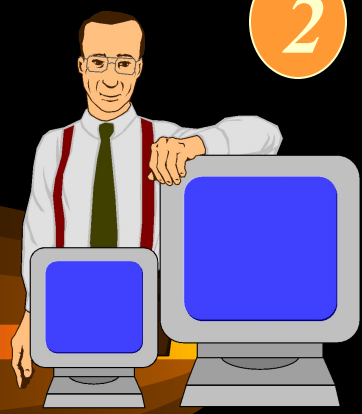
Лекция

Политика и модели безопасности в компьютерных системах



Учебные вопросы:

1. Понятие политики и моделей безопасности информации в компьютерных системах
2. Монитор (ядро) безопасности КС
3. Гарантирование выполнения политики безопасности. Изолированная программная среда

Политика безопасности организации

-совокупность руководящих принципов, правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности (ГОСТ Р ИСО/МЭК 15408)

Политика безопасности КС

-интегральная (качественная) характеристика, описывающая свойства, принципы и правила защищенности информации в КС в заданном пространстве угроз

Политика безопасности должна быть оформлена в виде специального документа (или комплекта документов), с которым должны быть ознакомлены все пользователи системы.

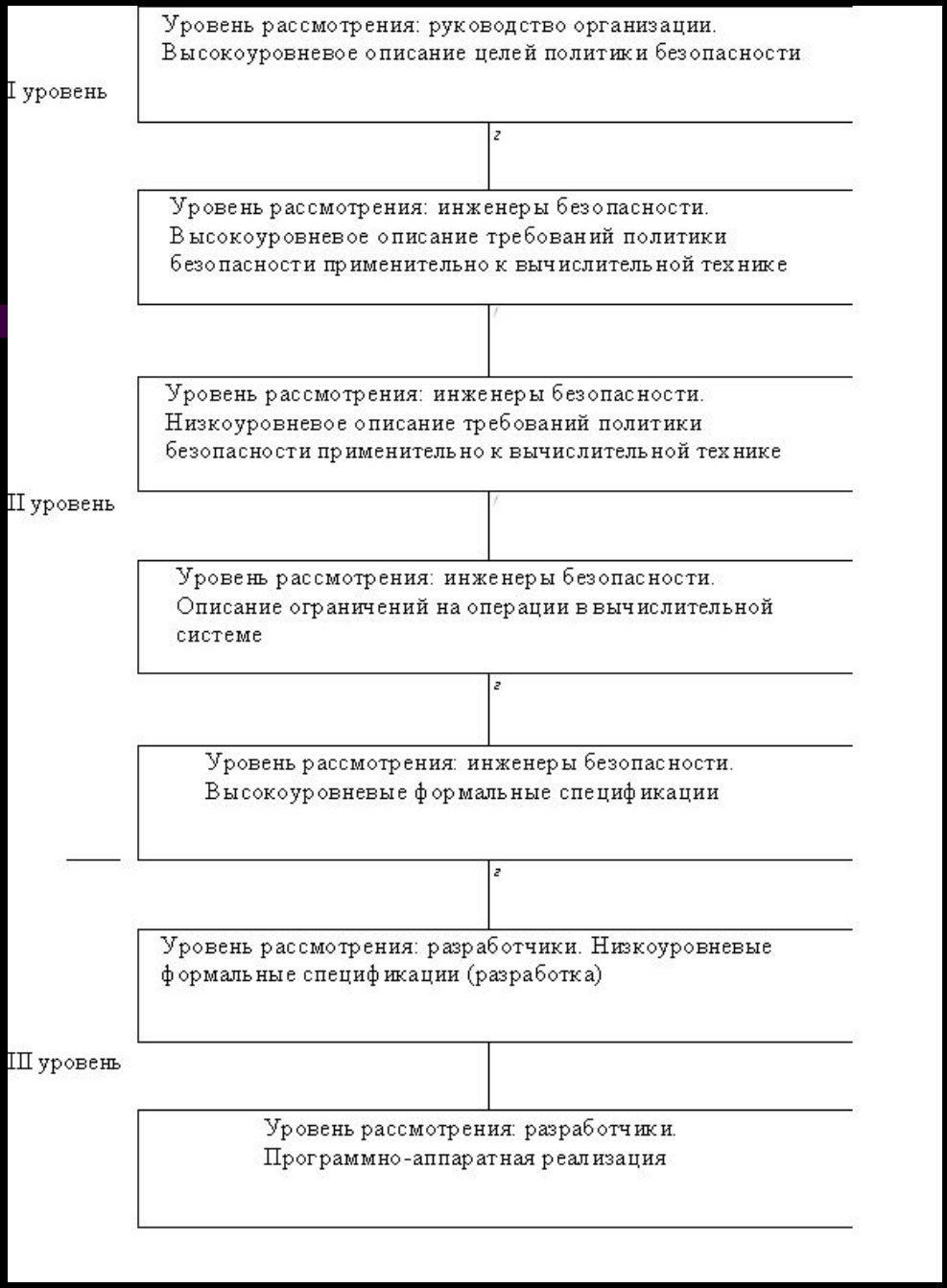
ПБ информирует пользователей о том, как правильно эксплуатировать систему

ПБ определяет множество механизмов безопасности, которые должны существовать в ИС

Процесс разработки политики безопасности

ПРИНЦИПЫ:

- невозможность миновать защитные средства;
- усиление самого слабого звена;
- недопустимость перехода в открытое состояние;
- минимизация привилегий;
- разделение обязанностей;
- многоуровневая защита;
- разнообразие защитных средств;
- простота и управляемость информационной системы;
- обеспечение всеобщей поддержки мер безопасности.



неформальное описания политики безопасности

Операция	*Конфиденциальная информация*	*Информация для служебного пользования*	*Общедоступная информация*
1	*2*	*3*	*4*
Создание документов	Пользователь, создающий информацию, отвечает за ее немедленную классификацию. Нежелательно присваивать информации классификацию сверх необходимости, так как это замедляет процессы в организации	Пользователь, создающий информацию, отвечает за ее немедленную классификацию. Нежелательно присваи вать информации классификацию сверх необходимости, так как это замедляет процессы в организации	Пользователь, создающий информацию, отвечает за ее немедленную классификацию. Нежелательно при сваивать информации классификацию сверх необходимости, так как это замедляет процессы в организации
Маркировка документов	Документ должен идентифицировать владельца и быть отмеченным как «Конфиденциально» на обложке или титульном листе	Нет специальных требований	Документ должен быть отмеченным как «Общедоступный» на обложке или титульном листе
Размножение документов	Осуществляется владельцем информации, определяющим полномочия доступа	Размножение только для деловых целей	Нет специальных требований

Операция	*Конфиденциальная информация*	*Информация для служебного пользования*	*Общедоступная информация*
Посылка документов по почте	Отсутствие классификации на внешнем конверте. Метка «Конфиденциально» на обложке или титульном листе. Подтверждение о получении по требованию владельца информации	Требования определяются владельцем информации	Нет специальных требований
Уничтожение документов	Владелец наблюдает за уничтожением документов и невозможностью их восстановления	Контролируется физи ческое разрушение	Нет специальных требований
Хранение документов	Заперты, если не используются	Оригинал охраняется от уничтожения	Оригинал охраняется от уничтожения
Доступ к доку менту	Владелец организует правила доступа к документу, обычно сильно ограниченные	Владелец организует правила доступа к документу, обычно широко доступные	Нет специальных требований. Обычно документы доступны внутри и вне организации
Рассмотрение уровня классификации документа	Владелец определяет дату пересмотра классификации документа(не реже раза в год)	Владелец пересматривает классификацию документа (не реже раза в год)	Нет специальных требований

Описание политики безопасности использования электронных коммуникаций организации **(Пример)**

1. Собственность. Под сообщениями электронных коммуникаций понимаются голосовая и электронная почта, а также факсы. Все сообщения, создаваемые и обрабатываемые с помощью электронных коммуникаций организации (включая резервные копии), принадлежат организации, а не пользователям электронных коммуникаций.
2. Авторизация. Система электронных коммуникаций организации может быть использована только в целях бизнеса. Личное использование электронных коммуникаций возможно, если оно:

занимает мало ресурсов;
не влияет на производительность труда;
не влияет на бизнес-процесс.

3. Минимальные привилегии. Пользователям должен быть дан минимум привилегий по использованию системы электронных коммуникаций, необходимых им для выполнения работы (например, рядовой пользователь не должен иметь прав изменять конфигурацию коммуникационного программного обеспечения).
4. Разделение пользователей. Система должна по возможности разделять деятельность разных пользователей, распознаваемых с помощью идентификаторов пользователей и паролей (это может быть затруднительно, например, для факсовых аппаратов).

5.Полномочия пользователей. Пользователи не должны разделять пароли или сообщения. При необходимости обмена полученными сообщениями следует использовать механизм распространения и другие авторизованные механизмы обмена информацией.

6.Отсутствие защиты по умолчанию. В системе не применяется шифрование сообщений по умолчанию. При пересылке чувствительной к раскрытию информации она должна быть зашифрована или защищена с помощью аналогичных шифрованию технологий.

7.Уважение права на тайну. За исключением специально оговоренных случаев, пользователи не могут вмешиваться в нормальную работу системы электронных коммуникаций с целью нарушения целостности или конфиденциальности сообщений. Компания уважает разумную конфиденциальность сообщений пользователей, организуя защиту системы электронных коммуникаций.

8.Отсутствие гарантий тайны сообщений. Компания не может гарантировать тайну сообщений. Пользователи должны быть осведомлены, что система электронных коммуникаций базируется на технологиях, которые не могут дать полной уве ренности в конфиденциальности информации. Более того, их сообщения в особых случаях (см. ниже) могут быть доступны другим пользователям.

9. Регулярный мониторинг сообщений. Содержимое сообщений не просматривается регулярно. Однако такой мониторинг может быть осуществлен в целях безопасности, поддержки функционирования бизнеса, а также при расследовании инцидентов. Пользователи должны быть проинформированы о возможности мониторинга.

10.Статистика. В организации собирается статистика по использованию системы электронных коммуникаций. На основании данной статистики можно сделать заключения, например, о доступности системы.
11.Раскрытие при происшествиях. Администратору системы может понадобиться просматривать содержимое сообщений при расследовании происшествий. При этом беспричинный просмотр содержимого сообщений запрещен.
12.Распространение сообщений. Вследствие того что некоторые виды информации предназначены для использования определенными пользователями, а не всеми пользователями системы, необходимо аккуратно распространять сообщения. Служебная информация организации не должна распространяться за пределы системы электронных коммуникаций организации без разрешения специального лица.
13.Удаление сообщений. Сообщения, необходимость которых для целей бизнеса исчерпана, должны периодически удаляться. По истечении определенного периода (обычно 6 месяцев) резервные копии сообщений удаляются. Если компания находится в особом режиме работы (например, вовлечена в судебный процесс), то сообщения могут удаляться только с разрешения специально оговоренного лица.
14.Запрещена посылка спама, в том числе рекламных сообщений, без получения предварительного запроса.
15.Запрещена подделка заголовков сообщений электронной почты.

Модель безопасности

-формальное (*математическое*, *алгоритмическое*, *схемотехническое* и т.п.) выражение политики безопасности

Модель безопасности служит для:

-выбора и обоснования базовых принципов архитектуры, определяющих механизмы реализации средств защиты информации

-подтверждения свойств (защищенности) разрабатываемой системы путем формального доказательства соблюдения политики (требований, условий, критериев) безопасности

-составления формальной спецификации политики безопасности разрабатываемой системы

Требования:

- адекватность;
- способность к предсказанию;
- общность.

1.Понятие политики и моделей безопасности информации в КС

Модель безопасности включает:

-модель компьютерной системы

-критерии, принципы или целевые функции защищенности и угроз

-формализованные правила, алгоритмы, механизмы безопасного функционирования КС

Большинство моделей КС относится к классу **моделей конечных состояний**

1. Компьютерная система – система, функционирующая в дискретном времени: $t_0, t_1, t_2, \ldots, t_k, \ldots$

В каждый следующий момент времени t_k КС переходит в новое состояние.

В результате функционирование КС представляет собой *детерминированный* или *случайный* **процесс**

- стационарность (временно́е поведение [количественных] параметров системы)
- эргодичность (поведение параметров системы по совокупность реализаций)
- марковость (память по параметрам системы)

2. Модели конечных состояний позволяют описать (спрогнозировать) состояние КС в момент времени $t_n, (n \geq 1)$, если известно состояние в момент t_0 и установлены некоторые правила (алгоритмы, ограничения) на переходы системы из состояния t_k в t_{k+1}

1.Понятие политики и моделей безопасности информации в КС

Большинство моделей конечных состояний представляет КС системой взаимодействующих сущностей двух типов субъектов и объектов (т.н. *субъектно-объектные модели КС*)

3. В каждый момент времени t_k КС представляется конечным множеством элементов, разделяемых на два подмножества:

-множество **субъектов - *S***

-множество **объектов – *O***

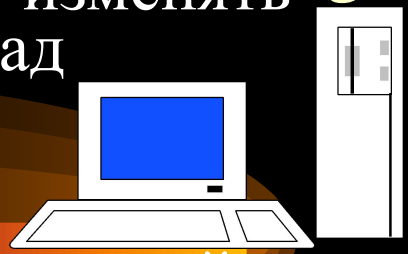
4. В каждый момент времени t_k субъекты могут порождать *процессы над объектами*, называемыми ***доступами***

Доступы субъектов к объектам порождают *информационные потоки*, переводящие КС в новое состояние t_{k+1}, в котором в т.ч. м. измениться декомпозиция КС на множество субъектов и множество объектов

Т.о. процесс функ-я КС нестационарный

1.Понятие политики и моделей безопасности информации в КС

Субъект -активная сущность КС, которая может изменять состояние системы через порождение процессов над объектами и, в т.ч., порождать новые объекты и инициализировать порождение новых субъектов

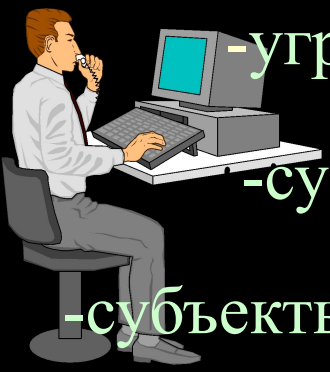


Объект -пассивная сущность КС, процессы над которой могут в определенных случаях быть источником порождения новых субъектов

Отличия пользователя от субъекта

Пользователь - лицо, внешний фактор, управляющий одним или несколькими субъектами, воспринимающий объекты и получающий информацию о состоянии КС через субъекты, которыми он управляет

Свойства субъектов:



-угрозы информации исходят от субъектов, изменяющих состояние объектов в КС

-субъекты-инициаторы могут порождать через объекты-источники новые объекты

-субъекты могут порождать потоки (передачу) информации от одних объектов к другим

1.Понятие политики и моделей безопасности информации в КС

Субъектно-объектная модель Щербакова

Множество объектов можно разделить на два непересекающихся подмножества
- объекты-источники;
- объекты-данные

Определение 1.Объект O_i называется ***источником*** для субъекта S_m если существует субъект S_j, в результате воздействия которого на объект O_i возникает субъект S_m

S_j – *активизирующий* субъект для субъекта S_m

S_m^j – *порожденный* субъект

$Create(S_j, O_i) \rightarrow S_m^j$

Функционирование КС – ***нестационарный*** процесс, но в субъектно-объектной модели КС действует ***дискретное время*** t_i. В любой момент времени t_i множество субъектов, объектов-источников, объектов-данных ***фиксировано!!!***

Определение 2.Объект в момент времени t_k ***ассоциирован*** с субъектом , если состояние объекта O_i повлияло на состояние субъекта S_m в след. момент времени t_{k+1}. (т.е. субъект S_m использует информацию, содержащуюся в объекте O_i).

Можно выделить: - множество ***функционально-ассоциированных объектов***

- множество ***ассоциированных объектов-данных*** с субъектом S_m в момент времени t_k

Следствие 2.1. В момент порождения объект-источник является ассоциированным с порожденным субъектом

1.Понятие политики и моделей безопасности информации в КС

Определение 3.***Потоком*** информации между объектом O_i и объектом O_j называется произвольная операция над объектом O_j, осуществляемая субъектом S_m, и зависящая от объекта O_i

$$Stream(S_m, O_i) \rightarrow O_j$$

– потоки информации м.б. только между объектами (а не между субъектом и объектом)

– объекты м.б. как ассоциированы, так и не ассоциированы с субъектом S_m

– операция порождения потока локализована в субъекте и сопровождается изменением состояния ассоциированных (отображающих субъект) объектов

– операция ***Stream*** может осуществляться в виде "*чтения*", "*записи*", "*уничтожения*", "*создания*" объекта

Определение 4.***Доступом*** субъекта к объекту O_j называется порождение субъектом S_m потока информации между объектом O_j и некоторым(и) объектом O_i (в т.ч., но не обязательно, объект O_i ассоциирован с субъектом S_m)

Будем считать, что все множество потоков информации P (объединение всех потоков во все t_k) разбито на два подмножества

- множество потоков P_L, характеризующих ***легальный доступ***
- множество потоков P_N, характеризующих ***несанкционированный доступ***

Определение 5.***Правила разграничения доступа***, задаваемые политикой безопасности, есть формально описанные потоки, принадлежащие множеству P_L.

Аксиомы защищенности компьютерных систем

Аксиома 1. В любой момент времени любой субъект, объект (процесс, файл, устройство) д.б. ***идентифициро-ваны*** и ***аутентифицированы***

Аксиома 2. В защищенной системе должна присутствовать активная компонента (субъект, процесс и объект-источник), осуществляющая *контроль процессов субъектов над объектами*

Аксиома 3. Для осуществления процессов субъектов над объектами необходима (должна существовать) *дополнительная информация* (и наличие содержащего ее объекта), помимо информации идентифицирующей субъекты и объекты

Аксиома 4. Все вопросы безопасности информации в КС описываются *доступами субъектов к объектам*

Аксиома 5. Субъекты в КС могут быть порождены только активной компонентой (субъектами же) из объектов

Аксиома 6. Система безопасна, если субъекты не имеют возможности нарушать (обходить) правила и ограничения ПБ

!!!Оси критерий безопасности

Политики безопасности компьютерных систем

Политика *избирательного* (*дискреционного*) доступа

- множество P_L задается явным образом внешним по отношению к системе фактором в виде указания дискретного набора троек "субъект-поток(операция)-объект"

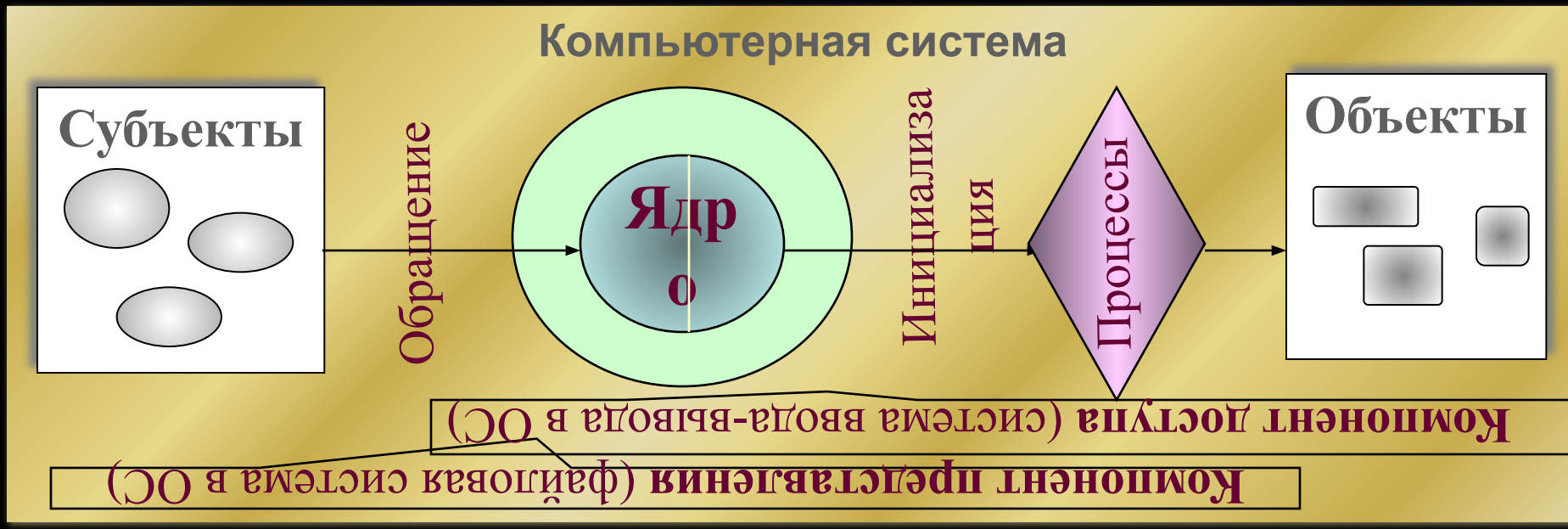
Политика *полномочного* (*мандатного*) доступа

- множество P_L задается неявным образом через предоставление субъектам неких полномочий (допуска, мандата) порождать определенные потоки над объектами с определенными характеристиками конфиденциальности (метками, грифами секретности)

Политика *ролевого* (*типизованного*) доступа

- множество P_L задается через введение в системе дополнительных абстрактных сущностей – ролей, с которыми ассоциируются конкретные пользователи, и наделение ролевых субъектов доступа на основе дискреционного или мандатного принципа правами доступа к объектам системы

Структура КС в программно-техническом аспекте

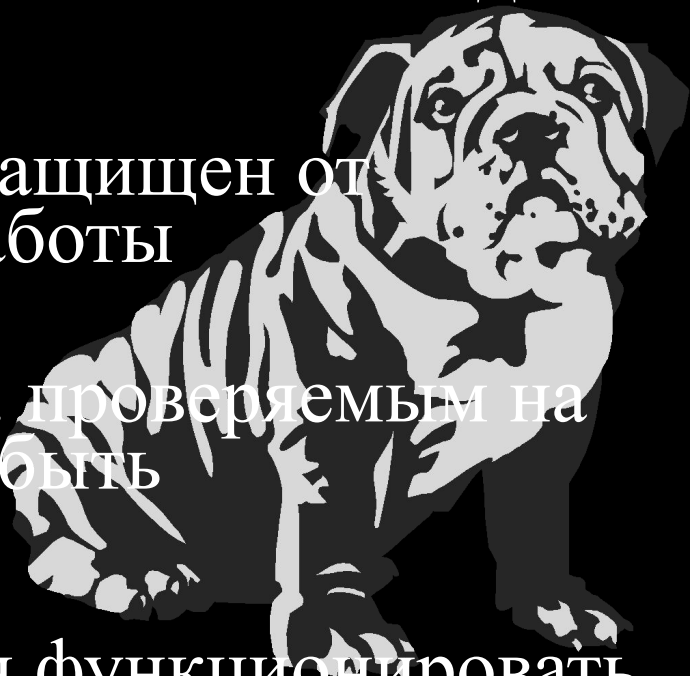


2. Монитор (ядро) безопасности КС

Монитор безопасности реализует политику безопасности на основе той или иной модели безопасности

Требования к монитору безопасности

Полнота - монитор должен вызываться при каждом обращении субъектов за сервисом к ядру системы и не д.б. никаких способов его обхода



Изолированность - монитор д.б. защищен от отслеживания и перехвата своей работы

Верифицируемость - монитор д.б. проверяемым на выполнение своих функций, т.е. быть тестируемым (самотестируемым)

Непрерывность - монитор должен функционировать при любых штатных и нештатных (в т.ч. и в аварийных) ситуациях

2. Монитор (ядро) безопасности КС

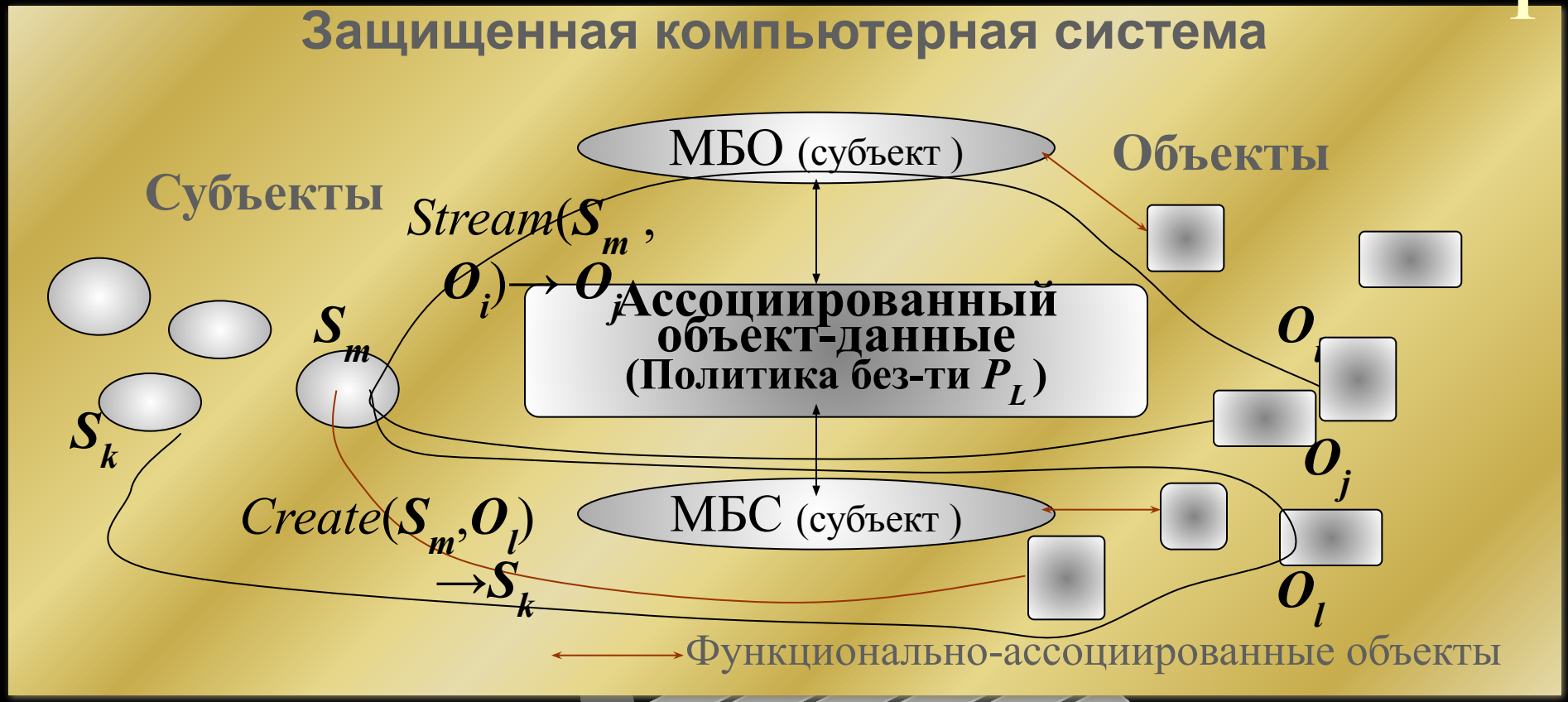
Особенности субъектно-объектной модели КС (определения 1, 2, 3 и 4) требуют структуризации монитора безопасности на две компоненты:

- **монитор безопасности объектов (*МБО*)**
- **монитор безопасности субъектов (*МБС*)**

Определение 6. ***Монитором безопасности объектов*** **(*МБО*)** называется субъект, активизирующийся при возникновении потока между любыми объектами, порождаемым любым субъектом, и разрешающий только те потоки, которые принадлежат множеству P_L

Определение 7. ***Монитором безопасности субъектов*** **(*МБС*)** называется субъект, активизирующийся при любом порождении субъектов, и разрешающий порождение субъектов только для фиксированного подмножества пар активизирующих субъектов и объектов-источников

2. Монитор (ядро) безопасности КС



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

3. Гарантирование выполнения политики безопасности. ИПС.

