Improved role-based access control model

Andrew Mayorov
BYTE-force
email: xor@byte-force.com

Abstract (English)

Paper covers general principles of building of access-control subsystems in applications and briefly describes base models which are usually employed thereto: mandatory, discretionary and role-based access controls. Paper considers restrictions of base role-based access control (RBAC) model which is widely adopted in modern applications due to relative simplicity of administration.

Paper in details covers features and components of access control model developed by authors, and shows that this model is free from restrictions of base role-based model. It proves that using new model it's possible to implement base discretionary and role-based models. There are also possibilities to combine presented model with mandatory access control.

Keywords: *access control models, role-based access control.*

Улучшенная ролевая модель управления доступом

А.В.Майоров
BYTE-force
email: xor@byte-force.com

Abstract (Russian)

В статье освещаются общие принципы построения систем безопасности, и дается описание базовых моделей, обычно использующихся для этой цели. Детально рассматриваются ограничения ролевой модели, которая, из-за сравнительной простоты администрирования, является предпочтительной к использованию в прикладных программах.

Подробно описываются возможности и составные части разработанной нами модели, и показывается, что она лишена вышеупомянутых ограничений. Доказывается, что в рамках предлагаемой модели можно реализовать базовые ролевую и дискреционную модели, а также обсуждаются возможные пути соединения ее с мандатной моделью. В заключении подчеркивается основное отличительное свойство нашей модели и кратко говорится о преимуществах, которые оно несет.

Keywords*: access control models, role-based access control.*

1. Постановка задачи и результат

Перед нами стояла задача разработать модель управления доступом к объектам приложения, позволяющую реализовывать любую разумную политику безопасности приложения, оставаясь при этом максимально удобной в администрировании.

В результате получена модель, которая, с одной стороны, совместима с известными базовыми моделями, а с другой стороны, вводит дополнительную степень свободы – привязку пользовательских полномочий к иерархии объектов системы. Подобная привязка позволяет ограничить область действия выданных пользователю полномочий и, как следствие, упростить схемы доступа к объектам.

2. Базовые модели

Общим подходом для всех моделей управления доступом является разделение множества сущностей, составляющих систему, на множества объектов и субъектов. При этом определения понятий «объект» и «субъект» могут существенно различаться. Мы будем подразумевать, что объекты являются некоторыми контейнерами с информацией, а субъекты – пользователи, которые выполняют различные операции над этими объектами.

Можно выделить три основные модели управления доступом к объектам: мандатную, дискреционную и ролевую.

3. Мандатная модель

Классической мандатной моделью считается модель Белла-ЛаПадулы [[1]]. Она базируется на правилах секретного документооборота, использующегося в правительственных учреждениях. В этой модели каждому объекту и субъекту (пользователю) системы назначается свой уровень допуска. Все возможные уровни допуска системы четко определены и упорядочены по возрастанию секретности. Действуют два основных правила:

1. Пользователь может читать только объекты с уровнем допуска не выше его собственного.
2. Пользователь может изменять только те объекты, уровень допуска которых не ниже его собственного.

Цель первого правила очевидна. Смысл второго в том, чтобы воспрепятствовать пользователю с высоким уровнем доступа случайно раскрыть какие-то известные ему тайны.

Одной из проблем этой модели считается беспрепятственность обмена информацией между пользователями одного уровня, так как эти пользователи могут выполнять в организации разные функции, и то, что имеет право делать пользователь А, может быть запрещено для Б. Поэтому в практике мандатную модель обычно используют совместно с какой-нибудь другой [[2]] [[3]].

4. Дискреционная модель

В дискреционной модели безопасности управление доступом осуществляется путем явной выдачи полномочий на проведение действий с каждым из объектов системы. Например, в модели Харрисона-Руззо-Ульмана [[4]] для этого служит матрица доступа, в которой определены права доступа субъектов системы к объектам. Строки матрицы соответствуют субъектам, а столбцы – объектам. Каждая ячейка матрицы содержит набор прав, которые соответствующий субъект имеет по отношению к соответствующему объекту.

Как правило, создатель объекта обладает на него полными правами и может делегировать часть прав другим субъектам.

Дискреционный подход позволяет создать гораздо более гибкую схему безопасности, чем мандатный, но при этом он и гораздо более сложен в администрировании. С программной точки зрения его реализация очень проста, но при достаточно большом количестве объектов и субъектов система становится практически неуправляемой.

