Модели распространения прав доступа

- Более сложный пример модели разграничения доступа

Пятимерное пространство Хартсона

Пятимерное пространство Хартсона

1. Система представляется совокупностью пяти наборов (множеств):
   - множества пользователей ***U*** ;
   - множества ресурсов ***R*** ;
   - множества состояний ***S*** ;
   - множества операций ***E*** ;
   - множества установленных полномочий ***A***.
2. Множество полномочий A – a_{ijkl} определяют: -
   - ресурсы,
   - вхождение пользователей в группы;
   - разрешенные операции для групп по отношению к ресурсам
3. Область безопасности представляется декартовым произведением:

   $A \times U \times E \times R \times S$ (*)

Пятимерное пространство Хартсона

4. Пользователи подают запросы на доступ к ресурсам, осуществление которых переводит систему в новое состояние.

5. Запросы на доступ представляются четырехмерными кортежами
$\boldsymbol{q} = (\boldsymbol{u}, \boldsymbol{e}, \boldsymbol{R}', \boldsymbol{s})$, где
$\boldsymbol{u} \in \boldsymbol{U}, \boldsymbol{e} \in \boldsymbol{E}, \boldsymbol{s} \in \boldsymbol{S}, \boldsymbol{R}' \subseteq \boldsymbol{R}$ ($\boldsymbol{R}'$- требуемый набор ресурсов).

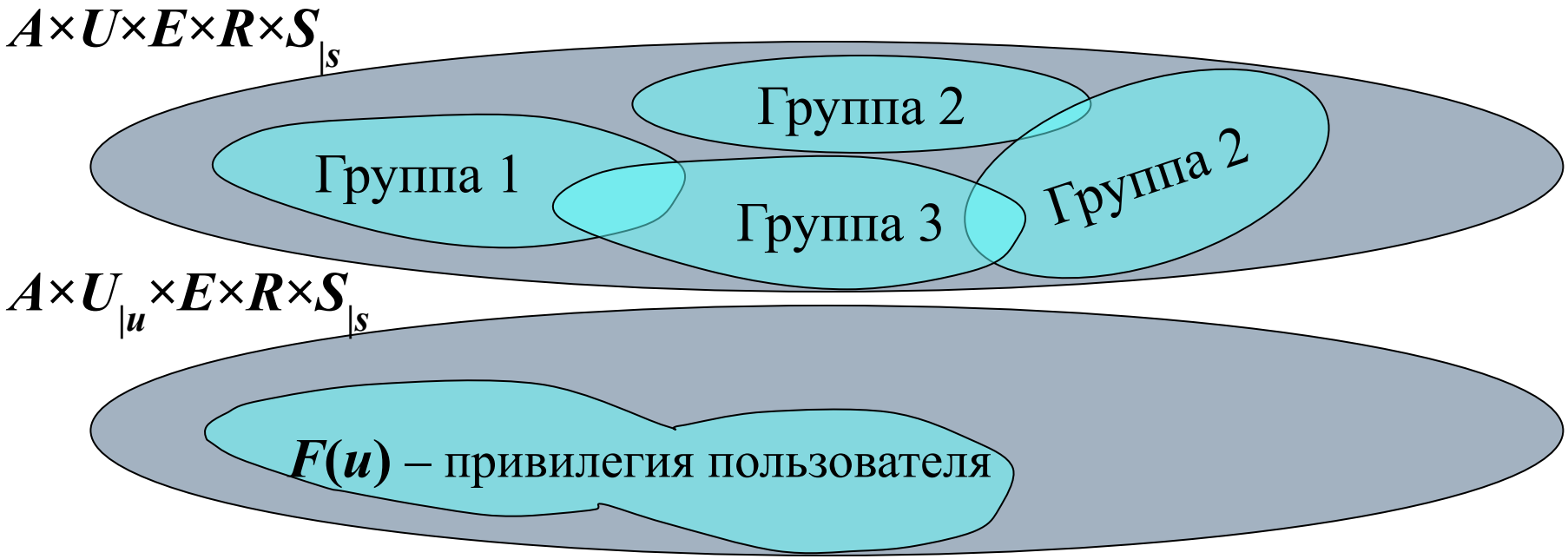
6. Запрос удовлетворяется, если он полностью заключен в области безопасности
$\boldsymbol{A} \times \boldsymbol{U} \times \boldsymbol{E} \times \boldsymbol{R} \times \boldsymbol{S}$ **(*)**

Пятимерное пространство Хартсона. Процесс организации доступа

1. Определить из ***U*** те группы пользователей, к которым принадлежит ***u***. Затем выбрать из ***A*** те спецификации, которым соответствуют выделенные группы пользователей. Этот набор полномочий *F*(***u***) определяет *привилегию пользователя **u***
2. Определить из множества ***A*** набор полномочий ***P*** =*F*(***e***), которые устанавливают ***e*** как основную операцию. Набор полномочий ***P*** =*F*(***e***) определяет *привилегию операции **e.***
3. Определить из множества ***A*** набор полномочий ***P*** =*F*(***R***′), разрешающих доступ к набору ресурсов ***R***′.
   Набор полномочий ***P*** =*F*(***R***′) определяет *привилегию ресурсов **R***′.
4. Полномочия, которые являются общими для всех трех привилегий, образуют так называемый
   *домен полномочий запроса **D**(**q**):* $\boldsymbol{D}(\boldsymbol{q}) = F(\boldsymbol{u}) \cap F(\boldsymbol{e}) \cap F(\boldsymbol{R}')$.

