На правах рукописи

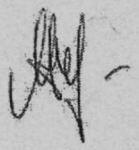
БИКТИМИРОВ МАРАТ РАМИЛЕВИЧ

Модели управления доступом в распределенных компьютерных системах

05.13.18 – Математическое моделирование, численные методы и комплексы программ

05.13.01 – Системный анализ, управление и обработка информации

Автореферат
диссертации на соискание ученой степени
кандидата технических наук



Казань, 2008

Работа выполнена в Казанском государственном техническом университете им. А. Н. Туполева

Научные руководители: доктор физ.-мат. наук, профессор, заслуженный деятель науки РТ
Елизаров Александр Михайлович;

доктор технических наук
Сиразетдинов Рифкат Талгатович

Официальные оппоненты: доктор физ.-мат. наук, профессор
Сотников Александр Николаевич;

доктор технических наук, профессор, заслуженный деятель науки и техники РТ
Песошин Валерий Андреевич

Ведущая организация: Институт системного программирования Российской академии наук (г. Москва)

Защита состоится «31» октября 2008 года в 13-00 часов на заседании Диссертационного совета Д 212.079.01 в Казанском государственном техническом университете им. А. Н. Туполева по адресу: 420111, Казань, ул. К. Маркса, д. 10

С диссертацией можно ознакомиться в научной библиотеке Казанского государственного технического университета им. А. Н. Туполева

Автореферат разослан «29» сентября 2008 г.

Ученый секретарь Диссертационного совета
доктор физ.-мат. наук, профессор П. Г. Данилаев

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. В настоящее время при проектировании и эксплуатации компьютерных систем (КС) различного назначения проблемы обеспечения информационной безопасности стали играть ключевую роль. Практика показала, что наиболее важными являются две задачи – обеспечение управления доступом в информационно-телекоммуникационных системах (ИТС) и учет влияния распределенности ресурсов и инфраструктуры ИТС. Управление доступом должно учитывать, с одной стороны, как наличие штатных средств реализации (механизмы, встроенные в операционные среды и прикладные системы), так и наличие различных уровней управления – персональный, корпоративный, региональный и федеральный. Проблема распределенности заключается в том, что интеграция различных коммуникационных и информационных ресурсов порождает проблемы как с управляемостью системы (включая компоненту информационной безопасности), так и с корректным формулированием и реализацией различных политик безопасности (ПБ). Однако уровень готовности к теоретическим и практическим решениям проблем безопасности далек от желаемого. В методологии проектирования систем безопасности основной проблемой является отсутствие единого обоснованного подхода к разработке и эксплуатации защищенных компьютерных систем. Достаточное поверхностное внимание уделяется проектированию и реализации процедур управления доступом к информации. Весьма важной проблемой является также серьезное отставание методов и моделей проектирования средств защиты информации и управления доступом к ней от достижений современных сетевых информационных технологий, практически доступных широкому кругу пользователей.

При разработке сложных систем обеспечения информационной безопасности основную роль играет так называемая модель управления доступом. В англоязычной литературе для обозначения сходного понятия используются термины «security model» (модель безопасности) и «security policy model» (модель политики безопасности). Эта модель определяет правила управления доступом к информации, потоки информации, разрешенные в системе таким образом, чтобы система всегда была безопасной. Целью построения модели управления доступом является выражение сути требований по безопасности к данной системе. Модель позволяет провести анализ свойств системы, но не накладывает ограничений на реализацию тех или иных механизмов защиты. Так как модель является формальной, возможно осуществить доказательство различных свойств безопасности всей системы. [1]

Таким образом, тема диссертационной работы является актуальной и непосредственно связана с глобальной проблемой управления техническим циклом жизни программно-технических изделий (в данном случае относящихся к обеспечению информационной безопасности).

Целью диссертации является разработка моделей управления доступом в распределенных компьютерных системах и их апробация в распределенных корпоративных

---

[1] Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. – М.: МИФИ, 1995. – 86 с.

сетях регионального уровня. Для достижения поставленной цели необходимо провести:

- уточнение моделей взаимодействия элементов КС с учетом механизма порождения и взаимовлияния субъектов;
- системный анализ процедур создания, эксплуатации и управления системой безопасности ИТС применительно к реальному жизненному циклу КС;
- формулирование и обоснование алгоритмов управления доступом и механизмами обеспечения безопасности КС;
- уточнение политик безопасности при проектировании механизмов защиты распределенных сетей.

Основной ***задачей*** диссертации является совершенствование методов управления доступом в компьютерных системах для решения задач в области математического моделирования, системного анализа, оптимизации, управления и обработки информации, а также разработки проблемно-ориентированных систем управления.

Методология исследования базируется на системно-концептуальном подходе к обеспечению безопасности и уточняет его, исходя из методологии достаточных условий. В работе использованы материалы справочного характера, описывающие работу конкретных компонент КС, отдельные механизмы обеспечения безопасности и протоколы взаимодействия КС. Диссертация опирается также на результаты В. А. Герасименко, А. А. Грушо, Е. Е. Тимониной, С. П. Расторгуева, А. Ю. Щербакова и др.

Положения, выносимые на защиту:

1. Решение задачи управления доступом в распределенных компьютерных системах и апробация полученных результатов для распределенных корпоративных сетей регионального уровня, включающие:

- уточнение модели субъектно-объектного взаимодействия в ИТС;
- доказательство достаточных условий выполнения произвольной ПБ в КС при управлении системой безопасности ИТС;
- конструктивную коррекцию ПБ при проектировании системы безопасности для сетевых сред;
- модели и алгоритмы управления доступом в распределенных КС, обеспечивающие работоспособность сложных программных комплексов и гарантирующие выполнение заданной при проектировании ПБ.

2. Теоретические и экспериментальные результаты создания подсистем безопасности ИТС, включающие:

- классификации механизмов безопасности в рамках сформулированных алгоритмов управления, в том числе механизмов обеспечения безопасности сетевого взаимодействия;
- рекомендации и требования к применению средств, реализующих корректное управление;
- описание программно-технических решений, реализующих предложенные алгоритмы.