Частично решить эту проблему позволяет группировка пользователей и типизация объектов. Применение этих методов существенно уменьшает матрицу доступа и, соответственно, упрощает ее администрирование.

5. Ролевая модель

В ролевой модели [[1]] операции, которые необходимо выполнять в рамках какой-либо служебной обязанности пользователя системы, группируются в набор, называемый «ролью». Например, операции по регистрации документов могут быть сгруппированы в роль «регистратор».

Каждый пользователь системы играет в ней одну или несколько ролей. Выполнение пользователем определенного действия разрешено, если в наборе его ролей есть нужная, и запрещено, если есть нежелательная.

В этой модели у объектов нет определенных хозяев. Вся информация расценивается как принадлежащая организации, владеющей системой. Соответственно, и роли пользователя внутри системы – это роли, которые он играет в данной организации. Как следствие, пользователю невозможно делегировать права на какой-то определенный объект. Либо у него есть доступ ко всем подобным объектам системы, либо нет.

Таким образом, преимуществом ролевой модели перед дискреционной является простота администрирования: назначение пользователей на роли и создание новых ролей не составляют никаких трудностей. Это позволяет рассматривать ролевую модель как наиболее подходящую для применения в

прикладных программах. В то же время в ней есть ограничения, которые в ряде случаев сильно затрудняют ее использование. Рассмотрим эти ограничения более подробно.

5.1 Ограничение: все роли глобальны

Первое ограничение состоит в том, что пользователь принимает свои роли по отношению ко всей системе сразу. Соответственно, для системы нет разницы в правах между двумя пользователями, находящимися на одинаковой должности, даже если они занимают эти должности в разных отделах. Например, любой пользователь в роли «начальник отдела» имеет право управлять любым отделом своей организации, а это, конечно, неправильно.

Решением могло бы стать введение отдельных ролей «начальник отдела А», «начальник отдела Б» и т.п., что позволило бы нам решить проблему, не выходя за рамки ролевой модели. К сожалению, подобный вариант привносит гораздо больше проблем, чем решает.

Более правильным будет разбить все множество объектов системы на несколько подмножеств (доменов) и дать пользователям возможность играть разные роли в разных доменах системы. Такой подход применяется, например, в библиотеке Microsoft Authorization Manager [[6]].

5.2 Ограничение: отсутствие владельца объекта

Второе препятствие перед использованием ролевой модели в ряде систем – это отсутствие в ней понятия владельца объекта. Другими словами, пользователь, создавший объект, не имеет на него никаких исключительных прав. Это вполне приемлемо для систем, поддерживающих, например, процесс купли-продажи, но перестает годиться, как только документы начинают содержать какие-то авторские материалы.

Зачастую для решения этой проблемы к объектам системы добавляют свойство «владелец», являющееся внешним по отношению к модели безопасности. Другой подход – ввести в ролевую модель элементы дискреционной и явным образом дать пользователю нужные права на созданный им объект.

Заметим, что оба эти варианта решают задачу, используя внешние по отношению к модели средства, и, соответственно, не снимают ограничений самой модели.

5.3 Ограничение: операции принадлежат ролям

Казалось бы, группировка операций системы в роли, в рамках которых они выполняются, упрощает администрирование, но это снова верно не для всех типов систем. Предположим, что в нашей системе есть десять различных типов объектов, для каждого из которых определена операция «удалить». Тогда, если мы добавляем эту операцию в какую-либо из ролей, то любой пользователь, играющий эту роль, получает право удалять объекты любого типа. Очевидно, что это далеко не всегда является желательным поведением.

Можно попытаться решить эту проблему, введя десять различных операций, предназначенных для удаления объекта каждого из типов. Такое решение оказывается не очень удачным, если типов не десять, а, например, сто.

Проблема еще более усугубляется, если в системе возможны различные схемы доступа к разным объектам одного типа. Например, объекты неких типов могут быть или открытыми для публики, или совершенно секретными. Создавать действия «удалить публичный объект», «удалить секретный объект» и т.п. кажется совершенно неразумным.

На практике, при использовании ролевой модели в сложных системах, разработчики обычно не пытаются декларативно задавать схему доступа к объектам системы. Вместо этого процедура проверки встраивается в нужное место программы. При этом проверяются как сведения, предоставляемые модулем ролевой безопасности (т.е. роли, в которых выступает пользователь), так и любые другие сведения об объекте (владелец объекта, уровень секретности и т.п.).

Подобный подход затрудняет изменение схемы доступа, так как для этого нужно исправлять код процедуры проверки и перекомпилировать приложение.

