На правах рукописи

Калинин Максим Олегович

АВТОМАТИЗИРОВАННЫЙ АНАЛИЗ ВЫПОЛНЕНИЯ ПРАВИЛ ПОЛИТИК БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Специальность:

05.13.19 – Методы и системы защиты информации, информационная безопасность

Автореферат диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург — 2003

Работа выполнена в Санкт-Петербургском государственном политехническом университете

Научный руководитель:

кандидат технических наук, доцент
Зегжда Дмитрий Петрович

Официальные оппоненты:

доктор технических наук, профессор
Корниенко Анатолий Адамович

кандидат технических наук
Сидоров Игорь Анатольевич

Ведущая организация:

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Защита состоится "___" _____ 2003 г. в ____ часов
на заседании диссертационного совета Д 212.229.27
Санкт-Петербургского государственного политехнического университета
195251, Санкт-Петербург, ул. Политехническая, 29, корп. __, ауд. _____

С диссертацией можно ознакомиться в библиотеке
Санкт-Петербургского государственного политехнического университета

Автореферат разослан "___" _____ 2003 г.

Ученый секретарь
диссертационного совета _____ (Платонов В.В.)

Общая характеристика работы

Актуальность. В наши дни обеспечение безопасности информационных систем (ИС) входит в круг интересов всех участников информационного процесса. Функционирование государственных и коммерческих ИС становится невозможным без поддержания их безопасности и целостности. Прогресс в области защищенных информационных технологий сопровождается усилением требований поддержания безопасности. Однако динамика статистики нарушений свидетельствует о кризисе информационной безопасности, основными причинами которого являются недостатки проектирования и эксплуатации средств защиты. Функции ИС должны выполняться при осуществлении надлежащего контроля информации, что гарантировало бы защиту информации от нежелательного распространения, изменения или потери. Для задания политики безопасности (ПБ) потребители вынуждены использовать решения, предлагаемые производителем. Отсутствие у потребителя гарантий, кроме утверждений разработчиков, что в используемой системе ПБ выполняется корректно, является одной из основных причин нарушений безопасности. Эта проблема особенно остро стоит в ИС, к которым предъявляются повышенные требования гарантированности защиты: в системах управления технологическими процессами, движением транспорта, проведения банковских операций, обработки секретной информации.

Значительным шагом на пути решения указанной проблемы является разработка и применение ГОСТ Р ИСО 15408, который совместим с системой международной стандартизации и предписывает составление профиля защиты (ПЗ), включающего ПБ. Стандарт накладывает требования обеспечения гарантированности выполнения системой правил ПБ. Согласно стандарту установление гарантированности основывается на активном исследовании ИС, в результате чего должны быть выявлены причины невыполнения ПБ. Поэтому введение нового ГОСТ требует создания методов и инструментария проверки выполнения ПБ. Автоматизация анализа выполнения ПБ позволит придать ему объективный характер, обеспечить

надежность защиты информации и качество сертификационных исследований.

Моделирование выполнения правил ПБ — это новое научное направление, теоретическая и методологическая базы которого в настоящее время только формируются в работах таких ученых как Грушо А.А., Расторгуев С. П., Щербаков А.Ю., Деннинг Д.Е., МакЛин Д., Сандху Р., Самарати П. Специалисты Гостехкомиссии и ее подведомственных организаций разрабатывают средства автоматизации анализа защитных свойств (например, НКВД, АИСТ). Однако упомянутые средства не решают задачу в полном объеме. Данная работа опирается на результаты указанных исследований и развивает их отдельные положения применительно к задачам моделирования защитных механизмов и автоматизации проверки выполнения правил ПБ.

С практической точки зрения наиболее важной является задача разработки средств проверки выполнения правил ПБ, которая представляет одно из направлений более общей задачи обеспечения информационной безопасности. В этой связи разработка подхода к автоматизации анализа выполнения правил ПБ является актуальной проблемой, имеющей важное теоретическое и практическое значение.

Целью работы является обеспечение сертификационных исследований информационных систем по ГОСТ Р ИСО 15408 средствами проверки выполнения правил политик безопасности, основанными на применении метода автоматизированного анализа безопасности достижимых состояний.