Исх. тезис -

при изменении объектов, функционально ассоциированных с субъектом монитора безопасности могут измениться свойства самого МБО и МБС, что м. привести к нарушению ПБ

Определение 8. Объекты O_i и O_j ***тождественны*** в момент времени t_k, если они совпадают как слова, записанные на одном языке

Определение 9. Субъекты S_i и S_j ***тождественны*** в момент времени t_k, если попарно тождественны все соответствующие ассоциированные с ними объекты

Следствие 9.1. Порожденные субъекты тождественны, если тождественны порождающие их субъекты и объекты-источники

Определение 10. 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

(Изменение состояние объекта – не тождественность в соотв. моменты времени)

3. Гарантирование выполнения политики безопасности. ИПС.

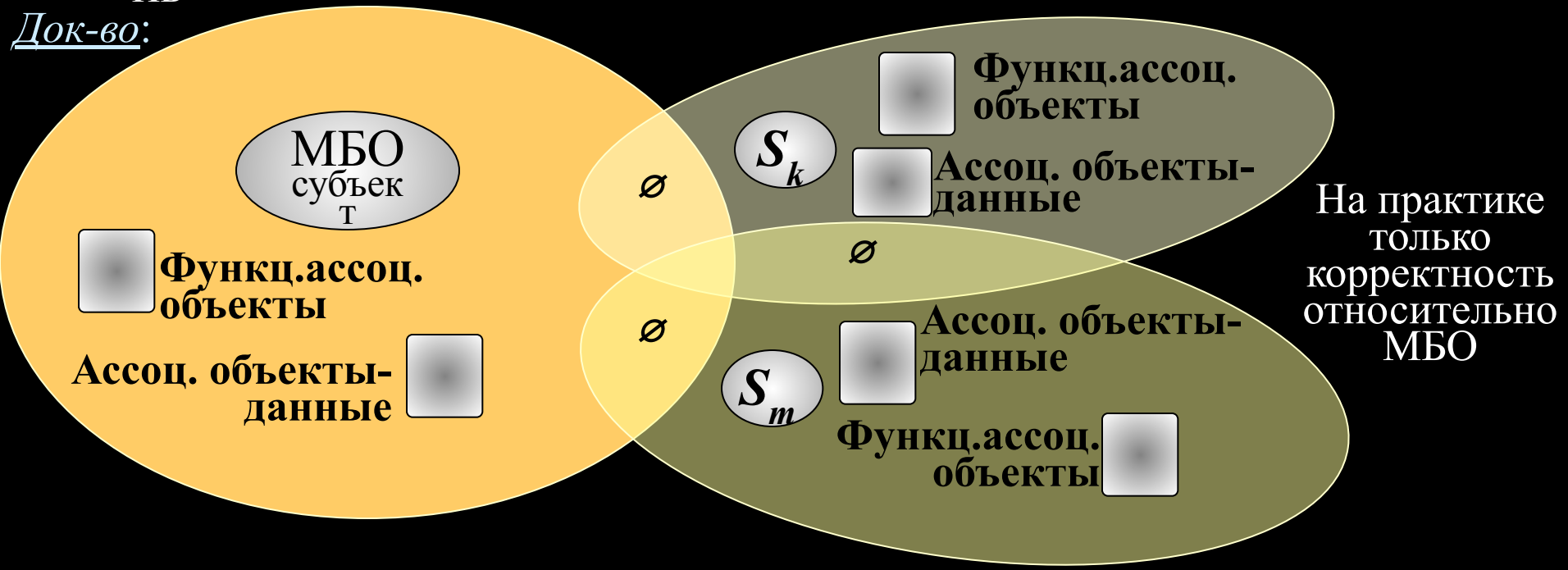
Определение 11. Субъекты S_i и S_j называются ***абсолютно невлияющими*** друг на друга (или ***абсолютно корректными*** относительно друг друга), если дополнительно к условию определения 10 множества ассоциированных объектов указанных субъектов не имеют пересечений

Утверждение 1. ПБ гарантированно выполняется в КС, если:

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

Достаточное условие гарантированного выполнения ПБ

Док-во:



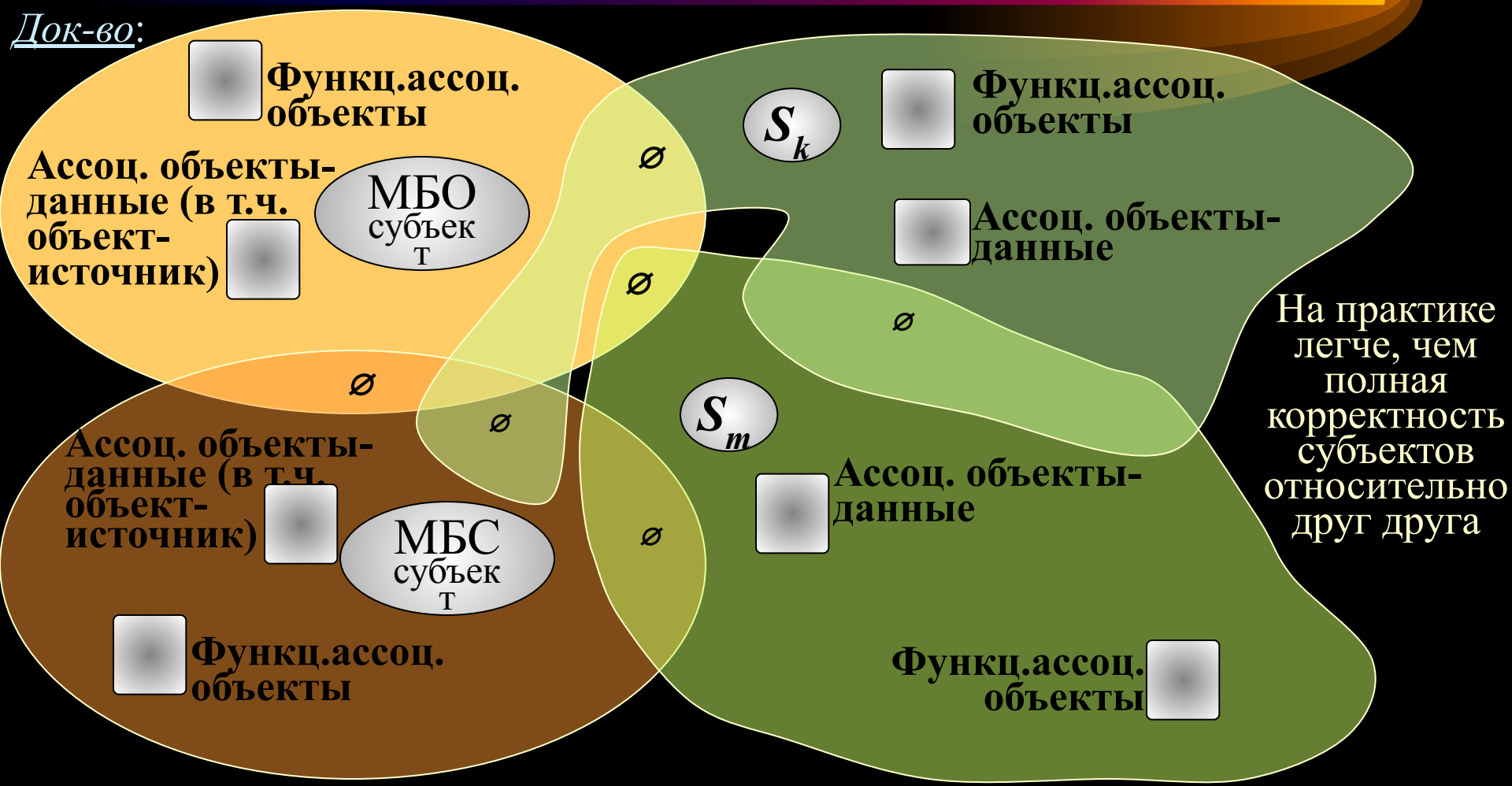
На практике только корректность относительно МБО

3. Гарантирование выполнения политики безопасности. ИПС.

Утверждение 2. Если в абсолютно изолированной КС существует МБО и порождаемые субъекты абсолютно корректны относительно МБО, а также МБС абсолютно корректен относительно МБО, то в КС реализуется доступ, описанный правилами разграничения доступа (ПБ)

Достаточное условие гарантированного выполнения ПБ

Док-во:



3. Гарантирование выполнения политики безопасности. ИПС.

Определение 12. КС называется ***замкнутой по порождению субъектов***, если в ней действует МБС, разрешающий порождение только фиксированного конечного подмножества субъектов для любых объектов-источников при фиксированной декомпозиции КС на субъекты и объекты

Определение 13. Множество субъектов КС называется ***изолированным (абсолютно изолированным)***, если в ней действует МБС и субъекты из порождаемого множества корректны (абсолютно корректны) относительно друг друга и МБС

Называют изолированной программной средой (ИПС)

Следствие 13.1. Любое подмножество субъектов изолированной (абсолютно изолированной) КС, включающее МБО и МБС, также составляет изолированную (абсолютно изолированную) программную среду

Следствие 13.2. Дополнение изолированной (абсолютно изолированной) КС субъектом, корректным (абсолютно корректным) относительно любого из числа входящих в ИПС субъектов, оставляет КС изолированной (абсолютно изолированной)

3. Гарантирование выполнения политики безопасности. ИПС.

Определение 16. Операция порождения субъекта $Create(S_i, O_j) \rightarrow S_m^6$ называется ***порождением с контролем неизменности объекта***, если для любого момента времени $t_k > t_0$, в который активизирована операция ***Create***, порождение субъекта S_m возможно только при тождественности объектов в соответствующие моменты времени – $O_i[t_k] = O_i[t_0]$

Следствие 16.1. При порождении с контролем неизменности объектов субъекты, порожденные в различные моменты времени, тождественны $S_m[t_1] = S_m[t_2]$. При $t_1 = t_2$ порождается один и тот же субъект.

Утверждение 3. Если в момент времени t_0 в изолированной КС действует только порождение субъектов с контролем неизменности объекта и существуют потоки между объектами через субъекты, не противоречащие условию корректности (абсолютной корректности) субъектов, то в любой момент времени КС также остается изолированной (абсолютно изолированной).

Базовая Теорема ИПС

Док-во: ***1.*** Из условия абс. корр. м.б. только такие потоки, которые изменяют состояние объектов, не ассоциированных в соотв. 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 нерасширяемо, и тем самым множество субъектов КС остается изолированным

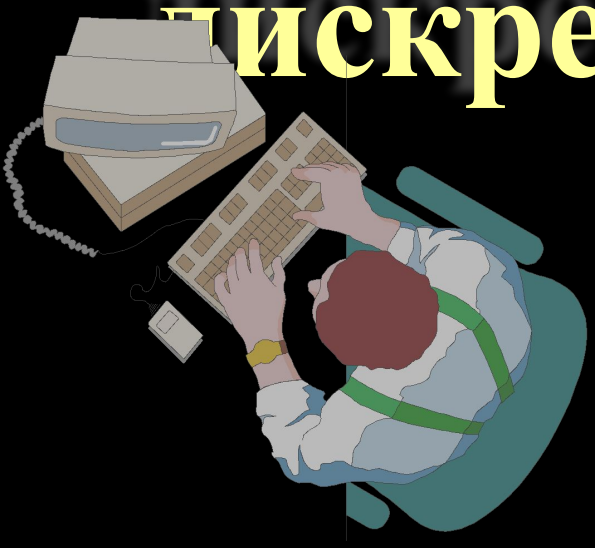
Проблемы реализации *Изолированной программной среды*

- 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***

Тема 2. Модели безопасности компьютерных систем

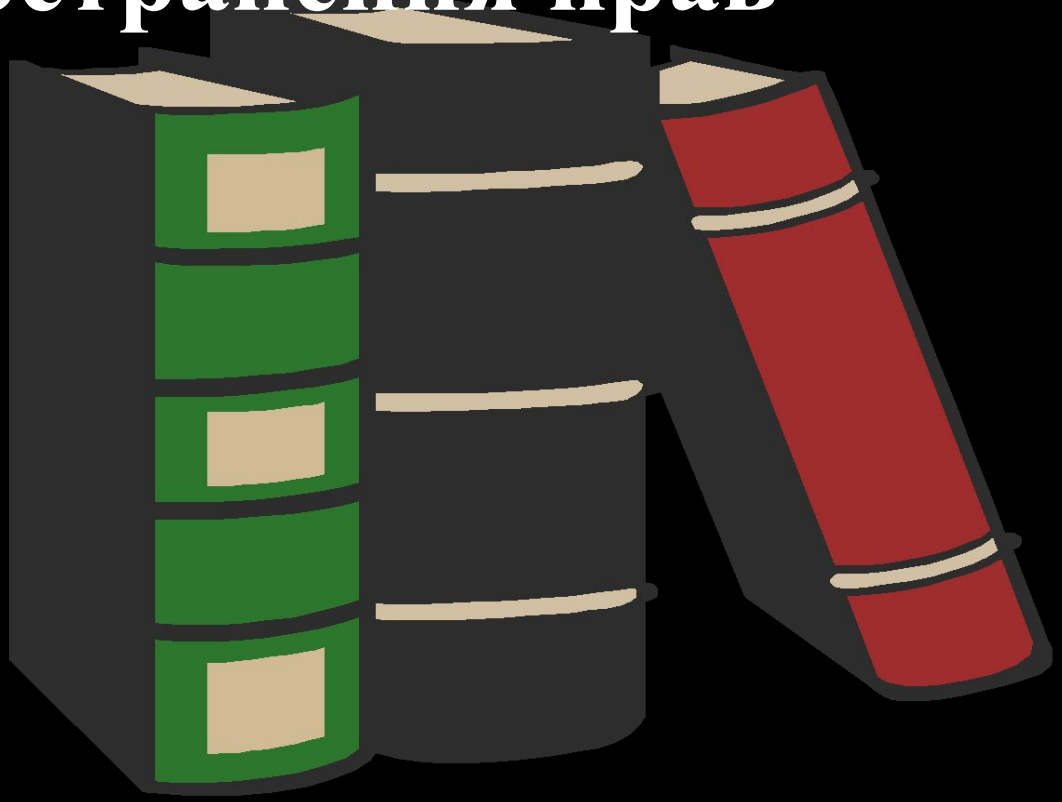
Лекция

Модели безопасности на основе дискреционной политики



Учебные вопросы:

1. Общая характеристика политики дискреционного доступа
2. Пятимерное пространство Хартсона
3. Модели на основе матрицы доступа
4. Модели распространения прав доступа



1. Общая характеристика политики дискреционного доступа

Исходные понятия

Разграничение доступа к информации (данным) КС

-разделение информации АИС на объекты (части, элементы, компоненты и т. д.), и организация такой системы работы с информацией, при которой пользователи имеют доступ только и только к той части информации (к тем данным), которая им необходима для выполнения своих функциональных обязанностей или необходима исходя из иных соображений

-создание такой системы организации данных, а также правил и механизмов обработки, хранения, циркуляции данных, которые обеспечивают функциональность КС и безопасность информации (ее конфиденциальность, целостность и доступность)

Доступ к информации (данным)

-действия субъектов на объектами КС, вызывающие одно- двунаправленные информационные потоки

Методы доступы

-виды действий (операций) субъектов над объектами КС (чтение/просмотр, запись/модификация/добавление, удаление, создание, запуск и т.п.)

Права доступа

-методы доступа (действия, операции), которыми обладают (наделяются, способны выполнять) субъекты над объектами КС

Политика (правила) разграничения доступа

-совокупность руководящих принципов и правил наделения субъектов КС правами доступа к объектам, а также правил и механизмов осуществления самих доступов и реализации информационных потоков

1. Общая характеристика политики дискреционного доступа

Виды политик (правил, механизмов) разграничения доступа

Политика дискреционного разграничения доступа

-разграничение доступа на основе *непосредственного* и *явного предоставления* субъектам *прав* доступа к объектам в виде троек «субъект-операция-объект»

Политика мандатного разграничения доступа

-предоставление прав доступа субъектов к объектам *неявным образом* посредством присвоения уровней (меток) безопасности объектам (*гриф конфиденциальности, уровень целостности*), субъектам (*уровень допуска/полномочий*) и организация доступа на основе соотношения «уровень безопасности субъекта-операция-уровень безопасности объекта»

Политика тематического разграничения доступа

-предоставление прав доступа субъектам к объектам *неявным образом* посредством присвоения тематических категорий объектам (*тематические индексы*) и субъектам (*тематические полномочия*) и организация доступа на основе соотношения «тематическая категория субъекта-операция-тематическая категория объекта»

Политика ролевого разграничения доступа

-агрегирование прав доступа к объектам в именованные совокупности (роли), имеющие определенный функционально-технологический смысл в предметной области КС, и наделение пользователей правом работы в КС в соответствующих ролях

Политика временно́го разграничения доступа

-предоставление пользователям прав работы в КС по определенному временному регламенту (по времени и длительность доступа)

Политика маршрутного доступа

-предоставление пользователям прав работы в КС при доступе по определенному маршруту (*с определенных рабочих станций*)

Общая характеристика политики дискреционного доступа

-множество легальных (неопасных) доступов P_L задается явным образом внешним по отношению к системе факторов в виде указания дискретного набора троек "субъект-поток(операция)-объект";

-права доступа предоставляются (*«прописываются» в специальных информационных объектах-стуктурах, ассоциированных с монитором безопасности*), отдельно каждому пользователю к тем объектам, которые ему необходимы для работы в КС;

-при запросе субъекта на доступ к объекту монитор безопасности, обращаясь к ассоциированным с ним информационным объектам, в которых «прописана» политика разграничения доступа, определяет «легальность» запрашиваемого доступа и разрешает/отвергает доступ

Модели и механизмы реализации дискреционного разграничения доступа

Различаются:

-в зависимости от принципов и механизмов программно-информационной структуры объекта(объектов), ассоциированных с монитором безопасности, в которых хранятся «прописанные» права доступа (тройки доступа)

-в зависимости от принципа управления правами доступа, т.е. в зависимости от того – кто и как заполняет/изменяет ячейки матрицы доступа (принудительный и добровольный принцип управления доступом)

Выделяют:

-теоретико-множественные (реляционные) модели разграничения доступа (пятимерное пространство Хартсона, модели на основе матрицы доступа)

-модели распространения прав доступа (модель Харисона-Рузо-Ульмана, модел типизованной матрицы доступа, теоретико-графовая модель TAKE-GRANT)

2. Пятимерное пространство Хартсона

Система защиты -пятимерное пространство на основе следующих множеств:

U - множество пользователей;
R - множество ресурсов;
E - множество операций над ресурсами;
S - множество состояний системы;
A - множество установленных полномочий.

Элементы множества ***A - a_{ijkl}*** специфицируют:
- ресурсы
- вхождение пользователей в группы;
- разрешенные операции для групп по отношению к ресурсам;

Декартово произведение ***A×U×E×R×S*** - область безопасного доступа

Запрос пользователя на доступ представляет собой *4-х мерный кортеж*: ***q = (u,e,R',s),*** где ***R'*** - требуемый набор ресурсов

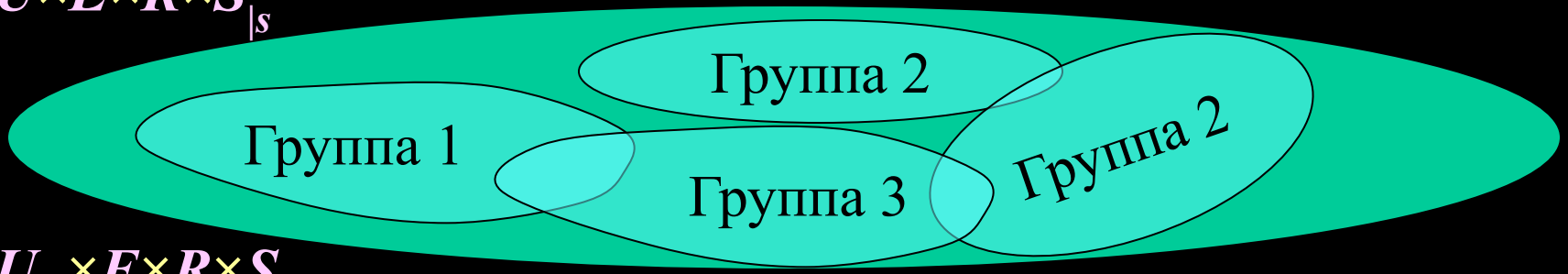
Процесс организации доступа по запросу осуществляется по следующему алгоритму:

*1.*Вызвать все вспомогательные программы для предварительного принятия решения

*2.*Определить те группы пользователей, в которые входит ***u***, и выбрать из ***A*** те спецификации полномочий ***P=F(u)***, которым соответствуют выделенные группы пользователей. Набор полномочий ***P=F(u)*** определяет т.н.**привилегию пользователя**

2. Пятимерное пространство Хартсона

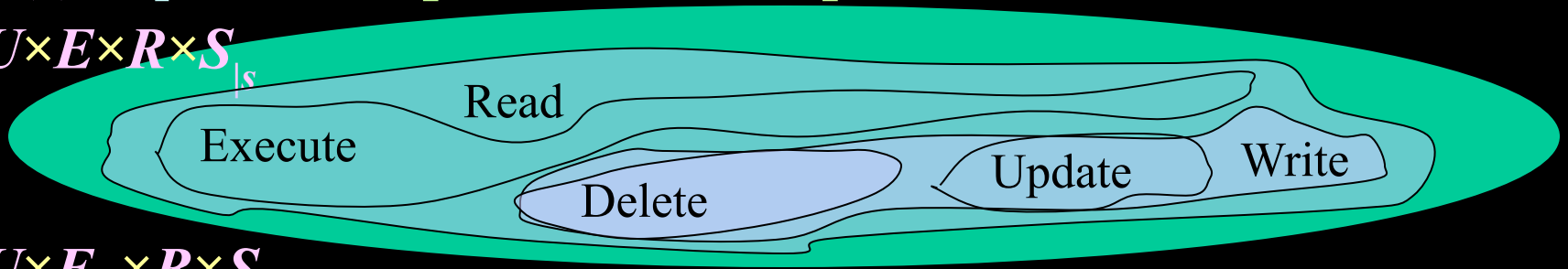
$A \times U \times E \times R \times S_{|s}$



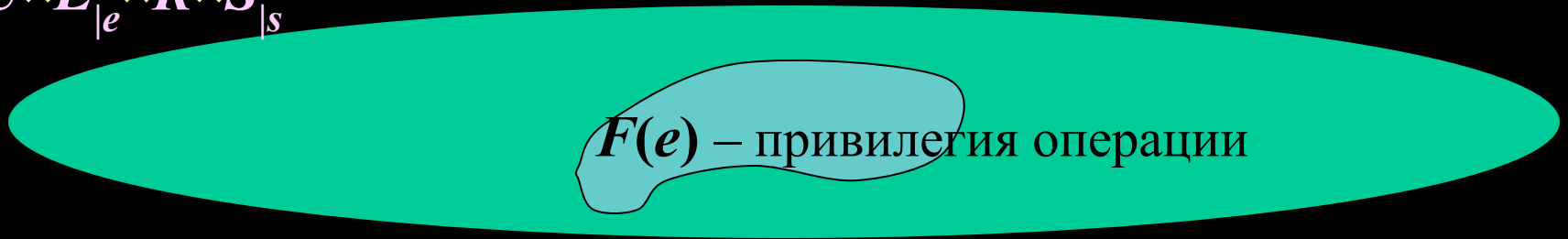
$A \times U_{|u} \times E \times R \times S_{|s}$

3. Определить из множества *A* набор полномочий ***P=F(e)***, которые устанавливают ***e***, как основную операцию. Набор полномочий ***P=F(e)*** определяет **привилегию операции**.

$A \times U \times E \times R \times S_{|s}$



$A \times U \times E_{|e} \times R \times S_{|s}$



2. Пятимерное пространство Хартсона

4. Определить из множества *A* набор полномочий ***P=F(R')***, разрешающих доступ к набору ресурсов ***R'***. Набор полномочий ***P=F(R')*** определяет **привилегию ресурсов**.

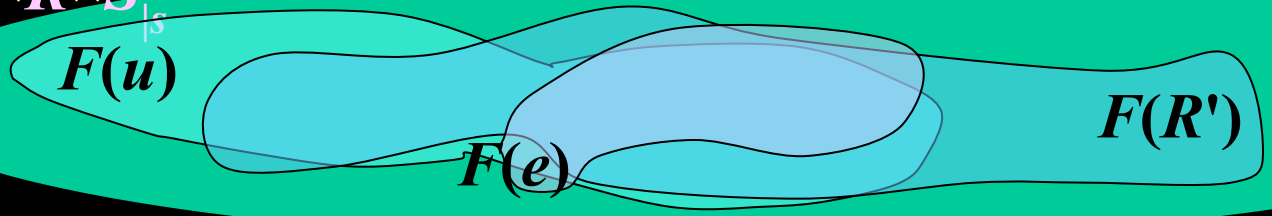
$A \times U \times E \times R_{|R'} \times S_{|S}$

F(R') – привилегия запрашиваемых ресурсов

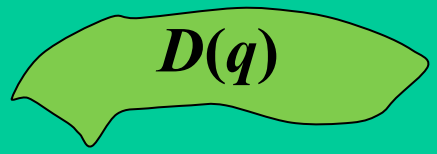
На основе ***P=F(u)***, ***P=F(e)*** и ***P=F(R')*** образуется т.н. **домен полномочий запроса**:

$$D(q) = F(u) \cap F(e) \cap P = F(R')$$

$A \times U \times E \times R \times S_{|S}$



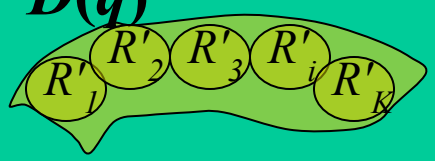
$A \times U_{|u} \times E_{|e} \times R_{|R'} \times S_{|S}$



2. Пятимерное пространство Хартсона

5. Убедиться, что запрашиваемый набор ресурсов R' полностью содержится в домене запроса $D(q)$, т.е. любой r из набора R' хотя бы один раз присутствует среди элементов $D(q)$.

$A \times U_{|u} \times E_{|e} \times R_{|R'} \times S_{|s}$



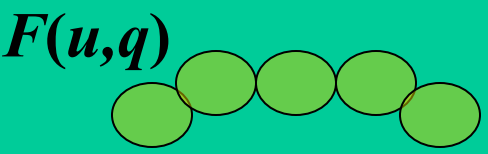
6. Осуществить разбиение $D(q)$ на эквивалентные классы, так, чтобы в один класс попадали полномочия (элементы $D(q)$), когда они специфицируют один и тот же ресурс r из набора R'.