6. Улучшенная ролевая модель (модель ForceField)

ForceField – это разработанная нами модель управления доступом, которая позволяет создавать простые в администрировании политики безопасности. Она является существенно более мощной, чем ролевая модель, и при этом лишена ее основных недостатков.

6.1 Дерево объектов

Мы обсуждали проблему диапазона действия ролей в базовой ролевой модели [[1]] и вариант ее решения с использованием доменов. Недостаток этого решения в том, что домены нужно создавать вручную, и они явным образом не связаны ни с какими объектами системы. К тому же отсутствует иерархия доменов, а значит, наборы ролей пользователя в разных доменах приложения совершенно независимы. Это создает трудности, если пользователь должен играть определенную роль во всей системе сразу – его придется назначить на эту роль в каждом домене в отдельности.

В модели ForceField все объекты системы объединяются в единое дерево. У каждого объекта, кроме единственного корневого, есть один родительский объект, и любое количество дочерних. Роль может быть назначена пользователю в контексте любого объекта. При этом пользователь начинает играть назначенную роль во всей ветви дерева, которая образована этим объектом.

Таким образом, любой объект приложения образует домен, в который входит он сам и все его дочерние объекты. Его дочерние объекты образуют домены, являющийся подчиненными по отношению к домену родительского объекта. Список ролей, которые пользователь играет в определенном домене, состоит из ролей, назначенных ему в данном домене, плюс роли из доменов вверх по иерархии. Роли, назначенные пользователю в корневом домене, имеют глобальный характер, т.е. действительны в контексте каждого объекта приложения.

6.2 Роль «владелец»

Вернемся еще раз к проблеме отсутствия владельцев у объектов в базовой ролевой модели. В качестве решения подойдет любой механизм, позволяющий выделить хозяина объекта и дать ему особые права на этот объект. В нашей модели для этого вводится роль «владелец», назначающаяся пользователям в контексте тех объектов, которыми они владеют.

Эта роль по своему поведению отличается от других ролей. Во-первых, только один пользователь может играть роль «владелец» в контексте какого-то определенного объекта. Во-вторых, объект не должен наследовать роль «владелец» от родителя, если в его собственном контексте такая роль кому-либо назначена.

Развивая эту идею, заметим, что роль может быть ограничена не только одним актером, но и большим их количеством. Таким образом, если роль ограничена *n* пользователями, то в контексте любого объекта системы не больше *n* пользователей могут играть эту роль. При этом, очевидно, что в системе в целом у этой роли может быть больше *n* назначений.

В базовой модели подобные ограничения называются кардинальностью роли и определены как максимальное количество пользователей, которые могут играть эту роль в рамках всей системы.

6.3 Класс доступа

Мы упоминали, что, хотя распределение операций по ролям кажется логичным, оно весьма затрудняет разработку схемы безопасности. Использование же сценариев для проверки прав доступа усложняет администрирование системы.

Для создания гибкой схемы безопасности без ручного программирования сценариев проверки, в ForceField введено понятие «класс доступа». Класс доступа содержит набор правил, задающих права выполнения определенных операций для определенных ролей. Порядок следования правил важен, так как при проверке поиск ведется сверху вниз до тех пор, пока не будет найдено правило, подходящее проверяемой ситуации. Правило из нашего примера подойдет, если будет запрошено разрешение на удаление объекта, а пользователь в контексте этого объекта будет администратором.

Каждому объекту системы ставится в соответствие ровно один класс доступа, а любой класс доступа может быть назначен произвольному количеству объектов. Это позволяет иметь в системе несколько разных схем доступа к объектам, не заставляя нас связывать эти схемы с типами или какими-то другими признаками объектов. Отметим также, что назначения классов никак не связаны с иерархией объектов: дочерний объект может иметь любой класс доступа, независимо от того, какой класс назначен родительскому объекту.

Класс может базироваться на другом классе, так что, если подходящего правила в классе нет, будет просмотрен базовый класс, потом его базовый класс и так далее. Если правило так и не будет найдено, то операция считается запрещенной. Этот механизм также служит для упрощения администрирования системы.

Перечислим некоторые возможные варианты распределения классов по объектам:

1. У всех объектов одного типа один и тот же класс доступа. Следует применять в системах, где различные типы отличаются друг от друга по правилам контроля доступа, но все объекты одного типа ведут себя одинаково.
2. Есть несколько классов доступа, которые могут быть назначены любому объекту, независимо от его типа. Например, классы, определяющие уровень секретности информации (публичная, для служебного пользования, совершенно секретная).
3. Есть всего один класс доступа, который назначается всем объектам.

