Монитор безопасности и основные типы политик безопасности

Аксиомы. Идентификация и аутентифиация

A. *В защищенной КС в любой момент времени любой субъект и объект должны быть*
   - *персонифицированы* (*идентифицированы*) *и*
   - *аутентифицированы*

- *Не должно быть возможность выдавать себя за других*

- Процедуры, механизмы и системы, осуществляющие идентификацию и аутентификацию пользователей, их субъектов и объектов доступа, являются исходным и важнейшим программно-техническим рубежом защиты информации в КС

- **Идентификация** – различение и представление экземпляров сущностей по именам-идентификаторам
- **Аутентификация** – проверка и подтверждение подлинности идентифицированных экземпляров сущностей

Аксиомы. «*Монитор безопасности*"

A. *В защищенной КС должна присутствовать активная компонента (субъект, процесс и т. д.) с соответствующим объектом(ами) источником, которая осуществляет*

- *управление доступом и*
- *контроль доступа субъектов к объектам.*

- За такой активной компоненты утвердился термин "*монитор безопасности*".

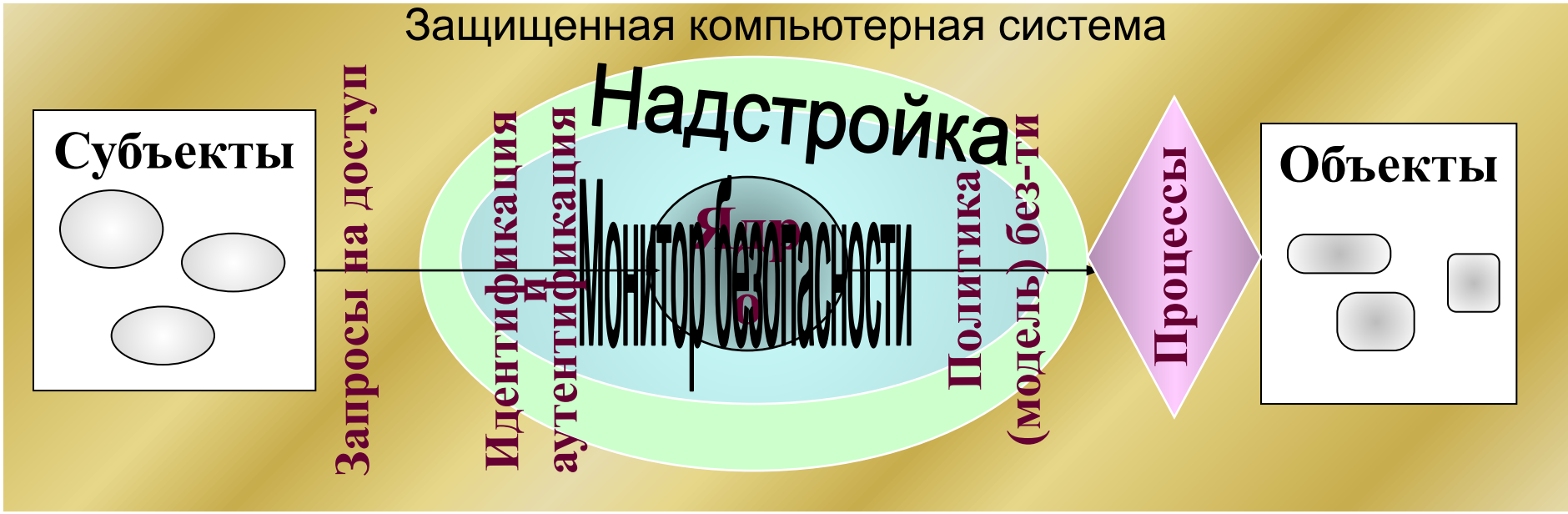
Архитектура незащищенной КС

- Компонента доступа – файловая система ОС, модель данных СУБД
- Компонента представления - система ВВ ОС, процессор запросов СУБД
- Надстройка - утилиты, сервис, интерфейсные компоненты

Архитектура защищенной КС

- МБ – доп. компонента, обеспечивающая процессы защиты информации – идентификации / аутентификации, а также управление доступом на основе некоторой Политики Безопасности (разграничения доступа)
- МБ д.б. реализован на нулевом уровне (на уровне ядра) системы
- Ядро должно проектироваться с учетом работы МБ


Компьютерная система
Субъекты
Обращение
Надстройка
ядро
Инициализация
Процессы
Объекты
Компонент доступа (система ввода-вывода в ОС)
Компонент представления (файловая система в ОС)


