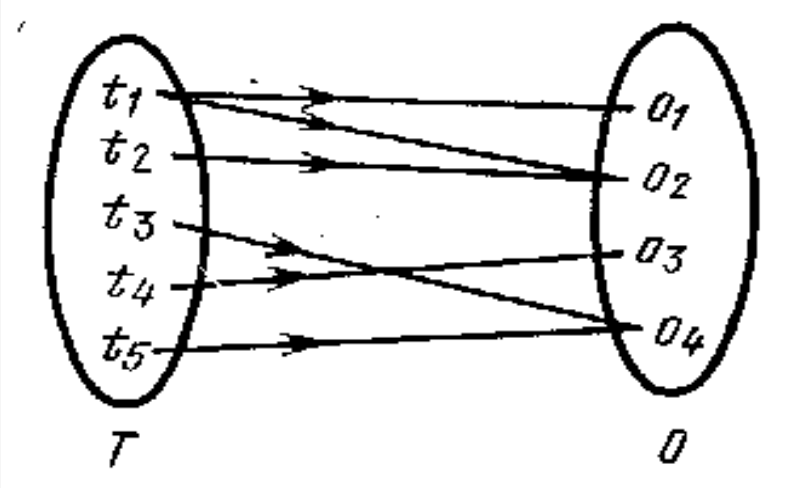
Лекция 3

Модели управления доступом

и информационными потками.

Субъектно-объектная модель компьютерной системы



Компьютерная система

Субъекты

(активные сущности)

Процессы субъектов

Объекты

(пассивные сущности)

Субъектно-объектная модель компьютерной системы

Положение 1. В КС действует дискретное время.

Положение 2. В каждый фиксированный момент времени t_k КС представляет собой конечное множество элементов, разделяемых на два подмножества:

- подмножество субъектов доступа S;
- подмножество объектов доступа O.

Положение 3. Пользователи КС представлены одним или некоторой совокупностью субъектов доступа, действующих от имени конкретного пользователя.

Положение 4. Субъекты КС могут быть порождены из объектов только активной сущностью (другим субъектом).

Положение 5. Все процессы безопасности в КС описываются доступами субъектов к объектам, вызывающими потоки информации.

Субъектно-объектная модель компьютерной системы

*Под **субъектом** доступа понимается активная сущность КС, которая может изменять состояние системы через порождение процессов над объектами, в том числе, порождать новые объекты и инициализировать порождение новых субъектов.*

*Под **объектом** доступа понимается пассивная сущность КС, процессы над которой могут в определенных случаях быть источником порождения новых субъектов.*

В модели предполагается наличие априорно безошибочного механизма различения активных и пассивных сущностей (т. е. субъектов и объектов) по свойству активности (например различия между файлом с кодом программы и исполняемой (запущенной) программой).

Предполагается также, что в любой момент времени t_k , в том числе и в начальный, множество субъектов доступа не пусто.

Субъектно-объектная модель компьютерной системы

*Под **пользователем** КС понимается лицо, внешний фактор, аутентифицируемый некоторой информацией, и управляющий одним или несколькими субъектами, воспринимающий объекты и получающий информацию о состоянии КС через субъекты, которыми он управляет.*

Понятия субъектов доступа и пользователей не тождественны.

Предполагается также, что пользовательские управляющие воздействия не могут изменить свойств самих субъектов доступа.

Субъектно-объектная модель компьютерной системы

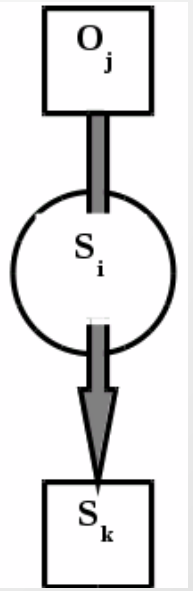
Субъекты порождаются - субъектами.

