***«Высокие интеллектуальные технологии образования и науки».***
*Материалы X Международной научно-методической конференции.С.90-98,* 2003.

# МОДЕЛИРОВАНИЕ ПОЛИТИК БЕЗОПАСНОСТИ ДЛЯ ИССЛЕДОВАТЕЛЬСКИХ И ОБУЧАЮЩИХ ЦЕЛЕЙ

**Зегжда П.Д., Зегжда Д.П., Калинин М.О.**
*Санкт-Петербургский государственный политехнический университет*

Существующие в настоящее время модели безопасности используют различные подходы к решению задачи управления доступом. Однако до сих пор не появились модели и политики, одинаково эффективные во всех случаях. Поэтому актуальной является проблема создания таких систем защиты, которые могли бы обеспечивать реализацию нескольких политик безопасности. Это позволило бы настраивать систему в зависимости от вида решаемых задач и применять различные политики для различных взаимодействий в системе. Для эффективной реализации такой системы необходимо разработать универсальные по отношению к политикам любого типа средства контроля доступа, представления атрибутов безопасности и правил политик безопасности.

Максимальной степени универсальности в механизмах реализации политики безопасности можно достичь разделением самой политики и механизмов ее осуществления путем спецификации правил доступа с использованием универсального языка описания. Применение этого метода требует разработки языка представления политик безопасности; составления описания различных политик; создания программы, реализующей машину логического вывода, обрабатывающую спецификации сущностей и правил доступа; а также построения программной среды для описания и исследования защищенных информационных систем.

Авторы статьи решали конкретную прикладную задачу – разработку универсального языка описания и программной среды моделирования политик безопасности с целью обеспечения исследовательского и образовательного процесса. Созданные средства моделирования предполагается использовать в учебных целях как обеспечение лабораторных занятий по курсам информационной безопасности, читаемых на кафедре «Информационная безопасность компьютерных систем» СПбГПУ.

## *Анализ существующих средств моделирования политик безопасности на основе языка авторизации*

Разработка универсальных механизмов реализации политик безопасности – актуальное направление исследований в сфере информационной безопасности. Важные результаты в области построения универсальных средств защиты информации были получены разработчиками концепции гибкой авторизации [1], базовым компонентом которой является универсальный язык авторизации. С его помощью администратор получает возможность задать фор-

мальное описание модели безопасности, включающее описание типа объектов; спецификацию групповой иерархии субъектов и описание взаимодействий субъектов и объектов (то есть правил политик безопасности).

Основу языка описания составляет фиксированный набор предикатов. Используя базовые предикаты, администратор создает спецификации различных моделей безопасности и включает их в так называемую программу авторизации. При этом для каждого объекта предоставляется возможность указать, какую схему авторизации необходимо применять при доступе к нему. Работа механизма авторизации сводится к перехвату запроса пользователя к объекту, трансляции запроса в специальном обработчике запроса в формат универсального языка авторизации и передаче запроса в программу авторизации. В случае положительного ответа программы авторизации доступ к объекту разрешается.

Предложенный механизм спецификации обладает необходимой универсальностью, но имеет ряд недостатков:

1. Возникновение сложностей при моделировании некоторых дискреционных моделей. Так, например, модель, основанная на ролевом управлении доступом, требует допущения вида «группа ≡ роль», что не соответствует действительности и может внести затруднения в процесс изучения ролевой политики.

2. Отсутствие математических операций сравнения (например, >, < , =, ≥, ≤, ≠) применительно к описанию отношений «субъект-объект», что усложняет процесс моделирования политик мандатного управления доступом. Так, например, правило NRU («no read up», правило «нет чтения вверх», или простое свойство безопасности) модели Белла-ЛаПадула включают сравнение уровней безопасности: субъект с уровнем безопасности $x_s$ может читать информацию из объекта с уровнем безопасности $x_o$, только если $x_s$ преобладает над $x_o$. Отсутствие операций сравнения делает невозможным описание этого правила.

