МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М. В. ЛОМОНОСОВА
Механико-математический факультет

На правах рукописи

Шапченко Кирилл Александрович

Методы и программные средства исследования моделей логического разграничения доступа на предмет выполнения требований по безопасности

05.13.19 – методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва – 2010

Работа выполнена на Механико-математическом факультете и в Институте проблем информационной безопасности Московского государственного университета имени М. В. Ломоносова.

Научный руководитель: доктор физико-математических наук, профессор *Васенин Валерий Александрович.*

Официальные оппоненты: доктор физико-математических наук, профессор *Галатенко Владимир Антонович*;

доктор технических наук, доцент *Девянин Петр Николаевич.*

Ведущая организация: ФГУП «НИИ «Квант».

Защита диссертации состоится 17 февраля 2010 г. в 16 час. 45 мин. на заседании диссертационного совета Д 501.002.16 при Московском государственном университете имени М. В. Ломоносова по адресу: Российская Федерация, 119991, ГСП-1, Москва, Ленинские горы, д. 1, Московский государственный университет имени М. В. Ломоносова, Механико-математический факультет, ауд. 14-08.

С диссертацией можно ознакомиться в библиотеке Механико-математического факультета Московского государственного университета имени М. В. Ломоносова (Главное здание МГУ, 14 этаж).

Автореферат разослан 15 января 2010 г.

Ученый секретарь
диссертационного совета
Д 501.002.16 при МГУ,
доктор физико-математических наук Корнев А. А.

Общая характеристика работы

Актуальность работы. Механизмы логического разграничения доступа к информационным активам, коммуникационным и вычислительным ресурсам (далее для краткости изложения используются сочетание «логическое разграничения доступа» и сокращение «ЛРД») являются важной составляющей современных компьютерных систем, к защищенности которых предъявляются повышенные требования.[1] С использованием механизмов логического разграничения доступа по заданному набору правил принимается решение о том, разрешено ли в автоматизированной системе некоторое действие, например, получение доступа к ее информационному ресурсу. Проблематике проектирования и разработки механизмов ЛРД, их интеграции в автоматизированные системы, информационные ресурсы которых подлежат защите, а также к построению математических моделей, описывающих процессы функционирования таких механизмов, уделяется повышенное внимание с конца 1960-х — начала 1970-х годов. К настоящему времени созданы многочисленные механизмы логического разграничения доступа, традиционным примером которых являются механизмы ЛРД в операционных системах (ОС), разработаны подходы к описанию математических моделей, составляющих основу функционирования подобных программных механизмов. К классическим формальным моделям логического разграничения доступа относятся модели дискреционного разграничения доступа, в том числе модель «take-grant», модели мандатного многоуровневого разграничения доступа, включая фундаментальные модели Белла-ЛаПадула и Биба. Получили широкое распространение модели ЛРД на основе ролей, ключевые положения которых начали формироваться в 1990-е годы. Активно ведутся исследования в рассматриваемой области отечественными учеными.[2]

Положения законов и подзаконных актов, нормативно-регламентирующих документов, стандартов и рекомендаций в области обеспечения безопасности информационных технологий определяют ряд требований к механизмам защиты в автоматизированных системах, в том числе — к механизмам логического разграничения доступа. Вместе с тем, практической реализации таких требований в современных системах препятствует то обстоятельство, что управление настройками подобных механизмов, как правило, осуществляется без должного анализа последствий. Изменения в настройки вносятся локально, модифицируются небольшие фрагменты правил логического разграничения доступа. При этом оценка влияния таких изменений на защищенность компьютерной системы в целом не производится. В результате уровень доверия к такой системе снижается. Отмеченная особенность характерна для механизмов ЛРД в современных Unix-подобных

[1] Н. А. Гайдамакин. Разграничение доступа к информации в компьютерных системах. — Екатеринбург: Изд-во Уральского университета. — 2003. — 328 с.

В. А. Галатенко. Основы информационной безопасности. Курс лекций. 4-е изд. — М.: «Интуит», 2008. — 205 с.

А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. Теоретические основы компьютерной безопасности. — М.: Academia. — 2009. — 272 с.

[2] П. Н. Девянин. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. — М.: Радио и связь, 2006. — 176 с.

операционных системах, например, в ОС на базе ядра ОС Linux, которые в настоящее время часто используются в автоматизированных системах с повышенным уровнем защищенности.

Формальной спецификации требований, которые предъявляются к механизмам и, как следствие, к моделям логического разграничения доступа, посвящено большое число работ. Значительное внимание уделяется задачам проверки выполнения ограничений на информационные потоки.[2, 3] Однако, результатов практического характера, целью которых является исследование моделей ЛРД, положенных в основу механизмов защиты современных Unix-подобных ОС, недостаточно для проведения анализа таких механизмов и их конфигурации на предмет выполнения требований по безопасности. Необходимость проведения такого анализа с учетом особенностей моделей и реализующих их механизмов ЛРД, которые используются в современных Unix-подобных ОС, значительный, как правило, объем конфигурационных данных таких механизмов и потребности в их совместном использовании на практике определяют актуальность настоящей работы.

Цель диссертационной работы состоит в исследовании и разработке математических моделей, алгоритмов и программных средств, поддерживающих процессы спецификации и анализа свойств моделей логического разграничения доступа, ориентированных на применение в инструментальных средствах автоматизации управления настройками механизмов логического разграничения доступа в компьютерных системах, в составе которых используются Unix-подобные операционные системы.

Научная новизна результатов диссертации состоит в создании новых доказательно обоснованных способов описания моделей логического разграничения доступа, корректного объединения таких моделей, в их анализе на предмет выполнения заданных требований по безопасности. Отличительной особенностью разработанных автором способов, формальных моделей и алгоритмов является возможность математически строго описывать и анализировать с их помощью конфигурацию механизмов логического разграничения доступа в современных компьютерных системах, которые используют Unix-подобные операционные системы, такие, как ОС на базе ядра Linux, имея в виду архитектурные и функциональные особенности механизмов ЛРД в таких системах.

Практическая значимость диссертации заключается в применении созданного автором программного комплекса в процессе анализа моделей логического разграничения доступа на предмет выполнения требований по безопасности. Потенциальные возможности комплекса продемонстрированы на дистрибутивах операционных систем на базе ядра ОС Linux и программного обеспечения с открытым исходным кодом. В процессе тестовых испытаний показаны функциональные возможности разработанного программного комплекса по анализу настроек механизмов логического разграничения доступа при создании специализированных дистрибутивов ОС.

---

[3] J. Frank, M. Bishop. Extending the Take-Grant Protection System. — Department of Computer Science. — University of California at Davis. — 1996.

J. McLean. Security Models and Information Flow. // In Proc. IEEE Symposium on Security and Privacy. — IEEE Computer Society Press. — 1990. — pp. 180–187.

На защиту выносятся следующие основные результаты:

- разработаны и сформулированы способы формального описания моделей логического разграничения доступа для достаточно широкого класса компьютерных систем, в первую очередь — для систем на базе ядра ОС Linux;
- сформулированы и строго обоснованы положения нового способа объединения и согласования математических моделей логического разграничения доступа, с помощью которого предоставляется возможность исследовать совместно используемые механизмы ЛРД в компьютерных системах, разрабатываемых на основе Unix-подобных операционных систем;
- разработан доказательно корректный способ спецификации и анализа свойств моделей логического разграничения доступа, с помощью которого может быть проверено выполнение ограничений на информационные потоки в компьютерной системе;
- предложен и апробирован в процессе тестовых испытаний программный комплекс для анализа моделей логического разграничения доступа, которые реализуются с помощью механизмов ЛРД в Unix-подобных ОС, на предмет выполнения ими требований по безопасности.

Внедрение результатов работы. Результаты работы нашли применение в процессе выполнения проектов: «Методы и средства противодействия компьютерному терроризму: механизмы, сценарии, инструментальные средства и административно-правовые решения» (НИР 2005-БТ-22.2/001 в рамках ФЦП «Исследования и разработки по приоритетным направлениям науки и техники»); «Разработка подходов к обеспечению информационной безопасности автоматизированных систем государственного управления на основе использования в их составе программного обеспечения с открытым кодом» (НИР 2007-4-1.4-15-04-001 в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007–2012 годы»). Получено свидетельство об официальной регистрации программы для ЭВМ «Набор специализированных дистрибутивов ОС Linux с повышенными требованиями к защищенности» (свидетельство № 2006613706).

Апробация работы. Результаты работы докладывались на научных конференциях «Математика и безопасность информационных технологий» (2005–2008 гг.), «Ломоносовские чтения» (2006–2009 гг.), «Актуальные проблемы вычислительной математики» (2006 г.), «Третья международная конференция по проблемам управления» (2006 г.), на семинаре «Проблемы современных информационно-вычислительных систем» под руководством д.ф.-м.н., проф. В. А. Васенина (механико-математический факультет МГУ имени М. В. Ломоносова, 2005, 2007, 2009 гг.).

Публикации. По теме диссертации опубликовано 14 работ, из которых 3 статьи [1–3] — в журналах из перечня ведущих рецензируемых изданий, рекомендованных ВАК. Материалы работы вошли в главу 3 опубликованной в 2008 году коллективной монографии «Критически важные объекты и кибертерроризм. Часть 2. Аспекты программной реализации средств противодействия» под ред. В. А. Васенина [8].

Личный вклад автора заключается в проведенном им анализе современного состояния в области формального описания моделей логического разграничения доступа, в способе, предложенном для объединения таких моделей, а также в разработанных автором и апробированных на практике методах, математических моделях, алгоритмах и программных средствах для анализа свойств механизмов логического разграничения доступа.

