Модели безопасности на основе ролевой политики

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

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

1. *Модели ролевого доступа*

Основная идея:
-политика и система защиты должны учитывать *организационно-технологическое взаимодействие пользователей*

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)

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:*

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

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

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: $f_{roles}(s)=\{\rho_i / (f_{user}(s), \rho_i) \in A_{u\rho}\}$

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

Критерий безопасности:

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

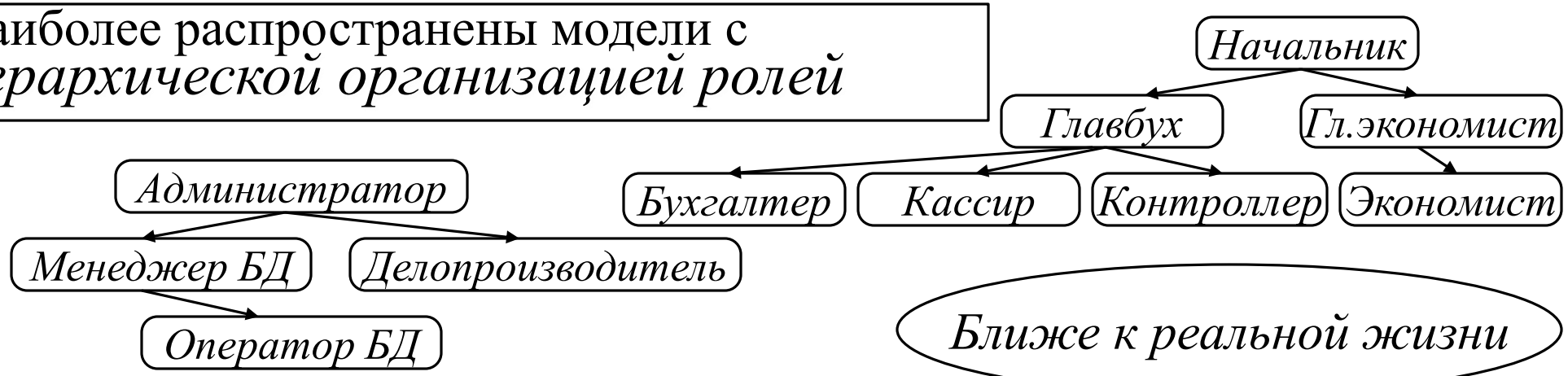
$p = f_{permissions}(s)$

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:

$F^h_{\mathcal{RR}}$ - $\mathcal{R}$ x $\mathcal{R}$ - частичное отношение порядка на множестве $\mathcal{R}$, которое определяет иерархию ролей и задает на множестве $\mathcal{R}$ оператор доминирования ≥, 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 x $\mathcal{R}$ - назначает каждому пользователю набор ролей, причем вместе с каждой ролью в него (набор ролей) включаются все роли, подчиненные ей по иерархии,

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

Функции:

f^{h}_{roles} - $S \rightarrow P(\mathcal{R})$ – 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 F_{PR})