3. Характеристика субъекта посредством одного атрибута «группа», а объекта — при помощи атрибута «тип». На практике сущность может ассоциироваться с несколькими атрибутами. Так, необходимость применения меток в мандатных моделях требует введения атрибута «уровень безопасности» и соответствующего расширения языка описания. В этой связи каждая сущность должна содержать список атрибутов, характеризующих данную сущность в терминах безопасности.

4. Отсутствие средств отладки и протоколирования, что ставит под сомнение возможность поиска ошибок, возникающих при описании модели, или отслеживания процесса выполнения правил авторизации.

Недостатки в схеме гибкой авторизации приводят к отсутствию ее наглядности и полноты, что делает этот механизм неприменимым для решения задач, определенных ранее.

### *Применение универсального языка описания политик безопасности*

С учетом вышеуказанного авторами данной статьи был разработан универсальный язык описания[2, 3]. Каждому объекту и субъекту поставлен в соответствие набор атрибутов безопасности, которые характеризуют его содержание, например, уровень безопасности, группу и т.д. и используются для определения правил политики безопасности. Каждому атрибуту присваивается уникальное имя, которое используется при обращении к нему, в качестве имени предиката. Над значениями атрибутов возможны операции сравнения (== – «равно», != – «не равно», <, > и т. д.).

Введены предикаты, используемые для описания моделируемой системы (субъектов, объектов и их атрибутов), а также предикаты для описания правил политики безопасности. Определяя множества субъектов, объектов, атрибутов и задавая правила вычисления перечисленных предикатов, можно описывать системы, подчиняющиеся той или иной политике безопасности.

Разработанный авторами универсальный язык описания положен в основу создания программной среды для моделирования и исследования классических политик безопасности.

### *Лабораторное средство моделирования политик безопасности*

Авторы ставили своей целью создание программного продукта, позволяющего описать существующую или проектируемую модель безопасности и провести практическое исследование механизмов защиты, реализованных в данной модели. Результатом этой работы является автоматизированный лабораторный стенд, который эксплуатируется в среде Windows и представляет собой интегрированную среду, применяя которую пользователь получает возможность моделировать политику безопасности, проверять выполнимость/невыполнимость требований, составляющих политику безопасности, и осуществлять мониторинг процесса выполнения/невыполнения правил доступа, реализующих данную политику.

Функция моделирования политики безопасности заключается в предоставлении пользователю средства описании защищенной системы (субъектов, объектов и правил доступа субъектов к объектам). Таким средством является предложенный универсальный язык представления политик безопасности. Данный язык предоставляет аппарат спецификации системы, а именно: задания описания составляющих систему активных (субъектов) и пассивных (объектов) сущностей, а также определения правил доступа субъектов к объектам.

Механизм моделирования, реализованный в стенде, основан на применении концепции логического программирования. Логическое программирование дает возможность описывать ситуации при помощи формул логики предикатов первого порядка, а затем, для выполнения выводов из этих формул применять автоматический решатель задач. В качестве системы логического программирования выбран SWI-Prolog – реализация Пролога, которая характеризуется наличием Windows-интерфейса и возможностью сопряжения с программой, написанной на языке Си.

Архитектура стенда представлена на **рис. 1**. Посредством Microsoft Visual C++ и библиотеки классов MFC создан пользовательский интерфейс, а также модули описания, трассирования и протоколирования (**рис. 1**, ***а***). При помощи Пролога разработаны языковые средства описания политик безопасности и механизм отладки (**рис. 1**, ***б***).

*Лабораторный практикум*

На основе автоматизированного лабораторного стенда разработан лабораторный практикум по курсам «Системный подход к защите информации» и «Защищенные операционные системы», читаемым на кафедре «Информационная безопасность компьютерных систем» в рамках бакалаврской и магистерской подготовки.