Объект O_f *называется* ***источником*** *для субъекта* S_m *если существует субъект* S_j*, в результате воздействия которого на объект* O_f *возникает субъект* S_m*.*

Соответственно, субъект S_j *, называется активизирующим для субъекта* S_m *.*

Create (S_j, O_f) — S_m
(Если это невозможно, то *Create* (S_j, O_f) — 0)

Create называют операцией порождения субъектов



Субъектно-объектная модель компьютерной системы

Субъекты порождаются - субъектами (воздействием в момент времени t_k , а новый субъект порождается уже в момент времени $t_k + 1$).

Объект O_f, в момент времени t_k ассоциирован с субъектом S_m , если состояние объекта повлияло на состояние субъекта в следующий момент времени t_k+1 (т.е. субъект S_m использует информацию, содержащуюся в объекте O_f).

- Т.е. объект-источник в момент порождения субъекта является ассоциированным с ним, а в последующие моменты времени может перестать быть или остаться ассоциированным с ним.
- В ассоциированных объектах отображается текущее состояние субъекта

Субъектно-объектная модель компьютерной системы

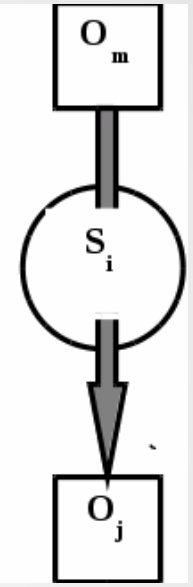
Объекты O_i и O_j
называются **тождественными в момент времени** t_k, если их содержимое совпадает (т. е. они имеют одинаковую запись в некотором языке).

Субъекты S_l и S_m
называются **тождественными в момент времени** t_k, если попарно тождественны все ассоциированные с ними объекты.

Замечание. Порожденные субъекты тождественны, если тождественны порождающие субъекты и объекты-источники.

Субъектно-объектная модель компьютерной системы

Потоком информации *между объектом* O_m *и объектом* O_j *называется произвольная операция над объектом* O_j*, реализуемая в субъекте* S_i *и зависящая от* O_m.



Stream(S_i O_m) → O_j

- Как O_j, так и O_m могут быть ассоциированными или неассоциированными объектами, а также «пустыми» объектами (NULL).
- Объект-источник в момент порождения потока субъектом является ассоциированным с ним, а в последующие моменты времени может перестать быть или остаться ассоциированным с ним.
- Говорить корректно о потоках информации можно лишь в отношении потоков между одинаковыми сущностями, т. е. объектами.

Субъектно-объектная модель компьютерной системы

Поток всегда инициируется (порождается) субъектом.

Доступом субъекта ***S***$_i$ *к объекту* ***O***$_j$ *будем называть порождение потока информации между некоторым объектом (например, ассоциированным с субъектом объектами* ***S****i*(***O***$_m$)) *и объектом* ***O***$_j$.

Пусть
P *- множество потоков для фиксированной декомпозиции КС на субъекты и объекты во все моменты времени (все множество потоком является объединением потоков по всем моментам дискретного времени);*
N *- подмножество потоков, характеризующее несанкционирован-ный доступ;*
L *- подмножество потоков, характеризующих легальный доступ.*

Субъектно-объектная модель компьютерной системы

Деление на L и N может описывать как свойство целостности (потоки из N нарушают целостность КС) или свойство конфиденциальности (потоки из N нарушают конфиденциальность КС), так и любое другое произвольное свойство.

***Правила разграничения доступа** субъектов к объектам есть (политика безопасности) это формально описанные потоки, принадлежащие подмножеству **L**.*

В предлагаемой модели не производится уточнений известных моделей политик безопасности, но формулируются условия корректного существования элементов КС, обеспечивающих реализацию той или иной политики безопасности, таким образом, модель инвариантна любой политике безопасности.

Монитор безопасности

Для разделения всего множества потоков в КС на подмножества **L** и **N** необходимо существование активной компоненты (субъекта), который:
- активизировался бы при возникновении любого потока;
- производил бы фильтрацию потоков в соответствии с принадлежностью множествам **L** или **N**.