Для достижения поставленной цели в работе решались задачи:

1. Анализ моделей контроля и управления доступом (КУД), средств защиты современных ИС, а также методов моделирования ПБ.

2. Разработка формы представления системных состояний, требований модели КУД и правил ПБ, предназначенной для моделирования и анализа средств защиты и универсальной по отношению к широкому классу моделей КУД.

3. Разработка метода проверки выполнения правил ПБ путем автоматизированного анализа безопасности достижимых состояний.

4. Разработка системы проверки выполнения правил ПБ, позволяющей автоматизировать процесс исследования ИС на предмет соблюдения ПБ.

5. Создание методики проверки выполнения правил ПБ в ходе сертификационных исследований ИС по ГОСТ Р ИСО 15408.

Методы исследования. Для решения поставленных задач использовались системный анализ, теория алгоритмов, теория множеств, теория вычислений, методы математического моделирования и математической логики.

Научная новизна диссертационной работы состоит в следующем:

1. Проведен сравнительный анализ методов, используемых для моделирования и исследования ПБ.

2. Предложен и обоснован подход к проверке выполнения правил ПБ путем автоматизированного анализа достижимых состояний ИС.

3. Разработаны концептуальные модели подсистем КУД для современных операционных систем (ОС).

4. Разработана форма представления системных состояний, требований модели КУД и правил ПБ в виде системы логических предикатов.

5. Предложен метод проверки выполнения правил ПБ путем анализа безопасности достижимых состояний на основе вычисления предикатов, описывающих ПБ, в контексте системных состояний и модели КУД.

6. Разработана система проверки выполнения правил ПБ, позволяющая автоматизировать процесс исследования ИС путем генерации ее логического описания, вычисления предикатов и интерпретации результатов.

7. Разработана методика проверки выполнения правил ПБ в ходе сертификационных исследований ИС по ГОСТ Р ИСО 15408.

Практическая ценность работы определяется возможностью использования полученных в ходе работы результатов для проведения анализа ПБ и проверки ИС на соответствие ПБ. Метод автоматизированной проверки выполнения ПБ и средство описания системных состояний, правил ПБ и требований модели безопасности использованы при разработке программ и методик сертификационных исследований специализированной ИС (акт об использовании от ЗАО "РНТ", г. Москва). Подход к проверке ПБ

путем автоматизированного анализа достижимых состояний испытываемой системы использован при разработке представления модели КУД, реализованной в системе мониторинга безопасности сложных информационных комплексов (акт об использовании от ЗАО "АРГО-Технолоджи", г. Москва). Метод автоматизированного анализа выполнения правил ПБ и разработанный комплекс средств оценки защищенности использованы при создании системы проверки выполнения ПБ организаций (акт об использовании от НИИ системотехники ХК "Ленинец", г. С.-Петербург). На основе теоретических и практических результатов работы разработаны учебно-методические материалы, используемые для подготовки специалистов в области защиты вычислительных систем по дисциплинам "Теоретические основы защиты информации" и "Безопасность ОС" в СПбГУАП (акт об использовании от СПбГУАП) и СПбГПУ.

Апробация работы. Основные теоретические и практические результаты диссертационной работы доложены и обсуждены: на Российской научно-технической конференции "Методы и технические средства обеспечения безопасности информации" (СПбГПУ, 1998-2002 гг.); на Санкт-Петербургском семинаре "Информационная безопасность-99" (СПбГТУ, 1999 г.); на ведомственной конференции "Проблемы обеспечения информационной безопасности на федеральном железнодорожном транспорте" (Внедренческий центр ГУП "Аттестационный центр Желдоринформзащита МПС РФ", 2001 г.); на Межрегиональной конференции "Информационная безопасность регионов России" (Институт информатики и автоматизации РАН, 2001, 2002 гг.); на Российской научно-технической конференции "Проблемы информационной безопасности в системе высшей школы" (МИФИ, 2002, 2003 гг.).

Публикации. По теме диссертации опубликовано 32 научные работы, в том числе 3 учебных пособия.

Основные положения, выносимые на защиту:

1. Обоснование подхода к проверке выполнения правил ПБ путем автоматизированного анализа безопасности достижимых состояний ИС.

2. Метод проверки выполнения правил ПБ, основанный на вычислении предикатов, описывающих системные состояния, требования модели КУД и правила ПБ.