Задачей практикума является изучение студентами теории классических политик безопасности, анализ их достоинств и недостатков, исследование реакций политик безопасности на попытки нарушения доступа.

В ходе практических занятий студент приобретает навыки в решении следующих проблем:

- моделирования поведения систем в зависимости от используемой политики безопасности;
- анализа ситуации и осуществления выбора соответствующей политики безопасности;
- применения механизмов политик безопасности, включающего поиск и устранение противоречий в требованиях политик безопасности и состояниях информационной системы;
- анализа существующих и синтеза новых средств защиты.

Все лабораторные работы проводятся с использованием автоматизированного стенда. Работа студента на лабораторном стенде включает несколько этапов, приведенных на **рис. 2.**

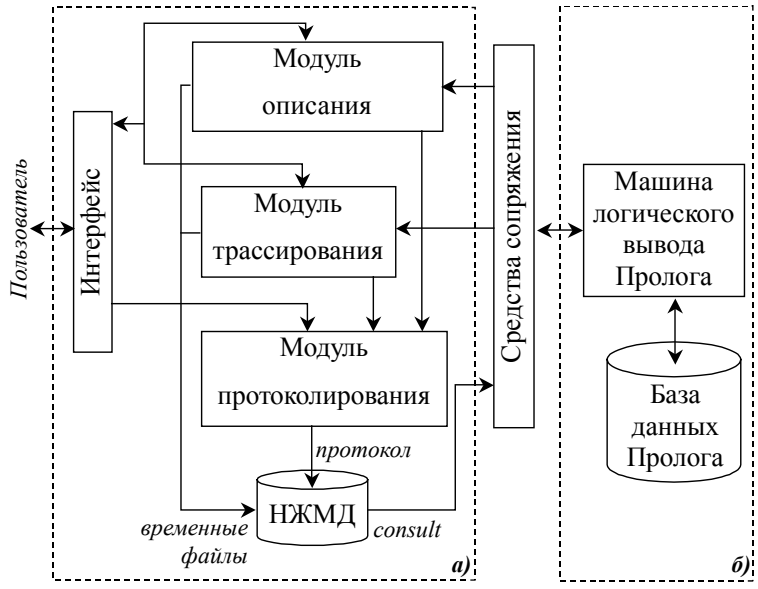


**Рис. 1.** Архитектура автоматизированного лабораторного стенда по моделированию политик безопасности

Ход лабораторной работы предлагается изучить на примере дискреционной модели Харрисона-Руззо-Ульмана.

Положительные черты дискреционных моделей следующие: хорошая гранулированность защиты и простота реализации. Но значительным недостатком модели является проблема троянских коней.

В терминах модели состояние системы характеризуется тройкой (S, O, M), где S – набор субъектов, O – набор объектов (в O могут быть включены и субъекты), M – матрица доступа. Для примера рассмотрим простейшую систему, состоящую из двух субъектов и двух объектов.

Допустим рассмотрение операций доступа: чтение, запись, выполнение и создание. При этом предположим, что в системе реализовано дискреционное управление доступом, заданное матрицей M (**табл. 1**), где r — обозначение операции чтения (read), w — записи (write), e — исполнения (execute), c — создания (create).


**Рис. 2.** Цикл проведения лабораторной работы

***Таблица 1***

Исходная матрица доступа

| | doc | prog | $s_1$ | $s_2$ | troy |
|---|---|---|---|---|---|
| $s_1$ | — | r,w,e | — | — | — |
| $s_2$ | r,w | e | — | — | c |

Моделирование правил доступа осуществляется при помощи универсального языка в следующей последовательности:

1. В ходе работы проводится проверка на доступ к объектам. Дискреционная модель обеспечивает надежную защиту, например, по чтению и записи. В отчете студент приводит соответствующий протокол работы монитора.

2. Затем моделируется поведение троянского коня, который эквивалентен получению неавторизованным субъектом доступа на чтение объекта prog.