Защищенная компьютерная система
Субъекты
Запросы на доступ
Надстройка
Идентификация и аутентификация
Монитор безопасности
ядро
Политика (модель) без-ти
Процессы
Объекты

Требования к реализации МБ

1. ***Полнота*.** МБ должен вызываться (активизироваться) при каждом обращении за доступом любого субъекта к любому объекту, и не должно быть никаких способов его обхода.
2. ***Изолированность*.** МБ должен быть защищен от отслеживания и перехвата своей работы.
3. ***Верифицируемость*.** МБ должен быть проверяемым (само- или внешне тестируемым) на предмет выполнения своих функций.
4. ***Непрерывность*.** МБ должен функционировать при любых штатных и нештатных, в том числе и аварийных ситуациях.

- МБ в защищенной КС является субъектом осуществления принятой **политики безопасности**, реализуя через алгоритмы своей работы соответствующие **модели безопасности**.
- п.2, п.3 - связанны **с гарантиями** выполнения политики безопасности
- не выполнение п.4 – основная причина атак

Особенности модели

- Монитор безопасности
  - МБ объектов (МБО)
    - называется субъект, активизирующийся при возникновении потока между любыми объектами, порождаемым любым субъектом, и разрешающий только те потоки, которые принадлежат P_L
  - МБ субъектов (МБС)
    - называется субъект, активизирующийся при любом порождении субъектов, и разрешающий порождение субъектов только для фиксированного подмножества пар активизирующих субъектов и объектов-источников

Гарантии выполнения политики безопасности обеспечиваются определенными требованиями к МБО и МБС, реализующими т.н. *изолированную программную среду* (*ИПС)*

Гарантии выполнения политики безопасности

- Гарантии выполнения политики безопасности обеспечиваются
  - определенными требованиями к МБО и МБС, реализующими т.н. *изолированную программную среду (**ИПС**)*
- Исходный тезис –
  - при изменении объектов, функционально ассоциированных с субъектом монитора безопасности, могут измениться свойства самого МБО и МБС, что может привести к нарушению ПБ

Достаточное условие гарантированного выполнения ПБ в КС

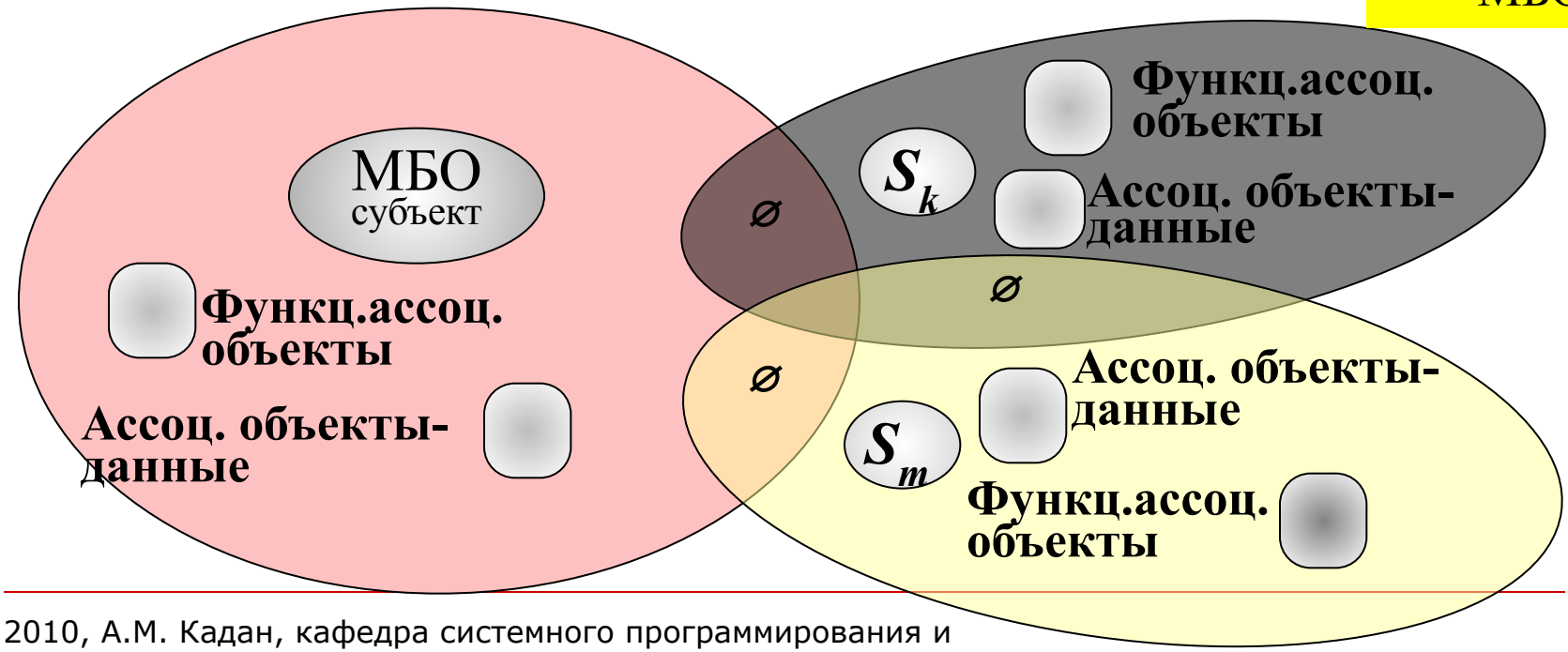
- МБО разрешает порождение потоков только из P_L;
- все существующие в КС субъекты абсолютно корректны относительно МБО и друг друга