3. Система проверки выполнения правил ПБ.

4. Методика проверки выполнения правил ПБ на основе автоматизированного анализа безопасности состояний.

Объем и структура. Диссертация состоит из введения, четырех глав, заключения и списка литературы из 95 наименований.

Содержание работы

Во введении обоснована и сформулирована задача разработки автоматизированных средств анализа выполнения правил ПБ.

В первой главе рассмотрены основные классы моделей КУД и их реализации в современных ОС, проведен анализ методов моделирования ПБ, сформулирована задача автоматизированной проверки выполнения правил ПБ с использованием логического подхода.

На основании потребительских требований, сформировавшихся на рынке информационных технологий, разработчики ИС предлагают готовые решения по обеспечению безопасности. В работе проанализированы теоретические и практические аспекты, связанные с базовыми моделями КУД, служащими основой для разработки защитных механизмов современных ИС: дискреционными и мандатными, рассмотрены реализации подсистем безопасности в ОС Windows 2000 и Linux. В настоящее время наблюдается развитие моделей КУД по пути комбинирования принципов различных классических моделей безопасности. Решением проблемы проверки выполнения правил ПБ является создание концептуальной модели системы в контексте модели КУД и правил ПБ и дальнейшая ее обработка с целью выявления нарушений безопасности и противоречий. В работе осуществлен анализ методов моделирования ПБ, в результате чего выделены аналитические (АМ), графовые (ГМ), объектные (ОМ) и логические (ЛМ) методы.

АМ, имеющие в своей основе аппарат представления в виде математических функций, наиболее точны и строги, но лишены наглядности для пользователя и требуют специальной подготовки. ГМ базируются на теории графов и топологии, обладают свойством наглядности. Недостатком ГМ является статичность моделирования, т.е. демонстрация определенных состояний без указания их взаимосвязи. ОМ позволяют моделировать защищенность крупных систем, поскольку правила применяются к группам сущностей. Принципы инкапсуляции и наследования способствуют универсальности и расширяемости представления. К недостаткам ОМ следует отнести сложность объектной декомпозиции ИС и необходимость поиска оптимального уровня абстрагирования. ЛМ, использующие аппарат матлогики, позволяют добиться простоты реализации и проведения автоматического анализа ПБ, т.к. программа исследований может быть задана в виде логических предикатов.

С целью определения метода, независимого от объекта изучения, простого и удобного в применении, проведено сравнение рассмотренных методов по таким характеристикам, как выразительная способность, моделирование иерархических структур, объяснение результатов вывода, наличие программной реализации, удобство применения и близость к естественному языку (таблица).

Сравнение методов моделирования ПБ

Характеристика	**АМ**	**ГМ**	**ОМ**	**ЛМ**
Выразительная способность	—	**É**	—	**É**
Моделирование иерархических структур	—	**É**	**É**	**É**
Объяснение результатов вывода	**É**	—	—	**É**
Программная реализация	—	—	**É**	**É**
Удобство применения	—	**É**	—	—
Близость к естественному языку	—	—	—	**É**

Под выразительной способностью понимается готовность метода к представлению произвольных объектов. Моделирование иерархических структур используется при задании сложных систем, что необходимо при

представлении ПБ в реальных ОС, например, для описания структуры объектов файловой системы. Объяснение результатов вывода состоит в возможности пошагового отслеживания процесса анализа ПБ, т.е. трассировки. Наличие программной реализации свидетельствует о готовности программной поддержки метода, что позволяет использовать уже готовые решения. Под удобством применения подразумевается наглядность результатов для пользователя. Близость к естественному языку означает, что метод предоставляет возможность задать ПБ с помощью лаконичных и понятных человеку конструкций.

Анализ методов показал, что наиболее перспективным в рамках моделирования правил ПБ и автоматизации анализа проверки их выполнения является логический подход, поскольку только этот способ обладает необходимыми характеристиками.

Во второй главе рассмотрен предложенный автором подход к проверке выполнения правил ПБ путем автоматизированного анализа достижимых состояний испытываемой системы. Приведена разработанная форма представления системных состояний, правил ПБ и требований модели КУД в виде логических предикатов.