Структура и объем диссертации. Работа состоит из введения, пяти глав, заключения и списка литературы. Общий объем диссертации составляет 128 страниц. Список литературы включает 94 наименования.

Содержание работы

Во введении сформулирована цель диссертационной работы, обоснована ее актуальность, аргументирована научная новизна и практическая значимость полученных результатов, представлены выносимые на защиту результаты исследований.

Глава 1 посвящена исследованию и систематизации актуальных задач в управлении настройками механизмов логического разграничения доступа.

Исходные посылки для проведения анализа моделей ЛРД на предмет выполнения требований безопасности формируются на основе положений политики информационной безопасности (ПИБ) исследуемой автоматизированной системы. Положениями такой политики в том числе определяется ряд требований к функциям по защите информации, которые в исследуемой компьютерной системе реализуются в используемых аппаратно-программных средствах, а также задаются высокоуровневые правила по использованию таких функций защиты. Объектом исследования в настоящей работе является программная реализация отдельного класса таких функций, а именно — функций логического разграничения доступа.

Определение 1. Программную реализацию функций ЛРД будем называть *механизмом логического разграничения доступа (механизмом ЛРД)*. В таком механизме реализуется вычислительный алгоритм принятия решения о доступе. Механизм ЛРД встраивается в автоматизированную систему с целью реализовать назначение функций ЛРД, а именно — разрешение или запрет выполнения некоторого множества операций в данной системе. Входными данными для реализуемого алгоритма принятия решения о доступе является *конфигурация механизма ЛРД* и тройка *(субъект доступа, объект доступа, тип доступа)*. В конфигурации механизма ЛРД некоторым зависящим от его реализации способом задаются множества объектов и субъектов доступа, а также правила логического разграничения доступа.

Результаты настоящей работы в первую очередь нацелены на их применение в процессе исследования настроек механизмов ЛРД в современных Unix-подобных операционных системах. Примером таких механизмов являются традиционные средства разграничения доступа в подобных ОС, а также механизмы системы защиты SELinux для ядра ОС Linux.

Как правило, алгоритм принятия решения о доступе функционирует согласно некоторой формальной модели, именуемой *моделью логического разграничения доступа*. Представим определение моделей ЛРД, которые являются предметом настоящего исследования.

Определение 2. *Моделью логического разграничения доступа* называется четверка $M = (S, O, A, \Delta)$, где

- S — конечное и непустое множество субъектов доступа;
- O — конечное и непустое множество объектов доступа;
- A — конечное и непустое множество типов доступа;
- Δ — предикат над множеством $S \times O \times A$, определяющий для тройки $(s, o, a) \in S \times O \times A$, разрешен ли доступ типа a субъекта s к объекту o (*предикат предоставления доступа*).

Модели логического разграничения доступа, которые задаются представленным определением и исследуются в настоящей работе, описывают так называемую «статическую» часть правил ЛРД. Такие правила определяют действия субъектов доступа над объектами доступа, которые разрешены в автоматизированной системе. Множества субъектов, объектов и типов доступа в модели ЛРД, а также предикат предоставления доступа рассматриваются как неизменные. Такой способ описания моделей ЛРД позволяет исследовать настройки механизмов логического разграничения доступа в рамках тех процессов функционирования автоматизированной системы, в которых не производится действий по созданию или удалению субъектов и объектов доступа, по изменению атрибутов таких сущностей, по изменению правил доступа субъектов к объектам, либо такие действия не оказывают влияния на предикат предоставления доступа в модели. Указанные условия вносят некоторые ограничения в класс автоматизированных систем, способ анализа настроек механизмов защиты которых предлагается в настоящей работе. Однако, такой класс остается достаточно широким и значимым в практическом плане.

С учетом представленных определений опишем схему, в рамках которой связываются понятия механизма и модели ЛРД, а также требования, которые предъявляются к ним (рис. 1). Требования к механизму ЛРД формируются на основе интерпретации требований политики информационной безопасности. В свою очередь, требования к модели ЛРД являются результатом интерпретации требований к механизму ЛРД в терминах реализуемой им модели. Такие требования, в отличие от требований ПИБ и требований к механизму ЛРД, описаны формально. Один из основных результатов настоящей работы, а именно — метод спецификации и проверки выполнения требований безопасности в моделях ЛРД, позволяет удостовериться, что модель ЛРД, реализуемая исследуемым механизмом ЛРД, удовлетворяет тем требованиям, которые были получены в результате интерпретации по указанной схеме. В том случае, если в автоматизированной системе используются несколько механизмов ЛРД, такая схема усложняется. Набор используемых механизмов ЛРД явным или неявным образом составляет объединенный механизм ЛРД, который реализует некоторую интегрированную модель ЛРД. Способ построения подобной объединенной модели является одним из основных результатов, представляемых в настоящей работе.

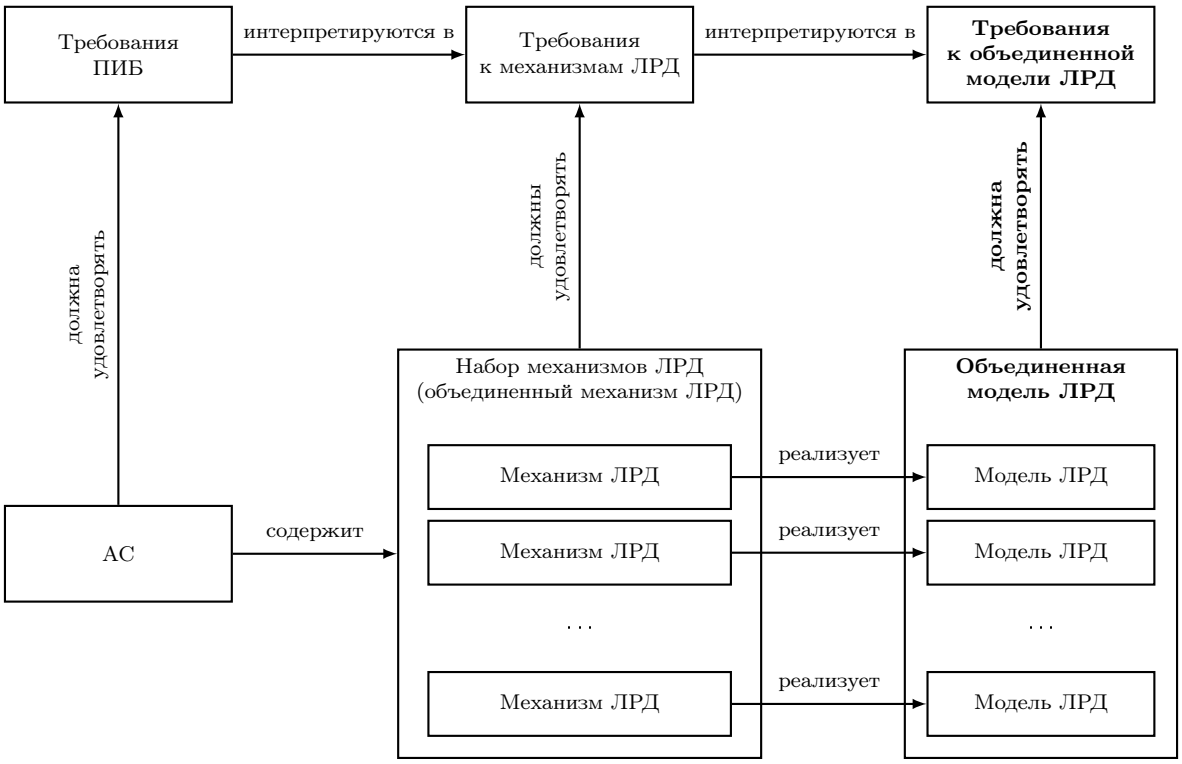

Рис. 1. Требования к механизмам и моделям логического разграничения доступа (случай использования нескольких механизмов ЛРД).

Целесообразно выделить следующий набор общих по постановке задач, связанных с исследованием, разработкой и использованием моделей логического разграничения доступа в современных компьютерных системах:

- построение моделей логического разграничения доступа по данным о конфигурации механизмов разграничения доступа в компьютерной системе («задача преобразования настроек в модель»);
- задание конфигурации механизмов логического разграничения доступа на основе формальной модели («задача преобразования модели в настройки»);
- объединение и согласование моделей логического разграничения доступа отдельных компонентов системы («задача объединения»);
- спецификация и проверка свойств моделей логического разграничения доступа («задача верификации»);
- проверка соответствия модели логического разграничения доступа механизму обеспечения безопасности компьютерной системы, функциональные возможности которого она моделирует («задача валидации»).

С учетом представленных выше общих задач на направлении разработки и использования моделей ЛРД в современных автоматизированных системах выделим те из них, которые составляют предмет исследования в настоящей работе. Перечисленные далее, эти задачи в первую очередь связаны с формальным описанием моделей ЛРД и проверкой (анализом) выполнения ими требований по безопасности. Их суть заключается в разработке методов и средств:

- формального описания используемых моделей ЛРД;
- объединения моделей ЛРД отдельных компонентов в составе сложно орга-

низованной системы;

- спецификации и проверки требований по безопасности в моделях ЛРД.

Отметим, что результаты решения первых двух задач закладывают основу для формирования методов и средств для исследования моделей ЛРД в последней из перечисленных задач.