- Субъекты S_i и S_j называются *невлияющими* друг на друга (или *корректными* относительно друг друга), если
  - в любой момент времени отсутствует поток (изменяющий состояние объекта) между любыми объектами O_i и O_j, ассоциированными соответственно с субъектами S_i и S_j,
  - причем O_i не ассоциирован с S_j, а O_j не ассоциирован с S_i

Достаточное условие гарантированного выполнения ПБ в КС

- МБО разрешает порождение потоков только из P_L;
- все существующие в КС субъекты абсолютно корректны относительно МБО и друг друга

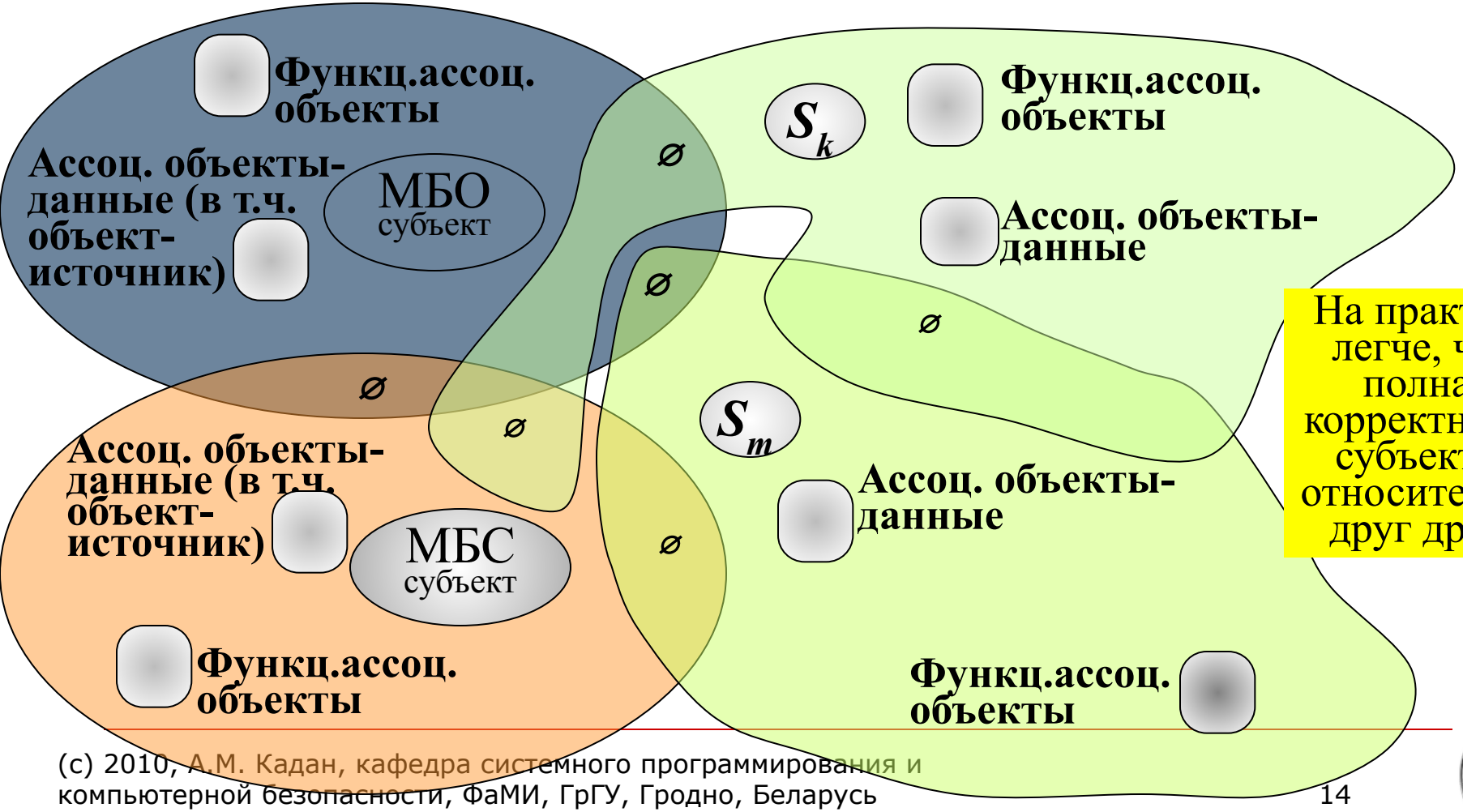
На практике только корректность относительно МБО