Машина состояний — распространенный инструмент моделирования различных аспектов ИС. В частности он используется при создании моделей КУД, т.н. моделей безопасности состояний. К этому классу относятся модели КУД большинства ОС. Базовыми элементами таких моделей являются состояния и переходы между нами. В общем случае под состоянием понимается образ ИС в некоторый момент времени, включающий все аспекты системы, связанные с безопасностью, а переход описывается функцией, которая определяет следующее состояние в зависимости от текущего состояния и поступившего запроса (функция перехода).

Обозначим через St множество системных состояний с точки зрения безопасности. Состояние есть перечисление элементов ИС, определяющих ее безопасность (например, учетные записи пользователей, права доступа, ключи реестра и т.д.). Произведем разграничение системных сущностей. С одной стороны, сущности могут быть активными, т.е. инициировать

операции, выполняемые с информацией. С другой стороны, сущности могут быть пассивными, т.е. являться контейнерами информации. Активные сущности назовем субъектами, пассивные — объектами. Объекты являются предметом операций, которые могут выполняться субъектами. В случае, когда субъект сам является предметом операции (например, при изменении членства в группе), над субъектом могут производиться действия, как над объектом. Субъекты и объекты обладают определенными атрибутами, которые содержат информацию, позволяющую ИС функционировать правильно. Некоторые атрибуты, например, параметры управления доступом, предназначены исключительно для осуществления ПБ. Последние назовем атрибутами безопасности. Обозначим через S — множество субъектов, O — множество объектов, SA — множество атрибутов безопасности. Тогда множество St есть декартово произведение $S \times O \times SA$.

Переход из состояния в состояние возможен как результат действий над сущностями ИС и их атрибутами. С точки зрения безопасности разрешения на операции выдаются в соответствии с требованиями, указанными в модели КУД. В ИС компонент, выполняющий разрешительные функции, называется монитором обращений, он выполняет проверку соответствия между запросом на доступ и требованиями модели. Обозначим через R требования модели КУД. При выполнении требований ИС переходит из состояния st в состояние st', где $st, st' \in St$ (например, успешное создание субъекта приводит к смене состояния). Обозначим переход из состояния в состояние посредством функции переходов δ, а запрос на доступ через q, тогда последующее состояние $st' = \delta(q, st)$. В общем случае, существует последовательность пар "запрос-состояние": $<(q_0, st_0), ..., (q^*, st^*)>$, которая моделирует изменения системы от начального состояния $st_0 \in St$ до некоторого состояния $st^* \in St$, называемого достижимым.

Потребитель вынужден осуществлять защиту информации путем введения своей ПБ и использования для этого предлагаемых производителями продуктов. ПБ задается в виде запретительных правил, например, "секретарям запрещено читать файлы менеджеров и директора",

которые должны выполняться в каждом состоянии системы. Правила преобразуются в простые высказывания (ограничения *C*) путем применения аппарата исчисления высказываний. Например, приведенное правило преобразуется в совокупность двух ограничений: "секретарям запрещено читать файлы менеджеров" и "секретарям запрещено читать файлы директора". Тогда выполнение правил ПБ в системе, находящейся в некотором состоянии, состоит в контроле выполнения всех ограничений из множества *C* для этого состояния.

Для проверки выполнения ограничений применен принцип доказательства основной теоремы безопасности Белла-ЛаПадулы по индукции относительно состояний. Для реальной системы при проверке ограничений *C* пространство перебора ограничивается областью определения. Предложенный в работе подход состоит в использовании для решения задачи анализа выполнения правил ПБ следующей последовательности действий: моделирование начального состояния и требований модели КУД, формирование ограничений, генерация достижимых состояний системы и проверка выполнения ограничений в полученных состояниях. Предложенный подход позволяет автоматизировать анализ выполнения правил ПБ.

