

Лекция 7

Модели безопасности на основе ролевой политики

Модели ролевого доступа

Основная Идея: *«политика и система защиты должны учитывать организационно-технологическое взаимодействие пользователей»*

Вместо субъекта: **пользователь** (конкретная активная сущность) и **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)

Модели ролевого доступа

Система защиты при ролевой политике

U - множество пользователей;

$\mathcal{R}$ - множество ролей;

P - множество полномочий на доступ к объектов;

S - множество сеансов системы

Устанавливаются *отношения*:

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

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

Модели ролевого доступа

Система защиты при ролевой политике

U - множество пользователей;

$\mathcal{R}$ - множество ролей;

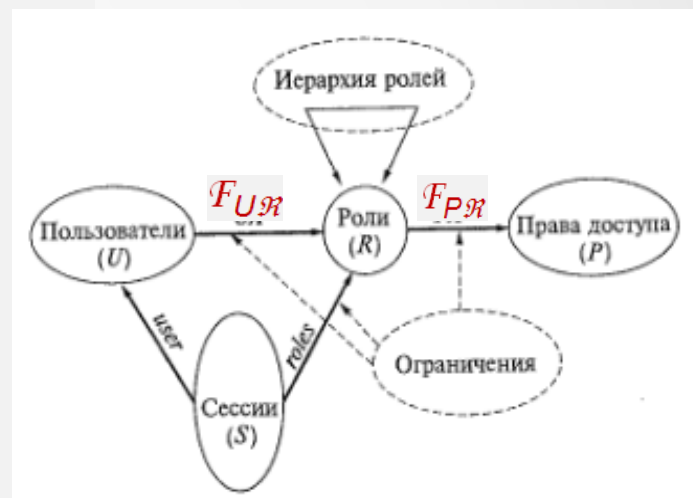
P - множество полномочий на доступ к объекту;

S - множество сеансов системы

Устанавливаются отношения:

$F_{P\mathcal{R}}$ - $P \times \mathcal{R}$ - отображение множества полномочий на множество ролей, например в виде ролевой матрицы доступа (A_{pr})

$F_{U\mathcal{R}}$ - $U \times \mathcal{R}$ - отображение множества пользователей на множество ролей, например, в виде матрицы "пользователи-роли", задающая набор доступных пользователю ролей (A_{ur})



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 - $f_{user}(s) = u$

$f_{roles} - S \rightarrow \mathcal{R}$ - для каждого сеанса s функция f_{roles} определяет набор ролей, которые могут быть одновременно доступны пользователю в этом сеансе: $f_{roles}(s) = \{\rho_i \mid (f_{user}(s), \rho_i) \in A_{u\rho}\}$

$f_{permissions} - S \rightarrow P$ - для каждого сеанса s функция $f_{permissions}$ задает набор доступных в нем полномочий, который определяется как совокупность полномочий всех ролей, задействованных в этом сеансе $f_{permissions}(s) = \bigcup_{\rho \in f_{roles}(s)} \{p_i \mid (p_i, \rho) \in A_{p\rho}\}$

Модели ролевого доступа

Критерий безопасности:

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

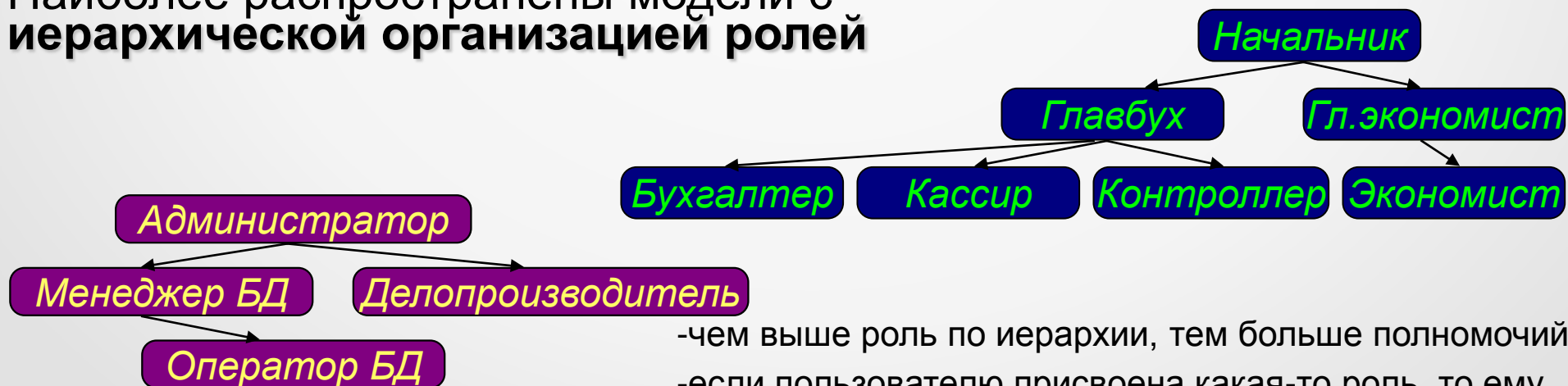
$$p = f_{permissions}(s)$$

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_{rp} и A_{ur}

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

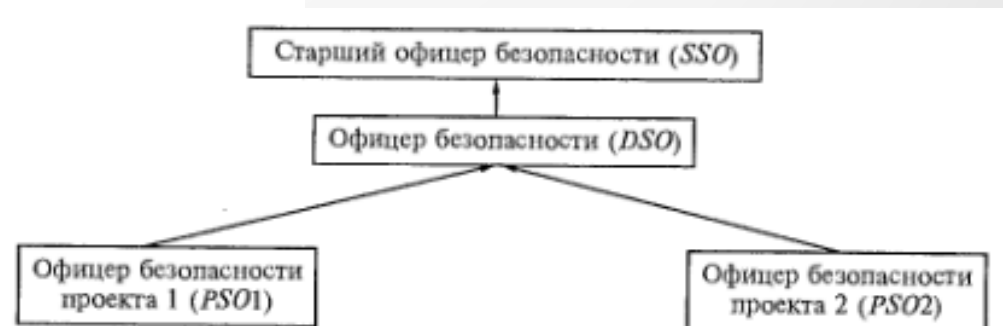
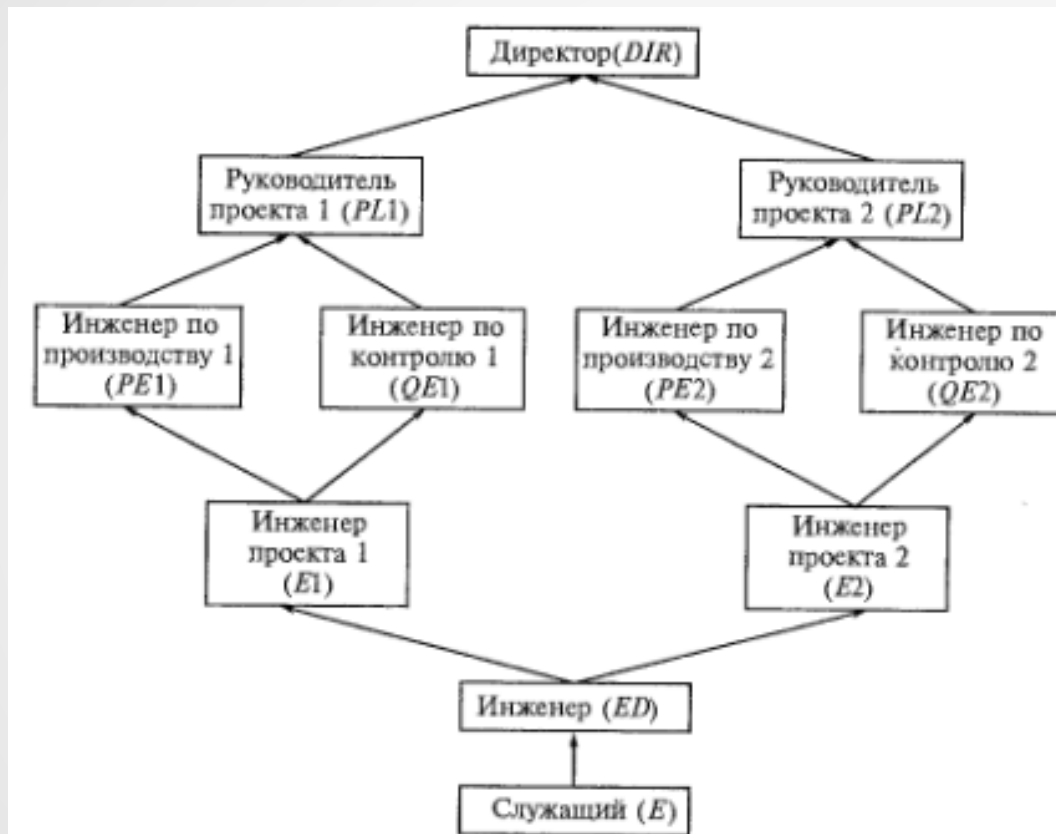
Отношения:

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

$F^h_{U\mathcal{R}}$ - $U \times \mathcal{R}$ - назначает каждому пользователю набор ролей, причем вместе с каждой ролью в него (набор ролей) включаются все роли, подчиненные ей по иерархии, т.е. для

$$\forall \rho, \rho' \in \mathcal{R}, u \in U: \rho \geq \rho' \wedge (u, \rho) \in A^h_{u\rho} \Rightarrow (u, \rho') \in A^h_{u\rho}$$

Отношения и функции при иерархической организации ролей



Отношения и функции при иерархической организации ролей

Функции:

$f^h_{roles} - S \rightarrow \mathcal{R}$ – 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 $F_{P\mathcal{R}}$)

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

Строго таксономический листовой подход

$$F_{P\mathcal{R}}^h(\rho^{\pi_j}) = \{\rho^{(j)}_1, \rho^{(j)}_2, \dots\},$$

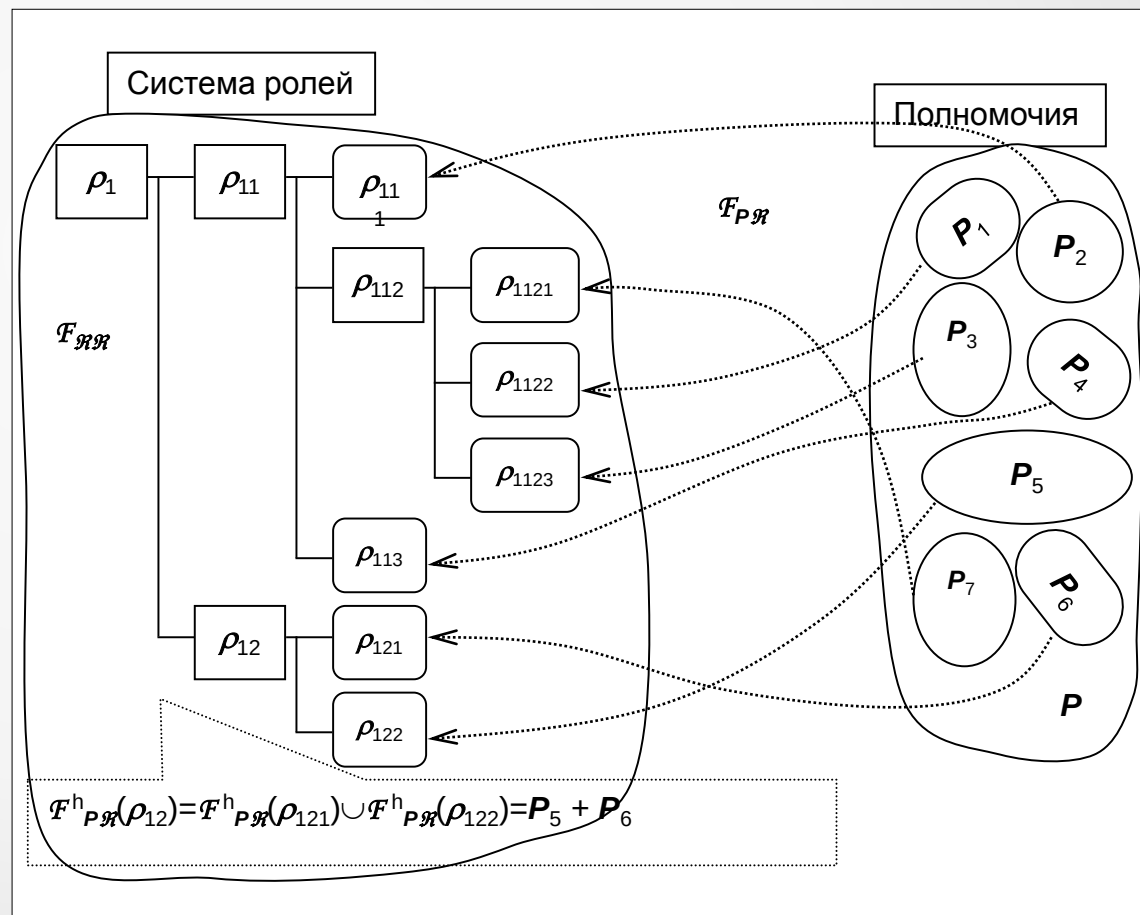
$$F_{P\mathcal{R}}^h(\rho^{\pi_j}) \cap F_{P\mathcal{R}}^h(\rho^{\pi_j}) \cap \dots = \emptyset,$$

