Расширенная модель TAKE-GRANT

Типы расширения модели

1. Правила де-факто, предназначенные для поиска и анализа информационных потоков.
2. Алгоритм построения замыкания графа доступов и информационных потоков.
3. Способы анализа путей распространения прав доступа и информационных потоков.

Де-факто правила расширения модели Take-Grant

Определение. Неявным информационным потоком между объектами системы называется процесс переноса информации между ними без их непосредственного взаимодействия.

Основные элементы модели:

O – множество объектов доступа,

S – множество субъектов доступа,

$R(r_1, r_2, \ldots, r_m) \cup \{t, g\} \cup \{r, w\}$ – множество прав доступа.

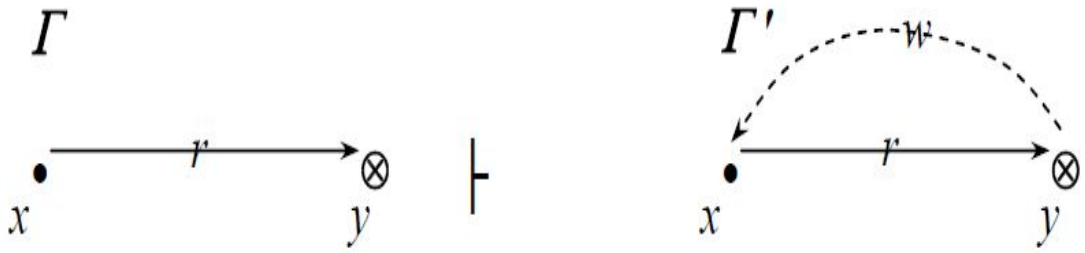
- Правила **де-юре**: take, grant, create, remove.

Совпадают с правилами в классической модели, в графе обозначаются сплошной линией («реальные» ребра). Элементы множества E.

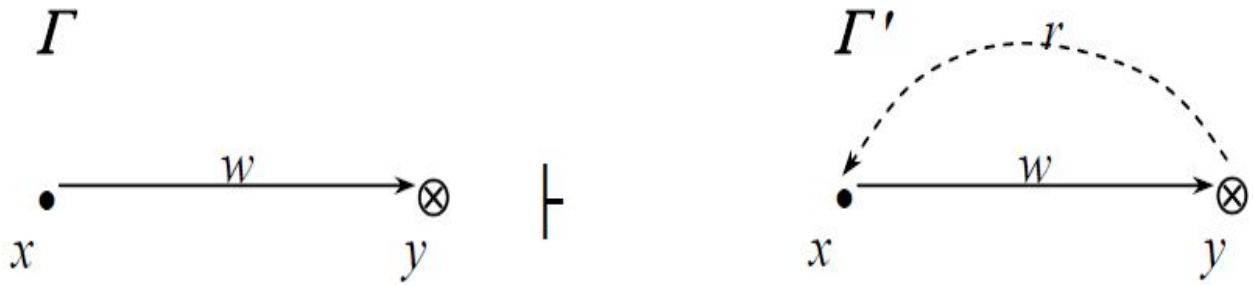
- Правила **де-факто**: read, write, spy, find, post, pass.

В графе обозначаются пунктирной линией («мнимые» ребра). Элементы множества F.