В каждом классе произвести операцию логического **ИЛИ** элементов $D(q)$ с учетом типа операции e.

В результате формируется новый набор полномочий на каж-дую единицу ресурса, указанного в $D(q)$ - $F(u,q)$.Набор $F(u,q)$ назы-вается **привилегией пользователя** u **по отношению к запросу** q.

авторизаци

$A \times U_{|u} \times E_{|e} \times R_{|R'} \times S_{|s}$



2. Пятимерное пространство Хартсона

7. Вычислить условие фактического доступа (*EAC*), соответствующее запросу *q* , через операции логического **ИЛИ** по элементам полномочий *F(u,q)* и запрашиваемым ресурсам *r* из набора *R'*, и получить тем самым набор *R''* - набор фактически доступных по запросу ресурсов

8. Оценить *EAC* и принять решение о доступе:
- разрешить доступ, если *R''* и *R'* полностью перекрываются;
- отказать в доступе в противном случае.

9. Произвести запись необходимых событий

10. Вызвать все программы, необходимые для организации доступа после "принятия решения".

11. Выполнить все вспомогательные программы, вытекающие для каждого случая по п.8.

12. При положительном решении о доступе завершить физическую обработку.

Но!!! Безопасность системы в строгом смысле не доказана

3. Модели на основе матрицы доступа

Система защиты -совокупность следующих множеств:

- множество исходных объектов $O\ (o_1,o_2,\ldots,o_M)$
- множество исходных субъектов $S\ (s_1,s_2,\ldots,s_N)$, при этом $S \subseteq O$
- множество операций (действий) над объектами $Op\ (Op_1,Op_2,\ldots,Op_L)$
- множество прав, которые м.б. даны субъектам по отношению к объектам $R\ (r_1,r_2,\ldots,r_K)$ – т.н. "общие права"
- NxM матрица доступа A, в которой каждому ***субъекту*** соответствует *строка*, а каждому ***объекту*** - ***столбец***. В ячейках матрицы располагаются права r соотв.субъекта над соотв. объектом в виде набора разрешенных операций Op_i

$A=$

Субъекты \ Объекты	o_1	o_2	. . .			o_M
s_1						
s_2						
				a_{ij}		
s_N						

$A[s_i,oj]= a_{ij}$ - право r из R (т. е. не общее, а конкр. право)

Каждый элемент прав r_k специфицирует совокупность операций над объектом

$r_k \sim (Op_{1k},Op_{2k},\ldots,Op_{Jk})$

3. Модели на основе матрицы доступа

Две разновидности моделей в зависимости от того, каким образом заполняются ячейки матрицы доступа *A*. Выделяют:

- ***системы с принудительным управлением доступа;***
- ***системы с добровольным управлением доступом.***

Принудительное управление доступом

- вводится т.н. доверенный субъект (администратор доступа), который и определяет доступ субъектов к объектам (централизованный принцип управления)
- в таких системах заполнять и изменять ячейки матрицы доступа может только администратор

Добровольное управление доступом

- вводится т.н. владение (владельцы) объектами и доступ субъектов к объекту определяется по усмотрению владельца (децентрализованный принцип управления)
- в таких системах субъекты посредством запросов могут изменять состояние матрицы доступа

3. Модели на основе матрицы доступа

Способы организации информационной структуры матрицы доступа

Централизованная единая информационная структура

Децентрализованная распределенная информационная структура

СУБД

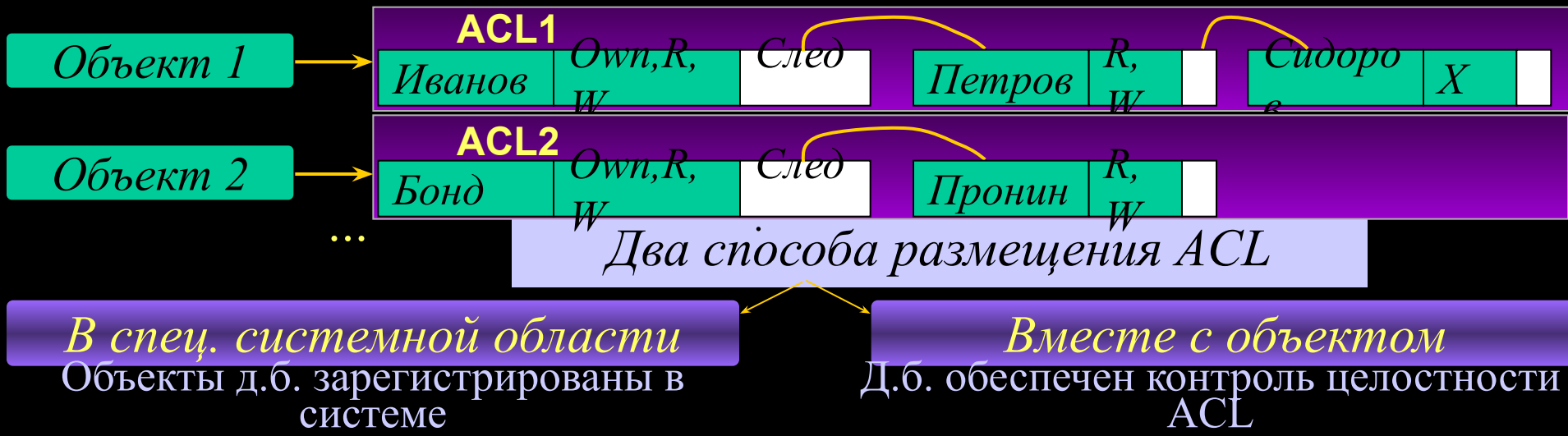
системная таблица с назначениями доступа

Биты защиты (UNIX)

	Владелец			*Группа*			*Остальные польз-ли*		
	Чтен ие	*Запис ь*	*Выпол нение*	*Чтен ие*	*Запис ь*	*Выпол нение*	*Чтен ие*	*Запис ь*	*Выпол нение*
Биты	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
Объект									
Объект 2	1	1	0	1	1	0	1	0	0
…	1	1	1	1	0	1	0	0	0

3. Модели на основе матрицы доступа

Списки доступа в файловой системе ОС Windows (Access Control List – ACL)



Структура списков доступа на примере NTFS

С каждым объектом *NTFS* связан т.н. дескриптор защиты, состоящий из:

ID влад.	*ID перв. гр. влад.*	*DACL*	*SACL*

Список дискр. контроля доступа

список контроля доступа

DACL – последовательность произв. кол-ва *элементов контроля доступа – ACE, вида:*

Allowed / Denied	*ID субъекта (польз., группа)*	*Права доступа (отображ-е)*	*Флаги, атрибуты*

SACL – данные для генерации сообщений аудита

4.Модели распространения прав доступа. 4.1.Модель Харрисона-Руззо-Ульмана (модель HRU)

Наиболее типичный представитель систем с добровольным управлением доступом - ***модель Харрисона-Руззо-Ульмана***

Разработана для исследования дискреционной политики

В модели ***Харрисона-Руззо-Ульмана*** помимо элементарных операций доступа ***Read***, ***Write*** и т.д., вводятся также т.н. **прими-тивные операции** Op_k по ***изменению*** субъектами матрицы доступа:

- ***Enter r into (s,o)*** - ввести право ***r*** в ячейку ***(s,o)***
- ***Delete r from (s,o)*** - удалить право ***r*** из ячейки ***(s,o)***
- ***Create subject s*** - создать субъект ***s*** (т.е. новую строку матрицы ***A***)
- ***Create object o*** - создать объект ***o*** (т.е. новый столбец матрицы ***A***)
- ***Destroy subject s*** - уничтожить субъект ***s***
- ***Destroy object o*** - уничтожить объект ***o***

Состояние системы *Q* изменяется при выполнении команд $C(\alpha_1, \alpha_2, \ldots)$, изменяющих состояние матрицы доступа *A*. Команды инициируются пользователями-субъектами

Структура команды

Название
[Условия] (необяз.)
Операции

Command $\alpha(x_1, \ldots x_k)$
if r_1 in $A[s_1,o_1]$ and r_2 in $A[s_2,o_2]$ …
then; Op_2 ; …;
end

x_i – идентификаторы задействованных субъектов или объектов

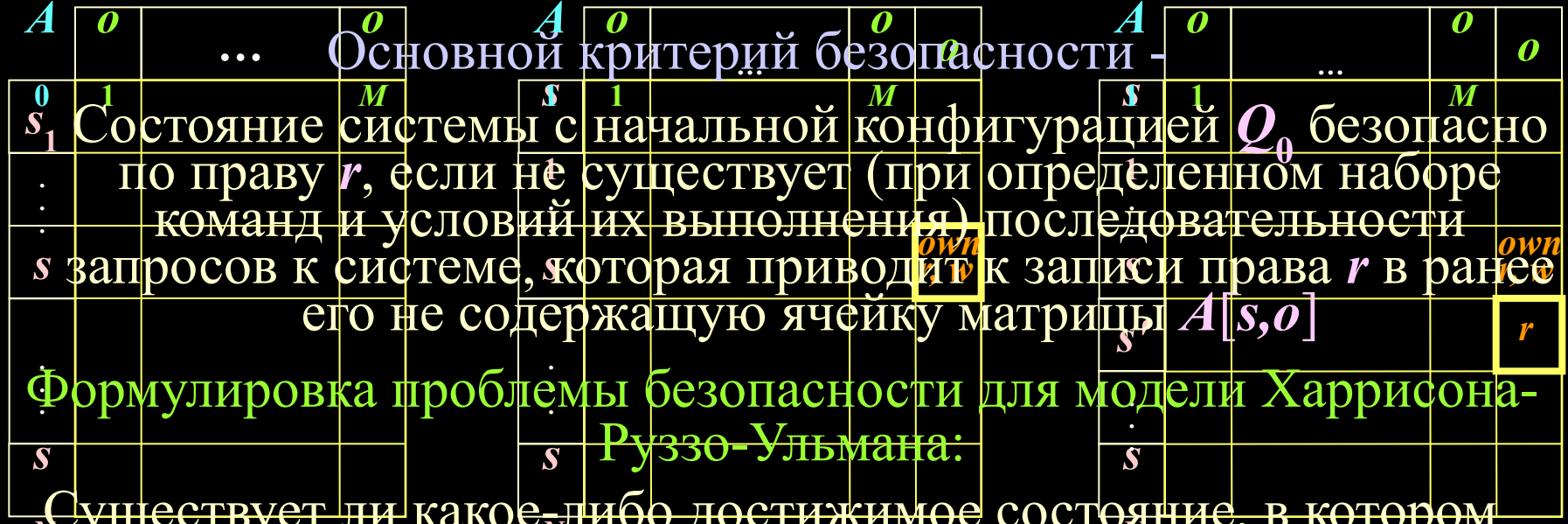
Команды с одной операцией – **монооперационные**, с одним условием - **моноусловные**

4. Модели распространения прав доступа. 4.1. Модель Харрисона-Руззо-Ульмана (модель HRU)

Примеры команд -

Command "создать файл"(*s, f*):
Create object f ;
Enter "own" into (*s, f*) ;
Enter "read" into (*s, f*) ;
Enter "write" into (*s, f*);
end

Command «ввести право чтения"(*s,s',f*):
if *own* ⊆ (*s, f*) ;
then
Enter r "read" into (*s', f*) ;
end



Основной критерий безопасности - Состояние системы с начальной конфигурацией Q_0 безопасно по праву *r*, если не существует (при определенном наборе команд и условий их выполнения) последовательности *s* запросов к системе, которая приводит к записи права *r* в ранее его не содержащую ячейку матрицы *A*[*s,o*]

Формулировка проблемы безопасности для модели Харрисона-Руззо-Ульмана:

Существует ли какое-либо достижимое состояние, в котором конкретный субъект обладает конкретным правом доступа к конкретному объекту? (т.е. всегда ли возможно построить такую последовательность запросов при некоторой исходной конфигурации когда изначально субъект этим правом не обладает?)

4.Модели распространения прав доступа. 4.1.Модель Харрисона-Руззо-Ульмана (модель HRU)

Харрисон, Руззо и Ульман показали :

Теорема 1. Проблема безопасности разрешима для ***моно-операционных*** систем, т.е. для систем которых запросы содержат лишь одну примитивную операцию

Док-во на основе моделирования системы машиной Тьюринга

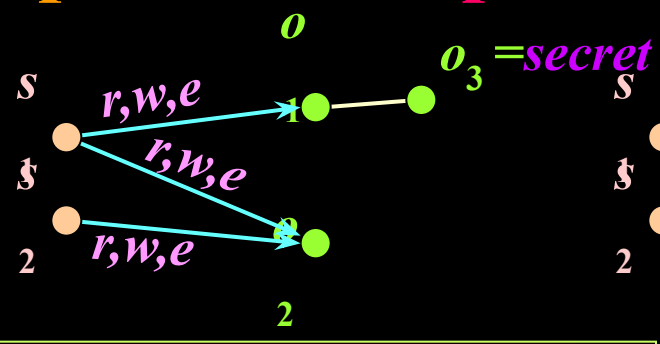
Теорема 2. Проблема безопасности неразрешима в общем случае

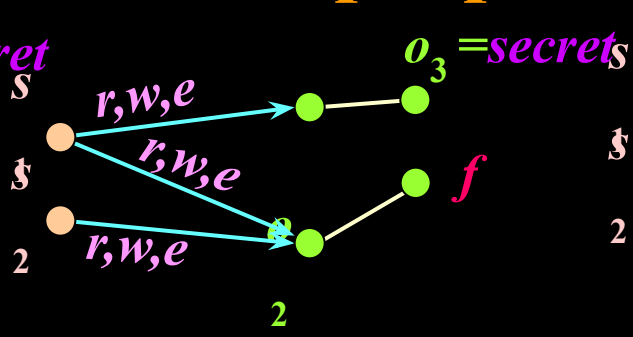
Выводы по модели Харрисона-Руззо-Ульмана:

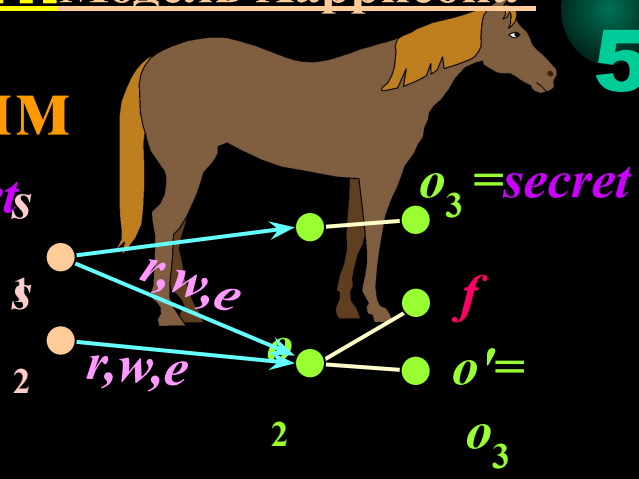
-данная модель в ее полном виде позволяет реализовать множество политик безопасности, но при этом проблема безопасности становится неразрешимой

-разрешимость проблемы безопасности только для монооперационных систем приводит к слабости такой модели для реализации большинства политик безопасности (т.к. нет операции автоматического наделения своими правами дочерних объектов, ввиду чего по правам доступа они изначально не различимы)

Проблема «троянских» программ



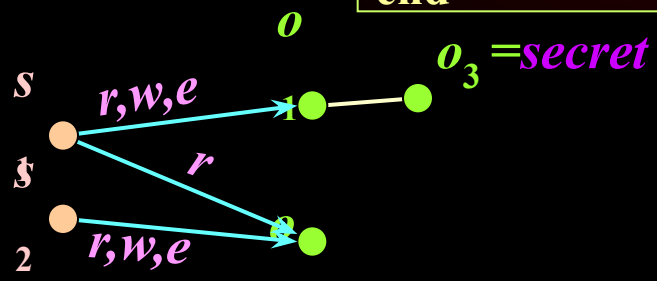




Command "создать файл" (s_2,*f*):
 if *write* ∈ [s_2, o_2] ;
 then
  Create object f ;
  Enter "read" into [s_2, *f*] ;
  Enter "write" into [s_2, *f*] ;
  Enter "execute" into [s_2, *f*];
 if *read* ∈ [s_1, o_2] ;
  then
  Enter "read" into [s_1, *f*] ;
 if *write* ∈ [s_1, o_2] ;
  then
  Enter "write" into [s_1, *f*] ;
 if *execute* ∈ [s_1, o_2] ;
  then
  Enter "execute" into [s_1, *f*] ;
end

Command "запустить файл"(s_1, *f*):
 if *execute* ∈ [s_1, *f*] ;
  then
  Create subject f ' ;
  Enter "read" into [*f '*,o_1];
  Enter "read" into [*f '*,o_3];
 if *write* ∈ [s_1,o_2] ;
  then
  Enter "write" into [*f'*,o_2];
end

Command "скопировать файл o_3 программой *f '* в o_2" (*f '*,o_3, o_2):
  if *read* ∈ [*f '*, o_3] and
   write ∈ [*f '*, o_2]
  then
   Create object o';
   Write (*f '*, o_3 , *o'*);
  if *read* ∈ [s_2, o_2] ;
  then
   Enter "read" into [s_2,*o'*];
end



Расширения модели HRU

Типизованная матрица доступа (Модель TAM) R. Sandhu,1992г.

Вводится фиксированное количество типов τ_k (например, "user"- пользователь, 'so"-офицер безопасности и "file"), которым могут соответствовать сущности КС (субъекты и объекты).

Command $\alpha(x_1:\tau_1, x_2:\tau_2,\ldots, x_k: \tau_k)$

Накладываются ограничения на условия и соответствие типов в монотонных операциях (порождающие сущности)

Смягчаются условия на разрешимость проблемы безопасности

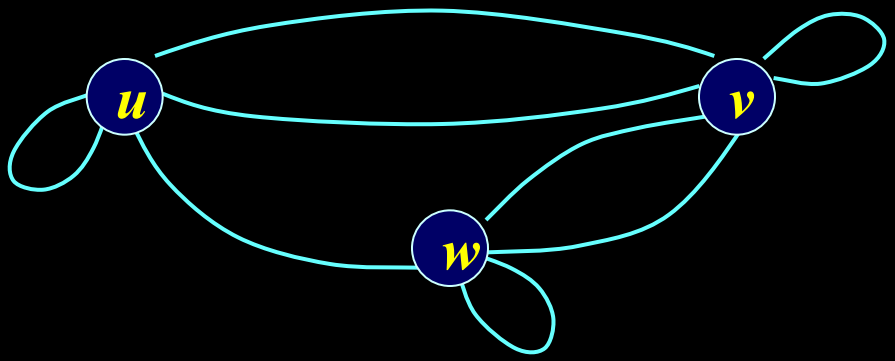
Анализ проблем безопасности в модели TAM основывается на понятии родительских и дочерних типов

Определение 1. *Тип τ_k является **дочерним** типом в команде создания $\alpha(x_1:\tau_1, x_2:\tau_2,\ldots, x_k:\tau_k)$, если и только если имеет место один из следующих элементарных операторов: **"Create subject x_k of type τ_k"** или **"Create object x_k of type τ_k"**. В противном случае тип τ_k является **родительским** типом.*

Вводится **Граф** отношений наследственности

4.Модели распространения прав доступа. 4.2.Модель типизованной матрицы доступа (модель TAM)

Пусть имеется три типа *u*, *v*, *w*



Функционирование системы осуществляется через последовательность следующих команд:

0-й шаг – в системе имеется субъект типа *u* - $(s_1:u)$

1-й шаг. $\alpha(s_1:u, s_2:w, o_1:v)$:
Create object o_1 *of type v* ;
Inter r into $[s_1, o_1]$;
Create subject s_2 *of type w* ;
Inter r' into $[s_2, o_1]$;
end

2-й шаг. $\alpha(s_3:u, o_1:v)$:
Create subject s_3 *of type u* ;
Inter r'' into $[s_3, o_1]$;
end

v – дочерний тип в команде **α**, в теле которой имеются еще типы *u*, *w*. Т. о. в **Графе отношений наследственности** возникают дуги (*u*,*v*), (*w*,*v*) и в т.ч. (*v*,*v*)

w – дочерний тип в команде **α**, в теле которой имеются еще типы *u*, *v*. Т. о. в **Графе отношений наследственности** возникают дуги (*u*,*w*), (*v*,*w*) и в т.ч. (*w*,*w*)

u – дочерний тип в команде **α**, в теле которой имеются еще тип *v*. Т.о. возникают дуги (*v*,*u*) и в т.ч. (*u*,*u*)

4.Модели распространения прав доступа. 4.2.Модель типизованной матрицы доступа (модель TAM)

Также, как и в модели **HRU**, используется понятие монотонной (**MTAM**) системы, которая не содержит примитивных операторов ***Delete*** и ***Destroy***.

Определение 2. *Реализация **MTAM** является **ациклличной** тогда и только тогда, когда ее граф отношений наследственности не содержит циклов*

Теорема 3. Проблема безопасности разрешима для ***ациклличных реализаций MTAM***

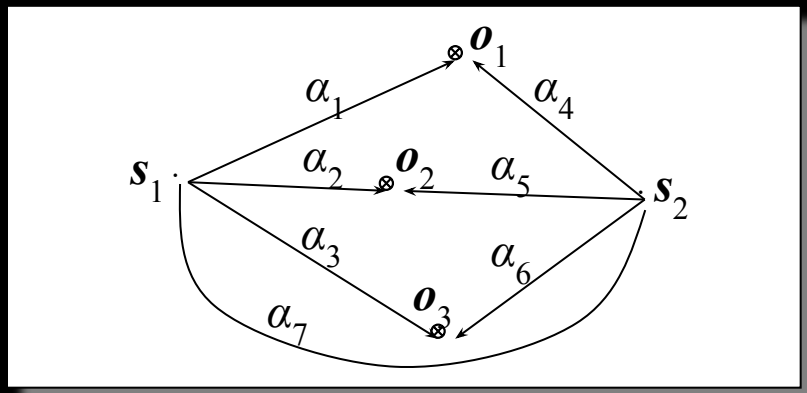
Джонс, Липтон, Шнайдер, 1976г.

Теоретико-графовая модель анализа распространения прав доступа в дискреционных системах на основе матрицы доступа

1.Также как и в модели HRU **система защиты** представляет совокупность следующих множеств:

- множество исходных объектов $O\ (o_1,o_2,\ldots,o_M)$
- множество исходных субъектов $S\ (s_1,s_2,\ldots,s_N)$, при этом $S \subseteq O$
- множество прав, которые м.б. даны субъектам по отношению к объектам $(r_1,r_2,\ldots,r_K) \cup \{t, g\}$, в том числе с двумя специфическими правами – правом ***take*** (t – *право брать права доступа у какого-либо объекта по отношению к другому объекту*) и правом ***grant*** (g – *право предоставлять права доступа к определенному объекту другому субъекту*)

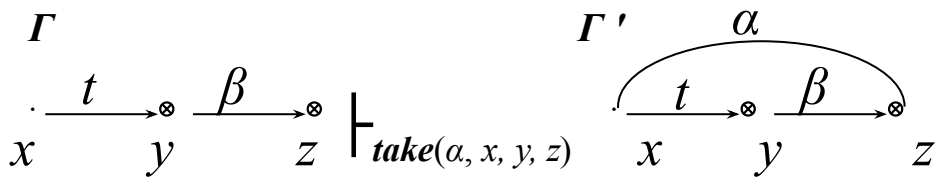
-множеством E установленных прав доступа (x, y, α) субъекта x к объекту y с правом α из конечного набора прав. При этом состояние системы представляется **Графом доступов** Γ



4.Модели распространения прав доступа. 4.4.Теоретико-графовая модель TAKE-GRANT

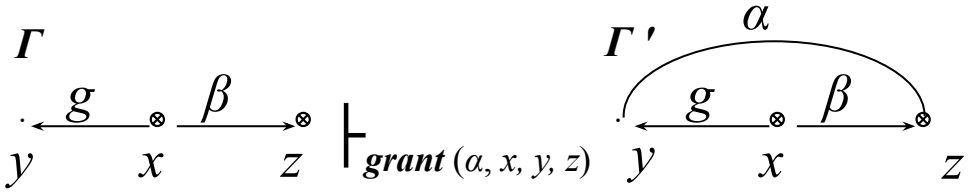
2.Состояние системы (**Графа доступов**) изменяется под воздействием элементарных команд 4-х видов

Команда "*Брать*" – *take*(*α, x, y, z*)



субъект ***x*** берет права доступа $\alpha \subseteq \beta$ на объект ***z*** у объекта ***y*** (обозначения: $\vdash_c$ – переход графа ***Г*** в новое состояние ***Г'*** по команде ***c*** ; $x \in S$; $y, z \in O$)

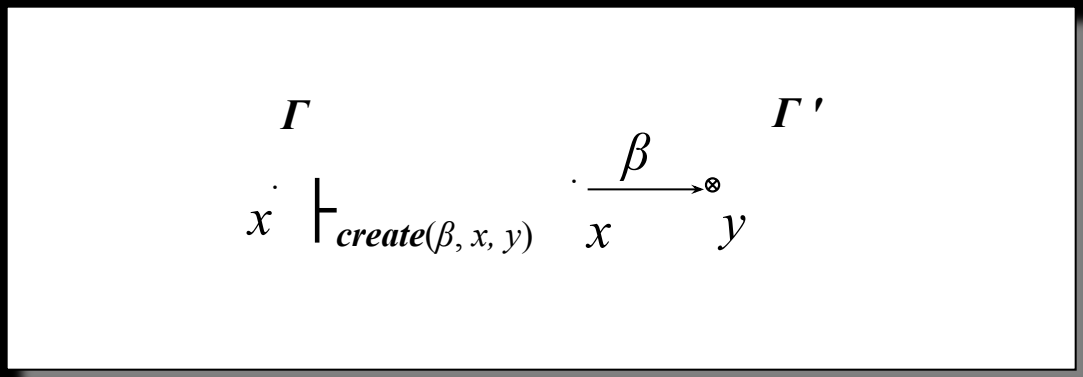
Команда «*Давать*" – *grant*(*α, x, y, z*)



субъект ***x*** дает объекту ***y*** право $\alpha \subseteq \beta$ на доступ к объекту ***z***

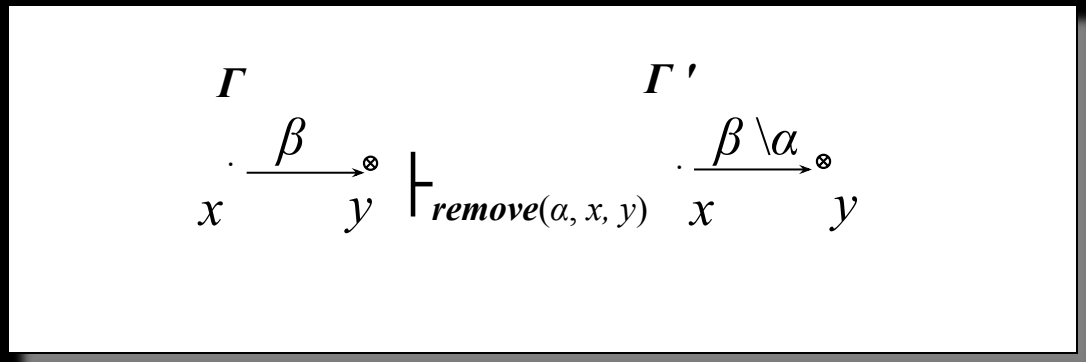
4.Модели распространения прав доступа. 4.4.Теоретико-графовая модель TAKE-GRANT

Команда "*Создать*" – *create*(*β*, *x*, *y*)



субъект ***x*** создает объект ***y*** с правами доступа на него ***β*** ⊆ ***R*** (***y*** – новый объект, ***O'=O*** ∪ {***y***}), в т. ч. с правами ***t***, или ***g***, или {***t***, ***g***}.