Научная новизна

Предлагаемый в работе общий подход состоит в моделировании систем управления доступом КС с точки зрения достаточных условий. Тем самым можно говорить о развитии методологии достаточных условий при проектировании и реализации решений по управлению безопасностью КС. В диссертации получены следующие новые научные результаты:

- уточнены субъектно-ориентированная модель безопасности компьютерной системы и некоторые основные термины, введены новые понятия (ассоциированные объекты, функция порождения субъекта и др.), позволяющие более корректно формулировать и доказывать утверждения, касающиеся свойств механизмов обеспечения безопасности КС в процессе их проектирования;
- сформулированы и доказаны утверждения, описывающие условия выполнения произвольной политики безопасности; разработана методология достаточных условий выполнения произвольной политики безопасности при проектировании КС;
- представлена модель управления механизмами реализации ПБ в распределенной КС; сформулировано понятие корректного управления и обоснованы достаточные условия корректности управления, предложены методы и алгоритмы проектирования систем управления доступом, обеспечивающие, с одной стороны, корректность управления, а с другой, – работоспособность сложных программных комплексов;
- уточнена модель взаимодействия локальных и удаленных сегментов КС, показана несостоятельность целого класса политик безопасности, связанных с полным проецированием прав пользователя на доступные ему субъекты; предложена конструктивная коррекция ПБ в сетевых средах при проектировании механизмов безопасности, проведен анализ двух классов защиты от несанкционированного доступа в сетевой среде: межсетевых экранов (МЭ) и локальной защиты; определены критерии классификации механизмов межсетевой защиты с учетом коррекций ПБ и механизмов генерации изолированной программной среды, могущие служить основой для автоматизированного проектирования средств защиты в распределенной системе.

Достоверность полученных результатов определяется обоснованностью применяемых методов исследования, доказательством сформулированных утверждений и подтверждением универсальности теоретических результатов работы при их использовании в практических приложениях.

Практическая ценность работы состоит в широком спектре ее практических приложений, что свидетельствует об определенной универсальности полученных результатов, применимых для КС различной архитектуры и назначения. В частности, сформулированные теоретические положения работы использованы в совокупности программно-технических решений Научно-производственного предприятия «Фактор-ТС» (технология «Дионис», Универсальная транспортная подсистема (УТП) ЦБ РФ и др.), предназначенных для построения корпоративных систем общего и специального назначения. Результаты работы апробированы при разработке распределенных высокопроизводительных систем обработки информации для решения больших вычислительных задач в таких предметных областях, как гидроаэромеханика, газодинамика,

расчет траекторий ракетно-космической техники, моделирование динамики функционирования и прогнозирования поведения сложных мультипараметрических систем (задачи метеорологии, сейсмологии и т. п.), ядерная физика, квантовая химия, молекулярная биология.

Работа выполнена при поддержке Российского фонда фундаментальных исследований (автор – исполнитель по проектам 01-07-90366-в, 02-07-90047-в, 02-07-90230-в, 03-07-90092-в, 03-07-90264-в; руководитель по проектам 00-07-92000-и, 01-07-90315-в, 02-07-92002-и, 04-07-90221-в, 07-07-00183-а).

Апробация работы. Результаты диссертации по мере их получения докладывались и обсуждались в Центре научных телекоммуникаций и информационных технологий РАН на семинарах Отдела телекоммуникаций (руководитель – чл.-корр. РАН А. Б. Жижченко), на международной научно-методической конференции «Телематика-2000», на 2-й Всероссийской конференции «Информационная безопасность России в условиях глобального информационного общества» (2001 г.), на VIII конференции представителей региональных научно-образовательных сетей «RELARN-2001», на научно-техническом совете НПП «Фактор-ТС» (ноябрь 2006 г.).

В 2003 году международная организация «ComputerWorld Honors Program» удостоила звания Лауреата Программы «A Search for New Heroes» Российскую академию наук за достижения в реализации проекта высокоскоростного доступа к суперкомпьютерным ресурсам для научно-образовательных организаций России, а руководитель проекта член-корреспондент РАН А. Б. Жижченко и координатор проекта М. Р. Биктимиров награждены медалями.

Публикации. Основные результаты исследования опубликованы в двух монографиях (в соавторстве), двух статьях в журнале из списка, рекомендованного ВАК РФ, и в трех статьях из сборников материалов международных и всероссийских конференций. Список публикаций приведен в конце автореферата.

Содержание, структура и объем работы. Диссертационная работа состоит из введения, четырех глав, заключения и списка литературы; содержит 4 таблицы и 14 рисунков. Общий объем диссертации 137 страниц. Библиографический список состоит из 114 наименований работ отечественных и зарубежных авторов.

Автор считает своим приятным долгом выразить глубокую благодарность своим научным руководителям доктору технических наук Р. Т. Сиразетдинову и доктору физ.-мат. наук, профессору А. М. Елизарову за внимательное отношение, ценные и своевременные консультации и рекомендации, а также советнику заместителя председателя ЦБ РФ доктору технических наук А. Ю. Щербакову и Генеральному директору НПП «Фактор-ТС», кандидату технических наук В. В. Яковлеву за дружескую поддержку и идеи по практическому применению результатов проведенной работы.

СОДЕРЖАНИЕ РАБОТЫ

Во ***введении*** кратко описана история исследования проблемы защиты информации в компьютерных системах, обоснована актуальность темы диссертации, сформулированы цели и задачи работы, указаны методологические и методические основы проведенного исследования и отражена научная новизна.

Проблематика защиты информации в компьютерных системах с момента формулирования основных проблем в середине 1970-х годов до современного состояния прошла длительный и во многом противоречивый путь. Первоначально сформулированные проблемы сводились, как правило, к задаче поддержания конфиденциальности в двух аспектах – вопросы криптографической защиты информации в средах передачи и хранения данных и программно-технические вопросы разграничения доступа к данным и ресурсам вычислительных систем. Позднее с появлением тенденции к распределенной обработке информации на лидирующее место вышли проблемы аутентификации взаимодействующих элементов компьютерных систем, а также способы управления криптографическими механизмами в распределенных системах.

В начале 1980-х годов возник ряд моделей защиты, основанных на декомпозиции КС на субъекты и объекты – модели Белла-ЛаПадула, модель Хартсона и т. д.[2] В них ставятся и исследуются вопросы взаимодействия элементов КС с заданными свойствами.

С середины 1980-х годов наметилась тенденция к появлению комплексных решений в области реализации механизмов защиты компьютерных систем.

В 1991 году В. А. Герасименко предложена модель системно-концептуального подхода к безопасности КС, которая описывает методологию анализа и синтеза системы безопасности[1].

В 1996 году в работе А. А. Грушо и Е. Е. Тимониной[3] высказан и обоснован тезис о гарантированной защищенности КС как гарантированному выполнению априорно заданной политики безопасности (ПБ). Настоящая диссертация опирается на основные положения этой работы.

В главе 1 «Реализация и гарантирование политик обеспечения информационной безопасности в компьютерной системе» введены основные понятия, сформулированы и доказаны утверждения и описаны методы, которые являются базовыми для последующего изложения. Тем самым заложена теоретическая и методологическая база работы.

В **§ 1.1** сформулировано понятие ***политики безопасности*** как интегральной характеристики, качественно (или качественно-количественно) описывающей свойства защищаемой системы в терминах, ее характеризующих.

