МОДЕЛЬ ОРГАНИЗАЦИИ ПРАВ ДОСТУПА В ВЕБ-ПРИЛОЖЕНИЯХ ДЛЯ ДИСКРЕЦИОННЫХ И РОЛЕВЫХ СХЕМ

Н.В. Курмышев, С.В. Попов

Докладчик:
Курмышев Николай Васильевич,
к.т.н.,
проректор по НИТ НовГУ,
Тел. +7 (8162) 62 72 18
E-mail: Nikolai.Kurmishev@novsu.ru

Новгородский государственный университет

www.novsu.ru

Назначение модели

Назначение модели:

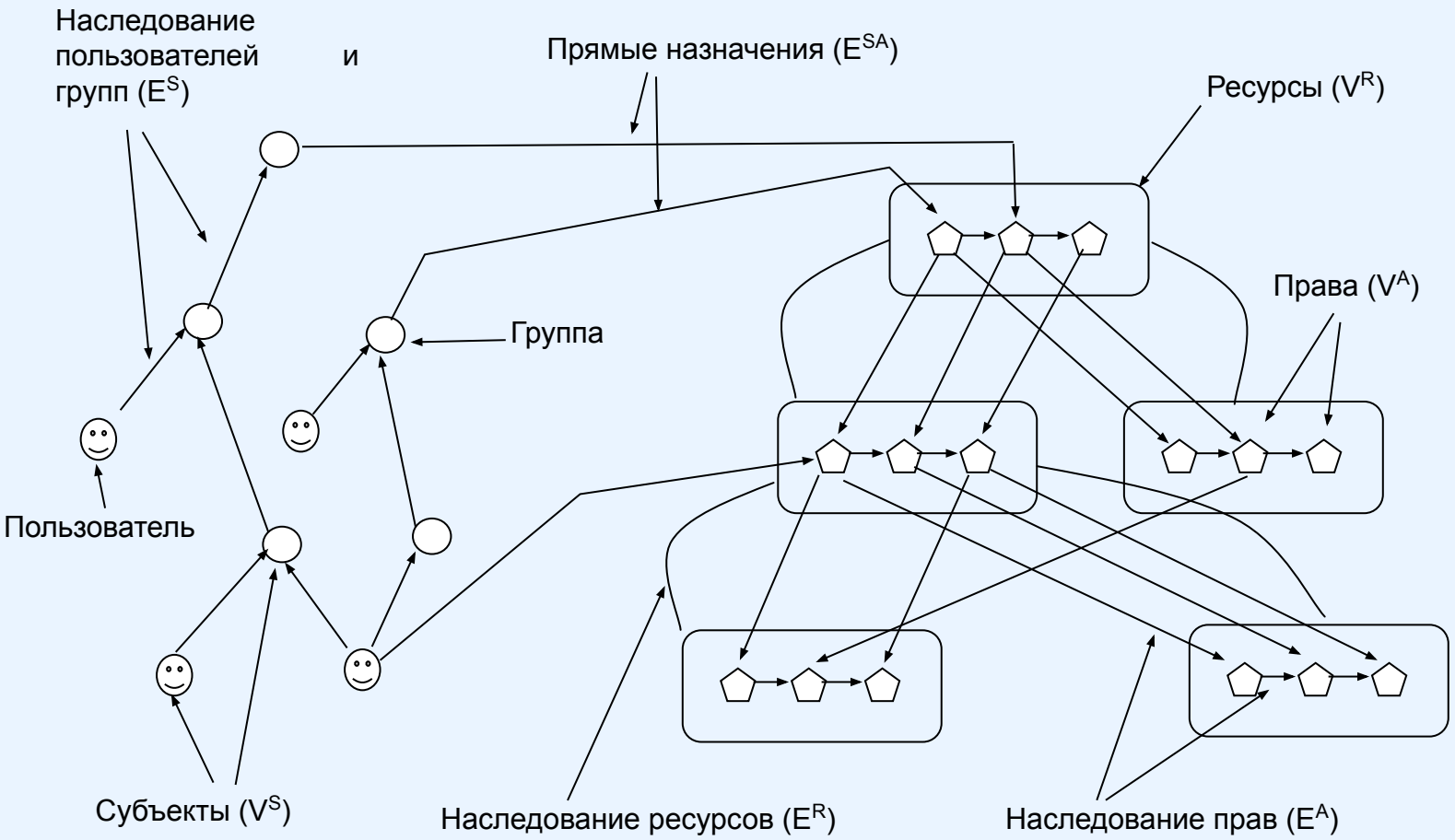
- Описание дискреционных и ролевых схем организации прав доступа.
- Анализ характеристик схем и систем прав доступа.