6.4 Наследование резолюции сверху

Существует также механизм наследования правил доступа от вышестоящих объектов. Подобный механизм часто встречается в файловых системах (дискреционная модель): файлы, лежащие в папке, могут не иметь своих собственных правил доступа, наследуя эти правила у папки.

В ForceField это реализуется следующим образом: в любом правиле класса кроме резолюций «разрешено» и «запрещено» можно использовать вариант «проверь родителя». В этом случае, для выдачи окончательного ответа будет проверено, можно ли данному пользователю выполнить запрашиваемое действие по отношению к родительскому объекту. Естественно, этот процесс может быть рекурсивным. Если по достижении корня иерархии объектов, явного разрешения или запрета так и не будет найдено, то действие считается запрещенным.

Чтобы продублировать описанное выше поведение файловой системы, достаточно создать класс, в котором объект наследует от родителя права на выполнение всех операций.

В то же время наша модель позволяет и такой вариант, когда права на часть операций наследуются, а для другой части задаются явным образом.

7. Гибридность модели ForceField

Докажем, что предлагаемая нами модель позволяет реализовать в своих рамках функциональность базовых ролевой и дискреционной моделей.

7.1 Реализация ролевой модели

Предположим, что в нашем приложении четыре объекта двух различных типов: A_1, A_2, B_1, B_2. Существуют две операции, которые можно выполнить над объектом типа A, и одна для объектов типа B: op_{A1}, op_{A2}, op_{B1}. Также в системе зарегистрировано два пользователя: U_1 и U_2.

Базовая ролевая модель предписывает нам ввести в систему роли и распределить операции между ролями. Введем следующие роли. Роль r_1 включает в себя операции op_{A2} и op_{B1}, а роль r_2 – операцию op_{A1}. Назначим на роли пользователей: U_1 играет в системе роль r_2, а U_2 – обе роли. Напомним, что пользователь, назначенный на определенную роль, имеет право выполнять операции, входящие в эту роль, по отношению к любому объекту системы.

Эта схема проиллюстрирована рисунком 1.

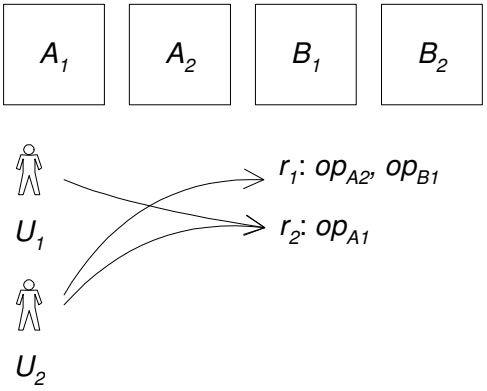

Рис. 1

Чтобы реализовать ее в нашей модели, необходимо сначала свести все объекты приложения в единую иерархию. Для этого достаточно добавить фиктивный корневой объект – *root* – и сделать объекты его прямыми потомками. Для того чтобы все роли были глобальными (как того требует базовая модель) мы должны будем назначать пользователей на них только в контексте корневого объекта, или, другими словами, в корневом домене d_{root}. Мы вводим роли r_1 и r_2 и назначаем на них пользователей.

После введения в систему операций остается только одна нерешенная проблема: необходимо, чтобы роль определялась операциями, выполняемыми в ее рамках. Действительно, роль в модели ForceField, в общем случае, не соответствует этому требованию. Фактически она ничем не отличается от группы пользователей.

Решение заключается во вводе в систему единого для всех объектов класса доступа c_0, в котором операции, составляющие определенную роль, для этой роли явным образом разрешены. Очевидно, что это и есть нужный нам способ записи соответствия между ролями и операциями.
Принципиальная схема реализации приведена на рисунке 2.