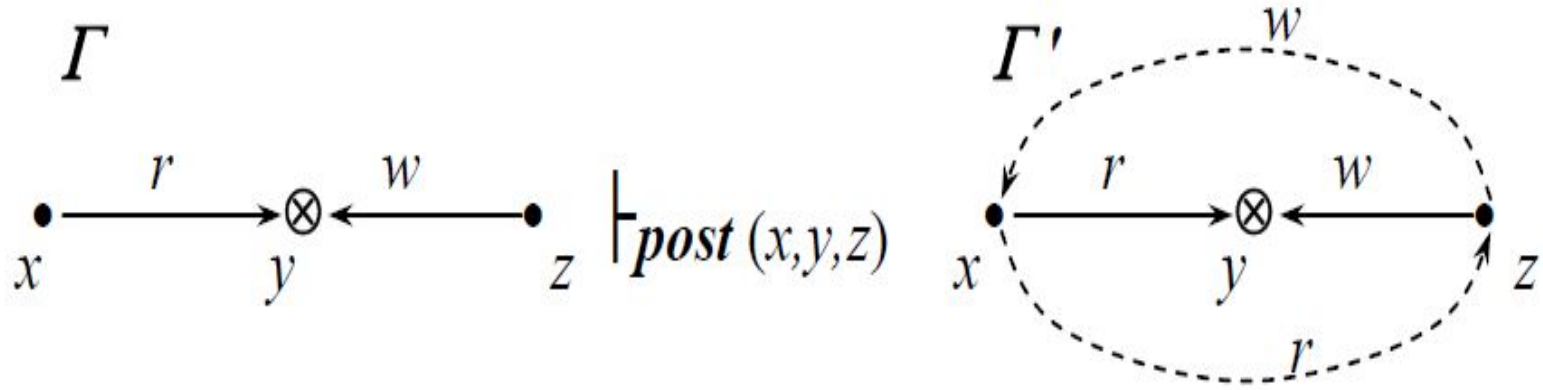
Первое правило. Субъект получает возможность записи информации, осуществляя доступ **r** к объекту.



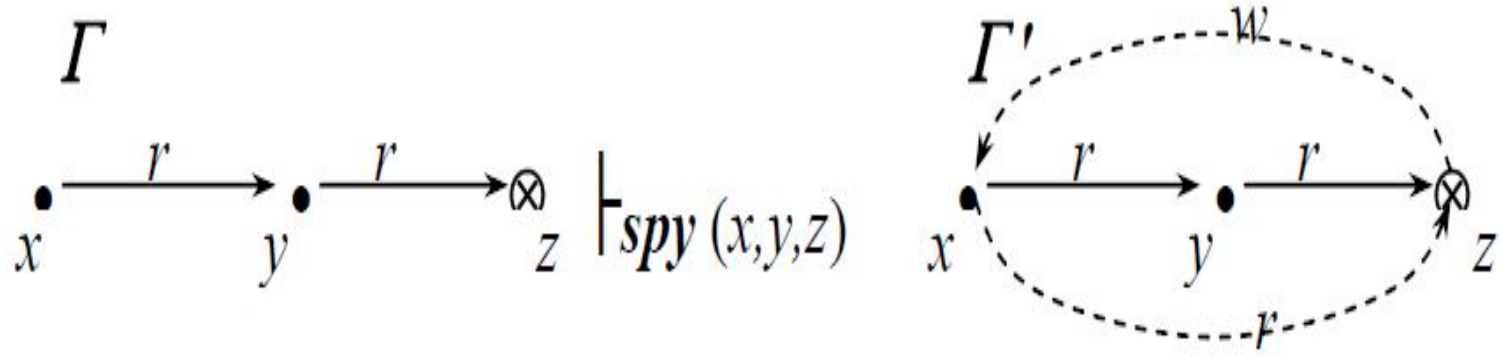
Второе правило. Субъект получает возможность чтения информации, осуществляя доступ **w** к объекту.



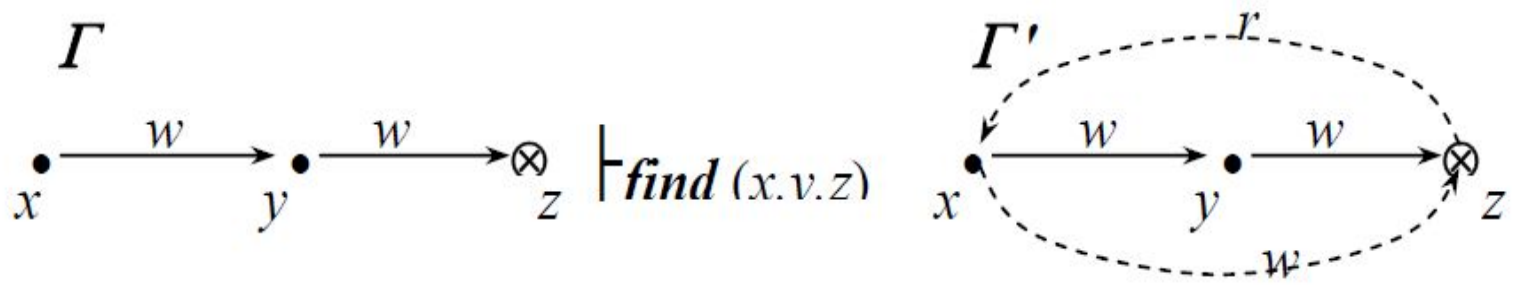
Команда post. Субъект **x** получает возможность чтения информации от другого субъекта **z**, осуществляя доступ **r** к объекту **y**, к которому субъект **z** осуществляет доступ **w**, а субъект **z**, в свою очередь, получает возможность записи своей информации в субъект **x**.