Требования к модели:

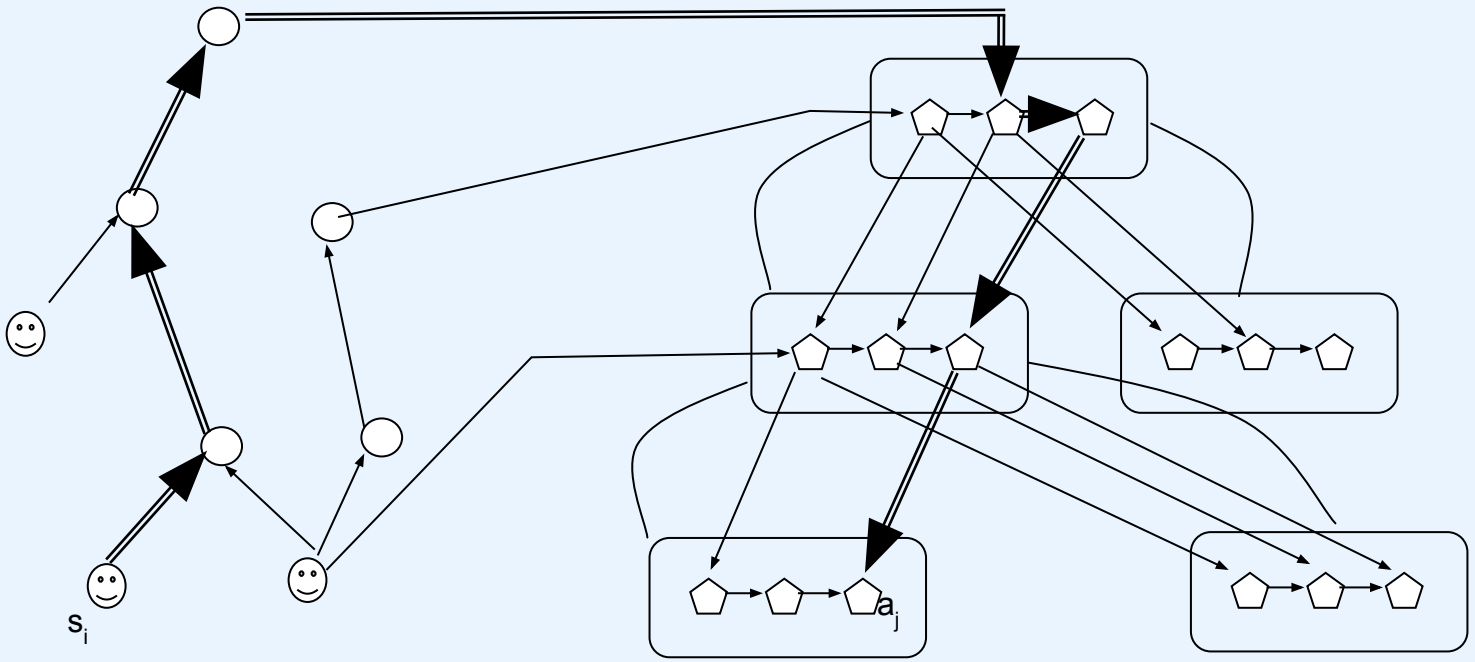
- позволять описывать различные дискреционные и ролевые схемы, определяющие права доступа пользователей к ресурсам;
- охватывать максимально возможное количество схем назначения прав доступа;
- позволять анализировать следующие характеристики схем:
    - сложность администрирования;
    - вычислительная сложность;
    - сложность реализации;
    - избыточность;
    - превышение доступа.

Общий вид модели

Модель представляется в виде ориентированного графа, объединяющего множества субъектов, ресурсов и прав доступа. При этом дуги графа обозначают передачу прав доступа от одного элемента системы другому.