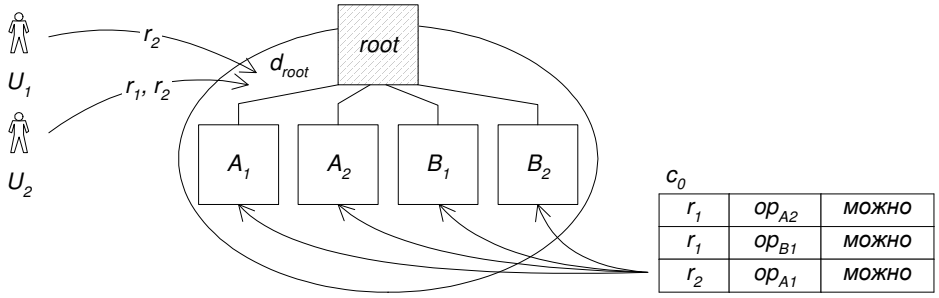

Рис. 2

7.2 Реализация дискреционной модели

Для приложения, описанного в предыдущей задаче, система контроля доступа по модели Харрисона-Руззо-Ульмана будет подобна схеме на рисунке 3. В ней столбцы соответствуют объектам, строки – пользователям. В ячейках прописаны индивидуальные права пользователя на соответствующий объект. Отметим, что, хотя в этом и нет большой необходимости, в таблице явным образом запрещены операции, не имеющие смысла для соответствующих объектов.

	A_1	A_2	B_1	B_2
U_1	op_{A1} - да op_{A2} - нет op_{B1} - нет	op_{A1} - да op_{A2} - нет op_{B1} - нет	op_{A1} - нет op_{A2} - нет op_{B1} - нет	op_{A1} - нет op_{A2} - нет op_{B1} - нет
U_2	op_{A1} - да op_{A2} - да op_{B1} - нет	op_{A1} - да op_{A2} - да op_{B1} - нет	op_{A1} - нет op_{A2} - нет op_{B1} - да	op_{A1} - нет op_{A2} - нет op_{B1} - да

Рис. 3

Для реализации этой модели в ForceField нужно создать четыре отдельных класса доступа (c_{A1}, c_{A2}, c_{B1} и C_{B2}) и назначить их соответствующим их объектам. В составляющих классы правилах разрешения будут даваться не ролям, а непосредственно пользователям. Необходимо подчеркнуть, что возможность указывать в правиле не роль, а пользователя, следует использовать только в крайних случаях, так как это может привести к созданию плохо управляемой политики безопасности.

В классы не включены правила, запрещающие не имеющие смысла операции, т.к. все явным образом не разрешенное автоматически считается запрещенным.

Результирующая схема приведена на рисунке 4.

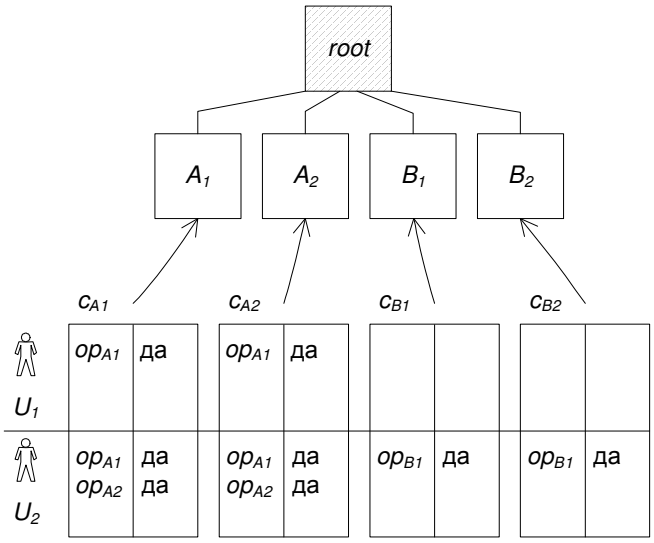

Рис. 4

На схеме не показан корневой домен и назначения пользователей на роли. Это связано с тем, что рассматриваемая модель является слишком простой, и роли в ней не используются. В таком виде модель не годится для большинства реальных применений, поэтому расширим ее, добавив типы объектов и группы пользователей.

В нашем приложении изначально есть два типа объектов, поэтому введем их в систему, связав с классами доступа. Таким образом, количество классов безопасности уменьшается до двух: класс безопасности для объектов типа A (c_A) и класс для объектов типа B (c_B).

Для группировки пользователей мы можем использовать роли, назначаемые пользователям в корневом домене. Поэтому введем две роли: g_1 и g_2. Изменим правила в классах доступа, с тем чтобы они выдавали разрешения группам пользователей (т.е. ролям), а не каждому пользователю в отдельности.

На рисунке 5 приведена схема реализации дискреционной модели, оптимизированной за счет типизации объектов и введения групп пользователей. В нашей модели можно реализовать и другие способы оптимизации. Например, наследование прав по аналогии с файловой системой легко реализуется за счет специального класса доступа на дочернем объекте. Он должен определять собственную схему доступа объекта и дополнять ее правилом «любая роль – любая операция – как у родителя».