Команда «*Изъять*" – *remove*(*α*, *x*, *y*)



субъект ***x*** удаляет права доступа ***α*** ⊆ ***β*** на объект ***y***

4. Модели распространения прав доступа. 4.4. Теоретико-графовая модель TAKE-GRANT

3. Безопасность системы рассматривается с точки зрения возможности получения каким-либо субъектом прав доступа к определенному объекту (в начальном состоянии $\Gamma_0 (O_0, S_0, E_0)$ такие права отсутствуют) при определенной кооперации субъектов путем последовательного изменения состояния системы на основе выполнения элементарных команд. Рассматриваются две ситуации – условия санкционированного, т.е. законного получения прав доступа, и условия «похищения» прав доступа

3.1. *Санкционированное получение прав доступа*

Определение **3**. *Для исходного состояния системы* $\Gamma_0 (O_0, S_0, E_0)$ *и прав доступа* $\alpha \subseteq R$ *предикат "**возможен доступ**(α, x, y, Γ_0)" является истинным тогда и только тогда, когда существуют графы доступов системы* $\Gamma_1 (O_1, S_1, E_1)$, $\Gamma_2 (O_2, S_2, E_2)$, ..., $\Gamma_N (O_N, S_N, E_N)$, *такие, что:*
$\Gamma_0 (O_0, S_0, E_0) \vdash_{c_1} \Gamma_1 (O_1, S_1, E_1) \vdash_{c_2} \ldots \vdash_{c_N} \Gamma_N (O_N, S_N, E_N)$ *и* $(x, y, \alpha) \in E_N$
где $c_1, c_2, \ldots, c_N$ *– команды переходов*

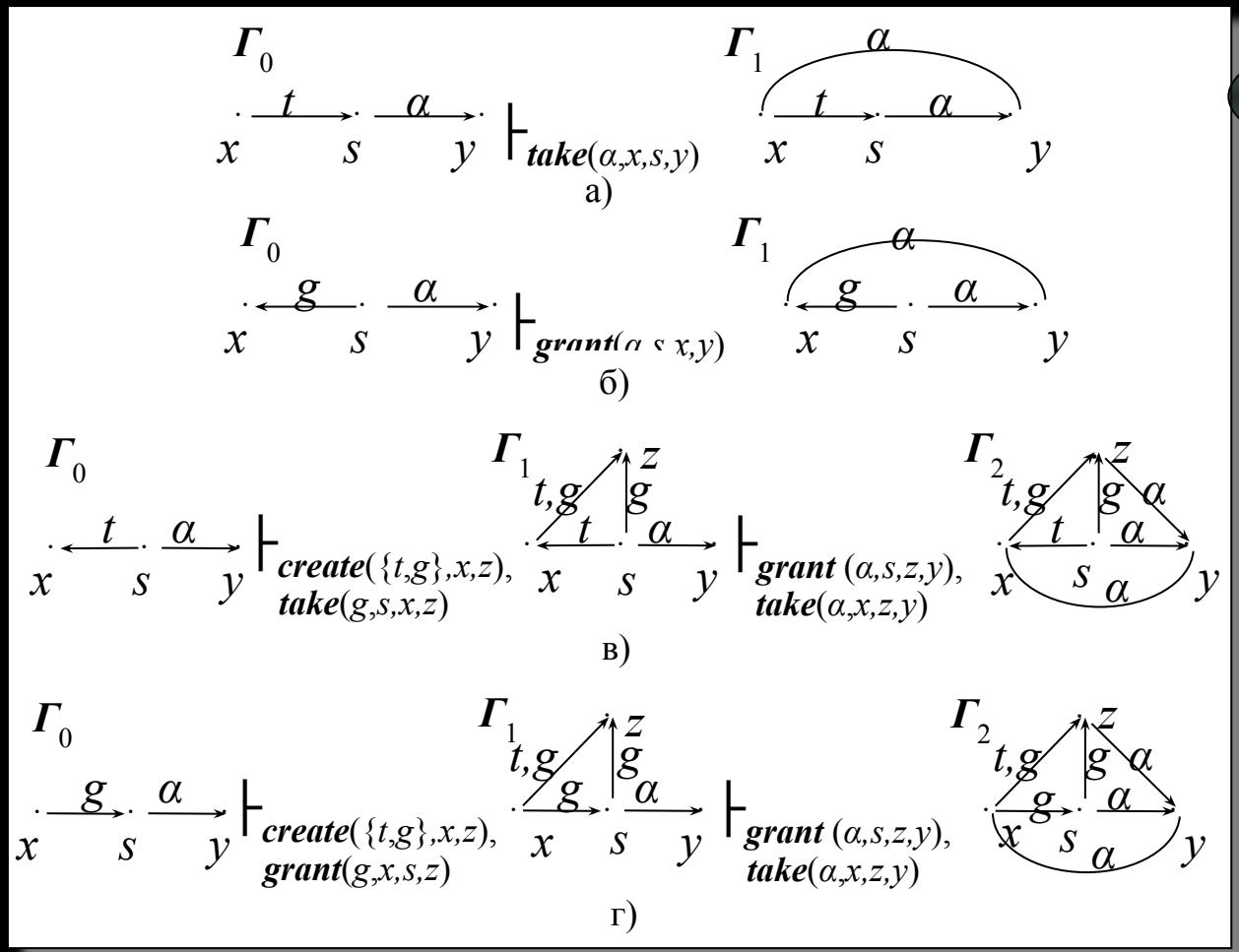
Определение **4**. *Вершины графа доступов являются **tg-связными** (соединены **tg**-путем), если в графе между ними существует такой путь, что каждая дуга этого пути выражает право **t** или **g** (без учета направления дуг)*

4.Модели распространения прав доступа. 4.4.Теоретико-графовая модель TAKE-GRANT

Теорема 4. *В графе доступов* $\Gamma_0 (O_0, S_0, E_0)$ *, содержащем только вершины-субъекты, предикат "**возможен доступ**(α, x, y, Γ_0)" истинен тогда и только тогда, когда выполняются следующие условия:*

- существуют субъекты $s_1,\ldots,s_m$ *такие, что* $(s_i, y, \gamma_i) \in E_0$ *для* $i=1, \ldots, m$ *и* $\alpha = \gamma_1 \cup \ldots \cup \gamma_m$.

- субъект x соединен в графе Γ_0 ***tg**-путем с каждым субъектом* s_i *для* $i=1, \ldots, m$



Доказательство

получение прав *α* доступа субъектом *x* у субъекта *s* на объект *y* при различных вариантах непосредственной *tg*-связности

4.Модели распространения прав доступа. 4.4.Теоретико-графовая модель TAKE-GRANT

Определение 5. *Островом в произвольном графе доступов* ***Г (O, S, E)*** *называется его максимальный* ***tg-связный*** *подграф, состоящий только из вершин субъектов.*

Определение 6. *Мостом в графе доступов* ***Г (O, S, E)*** *называется* ***tg–путь****, концами которого являются вершины-субъекты; при этом словарная запись* ***tg–пути*** *должна иметь вид*

$$\vec{t}^{\,*}, \overleftarrow{t}^{\,*}, \vec{t}^{\,*}\vec{g}\,\overleftarrow{t}^{\,*}, \vec{t}^{\,*}\overleftarrow{g}\,\overleftarrow{t}^{\,*}$$

*где символ * означает многократное (в том числе нулевое) повторение.*

Определение 7. *Начальным пролетом моста в графе доступов* ***Г (O, S, E)*** *называется* ***tg-путь****, началом которого является вершина-субъект; при этом словарная запись* ***tg-пути*** *должна иметь вид*

$$\vec{t}^{\,*}\vec{g}$$

Определение 8. *Конечным пролетом моста в графе доступов* ***Г (O, S, E)*** *называется* ***tg-путь****, началом которого является вершина-субъект; при этом словарная запись* ***tg-пути*** *должна иметь вид*

$$\vec{t}^{\,*}$$

4.Модели распространения прав доступа. 4.4.Теоретико-графовая модель TAKE-GRANT

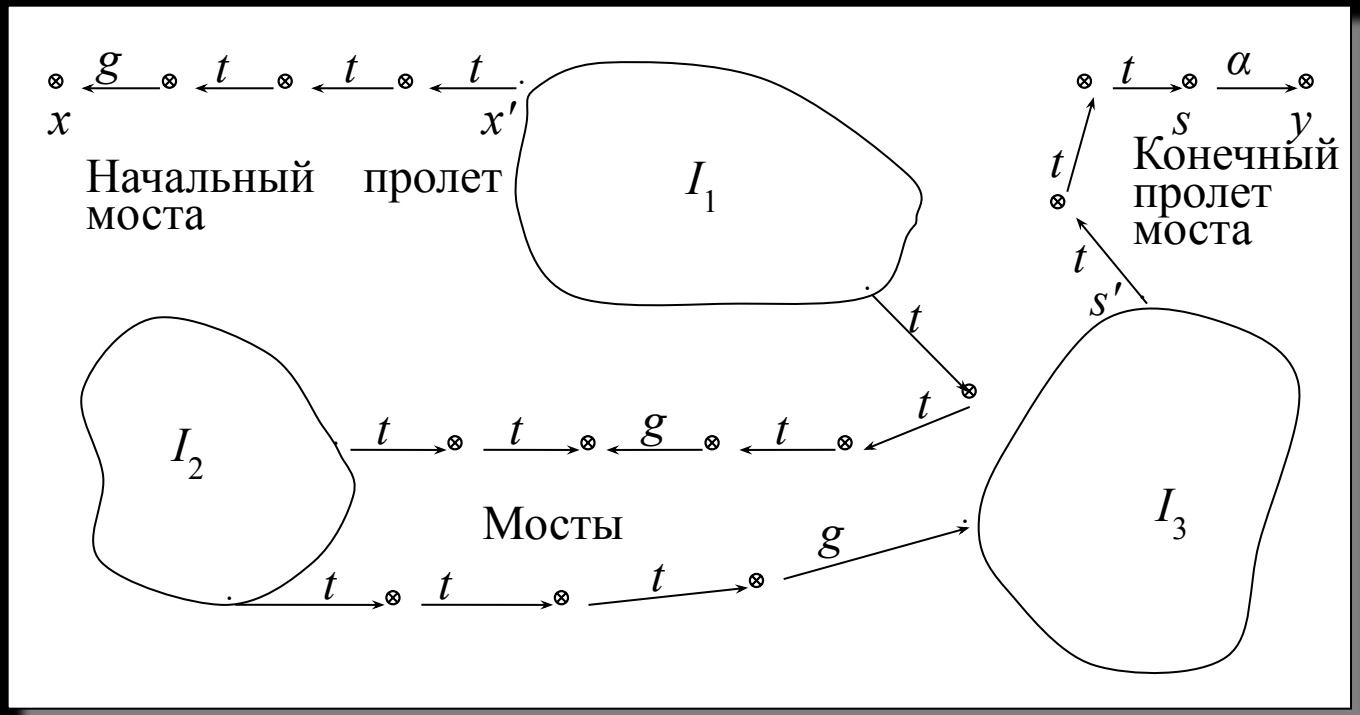
Теорема 4. *В произвольном графе доступов* $\Gamma_0 (O_0, S_0, E_0)$ *предикат "**возможен доступ**(α, x, y, Γ_0)" истинен тогда и только тогда, когда выполняются условия:*

- существуют объекты $s_1,\ldots,s_m$ *такие, что* $(s_i, y, \gamma_i)\in E_0$ *для* $i=1, \ldots, m$ *и* $\alpha =\gamma_1 \cup \ldots \cup \gamma_m$.

- существуют вершины-субъекты $x_1',\ldots,x_m'$ *и* $s_1',\ldots,s_m'$ *такие, что:*

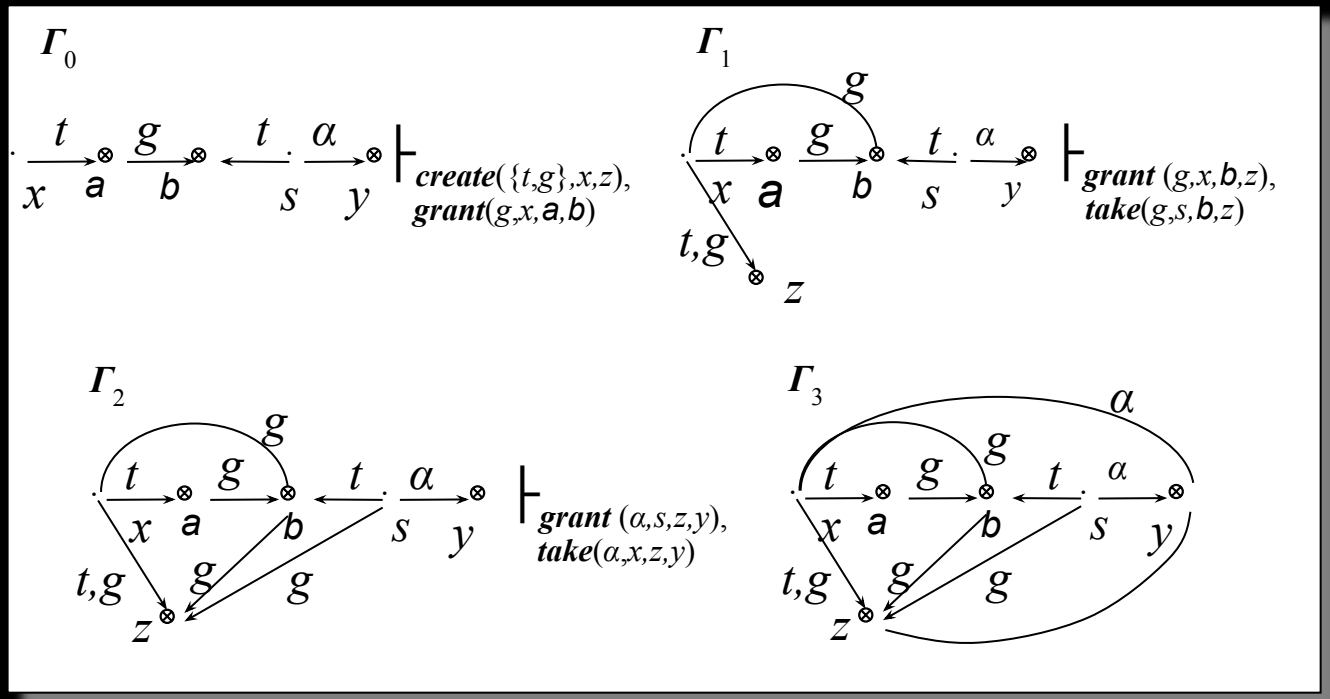
-- $x = x_i'$ *или* x_i' *соединен с* x *начальным пролетом моста для* $i=1, \ldots, m$;

-- $s_i = s_i'$ *или* s_i' *соединен с* s_i *конечным пролетом моста для* $i=1, \ldots, m$.



Пример графа доступов с возможностью передачи объекту x прав доступа α на объект y

4.Модели распространения прав доступа. 4.4.Теоретико-графовая модель TAKE-GRANT



Пример передачи прав доступа по мосту вида

3.1. *Похищение прав доступа*

Определение 9. *Для исходного состояния системы* $\Gamma_0 (O_0, S_0, E_0)$ *и прав доступа* $\alpha \subseteq R$ *предикат "**возможно похищение**(α, x, y, Γ_0)" является истинным тогда и только тогда, когда существуют графы доступов системы* $\Gamma_1 (O_1, S_1, E_1)$, $\Gamma_2 (O_2, S_2, E_2)$, ..., $\Gamma_N (O_N, S_N, E_N)$ *такие, что:*

$\Gamma_0 (O_0, S_0, E_0) \vdash_{c_1} \Gamma_1 (O_1, S_1, E_1) \vdash_{c_2} \ldots \vdash_{c_N} \Gamma_N (O_N, S_N, E_N)$ *и* $(x, y, \alpha) \in E_N$

где $c_1, c_2, \ldots, c_N$ *– команды переходов;*

при этом, если $\exists (s, y, \alpha) \in E_0$, *то* $\forall z \in S_j$, $j=0,1,\ldots, N$ *выполняется:*

$c_1 \neq$ *grant*(α, s, z, y).

4. Модели распространения прав доступа. 4.4. Теоретико-графовая модель TAKE-GRANT

Теорема 4. *В произвольном графе доступов* $\Gamma_0 (O_0, S_0, E_0)$ *предикат "**возможно похищение**(*α, x, y, Γ_0*)" истинен тогда и только тогда, когда выполняются условия:*

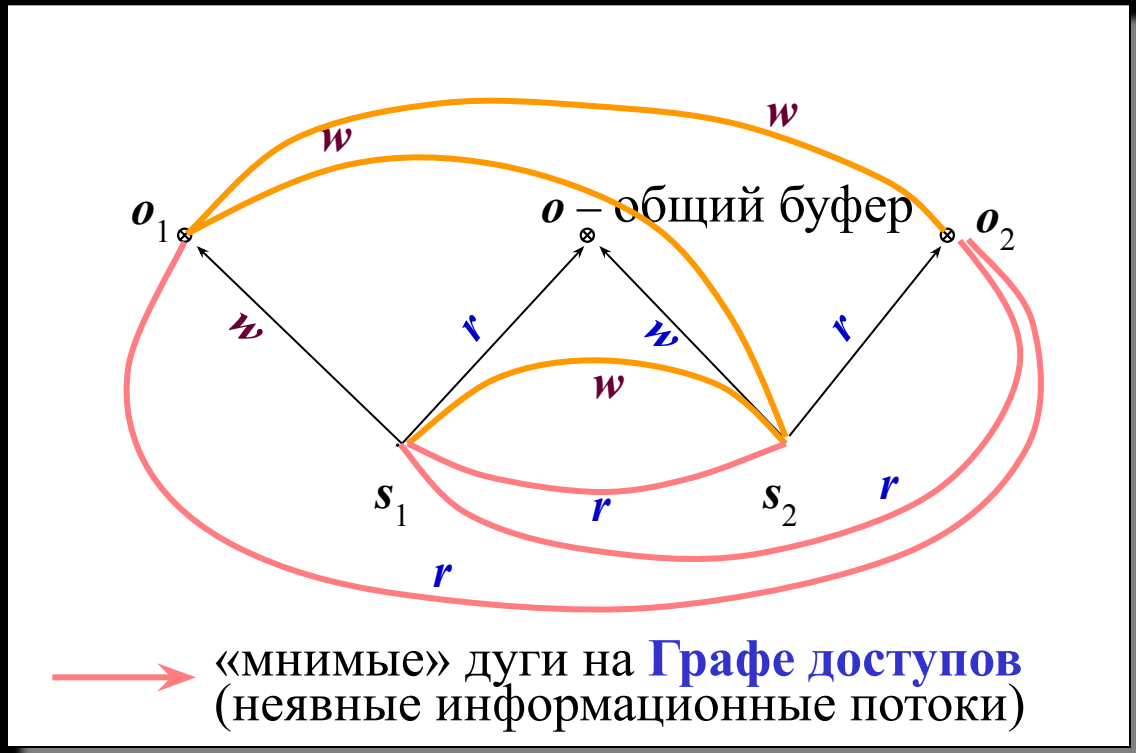
- $(x, y, \alpha) \notin E_0$.
- *существуют субъекты* $s_1,\ldots,s_m$ *такие, что* $(s_i, y, \gamma_i) \in E_0$ *для* $i=1, \ldots, m$ *и* $\alpha = \gamma_1 \cup \ldots \cup \gamma_m$
- *являются истинными предикаты "**возможен доступ**(*t, x, s_i, Γ_0*)" для* $i=1, \ldots, m$.

Если политика разграничения доступа в КС запрещает субъектам, имеющим в исходном состоянии права доступа к определенным объектам, непосредственно предоставлять эти права другим субъектам, которые изначально такими правами не обладают, то, тем не менее, такие первоначально "обделенные" субъекты могут получить данные права при наличии в графе доступов возможностей получения доступа с правом t к первым субъектам

4.Модели распространения прав доступа. 4.5.Расширенная (extended) модель TAKE-GRANT

Теоретическая основа для анализа неявных (скрытых) каналов утечки информации в системах с дискреционным доступом

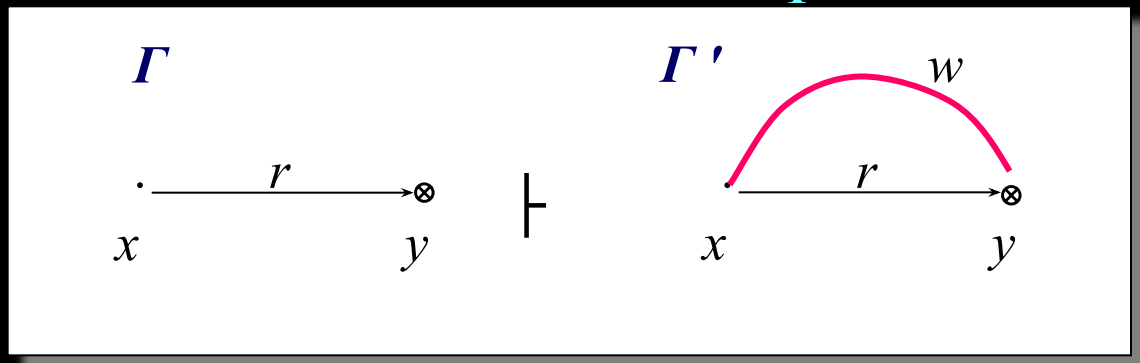
Определение **10**. *Неявным информационным потоком между объектами системы называется процесс переноса информации между ними без их непосредственного взаимодействия* (*операции **Read**, **Write***)



4.Модели распространения прав доступа. 4.5.Расширенная (extended) модель TAKE-GRANT

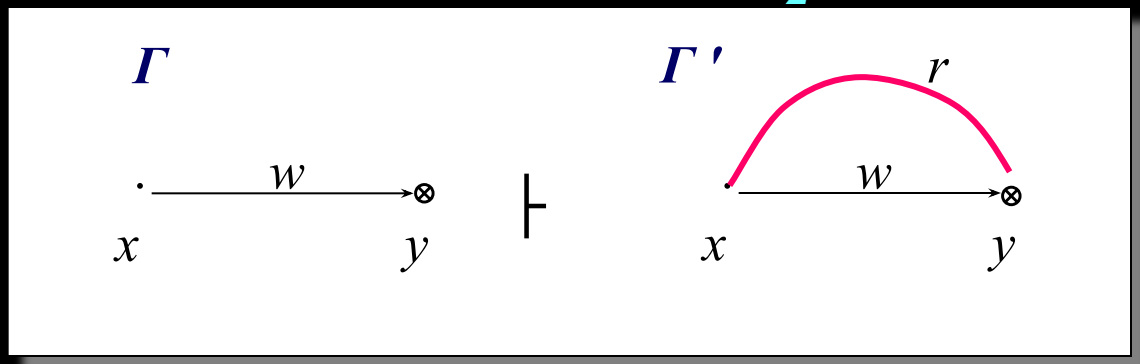
2.Состояние **Графа доступов** изменяется под воздействием элементарных команд 6-х видов (т.н. команды ***де-факто***)

Команда без названия $\alpha_1(x, y)$



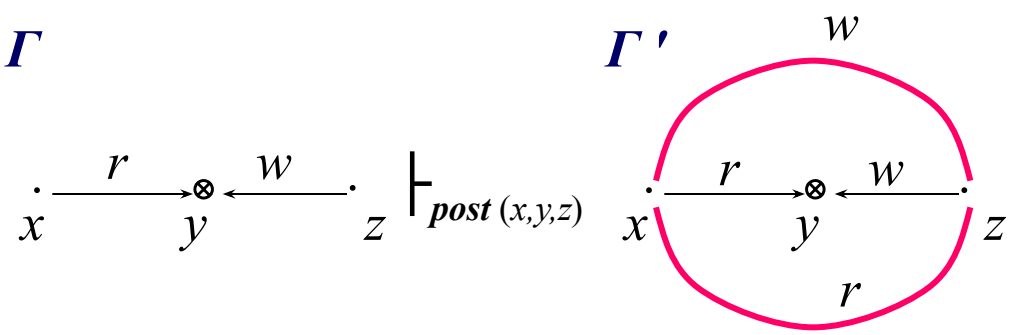
имеется неявная возможность передачи (записи) [конфиденциальной] информации из объекта ***y*** субъекту ***x***, когда тот осуществляет доступ ***r*** к объекту ***y***

Команда без названия $\alpha_2(x, y)$



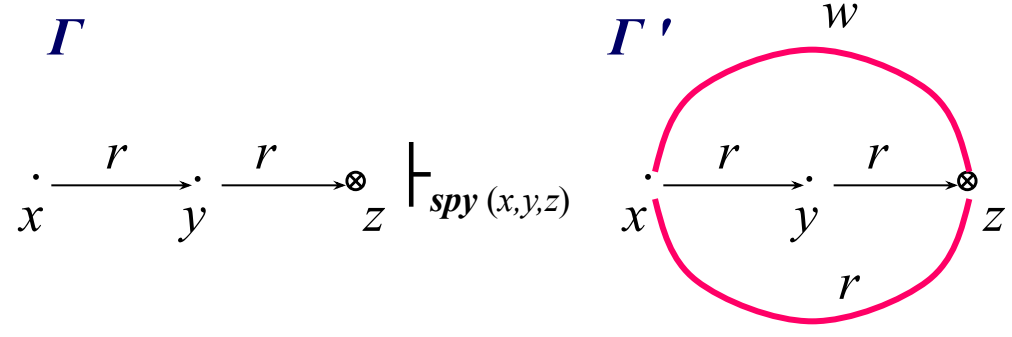
имеется неявная возможность получения (чтения) объектом ***y*** [конфиденциальной] информации от субъекта ***x***], когда тот осуществляет доступ ***w*** к объекту ***y***

Команда *post*(*x*, *y*, *z*)



субъект *x* получает возможность чтения информации от (из) другого субъекта *z*, осуществляя доступ *r* к объекту *y*, к которому субъект *z* осуществляет доступ *w*, а субъект *z*, в свою очередь, получает возможность записи своей информации в субъект *x*