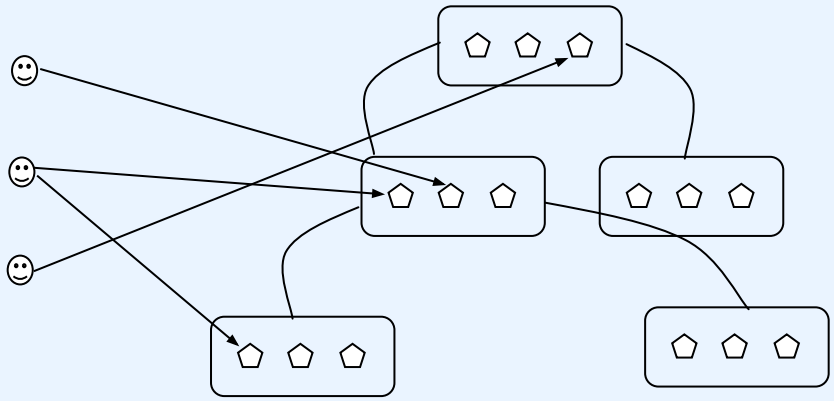


Пример маршрута доступа



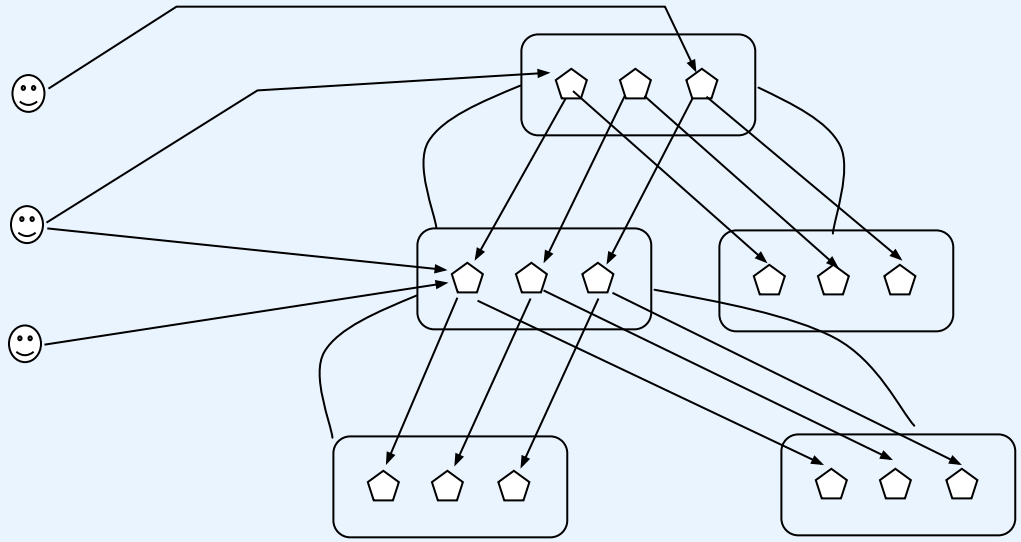
Пример маршрута доступа из субъекта s_i к праву a_j. Если такой маршрут существует, пользователь s_i имеет доступ a_j к ресурсу r_k

Пример представления табличной схемы



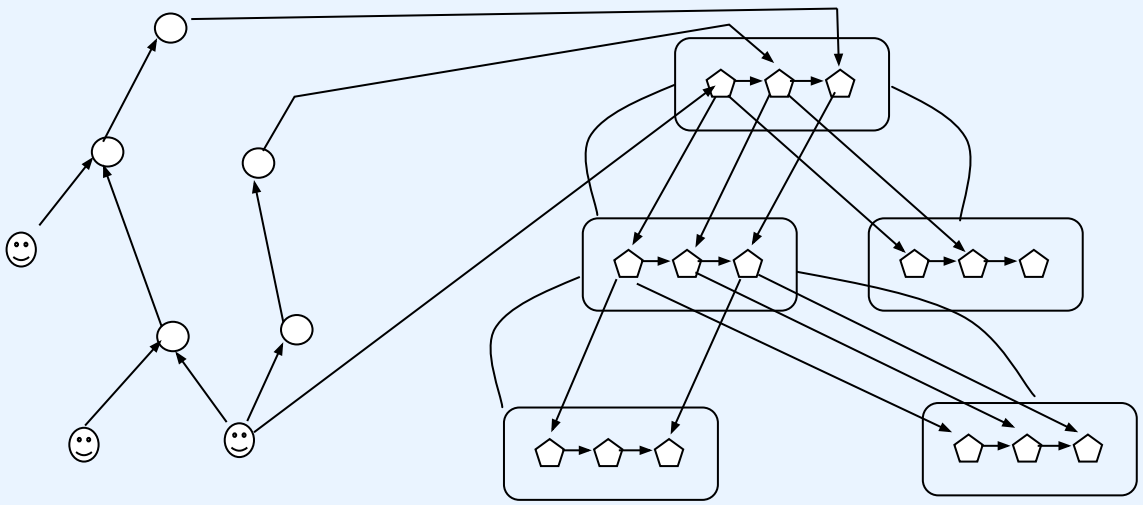
Табличная схема предполагает отсутствие наследования по всем множествам.

Пример представления схемы с наследованием по ресурсам



Наиболее популярная схема для простых веб-приложений.
Позволяет наследовать права по иерархии ресурсов.

Схема IBM WebSphere Portal



Схема, применяемая в WebSphere Portal является одной из наиболее универсальных из представленных на рынке.

Позволяет наследовать права по иерархии пользователей, ресурсов и прав внутри ресурсов. Также позволяет блокировать наследование определенной роли по иерархии ресурсов.

Сложность реализации

Сложность реализации – трудозатраты на программную реализацию схемы.

Сложность реализации имеет значение при реализации относительно небольших проектов, где на первое место ставится простота и быстродействие. Эта характеристика применима только к схемам, но не к конечным системам, поскольку именно схема определяет программный код.

$$C_{\text{реализации}} \sim$$
$$K_1 * \text{наличие схемы прав доступа} +$$
$$K_2 * \text{наличие групп} +$$
$$K_3 * \text{наличие связей между группами} +$$
$$K_4 * \text{наличие наследования ресурсов} +$$
$$K_5 * \text{наличие ролей}$$

Сложность администрирования

Сложность администрирования – трудозатраты на администрирование системы, построенной по заданной схеме.

Сложность администрирования возрастает с увеличением количества администрируемых объектов.

Будем рассматривать сложность администрирования как количество узлов и дуг графа, создаваемых вручную администратором.