Автором проводится исследование современных методов и средств спецификации и проверки свойств в моделях логического разграничения доступа. Анализируются предпосылки к проведению такой проверки. Приводится краткий обзор методов спецификации и проверки свойств механизмов логического разграничения доступа с использованием аппарата математических моделей ЛРД. Исследованию таких моделей на направлении выполнения в них требований по безопасности посвящен ряд современных работ как зарубежных авторов,[4] так и российских ученых.[5] В главе рассматривается несколько классов задач проверки выполнения требований, предъявляемых к моделям ЛРД:

- поиск конфликтов правил в моделях ЛРД;
- поиск конфликтов правил при объединении нескольких моделей ЛРД;
- сравнение двух моделей ЛРД;
- исследование свойств информационных потоков.

Особое внимание уделяется классу задач, связанных с так называемыми разрешенными (или допустимыми) составными информационными потоками (далее, для краткости, — информационными потоками). Понятие информационного потока определяется следующим образом для моделей ЛРД, в которых ряд типов доступа подразумевает передачу информации между сущностями в модели. Пусть в рассматриваемой модели ЛРД рассматривается субъект доступа C и объект доступа O. Будем считать, что *элементарный информационный поток* от C к O разрешен, если правилами ЛРД допускается доступ «на запись» от C к O. Аналогичным образом, элементарный информационный поток от O к C разрешен, если правилами допускается доступ «на чтение» от C к O. Под типами доступа «на чтение» и «на запись» в работе понимаются такие, что при реализации соответствующего доступа информация передается от объекта к субъекту (для типа доступа «на чтение») и от субъекта к объекту (для типа доступа «на запись»). Отметим, что типов доступа «на чтение» и «на запись» может быть несколько. Из набора элементарных информационных потоков складываются составные допустимые информационные потоки. Будем считать, что между сущностями A1 и A2, каждая из которых может быть субъектом или объектом доступа в модели ЛРД, разрешен информационный поток, если существует конечная последователь-

[4] J. D. Guttman, A. L. Herzog, J. D. Ramsdell, C. W. Skorupka. Verifying information flow goals in security-enhanced Linux. // Journal of Computer Security, vol. 13, 2004.

D. P. Guelev, M. D. Ryan, P.-Y. Schobbens. Model-checking access control policies. // In Information Security Conference, number 3225 in Lecture Notes in Computer Science. Springer-Verlag, 2004.

G. Hughes, T. Bultan. Automated verification of access control policies. // Technical Report 2004-22. — University of California, Santa Barbara, 2004.

[5] П. Н. Девянин. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. — М.: Радио и связь, 2006. — 176 с.

Д. Н. Колегов. Применение ДП-моделей для анализа защищенности сетей. // Прикладная и дискретная математика. — 2008. — № 1. — 71–87.

ность элементарных информационных потоков такая, что

- первый элементарный поток начинается в A1;
- последний элементарный поток заканчивается в A2;
- конечная сущность каждого элементарного потока кроме последнего совпадает с началом следующего элементарного потока.

По причине важности ограничения составных информационных потоков в практически значимых механизмах логического разграничения доступа, ставятся задачи проверки свойств таких потоков в моделях ЛРД. Общий вид одного из типовых свойств информационных потоков формулируется следующим образом. Пусть задано ограничение на информационный поток, в частности, указаны требования к начальной и конечной сущностям в потоке, а также — к последовательности сущностей и типов доступа в потоке, например, что одна сущность A2 всегда идет после сущности A1 и между ними всегда есть сущность A3. Необходимо проверить, выполняется ли это свойство для всех допустимых информационных потоков в заданной модели ЛРД. Отметим, что, как правило, кроме непосредственно проверки выполнения такого свойства появляется необходимость в построении контрпримера для случая, если оно не выполняется. Дополнительная информация, которая получается в процессе интерпретации подобного контрпримера, может упростить поиск некорректно заданных правил разграничения доступа. Отметим, что задание свойств, которыми должны обладать информационные потоки, зачастую составляют основу для формализации других задач проверки свойств моделей ЛРД. Например, ряд задач поиска конфликтов в модели ЛРД или в объединении таких моделей может быть сформулирован в терминах информационных потоков.

Далее в главе приводится описание основных положений и критический анализ методов проверки требований в моделях ЛРД. Рассматриваются следующие способы проверки требований безопасности в моделях ЛРД:

- поиск пути в графе и алгоритмы переписывания графов;
- методы «верификации на модели» («model checking»);
- методы автоматического доказательства теорем;
- исследование модели ЛРД как вычислительного алгоритма или программы на некотором императивном языке программирования.

Выявленные особенности методов проверки требований безопасности в моделях ЛРД являются одними из отправных положений, в соответствии с которыми автором разрабатывается новый метод проверки свойств моделей ЛРД. Такой метод проектируется с целью его дальнейшего использования на практике для исследования свойств моделей ЛРД в современных автоматизированных системах, использующих Unix-подобные операционные системы, в том числе — ОС на основе ядра Linux. Новый метод позволит отразить в математической модели ЛРД ряд типовых функциональных особенностей механизмов защиты таких систем, уменьшить объем исследуемых моделей с помощью отождествления «похожих» правил доступа, эффективно проверить свойства из некоторого класса требований, которые являются распространенными для целевых систем.

Во второй главе автором предложен способ формального описания моделей логического разграничения доступа, для которых будет проводиться анализ на

предмет выполнения требований по безопасности.

Автором предлагается унифицированный способ описания статической части моделей ЛРД, позволяющий в единообразной форме записывать модели логического разграничения доступа, которые относятся к рассмотренным ранее в главе традиционно используемым классам таких моделей. В основу предлагаемого способа описания положено расширение понятия «контекст безопасности» из модели ЛРД Type Enforcement. Ключевой особенностью этого понятия является то обстоятельство, что аргументами предиката предоставления доступа в модели ЛРД являются два контекста безопасности и тип производимого доступа. Таким образом, использование контекстов безопасности позволяет в рамках унифицированного описания абстрагироваться от особенностей субъектов и объектов доступа за счет инкапсуляции таких особенностей в понятие контекста безопасности.

Предлагаемый унифицированный способ описания моделей ЛРД не изменяет свойств (семантики) моделей ЛРД, а лишь позволяет записать их правила в унифицированном виде. В рамках этого способа описание модели ЛРД строится следующим образом. В модели определяются базовые множества $SC = \{sc_1, sc_2, \ldots\}$ — конечное и непустое множество контекстов безопасности, $A = \{r, w, \ldots\}$ — конечное и непустое множество типов доступа, а также определяется предикат предоставления доступа Δ_U над множеством $SC \times SC \times A$.

Определение 3. Тройку $\widetilde{M}_U = (SC, A, \Delta_U)$ назовем *унифицированной моделью ЛРД на основе контекстов безопасности.*

Для того, чтобы записать некоторую другую модель ЛРД M в рамках такого способа необходимо определить два отображения:

$\tau_M^{(S)} : S_M \to SC$ — отображение субъектов доступа из M на контексты безопасности в унифицированном описании;

$\tau_M^{(O)} : O_M \to SC$ — отображение объектов доступа из M на контексты безопасности в унифицированном описании.

Множество типов доступа остается неизменным: $A = A_M$.

Такие отношения должны удовлетворять следующему свойству: предикат предоставления доступа должен сохраняться, то есть

$$\forall s \in S_M \ \forall o \in O_M \ \forall a \in A : \quad \Delta_M(s, o, a) = \Delta_U(\tau_M^{(S)}(s), \tau_M^{(O)}(o), a). \qquad (1)$$

Определение 4. Пусть задана модель логического разграничения доступа $M = (S_M, O_M, A_M, \Delta_M)$ и определены множество SC и отображения $\tau_M^{(S)} : S_M \to SC$ и $\tau_M^{(O)} : O_M \to SC$. Пусть выполнено условие (1). В таком случае будем считать, что *модель логического разграничения доступа M может быть записана в унифицированном виде.*

Для ряда традиционно используемых и современных моделей ЛРД, а именно — моделей ЛРД с использованием матрицы доступа и списков доступа, базовых многоуровневых и базовых ролевых моделей ЛРД, моделей Type Enforcement, Role Compatibility и grsecurity/RBAC, автором представлены

доказательства утверждений о возможности их представления с помощью предложенного способа унифицированного описания.

Как отмечалось ранее, основными моделями ЛРД, для анализа которых автором разрабатывается способ проверки требований по безопасности, являются те модели, которые реализуются механизмами защиты в современных Unix-подобных ОС. Как правило, с помощью подобных механизмов ограничивается доступ к объектам (например, к объектам файловых систем), на множестве которых задана некоторая иерархическая структура. Особенности подобной структуры необходимо принимать во внимание при формировании подлежащей анализу модели ЛРД. По этой причине автором предложен способ формального описания моделей ЛРД, позволяющих учитывать древовидную иерархию, заданную на множестве объектов доступа. Он не является единственно возможным способом задания древовидной иерархии объектов доступа в модели ЛРД, однако позволяет учесть особенности правил ЛРД к объектам файловых систем в современных Unix-подобных ОС. Пусть задана модель ЛРД $M = (S, O, A, \Delta)$. Зададим отношение иерархии на множестве O и продемонстрируем, как построить такую модель ЛРД M', для которой будут выполнены следующие свойства:

- доступ к каждому объекту $o \in O$ в рамках ее правил будет разрешен только в том случае, если разрешен доступ к каждому из объектов, которые стоят выше в иерархии, чем объект o;
- если предыдущее условие выполнено, то доступ к объекту будет разрешен или запрещен по тем же правилам, что и в модели ЛРД M.