Монитор обращений *(МО)* - ***субъект, активизирующийся при возникновении потока от любого субъекта к любому объекту.***

МО бывают двух видов:
- индикаторный (устанавливающий только факт обращения);
- содержательный (при возникновении $Stream(\boldsymbol{S}_m,\boldsymbol{O}_i)\rightarrow\boldsymbol{O}_j$ и обратно существует ассоциированный с МО объект $\boldsymbol{O}_0$, тождественный $\boldsymbol{O}_i$ или одному из $[\boldsymbol{S}_m]_t$).

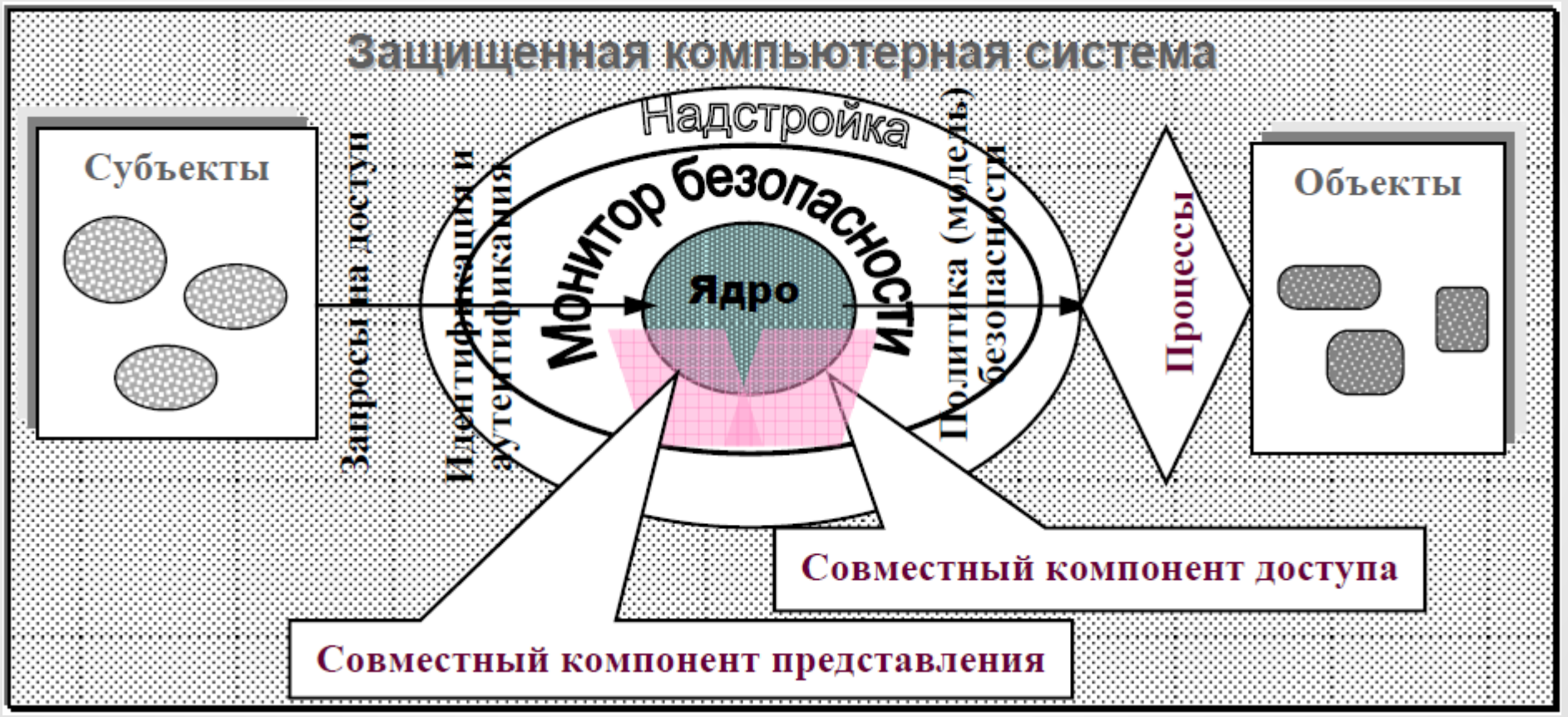
Монитор безопасности

***Монитор безопасности* объектов** *(МБО) - монитор обращений, который разрешает поток, принадлежащий только множеству легального доступа L. Разрешение потока в данном случае понимается как выполнение операции над объектом - получателем потока, а запрещение - как невыполнение (т. е. неизменность объекта - получателя потока).*

В литературе для данной активной компоненты утвердился термин "***монитор безопасности".***

МБО является механизмом реализации политики безопасности в КС.