$C_{\text{администрирования}} \sim$
(Среднее количество прав, назначаемых одному субъекту) *
(!Наличие групп * Количество пользователей +
Наличие групп *
(!Наличие связей между группами * Количество пользователей/Среднее количество пользователей в группе +
Наличие связей между группами / Среднее количество подгрупп всех уровней для групп схемы))

Вычислительная сложность

Вычислительная сложность – среднее количество операций, выполняемых системой для определения наличия права доступа.

Чем сложнее схема и больше объектов, тем выше вычислительная сложность.

$$C_{\text{вычислительная}} \sim \log(\text{Количество пользователей}) * \log(\text{Количество групп}) * \text{Средняя глубина наследования групп} * \log(\text{Количество ресурсов}) * \text{Средняя глубина наследования ресурсов} * \log(\text{Среднее количество прав доступа для ресурса}) * \text{Средняя глубина наследования ролей в ресурсе}$$

Избыточность

Избыточность – свойство схемы, позволяющее назначать право доступа несколькими путями в один момент времени (за счет наследования).

В конечном итоге влияет на безопасность системы, например администратор может удалить пользователя из группы с целью отобрать у него право доступа к определенному ресурсу. Но при этом пользователь будет наследовать это право через другую группу.

$$K_{изб} = \frac{S(M^*)}{S(M^{*1})}$$

S(M) – сумма элементов матрицы M,
M* - матрица количества всех возможных путей в графе,
M^{*1} – матрица, полученная из M* путем замены всех ненулевых элементов на 1

Превышение доступа

Превышение доступа – получение пользователями системы не запрошенных прав доступа.

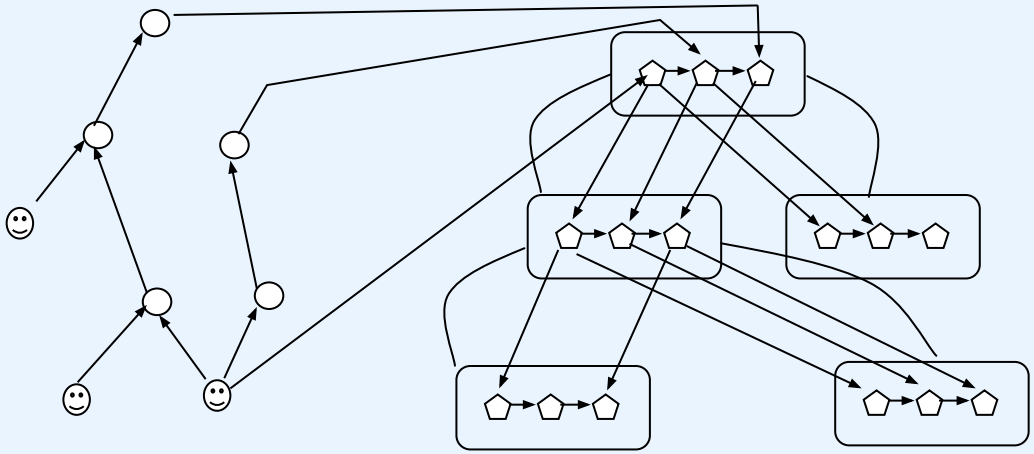
Возникает при наличии наследования. Пользователь может получить унаследованное право на ресурс, в то время как доступ к нему не был необходим.

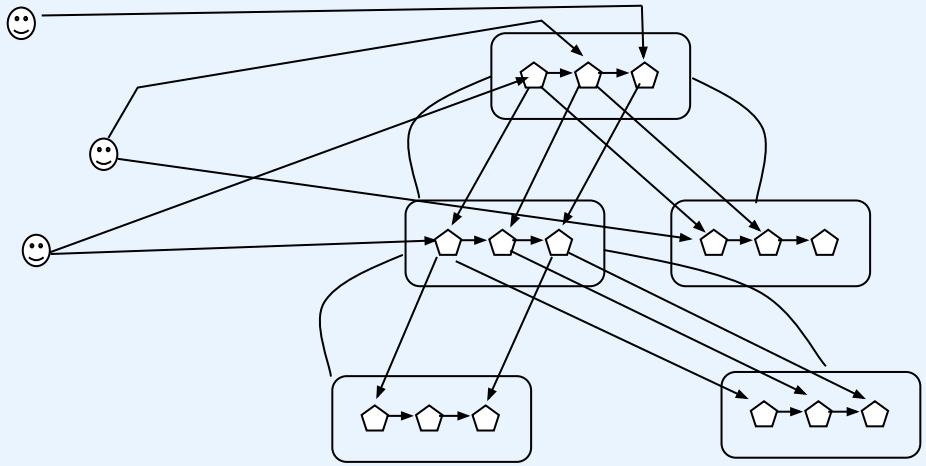
$$K_{прев} = \frac{\left| P^P - P^D \right|}{\left| P^D \right|}$$

P^D – множество запрошенных прав доступа,
P^P – множество предоставленных прав доступа