Определим функцию $parent : O \to O \sqcup \{None\}$, которая будет сопоставлять каждому объекту $o \in O$ другой объект $p \in O$, который является контейнером, содержащим объект o, либо выделенную константу $None$ в случае, если o является корневым элементом в древовидной иерархии.

Определение 5. Пусть задано конечное и непустое множество O, а также функция $parent : O \to O \sqcup \{None\}$. *Путем* в множестве O по отношению к функции $parent$ назовем конечную последовательность $\pi = o_0 o_1 \dots o_n$ такую, что $o_i \in O$, $i = 0, \dots, n$ и $parent(o_i) = o_{i+1}$, $i = 0, \dots, n-1$. Функция $parent$ *задает древовидную иерархию* на множестве O, если выполнены следующие условия:

- существует единственный элемент $o_{root} \in O$ (называемый *корневым элементом* в иерархии), такой что $parent(o_{root}) = None$;
- для любого $o \in O$ существует единственный путь $\pi = o_0 o_1 \dots o_n$, такой что $o_0 = o$ и $o_n = o_{root}$.

Автором предложен способ, как с помощью заданной в соответствии с определением 5 функции $parent$ по модели ЛРД $M = (S, O, A, \Delta)$ построить модель $M_{Hier} = (S, O, A_{Hier}, \Delta_{Hier}, parent)$, которая будет учитывать древовидную иерархию на множестве объектов доступа O описанным ранее способом.

Определение 6. Пусть задана модель ЛРД $M = (S, O, A, \Delta)$, а также определена функция $parent$, задающая древовидную иерархию на O. Пусть $A_{Hier} = A \cup \{a_x\}$, где дополнительный тип доступа a_x содержательно означает возможность проведения операций над элементами контейнера в заданной древовидной иерар-

хии, а модель ЛРД M расширена до модели $M' = (S, O, A_{Hier}, \Delta')$. При этом $\Delta'(s, o, a) = \Delta(s, o, a)$ для всех $s \in S$, $o \in O$ и $a \in A$. Определим предикаты Δ_{parent} и Δ'_{Hier} на множествах $S \times O \times A_{Hier}$ и $S \times (O \sqcup \{None\}) \times A_{Hier}$ соответственно:

$$\Delta_{parent}(s, o, a) \equiv \begin{cases} \text{истина}, & \text{если } parent(o) = None; \\ \Delta'_{Hier}(s, parent(o), a_x), & \text{иначе.} \end{cases} \quad (2)$$

$$\Delta'_{Hier}(s, o, a) \equiv \begin{cases} \text{ложь}, & \text{если } o = None; \\ \Delta_{parent}(s, o, a) \wedge \Delta'(s, o, a), & \text{иначе,} \end{cases} \quad (3)$$

Определим предикат Δ_{Hier} на множестве $S \times O \times A_{Hier}$ как совпадающий с предикатом Δ'_{Hier}. Тогда модель ЛРД $M_{Hier} = (S, O, A_{Hier}, \Delta_{Hier}, parent)$ назовем *расширением модели ЛРД* $M = (S, O, A, \Delta)$, *учитывающим древовидную иерархию, заданную функцией* $parent$.

Определение 6 корректно, то есть предикат предоставления доступа в расширенной модели ЛРД может быть вычислен, причем однозначным образом. Такое свойство гарантируется единственностью пути от объекта доступа к корневому элементу древовидной иерархии (определение 5).

Автором предложены формальные описания моделей ЛРД, которые используются в современных Unix-подобных операционных системах, а именно — традиционная модель прав доступа «Unix permissions», модель Type Enforcement для механизмов Security-Enhanced Linux (SELinux), модель Role Compatibility для механизмов Rule-Set Based Access Control (RSBAC), ролевая модель для набора механизмов grsecurity. Для двух моделей ЛРД, которые реализуются механизмами защиты grsecurity и RSBAC в ядре ОС Linux, а именно — моделей grsecurty/RBAC и Role Compatibility, автором доказаны утверждения об их представлении с помощью логико-языковых средств модели ЛРД Type Enforcement, используемой в системе SELinux.

Глава 3 посвящена новому, разработанному автором, методу объединения формальных моделей логического разграничения доступа. Отмечается актуальность задачи согласования моделей при анализе компьютерных систем, отдельные компоненты которых используют различные механизмы логического разграничения доступа. В первую очередь разработанный метод ориентирован на объединение моделей ЛРД, используемых в Unix-подобных ОС, в том числе — традиционной модели Unix Permissions и модели Type Enforcement. Необходимость объединения таких моделей в процессе их исследования на предмет выполнения требований по безопасности диктуется потребностями в их совместном использовании в современных сложно организованных компьютерных системах, включая одновременное использование нескольких механизмов ЛРД в операционных системах и в сервисах прикладного уровня. Однако, указанной областью применения использование предлагаемого способа не ограничивается. Например, в процессе функционирования больших распределенных информационно-вычислительных систем, состоящих из нескольких отдельных, возможно, автономно эксплуатируемых подсистем, возникает потребность в совместном использовании информационных ресур-

сов этих подсистем. В такой ситуации, кроме согласования схем совместно используемых данных, необходимо решать задачи интеграции политик информационной безопасности, принятых в отдельных сегментах распределенной автоматизированной системы. Требования к моделям и реализующим их механизмам логического разграничения доступа являются важной составляющей политики информационной безопасности. В процессе решения задачи интеграции политик безопасности большой системы возникает необходимость согласования реализованных в ней моделей логического разграничения доступа. Элементом совместного использования информационных ресурсов является предоставление доступа от субъекта одной подсистемы к объекту другой подсистемы. Решение о предоставлении доступа в таком случае должно основываться на модели ЛРД в подсистеме, содержащей объект доступа. В то же время, эффективный субъект доступа может быть определен с помощью выбранной схемы согласования моделей ЛРД.

При согласовании моделей ЛРД необходимо принимать во внимание следующие аспекты:

- сохранение правил, по которым определяется возможность доступа без взаимодействия между несколькими подсистемами, использующими различные модели ЛРД;
- комбинирование правил доступа в том случае, если некоторый субъект или объект доступа одновременно используется в нескольких моделях ЛРД (например, принадлежит нескольким подсистемам);
- разработка правил, по которым определяется возможность доступа от субъектов одной подсистемы к объектам другой.

Представим предложенную автором формальную постановку задачи согласования моделей логического разграничения доступа с использованием унифицированного способа их описанию на основе контекстов безопасности, положения которого сформулированы автором в главе 2.

Определение 7. Пусть заданы модели ЛРД $\widetilde{M_i} = (SC_i, A_i, \Delta_i)$, $i = 1, \ldots, k$ согласно определению 3. Модель ЛРД $\widetilde{M} = (SC, A, \Delta)$ назовем *объединенной моделью ЛРД* для $\widetilde{M_1}, \ldots, \widetilde{M_k}$, если для этого набора моделей заданы следующие множества, отображения и предикаты:

- $\xi_i : SC_i \to SC^{(i)} = \xi_i(SC_i) \subset SC$, $i = 1, \ldots, k$ — взаимно однозначные отображения контекстов безопасности;
- $A_{i \to j}$, $i, j = 1, \ldots, k$, $i \neq j$ — множество типов доступа от субъектов в модели $\widetilde{M_i}$ к объектам в модели $\widetilde{M_j}$;
- $\Delta_{i \to j}$, $i, j = 1, \ldots, k$, $i \neq j$ — предикаты над множествами $SC^{(i)} \times SC^{(i)} \times A_{i \to j}$, задающие правила, по которым определяется возможность доступа от контекстов безопасности в модели $\widetilde{M_i}$ к контекстам безопасности в модели $\widetilde{M_j}$;
- $\Delta_I^{\cap}$, $I \in 2^{\{1,\ldots,k\}}$, $|I| \geqslant 2$ — предикаты над множествами $\left(\bigcap_{i \in I} SC^{(i)}\right) \times \left(\bigcap_{i \in I} SC^{(i)}\right) \times \left(\bigcup_{i \in I} A_i\right)$, задающие правила предоставления доступа на множествах контекстов безопасности, принадлежащих нескольким объединяемым моделям ЛРД,

а также выполняются условия

$$SC = \bigcup_{i=1,\ldots,k} SC^{(i)};\ A = \left(\bigcup_{i=1,\ldots,k} A_i\right) \cup \left(\bigcup_{i,j=1,\ldots,k;\ i\neq j} A_{i\to j}\right); \tag{4}$$

$$\begin{gathered}\Delta(sc_1, sc_2, a) = \Delta_i\left(\xi_i^{-1}(sc_1), \xi_i^{-1}(sc_2), a\right) \wedge a \in A_i \text{ для всех} \\ sc_1, sc_2 \in SC^{(i)} \setminus \left(\bigcup_{j=1,\ldots,k; j\neq i} SC^{(j)}\right),\ i = 1, \ldots, k;\end{gathered} \tag{5}$$

$$\begin{gathered}\Delta(sc_1, sc_2, a) = \Delta_I^{\cap}(sc_1, sc_2, a), \text{ если } sc_1, sc_2 \in \left(\bigcap_{i\in I} SC^{(i)}\right), \\ a \in \left(\bigcup_{i\in I} A_i\right), \text{ где } I \in 2^{\{1,\ldots,k\}}, |I| \geqslant 2;\end{gathered} \tag{6}$$

$$\begin{gathered}\Delta(sc_1, sc_2, a) = \Delta_{i\to j}, \text{ для всех } sc_1 \in SC^{(i)}, sc_2 \in SC^{(j)}, a \in A_{i\to j}, \\ \text{где } i, j \in \{1, \ldots, k\}, i \neq j.\end{gathered} \tag{7}$$

Рассмотрим ряд предлагаемых автором операций (действий) по согласованию моделей логического разграничения доступа. Каждая такая операция проводится над несколькими моделями ЛРД. Ее результатом является новая модель ЛРД. К предлагаемым операциям по согласованию моделей ЛРД относятся:

- выражение одной модели ЛРД через другую;
- объединение моделей ЛРД без внесения дополнительных доступов («слияние» моделей ЛРД);
- объединение моделей ЛРД над совпадающими множествами субъектов и объектов доступа с помощью комбинирования предикатов предоставления доступа;
- согласование моделей ЛРД с помощью операции «обобщенного слияния», объединяющей операции «слияния» моделей и комбинирования предикатов предоставления доступа;
- объединение моделей ЛРД с использованием дополнительных доступов между субъектами и объектами доступа в разных, подлежащих объединению моделях (операция «связывания» моделей ЛРД).