$q = (u, e, R', s) \div D(q) = F(u) \cap F(e) \cap F(R')$ Домен полномочий запроса

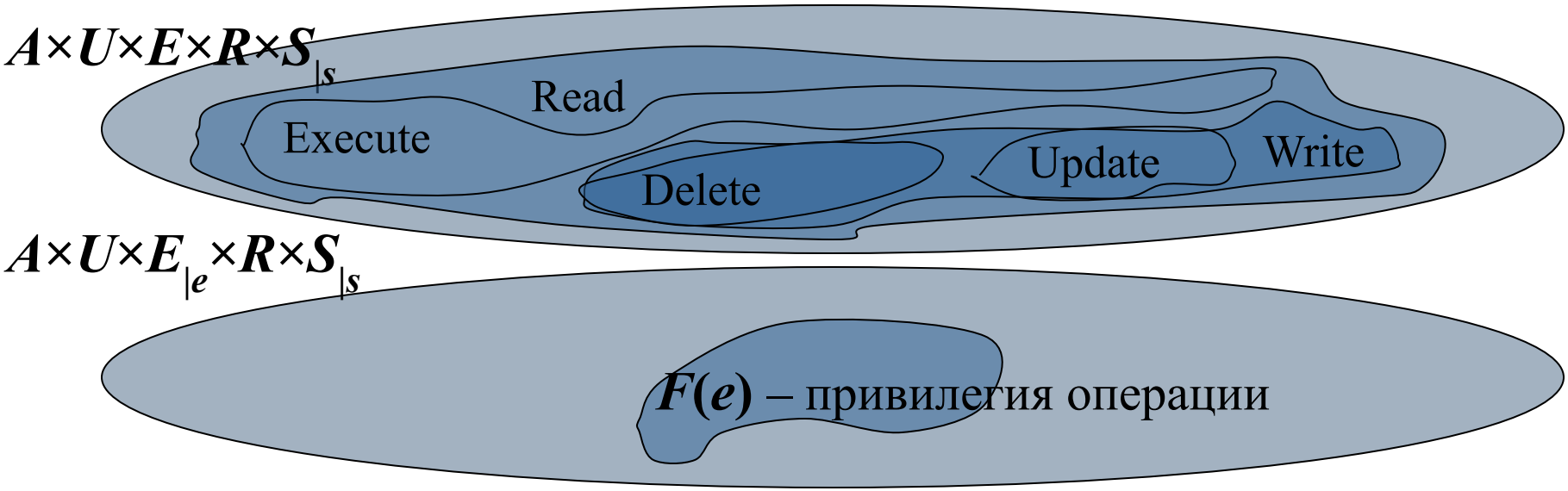
- *Определить из A*
  F(u) – привилегию пользователя