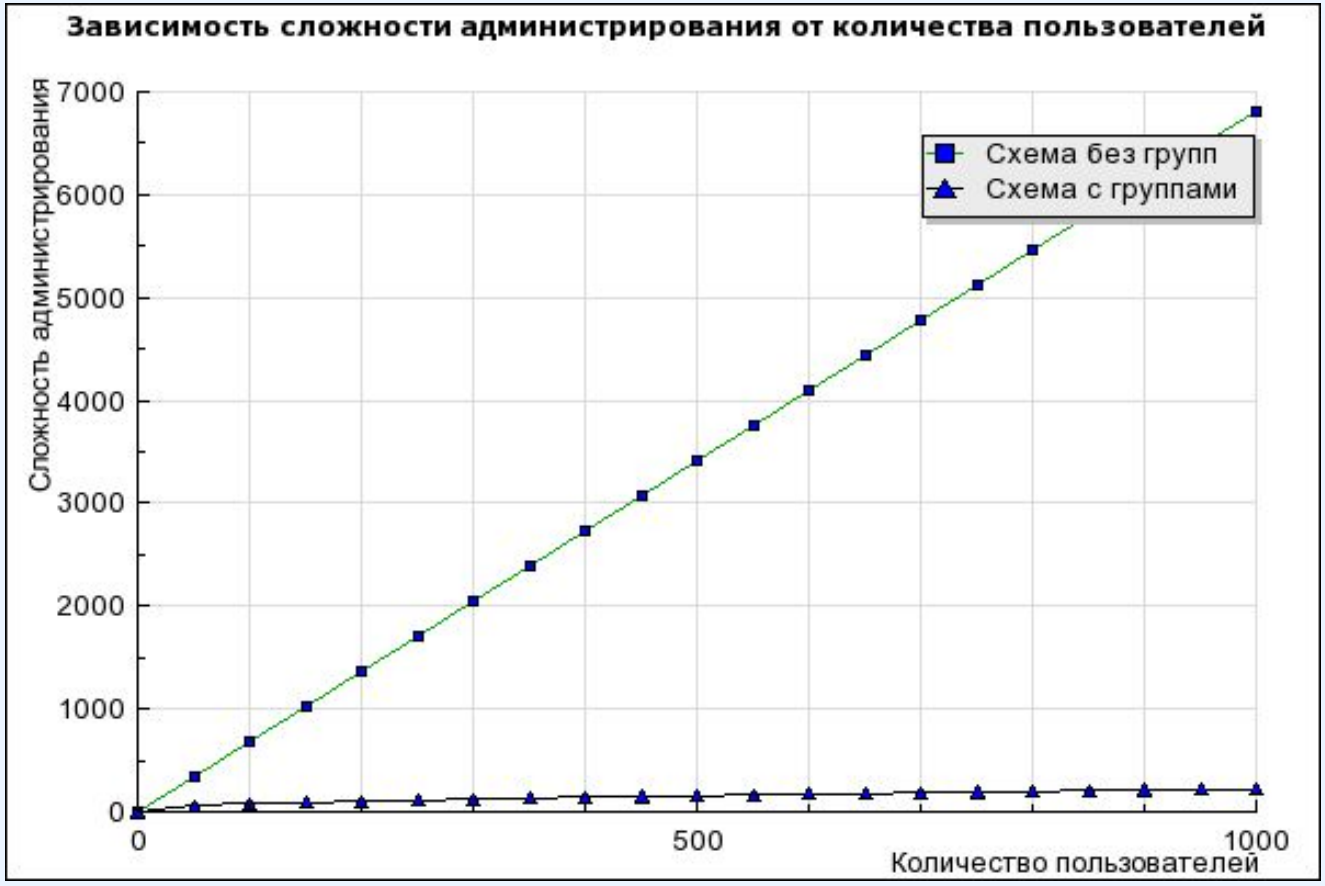
Сравнение различных схем

В качестве примера для сравнения приведем две схемы. В первой схеме используются группы пользователей, во второй группы отсутствуют.