В первую очередь такие операции ориентированы на применение к тем моделям ЛРД, которые реализуются механизмами защиты в Unix-подобных ОС. Операции комбинирования предикатов и «обобщенного слияния» используются для объединения моделей ЛРД, заданных над пересекающимися множествами субъектов и объектов доступа. Примером таких моделей являются совместно используемые модели Unix Permissions и Type Enforcement. Операция «связывания» применяется для согласования тех моделей ЛРД, множества субъектов и объектов доступа в которых не пересекаются. В качестве примера пары таких совместно используемых моделей ЛРД следует отметить модель ЛРД, действующую в ядре ОС, и модель ЛРД для информационных ресурсов в некотором приложении, функционирующем под управлением ОС. Остановимся более подробно на двух операциях согласования, играющих ключевую роль в предлагаемом автором методе, а именно — на операциях «обобщенного слияния» и «связывания» моделей ЛРД. Представим формальные определения этих операций и ряд доказанных автором утверждений об их свойствах.

Определение 8. Пусть заданы модели ЛРД $\widetilde{M_1} = (SC_1, A_1, \Delta_1)$ и $\widetilde{M_2} = (SC_2, A_2, \Delta_2)$, а также заданы две одноместные операции $op1, op2$ и одна двухместная операция op над булевыми аргументами. Назовем модель ЛРД $\widetilde{M} = (SC, A, \Delta)$ *результатом обобщенного слияния моделей ЛРД* $\widetilde{M_1}$ *и* $\widetilde{M_2}$ (введем обозначение: $\widetilde{M} = Merge(\widetilde{M_1}, \widetilde{M_2}, op, op_1, op_2)$), если выполняются следующие условия:

$$SC = SC_1 \cup SC_2 = (SC_1 \setminus SC_2) \sqcup (SC_1 \cap SC_2) \sqcup (SC_2 \setminus SC_1);\ A = A_1 \cup A_2; \quad (8)$$

$$\begin{gathered}\Delta(sc_1, sc_2, a) = \Delta_i(sc_1, sc_2, a) \wedge a \in A_i \text{ для всех} \\ (sc_1, sc_2) \in (SC_i \times SC_i) \setminus ((SC_1 \cap SC_2) \times (SC_1 \cap SC_2)),\ i = 1, 2;\end{gathered} \quad (9)$$

$$\begin{gathered}\Delta(sc_1, sc_2, a) = op\left(\Delta_1(sc_1, sc_2, a), \Delta_2(sc_1, sc_2, a)\right) \text{ для всех} \\ (sc_1, sc_2) \in ((SC_1 \cap SC_2) \times (SC_1 \cap SC_2)),\ a \in A_1 \cap A_2; \\ \Delta(sc_1, sc_2, a) = op_i\left(\Delta_i(sc_1, sc_2, a)\right) \text{для всех} \\ (sc_1, sc_2) \in ((SC_1 \cap SC_2) \times (SC_1 \cap SC_2)),\ a \in A_i \setminus A_{3-i}, i = 1, 2;\end{gathered} \quad (10)$$

$$\begin{gathered}\Delta(sc_1, sc_2, a) = \text{ложь} \\ \text{для всех } (sc_1, sc_2) \in (SC_1 \times SC_2) \setminus ((SC_1 \cap SC_2) \times (SC_1 \cap SC_2)), a \notin A_1 \\ \text{и } (sc_1, sc_2) \in (SC_2 \times SC_1) \setminus ((SC_1 \cap SC_2) \times (SC_1 \cap SC_2)), a \notin A_2.\end{gathered} \quad (11)$$

С использованием операции обобщенного слияния моделей логического разграничения доступа можно получить такие же объединенные модели ЛРД, что и в случаях применения операций слияния и комбинирования предикатов предоставления доступа. С целью расширения данного выше определения операции обобщенного слияния до случая объединения нескольких моделей ЛРД, автором формулируются и доказываются следующие две вспомогательные леммы о свойствах этой операции.

Лемма 1. ***(О коммутативности операции обобщенного слияния моделей ЛРД.)*** *Пусть модели ЛРД* $\widetilde{M_1} = (SC_1, A_1, \Delta_1)$ *и* $\widetilde{M_2} = (SC_2, A_2, \Delta_2)$ *дают при выполнении операции обобщенного слияния модель ЛРД* $\widetilde{M} = (SC, A, \Delta) = GMerge(\widetilde{M_1}, \widetilde{M_2}, op, op_1, op_2)$ *для некоторых операций* op, op_1, op_2. *Тогда, если* op *— коммутативная бинарная операция над булевыми аргументами, а* $op_1 \equiv op_2$, *то* $\widetilde{M} = GMerge(\widetilde{M_2}, \widetilde{M_1}, op, op_2, op_1)$.

Лемма 2. ***(Об ассоциативности операции обобщенного слияния моделей ЛРД.)*** *Пусть заданы модели ЛРД* $\widetilde{M_i} = (SC_i, A_i, \Delta_i)$, $i = 1, 2, 3$, *причем* $A_1 = A_2 = A_3 = A$. *Пусть при выполнении операции обобщенного слияния результатом являются модели* $\widetilde{M_{1,2}} = (SC_{1,2}, A_{1,2}, \Delta_{1,2}) = GMerge(\widetilde{M_1}, \widetilde{M_2}, op, op_1, op_2)$ *и* $\widetilde{M_{2,3}} = (SC_{2,3}, A_{2,3}, \Delta_{2,3}) = GMerge(\widetilde{M_2}, \widetilde{M_3}, op, op_1, op_2)$ *для некоторых булевых операций* op, op_1 *и* op_2. *Пусть* op *— логическое «И» или логическое «ИЛИ». Тогда* $M_{1,(2,3)} = GMerge(\widetilde{M_1}, \widetilde{M_{2,3}}, op, op_1, op_2) = GMerge(\widetilde{M_{1,2}}, \widetilde{M_3}, op, op_1, op_2) = M_{(1,2),3}$.

С использованием результатов лемм 1 и 2 автором доказана теорема о порядке выполнения операций обобщенного слияния.

Теорема 1. ***(О порядке применения операции обобщенного слияния моделей ЛРД.)*** *Пусть заданы модели ЛРД* $\widetilde{M}_i = (SC_i, A_i, \Delta_i)$, $i = 1, \ldots, k$, *причем* $A_1 = \ldots = A_k = A$. *Пусть* op — *логическое «И» или логическое «ИЛИ». Тогда при выполнении операций обобщенного слияния над моделями* $\widetilde{M}_i$ *попарно, вплоть до получения одной итоговой модели ЛРД, результат не зависит от порядка выполнения таких операций.*

Другой операцией объединения моделей ЛРД, определяемой автором в главе 3, является операция «связывания» таких моделей.

Определение 9. Пусть заданы модели ЛРД $\widetilde{M}_1 = (SC_1, A_1, \Delta_1)$ и $\widetilde{M}_2 = (SC_2, A_2, \Delta_2)$, а также заданы следующие множества и предикаты:

- $A'_{1\to2} = \left\{a_i^{(1\to2)},\ i = 1, \ldots, n_{1\to2}\right\}$ — множество типов доступа от сущностей модели $\widetilde{M}_1$ к сущностям модели $\widetilde{M}_2$;
- $A'_{2\to1} = \left\{a_i^{(2\to1)},\ i = 1, \ldots, n_{2\to1}\right\}$ — множество типов доступа от сущностей модели $\widetilde{M}_2$ к сущностям модели $\widetilde{M}_1$;
- $\Delta'_{1\to2}$ — предикат над множеством $SC_1 \times SC_2 \times A'_{1\to2}$, задающий правила разграничения доступа от сущностей модели $\widetilde{M}_1$ к сущностям модели $\widetilde{M}_2$;
- $\Delta'_{2\to1}$ — предикат над множеством $SC_2 \times SC_1 \times A'_{2\to1}$, задающий правила разграничения доступа от сущностей модели $\widetilde{M}_2$ к сущностям модели $\widetilde{M}_1$.