$q = (u, e, R', s) : \; D(q) = F(u) \cap F(e) \cap F(R')$

Домен полномочий запроса

- *Определить из A*
  P=F(e) - привилегию операции

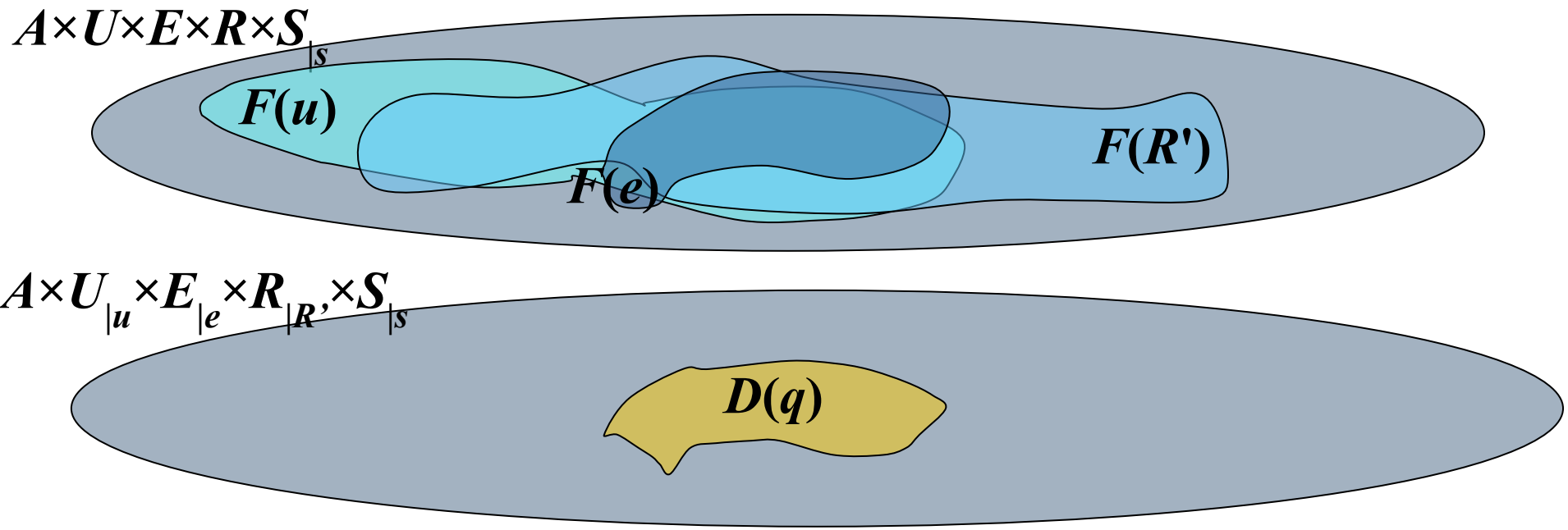


$q = (u, e, R', s) \Rightarrow D(q) = F(u) \cap F(e) \cap F(R')$
Домен полномочий запроса

- *Определить из A*
  F(R') - привилегию ресурсов

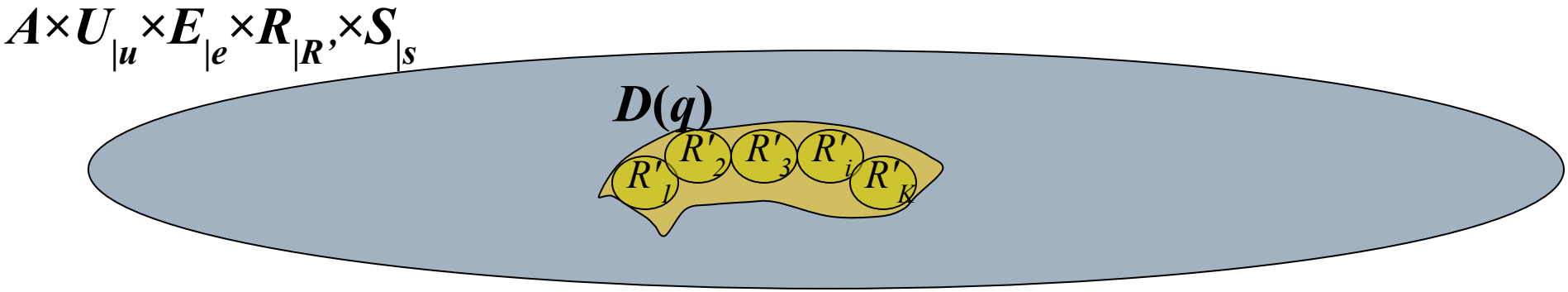
$q = (u, e, R', s)$: $D(q) = F(u) \cap F(e) \cap F(R')$ Домен полномочий запроса

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



Пятимерное пространство Хартсона. Процесс организации доступа

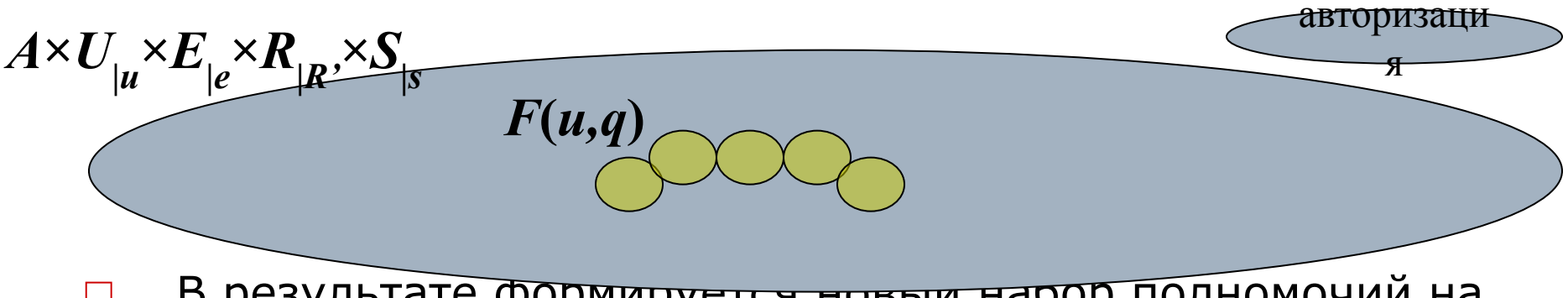
5. Убедиться, что запрашиваемый набор ресурсов *R'* полностью содержится в домене запроса *D*(*q*), т.е. любой *r* из набора *R'* хотя бы один раз присутствует среди элементов *D*(*q*).



Пятимерное пространство Хартсона. Процесс организации доступа

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 каждую единицу ресурса, указанного в $D(q)$: $F(u,q)$.
- Набор $F(u,q)$ называется **привилегией пользователя *u* по отношению к запросу *q***.

Пятимерное пространство Хартсона. Процесс организации доступа

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

- **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*