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

Строго таксономический листовой подход

$F^{h}_{PR}(\rho^{л}_{j}) = \{p^{(j)}_{1}, p^{(j)}_{2}, \dots\}$,

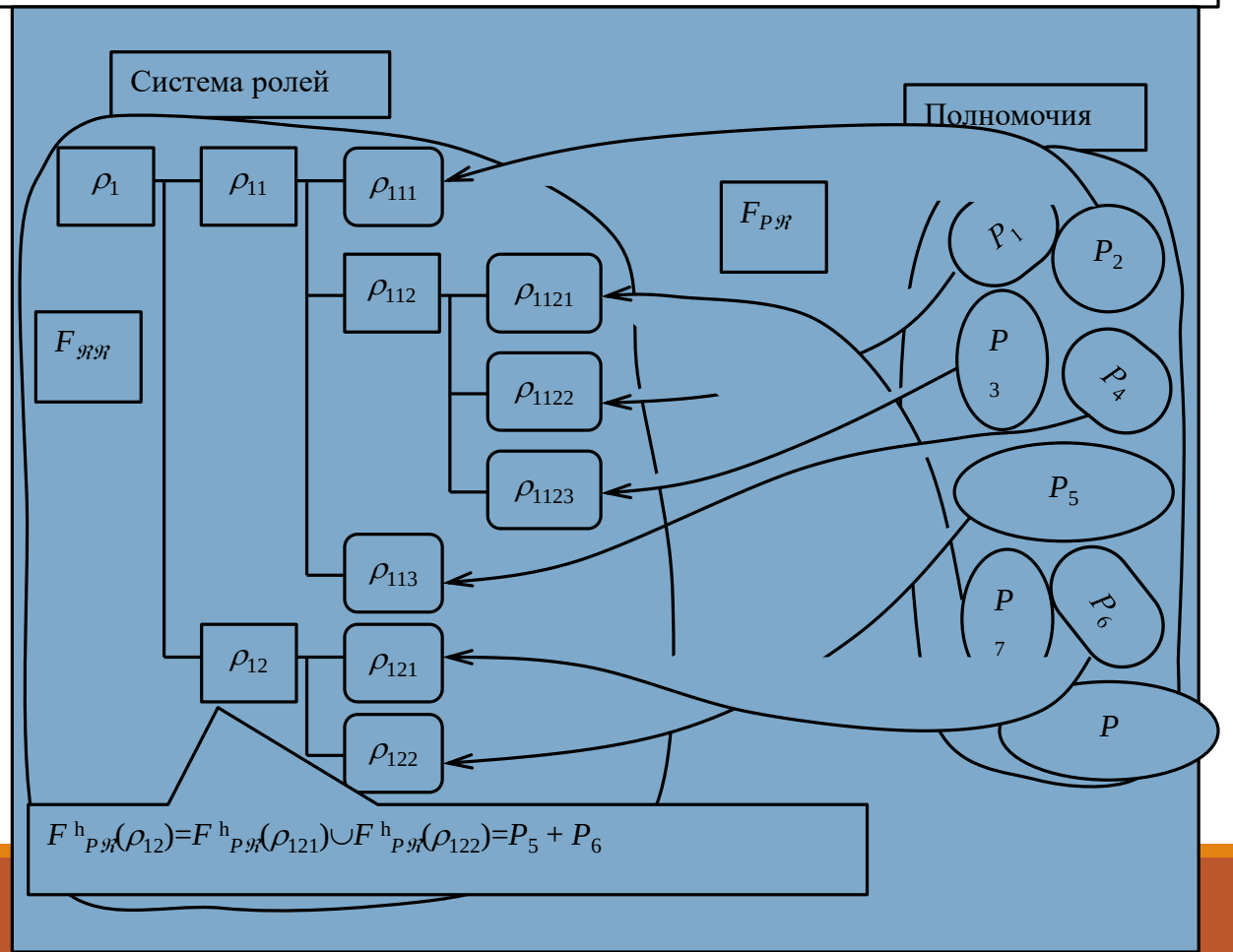
$F^{h}_{PR}(\rho^{л}_{j}) \cap F^{h}_{PR}(\rho^{л}_{i}) \cap \dots = \varnothing$,

$F^{h}_{PR}(\rho^{л}_{j}) \cup F^{h}_{PR}(\rho^{л}_{i}) \cup \dots = P$.

$F^{h}_{PR}(\rho^{и}_{k}) = F^{h}_{PR}(\rho^{(k)}_{i}) \cup$
$\cup F^{h}_{PR}(\rho^{(k)}_{j}) \cup \dots$,

где $\{\rho^{(k)}_{i}, \rho^{(k)}_{j}, \dots\}$ *– полный набор ролей-сыновей для роли* $\rho^{и}_{k}$.