Компьютерная безопасность решает четыре класса взаимосвязанных задач[4]:

- формулирование и изучение политик безопасности;
- реализация политик безопасности;
- гарантирование заданной политики безопасности;
- управление доступом.

---

[2] Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. – М.: Энергоатомиздат, 1994. – Кн. 1 – 400 с., Кн. 2 – 176 с.

[3] Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. – М.: Изд-во «Яхтсмен», 1996. – 192 с.

[4] Davies Donald W., Price Wyn L. Security for Computer Networks (Защита компьютерных сетей). – John Wiley & Sons, 2-е издание, 1989

Определяющей является задача формулирования такой системы гарантий ПБ, которую можно применить к существующим реализациям КС (для конкретных операционных сред, прикладных программных комплексов и т. д.). Основная проблема состоит в формулировании модели взаимодействия элементов КС с требованием более строгого описания воздействия на объекты и с учетом механизма порождения субъектов[5]. Данная модель должна легко проецироваться на архитектуру современных КС и служить основой для формулирования гарантий ПБ.

Субъектно-ориентированная модель безопасности КС – это *модель КС, находящаяся в рамках однозначной декомпозиции КС на субъекты и объекты, рассматривающая ведущую роль субъектов КС как в нарушении безопасности, так и в ее обеспечении, базирующаяся на понятии порождения субъекта и корректности субъектов относительно друг друга.*

В рамках субъектно-ориентированной модели рассмотрены условия гарантий выполнения произвольных политик безопасности.

В **§ 1.2** дано описание модели защищенной КС[6] и сформулировано понятие монитора безопасности. Монитор безопасности объектов (МБО) фактически является механизмом реализации политики безопасности в КС.

Основные введенные понятия – субъектно-ориентированная модель КС и изолированная программная среда (ИПС). Первое из них подчеркивает главенствующую роль субъектов КС как по поддержанию защищенности, так и по нарушению безопасности; второе понятие описывает метод проектирования КС с заданным свойствами (в терминологии защиты – выполнение априорно заданной политики безопасности). Введен также формальный аппарат для описания свойств КС, включающий описание свойств субъектов и их взаимодействия (понятия операции порождения субъектов и их взаимной корректности).

Вывод о возможности конструктивного описания свойств КС в части защищенности на языке межсубъектного взаимодействия и вывод о том, что реализация подходов к проектированию КС с гарантированным выполнением политики безопасности практически возможна, подкреплены доказательствами соответствующих утверждений (**§§ 1.3 – 1.4**). Получены два следующих достаточных условия гарантированного выполнения политики безопасности в КС.

Условие 1. *Монитор безопасности объектов (МБО) разрешает порождение потоков из множества L, если все существующие в системе субъекты абсолютно корректны относительно него и друг друга; где L – подмножество потоков, характеризующих легальный доступ, а N – несанкционированный доступ соответственно.*

Условие 2. *Если в абсолютно изолированной КС существует МБО и порождаемые субъекты абсолютно корректны относительно МБО, а также монитор безо-*

---

[5] Щербаков А. Ю. Методы и модели проектирования средств обеспечения безопасности в распределенных компьютерных системах на основе создания изолированной программной среды// Автореферат дис. … д-ра техн. н. – М., 1997

[6] Герасименко В. А. Основы теории управления качеством информации. – М.: 1989. Деп. в ВИНИТИ. – № 5392-В89

пасности субъектов (МБС) абсолютно корректен относительно МБО, то в такой КС реализуется только доступ, описанный в правилах разграничения доступа.

Доказана

Базовая теорема ИПС. *Если в момент времени t_0 в изолированной КС действует только порождение субъектов с контролем неизменности объекта и существуют потоки от любого субъекта к любому объекту, не противоречащие условию корректности (абсолютной корректности) субъектов, то в любой момент времени $t > t_0$ КС также остается изолированной (абсолютно изолированной).*

Рассмотренная концепция изолированной программной среды является расширением зарубежных подходов к реализации ядра безопасности.

На рис. 1.1 подчеркнута роль монитора безопасности субъектов при порождении субъектов из объектов. Взаимодействие субъектов и объектов при порождении потоков уточнено введением объектов, ассоциированных с субъектом.

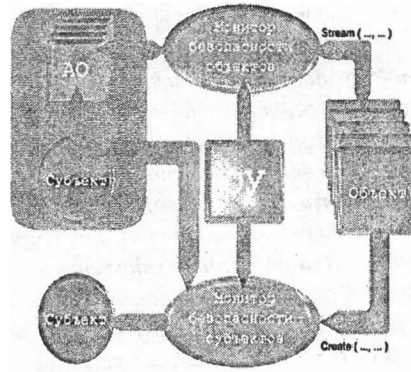


Рис. 1.1. Ядро безопасности с учетом контроля порождения субъектов

Описанный в §1.4 метод проектирования гарантировано защищенной КС – метод генерации ИПС – может быть практически реализован в реальных КС.

Смысл вводимых понятий и формулируемых далее утверждений состоит в задании предопределенной последовательности активизации субъектов КС.

Условие одинакового состояния КС. *Состояние КС в моменты времени t_1 и t_2 (t_1 и t_2 исчисляются для двух отрезков активности КС от нулевых моментов t_{01} и t_{02} ее активизации, например, включения питания аппаратной части) одинаково, если:*

- $t_1 = t_2$;
- *тождественны субъекты $S_t[t_{01}]$ и $S_t[t_{02}]$;*
- *неизменны все объекты из множества O_Z;*
- *неизменна последовательность Z_L;*

где Z_L – последовательность таких пар $(i,j)t$ длины l ($t = 0,1,2,...,l-1$ – моменты времени), что $\textbf{\textit{Create}}(S_i, O_j) \to S_m[t+1]$; S_Z – множество всех субъектов, включенных в Z_L; O_Z – множество всех объектов, включенных в Z_L; R – максимальный уровень представления объекта (фаза стационарного состояния).

С момента времени i наступает стационарная фаза функционирования КС. В этих условиях, а также при попарной корректности субъектов и действии МБС с контролем неизменности объектов-источников на уровне R с момента времени $m > k$ имеет место

Достаточное условие ИПС при ступенчатой загрузке. *При условии неизменности* Z_L *и неизменности объектов из* O_Z *в КС с момента времени установления неизменности* Z_L *и* O_Z *действует изолированная программная среда.*

Обобщенно достаточные условия можно сформулировать следующим утверждением.

Требования к субъектному наполнению изолированной программной среды. *Для того чтобы ИПС поддерживалась в течение всего времени активности КС, достаточно, чтобы в составе программного обеспечения, могущего быть инициированным в ИПС, не было функций порождения субъектов и прекращения их работы, кроме заранее предопределенных при реализации МБС, и не существовало возможностей влияния на среду выполнения любого процесса, а также инициирования потоков к объектам логического уровня менее* R *(под средой выполнения понимается множество ассоциированных объектов).*

Для практики также весьма важен вывод о том, что для генерации ИПС необходимо спроектировать и реализовать контроль запуска задач (порождения процессов) и контроль целостности объектов-источников, совмещенный с чтением реальных данных.