$$F_{P\mathcal{R}}^h(\rho^{\pi_j}) \cup F_{P\mathcal{R}}^h(\rho^{\pi_j}) \cup \dots = P.$$

$$F_{P\mathcal{R}}^h(\rho^{\pi_k}) = F_{P\mathcal{R}}^h(\rho^{(k)}_i) \cup \\ \cup F_{P\mathcal{R}}^h(\rho^{(k)}_j) \cup \dots,$$

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

$$F_{P\mathcal{R}}^h(\rho^{\pi_1}) = P$$



Агрегация прав при иерархической организации ролей (виды отношения $F_{P\mathcal{R}}$)

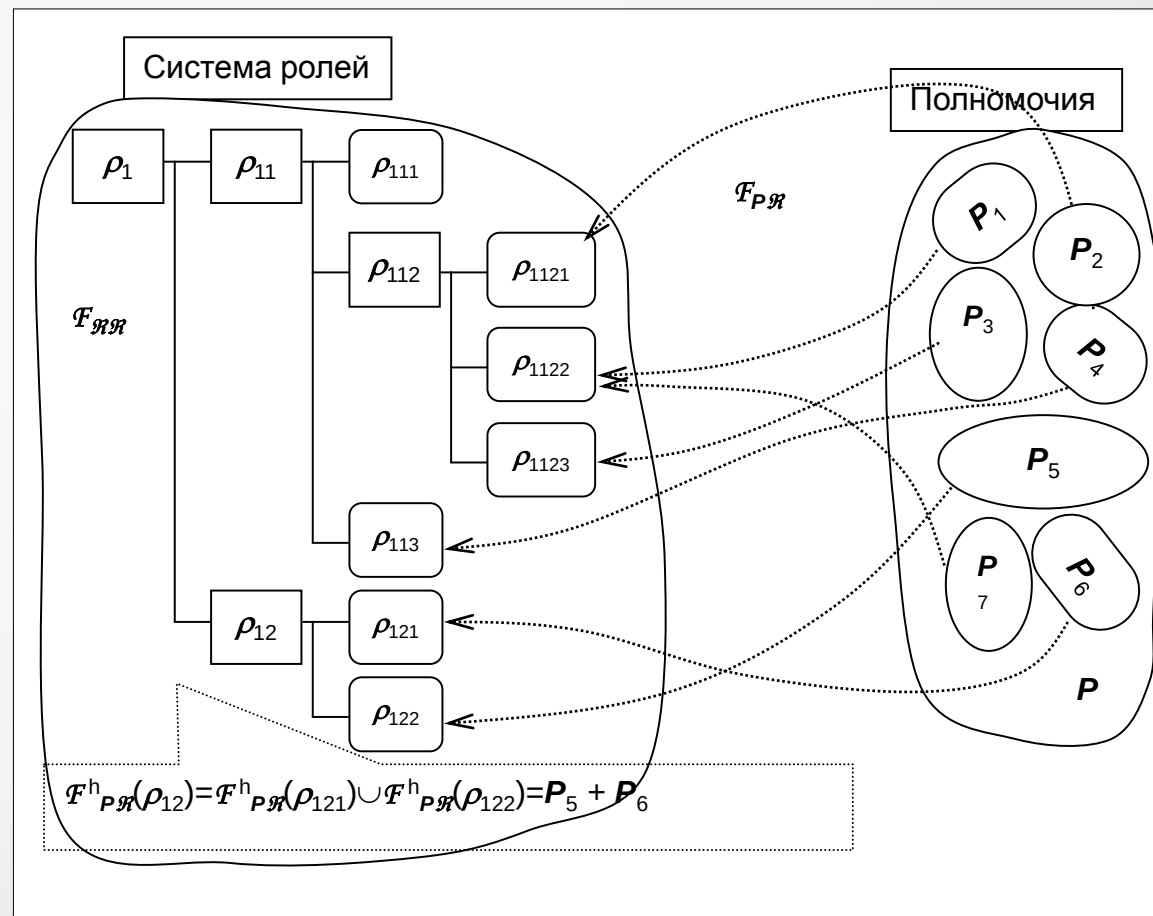
Нетаксономический листовой подход

$$F_{P\mathcal{R}}^h(\rho^{\Pi_j}) = \{\rho^{(j)}_1, \rho^{(j)}_2, \dots\},$$

$$F_{P\mathcal{R}}^h(\rho^{\Pi_j}) \cap F_{P\mathcal{R}}^h(\rho^{\Pi_i}) \cap \dots \neq \emptyset$$

$$F_{P\mathcal{R}}^h(\rho^{\Pi_k}) = F_{P\mathcal{R}}^h(\rho^{(k)}_i) \cup \\ \cup F_{P\mathcal{R}}^h(\rho^{(k)}_j) \cup \dots,$$

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



Агрегация прав при иерархической организации ролей (виды отношения $F_{P\mathcal{R}}$)