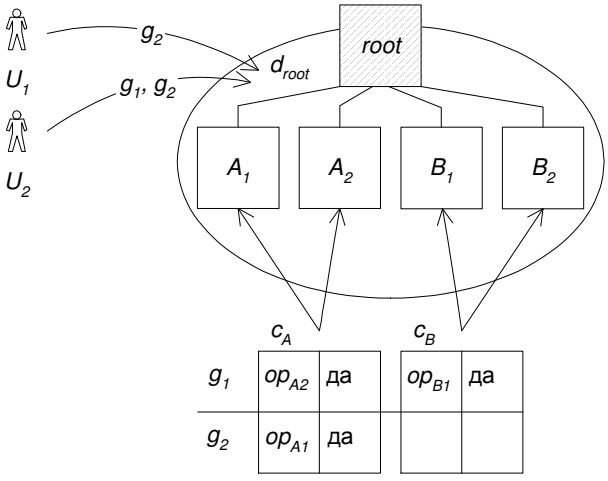

Рис. 5

8. Введение элементов мандатной модели

Самой первой из рассмотренных нами классических моделей была мандатная модель. В дальнейшем мы не уделяли ей достаточного внимания, так как она является весьма экзотичной, и крайне редко применяется в реальных приложениях. В связи с этим мы не ставили перед собой задачу охвата и этой модели, но наметили пути, по которым это может быть сделано.

Во-первых, классам доступа нужно назначить уровни секретности. Так как каждый объект приложения проассоциирован с определенным классом доступа, это автоматически назначит уровни секретности и всем объектам.

Во-вторых, мы должны назначить уровни допуска пользователям системы. В соответствии с моделью, пользователь будет иметь право читать документы с уровнем секретности не выше его собственного, и изменять документы с уровнем не ниже.

В-третьих, необходимо разделить все операции системы на две группы: группу чтения и группу записи. Тогда, при проверке на допустимость операции, мы будем точно знать, какое правило применить.

Наконец, модифицируется процедура проверки прав. Если у объекта и пользователя разные уровни, то мы проводим проверки по стандартным принципам мандатной модели. Если уровень одинаковый, то применяем обычные правила нашей модели.

Заметим, что нужно будет еще тщательно обдумать желаемое поведение системы в ситуации, когда по мандатной модели операция разрешена, а по модели ForceField – запрещена. Ответ на этот вопрос определит направленность системы безопасности. Нужно решить, что приоритетней: полная свобода пользователям с высоким уровнем или ограничение пользователей с низким.

9. Заключение

Мы показали, что предлагаемая модель контроля доступа объединяет в себе базовые модели. Что более важно, она расширяет их возможностью назначения пользователей на роли в контексте любого объекта системы. Поэтому множество ролей, которые пользователь играет в некий момент времени, не является одним и тем же для всех объектов приложения, а пополняется новыми ролями по мере спуска вглубь по объектной иерархии.

За счет этого появляется возможность максимально естественным образом ограничить область действия выданных пользователю полномочий определенной частью приложения. Это позволяет уменьшить необходимое количество ролей и упростить схемы доступа к объектам.

Таким образом, наша модель позволяет создавать легкие в администрировании политики безопасности, обладая, в то же время, необходимыми возможностями по ограничению несанкционированного доступа к объектам приложения.

10. Литература

[1] Leonard J. LaPadula and D. Elliott Bell. Secure Computer Systems: A Mathematical Model // MITRE Corporation Technical Report 2547. Volume II. 31 May 1973.

[2] Зегжда Д.П. Общая схема мандатных моделей безопасности и ее применение для доказательства безопасности систем обработки информации // Проблемы информационной безопасности. Компьютерные системы. СПбГТУ. 2000. 2.

[3] Степанов П.Г. Принципы управления доступом к кесурсам в защищенной ОС «Феникс» // Проблемы информационной безопасности. Компьютерные системы. СПбГТУ. 1999. 4.

[4] M. Harrison, W. Ruzzo, J. Uhlman Protection in operating systems // Communications of the ACM. 1976.

[5] Баранов А.П. Зегжда Д.П., Зегжда П.Д., Ивашко А.М., Корт С.С. Теоретические основы информационной безопасности (Дополнительные главы). СПб.: СПбГТУ. 1998.

[6] Mohan Rao Cavale. Role-Based Access Control Using Windows Server 2003 Authorization Manager. http://msdn.microsoft.com/library/en-us/dnnetserv/html/AzManRoles.asp