Внедренный в систему субъект может влиять на процесс чтения-записи данных и предъявлять системе контроля некоторые другие данные вместо реально существующих. Однако верно следующее

Достаточное условие чтения реальных данных. *Если субъект, обслуживающий процесс чтения данных (т. е. указанный субъект инициируется запрашивающим данные субъектом и участвует в потоке), содержал только функции тождественного отображения данных на ассоциированные объекты-данные любого субъекта, инициирующего поток чтения, и целостность объекта-источника для этого субъекта зафиксирована, то при его последующей неизменности чтение с использованием порожденного субъекта будет чтением реальных данных.*

Изложенный материал закладывает основы применения методологии достаточных условий к проблеме проектирования защищенной КС.

Необходимо также отметить, что введенная аксиоматика и доказанные на ее основе утверждения имеют значение и для решения более общей проблемы – проектирования КС с произвольными априорно заданными свойствами.

Далее результаты главы 1 использованы при формулировке и доказательстве тех или иных положений.

Глава 2 «Модель управления доступом в распределенной компьютерной системе» посвящена исследованию вопросов управления защитой в КС. Предлагается рассматривать систему управления доступом в едином «пространстве» с общей задачей поддержания гарантий ПБ, с одной стороны (включая единую терминологию и понятия), и, с другой стороны, формулировать процедуру управления так, чтобы не нарушать указанных гарантий.

Математическая модель ПБ рассматривает систему защиты в некотором стационарном состоянии, когда действуют защитные механизмы, а описание разрешенных или неразрешенных действий не меняется. На практике КС проходит путь от отсутствия защиты к полному оснащению защитными механизмами; при этом система управляется, т. е. разрешенные и неразрешенные действия в ней динамически изменяются. Отсюда понятно, что для поддержания гарантий ПБ необходимо рассматривать также управление доступом в КС. При этом процедуры управления должны быть в заданном смысле конструктивны, выполнимы и оптимальны с той или иной точки зрения (например, с точки зрения трудоемкости работы администратора либо с точки зрения объема объектов хранения, описывающих защиту). В рамках декомпозиции КС на субъекты и объекты управление также описывается потоками информации. При этом необходимо комплексно ставить задачу проектировочных и эксплуатационных гарантий, а также гарантий управления. В свою очередь гарантии управления требуют введения некоторых определений (например, понятия «корректного или гарантированного управления»), которые рассмотрены в **§ 2.1**.

В **§ 2.1** введено понятие управляемой КС: *КС называется **управляемой**, если в ней существует субъект (обозначим его Sa – субъект администрирования), для ассоциированных объектов которого существует поток к объекту управления. Компьютерная система называется **корректно управляемой**, если поток к объекту управления существует только для субъекта управления.*

Доказано следующее ***достаточное условие корректного управления в ИПС.*** *Если в КС поддерживается ИПС с контролем неизменности объектов-источников и существует МБО, который разрешает доступ на запись к ОУ только управляющему субъекту, то с момента активизации МБО управление в КС корректно.*

Смысл данного утверждения состоит в том, что условия, описывающие гарантии произвольной политики безопасности, и условия корректного управления как достаточные условия совпадают. Дополнительные требования для корректного управления корректируют политику безопасности КС (в части необходимости доступа на запись к ОУ только субъекта управления).

Важно описать также и условия нарушения корректности управления, которые связаны в ИПС с порождением некоторого произвольного субъекта, который имеет

доступ к ОУ (поток типа «запись»). Поэтому получены следующие ***условия нарушения корректности управления:*** *при существовании ИПС с контролем неизменности объектов-источников и наличии корректного управления нарушение ИПС (как возможность инициирования произвольного субъекта) возможно только при включении в ОУ МБС объекта-источника, порождающего указанный субъект.*

Если ИПС создает эксплуатационные гарантии политики безопасности, то при рассмотрении вопросов управления целесообразно говорить о гарантиях управления, которые описываются как достаточные условия приведенным выше утверждением.

КС с генерацией ИПС и контролем неизменности объектов-источников называется ***корректно управляемой в строгом смысле****, если невозможно размыкание ИПС (появление любого субъекта, не входящего в состав ИПС).*

В подтверждение тезиса о том, что достаточные условия ИПС и корректного управления в строгом смысле совпадают, сформулированы

Следствия:

- *В ИПС, содержащей субъект управления без возможности изменения объекта управления МБС, выполнены условия корректного управления в строгом смысле.*
- *При корректном управлении дополнение корректного субъекта не нарушает ИПС.*

Итак, получены основные условия поддержания ИПС в процессе управления.

Проблема управления доступом (далее – управление) является весьма важной для выполнения ПБ в течение всего времени существования защищенной КС. В рамках введенных выше понятий управление подразумевает изменение объекта (объекта управления, ОУ), хранящего информацию о множестве L в соответствии с текущим состоянием объектов, субъектов и пользователей. Например, возможно либо изменение перечня объектов, доступных какому-либо субъекту, либо изменение во множестве объектов-источников, доступных для порождения субъектов (для ИПС). Иначе говоря, управление доступом в некоторый момент времени описывает политику безопасности применительно к текущему состоянию КС.

Поскольку целью диссертационной работы является разработка единых методов проектирования механизмов выполнения произвольной ПБ, то целесообразно и процесс управления рассматривать в рамках существования субъекта реализации ПБ (МБО) и субъекта гарантирования ПБ (МБС). Очевидно, что управление должно быть организовано таким образом, чтобы ПБ при изменениях в ОУ не нарушалась (т. е. в ОУ не включались бы потоки из множества N).

В **§§ 2.2-2.4** рассмотрены варианты технологий управления доступом для различных архитектур корпоративной системы.

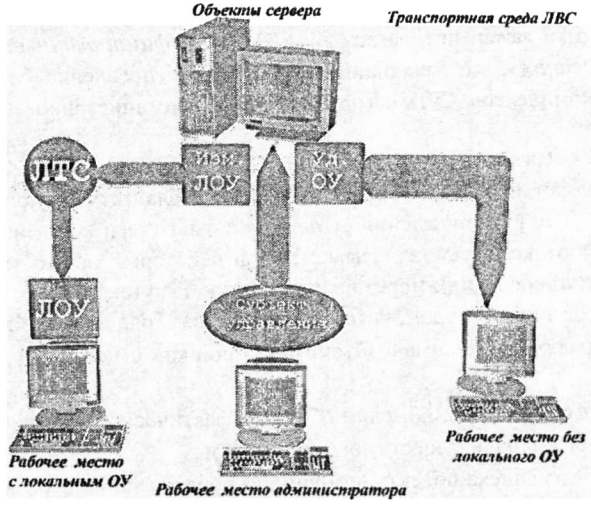


Рис. 2.1. Локализация субъекта и объектов управления в распределенной КС

Технически удобно реализовать работу субъекта управления в рамках другого локального сегмента (ЛС) КС (рабочего места администратора); субъект управления будет создавать ОУ где-либо во внешнем сегменте, доступном субъектам локальной КС.