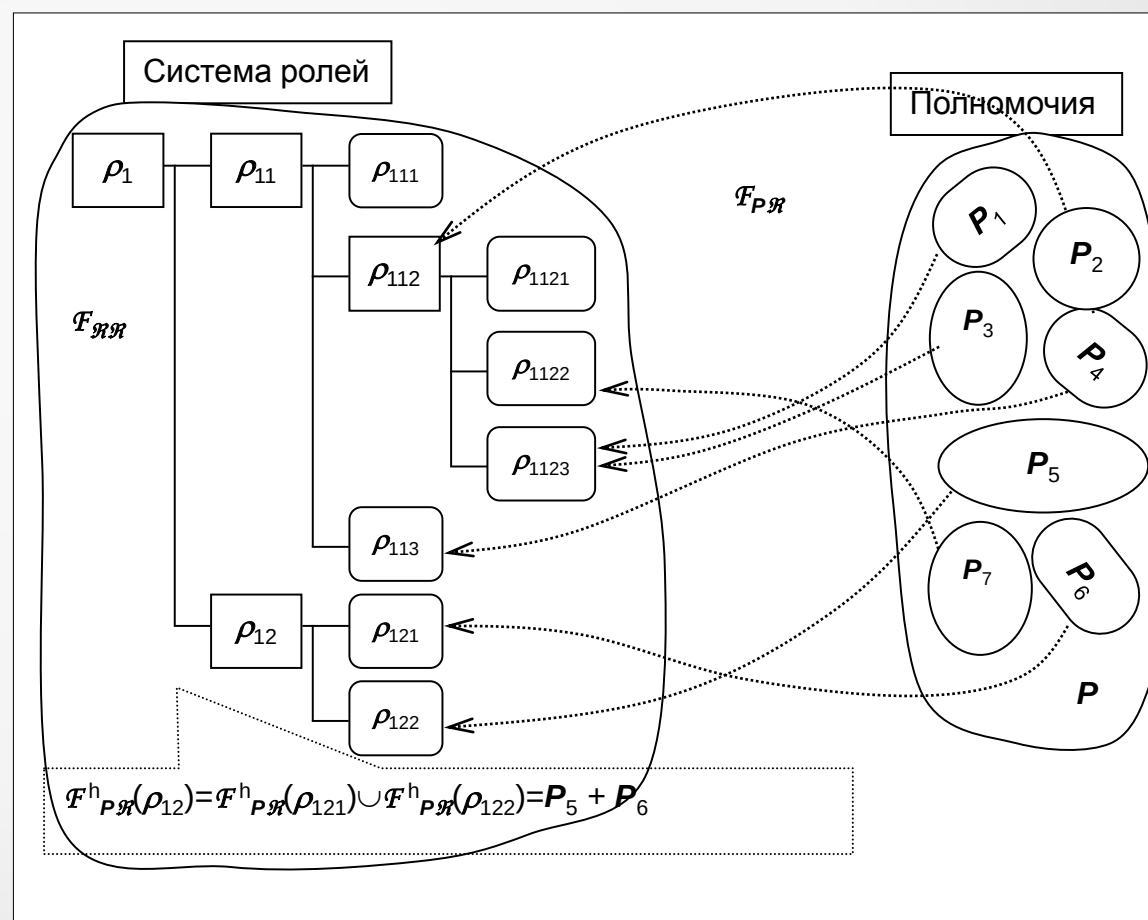
Иерархически охватный подход

$$F^h_{P\mathcal{R}}(\rho_i) = \{\rho^{(j)}_1, \rho^{(j)}_2, \dots\},$$

$$F^h_{P\mathcal{R}}(\rho^{\perp}_j) \cap F^h_{P\mathcal{R}}(\rho^{\perp}_i) \cap \dots \neq \emptyset,$$

$$F^h_{P\mathcal{R}}(\rho^{\perp}_k) \cap F^h_{P\mathcal{R}}(\rho_i) = \emptyset,$$

$$\text{где } \{\rho^{\perp}_k \geq \rho_i\}.$$



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 $f_{exclusive}: \mathcal{R} \rightarrow \mathcal{R}$, 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 (например "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

Модели индивидуально-группового доступа

1. КС представляется совокупностью следующих наборов сущностей:

- множества объектов доступа $O(o_1, o_2, \dots, o_M)$;
- множества пользователей $U(u_1, u_2, \dots, u_N)$;
- множества рабочих групп пользователей $G(g_1, g_2, \dots, g_K)$;
- множества прав доступа и привилегий $R(r_1, r_2, \dots, r_J)$;
- 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 $R(r_1, r_2, \dots, r_J)$, т. е. $A[u, o] \subseteq R$, $A[g, o] \subseteq R$.

Модели индивидуально-группового доступа

Определение.

Рабочей группой

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

$A =$