$F^{h}_{PR}(\rho^{и}_{1}) = P$



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

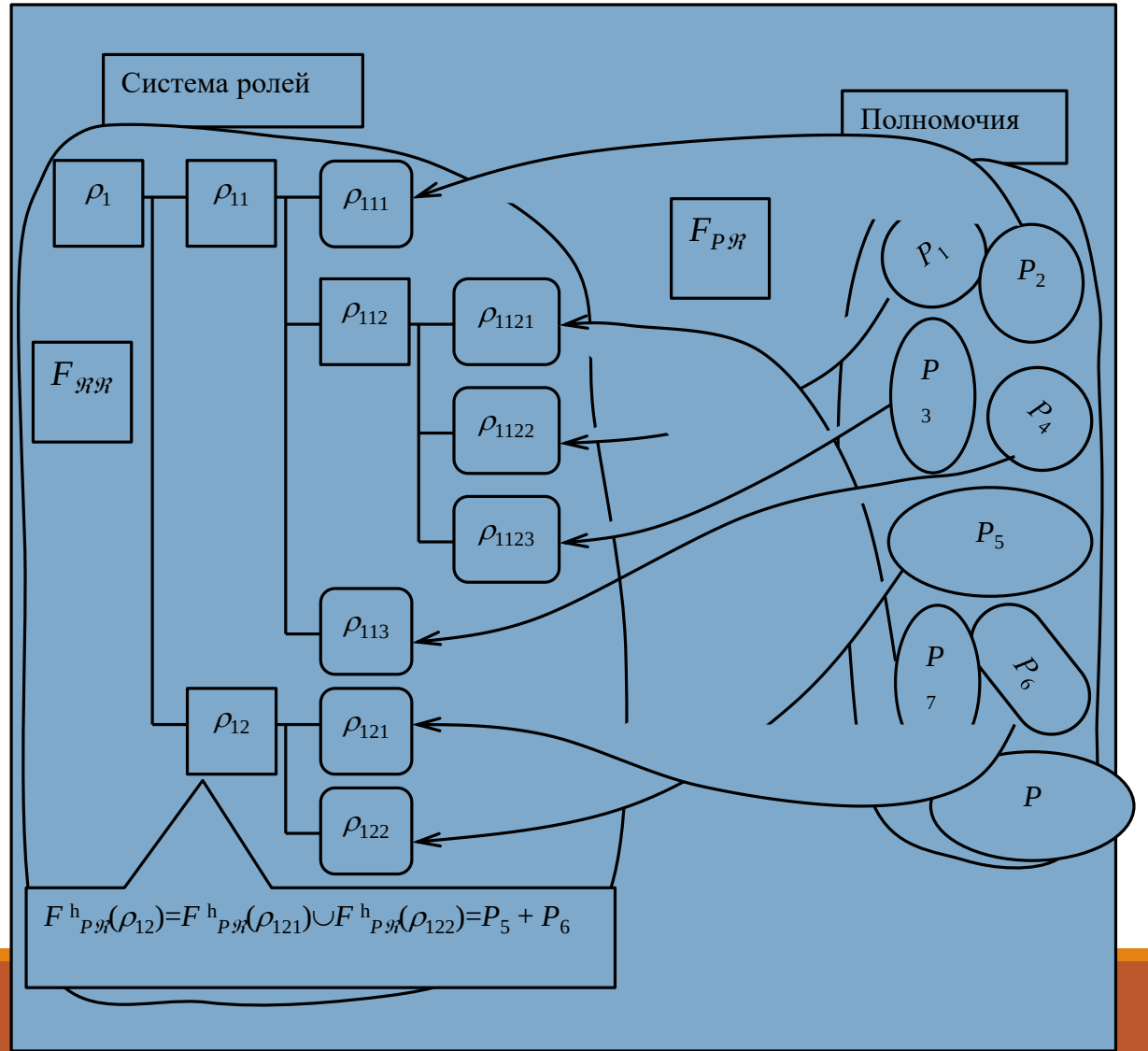
Нетаксономический листовой подход

$F^{h}_{PR}(\rho^{л}_{j}) = \{p^{(j)}_{1}, p^{(j)}_{2}, \ldots\}$,

$F^{h}_{PR}(\rho^{л}_{j}) \cap F^{h}_{PR}(\rho^{л}_{i}) \cap \ldots \neq \varnothing$,

$F^{h}_{PR}(\rho^{и}_{k}) = F^{h}_{PR}(\rho^{(k)}_{i}) \cup \cup F^{h}_{PR}(\rho^{(k)}_{j}) \cup \ldots$,

где $\{\rho^{(k)}_{i}, \rho^{(k)}_{j}, \ldots\}$ *– полный набор ролей-сыновей для роли* $\rho^{и}_{k}$.