Необходимым условием для выполнения МБО *заданной политики безопасности в рамках ЛС КС при наличии локальных объектов и выделении во множестве потоков непустого подмножества легальных потоков к локальным объектам является наличие в удаленном ОУ элементов, описывающих потоки между субъектами и локальными объектами.*

Несмотря на то, что данное утверждение является достаточно очевидным, оно, тем не менее, описывает важную техническую проблему, возникающую при управлении МБО и МБС. Она заключается в необходимости доступа к объектам ЛС КС при формировании удаленного ОУ со стороны удаленного управляющего субъекта.

Способ постоянного доступа к объектам ЛС КС требует активности некоторого локального субъекта, управляемого удаленным субъектом администрирования. Основной проблемой в данном случае является возможность управления локальным субъектом со стороны злоумышленника. Уменьшить или заблокировать возможности удаленного злоумышленника (в частности, полностью исключить возможности изменения объектов ЛС КС (доступ на запись)) возможно, если субъект постоянного доступа имеет доступ только на чтение к объектам ЛС КС.

Для обеспечения корректного управления необходимо отсутствие злоумышленных субъектов во всей КС. Достаточным условием для этого является существование ИПС на каждом ЛС КС и наличие МБО, запрещающего доступ к объектам ЛС КС любого субъекта, кроме управляющего.

Для практики важен предлагаемый в **§2.3** ***модифицированный метод «мягкого администрирования»,*** позволяющий организовать управление МБС для сложных программных комплексов. Суть алгоритма мягкого администрирования заключается в следующем.

До установки защитных модулей в КС (имеются в виду МБО и МБС) в программную среду устанавливается субъект, который обладает следующими свойствами: отслеживает все факты порождения субъектов с фиксацией (как минимум) объектов-источников и протоколирует (записывает) их в некоторый объект (исходный список мягкого администрирования). Через некоторый промежуток времени содержимое объекта изучается администратором, который проделывает ряд действий:

- проводит сортировку имен объектов-источников с целью удаления повторяющихся;
- проверяет по указанным именам объектов фактическое их наличие в КС;
- редуцирует имена несуществующих объектов;
- исключает из списка объекты-источники, порождающие субъекты со свойством заведомой некорректности (инструментальные, отладочные средства и т. д.).

После выполнения этих действий администратор получает список объектов-источников, который он может использовать для формирования ОУ МБС. Условием применения модифицированного метода мягкого администрирования является наличие эталонного перечня объектов-источников для некоторого программного пакета.

Ценность метода состоит в том, что администратор безопасности выполняет только операцию редуцирования (сокращения) списков и сравнение функций целостности объектов с эталонными. Возможность применения мягкого администрирования целесообразно предусмотреть еще на этапе проектирования. Применение этого метода позволяет говорить о процессе автоматизации составления правил разграничения доступа (ПРД), что является новым результатом.

Итак, в главе 2 изучены вопросы управления защитой, а именно, формирование и изменение объектов управления для субъектов реализации политики безопасности (МБО) и субъектов гарантий политики безопасности (МБС). Управление описывает методы формирования ОУ, доставки ОУ на локальные сегменты КС, а также методы оперативного изменения ОУ при изменении прав пользователей.

Основным теоретическим выводом этой главы является вывод о том, что условия гарантий ПБ и условия корректного управления как достаточные условия совпадают при доверии администратору (т. е. в том случае, когда администратор не допускает преднамеренных действий по нарушению ПБ). Этот вывод представляется весьма важным для проектирования защищенных систем в целом. Действительно, если придерживаться методологии достаточных условий при реализации заданной ПБ в КС, применяя для этого генерацию ИПС, то корректное управление будет автоматически обеспечиваться (при соответствующей политике безопасности реализации субъекта управления, замкнутого в ИПС).

Основной практический вывод главы состоит в возможности описания моделей и методов формирования объектов управления, учитывающих, с одной стороны, распре-

деленность системы и ставящих целью централизованное управление с рабочего места администратора, и, с другой стороны, удовлетворяющих условиям корректности управления, а в ряде случаев и корректности управления в строгом смысле (без размыкания ИПС).

Изложенный материал представляется весьма важным как для проектирования программно-технических решений по управлению доступом, так и с методологической точки зрения для организации работы администратора с соблюдением реализованной в КС политики безопасности.

В главе 3 «Разработка моделей сетевых сред. Создание механизмов безопасности в распределенной компьютерной системе» рассмотрены весьма важные вопросы, касающиеся зависимости свойств защищенности от распределенности КС.

Выше уже упоминалась проблема распределенности КС с точки зрения влияния на безопасность. В ряде случаев политики безопасности, гарантировано выполняемые для локального подмножества элементов КС, несостоятельны при интеграции локальной КС в распределенную сеть. Подходы к межсетевой защите (межсетевое экранирование), применяемые в настоящее время, характеризуются, с одной стороны, теоретической необоснованностью (т. е. идут от практически возможной реализации, а не от осмысления цели защиты), с другой, – недостаточной надежностью[7]. Формализация задачи межсетевой защиты, анализ существующих методов и формулирование комплексных решений содержатся в третьей главе.

В **§ 3.1** построена модель распределенной системы с точки зрения защиты от несанкционированного доступа (НСД) и изучены ее основные свойства. Определим использованные ранее понятия локального и внешнего сегментов КС.

Локальный сегмент *КС (ЛС КС) – подмножество субъектов и объектов КС, выделяемое по одному из следующих критериев:*

– критерию группирования в одно множество всех субъектов с возможностью непосредственного управления субъектами (если такая возможность присутствует в субъекте);

– критерию локализации некоторого подмножества объектов и субъектов в рамках некоторой технической компоненты КС;

– критерию присвоения объектам и субъектам ЛС КС некоторой информации, однозначно характеризующей субъект или объект (которая, как правило, называется адресом или сетевым адресом ЛС КС).

Внешний сегмент *КС – дополнение множества субъектов и объектов локального сегмента до всего множества объектов КС.*

Доступ удаленного субъекта к локальному объекту подразумевает организацию сложного потока от удаленного субъекта к ассоциированным объектам локального субъекта, т. е. фактически управление локальным субъектом со стороны удаленного субъекта. Целью удаленного злоумышленника (пользователя, управляющего удален-

---

[7] Гайкович В., Першин А. Безопасность электронных банковских систем. – М.: Изд-во «Единая Европа», 1993. – 365 с.