Достаточное условие выполнения ПБ в ИПС

- ИПС – золированная программная система
- Если
  - существует МБО и
  - порождаемые субъекты абсолютно корректны относительно МБО,
  - а также МБС абсолютно корректен относительно МБО, то в КС реализуется доступ, описанный ПБ

Достаточное условие выполнения ПБ в ИПС



На практике легче, чем полная корректность субъектов относительно друг друга

Проблемы реализации ИПС

- *проблема производительности*
  - повышенные требования к вычислительным ресурсам
- *проблема загрузки* (*начального инициирования*) *ИПС*
  - нестационарность функционирования КС (особенно в нач. момент времени) из-за изменения уровня представления объектов
- *проблема целостности объектов* и *проблема чтения реальных данных*
  - сложность технической реализацией контроля неизменности объектов

А. Аксиома 1.3.3. *Для реализации принятой политики безопасности, управления и контроля доступа субъектов к объектам должна существовать информация и объекты, ее содержащие (помимо информации для идентификации и аутентификации пользователей).*

- Т.е. МБ, как и любая активная сущность в КС, является субъектом с соответствующим объектом-источником и ассоциированными объектами.

1. Следствие 1. *В защищенной КС существуют особая категория субъектов (активных сущностей), которые не инициализируют и которыми не управляют пользователи системы – т. н. системные процессы (субъекты), присутствующие (функционирующие) в системе изначально*

- К числу таких системных субъектов относится исходный системный процесс, который инициализирует первичные субъекты пользователей, а, также МБ который управляет доступами субъектов пользователей к объектам системы.
- Для обеспечения защищенности в КС свойства системных субъектов должны быть неизменными, от чего напрямую зависят гарантии безопасности.

A. Аксиома 1.3.3. *Для реализации принятой политики безопасности, управления и контроля доступа субъектов к объектам необходима* (*должна существовать*) *информация и объект*(*ы*), *ее содержащий*(*ие*) (*помимо информации для идентификации и аутентификации пользователей*).

1. Следствие 1.3.1 (из аксиомы 1.3.3). *В защищенной КС существуют особая категория субъектов* (*активных сущностей*), *которые не инициализируют и которыми не управляют пользователи системы – т. н. системные процессы* (*субъекты*), *присутствующие* (*функционирующие*) *в системе изначально*
2. Следствие 1.3.2 (из аксиомы 1.3.3). *Ассоциированный с монитором безопасности объект, содержащий информацию по системе разграничения доступа, является наиболее критическим с точки зрения безопасности информационным ресурсом в защищенной КС.*
3. Следствие 1.3.3 (из аксиомы 1.3.3). *В защищенной системе может существовать доверенный пользователь* (*администратор системы*), *субъекты которого имеют доступ к ассоциированному с монитором безопасности объекту-данным для управления политикой разграничения доступа.*

Типы политик безопасности

- В упрощенной трактовке ПБ –
  - общий принцип (методология, правила, схема) безопасной работы (доступа) коллектива пользователей с общими информационными ресурсами.

- Важнейшее значение имеет **критерий безопасности доступов** субъектов к объектам,
  - т. е. правило разделения информационных потоков, порождаемых доступами субъектов к объектам, на **опасные и неопасные**.