Монитор безопасности



Монитор безопасности

В практическом плане, в том числе и с учетом отечественных и международных нормативных требований по сертификации защищенных систем, к реализации монитора безопасности предъявляются следующие обязательные требования:

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

Монитор безопасности

При изменении ассоциированных с МБО объектов могут измениться свойства самого МБО и в результате возникнуть запрещенные потоки.
Например, субъект ***S*** создает субъекта ***S'***, через которого реализует запрещенный поток из ***O*** в ***O'***:
(*Stream*(***S'***,***O***)→***O'*** вместо *Stream*(***S***,***O***)→***O'***)

Субъекты ***S*** и ***S'*** называются **невлияющими друг на друга** (корректными), если в любой момент времени *t* отсутствует поток между объектами $O \in [S]_t$ и $O' \in [S']_t$.

Смысл корректности: существующие в одном пространстве ОС программы не должны иметь возможности изменения «чужого» вектора кода и состояния переменных.

Субъекты ***S*** и ***S'*** называются **абсолютно невлияющими друг на друга** (абсолютно корректными), если в любой момент времени t $[S]_t \cap [S']_t = \varnothing$.

Монитор безопасности

Теорема №1 (достаточное условие гарантированного выполнения политики безопасности в КС).

МБО разрешает порождение потоков только из L, если все существующие в системе субъекты абсолютно корректны относительно него и друг друга.

Доказательство:

Из условия абсолютной корректности любых субъектов с **МБО** вытекает отсутствие потоков, которые могут изменить функционально-ассоциированные и ассоциированные объекты-данные с **МБО** и тем самым изменить его свойства для осуществления обхода (нарушения) политики безопасности. С другой стороны, отсутствуют также потоки между ассоциированными объектами и всех любых других субъектов, и, следовательно, отсутствует возможность изменения одними субъектами свойств других субъектов для возможного нарушения (обхода) политики безопасности. Тем самым утверждение доказано. ■

Монитор безопасности

Данная теорема, однако, для обеспечения гарантий безопасности накладывает чрезвычайно жесткие условия, практически не выполнимые на практике, или существенно снижающие функциональные возможности КС (отсутствие общих объектов-источников для запуска программ разными пользователями, отсутствие общих участков памяти, буферов для обмена данными и т. п.).
Для исследования подходов, в большей степени возможных при практической реализации, вводятся понятия замкнутости и изолированности подмножества субъектов системы (А.Грушо, А.Щербаков).

Монитор порождения субъектов (МПС) — субъект, активизирующийся при любом порождении субъектов.

Монитор безопасности субъектов (МБС) — субъект, который разрешает порождение субъектов только для фиксированного подмножества пар активизирующих субъектов и объектов-источников.

Воздействие МБС выделяет подмножество разрешенных субъектов

$$E \subset S$$

Изолированная программная среда (ИПС)

КС называется **замкнутой по порождению субъектов** (имеет замкнутую программную среду (ПС)), если в ней действует МБС, разрешающий порождение только фиксированного конечного подмножества субъектов, для любых объектов-источников, рассматриваемых для фиксированной декомпозиции КС на субъекты и объекты.

Множество субъектов программной среды называется **изолированным (абсолютно изолированным)**, если в ней действует МБС, и субъекты из порождаемого множества корректны (абсолютно корректны) относительно друг друга и МБС.

- Любое подмножество субъектов изолированной (ИПС) (абсолютно изолированной (АИПС)) программной среды вместе с МБС также составляет ИПС (АИПС).

- Дополнение ИПС (АИПС) субъектом, корректным (абс. корректным) относительно любого числа субъектов, входящих в ИПС (АИПС), оставляет ее изолированной (абсолютно изолированной).