ным субъектом) является организация потоков от локальных объектов, не принадлежащих множеству L.

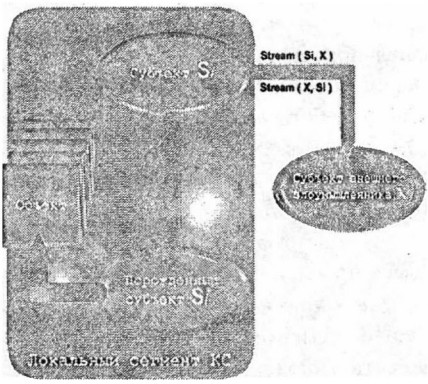


Рис. 3.1. К моделям воздействия внешнего злоумышленника на локальный сегмент КС

Сформулируем ***обобщенную модель***[8] на языке потоков.

Обозначим потоки от ассоциированного объекта O_x субъекта X к ассоциированному объекту O_k субъекта S_i и, наоборот, через $\boldsymbol{Stream}(X,O_x)\rightarrow O_k$ и $\boldsymbol{Stream}(X,O_k)\rightarrow O_x$. Предположим также, что свойства субъекта S_i таковы, что возможно существование потоков вида $\boldsymbol{Stream}\ (S_i,O_i)\rightarrow O_k$ и $\boldsymbol{Stream}(S_i,O_k)\rightarrow O_i$. По свойству транзитивности потоков имеет место доступ субъекта X к объекту O_i через субъект S_i.

В **§3.2** рассмотрены механизмы реализации политики безопасности в локальном сегменте компьютерной системы.

Политикой безопасности с полным проецированием прав *пользователя или методом доступа с полным проецированием прав пользователя P_n на объекты КС называется такой порядок составления правил разграничения доступа(ПРД), при котором любой из субъектов, принадлежащий S_n, обладает одним и тем же правом доступа T к любому объекту множества L(T).*

Из доказанного утверждения, описывающее потоки в ЛС КС в присутствии телекоммуникационного субъекта S_i, следует важный факт: система защиты от НСД любого ЛС КС, в котором гарантированно выполнена политика безопасности с полным проецирование прав доступа пользователей (к системам с такой политикой безопасности относится подавляющее большинство программно-аппаратных систем защиты ло-

[8] Щербаков А. Ю. Тенденции применения средств защиты информации в сфере информационного обеспечения банковской деятельности // Информационная безопасность: Сб. материалов конф. – М., 1994. – С. 25-26

кальных ресурсов, а также практически все штатные средства защиты в ОС) является потенциально ненадежной (т. е. допускающей возможность злоумышленных действий) при подключении к внешним сетям (т. е. при дополнении множества субъектов телекоммуникационным субъектом для взаимодействия с внешним сегментом КС). Необходима коррекция методов составления ПРД в системах, где возможно воздействие внешнего злоумышленника.

Методом расщепления прав пользователя по отношению к множеству доступных ему субъектов *называется такой порядок составления правил разграничения доступа (ПРД), при котором права доступа пользователя* P_n *задаются отдельно для каждого доступного ему субъекта (или подмножества субъектов), принадлежащего множеству* S_n.

Доказано следующее утверждение (**о доступе в системах с проецированием прав**), описывающее условия защиты локальных объектов от внешнего злоумышленника: *в условиях расщепления прав субъект* X *получит тот же доступ к объекту* O_i, *что и субъект* S_i, *при условии существования потоков* $\textbf{\textit{Stream}}(X, O_x) \rightarrow O_k$ *и* $\textbf{\textit{Stream}}(X, O_k) \rightarrow O_x$ *и отсутствии в ЛС КС других субъектов, для которых существуют потоки между их ассоциированными объектами и* O_x.

Следствием данного утверждения является то, что *в условиях расщепления прав субъект* X *не получит доступ к объекту* O_i *в том случае, если субъект* S_i *не имеет доступа к* O_i *и не существует другого субъекта* S_r *в локальном сегменте КС, для которого существуют потоки между ассоциированными объектами данного субъекта и* O_x.

Доказанные утверждения позволили сформировать методику проектирования защиты ЛС КС при условии попарной корректности всех субъектов (включая телекоммуникационный) с гарантированным выполнением политики безопасности. Эта методика описывается следующей последовательностью шагов.

1. Формулируется политика безопасности с расщеплением прав пользователей (допустимо выделить два множества субъектов – чисто локальные и телекоммуникационные – и установить раздельные права для этих групп).

2. Для каждого субъекта или групп субъектов формируется множество прав доступа к конкретным объектам (или группам объектов).

3. Реализуется МБО, выполняющий указанную политику безопасности.

4. Субъекты ЛС КС замыкаются в ИПС с контролем целостности объектов-источников.

Далее в **§3.3** рассмотрен один из основных подходов к защите – метод межсетевого экранирования (основной зарубежный подход)[9], который дополнен рядом решений, базирующихся на свойствах построенной модели.

---

[9]Carson M. Sendmail without the superuser (Почтовые отправления без суперпользователя) // Fourtth Usenix UNIX Security Symposium: По материалам симп., Santa Clara, CA, октябрь 1993. – С. 139-144

Суть экранирования состоит в прохождении потоков между O_k и O_x через дополнительный объект (возможно, более низкого уровня представления), ассоциированный с субъектом-анализатором потока.

Субъект S_f называется ***корректно экранирующим (или корректно фильтрующим) на выход*** *относительно субъекта S_i, если для любого объекта O_i при* $\textbf{Stream}(S_i,O_i)\rightarrow O_f$ *по последовательности $O_f[1], ..., O_f[k]$ можно однозначно восстановить O_i.*

Субъект S_f называется ***корректно экранирующим (или корректно фильтрующим) на вход*** *относительно субъекта S_i, если для любого объекта O_j при* $\textbf{Stream}(S_i,O_f)\rightarrow O_i$ *по последовательности $O_f[1], ..., O_f[k]$ можно однозначно восстановить O_i.*

Субъект S_f называется ***корректным фильтром,*** *если он является корректно фильтрующим на вход и на выход.*

Доказана

Основная теорема о корректном экранировании. *Экранирующий субъект S_f, участвующий в потоке подобъектов уровня r, будет корректным на вход и на выход тогда и только тогда, когда для любого S_i и для любого O_j по последовательности O_r^* однозначно определяется объект O_i.*

Приведенная теорема, хотя и является критерием, но, тем не менее, недостаточно конструктивна. Кроме того, субъект-фильтр не производит разделение потоков на множества L и N. Необходимо отметить два принципиально важных момента:

- субъект-фильтр должен иметь информацию о самих объектах O_i для осуществления сравнений;
- субъект-фильтр должен иметь информацию о разрешенных или запрещенных потоках между объектами O_k и O_x.