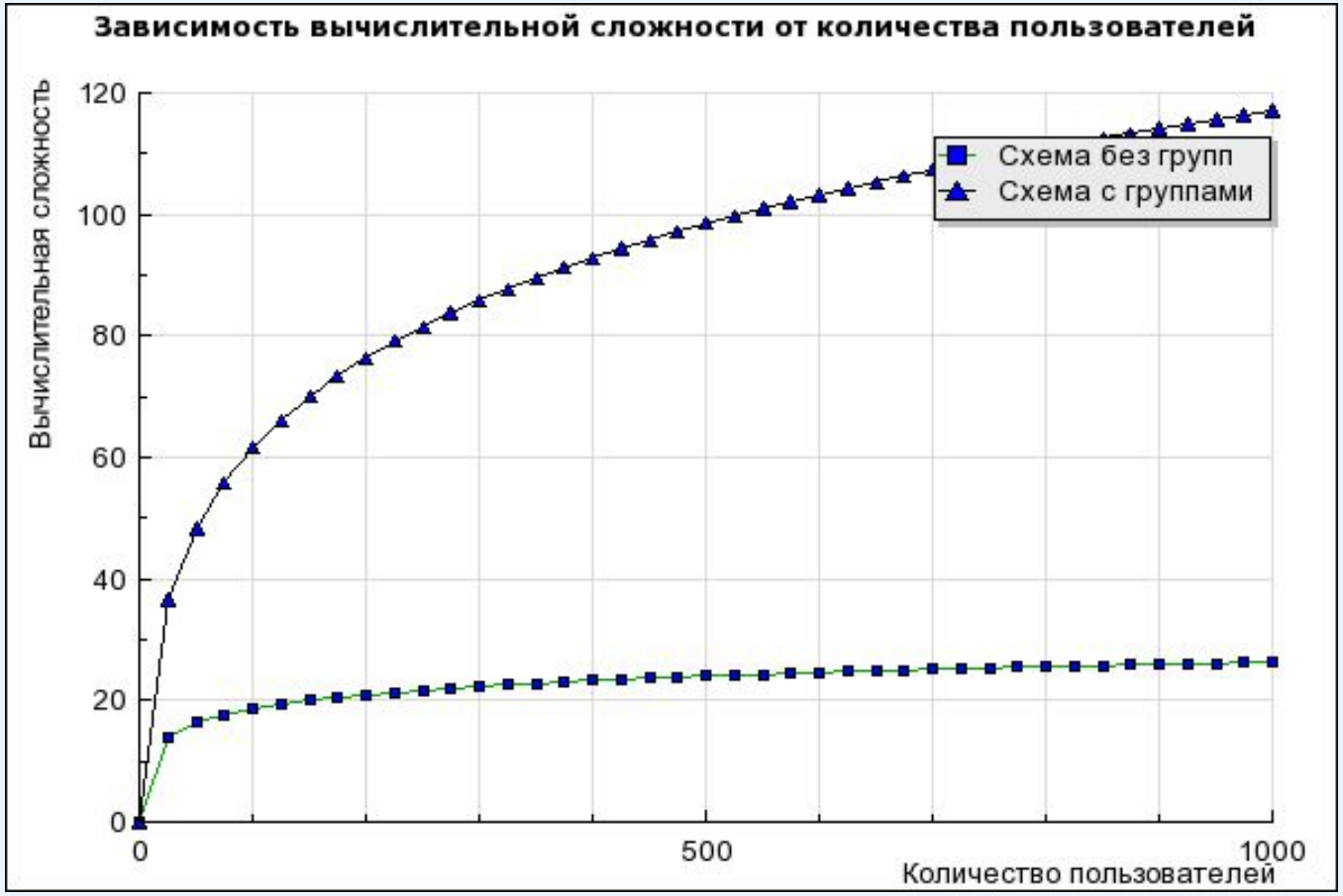


Зависимость сложности администрирования от количества пользователей



При наличии групп сложность администрирования значительно ниже.

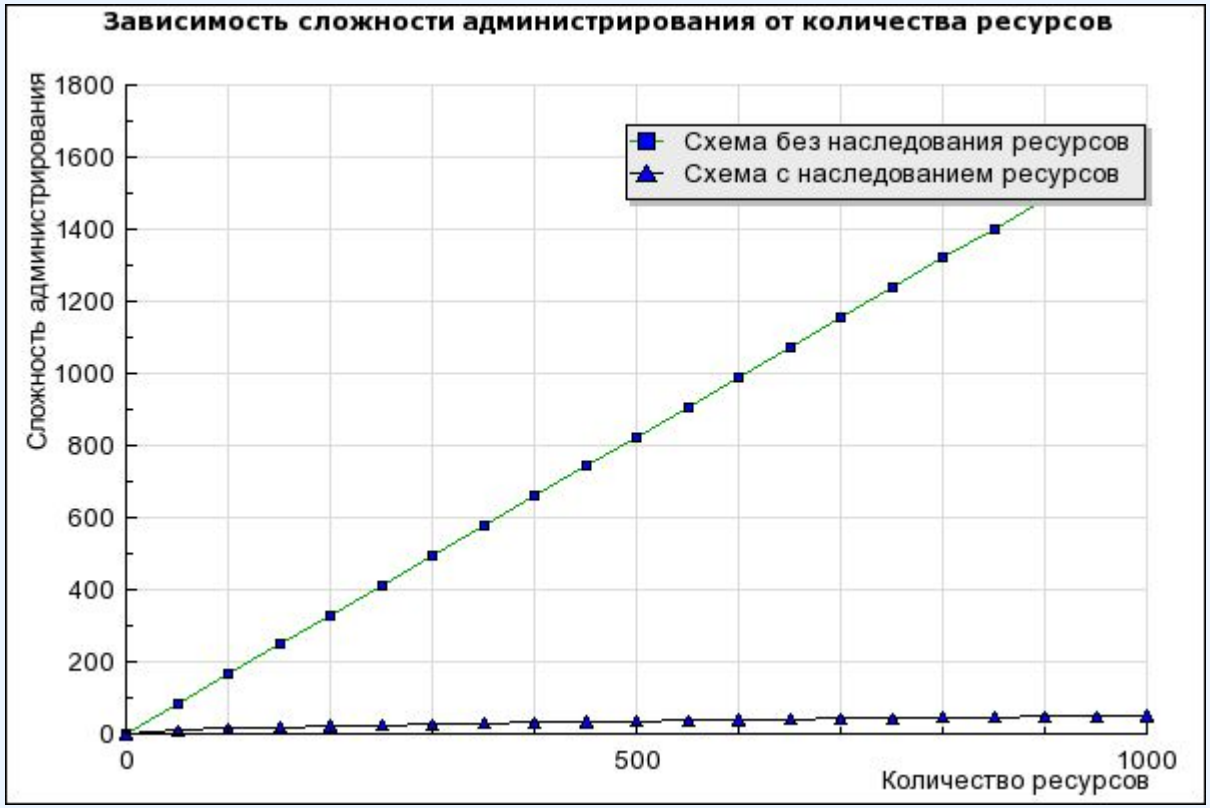
Зависимость вычислительной сложности от количества пользователей