Изолированная программная среда (ИПС)

Теорема №2. (достаточное условие гарантированного выполнения политики безопасности в КС)

Если в АИПС существует МБО, и порождаемые субъекты абсолютно корректны с МБО, МБС и другими субъектами, а МБС абсолютно корректен с МБО, то МБО разрешает выполнение только потоков из **L**.

Доказательство: В системе могут существовать только абсолютно корректные относительно **МБС** и друг друга субъекты из некоторого их конечного множества. Следовательно, отсутствует возможность изменения свойств **МБС.** Абсолютная корректность **МБС** и других субъектов по отношению к **МБО** обеспечивает отсутствие возможностей изменения свойств **МБО,** что в итоге автоматически обеспечивает разрешение только тех потоков, которые входят в множество ***L.***■

Данная теорема дает более конструктивные условия безопасности. В КС, очевидно, необходим механизм проверки абсолютной корректности субъектов.

Изолированная программная среда (ИПС)

В реальных КС одинаково поименованные объекты в различные моменты времени могут иметь различное размещение.

Размещение объекта ***O*** в момент времени *t* обозначим ***O***[t].

Операция порождения субъекта Create(S,O)→S' называется ***порождением с контролем неизменности объекта-источника****, если* $\forall t>t_0$ *порождение S' возможно только при* $O[t_0]=O[t]$.

В условиях определения, порожденные с контролем неизменности субъекты $\mathbf{S}'[t_1]$ *и* $\mathbf{S}'[t_2]$ *тождественны, при* $t_1,t_2>t_0$.
При $t_1=t_2$ *порождается один и тот же субъект.*

Изолированная программная среда (ИПС)

Теорема (базовая теорема ИПС)

Если с момента времени t_0 в ИПС (АИПС) действует только порождение субъектов с контролем неизменности объекта, и существуют потоки между объектами через субъекты, которые корректны (абсолютно корректны) относительно друг друга, то $\forall t > t_0$ программная среда также ИПС (АИПС).

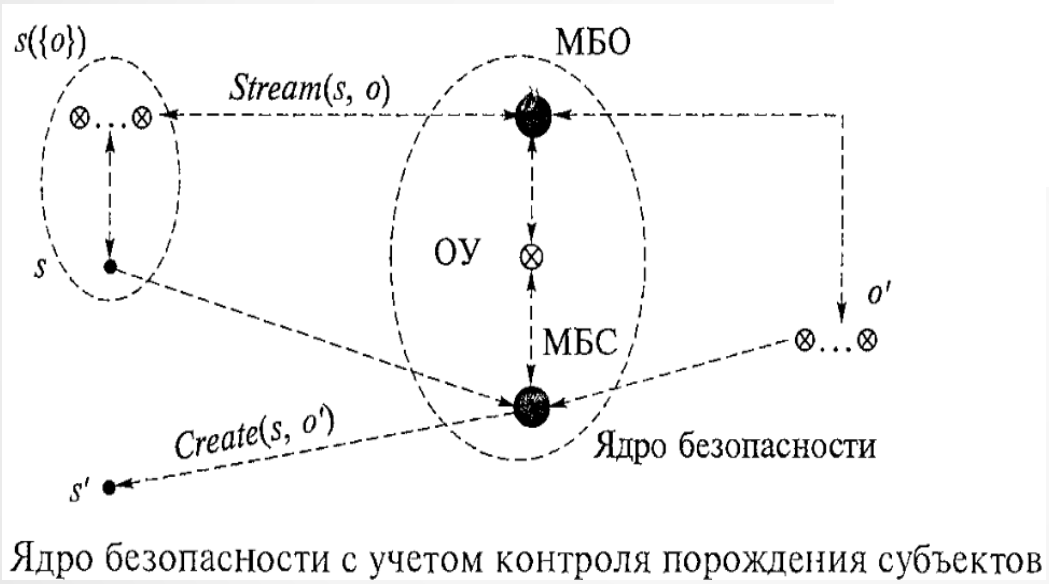
Доказательство:

1. Из условия абсолютной корректности следует, что м.б. только такие потоки, которые изменяют состояние объектов, не ассоциированных в соответствующие моменты времени с каким-либо субъектом. Отсюда не м.б. изменены объекты-источники.