Реализация подхода включает разработку средств моделирования состояния ИС, требований модели КУД и ограничений. На основе исследования средств защиты современных ОС предложены их концептуальные модели, которые были обобщены и представлены в виде концептуального графа системных состояний, требований модели КУД и правил ПБ, на базе чего была разработана и реализована система логических предикатов, позволяющая описывать элементы и характеристики безопасности ИС по следующей форме:

```
атрибут_субъекта(имя_атрибута_субъекта).
атрибут_объекта(имя_атрибута_объекта).
субъект(имя_субъекта,имя_атрибута_субъекта1(значение_a_c1,…,значение_a_ck),…,
          имя_атрибута_субъектаn(значение_a_c1, …, значение_a_ct)).
объект(имя_объекта,имя_атрибута_объекта1(значение_a_o1, …, значение_a_of),…,
          имя_атрибута_объектаm(значение_a_o1, …, значение_a_oh)).
правило(параметр_правила1, …, параметр_правилаp):- логическая_функция.
```

Система предикатов реализована как совокупность логических термов и правил на языке Пролог и позволяет задать субъекты, объекты ИС, их атрибуты безопасности, требования модели КУД и ограничения. В работе приведены примеры применения предложенных предикатов при описании ПБ, основанных на дискреционных, мандатных и комбинированных моделях КУД, что показало применимость предложенного подхода для моделирования широкого класса ПБ.

В третьей главе изложены теоретические основы предложенного автором метода проверки выполнения правил ПБ путем анализа безопасности достижимых состояний на основе вычисления предикатов. Приведена разработанная архитектура системы проверки выполнения правил ПБ, позволяющей автоматизировать процесс исследований ИС.

Зададим требование $rule \in R$ модели КУД в форме логического предиката $rule(st, st')$, определенного на декартовом произведении множеств состояний $St \times St$ и определяющего допустимость перехода в новое состояние st'. Ограничение $constraint \in C$ зададим в форме предиката $constraint(st)$, определенного на множестве St и проверяющего соответствие состояния st правилам политики. В работе предлагается следующий критерий: в ИС выполняются правила ПБ, если выполняются условия:

1. $constraint(st_0)$ истинен для $\forall constraint \in C$ и $st_0 \in St$: st_0 — начальное состояние.

2. $rule(st, st')$ истинен для $\forall rule \in R$ и $\forall st, st' \in St$: $st' = \delta(q, st)$.

3. $constraint(st^*)$ истинен для $\forall constraint \in C$, $st_0 \in St$: st_0 — начальное состояние и $\forall st^* \in St$: $st^* = \delta(q^*, \delta(\ldots(q', \delta(q_0, st_0))\ldots))$.

Проверка предложенного критерия составляет основу метода автоматизированного анализа выполнения правил ПБ. С помощью разработанной системы предикатов создается описание начального состояния, требований КУД и ограничений. Далее проводится проверка выполнения ограничений в начальном состоянии. После чего генерируется множество достижимых состояний и для каждого достижимого состояния проверяется выполнение ограничений.

Метод реализован в виде модуля резолюций (МР), который генерирует множество состояний и с помощью машины логического вывода Пролога проверяет выполнение ограничений в полученных состояниях ИС (рис. 1).

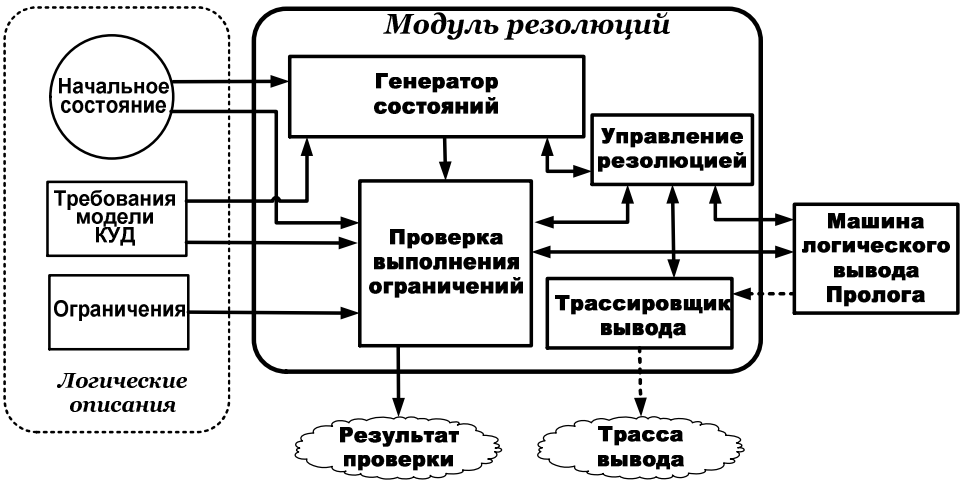

Рис. 1. Модуль резолюций

Модуль реализован на платформе ОС Windows в виде динамической библиотеки с использованием ядра системы SWI-Prolog. Входные параметры МР составляют три описания, которые моделируют начальное состояние системы, требования модели КУД и ограничения. В процессе логического вывода (резолюции) МР для каждого полученного состояния обрабатывает список ограничений для проверки их выполнения. По результатам работы создается протокол анализа с трассой логического вывода.