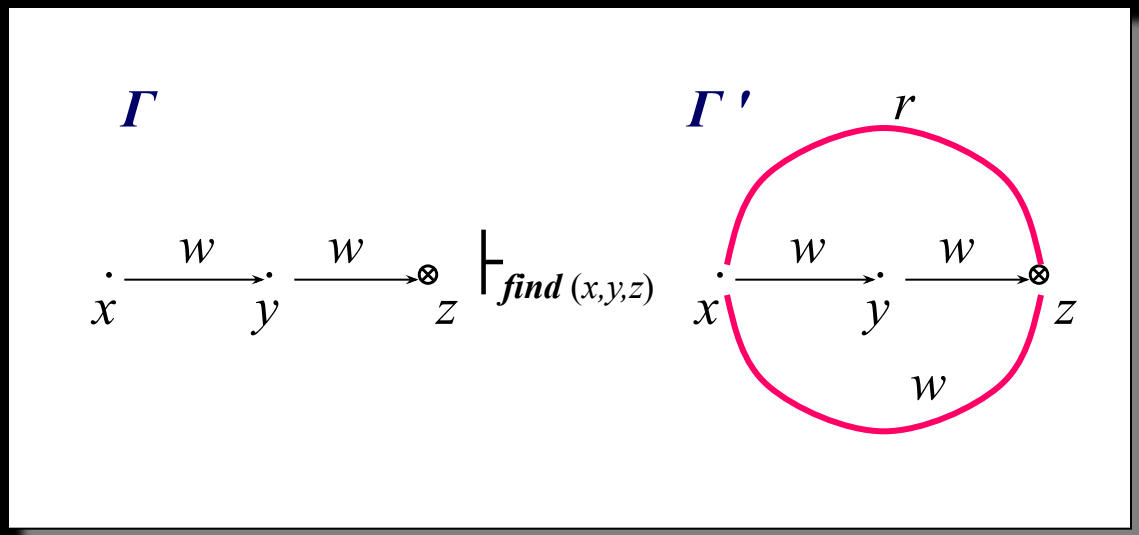
Команда *spy*(*x*, *y*, *z*)



субъект *x* получает возможность чтения информации из объекта *z*, осуществляя доступ *r* к субъекту *y*, который, в свою очередь, осуществляет доступ *r* к объекту *z*, при этом также у субъекта *x* возникает возможность записи к себе информации из объекта *z*

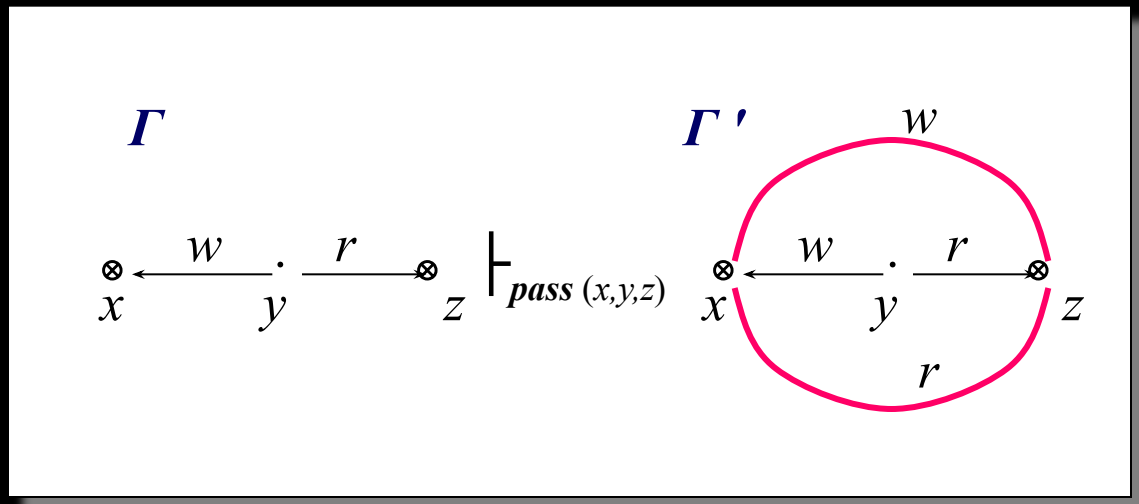
4. Модели распространения прав доступа. 4.5. Расширенная (extended) модель TAKE-GRANT

Команда *find*(*x*, *y*, *z*)



субъект *x* получает неявн. возможность передачи (записи) конф. информации в объект *z*, осуществляя доступ *w* к субъекту *y*, который, в свою очередь, осуществляет доступ *w* к объекту *z*, при этом также у субъекта *z* возникает неявн. возможность чтения конф. информации из субъекта *x*

Команда *pass*(*x*, *y*, *z*)



при осуществлении субъектом *y* доступа *r* к объекту *z* возникает неявная возможность внесения из него конф. информации в другой объект *x*, к которому субъект *y* осуществляет доступ *w*, и, кроме того, возникает возможность получения информации (чтения) объектом *x* из объекта *z*

Правила *де-юре* к мнимым дугам не применяются

4.Модели распространения прав доступа. 4.5.Расширенная (extended) модель TAKE-GRANT

3. Анализ возможности возникновения неявного информационного канала (потока) между двумя произвольными объектами (субъектами) ***x*** и ***y*** системы осуществляется на основе поиска и построения в графе доступов **пути** между ***x*** и ***y***, образованного **мнимыми дугами**, порождаемыми применением команд ***де-факто*** к различным фрагментам исходного **Графа доступов**

Расширенная модель TAKE-GRANT позволяет анализировать специфические проблемы в дискреционных системах разграничения доступа:

- при допущении возможности или при наличии достоверных фактов о состоявшемся неявном информационном потоке от одного объекта(субъекта) к другому объекту(субъекту), анализировать и выявлять **круг возможных субъектов-"заговорщиков"** несанкционированного информационного потока

- для какой-либо пары объектов (субъектов) осуществлять анализ не только возможности неявного информационного потока, но и **количественных** характеристик по тому или иному маршруту:

  возможно взвешивание мнимых дуг на Графе доступов посредством оценки вероятности их возникновения

  возможны количественные сравнения различных вариантов возникновения неявного потока по длине пути на Графе доступов

- **оптимизировать** систему назначений доступа по критериям минимизации возможных неявных информационных потоков

Достоинства дискреционных моделей

- *Хорошая гранулированность защиты (позволяют управлять доступом с точностью до отдельной операции над отдельным объектом)*
- *Простота реализации*

Недостатки дискреционных моделей

- *Слабые защитные характеристики из-за невозможности для реальных систем выполнять все ограничения безопасности*
- *Проблема "троянских коней"*
- *Сложности в управлении доступом из-за большого количества назначений прав доступа*

Тема 2. Модели безопасности компьютерных систем

Лекция

Модели безопасности на основе мандатной политики

Учебные вопросы:

1. **Общая характеристика моделей полномочного (мандатного) доступа**
2. **Модель Белла-ЛаПадулы**
3. **Расширения модели Белла-ЛаПадулы**

1. Общая характеристика моделей мандатного доступа

Основаны:
-на *субъектно-объектной* модели КС
- на *правилах организации секретного делопроизводства*
принятых в гос. учреждениях многих стран

Информация (точнее документы, ее содержащие) категорируется специальными метками конфиденциальности – т.н. ***грифы секретности*** документов

Сотрудники по уровню благонадежности (доверия к ним) получают т.н. ***допуска*** определенной ***степени***

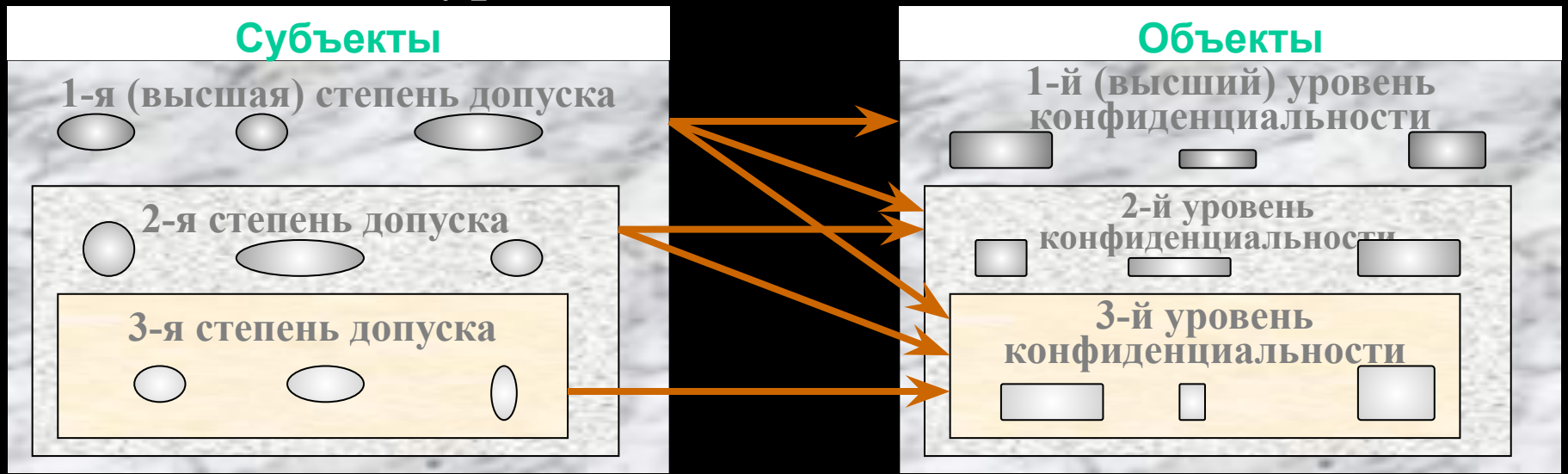
Сотрудники с допуском определенной степени приобретают ***полномочия*** работы с документами определенного грифа секретности

Гл. задача:
-не допустить утечки информации из документов
с высоким грифом секретности к сотрудникам
с низким уровнем допуска

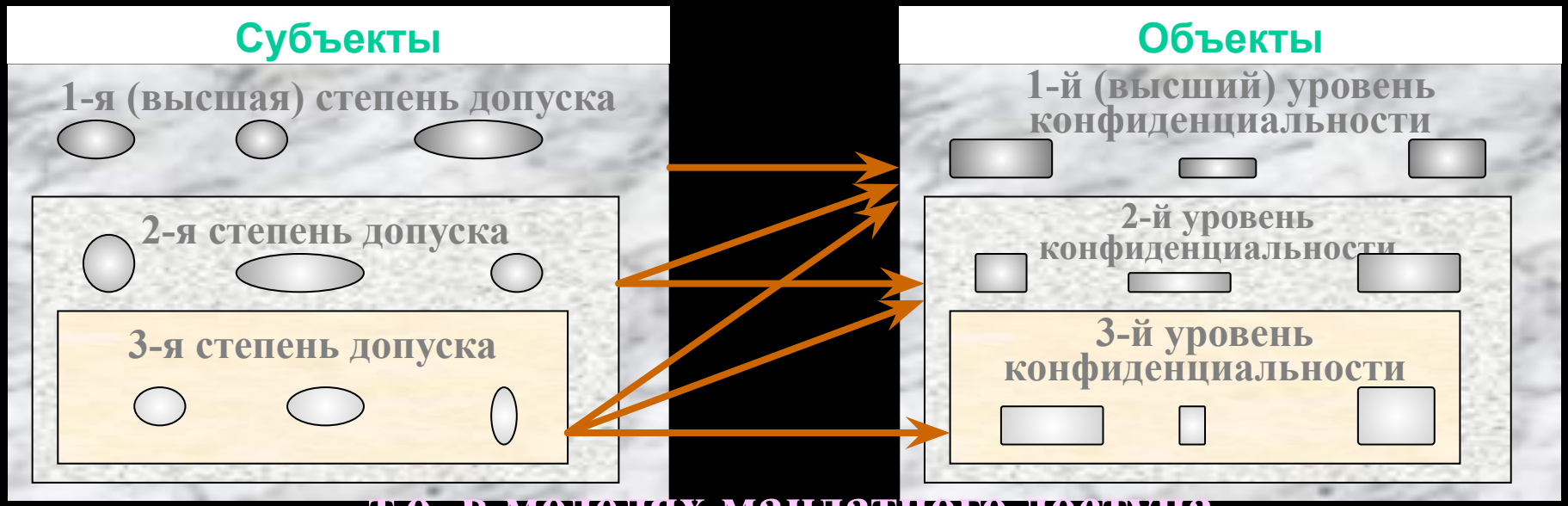
Основные положения *моделей мандатного доступа*

- Вводится система "***уровней безопасности***" – решетка с оператором доминирования
- Устанавливается функция (процедура) присваива-ния субъектам и объектам уровней безопасности
- Управление и контроль доступом субъектов к объектам производится на основе двух правил:

1.Запрет чтения вверх (*no read up - NRU*) - субъект не может читать объект с уровнем безопасности, большим своего уровня безопасности



2.Запрет записи вниз (*no write down - NWD*) - субъект не может писать информацию в объект, уровень безопасности которого ниже уровня безопасности самого субъекта (т.н. ****-свойство***)



т.о. в моделях мандатного доступа устанавливается жесткое управление доступом с целью контроля не столько операций, а потоков между сущностям с разным уровнем безопасности

- Для управления (разграничения) доступом к объектам одного уровня конфиденциальности используют дискреционный принцип, т.е. дополнительно вводят матрицу доступа

Решетка уровней безопасности Λ_L

- алгебра $(L, \leq, \cdot, \otimes)$, где

L – базовое множество уровней безопасности

$\leq$ – оператор доминирования, определяющий частичное нестрогое отношение порядка на множестве **L**. Отношение, задаваемое $\leq$, *рефлексивно*, *антисимметрично* и *транзитивно*:

$\forall\, l \in L: l \leq l$;

$\forall\, l_1, l_2 \in L: (l_1 \leq l_2 \wedge l_2 \leq l_1) \Rightarrow l_1 = l_2$;

$\forall\, l_1, l_2, l_3 \in L: (l_1 \leq l_2 \wedge l_2 \leq l_3) \Rightarrow l_1 \leq l_3$;

$\cdot$ – оператор, определяющий для любой пары $l_1, l_2 \in L$ наименьшую верхнюю границу -

$l_1 \cdot l_2 = l \Leftrightarrow l_1, l_2 \leq l \wedge \forall\, l' \in L: (l' \leq l) \Rightarrow (l' \leq l_1 \vee l' \leq l_2)$

$\otimes$ – оператор, определяющий для любой пары $l_1, l_2 \in L$ наибольшую верхнюю границу -

$l_1 \otimes l_2 = l \Leftrightarrow l \leq l_1, l_2 \wedge \forall\, l' \in L: (l' \leq l_1 \wedge l' \leq l_2) \Rightarrow (l' \leq l)$

Функция уровня безопасности $f_L: X \rightarrow L$

- однозначное отображение множества сущностей КС $X = S \cup O$ во множество уровней безопасности L решетки Λ_L .

Обратное отображение $f_L^{-1}: L \rightarrow X$ задает разделение всех сущностей КС на **классы безопасности** X_i, такие что:

$X_1 \cup X_2 \cup \ldots \cup X_N = X$,

где N - мощность базового множества уровней безопасности L;

$X_i \cap X_j \equiv \varnothing$, где $i \neq j$;

$\forall x' \in X_i \Rightarrow f_L(x') = l_i$, где $l_i \in L$

2. Модель Белла-ЛаПадулы

D.Elliott **Bell**, Leonard J.**LaPadula**, 1973-75

Система защиты - совокупность

- множества субъектов ***S***
- множества объектов ***O***
- множества прав доступа ***R*** (в исх. виде всего два элемента - ***read*** и ***write***)
- матрицы доступа $A[s,o]$
- решетки уровней безопасности ***L*** субъектов и объектов (допуска и грифы секретности)
- функции уровней безопасности f_L, отображающей элементы множеств ***S*** и ***O*** в ***L***
- множества состояний системы ***V***, которое определяется множеством упорядоченных пар (f_L, A)
- начального состояния v_0
- набора запросов ***Q*** субъектов к объектам, выполнение которых переводит систему в новое состояние
- функции переходов $\mathcal{F}_T : (V \times Q) \rightarrow V$, которая переводит систему из одного состояния в другое при выполнении запросов

Белл и ЛаПадула ввели следующее определение безопасного состояния системы

1. Состояние называется **безопасным по чтению** (или *просто безопасным*) тогда и только тогда, когда для каждого субъекта, осуществляющего в этом состоянии доступ чтения к объекту, уровень безопасности этого субъекта доминирует над уровнем безопасности этого объекта:

$$\forall s \in S,\ \forall o \in O,\ read \in A[s,o] \rightarrow f_L(s) \geq f_L(o)$$

2. Состояние называется **безопасным по записи** (или **-безопасным*) тогда и только тогда, когда для каждого субъекта, осуществляющего в этом состоянии доступ записи к объекту, уровень безопасности объекта доминирует над уровнем безопасности этого субъекта:

$$\forall s \in S,\ \forall o \in O,\ write \in A[s,o] \rightarrow f_L(o) \geq f_L(s)$$

3. Состояние **безопасно** тогда и только тогда, когда оно безопасно *и по чтению, и по записи*

На основе определений 1,2 и 3 *критерий безопасности:*

Система $\Sigma(v_0, Q, F_T)$ безопасна тогда и только тогда, когда ее начальное состояние v_0 безопасно и все состояния, достижимые из v_0 путем применения конечной последовательности запросов из Q безопасны

Белла и ЛаПадула доказали т.н. *Основную теорему безопасности:*

Теорема ОТБ. **Система $\Sigma(v_0, Q, \mathcal{F}_T)$ безопасна тогда и только тогда, когда:**

1. Состояние v_0 безопасно

2. Функция переходов $\mathcal{F}_T$ такова, что любое состояние v, достижимое из v_0 при выполнении конечной последовательности запросов из множества Q, также безопасно

3. Если при $\mathcal{F}_T(v,q)=v^*$, где $v=(f_L, A)$ и $v^*=(f_L^*, A^*)$, переходы системы из состояния в состояние подчиняются следующим ограничениям для $\forall s \in S$ и для $\forall o \in O$:

- если $read \in A^*[s,o]$ и $read \notin A[s,o]$, то $f_L^*(s) \geq f_L^*(o)$
- если $read \in A[s,o]$ и $f_L^*(s) < f_L^*(o)$, то $read \notin A^*[s,o]$
- если $write \in A^*[s,o]$ и $write \notin A[s,o]$, то $f_L^*(s) \leq f_L^*(o)$
- если $write \in A[s,o]$ и $f_L^*(o) < f_L^*(s)$, то $write \notin A^*[s,o]$

Правила доступа и ограничения NRU и NWD должны работать независимо от предыстории конкретных объектов и субъектов

При переходе в новое состояние не возникает никаких новых и
не сохраняется никаких старых отношений доступа, которые небезопасны
по отношению к функции уровня безопасности нового

Достоинства модели Белла-ЛаПадулы:

- ясность и простота реализации
- отсутствие проблемы "Троянских коней" (контролируется направленность потоков, а не взаимоотношения конкретного субъекта с конкретным объектом, поэтому недекларированный поток троянской программы «сверху-вниз» будет считаться опасным и отвергнут МБО)
- каналы утечки не заложены в саму модель, а могут возникнуть только в практической реализации

Недостатки модели Белла-ЛаПадулы:

- возможность ведения операций доступа (Delete), не влияющих с т.зр. модели на безопасность, которые тем не менее могут привести к потери данных
- проблема Z-системы (Мак-Лин) - такая система, в которой при запросе все сущности м.б. деклассифицированы до самого низкого уровня и тем самым м.б. осуществлен любой доступ (в модели не заложены принципы и механизмы классификации объектов)
- отсутствие в модели доверенных субъектов-администраторов Типовые действия администраторов (создание пользователей, установление их полномочий и т.д.) не могут ни приводить к нарушениям безопасности с т. зр. модели Белла-ЛаПадулы

Безопасная функция перехода (*Мак-Лин*)

Гарантии безопасности в процессе осуществления переходов между состояниями

Функция перехода $F_T(v,q)=v^*$ *безопасна* по чтению когда:

1. Если $read \in A^*[s,o]$ и $read \notin A[s,o]$, то $f_{Ls}(s) \geq f_{Lo}(o)$ и $f_L = f_L^*$
2. Если $f_{Ls} \neq f_{Ls}^*$, то $A=A^*$, $f_{Lo}=f_{Lo}^*$, для $\forall$ s и o, у которых $f_{Ls}^*(s) < f_{Lo}^*(o)$, - $read \notin A[s,o]$
3. Если $f_{Lo} \neq f_{Lo}^*$, то $A=A^*$, $f_{Ls}=f_{Ls}^*$, для $\forall$ s и o, у которых $f_{Ls}^*(s) < f_{Lo}^*(o)$, - $read \notin A[s,o]$

Функция перехода $F_T(v,q)=v^*$ *безопасна* по записи когда:

1. Если $write \in A^*[s,o]$ и $write \notin A[s,o]$, то $f_{Lo}(o) \geq f_{Ls}(s)$ и $f_L = F_L^*$
2. Если $f_{Ls} \neq f_{Ls}^*$, то $A=A^*$, $f_{Lo}=f_{Lo}^*$, для $\forall$ s и o, у которых $f_{Ls}^*(s) > f_{Lo}^*(o)$, - $write \notin A[s,o]$
3. Если $f_{Lo} \neq f_{Lo}^*$, то $A=A^*$, $f_{Ls}=f_{Ls}^*$, для $\forall$ s и o, у которых $f_{Ls}^*(s) > f_{Lo}^*(o)$, - $write \notin A[s,o]$

Нельзя изменять одновременно более одного компонента состояния системы. Можно:
-либо ввести новое отношение доступа
-либо изменить уровень субъекта
-либо изменить уровень объекта

Критерий безопасности Мак-Лина для функции перехода

Функция перехода $F_T(v,q)=v^*$ является безопасной тогда и только тогда, когда она *изменяет только один* из компонентов состояния и изменения не приводят к нарушению безопасности системы

Теорема безопасности Мак-Лина.

Система безопасна в любом состоянии и в процессе переходов между ними, если ее начальное состояние безопасно, а функция перехода удовлетворяет критерию безопасности Мак-Лина

Но! Нет контроля самого процесса изменения уровней безопасности сущностей в процессе осуществления переходов

Уполномоченные (доверенные) субъекты (*Мак-Лин*)

В базовую модель дополнительно вводится подмножество доверенных субъектов, которым (и только им) разрешается инициировать переходы с изменениями уровней безопасности сущностей системы – $C(S)$

Соответственно функция переходов системы $\Sigma(v_0, Q, \mathcal{F}_T^a)$ – $\mathcal{F}_T^a$ приобретает дополнительный параметр *авторизации*

Функция перехода $\mathcal{F}_T^a(v,s,q)$ в модели с называется авторизованной тогда и только тогда, когда для каждого перехода $\mathcal{F}_T^a(v,s,q)=v^*$, при котором:

для $\forall x \in S \cup O$**:** если $f_L(x) \neq f_L(x)$, то $s \in C(S)$

Система $\Sigma(v_0, Q, \mathcal{F}_T^a)$ с доверенными субъектами безопасна если :

1. Начальное состояние v_0 безопасно и все достижимые состояния безопасны по критерию Белла-ЛаПадулы
2. Функция переходов $\mathcal{F}_T^a$ является ***авторизованной***

Другие расширения модели Белла-ЛаПадулы

Модель *Low-WaterMark*

Вводится дополнительная операция *reset*(*s*,*o*), которая повышает до максимального уровень безопасности объекта при условии *F*(*s*)>*F*(*o*). В результате субъекту м.б. доступен по *write* любой объект

Модифицируется *write*(*s*,*o*) Если при операции *write* уровень объекта выше уровня субъекта то:

- происходит понижение уровня безопасности объекта до уровня безопасности субъекта;

- перед внесением новой старая информация в объекте стирается (чтобы потом нельзя было прочесть)

Модель *совместного доступа*

Доступ к определенной информации или модификация ее уровня безопасности может осуществляться только в результате совместных действий нескольких пользователей (т.е. только в результате группового доступа- z.b. гриф секретности документа м.б. изменен только совместными действиями владельца-исполнителя и администратора безопасности)

В матрице доступа вводятся групповые объекты и др.