Назовем модель ЛРД $\widetilde{M}_{1\leftrightarrow2} = (SC_{1\leftrightarrow2}, A_{1\leftrightarrow2}, \Delta_{1\leftrightarrow2})$ *результатом связывания моделей ЛРД* $\widetilde{M}_1$ *и* $\widetilde{M}_2$ (введем обозначение: $\widetilde{M}_{1\leftrightarrow2} = Link(\widetilde{M}_1, \widetilde{M}_2, A'_{1\to2}, A'_{2\to1}, \Delta'_{1\to2}, \Delta'_{2\to1})$), если выполняются следующие условия:

$$SC_{1\leftrightarrow2} = SC_1 \sqcup SC_2;\ A_{1\leftrightarrow2} = A_1 \cup A_2 \cup A'_{1\to2} \cup A'_{2\to1}; \tag{12}$$

$$\Delta_{1\leftrightarrow2}(sc_1, sc_2, a) = \begin{cases} \Delta_1(sc_1, sc_2, a), & \text{если } sc_1 \in SC_1, sc_2 \in SC_1, a \in A_1, \\ \text{ложь}, & \text{если } sc_1 \in SC_1, sc_2 \in SC_1, a \in A_{1\leftrightarrow2} \setminus A_1, \\ \Delta_2(sc_1, sc_2, a), & \text{если } sc_1 \in SC_2, sc_2 \in SC_2, a \in A_2, \\ \text{ложь}, & \text{если } sc_1 \in SC_2, sc_2 \in SC_2, a \in A_{1\leftrightarrow2} \setminus A_2, \\ \Delta'_{1\to2}(sc_1, sc_2, a), & \text{если } sc_1 \in SC_1, sc_2 \in SC_2, a \in A'_{1\to2}, \\ \text{ложь}, & \text{если } sc_1 \in SC_1, sc_2 \in SC_2, a \in A_{1\leftrightarrow2} \setminus A'_{1\to2}, \\ \Delta'_{2\to1}(sc_1, sc_2, a), & \text{если } sc_1 \in SC_2, sc_2 \in SC_1, a \in A'_{2\to1}, \\ \text{ложь}, & \text{если } sc_1 \in SC_2, sc_2 \in SC_1, a \in A_{1\leftrightarrow2} \setminus A'_{2\to1}. \end{cases} \tag{13}$$

Автором сформулированы в виде вспомогательных лемм и доказаны два свойства операции связывания моделей ЛРД.

Лемма 3. ***(О коммутативности операции связывания моделей ЛРД.)*** *Пусть модели ЛРД* $\widetilde{M}_1 = (SC_1, A_1, \Delta_1)$ *и* $\widetilde{M}_2 = (SC_2, A_2, \Delta_2)$ *при выполнении операции связывания позволяют получить модель ЛРД* $\widetilde{M}_{1\leftrightarrow2} = (SC_{1\leftrightarrow2}, A_{1\leftrightarrow2}, \Delta_{1\leftrightarrow2}) = Link(\widetilde{M}_1, \widetilde{M}_2, A'_{1\to2}, A'_{2\to1}, \Delta'_{1\to2}, \Delta'_{2\to1})$, *где множества* $A'_{1\to2}$, $A'_{2\to1}$ *и предикаты* $\Delta'_{1\to2}$, $\Delta'_{2\to1}$ *удовлетворяют определению 9. Тогда*

$\widetilde{M}_{1\leftrightarrow 2} = Link(\widetilde{M}_2,\ \widetilde{M}_1,\ A'_{2\to 1},\ A'_{1\to 2},\ \Delta''_{2\to 1},\ \Delta''_{1\to 2})$, *где* $\Delta''_{j\to i}(sc_2, sc_1, a) = \Delta'_{i\to j}(sc_1, sc_2, a)$, $(i, j) \in \{(1, 2),\ (2, 1)\}$.

Лемма 4. ***(Об ассоциативности операции связывания моделей ЛРД.)*** *Пусть модели ЛРД* $\widetilde{M}_i = (SC_i, A_i, \Delta_i)$, $i = 1, 2, 3$ *при выполнении операции связывания приводят к модели ЛРД* $\widetilde{M}_{1\leftrightarrow 2} = Link(\widetilde{M}_1,\ \widetilde{M}_2,\ A'_{1\to 2},\ A'_{2\to 1},\ \Delta'_{1\to 2},\ \Delta'_{2\to 1}) = (SC_{1\leftrightarrow 2},\ A_{1\leftrightarrow 2},\ \Delta_{1\leftrightarrow 2})$ *и* $\widetilde{M}_{2\leftrightarrow 3} = Link(\widetilde{M}_2,\ \widetilde{M}_3,\ A'_{2\to 3},\ A'_{3\to 2},\ \Delta'_{2\to 3},\ \Delta'_{3\to 2}) = (SC_{2\leftrightarrow 3},\ A_{2\leftrightarrow 3},\ \Delta_{2\leftrightarrow 3})$. *Тогда, если* $\widetilde{M}_{1\leftrightarrow(2\leftrightarrow 3)} = Link(\widetilde{M}_{(2\leftrightarrow 3)},\ \widetilde{M}_1,\ A'_{1\to(2\leftrightarrow 3)},\ A'_{(2\leftrightarrow 3)\to 1},\ \Delta'_{1\to(2\leftrightarrow 3)},\ \Delta'_{(2\leftrightarrow 3)\to 1})$, *то* $\widetilde{M}_{1\leftrightarrow(2\leftrightarrow 3)} = \widetilde{M}_{(1\leftrightarrow 2)\leftrightarrow 3} = (SC_{(1\leftrightarrow 2)\leftrightarrow 3},\ A_{(1\leftrightarrow 2)\leftrightarrow 3},\ \Delta_{(1\leftrightarrow 2)\leftrightarrow 3}) = Link(\widetilde{M}_{(1\leftrightarrow 2)},\ \widetilde{M}_3,\ A'_{(1\leftrightarrow 2)\to 3},\ A'_{3\to(1\leftrightarrow 2)},\ \Delta'_{(1\leftrightarrow 2)\to 3},\ \Delta'_{3\to(1\leftrightarrow 2)})$, *причем предикаты* $\Delta'_{(1\leftrightarrow 2)\to 3},\ \Delta'_{3\to(1\leftrightarrow 2)}$ *определяются однозначным образом.*

На основе результатов лемм 3 и 4 автором доказана теорема о порядке выполнения операций связывания моделей ЛРД.

Теорема 2. ***(О порядке применения операции связывания моделей ЛРД.)*** *Пусть заданы модели ЛРД* $\widetilde{M}_i = (SC_i, A_i, \Delta_i)$, $i = 1, \ldots, k$. *Тогда при выполнении операций связывания над моделями* $\widetilde{M}_i$ *попарно, вплоть до получения одной итоговой модели ЛРД, результат не зависит от порядка выполнения таких операций.*

Рассмотренные операции обобщенного слияния и связывания моделей ЛРД согласно теоремам о порядке применения таких операций позволяют производить объединение нескольких моделей ЛРД, которые реализуются в исследуемой автоматизированной системе с помощью различных механизмов защиты. Результаты такого объединения по построению являются моделями ЛРД, а значит к ним тоже, при определенных условиях могут быть применены указанные операции. Автором доказана следующая теорема, являющаяся базовой для созданного метода согласования моделей ЛРД.

Теорема 3. *Пусть задано множество моделей ЛРД* $\mathcal{M}_0 = \{\widetilde{M}_i = (SC_i, A, \Delta_i)\}$, $i = 1, \ldots, k$ *с одинаковыми множествами типов доступа. Пусть множество* $\mathcal{M}_{i+1}$ *строится по множеству* $\mathcal{M}_i$, $i \geqslant 0$ *следующим образом:*

(1) производится выбор множества из $m \geqslant 2$ *моделей* $\mathcal{M}'_i = \{\widetilde{M}_{j_1}, \ldots, \widetilde{M}_{j_m}\} \subset \mathcal{M}_i$;

(2) к множеству $\mathcal{M}'_i$ *применяется операция обобщенного слияния с использованием бинарной булевой операции «И» или «ИЛИ», либо операция связывания, в результате получается модель ЛРД* $\widetilde{M}'_i$;

(3) строится искомое множество $\mathcal{M}_{i+1} = (\mathcal{M}_i \setminus \mathcal{M}'_i) \cup \{\widetilde{M}'_i\}$.

Тогда для некоторого i_0, $1 \leqslant i_0 < k$ *множество моделей ЛРД* $\mathcal{M}_{i_0}$ *будем содержать ровно одну модель ЛРД.*

Замечание. Выбор множества $\mathcal{M}'_i$ на шаге (1) целесообразно осуществлять таким образом, что выполняется одно из следующих двух свойств:

- модели ЛРД из $\mathcal{M}'_i$ действуют над пересекающимися (например, полностью совпадающими) множествами субъектов и объектов доступа;
- модели ЛРД из $\mathcal{M}'_i$ полностью независимы по субъектам и объектам доступа.

Первый случай характерен для объединения результатов одновременного использования нескольких механизмов ЛРД над одними и теми же множествами субъектов и объектов доступа. В качестве примера такого случая следует отметить совместное использование модели Type Enforcement и традиционной модели прав доступа Unix-подобных ОС в механизмах защиты SELinux. В этом случае производится операция обобщенного слияния. Второй случай возникает при одновременном использовании не связанных явным образом моделей ЛРД, например, в операционной системе и в программном сервисе, работающем под управлением этой ОС. В таком случае представляется целесообразным использование операции связывания.

Разработанный автором метод согласования моделей ЛРД используется как необходимый подготовительный шаг при исследовании свойств таких моделей, которые реализуются с использованием механизмов ядра ОС Linux, а также — механизмов ЛРД в прикладных программах. Использование предложенного метода согласования позволяет корректным образом объединить используемые разнородные модели и, тем самым, расширить класс проверяемых свойств безопасности.