Рабочая группа в отличие от роли не является самостоятельным субъектом доступа

Группы Пользователи

Объекты

	O_1	O_2	$\dots$			O_M
u_1						
u_2						
				a_{ij}		
u_N						
g_1						
g_K						

Модели индивидуально-группового доступа

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

$F_{UG} : U \times G$ – 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 $G = \{g_{u_1}, g_{u_2}, \dots\} \subseteq G$, в которые пользователь u включен по отображению F_{UG} ;

$f_{users} : G \rightarrow U$ – значением функции $U = f_{users}(g)$ является набор пользователей $U = \{u_{g_1}, u_{g_2}, \dots\} \subseteq U$, которые рабочая группа g включает по отношению F_{UG} .

Отношение

«Пользователи-группы» -

«многие-ко-многим»

$W =$

		Рабочие группы				
		g_1	g_2	...		g_k
Пользователи	u_1		0			
	u_2					
					1	
	u_N					

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 F_{UG} :*

$$\mathcal{R} \subseteq \{A[u, o] \cup A[g^u_1, o] \cup A[g^u_2, o] \cup \dots\}, \text{ где } \{g^u_1, g^u_2, \dots\} = f_{\text{groups}}(u).$$

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:*

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

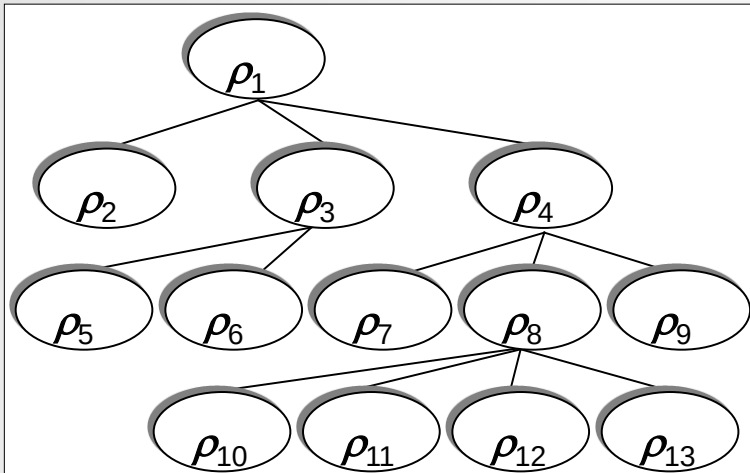
если для $g_1, g_2 \in G$, $g_1 \geq g_2$, то g_1 включает g_2 .