2. Т.к. объекты-источники остаются неизменными, то мощность множества порождаемых субъектов не расширяема, и тем самым множество субъектов КС остается изолированным. ■

Изолированная программная среда (ИПС)

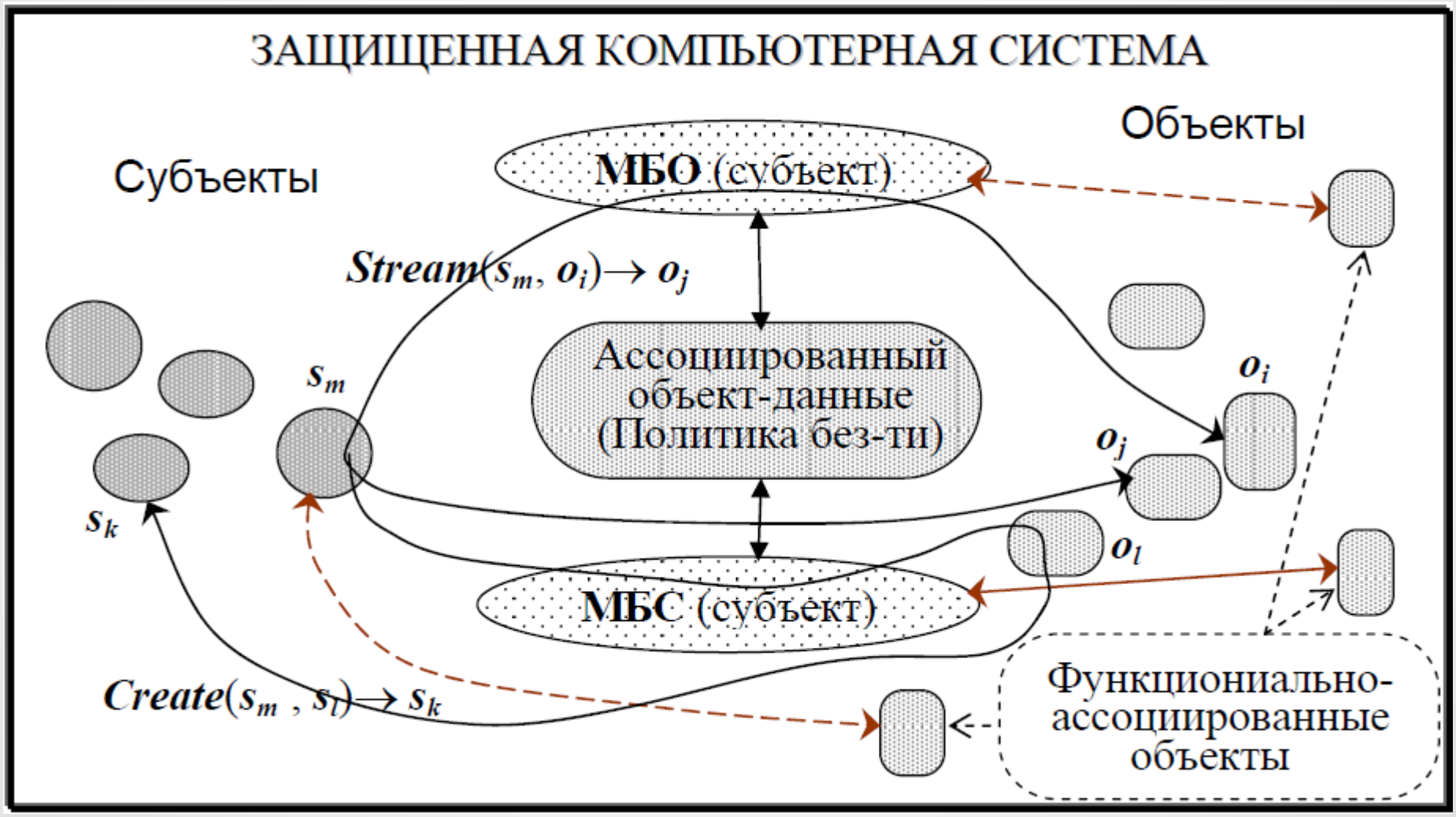
Классическая схема ядра безопасности



Ядро безопасности с учетом контроля порождения субъектов

Рассмотренная концепция ИПС является расширением классического подхода к реализации ядра безопасности, когда потоки разделены на потоки «по белому списку» и «по черному списку», и реализуются через объект управления (ОУ). ОУ разрешает первые и запрещает вторые.

Изолированная программная среда (ИПС)



Изолированная программная среда (ИПС)

В модели ИПС порождение потоков усложнено введением ассоциированных объектов. ОУ содержит информацию о разрешенных значениях отображений *Stream*() и *Create*(). ОУ может быть ассоциирован как с МБО, так и с МБС.

Опираясь на базовую теорему ИПС, опишем метод субъектно-объектного взаимодействия в рамках ИПС.
Согласно теореме, нужно:
1. Убедиться в попарной корректности субъектов, замыкаемых в ИПС (или их корректности с МБО и МБС).
2. Спроектировать и реализовать МБС так, чтобы:
а) для всех субъектов и объектов производился контроль порождения субъектов;
б) порождение любого субъекта происходило с контролем неизменности объекта-источника.
3. Реализовать МБО в рамках сформулированной политики безопасности.

Изолированная программная среда (ИПС)

Проблемы реализации изолированной программной среды:

- повышенные требования к вычислительным ресурсам – ***проблема производительности***

- нестационарность функционирования КС (особенно в нач. момент времени) из-за изменения уровня представления объектов (сектора-файлы) – ***проблема загрузки (начального инициирования) ИПС***