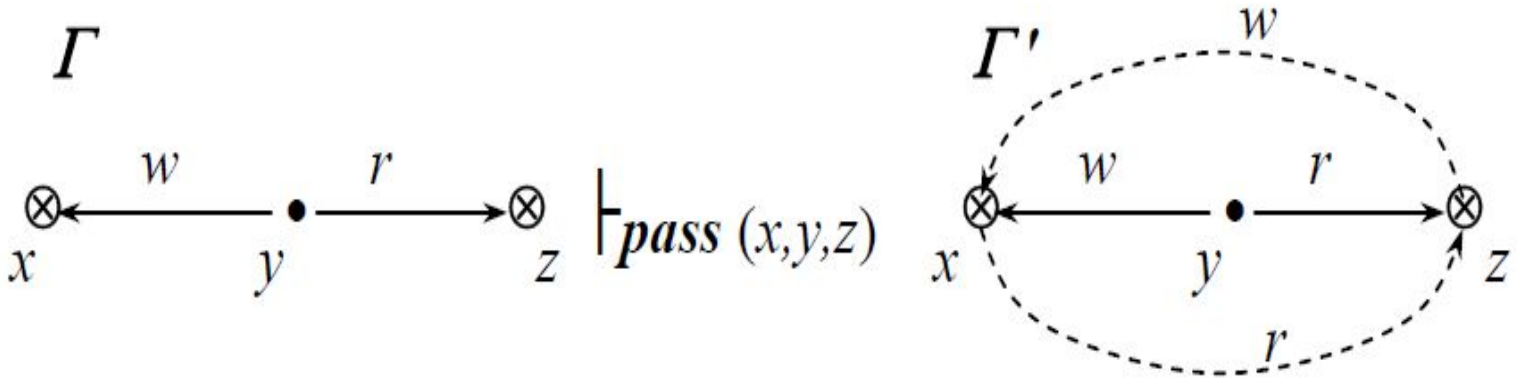
Команда spy. Субъект **x** получает возможность чтения информации из объекта **z**, осуществляя доступ **r** к субъекту **y**, который в свою очередь, осуществляет доступ **r** к объекту **z**, при этом также у субъекта **x** возникает возможность записи к себе информации из объекта z



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



Команда pass. При осуществлении субъектом **y** доступа **r** к объекту **z** возникает возможность внесения из него информации в другой объект **x**, к которому субъект **y** осуществляет доступ **w**, и, кроме того, возникает возможность получения информации в объекте **x** из объекта **z**



Определение 1. Пусть x, y $\in O_0, x \neq y$. Определим предикат «возможна запись (x,y,q_0)», который будет истинным тогда и только тогда, когда существуют графы $q_1 =(S_1, O_1, E_1)$, $q_2=(S_2, O_2, E_2)$, ..., $q_N = (S_N, O_N, E_N)$ и де-юре или де-факто правила p_1, … , p_N такие что:

$q_0(S_0, O_0, E_0) \vdash_{p1} (S_1, O_1, E_1) \vdash_{p2} \ldots \vdash_{pN} q_N (S_N, O_N, E_N)$ и (x, y, w) $\in F_N$

Теорема. Пусть $q_0 = (S_0, O_0, E_0 \cup F_0)$ – граф доступов и информационных потоков, $x,y \in O_0, x \neq y$. Тогда предикат «возможна запись (x,y, q_0)» истинен только тогда, когда существуют объекты