Другие недостатки модели Белла-ЛаПадулы

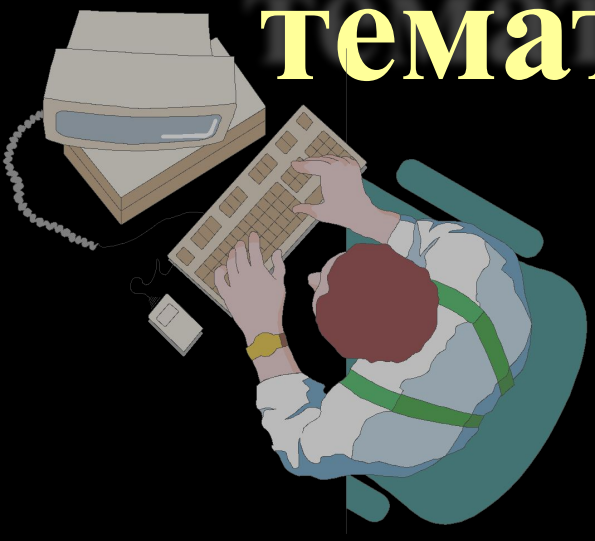
- **возможность скрытых каналов утечки** - механизм, посредством которого субъект с высоким уровнем безопасности м. предоставить определенные аспекты конфиденциальной информации субъекту, уровень безопасности которого ниже уровня безопасности конф. информации
- **проблема удаленного доступа**. В распределенных системах осуществление доступа всегда сопровождается потоком информации в прямом и обратном направлении, что результате может приводить к нарушениям привил NRU и NWD
- **проблема избыточности прав доступа**. Без учета матрицы доступа (т.е. без использования дискреционного доступа) мандатный принцип доступа организует доступ более жестко, но и более грубо, без учета потребностей конкретных пользователей-субъектов

Тем не менее **модель Белла-ЛаПадулы оказала сильное влияние на развитие моделей безопасности и *стандартов защищенности КС***

Тема 2. Модели безопасности компьютерных систем

Лекция

Модели безопасности на основе тематической политики

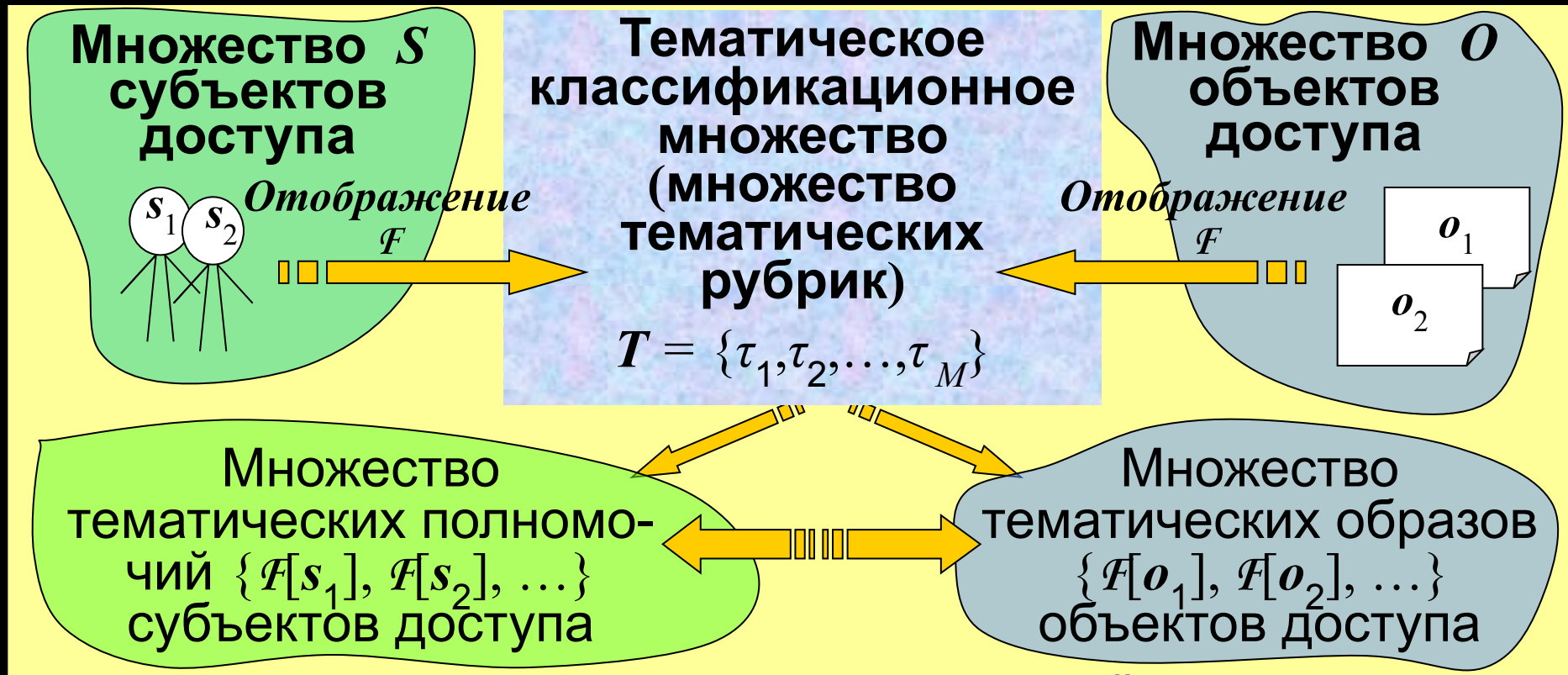


Учебные вопросы:

1. Общая характеристика тематического разграничения доступа
2. Тематическая решетка мультирубрик иерархического рубрикатора
3. Модели тематико-иерархического разграничения доступа

Политика тематического разграничения доступа

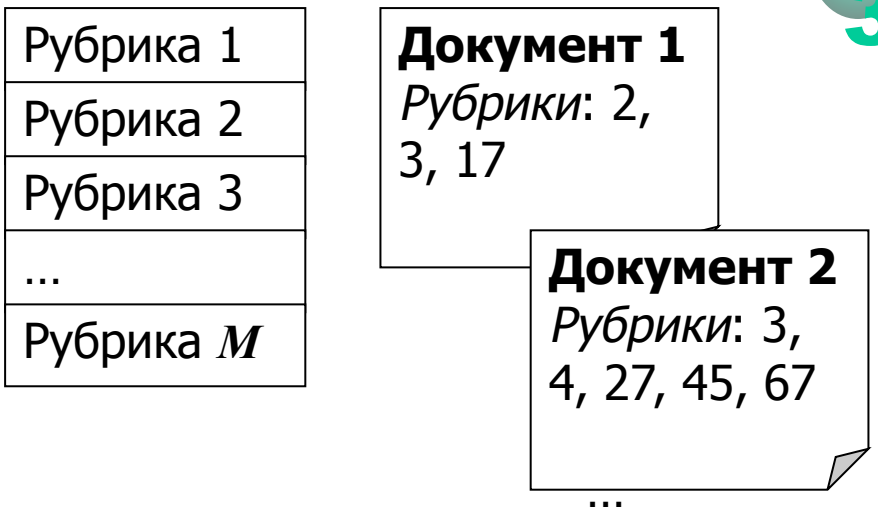
1.Множество субъектов и объектов доступа $X = S \cup O$ тематически классифицируются



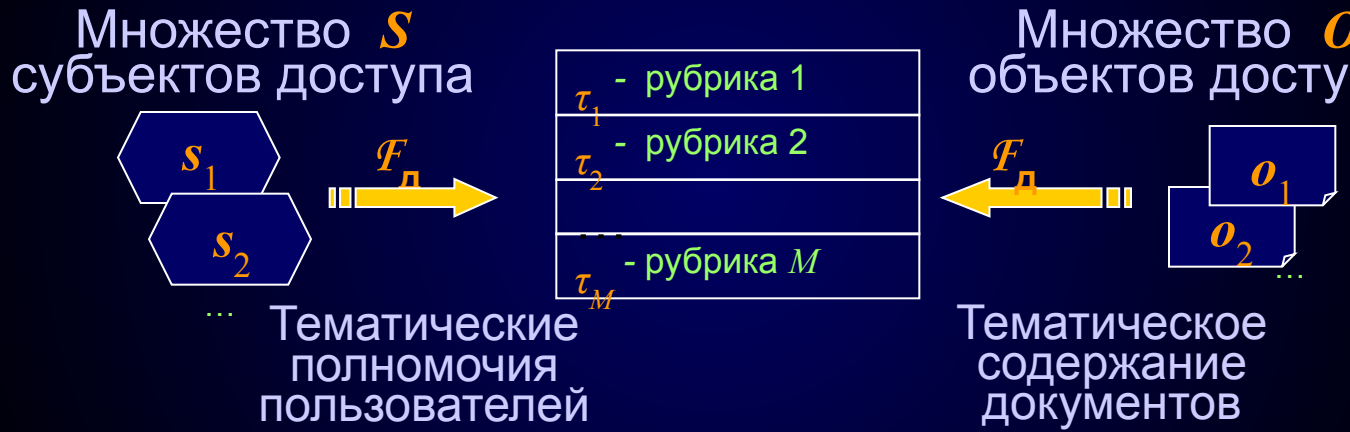
На множестве тематических полномочий субъектов и тематических образов устанавливается частичный порядок (отношение доминирования ≤, т.е. шире, уже, несравнимо)

2. Три способа тематической классификации

- дескрипторная
- иерархическая
  - -- монорубрицированная
  - -- мультирубрицированная
- фасетная



Дескрипторное классифицирующее тематическое множество $T_д$ – множество неупорядоченных тематических рубрик (дескрипторов)

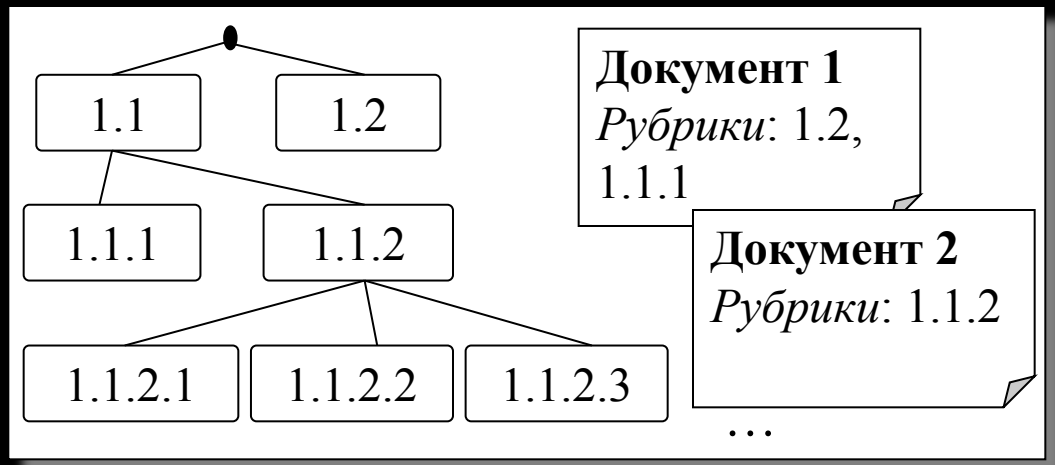


$$F_д[x_i] = \{\tau_{i1}, \tau_{i2}, \ldots, \tau_{iI}\} \wedge \tau_{ik} \neq \tau_{im}, \quad x_i \in S \cup O, I \leq M$$

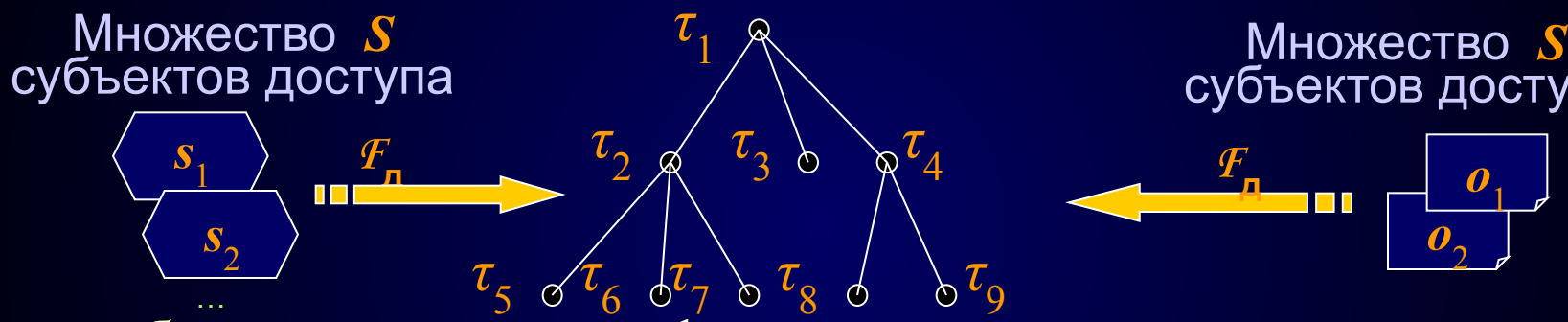
Дескрипторная тематическая классификация

1.Общая характеристика тематического разграничения доступа

Иерархическая тематическая классификация



Иерархический тематический классификатор – множество рубрик $T_и$, на котором посредством корневого дерева установлено отношение частичного порядка элементов $\leq$



Монорубрицованная классификация

$\mathcal{F}_{имн}[x_i] = \tau_i \cup \{\tau_{i1}, \tau_{i2}, \ldots, \tau_{iI}\}$, где $\tau_{ik} \leq \tau_i$, $x_i \in S \cup O$, $I < M$.

Мультирубрицированная классификация

$\mathcal{F}_{имл}[x_i] = \{\tau_{i1}, \tau_{i2}, \ldots, \tau_{iI}\} \cup \{\tau_{i11}, \tau_{i12}, \ldots, \tau_{i21}, \tau_{i22}, \ldots, \tau_{iI1}, \tau_{iI2}, \ldots\} \wedge \tau_{im} \not\leq\geq \tau_{in}$

$\wedge \vee_{и} \{\tau_{k1}, \tau_{k2}, \ldots, \tau_{kL}\} = \varnothing$, $\tau_{ik} \leq \tau_{ikj}$

Политика тематического разграничения доступа

3.Недопустимы доступы (вызывающие опасные потоки)

- от сущностей x_1 с более широкой тематикой к сущностям x_2 с более узкой тематикой $(x_1 \rightarrow x_2)$

$\mathcal{F}[x_1] \geq \mathcal{F}[x_2]$

- между сущностями x_1 и x_2 с несравнимой тематикой $(x_1 \leftrightarrow x_2)$

$\mathcal{F}[x_2] \geq \leq \mathcal{F}[x_2]$

2. Тематическая решетка мультирубрик иерархического рубрикатора

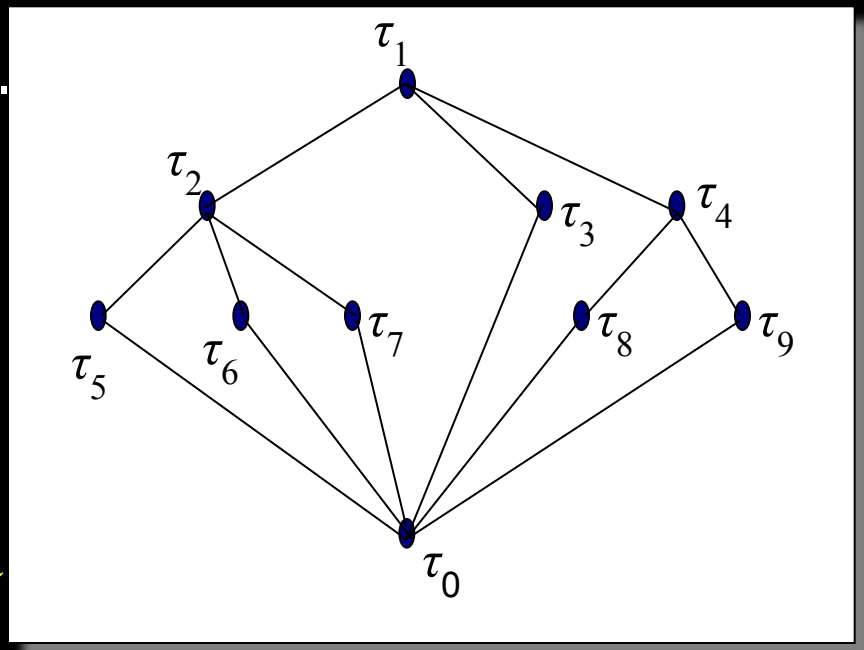
Тематические решетки

1. При дескрипторной тематической классификации

- решетка $\Lambda_д(P_д, \subseteq, \cup, \cap)$ подмножеств множества $T_д = \{\tau_1, \tau_2, \ldots, \tau_M\}$, где $P_д = \mathcal{F}_д[x] \subseteq T_д$, $x \in S \cup O$

2. На иерархическом рубрикаторе при монорубрицированной классификации

- решетка $\Lambda_и(T_{и\varnothing}, \leq, \sup_и, \inf_и)$ на корневом дереве рубрикатора $T_и = \{\tau_1, \tau_2, \ldots, \tau_M\}$ путем добавления вершины τ_0 (с пустой тематикой) и замыкания на нее всех листовых вершин



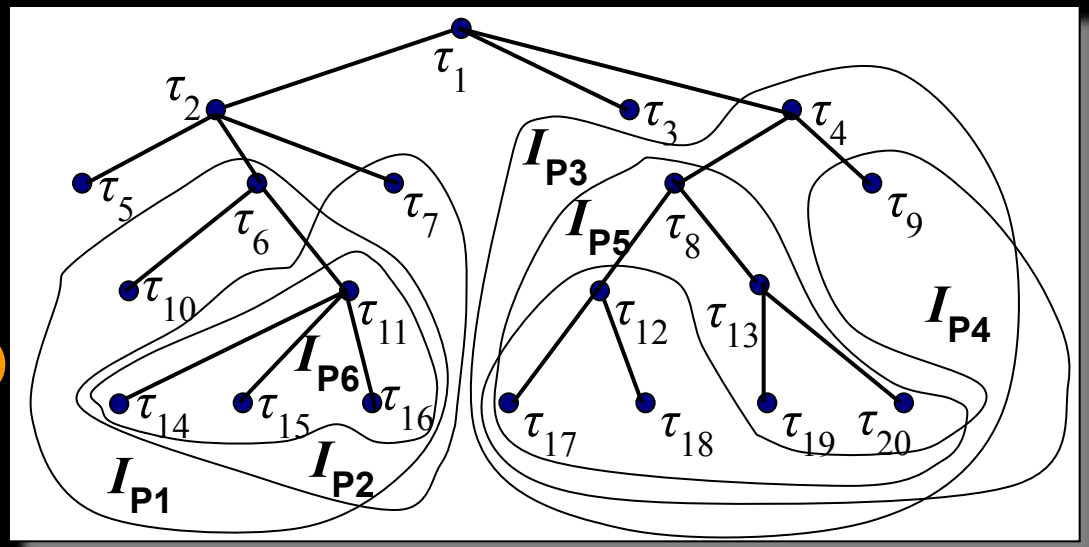
- решетка $\Lambda_и(\mathcal{T}^{\sqcap}, \subseteq, \cup_{ил}, \cap)$ листовых подмножеств вершин на корневом дереве рубрикатора. Решетки $\Lambda_и(T_{и\varnothing}, \leq, \sup_и, \inf_и)$ и $\Lambda_и(\mathcal{T}^{\sqcap}, \subseteq, \cup_{ил}, \cap)$ изоморфны

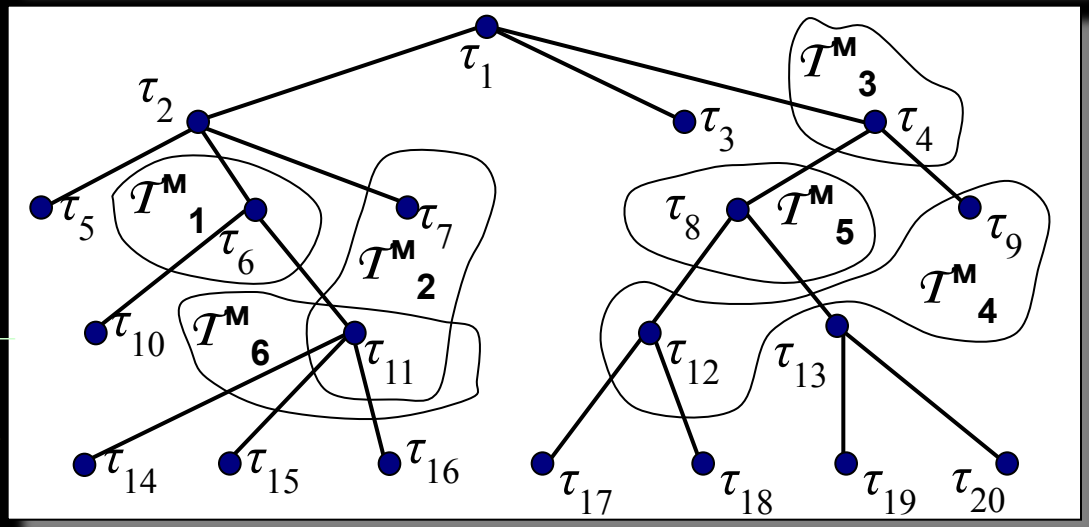
2. Тематическая решетка мультирубрик иерархического рубрикатора

Тематические решетки (продолжение)

3. На иерархическом рубрикаторе при мультирубрицированной классификации

- **решетка $\Lambda_и(I_Р, \subseteq, \cup_{ир}, \cap)$ рубрикаторных идеалов $I_{P2} \subseteq I_{P6}$, $I_{P2} \subseteq I_{P1}$, $I_{P4} \subseteq I_{P3}$, $I_{P5} \subseteq I_{P3}$, $I_{P6} = I_{P1} \cap I_{P2}$, $I_{P3} = I_{P4} \cup_{ир} I_{P5}$**
- **решетка мультирубрик $\Lambda_и(\mathcal{T}^м, \leq_м, \cup_м, \cap_м)$**





Определение 1. *Мультирубрика $\mathcal{T}^м_i$ **доминирует** над мультирубрикой $\mathcal{T}^м_j$ $\{\tau^{(j)}_1, \tau^{(j)}_2, \ldots, \tau^{(j)}_J\} \leq \{\tau^{(i)}_1, \tau^{(i)}_2, \ldots, \tau^{(i)}_I\}$ в том и только в том случае, когда для любого $m=1,\ldots,J$ существует $k=1,\ldots,I$ такое, что $\tau^{(j)}_m \leq \tau^{(i)}_k$ (вершина $\tau^{(j)}_m$ подчинена по корневому дереву вершине $\tau^{(i)}_k$):*

$$\forall\ \tau^{(j)}_m \in \mathcal{T}^м_j,\quad \exists\ \tau^{(i)}_k \in \mathcal{T}^м_i \wedge \tau^{(j)}_m \leq \tau^{(i)}_k$$

$$\mathcal{T}^м_2 \leq_м \mathcal{T}^м_6,\ \mathcal{T}^м_4 \leq_м \mathcal{T}^м_3,\ \mathcal{T}^м_5 \leq_м \mathcal{T}^м_3,$$
$$\mathcal{T}^м_6 = \mathcal{T}^м_1 \cap_м \mathcal{T}^м_2,\quad \mathcal{T}^м_3 = \mathcal{T}^м_4 \cup_м \mathcal{T}^м_5$$

2. Тематическая решетка мультирубрик иерархического рубрикатора

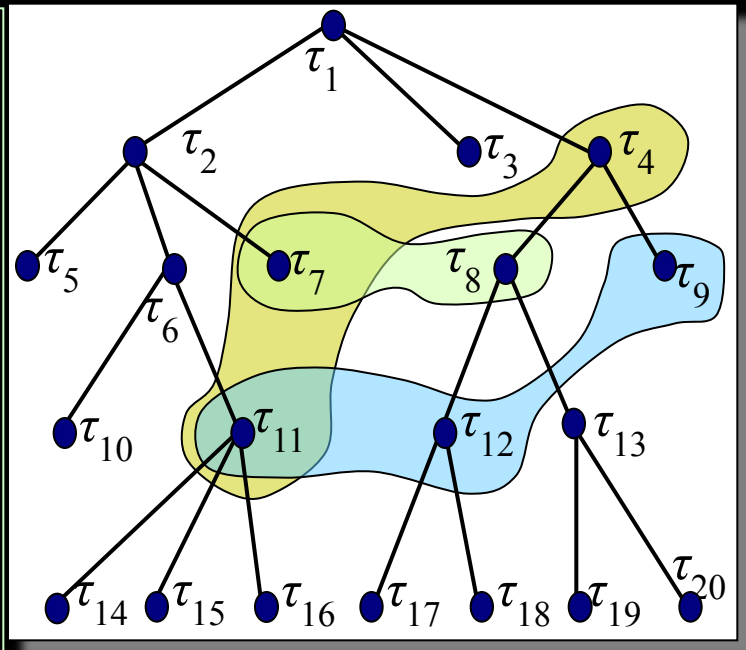
Решетка мультирубрик $\Lambda_{и}(\mathcal{T}^{м}, \leq_{м}, \cup_{м}, \cap_{м})$

Определение 2. ***Объединением*** $\cup_{м}$ *мультирубрик* $\mathcal{T}^{м}_{i}=\{\tau^{(i)}_{1},\tau^{(i)}_{2},\ldots,\tau^{(i)}_{I}\}$ и $\mathcal{T}^{м}_{j}=\{\tau^{(j)}_{1},\tau^{(j)}_{2},\ldots,\tau^{(j)}_{J}\}$ *называется операция формирования множества вершин иерархического рубрикатора* $\mathcal{T}^{м\cup} = \mathcal{T}^{м}_{i} \cup_{м} \mathcal{T}^{м}_{j}$ *на основе следующего алгоритма:*

1) *Формируется теоретико-множественное объединение множеств вершин, составляющих мультирубрики –*
$\mathcal{T}^{\cup} = \{\tau^{(i)}_{1}, \tau^{(i)}_{2},\ldots, \tau^{(i)}_{I}\} \cup \{\tau^{(j)}_{1}, \tau^{(j)}_{2},\ldots, \tau^{(j)}_{J}\}$;

2) *Формируется набор вершин* $\mathcal{T}^{м\cup'}$ *путем исключения из него тех вершин из* $\mathcal{T}^{\cup}$, *которые доминируются хотя бы одной вершиной из того же набора* $\mathcal{T}^{\cup}$ –
$(\tau_{k} \in \mathcal{T}^{\cup} \wedge \tau_{k} \in \mathcal{T}^{м\cup}) \equiv (\exists\, \tau_{m} \in \mathcal{T}^{\cup} \wedge \tau_{m} \leq \tau_{k})$;

3) *Формируется итоговый набор вершин* $\mathcal{T}^{м\cup}$ *путем добавления в него результатов иерархического сжатия по всем подмножествам набора вершин* $\mathcal{T}^{м\cup'}$ *и одновременным исключением соответствующих наборов сыновей при непустом результате сжатия*



$\{\tau_7, \tau_8\} \cup_{м} \{\tau_{11}, \tau_{12}, \tau_9\}$

1) $\{\tau_7, \tau_8, \tau_{11}, \tau_{12}, \tau_9\}$

2) $\{\tau_7, \tau_8, \tau_{11}, \tau_9\}$

3) $\{\tau_{11}, \tau_7, \tau_4\}$

Лемма 1. *Множество рубрик* $\mathcal{T}^{м\cup} = \mathcal{T}^{м}_{i} \cup_{м} \mathcal{T}^{м}_{j}$, *формируемое на основе объединения мультирубрик по определению 2,*

a) *является мультирубрикой;*

b) *доминирует над мультирубриками* $\mathcal{T}^{м}_{i}$ *и* $\mathcal{T}^{м}_{j}$, *т.е.* $\mathcal{T}^{м}_{i} \leq \mathcal{T}^{м\cup} \wedge \mathcal{T}^{м}_{j} \leq \mathcal{T}^{м\cup}$;

c) *является наименьшей верхней границей мультирубрик* $\mathcal{T}^{м}_{i}$ *и* $\mathcal{T}^{м}_{j}$.

