УДК 004.056.53

МЕТОДИКА ПОСТРОЕНИЯ ПРОСТРАНСТВА РЕШЕНИЙ В МОДЕЛИ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ ДОСТУПОМ НА ОСНОВЕ РОЛЕЙ

Д.В. Кириллов

Предлагается концепция автоматизированного управления доступом на основе ролей и методика построения пространства решений для автоматизированного выполнения операций, связанных с изменением состояния компонентов и отношений механизма разграничения доступа на основе ролей корпоративных информационных системах. Анализируются причины сложности управления механизмами управления доступа на основе ролей на основе данных экспериментальных исследований.

Ключевые слова: управление доступом, контроль доступа на основе ролей, событийно-обусловленное делегирование полномочий, пространство решений

Актуальность

При автоматизации механизмов управления доступом на основе ролей [1] главной задачей является построение пространства возможных решений о выполнении административных операций над компонентами и отношениями реализующими политику безопасности [2].

Для того, чтобы такое пространство было построено, необходимо определить, что выступает в качестве факторов, влияющих на принятие решения выполнении той или иной административной операции или операции по проверке полномочий. Основной вопрос, ответ на который позволяет принять решение, звучит как:

*Совокупностью каких свойств должен обладать субъект для того, чтобы иметь право выполнить определенное действие над объектом, обладающим определенным набором характеристик***.**

Таким образом, с позиции субъекта принимающим решение о выполнении операции необходимо выполнить следующие процедуры:

- P1. Определение значимых характеристик объекта (или объектов, в случае участия в рамках операции нескольких объектов) с точки зрения выполнения определенной операции;
- P2. Определение требуемых свойств субъекта необходимых для сопоставления свойства субъекта – операция – характеристики объекта
- P3. Определение функции сопоставления тройки (свойства субъекта, операция, характеристики объекта)
- P4. Вычисление булевого значения функции определенной в процедуре P3 на основании информации из P1 и P2.

Несмотря на кажущуюся простоту, решить поставленную задачу без участия человека не всегда представляется возможным, по следующим причинам:

- C1. Сложность или невозможность формализации значимых характеристик объектов с точки зрения принятия решения. Чаще всего, такая проблема возникает в тех случаях, когда значимые характеристики определяются семантикой содержимого. Данная проблема может быть решена путем дополнения объекта атрибутами, не семантического свойства, определяемыми до момента принятие решения.
- C2. Отсутствие у субъекта свойств, содержащих информацию, требуемую для принятия решения.
- C3. Невозможность формализации свойств субъекта необходимых для принятия решений
- C4. Невозможность формализации функций сопоставления из П3 однозначно определяющей положительность или отрицательность решения.

Эти причины являются *ограничениями* модели автоматизированного управления доступа, которые фактически разбивают все пространство возможных решений на два подпространства - формализуемых и неформализуемых.

Определяемое в результате выполнения процедур P1-P4 пространство решений и его структура должны, прежде всего, дать ответ на вопрос - возможно ли реализовать в заданной системе модель автоматизированного управления полномочиями. В идеальном слу-

чае, все пространство принятия решений является формализуемым. В худшем случае, все пространство решений является неформализуемым. Любое другое распределение пространства, является наиболее часто встречающимся случаем, и подразумевает, что в той или иной мере механизм автоматизированного управления доступа может применятся в такой системе.

В любом случае, кроме идеального, следующим этапом становится “улучшение” распределения внутри пространства решений. Гипотетически, любое предварительно определенное не формализуемое решение может быть преобразовано в формализуемое, за исключением тех случаев, когда отсутствует возможность формализовать функцию сопоставления P4. Однако, на основании имеющихся данных исследований, в большинстве случаев, такие случаи связаны с некачественной реализацией принципов управления организацией и бизнес-процессами реализуемыми в таких организациях.

Методика построения пространства принятия решений

Для того, чтобы определить пространство принятия решений по управлению доступом наиболее целесообразно использовать следующий алгоритм.

Этап 1. Построение пространства значимых характеристик объектов

1. Определение для каждого типа объектов набора полномочий, связанных с данным объектом;
2. Для каждого полномочия связанного с объектом определяются характеристики объекта значимые с точки зрения выполнения операции над объектом в рамках данного полномочия, а также агрегаты этих характеристик в случае иерархичности атрибутов;
3. Строится пространство характеристик, представляющее объединение выделенных характеристик объектов с учетом их эквивалентности.

Схематично результат такой последовательности действий представлен на рисунке 1.