$o_1=x ,..., o_m=y \in O_0$, такие что или $m=2$ и $(x,y,w) \in F_0$

или для $i =1,...,m-1$ выполняется одно из условий:

- $o_i \in S_0$ и или истинен предикат «возможен доступ» $(\{w\},o_i,o_{i+1},q_0)$, или $(o_i,o_{i+1},w) \in E_0 \cup F_0$
- $o_{i+1} \in S_0$ и или истинен предикат «возможен доступ» $(\{r\},o_{i+1},o_i,q_0)$, или $(o_{i+1},o_i,r) \in E_0 \cup F_0$
- o_i, o_{i+1} и или истинен предикат «возможен доступ» $(\alpha ,o_i,o_{i+1},q_0)$, или истинен предикат «возможен доступ $(\alpha ,o_{i+1},o_i,q_0)$», где $\alpha \in \{t,g\}$.

Построение замыкания графа доступов и информационных потоков

Алгоритм построения замыкания графа доступов состоит из трех этапов:

1. Построение tg-замыкания.
2. Построение де-юре-замыкания.
3. Построение де-факто-замыкания.

Определение 2. Пусть q =(S, O, E∪F) –граф доступов и информационных потоков такой, что для каждого s∈S существует o ∈ O и при этом (s,o,{t,g,r,w}) ⊂E. Тогда замыканием (де-факто-замыканием) графа q называется граф доступов и информационных потоков q*, полученный из q применением последовательности правил take, grant и де-факто правил. При этом применением к графу q* правил не приводит к появлению новых ребер.

Определение 3. Пусть q =(S, O, E∪F) –граф доступов и информационных потоков такой, что для каждого s∈S существует o ∈ O и при этом (s,o,{t,g,r,w}) ⊂E. Тогда tg-замыканием графа q называется граф доступов и информационных потоков $q^{tg} = (S, O, E^{tg} \cup F)$ полученный из q применением последовательности правил take и grant. При этом каждое ребро (s,o,α) имеет вид (s,o,t) или (s,o,g) и применение к графу q^{tg} правил take или grant не приводит к появлению новых ребер.

Определение 4. Пусть q =(S, O, E∪F) –граф доступов и информационных потоков такой, что для каждого s∈S существует o ∈ O и при этом (s,o,{t,g,r,w}) ⊂E. Тогда де-юре-замыканием графа q называется граф доступов и информационных потоков $q^{de\ jure} = (S, O, E^{de\ jure} \cup F)$ полученный из q применением последовательности правил take и grant. При этом применение к графу $q^{de\ jure}$ правил take или grant не приводит к появлению новых ребер.

- **Алгоритм построения tg-замыкания**

1 шаг. Для каждого s∈S выполнить правило create({t,g},s,o), при этом создаваемые объекты заносить в множество O.