В главе 4 рассматривается оригинальный метод спецификации и проверки свойств моделей логического разграничения доступа. Метод основан на использовании алгоритмов теории графов и технологии «верификации на модели» («model checking»). Отмечаются особенности его применения на практике.

Основной областью применения предлагаемого автором метода к спецификации и проверке свойств в моделях ЛРД является исследование свойств безопасности таких моделей, которые используются в современных Unix-подобных операционных системах. Применение разрабатываемого метода не ограничивается указанной областью и расширяется на задачи проверки других моделей логического разграничения доступа. Такое расширение может быть произведено с учетом результатов, изложенных в главах 2 и 4. Ключевой особенностью нового метода, отличающего его от других решений в этой области, является возможность учета иерархической структуры на множестве объектов доступа при автоматизированной проверке свойств. Общая задача проверки свойств моделей ЛРД в рамках создаваемого метода ставится следующим образом. В качестве входных данных предоставляются:

- модель ЛРД, правила которой сформулированы с помощью способа унифицированного описания, который предложен автором в главе 2;
- подлежащее проверке свойство или набор свойств, которые заданы на языке спецификации свойств информационных потоков.

В результате проверки необходимо доказать выполнение или невыполнение подлежащих проверке свойств, а в случае невыполнения какого-либо из свойств — предоставить описание контрпримера, а именно — последовательности действий, с помощью которой это свойство может быть нарушено. В предлагаемом методе

процедура доказательства и построение контрпримеров ориентированы на выполнение в автоматизированном режиме.

В качестве базового свойства, на котором демонстрируется применение методов верификации, выбрано следующее требование: при заданных классах сущностей модели E_1, E_2 и E_3 любой информационный поток от сущности из E_1 к сущности из E_2 проходит через одну из сущностей E_3.

Общая схема метода проверки выполнения требований по безопасности представляет следующую последовательность действий:

- сбор данных о конфигурации механизмов ЛРД;
- представление полученных данных в виде формальной модели;
- задание подлежащих проверке свойств на используемом для этих целей языке спецификации;
- проведение проверки выполнения свойств в модели;
- интерпретация результатов с позиции настроек механизмов ЛРД.

В основе предлагаемого метода, а именно — в процессе проведения проверки, используются отмеченные в главе 1 алгоритмы верификации на модели. Такие методы основаны на задании модели как системы переходов между состояниями, для каждого из которых задан набор истинных в нем атомарных высказываний пропозициональной логики (модели Крипке). Проверяемое (анализируемое) свойство специфицируется в виде формулы временной логики, накладывающей ограничения на состояния в путях в заданной системе переходов.

Автором разработаны и представлены в работе:

- способ построения основной модели для проверки, а именно — модели Крипке, состояния которой соответствуют производимым доступам;
- способ спецификации типовых требований безопасности, предъявляемых к моделям ЛРД, на основе линейной временно́й логики;
- два метода проверки выполнения таких требований с использованием специализированных алгоритмов верификации на модели («model checking») и интерпретации полученных результатов.

Автором предложены два метода проверки выполнения заданных требования по безопасности. Первый из них использует в своей основе универсальные средства верификации на модели, такие как NuSMV2. Второй — основан на предлагаемом автором специализированном алгоритме проверки, который использует методы теории графов. Применение универсальных средств верификации на модели, как правило, является вычислительно трудоемким процессом по причине того, что класс свойств, которые могут быть проверены с помощью таких средств, достаточно широк. В таком контексте целесообразной представляется разработка специализированных алгоритмов, предоставляющих возможность проверить в исследуемой модели ЛРД более узкий класс свойств, вместе с тем позволяющих сделать процесс такой проверки более эффективным. Опишем предлагаемый автором алгоритм проверки свойств о прохождении информационного потока. Отметим, что проверка такого свойства может быть осуществлена с использованием алгоритмов на графе доступов, включая традиционные алгоритмы вычисления возможности доступа в классической модели «take-grant» и ее расширенном ва-

рианте,[6] а также с использованием современных методов исследования графа доступов.[7] Предлагаемый автором алгоритм формулируется в рамках способа унифицированного описания моделей ЛРД и ориентирован на проверку требований безопасности к тем моделям ЛРД, которые используются в Unix-подобных ОС.

Определение 10. Пусть задана модель ЛРД $\widetilde{M} = (SC, A, \Delta)$. Назовем *состоянием системы переходов* тройку sc_1, sc_2, a, где $sc_1, sc_2 \in SC$, $a \in A$. *Корректным* состоянием системы переходов назовем такое состояние, для которого истинен предикат $\Delta(sc_1, sc_2, a)$, если a является доступом на запись, либо истинен предикат $\Delta(sc_2, sc_1, a)$, если a является доступом на чтение.

Пусть на множестве всех корректных состояний (обозначим его через S) задано отношение R такое, что

$$(s_\alpha = (sc_{\alpha,1}, sc_{\alpha,2}, a_\alpha), s_b = (sc_{\beta,1}, sc_{\beta,2}, a_\beta)) \in R \iff sc_{\alpha,2} = sc_{\beta,1}.$$

Пусть требуется проверить свойство, что любой информационный поток от множества контекстов безопасности $E_1 \subset SC$ к множеству $E_2 \subset SC$ проходит через множество контекстов безопасности $E_3 \subset SC$. Предлагаемый алгоритм проверки состоит в выполнении следующих шагов:

(0) $\mathcal{F} := \{(s, None) : \ s = (sc_1, sc_2, a) \in S, sc_1 \in E_1\}$;
(1) $\mathcal{V} := \varnothing$;
(2) пока $|\mathcal{F}| \neq \varnothing$, выполнять шаги (3)–(7):
(3) выбрать $f \in \mathcal{F}$, $f = (s_1, s_0)$, $s_1 = (sc_1, sc_2, a)$, $\mathcal{F} := \mathcal{F} \setminus \{f\}$;
(4) если $sc_2 \in E_3$, то перейти к шагу (2);
(5) если $\{(s_\alpha, s_\beta) \in \mathcal{V} : \ s_\alpha = s_1\} = \varnothing$, то $\mathcal{V} := \mathcal{V} \cup \{(s_1, s_0)\}$;
(6) если $sc_2 \in E_2$, то выйти с возвращаемым значением $(\mathcal{V}, f)$;
(7) $\mathcal{F} := \mathcal{F} \cup \{(sc_\alpha, sc_\beta) : \ (sc_1, sc_\alpha) \in R\}$;
(8) выйти из алгоритма с возвращаемым значением $(\mathcal{V}, None)$.

Такой алгоритм является модификацией алгоритма поиска «в глубину» в графе, который задается множеством вершин S и отношением инцидентности R. По причине конечности множеств S и R алгоритм всегда завершает свою работу. Возвращаемое значение алгоритма, а именно — пара $(\mathcal{V}, f)$, содержит последовательность состояний системы переходов, на которой не выполняется проверяемое свойство прохождения информационных потоков. В случае, если рассматриваемое свойство выполняется в исследуемой модели ЛРД, $f = None$. Если $f \neq None$,

[6] M. Harrison, W. Ruzzo, J. Ullman. Protection in Operating Systems. // Communications of the ACM. — 1976. — № 19(8). — pp. 461–471.

A. Jones, R. Lipton, L. Snyder. A Linear Time Algorithm for Deciding Security. // Proc. 17th Annual Symp. on the Foundations of Computer Science. — 1976. — pp. 33–41.

J. Frank, M. Bishop. Extending the Take-Grant Protection System. — Department of Computer Science. — University of California at Davis. — 1996.

[7] П. Н. Девянин. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. — М.: Радио и связь, 2006. — 176 с.

Д. Н. Колегов. Применение ДП-моделей для анализа защищенности сетей. // Прикладная и дискретная математика. — 2008. — № 1. — 71–87.

то f содержит состояние системы переходов, в котором реализуется последний элементарный информационный поток. Множество $\mathcal{V}$ содержит пары (s_1, s_0), для которых выполняется свойство $(s_0, s_1) \in R$. Таким образом, по значению f и парам $(s_1, s_0) \in \mathcal{V}$ может быть восстановлена последовательность операций, приводящих в исследуемой модели ЛРД нарушения подлежащего проверке свойства.

В главе 5 излагаются предложенный автором способ реализации программного комплекса средств для исследования моделей логического разграничения доступа на предмет выполнения требований по безопасности. Назначением разрабатываемого программного комплекса является анализ выполнения требований безопасности (свойств), которые формулируются в виде ограничений на информационные потоки в моделях логического разграничения доступа. Комплекс предназначен для определения того факта, выполняется ли заданное свойство из указанного класса в модели ЛРД, построенной на основе сбора данных о конфигурации механизмов ЛРД. Комплекс ориентирован на исследование конфигурации таких механизмов в Unix-подобных операционных системах на основе ядра ОС Linux.

Программный комплекс состоит из следующих компонентов (рис. 2):

- средства сбора данных о настройках механизмов ЛРД и преобразования таких настроек механизмов ЛРД во внутреннее представление моделей ЛРД;
- генераторы внутреннего представления моделей ЛРД;
- средство согласования моделей ЛРД;
- средства проверки свойств в моделях ЛРД;
- средства интерпретации результатов проверки.