Представленный на рисунке пример демонстрирует следующее. Объекты 1 и 2 типа обладают характеристиками *A1,A2,A3, A4* и *A1,A3,A5* соответственно. При этом над объектом первого типа определены операции O1 и O2, на объектом второго типа определена только операция O3. Связи между операциями и характеристиками показывают то, какие характеристики являются важными для принятия решения о допустимости выполнения операции над объектом данного типа при определенном значении соответствующей характеристики.

Исходя из рисунка видно, что в результате выделено четыре измерения характеристик, образующие пространство значимых измерений характеристик объектов системы.

Представленный на рисунке пример демонстрирует следующее. Объекты 1 и 2 типа обладают характеристиками *A1,A2,A3, A4* и *A1,A3,A5* соответственно.

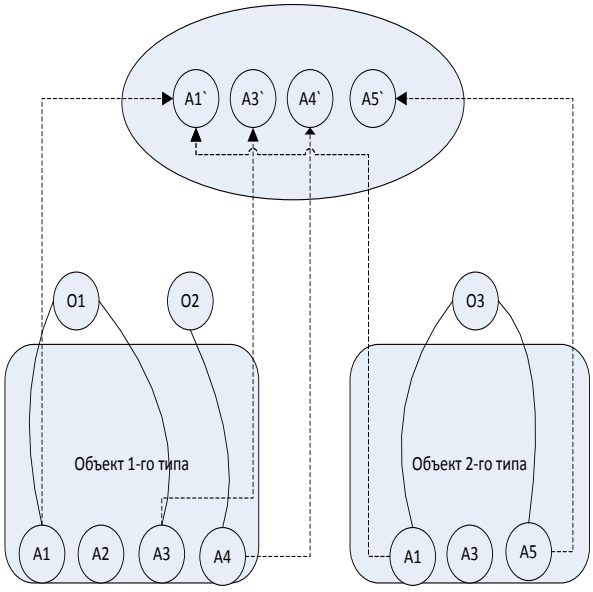

Рисунок 1 - Построение пространства характеристик объектов

При этом над объектом первого типа определены операции O1 и O2, над объектом второго типа определена только операция O3. Связи между операциями и характеристиками показывают то, какие характеристики являются важными для принятия решения о допустимости выполнения операции над объектом данного типа при определенном значении соответствующей характеристики. Из рисунка видно, что в результате выделено четыре измерения пространства характеристик, образующие пространство значимых измерений характеристик объектов системы.

Другими словами, субъект, принимающий решение о назначении пользователю некоторой роли включающей полномочия по выполнению операций *O1 и O2* над объектом 1-го типа и *O3* над объектом 2-го типа, будет учитывать значимые характеристики этих объектов. С другой стороны характеристика A2 не будет учитываться при принятии решения.