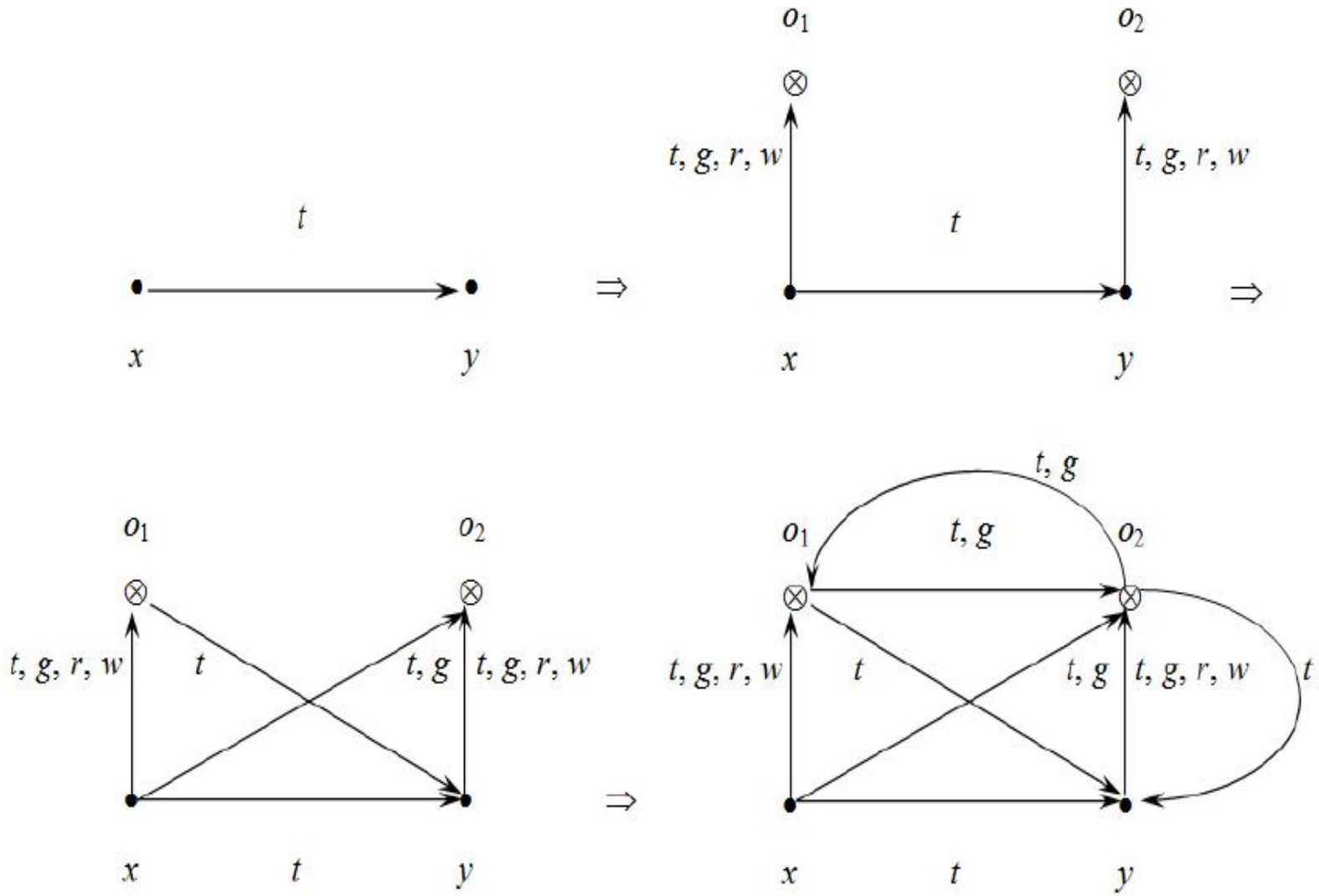
2 шаг. Инициализировать список ребер графа доступов L={(x,y, α) ∈ E: α ∈{t,g}}. N=∅ - множество вершин.

3 шаг. Выбрать из списка L первое ребро (x,y,α). Занести x, y в множество N. Удалить ребро (x,y,α) из списка L.

4 шаг. Для всех вершин z ∈ N проверить возможность применения правил take или grant на тройке вершин x, y, z с использованием ребра(x,y,α). Если в результате применения появляются новые ребра вида (a, b, β), где {a,b}⊂{x,y,z}, β ∈{t,g}, то занести их в конец списка L и множество E.

5 шаг. Пока список L не пуст, перейти на шаг 3.

Пример построения tg-замыкания



- **Алгоритм построения де-юре-замыкания**

1 шаг. Выполнить tg-замыкание

2 шаг. Для каждой пары ребер вида (x,y,t), (y,z,α) $\in E^{tg}$, где x ∈S, применить правило

take (α,x,y,z) и, если полученное ребро (x,z,α)$\notin E^{tg}$, занести его в множество E^{tg}.

3 шаг. Для каждой пары ребер вида (x,y,g), (x,z,α) $\in E^{tg}$, где x ∈S, применить правило

grant(α,x,y,z) и, если полученное ребро (y,z,α)$\notin E^{tg}$, занести его в множество E^{tg}.

4 шаг. Для каждой пары ребер вида (x,y,t), (y,z,α) $\in E^{tg}$, где x ∈S, применить правило

take (α,x,y,z) и, если полученное ребро (x,z,α)$\notin E^{tg}$, занести его в множество E^{tg}.