$f_{\text{hgroups}} : G \rightarrow G$ – значением функции $f_{\text{groups}}(g)$ является набор рабочих групп $\{g_{g_1}, g_{g_2}, \dots\} \subseteq G$, в которые рабочая группа g включена по отношению F_{GG} .

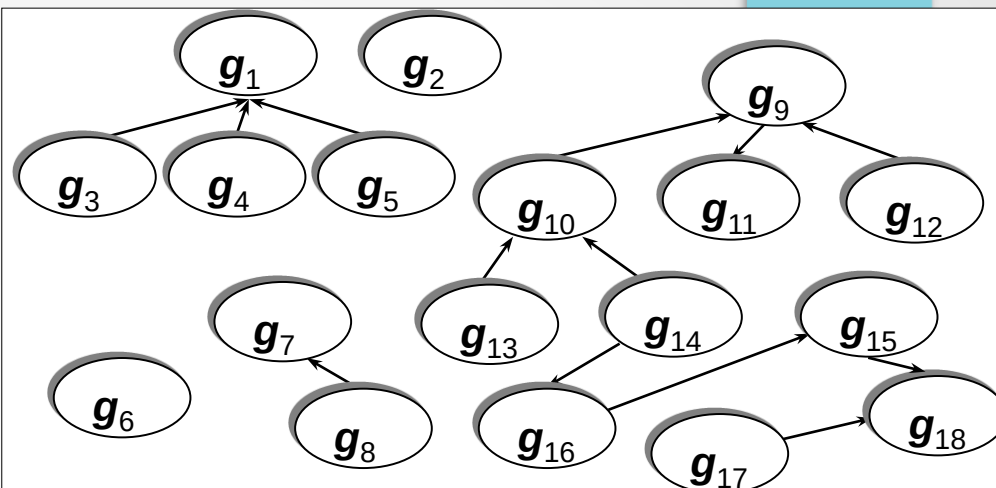
Наследование прав по групповой иерархии происходит «сверху-вниз»

$$R_g = A[g, o] + A[g_{g_1}, o] + A[g_{g_2}, o] + \dots, \text{ где } \{g_{g_1}, g_{g_2}, \dots\} = f_{\text{groups}}(g)$$

Модели индивидуально-группового доступа



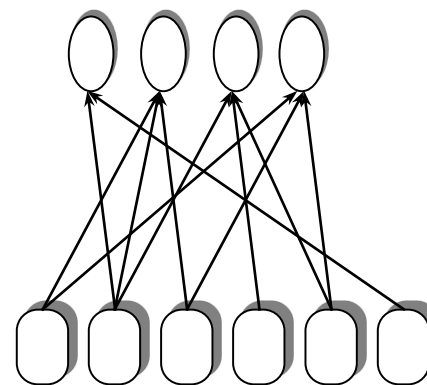
Иерархическая система ролей



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

MMS (military message system)-модель

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)

MMS (military message system)-модель

Определения MMS-модели (формализация системы защиты)

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

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.

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)

Ограничения безопасности в MMS-модели

В1. 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

В2. Классификационная иерархия - классификация контейнера всегда больше или равна классификации сущностей, которые он содержит

В3. Изменения в объектах - информация, переносимая из объекта всегда содержит классификацию объекта. Информация, вставляемая в объект, должна иметь классификацию ниже классификации этого объекта (аналог NWD)

В4. Просмотр - пользователь может просматривать (на некотором устройстве вывода) только сущности с классификацией меньше, чем классификация устройства вывода и степень доверия контейнера-устройства к пользователям (аналог NRU + NRUустройств)

В5. 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

В6. Преобразование косвенных ссылок - пользовательский индикатор признается законным для сущности, к которой он обратился косвенно, если только он авторизован для просмотра этой сущности через ссылку

Ограничения безопасности в MMS-модели

В7. Требование меток - сущности, просмотренные пользователем, д.б. помечены его степенью доверия (т.е. впоследствии они ему доверяют)

В8. 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

В9. 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"

Модель Лендвера-Маклина (MMS)

сочетает принципы:

ролевого, дискреционного и мандатного принципов

и оказывает сильное влияние на модели и технологии современных защищенных КС