2. Тематическая решетка мультирубрик иерархического рубрикатора

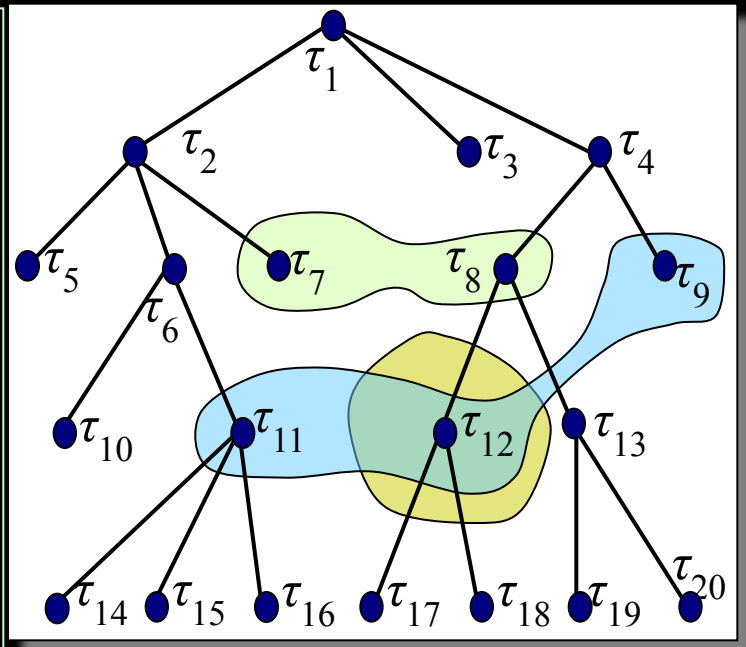
Решетка мультирубрик $\Lambda_{и}(T^{м}, \leq_{м}, \cup_{м}, \cap_{м})$

Определение 3. ***Пересечением*** $\cap_{м}$ *мультирубрик* $T^{м}_{i} = \{\tau^{(i)}_{1}, \tau^{(i)}_{2}, \ldots, \tau^{(i)}_{I}\}$ и $T^{м}_{j} = \{\tau^{(j)}_{1}, \tau^{(j)}_{2}, \ldots, \tau^{(j)}_{J}\}$ *называется операция формирования множества вершин иерархического рубрикатора* $T^{м\cap} = T^{м}_{i} \cap_{м} T^{м}_{j}$ *на основе следующего алгоритма:*

1) *Из множества вершин мультирубрики* $T^{м}_{i} = \{\tau^{(i)}_{1}, \tau^{(i)}_{2}, \ldots, \tau^{(i)}_{I}\}$ *формируются множество вершин* $T^{м'}_{i}$, *которые доминируются хотя бы одной вершиной из множества вершин другой мультирубрики* $T^{м}_{j} = \{\tau^{(j)}_{1}, \tau^{(j)}_{2}, \ldots, \tau^{(j)}_{J}\}$;

2) *Из множества вершин мультирубрики* $T^{м}_{j} = \{\tau^{(j)}_{1}, \tau^{(j)}_{2}, \ldots, \tau^{(j)}_{J}\}$ *формируются множество вершин* $T^{м'}_{j}$, *которые доминируются хотя бы одной вершиной из множества вершин первой мультирубрики* $T^{м}_{i} = \{\tau^{(i)}_{1}, \tau^{(i)}_{2}, \ldots, \tau^{(i)}_{I}\}$;

3) *Формируется теоретико-множественное объединение* $T^{м\cap} = T^{м'}_{i} \cup T^{м'}_{j}$



$\{\tau_7, \tau_8\} \cap_{м} \{\tau_{11}, \tau_{12}, \tau_9\}$

1) $\{\tau_7, \tau_8\} \rightarrow \varnothing$

2) $\{\tau_{11}, \tau_{12}, \tau_9\} \rightarrow \{\tau_{12}\}$

3) $\varnothing \cup \{\tau_{12}\} = \{\tau_{12}\}$

Лемма 2. *Множество рубрик* $T^{м\cap} = T^{м}_{i} \cap_{м} T^{м}_{j}$, *формируемое на основе пересечения мультирубрик по определению 3,*

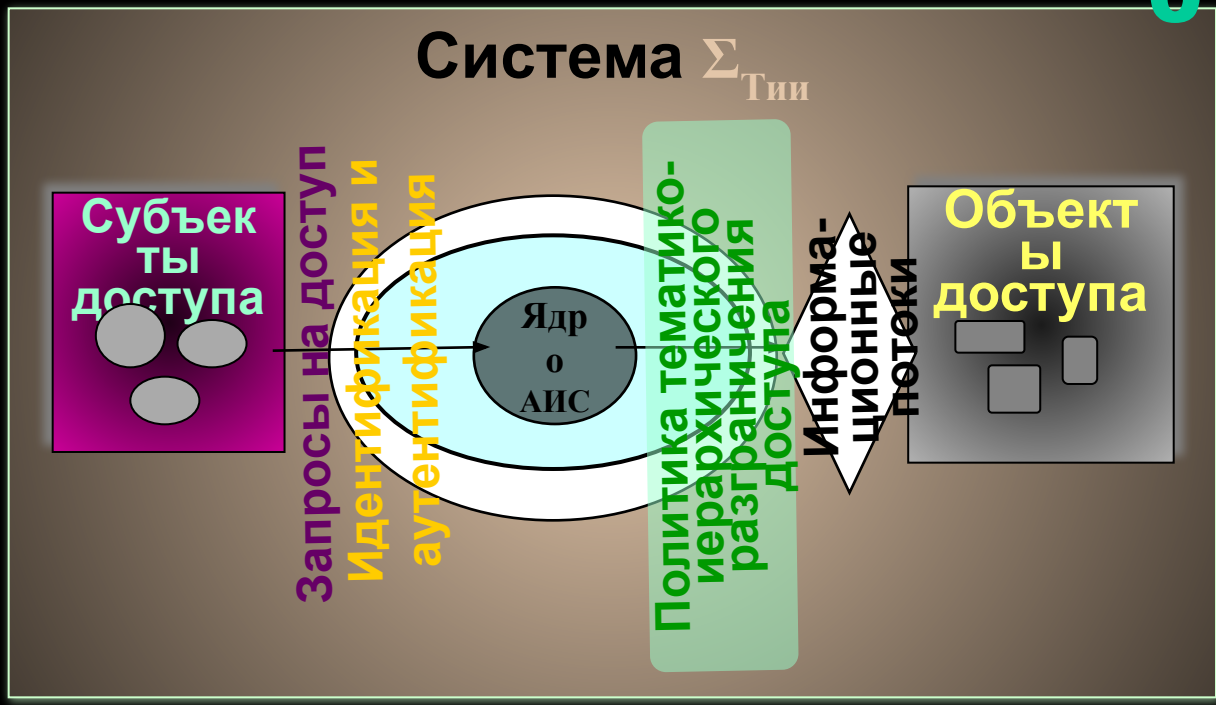
a) является мультирубрикой;

b) доминируется мультирубриками $T^{м}_{i}$ *и* $T^{м}_{j}$, *т.е.* $T^{м\cap} \leq T^{м}_{i} \wedge T^{м\cap} \leq T^{м}_{j}$;

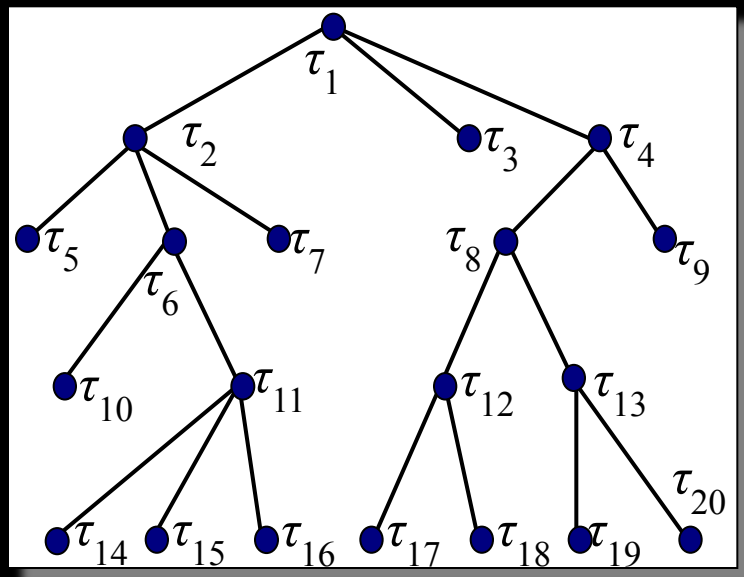
c) является наибольшей нижней границей мультирубрик $T^{м}_{i}$ *и* $T^{м}_{j}$.

3. Модель тематико-иерархического разграничения доступа

1. Компьютерная система $\Sigma_{Тии}$ представляется совокупностью субъектов и объектов доступа. В системе $\Sigma_{Тии}$ действует **МБО**, санкционирующий запросы субъектов на доступ к объектам, и **МБС**, управляющий инициализацией субъектов



2. Информационно-логическая схема предметной области системы $\Sigma_{Тии}$ представляется тематическим иерархическим классификатором (рубрикатором). Рубрикатор включает конечное множество тематических рубрик $T_и = \{\tau_1, \tau_2, \ldots, \tau_M\}$, на котором установлен частичный порядок, задаваемый корневым деревом



3. Модель тематико-иерархического разграничения доступа

3. Множество сущностей системы $X = S \cup O$ тематически классифицируется на основе отображения на множество мультирубрик $T^{м}$, определенных на корневом дереве иерархического рубрикатора.

Существует функция тематического окрашивания $f_{м}$, которая в каждый момент времени для любой сущности системы $x \in X$ определяет соответствующую ей мультирубрику:

$$f_{м}[x] = \mathcal{T}^{м}_{i}, \quad \mathcal{T}^{м}_{i} \in T^{м}.$$

4. **Тематический критерий безопасности.** *Система* $\Sigma_{Тии}$ *безопасна тогда и только тогда, когда в ней отсутствуют потоки следующих видов:*

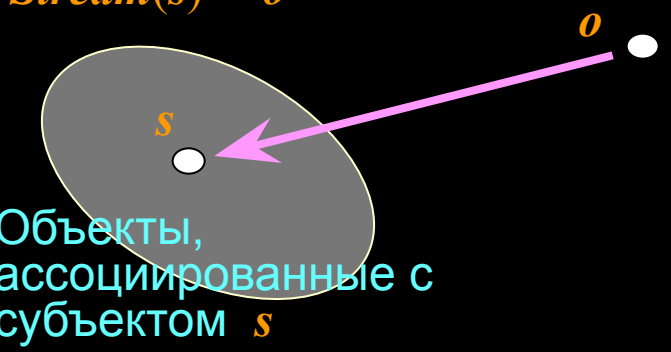
- *от сущностей с более широкой тематикой к сущностям с более узкой тематикой;*
- *между несравнимыми по тематике сущностями.*

3. Модель тематико-иерархического разграничения доступа

5. Переходы системы $\Sigma_{\text{Тии}}$, обусловленные запросами и осуществлением доступов существующих субъектов к существующим объектам, санкционируются МБО на основе следующих правил:

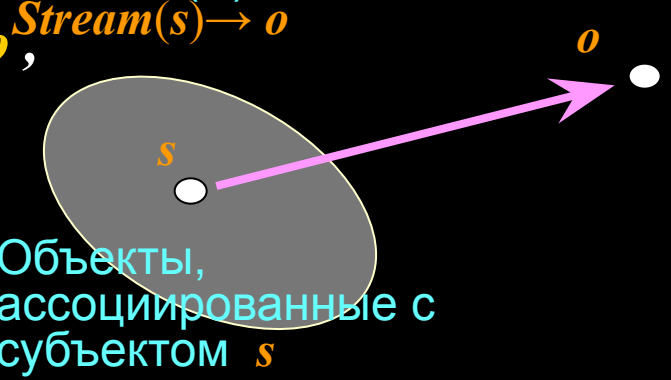
Правило 1. *Доступ субъекта s к объекту o, вызывающий поток по чтению Stream(s)←o , неопасен и может быть МБО разрешен тогда и только тогда, когда мультирубрика субъекта доминирует над мультирубрикой объекта:*

$$f_{\text{м}}[s] \geq f_{\text{м}}[o]$$



Правило 2. *Доступ субъекта s к объекту o, вызывающий поток по записи Stream(s)→o, неопасен и может быть МБО разрешен тогда и только тогда, когда мультирубрика объекта доминирует над мультирубрикой субъекта:*

$$f_{\text{м}}[o] \geq f_{\text{м}}[s]$$



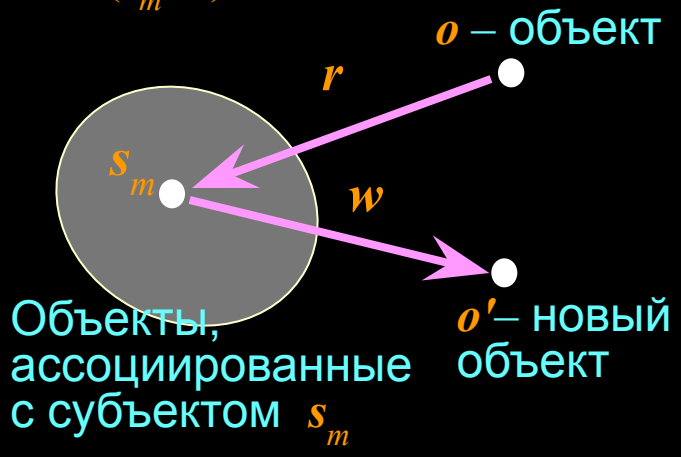
3. Модель тематико-иерархического разграничения доступа

6. Переходы системы $\Sigma_{\text{Тии}}$, связанные с порождением новых объектов и субъектов доступа, санкционируются МБО и МБС на основе следующих правил:

Правило 3. *Порождение субъектом s нового объекта o', в том числе и за счет чтения из другого объекта o, неопасно и может быть МБО разрешено тогда и только тогда, когда мультирубрика субъекта доминирует над мультирубрикой объекта o, при этом МБО присваивает новому объекту o' мультирубрику, равную или доминирующую над мультирубрикой субъекта:*

$$f_{\text{м}}[o] \le f_{\text{м}}[s] \le f_{\text{м}}[o']$$

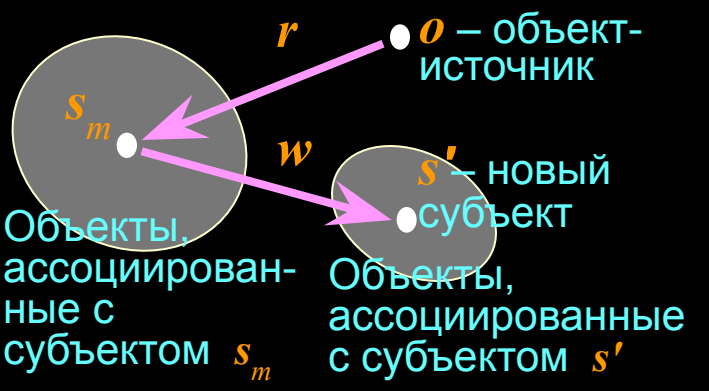
Создание нового объекта $Create(s_m, o) \to o'$



Правило 4. *Инициализация субъектом s нового субъекта s' посредством воздействия на объект источник o неопасна и может быть МБС разрешена тогда и только тогда, когда мультирубрика субъекта доминирует над мультирубрикой объекта-источника, при этом МБС присваивает новому субъекту мультирубрику, тождест-венную мультирубрике инициализирующего субъекта:*

$$f_{\text{м}}[o] \le f_{\text{м}}[s] \equiv f_{\text{м}}[s']$$

Инициализация нового субъекта $Create(s_m, o) \to s'$



3. Модель тематико-иерархического разграничения доступа

7. Переходы системы $\Sigma_{\text{Тии}}$, обусловленные запросами на предоставление множественных доступов, санкционируются МБО на основе следующего правила:

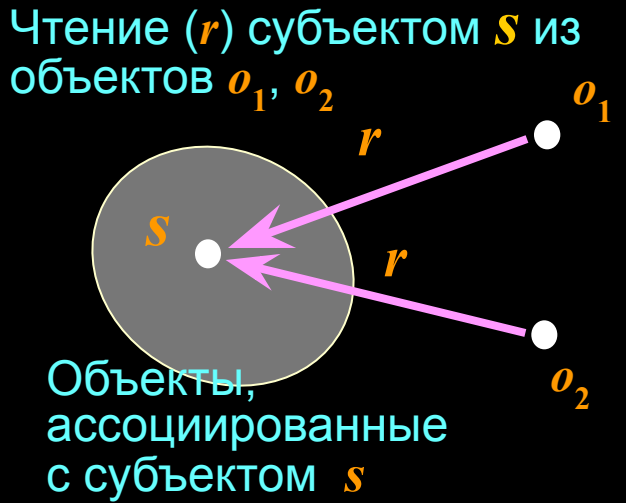
Правило 5. ***Одновременный множественный доступ субъекта s к объектам o_1, o_2,… или субъектов s_1, s_2,… к объекту o может быть разрешен (неопасен) тогда и только тогда, когда выполняются следующие условия:***

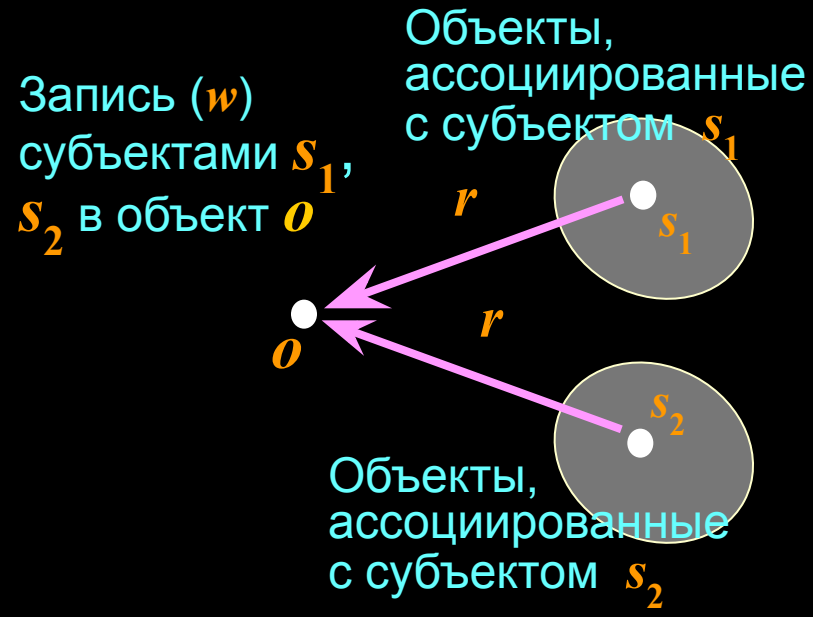
- ***при доступе по чтению***

$$f_{\text{м}}[s] \geq \cup_{\text{м}}\{f_{\text{м}}[o_1], f_{\text{м}}[o_2],\ldots\}$$
$$f_{\text{м}}[o] \leq \cup_{\text{м}}\{f_{\text{м}}[s_1], f_{\text{м}}[s_2],\ldots\}$$

- ***при доступе по записи***

$$f_{\text{м}}[s] \leq \cap_{\text{м}}\{f_{\text{м}}[o_1], f_{\text{м}}[o_2],\ldots\}$$
$$f_{\text{м}}[o] \geq \cap_{\text{м}}\{f_{\text{м}}[s_1], f_{\text{м}}[s_2],\ldots\}$$

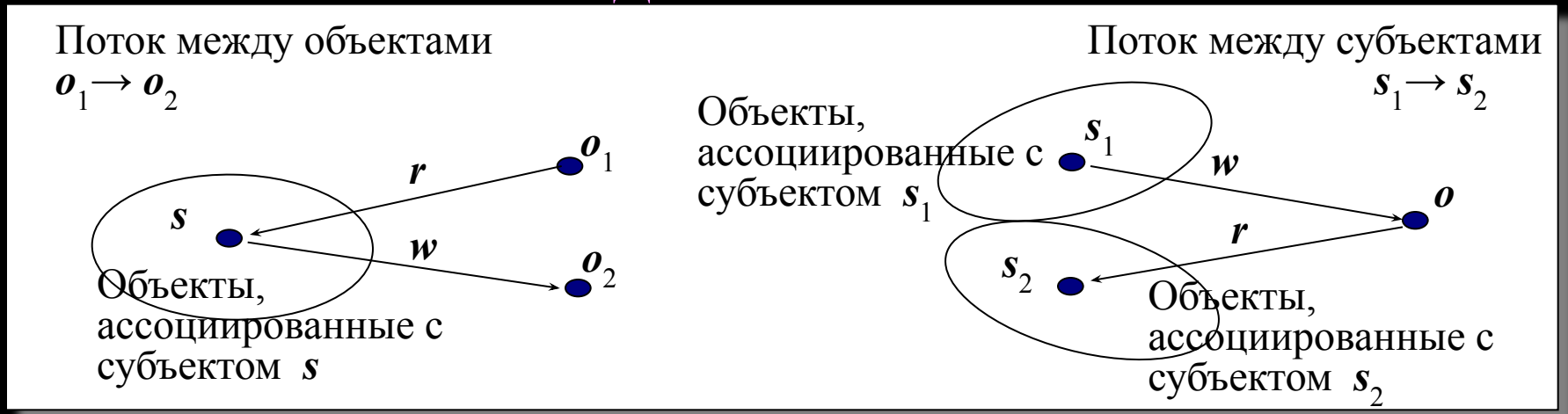




3. Модели тематико-иерархического разграничения доступа

Теорема 1. *В системе $\Sigma_{\text{Тии}}$ с отображением множества субъектов и объектов доступа на множество тематических мультирубрик, в которой доступы санкционируются по правилам 1, 2, 3, 4 и 5, реализуется множество только таких потоков, которые удовлетворяют тематическому* **критерию безопасности**

Доказательство



По условиям теоремы при санкционировании потока $o_1 \to o_2$ имеем:

$$f_{\text{м}}[s] \geq f_{\text{м}}[o_1] \quad \wedge \quad f_{\text{м}}[o_2] \geq f_{\text{м}}[s]$$

Отсюда следует, что: $f_{\text{м}}[o_2] \geq f_{\text{м}}[o_1]$

Аналогично по условиям теоремы при санкционировании потока $s_1 \to s_2$ имеем

$$f_{\text{м}}[s_1] \leq f_{\text{м}}[o] \quad \wedge \quad f_{\text{м}}[s_2] \geq f_{\text{м}}[o] .$$

Отсюда следует, что: $f_{\text{м}}[s_2] \geq f_{\text{м}}[s_1]$

Тема 2. Модели безопасности компьютерных систем

Лекция

Модели безопасности на основе ролевой политики

Учебные вопросы:

1. **Модели ролевого доступа**
2. **Модели индивидуально-группового доступа**
3. **MMS-модель**

1. *Модели ролевого доступа*

Осн. идея:

-политика и система защиты должны учитывать

организационно-технологическое взаимодействие пользователей

Впервые в продуктах управления доступом корп. IBM(70-80.гг.)

Вместо субъекта

- ***пользователь*** (конкретная активная сущность)
- ***роль*** (абстрактная активная сущность)

Неформально ***Роль***: - типовая работа в КС (ИС) определенной группы пользователей

Аналог -нормативное положение, функциональные обязанности и права сотрудников по определенной должности

например м.б. роли- кассира, бухгалтера, делопроизводителя, менеджера и т.п.

Формально ***РОЛЬ*** - активно действующая в КС абстрактная сущность, обладающая логически взаимосвязанным набором полномочий, необходимых для выполнения определенных функциональных обязанностей

- выделенная и обособленная совокупность полномочий над определенной группой или тематикой ресурсов (объектов), имеющая отдельное и самостоятельное значение в предметной области КС (ИС)

1. *Модели ролевого доступа*

Организация доступа в ***две стадии***-

-создаются роли и для каждой из них определяются полномочия

-каждому пользователю назначается список доступных ролей

Система защиты при ролевой политики

U - множество пользователей;

$\mathcal{R}$ - множество ролей;

P - множество полномочий на доступ к объектов;

S - множество сеансов системы

Устанавливаются ***отношения:***

$\mathcal{F}_{P\mathcal{R}}$ - P x $\mathcal{R}$ - отображение множества полномочий на множество ролей, например в виде ролевой матрицы доступа ($A_{p\rho}$)

$\mathcal{F}_{U\mathcal{R}}$ - U x $\mathcal{R}$ - отображение множества пользователей на множество ролей, например, в виде матрицы "пользователи-роли", задающая набор доступных пользователю ролей ($A_{u\rho}$)

1. Модели ролевого доступа

Устанавливаются ***функции:***

f_{user} - $S \rightarrow U$ - для каждого сеанса s функция f_{user} определяет пользователя, который осуществляет этот сеанс работы с системой - $f_{user}(s)=u$

f_{roles} - $S \rightarrow P(\mathcal{R})$ - для каждого сеанса s функция f_{roles} определяет набор ролей, которые могут быть одновременно доступны пользователю в этом сеансе:

$f_{roles}(s)=\{\rho_i \mid (f_{user}(s), \rho_i) \in A_{up}\}$

$f_{permissions}$ - $S \rightarrow P$ - для каждого сеанса s функция $f_{permissions}$ задает набор доступных в нем полномочий, который определяется как совокупность полномочий всех ролей, задействованных в этом сеансе

$f_{permissions}(s)= \bigcup_{\rho \in froles(s)} \{p_i \mid (p_i, \rho) \in A_{pp}\}$

Критерий безопасности:

-система считается безопасной, если любой пользователь, работающий в сеансе s, может осуществить действия, требующие полномочий p, только в том случае , если

$p=f_{permissions}(s)$

1. Модели ролевого доступа

Ролевая политика – особый тип политики, основанный на ***компромиссе*** между ***гибкостью*** *управлением доступа* ***дискреционных*** *моделей и* ***жесткостью*** *правил контроля доступа* ***мандатных*** *моделей*

Разновидности *ролевых моделей определяется особенностями функций* f_{user}, f_{roles}, $f_{permissions}$, *и ограничений, накладываемых на отношения* A_{pp} *и* A_{up}

Наиболее распространены модели с ***иерархической организацией ролей***

-чем выше роль по иерархии, тем больше полномочий

-если пользователю присвоена какая-то роль, то ему автоматически присваиваются все роли ниже по иерархии

Отношения и функции при иерархической организации ролей

Отношения:

F^h_{RR} - $R \times R$ - частичное отношение порядка на множестве R, которое определяет иерархию ролей и задает на множестве R оператор доминирования $\geq$, такой, что если $\rho_1 \geq \rho_2$, то роль ρ_1 находится выше по иерархии, чем роль ρ_2

F^h_{UR} - $U \times R$ - назначает каждому пользователю набор ролей, причем вместе с каждой ролью в него (набор ролей) включаются все роли, подчиненные ей по иерархии, т.е. для $\forall \rho, \rho' \in R, u \in U: \rho \geq \rho' \wedge (u,\rho) \in A^h_{u\rho} \Rightarrow (u,\rho') \in A^h_{u\rho}$

Функции:

f^h_{roles} - $S \rightarrow (R)$ – назначает каждому сеансу s определяет набор ролей из иерархии ролей пользователя, работающего в этом сеансе: $f^h_{roles}(s)=\{\rho_i \mid (\exists \rho' \geq \rho_i (f_{user}(s), \rho') \in A^h_{u\rho})\}$

$f^h_{permissions}$ - $S \rightarrow P$ – определяет полномочия сеанса s как совокупность полномочий всех задействованных пользователем в нем ролей и полномочий всех ролей, подчиненных им: $f^h_{permissions}(s)= \cup_{\rho \in f^h_{roles}(s)} \{p_i \mid (\exists \rho'' \leq \rho (p_i,\rho'') \in A_{p\rho})\}$

Агрегация прав при иерархической организации ролей (виды отношения $\mathcal{F}_{PR}$)

- строго таксономический листовой подход;
- нетаксономический листовой подход;
- иерархически охватный подход