Средства сбора данных организуют взаимодействие с исследуемыми механизмами ЛРД и производят считывание их конфигурации. Процедуры преобразования настроек механизмов ЛРД во внутреннее представление, реализованные в таких средствах, являются адаптером, позволяющим единообразно использовать модели ЛРД в рассматриваемом комплексе. Средства проверки свойств в моделях ЛРД реализуют метод проверки, представленный в главе 5. Входными данными является внутреннее представление модели ЛРД, а также набор спецификаций свойств для проверки, полученных от пользователя программного комплекса. Результатом являются структурированные данные об истинности либо ложности каждого из проверяемых свойств, а также дополнительная информация, включая описания последовательностей действий, которые демонстрируют невыполнение свойств в исследуемой модели ЛРД. Одно из средств проверки использует универсальное средство верификации на модели NuSMV2, другое — программу, реализующую предложенный автором специализированный алгоритм проверки.

По результатам тестовых испытаний на экспериментальном полигоне демонстрируется возможность применения на практике созданных инструментальных средств для исследования свойств безопасности дистрибутивов ОС Linux, а именно — анализа информационных потоков, задаваемых настройками механизмов логического разграничения доступа. В качестве полигона для тестирования используется дистрибутив операционной системы на основе ядра ОС Linux и набора программного обеспечения с открытым исходным кодом. На полигоне для тестирования используются (в том числе — совместно) только традиционные механизмы

Рис. 2. Схема взаимодействия компонентов программного комплекса для исследования моделей логического разграничения доступа на предмет выполнения требований по безопасности.

разграничения доступа в Unix-подобных ОС и механизмы SELinux, реализующие модель Type Enforcement. Дистрибутив ОС обладает программными средствами и библиотеками, необходимыми для сбора данных о настройках механизмов ЛРД, а в процессе сбора данных о настройках механизмов ЛРД, их изменение не производится. Состав такого дистрибутива расширяется за счет добавления веб-сервера и работающей поверх него веб-системы управления контентом. Механизмы защиты веб-системы реализуют отдельную модель ЛРД, не связанную с моделями ЛРД, которые выполняются непосредственно механизмами операционной системы. В качестве такой модели выбрана модель ЛРД класса $RBAC_0$.

Автором предложена программа тестовых испытаний разработанного прототипа программного комплекса для проверки выполнения требований в моделях ЛРД. Содержание такой программы испытаний составляет решение следующих задач:

- проверка выполнения требования изоляции пользователей при использова-

нии традиционных средств разграничения доступа в Unix-подобных ОС;
- проверка выполнения требования изоляции сервисов в комбинированной модели ЛРД;
- проверка выполнения требования ограничения доступа к средствам управления настройками механизмов ЛРД при использовании комбинированной модели ЛРД;
- проверка выполнения требования изоляции пользователей веб-системы управления контентом.

В рамках решения перечисленных задач проверяются случаи корректной и некорректной настройки механизмов ЛРД. Оценивается время выполнения такой проверки для нескольких вариантов задания настроек подлежащих анализу механизмов ЛРД. Для моделей, исследуемых в рамках тестовых испытаний, предложен способ их параметризации. Для ряда значений количественных параметров, которые определяют анализируемые модели, произведено измерение времени работы универсального и специализированного алгоритмов проверки. Получена оценка эффективности алгоритмов и средств проверки выполнения требований безопасности в автоматизированных системах с большим числом субъектов и объектов доступа. Результаты тестовых испытаний демонстрируют возможность практического применения разработанных методов и средств проверки выполнения требований по безопасности в моделях ЛРД.

В заключении диссертационной работы перечисляются ее основные результаты.

- На основе систематизации и анализа современных программных механизмов и формальных моделей логического разграничения доступа, которые они реализуют, методов их спецификации и анализа на предмет соответствия принятым требованиям безопасности, автором разработаны и сформулированы способы формального описания таких моделей для достаточно широкого класса компьютерных систем, в первую очередь — для систем на базе ядра ОС Linux.
- Сформулированы и доказательно обоснованы положения нового способа объединения и согласования математических моделей логического разграничения доступа, с помощью которого можно исследовать совместно используемые механизмы ЛРД в компьютерных системах, разрабатываемых на основе Unix-подобных операционных систем.
- Предложен корректный способ спецификации и анализа свойств моделей логического разграничения доступа, с помощью которого может быть проверено выполнение ограничений на информационные потоки в компьютерной системе.
- Предложено и прошло тестовые испытания математическое и программное обеспечение, составляющее основу комплекса средств для анализа моделей логического разграничения доступа, которые реализуются механизмами ЛРД в Unix-подобных ОС, на предмет выполнения ими требований по безопасности, а именно — ограничений на допустимые информационные потоки.

Автор выражает глубокую благодарность своему научному руководителю доктору физико-математических наук, профессору Валерию Александровичу Васенину за постановку задач и постоянное внимание к работе.

Публикации по теме диссертации

[1] **К. А. Шапченко. Способ проверки свойств безопасности в моделях логического разграничения доступа с древовидной иерархией объектов доступа. // Информационные технологии. — М.: Новые технологии. — 2009. — №10. — С. 13–17.**

[2] **В. А. Васенин, К. А. Шапченко. Проблемы управления персональными данными. // Открытые системы. — М.: «Открытые системы». — 2009. — № 9. — С. 42–45. (К. А. Шапченко принадлежат результаты по систематизации подходов к использованию программно-технических средств защиты).**

[3] **Ф. М. Пучков, К. А. Шапченко. Статический метод анализа программного обеспечения на наличие угроз переполнения буферов. // Программирование. — М.: «Pleiades Publishing» — 2005.— № 4. — С. 19–34. (К. А. Шапченко принадлежат результаты по подготовке программ к исследованию на предмет наличия ошибок вида «переполнение буфера»).**

[4] К. А. Шапченко. К вопросу о средствах ОС Linux для управления доступом при использовании ролевых политик безопасности. // Математика и безопасность информационных технологий. Материалы конференции в МГУ 2–3 ноября 2005 г., — М.: МЦНМО. — 2006. — С. 257–281.

[5] Набор специализированных дистрибутивов ОС Linux с повышенными требованиями к защищенности. / В. А. Васенин, К. А. Шапченко, А. Н. Водомеров, А. В. Инюхин, О. О. Андреев, В. Б. Савкин. // Свидетельство о государственной регистрации программы для ЭВМ № 2006613706. — 2006.

[6] В. А. Васенин, К. А. Шапченко, О. О. Андреев. Математические модели и механизмы логического разграничения доступа в операционной системе Linux: текущее состояние и перспективы развития. // Материалы Второй международной научной конференции по проблемам безопасности и противодействия терроризму. Пятая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-06). МГУ имени М. В. Ломоносова, 25–26 октября 2006 г. — М.: МЦНМО. — 2007. — С. 159–171. (К. А. Шапченко принадлежат результаты по исследованию и разработке методов проверки выполнения требований по безопасности в настройках механизмов логического разграничения доступа).

[7] Ф. М. Пучков, К. А. Шапченко, О. О. Андреев. К созданию автоматизированных средств верификации программного кода. // Материалы Второй международной научной конференции по проблемам безопасности и противодействия терроризму. Пятая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-06). МГУ

имени М. В. Ломоносова, 25–26 октября 2006 г. — М.: МЦНМО. — 2007. — С. 401-439. (К. А. Шапченко принадлежат результаты по подготовке программ к исследованию на предмет наличия ошибок вида «переполнение буфера»).

[8] К. А. Шапченко, О. О. Андреев, В. Б. Савкин, А. А. Иткес. Специализированные дистрибутивы операционной системы Linux с повышенным уровнем защищенности. // Критически важные объекты и кибертерроризм. Часть 2. Аспекты программной реализации средств противодействия. / О. О. Андреев и др. Под ред. В. А. Васенина. — М.: МЦНМО. — 2008. — 607 с. — С. 168–216. (К. А. Шапченко принадлежат доказательства теорем о представлении одной модели ЛРД через другую, а также результаты по исследованию и разработке методов проверки выполнения требований по безопасности в настройках механизмов логического разграничения доступа).

[9] К. А. Шапченко, О. О. Андреев. Подход к управлению настройками механизмов безопасности в дистрибутивах ОС Linux. // Материалы Четвертой международной научной конференции по проблемам безопасности и противодействия терроризму. Московский государственный университет им. М. В. Ломоносова. 30–31 октября 2008 г. Том 2. Материалы Седьмой общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2008). — М.: МЦНМО. — 2009. — С. 153–160. (К. А. Шапченко принадлежит подход к интеграции методов проверки выполнения требований по безопасности в настройках механизмов ЛРД в процессы проектирования и эксплуатации дистрибутивов операционных систем).

[10] К. А. Шапченко. Современные методы проверки свойств безопасности в моделях логического разграничения доступа. // Проблемы информатики. — Новосибирск: НГТУ. — 2009. — № 3. — С. 22–32.

[11] Способ генерации баз данных для систем верификации программного обеспечения распределенных вычислительных комплексов и устройство для его реализации. / Ф. М. Пучков, К. А. Шапченко. // Патент на изобретение № 2364929. — 2009.

[12] Способ генерации баз знаний для систем верификации программного обеспечения распределенных вычислительных комплексов и устройство для его реализации. / Ф. М. Пучков, К. А. Шапченко. // Патент на изобретение № 2364930. — 2009.

[13] Способ генерации баз данных и баз знаний для систем верификации программного обеспечения распределенных вычислительных комплексов и устройство для его реализации. / Ф. М. Пучков, К. А. Шапченко. // Патент на изобретение № 2373569. — 2009.

[14] Способ верификации программного обеспечения распределенных вычислительных комплексов и система для его реализации. / Ф. М. Пучков, К. А. Шапченко. // Патент на изобретение № 2373570. — 2009.