Приведем ***определение фильтра***, учитывающего разделение потоков на множества L и N.

Гарантированно-изолирующим фильтром *называется корректный фильтр, который разрешает прохождение потока* $\textbf{Stream}(X,O_x)\rightarrow O_j$ *и* $\textbf{Stream}(X,O_j)\rightarrow O_x$ *только для потоков, принадлежащих множеству L.*

Существующие методики проектирования и реализации экранирующих субъектов и управления ими [10] рассматривают процесс фильтрации применительно к особенностям функции ***Decomp***. Рассматривают полученную после декомпозиции последова-

---

[10]Treese W., Wolman A. X throug the firewall, and other application relays (Прохождение через межсетевой барьер и другие фильтры приложений) // USENIX Conference: По материалам конф., Cincinnati, OH, июнь 1993. – С. 87-99

тельность с точки зрения информационных подобъектов (A_{jm}), которые интегрально описывают подмножество объектов, относящихся к выделенному адресу, либо рассматривают указанную последовательность относительно некоторого субъекта, который производит декомпозицию на подобъекты.

С точки зрения особенностей работы субъекта, производящего декомпозицию объекта, зарубежные работы вводят понятие сервиса, описывая его как субъект, в котором локализованы конкретные алгоритмы декомпозиции (т. е. порождающие некие последовательности подобъектов, свойственные только данному субъекту).

Требование гарантированной фильтрации в части доступа S_f к любому объекту ЛС КС технически достаточно сложно реализовать в силу возможной гетерогенности операционных сред ЛС КС, скоростных параметров и т. д. Однако можно предложить альтернативный метод проектирования гарантированно-изолирующего субъекта-фильтра.

Предположим, что в субъекте-фильтре однозначно выделяются информационные подобъекты и реализация $\boldsymbol{Stream}(S_i, O_{jm}) \to O_f$ является тождественным отображением (технически это означает безошибочную передачу в тракте фильтр – ЭВМ).

Для всех объектов ЛС КС вычислим хеш-функции $H(O_j, K_g) = h_{jg}$ и гарантируем их доступность для субъекта-фильтра, хеш-функция, возможно, зависит от индивидуальной информации пользователя K_i. Процедура фильтрации на выход (относительно существующих объектов) формулируется следующим образом:

- по последовательности подобъектов $D_{j1r}, \ldots, D_{jkr}$ восстанавливается объект D_j;
- вычисляется $H(D_j, K_i) = h^*_{ji}$;
- вычисленное значение h^*_{ji} сравнивается с h_{ji};
- в случае совпадения проверяются права доступа к объекту O_i;
- в случае доступности объекта для передачи во внешний сегмент КС разрешается передача подобъектов, соответствующих декомпозиции объекта во внешнюю сеть;
- в случае несовпадения передача запрещается.

Указанный метод может быть дополнен фильтрацией сервисов для обеспечения достоверного восстановления объекта по последовательности подобъектов.

Основными теоретическими результатами данной главы являются:

- построение модели распределенной системы на базе уточнения субъектно-ориентированной модели КС;
- доказательство несостоятельности класса политик безопасности с полным проецированием прав пользователя на все доступные ему субъекты;
- формулирование понятий корректной фильтрации и ее условий, доказательство функционального тождества ИПС и фильтра приложений (фильтра прикладного уровня – ФПУ);

- формулирование методов расщепления прав пользователя и методов проектирования механизмов комплексной защиты на базе экрана и локальной защиты.

Основным практическим результатом главы являются анализ свойств межсетевого взаимодействия с указанием его конкретных свойств и его коррелирование с теоретическими выводами.

Проведенные исследования могут служить основой как для анализа готового технического решения, так и для проектирования механизмов программно-технической защиты от НСД при межсетевом взаимодействии.

Глава 4 «Практические аспекты организации управления доступом в корпоративной системе регионального уровня» содержит описание апробации и практического использования полученных результатов при разработке технологий построения корпоративных систем общего и специального назначения.

Описание некоторых сфер применения результатов исследования приведено в **§ 4.1**. Сформулированные в предыдущих главах теоретические положения работы оказались полезны и востребованны в совокупности программно-технических решений Научно-производственного предприятия «Фактор-ТС» (г. Москва) при разработке и усовершенствовании технологии «Дионис», а также при создании специализированных корпоративных универсальных транспортных подсистем. В их числе – УТП ЦБ РФ и других финансовых и государственных институтов, распределенные системы высокопроизводительных вычислений для фундаментальных и прикладных научных исследований в аэрогидродинамике, баллистике, ядерной физике, квантовой химии, молекулярной биологии и др.

В **§§ 4.2 – 4.5** рассмотрены принципы и особенности организации управления доступом в распределенных корпоративных системах общего и специального назначения на примерах технологических решений Научно-производственного предприятия «Фактор-ТС» (технология «Дионис») и Корпорации IBM (MQSeries). Все технологии, используемые НПП «Фактор» при создании корпоративных сетей передачи данных, предоставляют возможность обмена конфиденциальной информацией, перекрывая каналы возможной утечки информации и контролируя целостность данных и права доступа абонентов. При этом в зависимости от технологической схемы Заказчика применяются:

- сетевые экраны, обеспечивающие контроль доступа и обмена данными на стыке LAN ↔ WAN (технология «Дионис»);
- криптомаршрутизаторы для шифрации трафика на уровне пакетов данных при передаче данных LAN ↔ LAN через открытые каналы связи (технология «Дионис»);
- Proxy-серверы (серверы-посредники) для подключения к сервисам по протоколам Telnet, FTP, SMTP, HTTP и др.;
- модули шифрации транзакций при использовании технологий передачи сообщений (технология MQSeries);
- защищенные почтампты, обеспечивающие аутентификацию пользователей, а также шифрацию данных, передаваемых по открытым каналам связи (технология «Дионис»);

- почтовые агенты и транспортные модули, предоставляющие средства электронной подписи и шифрования данных на рабочих местах абонентов сети (технология «Дионис»).

Перечисленные выше средства защиты информации совместимы по ключевым системам и могут использоваться совместно в любых сочетаниях. Использование комбинированных решений, например, на основе независимого шифрования как на прикладном, так и на транспортном уровнях, позволяет существенно увеличить криптостойкость отдельных элементов и корпоративной сети в целом.

В **§ 4.3** особое внимание уделено проблеме адаптации используемых технологий промежуточного слоя, ориентированных на передачу информации в виде сообщений, или MOM-технологий (Message Oriented Middleware). Отмечено, что в специализированных корпоративных сетях, основанных на MOM-технологиях передачи сообщений, передача конфиденциальной информации по любым открытым линиям связи реализуется с использованием крипто-интерфейсов, обеспечивающих подключение сертифицированных технических средств.