В схеме с группами вычислительная сложность выше.

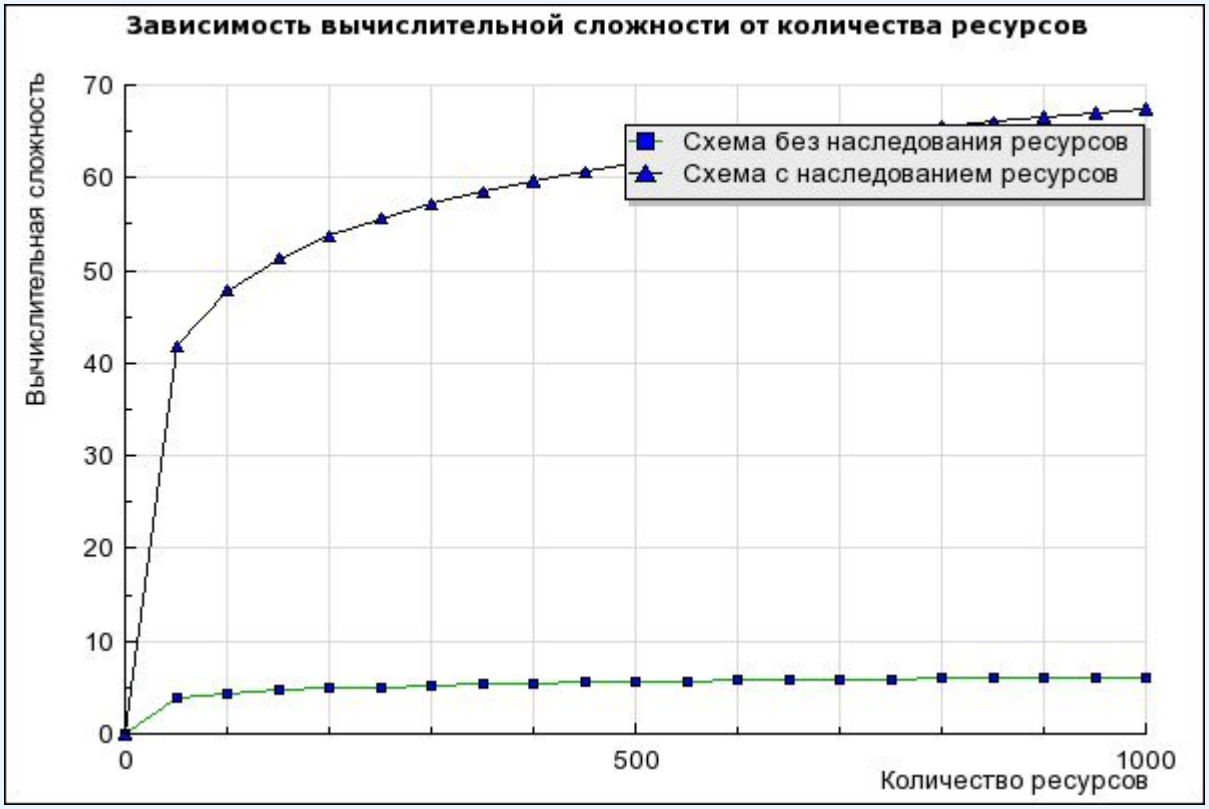
Зависимость сложности администрирования от количества ресурсов

Сравним две другие схемы. В первой присутствует наследование ресурсов, во второй – нет.



Наличие наследования ресурсов так же существенно снижает сложность администрирования, как и наличие групп пользователей.