1. *Модели ролевого доступа*

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

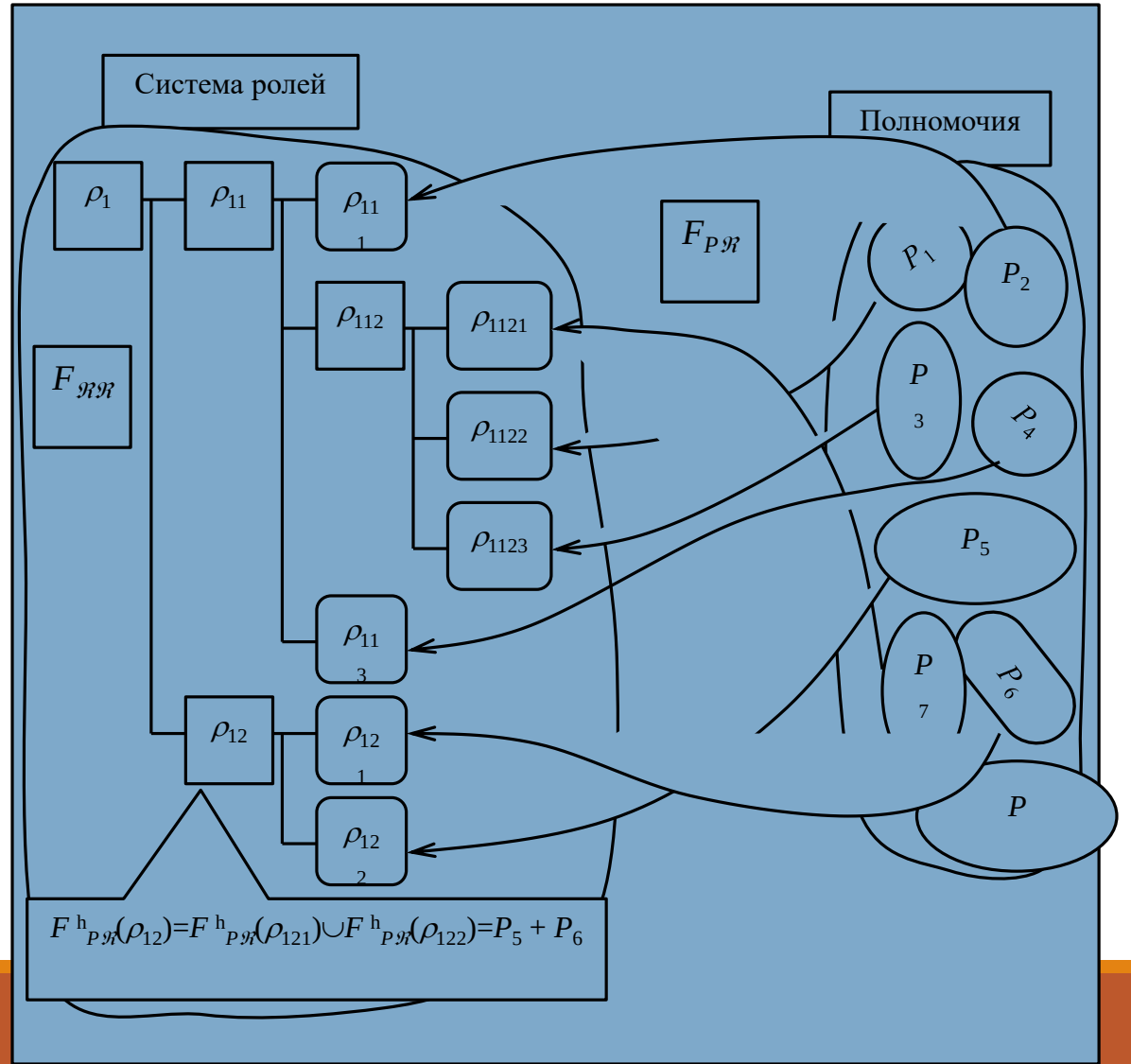
Иерархически охватный подход

$$F^{h}_{PR}(\rho^{л}_{j}) = \{p^{(j)}_{1}, p^{(j)}_{2}, \dots\},$$

$$F^{h}_{PR}(\rho^{л}_{j}) \cap F^{h}_{PR}(\rho^{л}_{i}) \cap \dots \neq \varnothing,$$

$$F^{h}_{PR}(\rho^{и}_{k}) \cap F^{h}_{PR}(\rho_{i}) = \varnothing,$$

где $\{\rho^{и}_{k} \geq \rho_{i}\}$.