- **Алгоритм построения де-факто-замыкания**

***1 шаг*.** Для всех ребер (x,y,α)∈ $E^{de\ jure} \cup F$, где

x∈S, α ∈{w,r}, применить первые два де-факто правила. Если будут получены новые ребра, то занести их в множество F.

2 шаг. Инициализировать список ребер графа доступов L={(x,y, α) ∈ $E^{de\ jure} \cup F$: α ∈{w,r}}.

N=∅ - множество вершин.

3 шаг. Выбрать из списка L первое ребро (x,y,α). Занести x, y в множество N. Удалить ребро (x,y,α) из списка L.

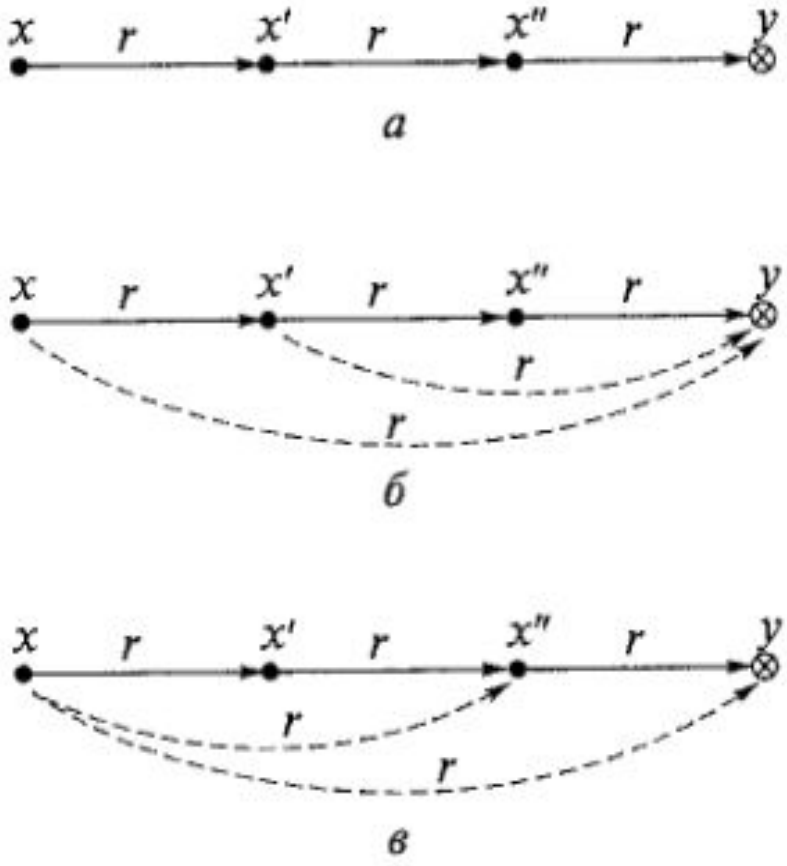
4 шаг. Для всех вершин z ∈ N проверить возможность применения де-факто правил на тройке вершин x, y, z с использованием ребра(x,y,α). Если в результате применения правил spy, find, post, pass появляются новые ребра вида (a, b, β), где {a,b}⊂{x,y,z}, β ∈{r,w}, то занести их в конец списка L и множество F.

5 шаг. Пока список L не пуст, перейти на шаг 3.

Анализ путей распространения прав доступа и информационных потоков

Включено понятие стоимости (вероятности) пути передачи прав доступа.

Путям меньшей стоимости соответствует наибольшая вероятность



Определение стоимости путей.

1 способ основан на присвоении стоимости ребрам графа, находящимся на пути передачи прав доступа или возникновении информационного потока. В этом случае стоимость ребра определяется в зависимости от прав доступа. А стоимость пути есть сумма стоимостей пройденных ребер.

2 способ основан на присвоении стоимости каждому используемому де-юре или де-факто правилу. Стоимость правил определяется из условий:

- Является константой,
- Зависит от специфики правила,
- Зависит от числа и состава участников при применении правила,
- Зависит от степени требуемого взаимодействия субъектов.

Стоимость пути определяется как сумма стоимостей примененных правил.