Основные политики безопасности

- Две базовых политики безопасности –
  - дискреционная (политика избирательного доступа)
  - мандатная (политика полномочного доступа).
- Ролевая политика безопасности
  - Объединяет известные модели ролевого доступа
- Политика тематического разграничения доступа
  - в документальных информационно-поисковых системах
  - "подсмотрена" во внекомпьютерной (библиотечно-архивной) сфере.

Политика дискреционного (избирательного) доступа

- Политика дискреционного (избирательного) доступа (ПДД)
  - *Множество безопасных* (*разрешенных*) *доступов* ***PL*** *задается для именованных пользователей* (*субъектов*) *и объектов явным образом в виде дискретного набора троек* ***"Пользователь (субъект)-поток(операция)-объект"****.*
- Принцип ПДД
  - охарактеризовать схемой "каждый-с каждым", т. е.
  - иными словами для любой из всевозможных комбинаций "пользователь (субъект)-ресурс (объект)" должно быть явно задано ("прописано") разрешение/запрещение доступа и вид соответствующей разрешенной/запрещенной операции (***Read, Write*** и т. д.).
- Таким образом, при ПДД разграничение доступа осуществляется самым детальным образом – до уровня отдельно взятого субъекта, отдельно взятого объекта доступа и отдельно взятой операции.

Политика мандатного (полномочного) доступа

- *Множество безопасных (разрешенных) доступов **PL** задается неявным образом через введение*
  - ***уровня допуска -** для пользователей-субъектов некоторой дискретной характеристики доверия,*
  - ***грифа секретности -** для объектов некоторой дискретной характеристики конфиденциальности,*
- *На этой основе*
  - *пользователи-субъекты наделяются некими полномочиями порождать определенные потоки в зависимости от соотношения "уровень допуска-поток(операция)-уровень конфиденциальности".*
- В отличие от ПДД, при МПД разграничение доступа производится менее детально –
  - до уровня группы пользователей с определенным уровнем допуска и
  - группы объектов с определенным уровнем конфиденциальности.
- Это создает условия для
  - упрощения и улучшения управления доступом ввиду существенного уменьшения количества субъектов управления и контроля.

Политика тематического доступа

- *Множество безопасных доступов **PL** задается неявным образом через*
  - *введение для пользователей-субъектов некоторой тематической характеристики – разрешенных тематических информационных рубрик,*
  - *а для объектов аналогичной характеристики в виде набора тематических рубрик, информация по которым содержится в объекте, и*
  - *наделение на этой основе субъектов-пользователей полномочиями порождать определенные потоки в зависимости от соотношения "набор тематических рубрик субъекта–набор тематических рубрик объекта".*
- Как и при ПМД, ПТД определяет доступ субъекта к объекту неявно, через соотношение предъявляемых специальных характеристик субъекта и объекта и, соответственно, по сравнению с ПДД существенно упрощает управление доступом.

Политика ролевого доступа

- *Множество безопасных (разрешенных) доступов **PL** задается через*
  - *введение в системе дополнительных абстрактных сущностей – **ролей**, выступающих некими "типовыми" (ролевыми) субъектами доступа, с которыми ассоциируются конкретные пользователи (в роли которых осуществляют доступ), и*
  - *наделение ролевых субъектов доступа на основе дискреционного или мандатного принципа правами доступа к объектам системы.*
- Ролевая политика разграничивает доступ не на уровне пользователей-субъектов, а на уровне ролей, являющихся группами однотипного доступа к объектам системы, и на этой основе развивает ту или иную базовую политику безопасности (дискреционную или мандатную).
- Поэтому обычно ролевой принцип разграничения доступом не выделяется в отдельную политику, а рассматривается в качестве неких дополнений к моделям дискреционного или мандатного доступа.