1. *Модели ролевого доступа*

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) x 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

$A=$

Пользователи / Группы	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:

F_{UG} : U x 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 $f_{\text{groups}}(u) = G$ является набор рабочих групп $G = \{g_{u1}, g_{u2}, \ldots\} \subseteq G$, в которые пользователь u включен по отображению F_{UG} ;

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

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

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*:

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

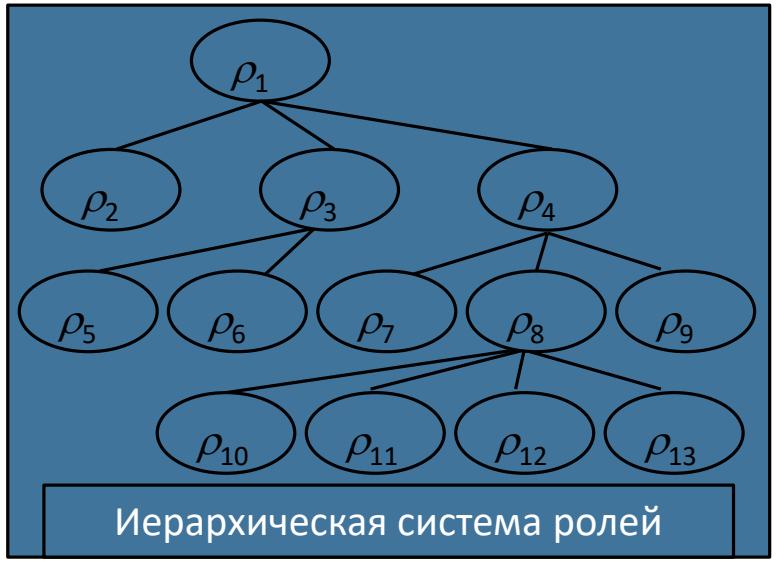
если для $g_1, g_2 \in G$, $g_1 \geq g_2$, то g_1 включает g_2 .

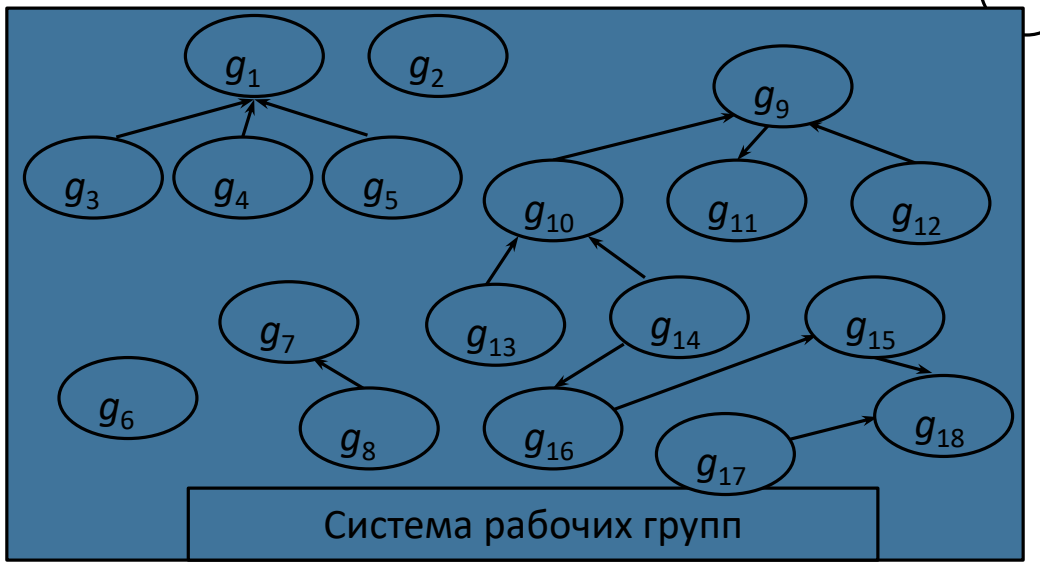
$f_{\text{hgroups}}: G \to G$ – значением функции $f_{\text{groups}}(g)$ является набор рабочих групп $\{g_{g_1}, g_{g_2}, \ldots\} \subseteq G$, в которые рабочая группа g включена по отношению F_{GG} .

Наследование прав по групповой иерархии происходит «сверху-вниз»

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

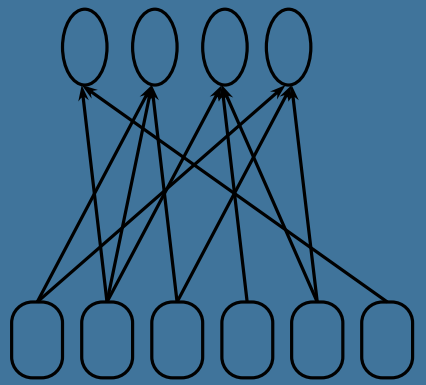
2. *Модели индивидуально-группового доступа*





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 использова- ния 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 к пользователям (аналог NRU + NRUустройств)

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