На базе МР была разработана архитектура системы проверки (СП) выполнения правил ПБ, позволяющей автоматизировать процесс исследования ИС путем моделирования системных состояний и правил ПБ, вычисления предикатов и интерпретации результатов (рис. 2).

Заданное состояние исследуемой ИС, требования модели КУД и правила ПБ записываются посредством предложенной в работе системы предикатов. Генератор описания начального состояния предназначен для автоматического создания описания заданного состояния ИС. Правила ПБ преобразуются экспертом в ограничения, которые с помощью редактора ограничений записываются в соответствующее описание. Описание

требований модели КУД — единственное описание, требующее ручной работы эксперта на основании анализа спецификации системы, но данное описание создается один раз для заданной системы.

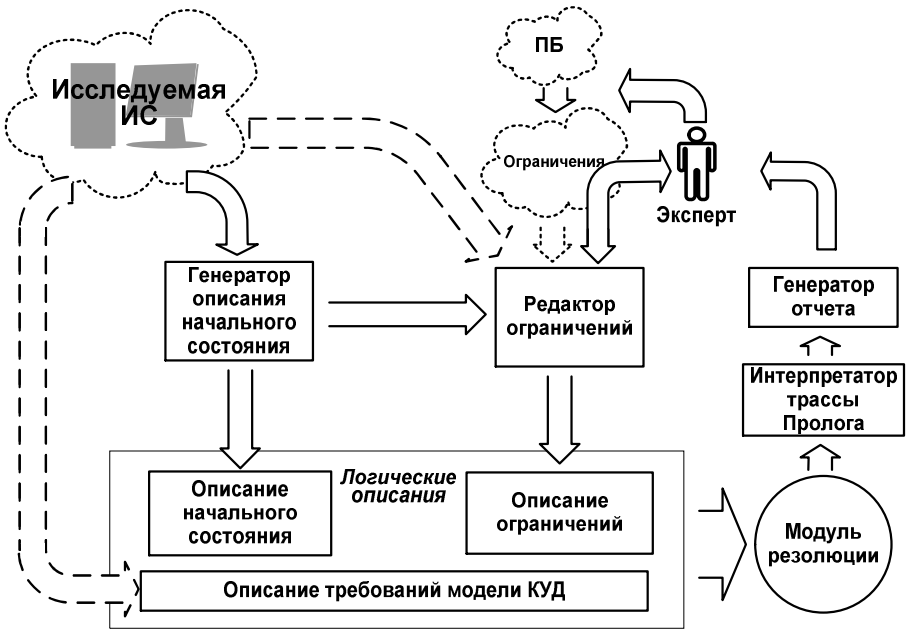

Рис. 2. Архитектура СП

Описания поступают на вход МР. Если МР достигает состояния, в котором не выполняется хотя бы одно ограничение, то интерпретатор преобразует трассу, полученную от логической машины вывода Пролога, в удобочитаемый вид и демонстрирует последовательность состояний, которые ведут к нарушению. Генератор отчетов формирует итоговый отчет, содержащий результаты проверки системы и трассу вывода для состояния, в котором не выполняются ограничения.

Использование СП придает объективный характер процессу исследования защищенности ИС. Инструментарий СП применим при разработке новых защитных механизмов систем обработки информации, при тестировании и отладке средств защиты, при сертификации систем и классификации в соответствии с государственными нормативами, а также во время эксплуатации систем защиты для поиска состояний системы, не соответствующих ПБ.

В четвертой главе рассмотрена разработанная автором методика проверки выполнения правил ПБ на основе автоматизированного анализа безопасности состояний, приведен пример применения СП при анализе подсистемы защиты, реализованной в ОС Windows 2000.

