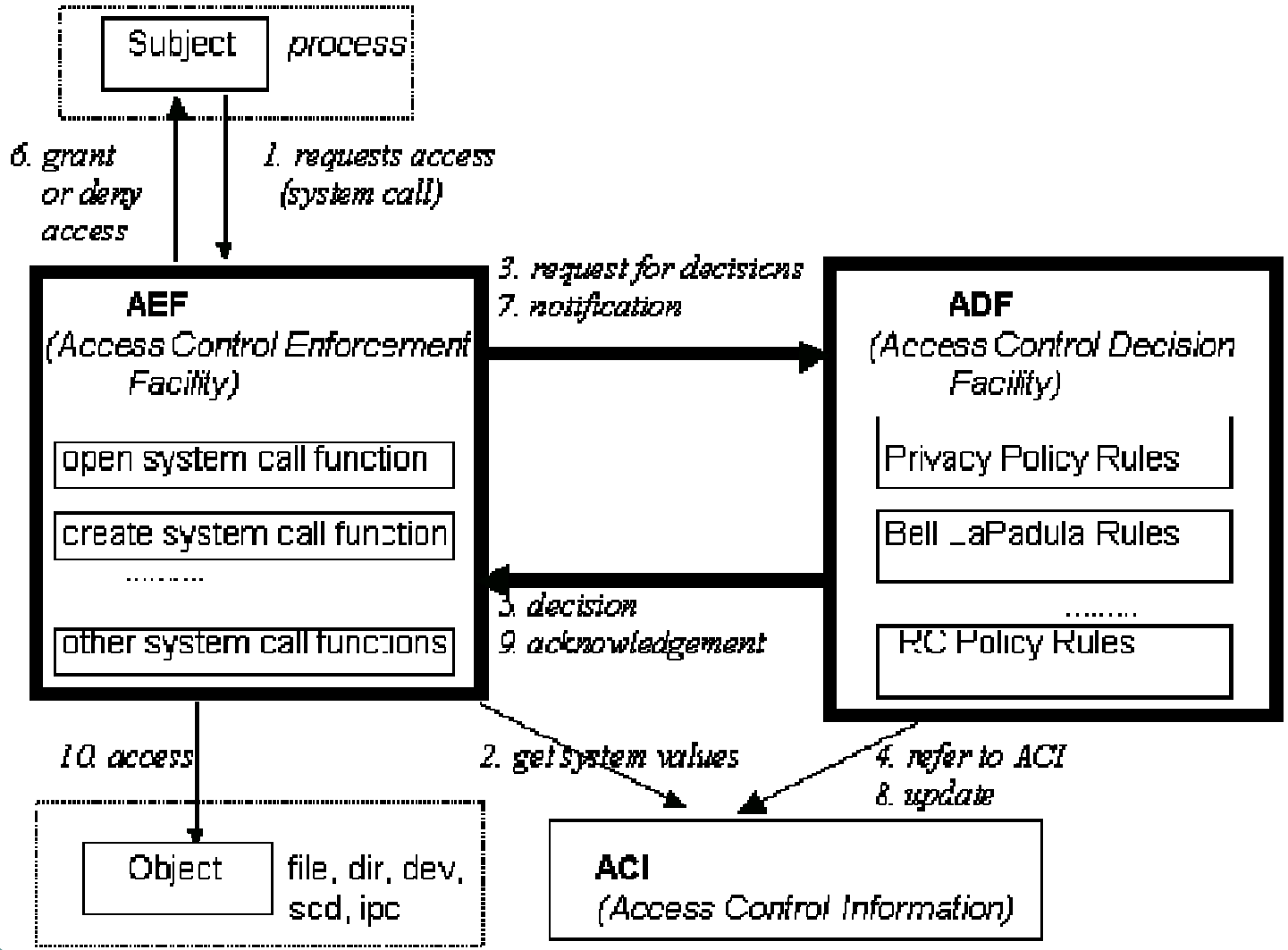
Оценка защищенности

- Достоинством формального подхода является то, что он позволяет получить точные количественные оценки различных показателей защищенности АС. Однако из-за ограниченности формального подхода, практическая реализация которого представляется делом весьма затруднительным
- В основе классификационных методик, получивших широкое распространение, лежат критерии оценки безопасности ИТ, устанавливающие классы и уровни защищенности.

Расширения *nix систем в области безопасности

- RSBAC - Rule Set Based Access Control (RSBAC) Linux Kernel Security Extension
  - Основана на Generalized Framework for Access Control (GFAC), разработка Abrams и LaPadula
  - Модель ОС Unix System V/MLS, Version 1.2.1, 1989, National Computer Security Center (США), B1/TCSEC
  - Проект закрыт
- TrustedBSD
  - нацелен на требования Common Criteria for Information Technology Security Evaluation
  - находится в стадии разработки

Архитектура RSBAC



работа перехватчика вызовов AEF

Ссылки

- Девянин П.Н. и др. Теоретические основы компьютерной безопасности: Учебное пособие для вузов. - М.: Радио и связь, 2000. - 192 с.
- Реализация Generalized Framework for Access Control (GFAC), http://www.rsbac.org/
- Проект TrustedBSD, http://www.trustedbsd.org/