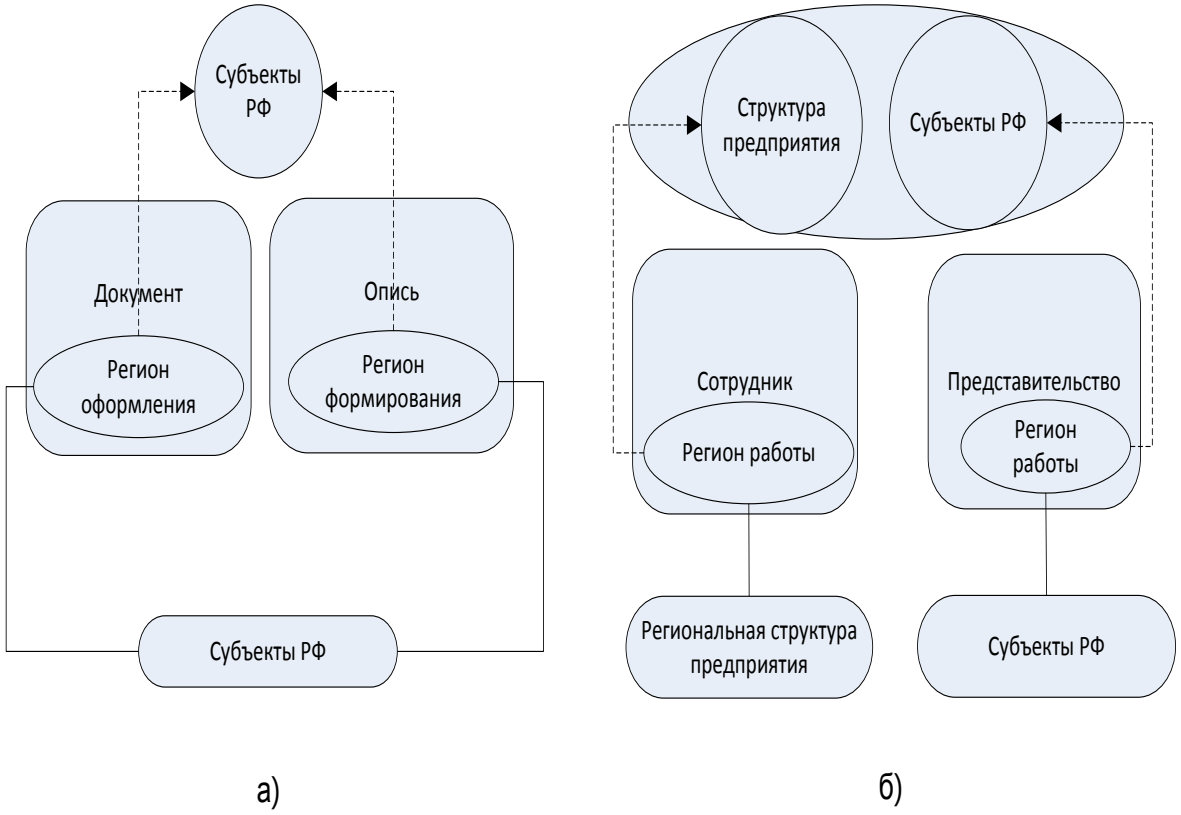

Рисунок 2 - Измерения характеристик, а) эквивалентные, б) неэквивалентные

При выполнении процедуры построения пространства, важным является то, что объединяемые измерения должны быть эквивалентными. Например, в структуре, представленной на рисунке 2а, представлены эквивалентные измерения для разных объектов, а на рисунке 2б, несмотря на то, что характеристики объектов имеют совпадающие наименования, фактически они должны существуют в различных измерениях.

Полученное пространство характеристик объектов само по себе не определяет того, каким образом будут определяться полномочия, но фактически замыкают множество характеристик объектов всех типов системы, значимых с точки зрения принятия решений.

Несмотря на то, что на первый взгляд, количество измерений характеристик, получаемое в результате анализа типов объектов системы, может быть очень большим, в реальности это не так, что подтверждается, в том числе и результатами экспериментальных исследований разнородных систем приведенных в таблице 1.

Как видно из результатов, представленных в таблице, связь между количеством типов объектов и количеством измерений характеристик напрямую не прослеживается. Качественный же анализ показал, что куда большее значение имеет предметная область (или области) охватываемая соответствующей системой и теми принципами организационного управления, которые реализуются в этой организации, другими словами, большее влияние оказывают “разнородность” типов объектов и сложность структуры организации.

Кроме измерений характеристик объектов, дополнительно определяется измерение типов объектов, так как очевидно, что тип объекта также является одновременно и характеристикой объекта, представленной в неявном виде. Также вероятна ситуация, при которой тип объекта является единственной характеристикой, значимой с точки зрения предоставления прав доступа.

Еще одним “виртуальным” измерением является так называемое измерение ключевой идентификации. Это измерение отображает ключевые идентификаторы тех объектов, возможность выполнения тех или иных операций над которыми зависит только от того, установлена ли эта возможность для конкретного объекта или нет. В идеальном случае, такое измерение в пространстве должно отсутствовать, так как наличие такого

измерения однозначно показывает, что полностью замкнуть на самой системе пространство решений по предоставлению доступа невозможно. Следовательно, невозможно и полностью автоматизировать процесс управления полномочиями, так как фактически существует некоторые неформализуемые внешние факторы необходимые для принятия и реализации такого решения.

Определив пространство характеристик можно сказать, что любое полномочие лежит в определенной проекции построенного пространства, таким образом, пространство принятие решений с точки зрения объектов системы полностью замыкается.

Таблица 1. Результаты экспериментального построения пространств

Система	Кол-во типов объектов	Кол-во измерений пространства характеристик
S_1	1200	12
S_2	1208	8
S_3	1301	6
S_4	34	7
S_5	219	14
S_6	3210	4
S_7	88	5
S_8	21	2
S_9	982	8
S_{10}	4506	9
S_{11}	1301	6
S_{12}	57	5
S_{13}	124	7
S_{14}	1208	8
S_{15}	456	9
S_{16}	211	3
S_{17}	120	2
S_{18}	112	5
S_{19}	1301	6
S_{20}	506	7
S_{21}	780	9
S_{22}	2140	5

Этап 2. Построение пространства значимых характеристик субъектов

Следующим шагом, является построение пространства характеристик субъектов, которые важны для предоставления доступа на выполнение некоторой операции над тем или иным объектом системы.