Разработанная методика представлена на рис. 3.

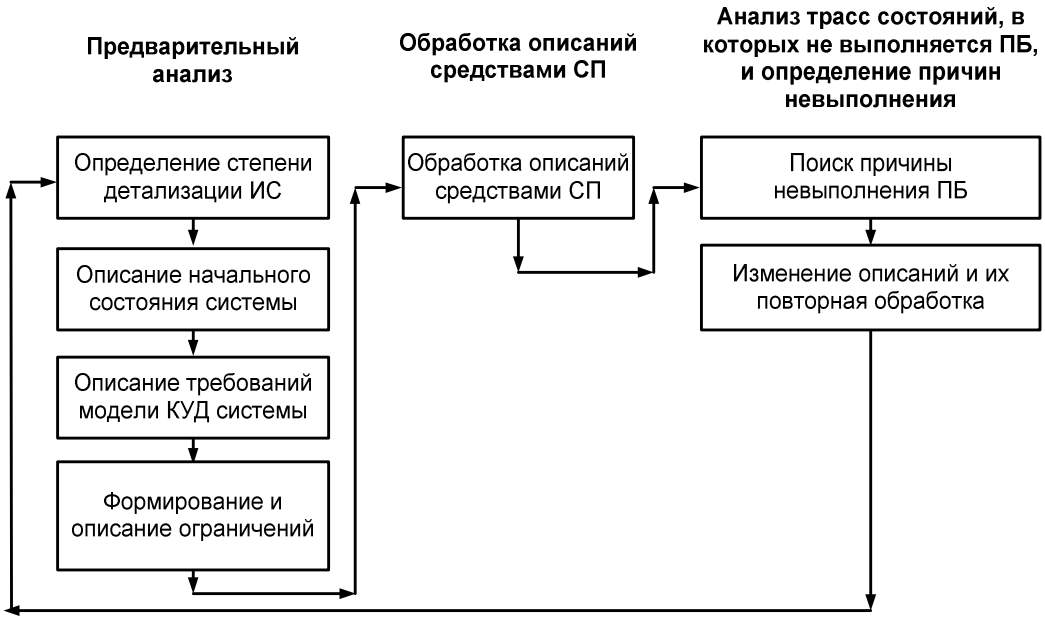

Рис. 3. Методика проверки выполнения правил ПБ

На этапе предварительного анализа выполняется определение степени детализации ИС: определяется, какие субъекты, объекты, атрибуты безопасности следует вносить в описание системных состояний. Выбирается, какие требования КУД из реализованной в системе модели безопасности следует записывать в форме предикатов и правила ПБ, по которым будет проверяться ИС. После этого формируются логические описания, которые затем обрабатываются средствами СП.

Результатом проверки является итоговый отчет о выполнении правил ПБ. Процесс проверки считается успешно завершенным, если выполнены все ограничения. В случае нарушения какого-либо ограничения указывается состояние ИС, в котором оно не выполнилось. При этом с помощью трассы логического вывода определяется причина невыполнения ПБ. Средства СП

позволяют выполнить этот поиск автоматически. Описания корректируются и вновь обрабатываются в СП, чтобы повторной проверкой подтвердить решение проблемы.

В качестве примера применения методики проведена проверка ОС Windows 2000 на предмет невыполнений ПБ, возникающих из-за некорректной реализации модели КУД данной ОС. В частности при проверке данной ОС обнаружены следующие нарушения ПБ:

- настройки безопасности имеют приоритет выше, чем права пользователей,
- файлы можно копировать при наличии разрешения на их запуск,
- копирование файла может привести к смене владельца,
- пользователь из группы Power User может оперировать членствами субъектов, которых сам не создавал,
- пользователь не может удалить каталог, которым владеет.

Использование СП позволило автоматически выявить те состояния Windows 2000, в которых из-за ошибок разработчиков ОС не выполняется ПБ, что позволило повысить гарантированность защиты информации.

Разработанную СП можно использовать как средство проверки разрешительной подсистемы ИС на предмет выполнения правил ПБ в соответствии с требованиями ГОСТ Р ИСО 15408. Применение СП гарантирует выполнение функций защиты существующих и создаваемых ИС.