- сложность технической реализацией контроля неизменности объектов - ***проблема целостности объектов*** и ***проблема чтения реальных данных***

Модели (политики) безопасности

Методологической основой для формирования политик безопасности в защищенных КС послужили реальные организационно-технологические схемы обеспечения безопасности информации во вне (до) компьютерных сферах.
Многие подходы к защите компьютерной информации были "подсмотрены", в частности, в сфере работы с "бумажными" конфиденциальными документами, проще говоря, в сфере делопроизводства.

Выделяется две основных (базовых) политики безопасности - дискреционная и мандатная. Или иначе в терминологии сферы защиты компьютерной информации, первую называют политикой избирательного доступа или матричной моделью доступа, а вторую - политикой полномочного доступа или потоковой моделью доступа.

Модели (политики) безопасности

Политика дискреционного (избирательного) доступа.

*Множество безопасных (разрешенных) доступов **L** задается для именованных пользователей (субъектов) и объектов явным образом в виде дискретного набора троек "Пользователь(субъект)-поток(операция)-объект".*

Модели (политики) безопасности

Политика мандатного (полномочного) доступа.

Множество безопасных (разрешенных) доступов ***L*** задается неявным образом через введение для пользователей-субъектов некоторой дискретной характеристики доверия (уровня допуска), а для объектов некоторой дискретной характеристики конфиденциальности (грифа секретности), и наделение на этой основе пользователей-субъектов некими полномочиями порождать определенные потоки в зависимости от соотношения "уровень допуска – поток (операция) - уровень конфиденциальности ".

Модели (политики) безопасности

Политика тематического доступа.