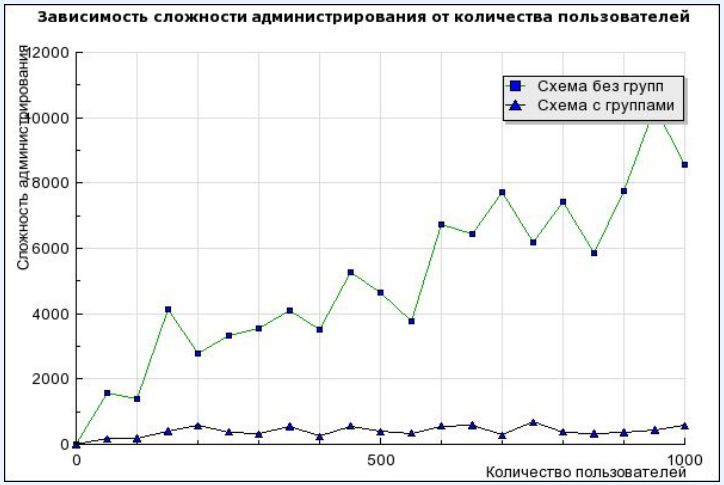
Зависимость вычислительной сложности от количества ресурсов

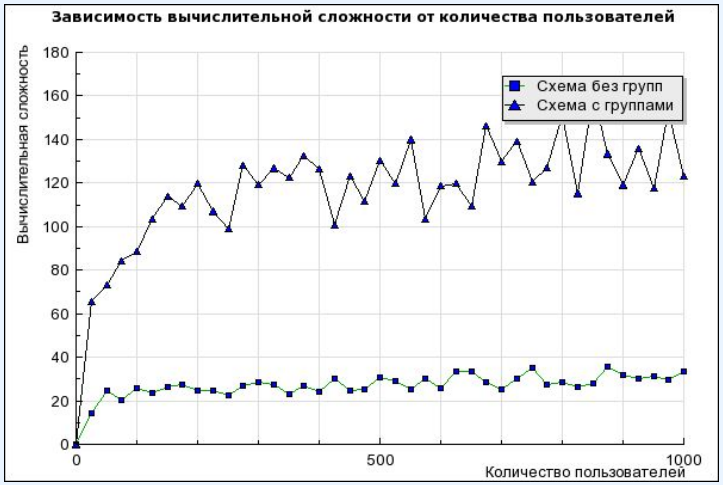


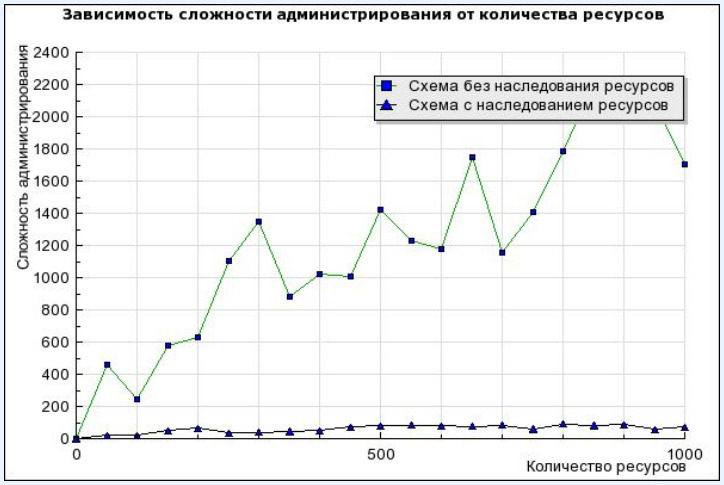
Вычислительная сложность при наличии наследования значительно выше, чем без наследования ресурсов.

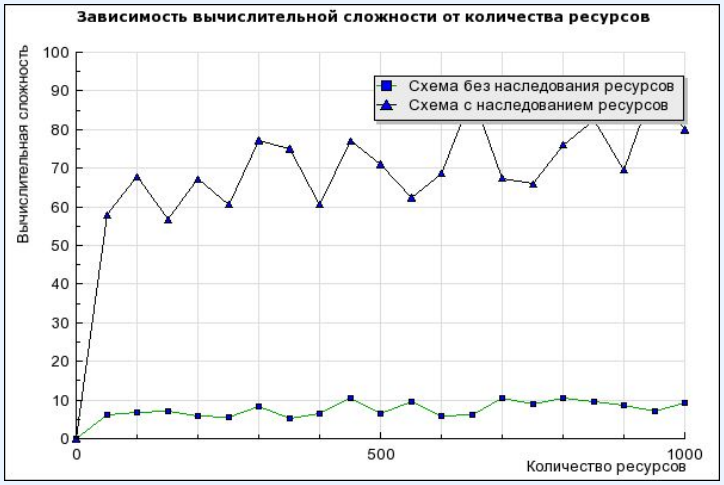
Имитационная модель

Для подтверждения результатов аналитической модели была разработана имитационная модель, эмулирующая различные схемы.
В ходе имитации был подтвержден характер зависимостей, проанализированных в аналитической модели.









Спасибо за внимание!

Докладчик:
Курмышев Николай Васильевич,
к.т.н.,
проректор по НИТ НовГУ,
Тел. +7 (8162) 62 72 18
E-mail: Nikolai.Kurmishev@novsu.ru

Новгородский государственный университет

www.novsu.ru