Для объекта каждого типа определяются характеристики субъектов, необходимые для того чтобы субъект мог выполнить какую-либо операцию над объектом данного типа. Здесь возможно использовать два подхода:

В первом подходе происходит абстрагирование от конкретной операции над объектами каждого типа, а фактически определяются все возможные характеристики требуемые для фактического доступа к субъекту, безотносительно того какая операция подразумевается под доступом [5].

Во втором подходе анализируются все возможные сочетания операция-объект (т.е. полномочия), для каждого полномочия определяется требуемые характеристики субъекта и в дальнейшем путем объединения характеристик, формируются измерения пространства принятия решений для субъектов.

Первый способ позволяет решить задачу более быстро, однако второй способ позволяет уже на первом этапе построения пространства решений избежать потери измерений.

Как и для пространства характеристик объектов, для пространства субъектов существуют особые измерения – измерения типов субъектов и измерение ключевой идентификации и также как и для объектов, наличие измерения ключевой идентификации свидетельствует о том, что полностью замкнуть пространство принятия решений на системе невозможно.

Этап 3. Замыкание пространств субъектов и объектов

Построенное пространство характеристик субъектов, изначально не пересекается с пространством характеристик объектов, так как в соответствии с моделью контроля доступа на основе ролей между ними не существует какой-либо ассоциативной связи. Кроме того, в отличие от характеристик объектов, которые полностью определяются в системе, характеристики субъектов могут вообще не определяться в системе на уровне объектов, т.е. исходя из принятой нами терминологии множество субъектов не замкнуто над системой.

Для того, чтобы осуществить замыкание пространства характеристик субъектов на системе, для последующего построения общего пространства характеристик объектов, необходимо ассоциировать характеристики субъекты системы с объектами этой системы. Это принципиально возможно в том случае, если:

1. Информация о субъекте системы существует в объектах данной системы;

2. Существует механизм отображения субъекта в объекты данной системы.

3. Характеристики субъектов системы могут быть выражены через объекты системы и их характеристики.

В том случае, если данные условия не выполнимы, пространство характеристик субъектов не может быть полностью замкнуто на систему.

Существующие расширенные модели контроля доступа на основе ролей, такие как например атрибутная или основанная на правилах, решают проблему разомкнутости пространства характеристик субъектов по отношению к объектам путем дополнения субъектов характеристиками из пространства характеристик объектов. Проблемы такой концепции заключаются в следующем:

1.Избыточность данных – фактически, происходит искусственное дублирование информации как правило из уже существующих объектов уровня бизнес-логики и их характеристик;

2.Порождение искусственных потоков данных между административными субъектами и компонентами подсистемы безопасности, для которых трудно обеспечить приемлемый уровень синхронизации с изменением реальных объектов-источников данных;

3.Формирование сложных характеристик субъектов практически не возможно, так как это приводит в некоторых случаях к полному дублированию информации содержащейся в реальных объектов-источников данных.

Вместо этого, в предлагаемой концепции автоматизированного управления доступом на основе ролей, используется подход основной на связывании субъектов и их характеристик с объектами и их характеристиками на основе определяемых функциональных зависимостей. В этом случае, субъекты связываются с объектами на основе функциональных зависимостей корректных для данной системы с целью отображения характеристик субъектов на характеристики объектов. В том случае, если для характеристик субъектов невозможно определить соответствующие характеристики в пространстве характеристик объектов, то происходит процедура обогащения объектов теми данными, которые необходимы для связывания, при этом источником этих данных являются те субъекты системы, которые являются источниками данных и для других характеристик соответствующих объектов [3].

Таким образом, пространство характеристик субъектов и объектов замыкается за исключением следующих случаев:

1. Характеристики не могут быть формализованы ни в объектах и их характеристиках, ни в характеристиках субъектов;

2. Характеристики субъектов не могут быть формализованы в объектах и их характеристиках, так как характеризуют субъект как компонент подсистемы безопасности.

Первый случай по аналогии со случаем описанным для объектов определяет неформализуемые характеристики субъектов, соответственно такие характеристики аналогичны измерению ключевой идентификации.

Второй случай подразумевает, то что, несмотря на то, что определяемые в нем измерения не имеют совпадений с измерением пространства характеристик объектов. Тем не менее, такие измерения, вполне могут быть включены в общее пространство характеристик субъектов, но источником показателей данных характеристик не будет являться уровень бизнес-логики системы, что, однако не мешает использовать их при автоматизированном принятии решения о назначении полномочий.