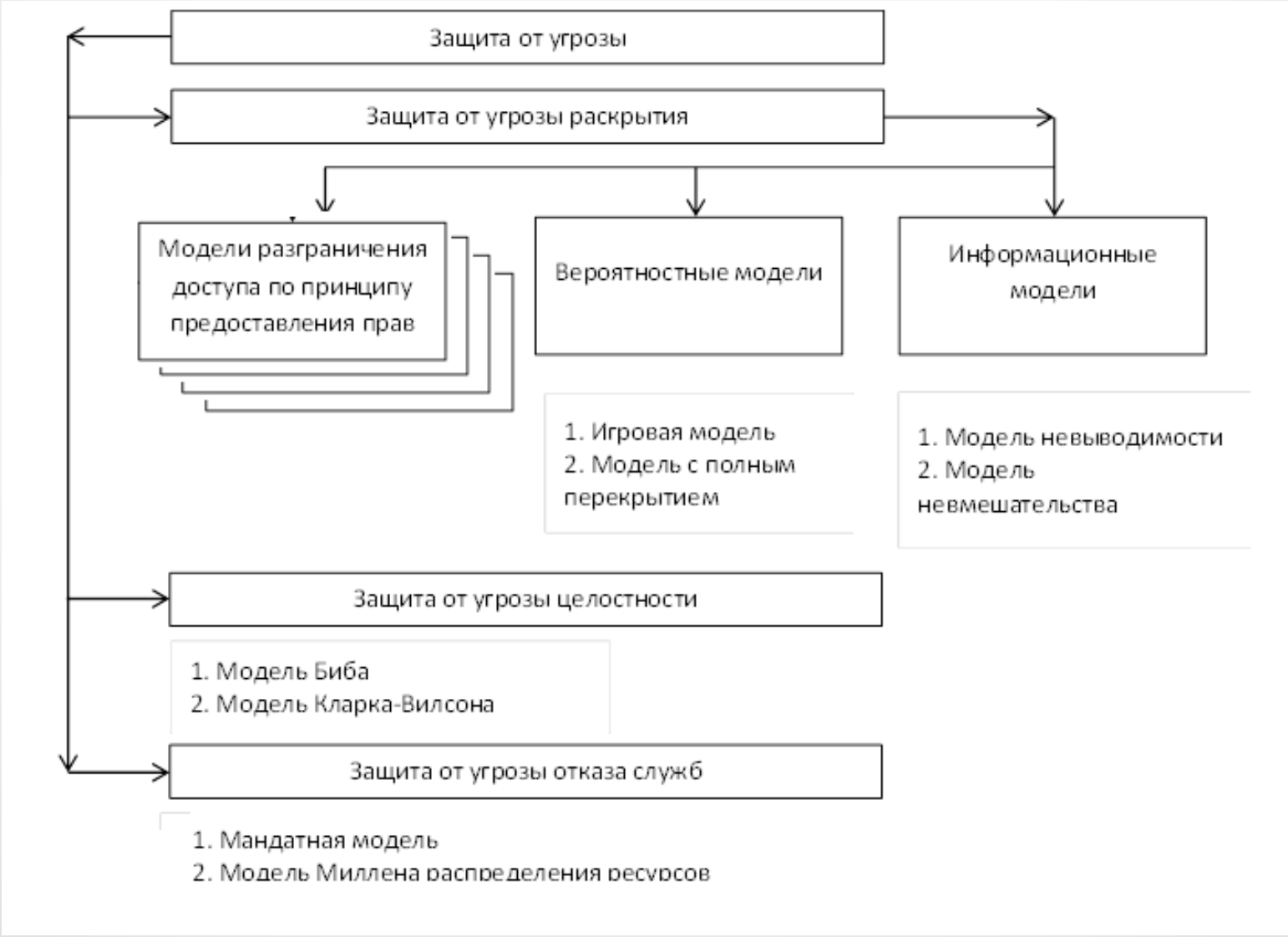
Множество безопасных (разрешенных) доступов ***L*** задается неявным образом через введение для пользователей-субъектов некоторой тематической характеристики - разрешенных тематических информационных рубрик, а для объектов аналогичной характеристики в виде набора тематических рубрик, информация по которым 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".

Модели (политики) безопасности

Политика ролевого доступа.

Множество безопасных (разрешенных) доступов ***L*** 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.

Модели (политики) безопасности



Модели (политики) безопасности

1. Матрица доступов
2. Модель Харрисона-Руззо-Ульмана
3. Модель Take-Grant
4. Модель АДЕПТ-50
5. Модель Харстона

1. Модель Белла-ЛаПадула
2. Модель Деннинг