3. Многократное повторение операций создания, удаления или смены атрибутов сущностей в системе переводит ее в новое состояние. Студенту предлагается убедиться в безопасности этого состояния. Для этого необходимо исследовать систему на предмет прежней корректности правил доступа и выяснить, не получили ли субъекты возможность доступа к объектам, к которым они раньше не имели доступа.

При помощи языка описания политик безопасности правила чтения и записи будут представлены следующим образом:

```
readSO(S,O):-
  validSubject(S),
  validObject(O),
  checkAttr(S,O,r).
```

```
writeSO(S,O):-
  validSubject(S),
  validObject(O),
  checkAttr(S,O,w).
```

Создание и наделение правами субъекта «Троянский конь» (troy) представлено следующим предикатом:

```
createTroy(P):-
  validSubject(P),
  checkAttr(P,troy,c),
  insertSubject(troy,[doc(w),prog(r), s1,s2,troy]).
```

Следовательно, в матрице доступа появляется новая строка (**табл. 2**).

***Таблица 2***

Создание троянского коня

| | doc | prog | s1 | s2 | troy |
|---|---|---|---|---|---|
| troy | w | r | — | — | — |
| s1 | — | r,w,e | — | — | — |
| s2 | r,w | e | — | — | c |

Появление троянского коня позволяет субъекту, ранее не имевшему доступа к объекту prog, получить его (табл. 2).

Многократно применяя операцию создания субъектов, пользователь переводит систему в качественно новое состояние. Поэтому на третьем этапе изучения дискреционной политики безопасности студенту предлагается проверить прежнюю корректность требований исследуемой политики безопасности.

Подобно рассмотренной другие лабораторные работы данного цикла посвящены детальному изучению моделей безопасности, реализующих защиту вычислительных систем от различного рода угроз, посредством описательных и тестовых механизмов лабораторного стенда.

Таким образом, на основе разработанного авторами универсального языка описания была реализована система моделирования и исследования политик безопасности, включающая интерпретатор данного языка и машину логического вывода. На базе этой системы был создан автоматизированный лабораторный стенд, позволяющий интерпретировать описания различных политик безопасности, моделировать поведение системы, подчиняющейся заданной политике, в различных ситуациях и получать контрольную информацию об использовании правил политик безопасности.

Наличие такого стенда позволило реализовать лабораторный практикум, предназначенный для изучения различных политик безопасности и включающего следующие лабораторные работы: «Дискреционные модели управления доступом. Модель Харрисона-Руззо-Ульмана», «Модели мандатного управления доступом. Модель Белла-ЛаПадула», «Ролевое управление доступом», «Дискреционная модель, основанная на типизированной матрице доступа», «Модель доменов и типов» и «Информационные модели безопасности».

Кроме того, стенд может быть применен как для исследования существующих политик безопасности для определения возможности их применения в различных системах, так и в процессе проектирования новых моделей, поскольку позволяет интерактивно тестировать свойства разрабатываемой модели и подбирать правила политики безопасности.

Наконец, язык описания политик безопасности и разработанный к нему инструментарий могут быть использованы при построении гибких и адаптивных защищенных информационных систем, инвариантных к политикам безопасности.

## ЛИТЕРАТУРА

1. Jajodia S., Samarati P., Subrahmanian V.S., Bertino E. A Unified Framework for Enforcing Multiple Access Control Policies. In Proc. ACM SIGMOD Conf. on Management of Data, Tucson, AZ, May 1997.

2. Зегжда Д.П., Калинин М.О. Реализация универсального языка описания политики безопасности // Методы и технические средства обеспечения безопасности информации: Тез. докл. – СПб: Изд-во СПбГТУ, 1998.

3. Калинин М.О. Язык описания политик безопасности информационных систем / Современное машиностроение: Сб. трудов молодых ученых. Вып. 1. – СПб: Изд-во СПбИМаш, 1999. – с. 69-74.