Этап 4. Построение пространства значимых характеристик ролей

Роль является центральным понятием контролем доступа на основе ролей, так как фактически управление полномочиями в системах реализующих КДОР строится вокруг управления ролями – полномочия назначаются пользователям, роли назначаются пользователям. Полномочия субъектов таким образом полностью определяются совокупностью полномочий назначенных пользователей ролей. Таким образом, роль выступает некоторым абстрактным контейнером полномочий.

Изначально, авторами модели контроля доступа на основе ролей предполагалось отождествление роли с понятием должности в контексте организационного управления [1].

Ключевой проблемой такого подхода является то, что, пользуясь терминологией рассматриваемой концепции пространства характеристик, предполагается одномерность пространства характеристик субъектов с единственным измерением – должностью организационной структуры. Действительно, в случае одномерного пространства характеристик субъектов, мощность множества ролей будет равняться множеству показателей соответствующего измерения.

Однако при добавлении каждого нового измерения мощность множества ролей будет стремительно расти, и в случае независимых измерений будет, равна мощности декартова произведения множеств показателей соответствующих измерений.

Для того чтобы правильно определить пространство характеристик ролей, предлагается использовать следующие принципы:

1. Пространство характеристик ролей есть подпространство характеристик субъектов;

2. Пространство характеристик ролей не должно включать

3. Отношение мощности множества ролей получаемого над пространством характеристик к мощности декартова произведения мощностей множеств показателей измерений субъектов должна должно быть минимально возможной.

Этап 5. Построение функций принятия решений

Функции принятия решения по управлению доступом, делятся на два класса:

1. административные функции - выполняемые административными субъектами для изменения компонентов и отношениями ПБ;

2. функции проверки прав доступа – функции вызываемые системой для фактической проверки прав доступа.

Функции принятия решения представляют собой булевы функции, аргументами которых являются:

1. для функций первого класса - проекции пространств характеристик компонентов, в зависимости от того, над какими компонентами выполняется действие. В функции реализуется непосредственно алгоритм отображения связанных между собой характеристик компонентов;

2. для функций второго класса это проекция пространства характеристик по отношению к четверке (субъект, роль, операция, объект). Функция реализует сопоставление показателей проекций и дает истинный результат в том случае, если условия сопоставления характеристик выполнены и ложный, в том случае если это не так.

В общем случае, логика алгоритма каждой функции определяется в каждом конкретном случае, однако как показывает практика, зачастую существует возможность вынесения логики в отдельные общие функции, в тех случаях, когда используется достаточно небольшой, часто применяемый набор условий. Выделение таких условий с одной стороны значительно упрощает управление системой, а с другой – позволяет решить задачу универсализации и масштабируемости подсистемы управления доступа.

Выводы

Таким образом, представленная методика построения пространства решений для модели автоматизированного управления доступом на основе ролей является необходимым условием корректной реализации такой модели. Она позволяет осуществить принципиальную возможность замыкания пространства компонентов подсистемы разграничения доступа и объектов уровня бизнес-логики, что является одним из условий корректного решения задачи автоматизации процессов администрирования ПБ и принятия решения о предоставлении доступа в автоматизированных системах различных классов [5].

СПИСОК ЛИТЕРАТУРЫ

1. Sandhu, R. Role-based access control models / R. Sandhu, E. Coyne, H. Feinstein, C.Youman. // IEEE Computer, 29(2):38-47, 1996.

2. Кириллов, Д.В. Основные принципы событийно-обусловленного делегирования полномочий в системах контроля доступа на основе ролей [Текст] / Д.В. Кириллов // Вестник УГАТУ, 2009. - т.1(30). - с. 218-225.

3. Кириллов, Д.В. Классификация моделей делегирования полномочий в контроле доступа на основе ролей [Текст] / Д.В. Кириллов // Доклады Томского государственного университета систем управления и радиоэлектроники, 2010 - № 1(21) - с. 146-150.

4. Кириллов, Д.В. Особенности механизма обработки событий в СОДОП [Текст] / Д.В. Кириллов // Материалы Зимней школы аспирантов и молодых ученых УГАТУ. - Уфа, 2009.

5. Миронова, В.Г. Методика классификации ИС, обрабатывающих конфиденциальную информацию ролей [Текст] / В.Г. Миронова // Ползуновский вестник. - Барнаул: АлтГТУ, 2013. - №2. - с. 259-264.

Кириллов Д.В., *старший преподаватель кафедры безопасности информационных систем, аспирант кафедры БИС, Email: kirillov@ssu.samara.ru - ГОУ ВПО "Самарский государственный университет"*