Макет СП и результаты, полученные при реализации проекта, неоднократно демонстрировались на различных конференциях и семинарах.

В заключении приведены результаты и выводы, полученные автором в ходе выполнения работы.

В работе получены следующие основные результаты:

1. На основании анализа моделей КУД и методов моделирования ПБ обоснован подход к проверке выполнения правил ПБ путем логического моделирования и вычисления предикатов.

2. Разработаны концептуальные модели подсистем КУД для современных ОС и на их базе реализована система предикатов для описания

системных состояний, требований модели КУД и правил ПБ в качестве формы представления средств защиты.

3. Впервые предложен метод проверки выполнения правил ПБ на основе вычисления логических предикатов, описывающих системные состояния, требования модели КУД и правила ПБ, который закладывает основы для автоматизации сертификационных исследований по ГОСТ Р ИСО 15408.

4. Разработан МР, позволяющий выполнять анализ системных состояний путем вычисления предикатов и предоставляющий средства объяснения достигнутых результатов посредством демонстрации последовательности логического вывода.

5. Разработана система проверки выполнения правил ПБ, применяемая для автоматизированных исследований ИС.

6. Разработана методика проверки выполнения правил ПБ в ходе сертификационных исследований ИС по ГОСТ Р ИСО 15408.

Основные результаты диссертационной работы изложены в 32 печатных трудах. Ниже приведены основные из них:

1. 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.

2. Зегжда Д.П., Калинин М.О. Моделирование политик безопасности для исследовательских и обучающих целей // Проблемы информационной безопасности. Компьютерные системы. 2000. №2. С. 105-111.

3. Калинин М.О. Лабораторное моделирование и исследование политик безопасности // Методы и технические средства обеспечения безопасности информации: Тез. докл. СПб: Изд-во СПбГТУ. 2000. С. 204-207.

4. Зегжда П.Д., Калинин М.О. Тестирование систем разграничения доступа, основанных на формальных политиках безопасности // Проблемы обеспечения информационной безопасности на федеральном железнодорожном транспорте: Доклады, тезисы, статьи. СПб: Изд-во СПб фил. "Внедренческий центр" ГУП "Аттест. центр Желдоринформзащита МПС РФ". 2001. С. 123-127.

5. Калинин М.О. Моделирование политик безопасности с применением метода графов // ИБРР-2001: Материалы конф. СПб: Политехника-сервис. 2001. Т. 1. С. 150.

6. Калинин М.О. Структура и применение языка описания политик безопасности // Проблемы информационной безопасности. Компьютерные системы. 2002. №1. С. 18-26.

7. Калинин М.О. Автоматическое доказательство защищенности систем дискреционного управления доступом // Методы и технические средства обеспечения безопасности информации: Докл. СПб: Изд-во СПбГТУ. 2002. С. 9-11.

8. Калинин М.О. Классификация методов моделирования политик безопасности // Методы и технические средства обеспечения безопасности информации: Докл. СПб: Изд-во СПбГТУ. 2002. С. 12-15.

9. Калинин М.О. Средство автоматического доказательства безопасности систем дискреционного управления доступом // ИБРР-2002: Материалы конф. СПб: Политехника-сервис. 2002. С. 144.

10. Зегжда Д.П., Калинин М.О. Оценка защищенности информационных систем // Проблемы информационной безопасности. Компьютерные системы. 2002. №3. С. 7-12.

11. Калинин М.О. Методы моделирования политик безопасности // ИБРР-2002: Материалы конф. СПб: Политехника-сервис. 2002. С. 144.

12. Зегжда Д.П., Калинин М.О. Безопасность операционных систем. Модели контроля и управления доступом: Лаб. практикум. Ч.1. Дискреционные модели. СПб: Изд-во СПбГПУ, 2003. 104 с.

13. Зегжда Д.П., Калинин М.О. Безопасность операционных систем. Модели контроля и управления доступом: Лаб. практикум. Ч.2. Мандатные, информационные и комбинированные модели. СПб: Изд-во СПбГПУ, 2003. 76 с.

14. Калинин М.О. Автоматический анализ состояний операционной системы Windows 2000 // Проблемы информационной безопасности. Компьютерные системы. 2003. №1. С. 4-6.