Строго таксономический листовой подход

$$\mathcal{F}^h_{PR}(\rho^{л}_j) = \{P^{(j)}_1, P^{(j)}_2, \dots\},$$

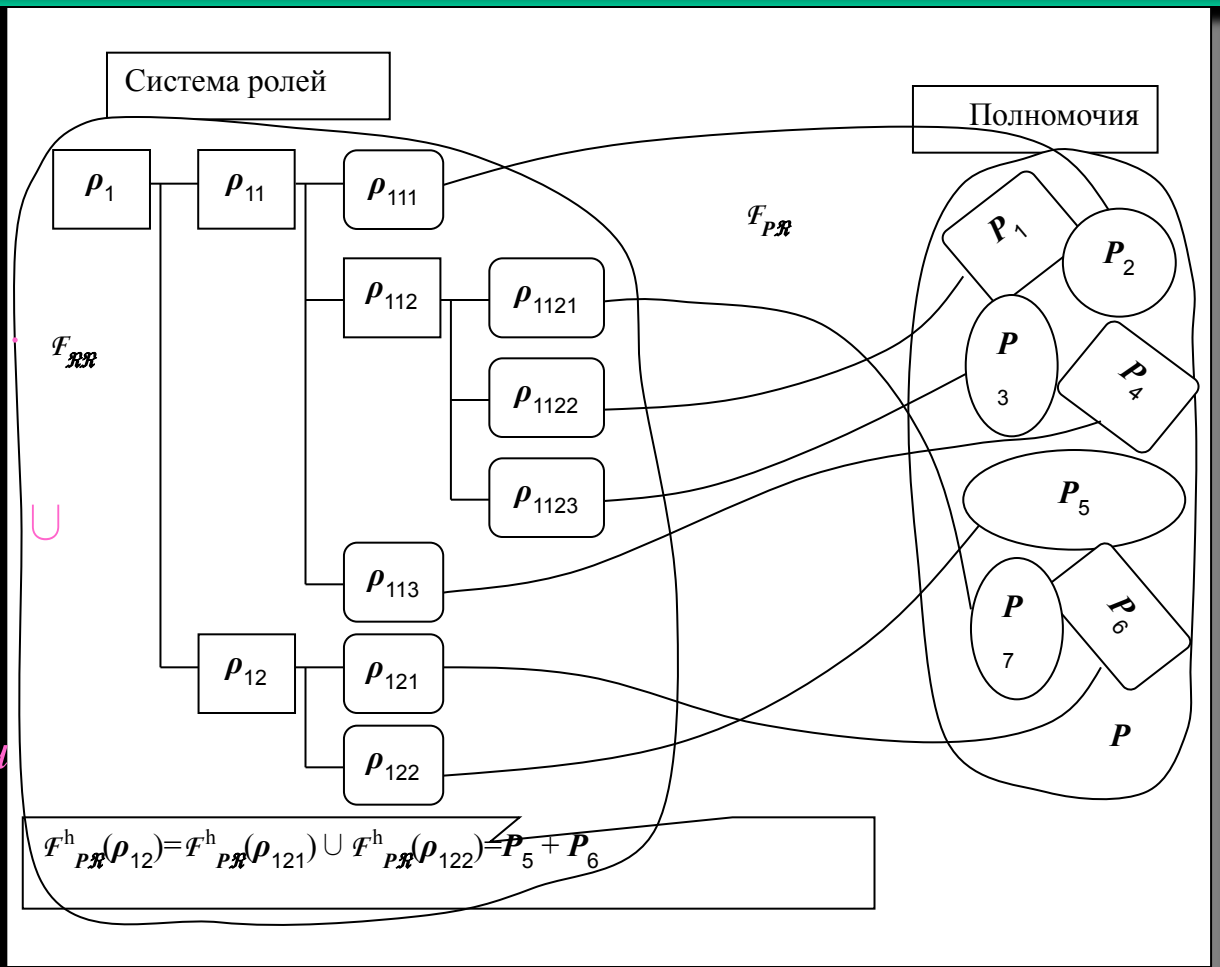
$$\mathcal{F}^h_{PR}(\rho^{л}_j) \cap \mathcal{F}^h_{PR}(\rho^{л}_i) \cap \dots = \varnothing,$$

$$\mathcal{F}^h_{PR}(\rho^{л}_j) \cup \mathcal{F}^h_{PR}(\rho^{л}_i) \cup \dots = P.$$

$$\mathcal{F}^h_{PR}(\rho^{и}_k) = \mathcal{F}^h_{PR}(\rho^{(k)}_i) \cup \mathcal{F}^h_{PR}(\rho^{(k)}_j) \cup \dots,$$

где $\{\rho^{(k)}_i, \rho^{(k)}_j, \dots\}$ *– полный набор ролей-сыновей для роли* $\rho^{и}_k$.

$$\mathcal{F}^h_{PR}(\rho^{и}_1) = P$$



Агрегация прав при иерархической организации ролей (виды отношения $\mathcal{F}_{PR}$)

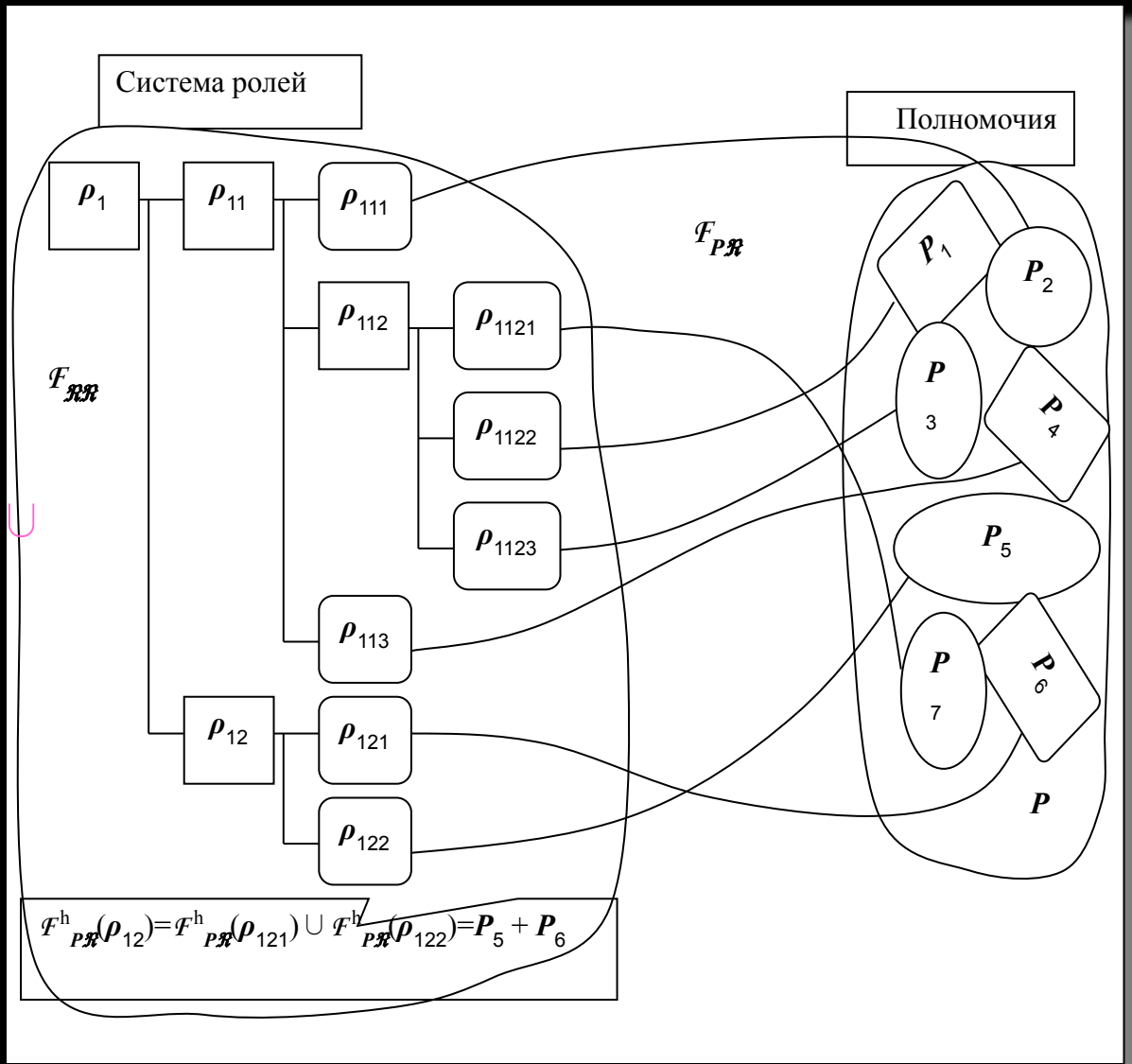
Нетаксономический листовой подход

$$\mathcal{F}^h_{PR}(\rho^{л}_j) = \{p^{(j)}_1, p^{(j)}_2, \dots\},$$

$$\mathcal{F}^h_{PR}(\rho^{л}_j) \cap \mathcal{F}^h_{PR}(\rho^{л}_i) \cap \dots \neq \varnothing,$$

$$\mathcal{F}^h_{PR}(\rho^{и}_k) = \mathcal{F}^h_{PR}(\rho^{(k)}_i) \cup \mathcal{F}^h_{PR}(\rho^{(k)}_j) \cup \dots,$$

где $\{\rho^{(k)}_i, \rho^{(k)}_j, \dots\}$ *– полный набор ролей-сыновей для роли* $\rho^{и}_k$.



Агрегация прав при иерархической организации ролей (виды отношения F_{PR})

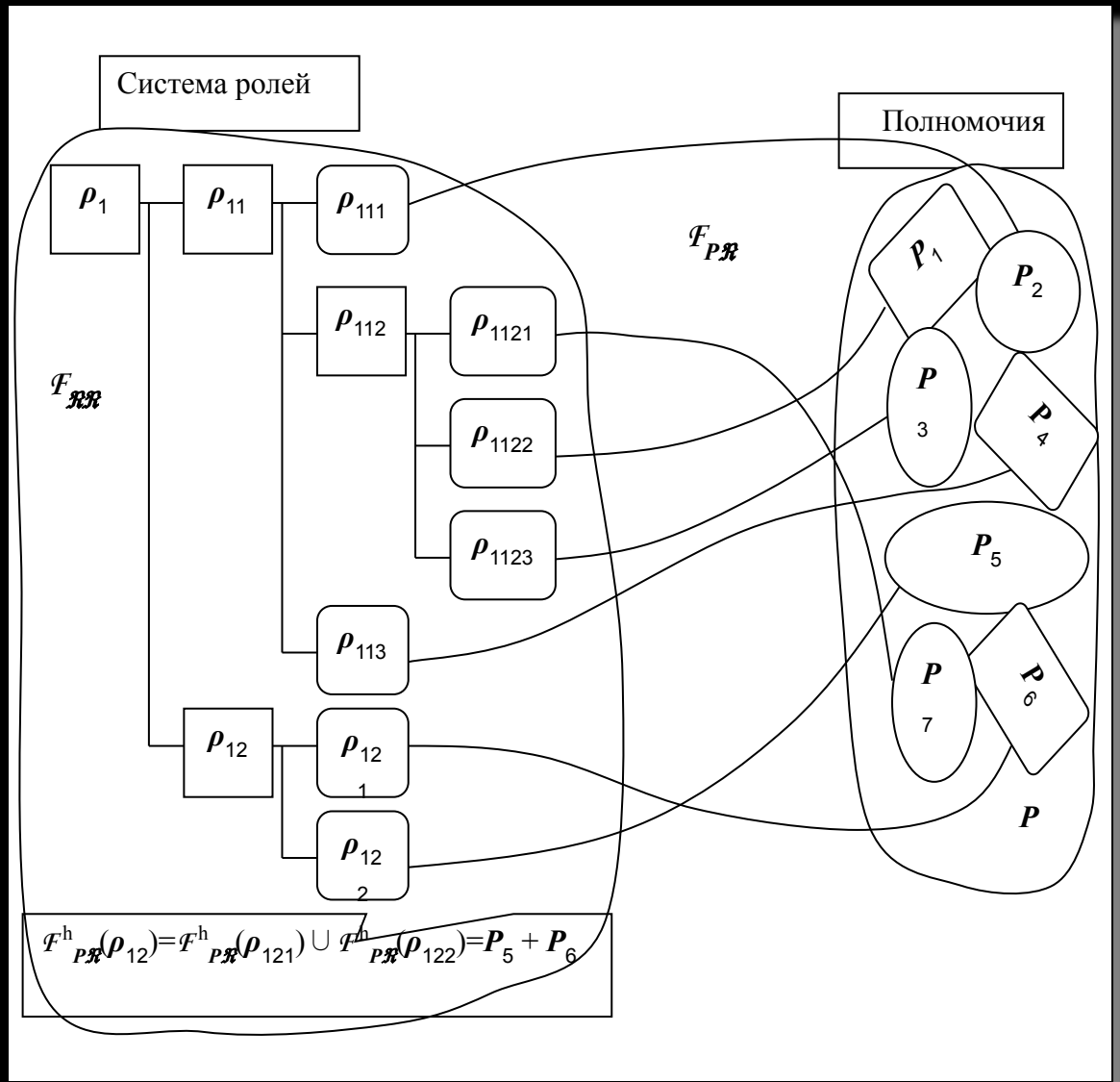
Иерархически охватный подход

$$F^h_{PR}(\rho^{л}_j) = \{p^{(j)}_1, p^{(j)}_2, \dots\},$$

$$F^h_{PR}(\rho^{л}_j) \cap F^h_{PR}(\rho^{л}_i) \cap \dots \neq \varnothing,$$

$$F^h_{PR}(\rho^{и}_k) \cap F^h_{PR}(\rho_i) = \varnothing,$$

где $\{\rho^{и}_k \geq \rho_i\}$.



Другие разновидности организации ролей

Взаимоисключающие роли

т.н. ***статическое разделение обязанностей***

- множество ролей разбивается на подмножества, объединяющие роли, которые не м.б. назначены одновременно одному пользователю (z.b. "кассир"-"контроллер"). Задается функция $f_{exclusive}: \mathcal{R} \rightarrow P(\mathcal{R})$, которая для каждой роли определяет множество несовместимых с ней ролей.

Ограничения на одновременное использование ролей в одном сеансе

т.н. ***динамическое разделение обязанностей***

- множество ролей разбивается на подмножества, несовместимых ролей(z.b. "администратор"-"аудитор"). В ходе одного сеанса пользователь может активизировать из каждого подмножества не более одной роли.

Количественные ограничения по назначению ролей одному пользователю

Групповое назначение ролей одному пользователю

- роль м.б. назначена тогда, когда одновременно назначена еще группа обязательных для данной роли других ролей

2. Модели индивидуально-группового доступа

1. КС представляется совокупностью следующих наборов сущностей:

множества объектов доступа $O\ (o_1, o_2, \ldots, o_M)$;

множества пользователей $U\ (u_1, u_2, \ldots, u_N)$;

множества рабочих групп пользователей $G\ (g_1, g_2, \ldots, g_K)$;

множества прав доступа и привилегий $R\ (r_1, r_2, \ldots, r_J)$;

матрицей доступа A размерностью $((N+K) \times M)$, каждая ячейка которой специфицирует права доступа и привилегии пользователей или их рабочих групп к объектам из конечного набора прав доступа и привилегий $R\ (r_1, r_2, \ldots, r_J)$, т. е. $A[u, o] \subseteq R$, $A[g, o] \subseteq R$.

Определение. **Рабочей группой** называется совокупность пользователей, объединенных едиными правами доступа к объектам и (или) едиными привилегиями (полномочиями) выполнения определенных процедур обработки данных

Рабочая группа в отличие от роли не является самостоятельным субъектом доступа

$A=$

Группы Пользователи	Объекты o_1	o_2	. . .			o_M
u_1						
u_2						
				a_{ij}		
u_N						
g_1						
g_K						

2. Модели индивидуально-группового доступа

2. Групповые отношения в системе устанавливаются отображением множества пользователей на множество рабочих групп:

$\mathcal{F}_{UG} : U \times G$ – такое, что одна рабочая группа объединяет нескольких пользователей, а один пользователь может входить в несколько рабочих групп.

$f_{groups}: U \rightarrow G$ – значением функции $f_{groups}(u) = G$ является набор рабочих групп $G = \{g_{u1}, g_{u2}, \ldots\} \subseteq G$, в которые пользователь u включен по отображению $\mathcal{F}_{UG}$;

$f_{users}: G \rightarrow U$ – значением функции $U = f_{users}(g)$ является набор пользователей $U = \{u_{g1}, u_{g2}, \ldots\} \subseteq U$, которые рабочая группа g включает по отношению $\mathcal{F}_{UG}$.

Отношение «Пользователи-группы» - «многие-ко-многим»

$W =$

Пользователи \ Рабочие группы	g_1	g_2	. . .			g_K
u_1		0				
u_2						
				1		
u_N						

2. Модели индивидуально-группового доступа

3. Управление индивидуально-групповым доступом в системе осуществляется на основе следующего правила (критерия безопасности) индивидуально-группового доступа.

Критерий безопасности индивидуально-группового доступа: *Система функционирует безопасно, если и только если любой пользователь* $u \in U$ *по отношению к любому объекту* $o \in O$ *может осуществлять доступ с правами* $\mathcal{R}$*, не выходящими за пределы совокупности индивидуальных прав* $A[u,o]$ *и прав рабочих групп* $A[g^u_i,o]$*, в которые пользователь входит по отношению* $\mathcal{F}_{UG}$:

$$\mathcal{R} \subseteq \{A[u,o] \cup A[g^u_1, o] \cup A[g^u_2, o] \cup \ldots\},$$

где $\{ g^u_1, g^u_2, \ldots\} = f_{\text{groups}}(u)$.

Разделение процесса функционирования на КС не является существенным, поскольку пользователь всегда получает полномочия всех групп, в которые входит

2. *Модели индивидуально-группового доступа*

4. Членами рабочих групп могут быть *коллективные члены*, т.е. другие рабочие группы. Вхождение одних групп в другие д.б. *транзитивно*, *антисимметрично* и *рефлексивно*:

$\mathcal{F}_{GG} : G \times G$ - отношение частичного порядка, определяющее иерархию (вложенность) рабочих групп и задающее оператор доминирования $\geq$ такое, что

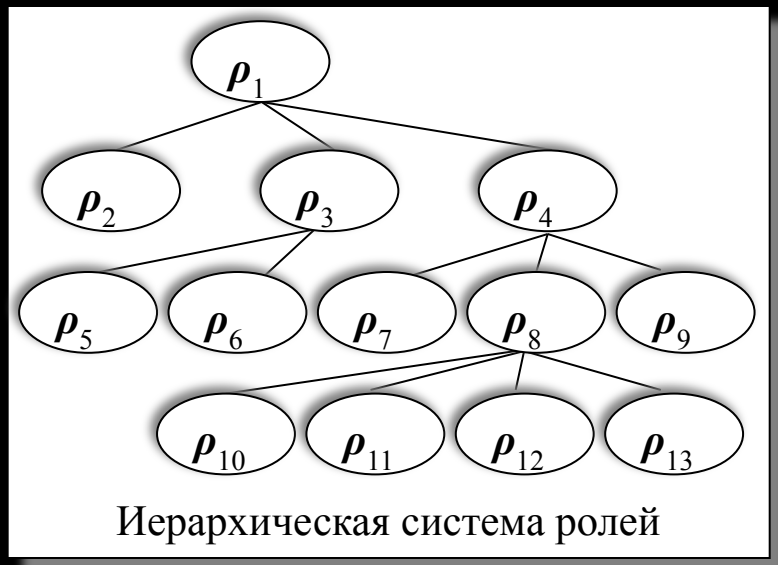
если для $g_1, g_2 \in G$, $g_1 \geq g_2$, то g_1 включает g_2 .

$f_{\text{hgroups}} : G \to G$ – значением функции $f_{\text{groups}}(g)$ является набор рабочих групп $\{g_{g1}, g_{g2}, \ldots\} \subseteq G$, в которые рабочая группа g включена по отношению $\mathcal{F}_{GG}$.

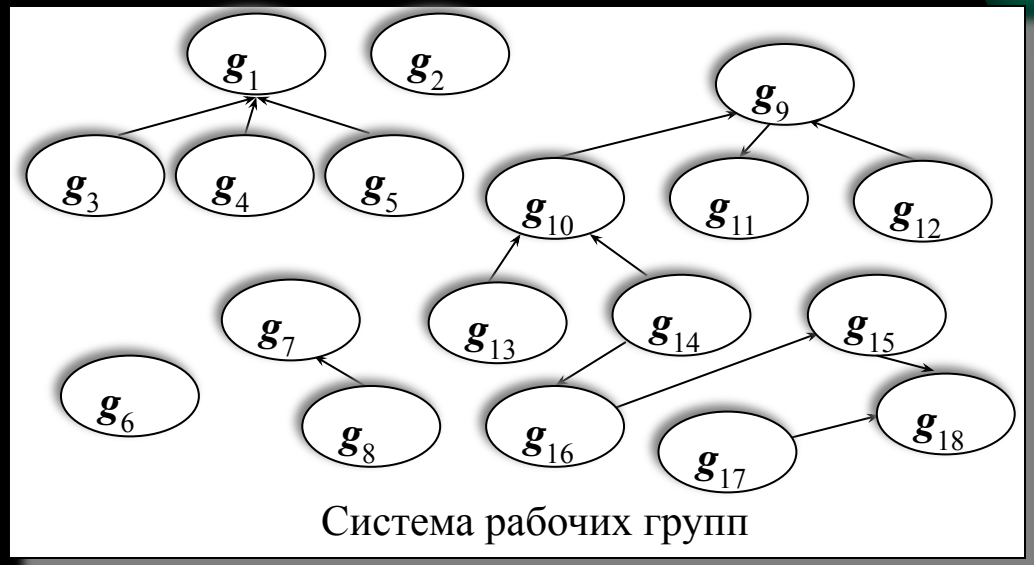
Наследование прав по групповой иерархии происходит «сверху-вниз»

$\mathcal{R}_g = A[g,o] + A[g_{g1},o] + A[g_{g2},o] + \ldots$, где $\{g_{g1}, g_{g2}, \ldots\} = f_{\text{groups}}(g)$

2. *Модели индивидуально-группового доступа*



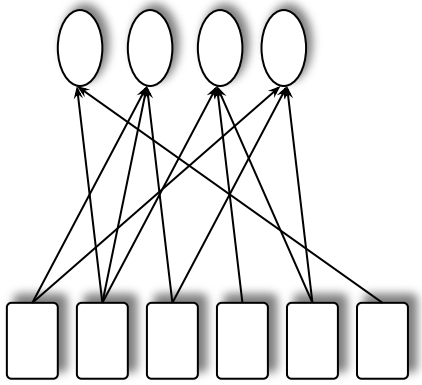
Иерархическая система ролей



Система рабочих групп

5. На графе вхождения одних групп в другие не должно быть циклов

Теоретико-графовые методы поиска циклов, в т.ч. по матрице смежности



Группы, которые не могут входить в другие группы, но могут включать как пользователей, так и группы

Группы, включающие только пользователей

3. *MMS (military message system)-модель*

Лендвер, МакЛин, 1984г.

Определения MMS-модели (*формализация системы защиты*)

Классификация- обозначение, накладываемое на информацию, отражающее ущерб, который м.б. причинен неавторизованным доступом (TOP SECRET, SECRET, + возможно дополн. функц. разгр. - CRYPTO, NUCLEAR и т.п.)

Степень доверия пользователю- уровень благонадежности персоны (иначе допуск пользователя) - априорно заданная характеристика

Пользовательский идентификатор- строка символов, используемая для того, чтобы отметить пользователя в системе. Для использования системы пользователь д. предъявить ей идентификатор, система должна провести аутентификацию пользователя (login)

Пользователь- персона, уполномоченная для использования системы

Роль - работа, исполняемая пользователем. Пользователь в любой момент времени (после login до logon) всегда ***ассоциирован*** как минимум с одной ролью из нескольких. Для действий в данной роли пользователь д.б. ***уполномочен***. Некоторые роли в конкр. момент времени м.б. связаны *только с одним пользователем*. С любой ролью связана способность выполнения определенных ***операций***

Объект- одноуровневый блок информации. Это минимальный блок информации в системе, который м. иметь классификацию, т.е. м.б. раздельно от других поименован. Объект не содержит других объектов (т.е. он не многоуровневый)

3. *MMS (military message system)-модель*

Определения MMS-модели (продолжение)

Контейнер- многоуровневая информационная структура. Имеет классификацию и м. содержать объекты (со своей классификацией) и др. контейнеры (также со своей классификацией)

Сущность- объект или контейнер

Требование степени доверия объектов- атрибут некоторых контейнеров. Для некоторых контейнеров важно требовать минимум степени доверия, т.е. пользователь, не имеющий соответствующего уровня благонадежности, не может просматривать содержимое контейнера. Такие контейнеры помечаются соотв. атрибутом.

Идентификатор (ID)- имя сущности без ссылки на другие сущности

Ссылка на сущность ***прямая-*** если это идентификатор сущности

Ссылка на сущность ***косвенная-*** если это последовательность двух и более идентификаторов (имен) сущностей, первая из которых - контейнер.

Операция- функция, которая м.б. применена к сущности (читать, модифицировать и т.д.). Некоторые операции м. использовать более одной сущности (z.b. Copy)

Множество доступа- множество троек (*Пользовательский идентификатор* или *роль* - *Операция* - *Индекс операнда*), которое связано с сущностью (т.е. дескрипторы доступа объекта)

3. *MMS (military message system)-модель*

Основная схема функционирования системы -пользователи после ***идентификации*** запрашивают у системы операции над сущностями от своего ***ID*** или от имени ***Роли***, с которой в данный момент ***авторизованы***

Система функционирует безопасно, если

-пользователи ведут себя корректно (не компрометируют систему) на основе некоторых предположений

- система защиты (монитор безопасности) реализует определенные ограничения политики безопасности)

Предположения MMS-модели*,которым д. следовать* ***пользователи*** *системы*

A1. Администратор безопасности корректно присваивает уровни доверия, классификацию устройств и правильные множества ролей

A2. Пользователь определяет корректную классификацию, когда вводит, изменяет, объединяет или переклассифицирует информацию

A3. В пределах установленной классификации пользователь классифицирует сообщения (информацию) и определяет набор (множество) доступа (роли,операции,требуемые степени доверия) для сущностей, которые он создает

A4. Пользователь должным образом контролирует информацию объектов, требующих благонадежности

3. *MMS (military message system)-модель*

Ограничения безопасности в MMS-модели

B1. Авторизация - пользователь м. запрашивать операции над сущностями, если только пользовательский идентификатор или его текущая роль присутствуют в множестве доступа сущностей вместе с этой операцией и с этим значением индекса, соответствующим позиции операнда,в которой сущность относят в требуемой операции

B2. Классификационная иерархия - классификация контейнера всегда больше или равна классификации сущностей, которые он содержит

B3. Изменения в объектах - информация, переносимая из объекта всегда содержит классификацию объекта. Информация, вставляемая в объект, должна иметь классификацию ниже классификации этого объекта (аналог NWD)

B4. Просмотр - пользователь может просматривать (на некотором устройстве вывода) только сущности с классификацией меньше, чем классификация устройства вывода и степень доверия контейнера устройства вывода к пользователям (аналог NRU + NRUустроств)

B5. Доступ к объектам, требующим степени доверия - пользователь может получить доступ к косвенно адресованной сущности внутри контейнера, требующего степени доверия, если только его степень доверия не ниже классификации контейнера

B6. Преобразование косвенных ссылок - пользовательский индикатор признается законным для сущности, к которой он обратился косвенно, если только он авторизован для просмотра этой сущности через ссылку

3. *MMS (military message system)-модель*

Ограничения безопасности в MMS-модели (*продолжение*)

B7. Требование меток - сущности, просмотренные пользователем, д.б. помечены его степенью доверия (т.е. впоследствии они ему доверяют)

B8. Установка степеней доверия, ролей, классификация устройств - только пользователь с ролью администратора безопасности системы м. устанавливать данные значения. Текущее множество ролей пользователя м.б. изменено только администратором безопасности системы или самим же этим пользователем

B9. Понижение классификации информации - никакая классифицированная информация не м.б. понижена в уровне своей классификации, за исключением случая, когда эту операцию выполняет пользователь с ролью "Пользователь, уменьшающий классификацию информации"

B10. Уничтожение - операция уничтожения информации проводится только пользователем с ролью "Пользователь, уничтожающий информацию"

Модель Лендвера-Маклина (MMS) сочетает принципы:

ролевого, дискреционного и мандатного принципов и оказывает сильное влияние на модели и технологии современных защищенных КС