Основной практический вывод главы 4 состоит в том, что наивысший уровень защиты информации в корпоративной сети обеспечивается при комплексном использовании всех средств защиты данных, соответствующих используемой технологии получения информации. Материал главы представляется полезным для практической реализации решений по управлению доступом к информации при построении публичных и специализированных региональных корпоративных систем.

В ***заключении*** сформулированы общие принципы управления доступом в защищенных КС в рамках методологии достаточных условий, приведено описание взаимосвязанных процедур управления и общая структура процесса проектирования системы управления доступом в распределенной КС.

Далее кратко подведены итоги выполненной работы.

Основным результатом диссертационной работы является решение задачи управления доступом в распределенных компьютерных системах на основе исследования, обобщения и развития методов и моделей проектирования систем безопасности для широкого класса гетерогенных компьютерных систем и сетей с территориально распределенной обработкой информации, имеющих субъектно-объектную иерархическую декомпозицию:

- Уточнена модель субъектно-объектного взаимодействия в ИТС;
- Проведено доказательство достаточных условий выполнения произвольной ПБ в КС при управлении системой безопасности ИТС;
- Предложена конструктивная коррекция ПБ при проектировании системы безопасности для сетевых сред;
- Предложены модели и алгоритмы управления доступом в распределенных КС, обеспечивающие работоспособность сложных программных комплексов и гарантирующие выполнение заданной при проектировании ПБ.

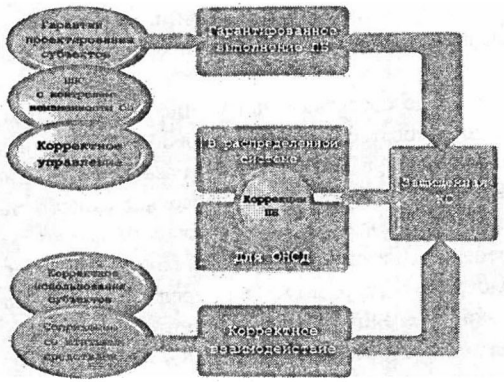


Рис. Взаимосвязь методов проектирования защищенной КС

Получены следующие теоретические и экспериментальные результаты, применимые при создании подсистем безопасности ИТС:

- Произведена классификация механизмов безопасности в рамках сформулированных алгоритмов управления, включающих механизмы обеспечения безопасности сетевого взаимодействия;
- Даны рекомендации и сформулированы требования к применению средств, реализующих корректное управление;
- Приведено описание программно-технических решений, реализующих предложенные алгоритмы.

Правомерность такого подхода к решению поставленной задачи подтверждена практической апробацией полученных результатов в технологиях построения распределенных корпоративных сетей.

В процессе выполнения диссертационной работы получены новые научные результаты, представляющие самостоятельную теоретическую и практическую ценность для разработки методов управления доступом при проектировании систем управления безопасностью в широком классе КС. Уточнены субъектно-ориентированная модель безопасности КС и основные термины, введены новые понятия; представлена модель управления механизмами реализации ПБ в распределенной КС; сформулировано понятие корректного управления и обоснованы достаточные условия корректности управления, предложены методы и алгоритмы управления доступом; уточнена модель взаимодействия локальных и удаленных сегментов КС, показана несостоятельность целого класса политик безопасности; предложена конструктивная коррекция ПБ в сетевых средах при проектировании механизмов безопасности; проведен анализ двух классов защиты от несанкционированного доступа в сетевой среде ИТС; определены критерии классификации механизмов межсетевой защиты с учетом коррекций ПБ и механизмов генерации изолированной программной среды.

Таким образом, полученные результаты являются решением важной теоретико-прикладной задачи совершенствования методов управления доступом в компьютерных системах, имеющей существенное значение для развития методологии решения задач

в области математического моделирования, системного анализа, оптимизации, управления и обработки информации, разработки проблемно-ориентированных систем управления с целью повышения эффективности, надежности и качества исследуемых объектов.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

Монографии:

1. Биктимиров М. Р. Избранные главы компьютерной безопасности / М. Р. Биктимиров, А. Ю. Щербаков. – Казань: Изд-во Казан. матем. об-ва, 2004. – 372 с.

2. Биктимиров М. Р. Инженерные основы защиты интеллектуальной собственности / М. Р. Биктимиров, А. В. Домашев, Е. А. Дуйков, С. В. Сотский, А. Ю. Щербаков – Казань: Изд-во Казан. матем. об-ва, Изд-во Казан. ун-та, 2008. – 174 с.

Статьи в журналах из списка, рекомендованного ВАК РФ:

3. Биктимиров М. Р. К вопросу о разработке требований к защите от несанкционированного доступа конфиденциальной информации / М. Р. Биктимиров, В. В. Засыпкина, А. Ю. Щербаков // Безопасность информационных технологий. – М.: МИФИ, 2001. – № 1. – С. 62-69.

4. Биктимиров М. Р. Система требований к обеспечению информационной безопасности типовой Единой информационно-телекоммуникационной системы (ЕИТС) регионального уровня / М. Р. Биктимиров, Г. И. Лаврешин, А. Ю. Щербаков. // Безопасность информационных технологий. – М.: МИФИ, 2003. – № 2. – С. 22-28.

Материалы конференций:

5. Биктимиров М. Р. Создание инфраструктуры информационного и компьютерного обеспечения науки и образования в Республике Татарстан // Телематика-2000: Материалы межд. науч-метод. конф. г. Санкт-Петербург, 2000 г. – С-Пб., 2001. – http://it.knc.ru/publications/tm2000.shtml.

6. Биктимиров М. Р. Концепция построения опытной зоны государственной защищенной информационной системы / М. Р. Биктимиров, А. Б. Жижченко // Информационная безопасность России в условиях глобального информационного общества: Материалы 2-й Всерос. конф., г. Москва, 2001 г. – М., 2001. – http://www.infoforum.ru/news/?p=11&n=56.

7. Биктимиров М. Р. Компьютерная сеть научно-образовательного сообщества Республики Татарстан / М. Р. Биктимиров Э. Е. Шабашвили, А. М. Елизаров, Д. О. Соловьев // «RELARN-2001»: Материалы VIII конф. представителей региональных научно-образовательных сетей. Санкт-Петербург, 2001 г. – С-Пб., 2001. – http://www.relarn.ru/conf/conf2001/ report_31.html.

Отпечатано с готового оригинал-макета
в типографии Издательства
Казанского государственного университета
Тираж 100 экз. Заказ 64/9

420008, ул. Профессора Нужина, 1/37
тел.: 231-53-59, 292-65-60