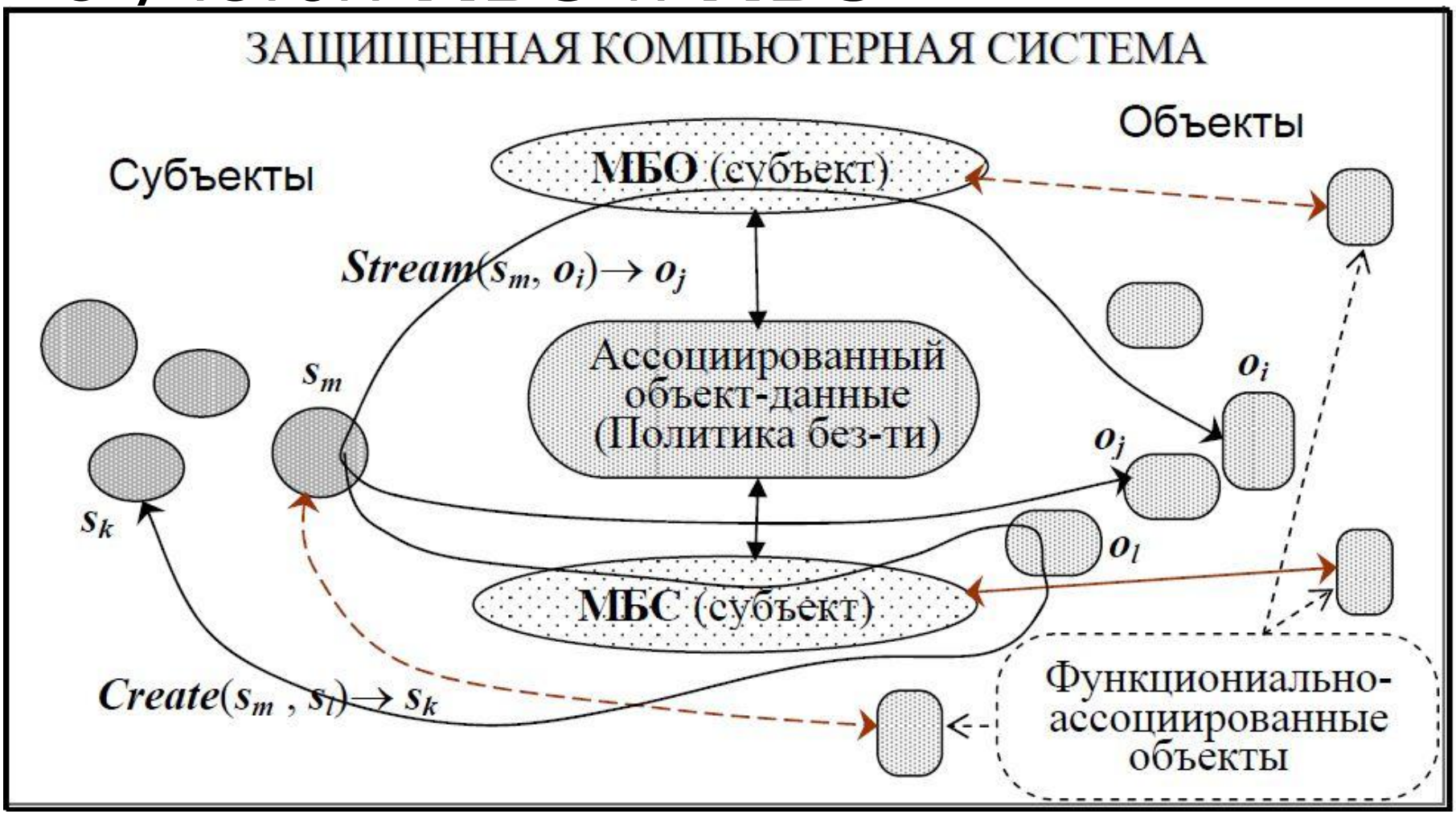
Временн’ая и маршрутная политики разграничения доступа

- Широко используется в практике функционирования защищенных компьютерных систем (в распределенных КС) ограничения доступа
  - **Временная П** - предоставление пользователям прав работы в КС по определенному временному регламенту (по времени и длительность доступа)
  - **Маршрутная П** - предоставление пользователям прав работы в КС при доступе по определенному маршруту (*с определенных рабочих станций*)
- Это позволяет говорить, что они дополняют базовые политики безопасности

Гарантирование выполнения политики безопасности

- Общий критерий безопасности КС
  - *Компьютерная система безопасна тогда и только тогда, когда субъекты не имеют никаких возможностей нарушать* (*обходить*) *установленную в системе политику безопасности.*
- Субъект обеспечения политики безопасности
  - монитор безопасности (МБС + МБО).
- *Необходимое* условием безопасности КС
  - наличие монитора безопасности в структуре КС
- *Достаточное* условие безопасности КС
  - в безопасности самого монитора безопасности.

Порождение потоков и субъектов с учетом **МБО** и **МБС**



- Подтверждением данного тезиса является обязательное включение в состав спецификаций по созданию (разработке) и оценке (сертификации) защищенных КС требований корректности, верификации, адекватности и т. д. средств защиты информации (т. е. монитора безопасности) во всех, в том числе, и отечественных стандартах и руководящих документах по компьютерной безопасности.