На правах рукописи

Зегжда Дмитрий Петрович

ПРИНЦИПЫ И МЕТОДЫ СОЗДАНИЯ ЗАЩИЩЕННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

Специальность: 05.13.19 – Методы и системы защиты информации, информационная безопасность

Автореферат диссертации на соискание ученой степени доктора технических наук

Санкт-Петербург - 2002

Работа выполнена в Санкт-Петербургском государственном политехническом университете.

Официальные оппоненты:
доктор технических наук, профессор Левин Владимир Константинович

доктор технических наук, профессор Стрельцов Анатолий Александрович

доктор технических наук, профессор Хомоненко Анатолий Дмитриевич

Ведущая организация: ЗАО "Российские наукоемкие технологии"

Защита состоится “ ” декабря 2002 г. в часов на заседании диссертационного совета Д 212.229.27
Санкт-Петербургского государственного политехнического университета
95251, Санкт-Петербург, Политехническая 29/1, ауд.

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

Автореферат разослан “20” ноября 2002 г.

Ученый секретарь
диссертационного совета Платонов В.В.

Общая характеристика работы

Актуальность проблемы

Высочайшая степень информатизации, к которой стремится современное общество, ставит его безопасность в зависимость от защищенности информационных технологий, обеспечивающих благополучие и даже жизнь множества людей. Сегодня компьютерные системы и телекоммуникации во многом определяют надежность систем обороны и безопасности страны, стабильность банковской системы, обеспечивая хранение конфиденциальной информации, ее обработку, доставку и представление потребителям. Массовое применение компьютерных систем, позволившее решить задачу автоматизации процессов обработки постоянно нарастающих объемов информации, сделало эти процессы чрезвычайно уязвимыми по отношению к агрессивным информационным воздействиям и поставило перед потребителями современных технологий новую проблему — проблему информационной безопасности. Данная работа посвящена техническим аспектам этой проблемы, а именно поиску решений в области технологии построения защищенных компьютерных систем обработки информации.

Опыт эксплуатации современных компьютерных систем показывает, что на сегодняшний день проблема информационной безопасности еще не решена, потому что существующие средства защиты не в состоянии предотвратить нарушения, число которых растет год от года. Примеры, подтверждающие это, можно во множестве найти как в многочисленных публикациях, так и в Интернет. Переломить ситуацию можно только путем разработки новых подходов к решению проблемы безопасности, способных обеспечить адекватное противодействие современным угрозам и удовлетворить постоянно возрастающие требования.

Отечественная специфика проблемы защиты компьютерных систем состоит в том, что используемые повсеместно в нашей стране популярные импортные средства не рассчитаны на применение в тех ситуациях, когда безопасность имеет существенное значение, поскольку они предназначались для массового рынка, а не для обработки конфиденциальной информации. Встраивание дополнительной защиты в эти продукты в силу особенностей их архитектуры не может обеспечить уровень информационной безопасности, требуемый отечественными стандартами. Кроме того, информационная безопасность — это область, в которой просто невозможно обойтись без отечественных разработок и соблюдения национальных приоритетов. Следовательно, радикальным выходом из создавшегося положения является разработка отечественных защищенных систем. В связи с этим актуальной является задача разработки общесистемных принципов и эффективных методов построения защищенных систем, решение которой позволит получать научно-обоснованные технические решения, внедрение которых будет способствовать

повышению безопасности информационных технологий и обеспечению обороноспособности страны.

Исследованию различных теоретических и практических аспектов проблемы информационной безопасности, различным подходам к ее решению, методам построения защищенных компьютерных систем посвящены многочисленные работы ведущих российских ученых В. А. Герасименко, С. П. Расторгуева, Л. М. Ухлинова, А. И Толстого, С. Н. Смирнова, А. А. Грушо, А. Ю. Щербакова, а также зарубежных К. Лендвера, Д. МакЛина, Р. Сандху, П. Самарати, М. Бишопа, К. Брайса, П. Ньюмена, Т. Джегера и многих других.

Опираясь на результаты этих исследований, автор предлагает феноменологический подход к проблеме, в соответствии с которым безопасность системы определяется с одной стороны отсутствием в ней т. н. уязвимостей, использующихся в качестве механизма нарушения безопасности, а с другой — способностью средств контроля и управления доступом реализовать требуемые ограничения на доступ к информации и обеспечивать их безусловное выполнение, т.е. их толерантностью к несанкционированному доступу. На основе предложенного подхода автор формулирует базовые принципы технологии разработки защищенных систем и предлагает практические методы их построения.

Целью диссертации является разработка базовых принципов защищенных информационных технологий, устраняющих причины возникновения уязвимостей с помощью средств контроля доступа, толерантных к НСД, и методологии их реализации на основе специальной защищенной операционной системы.

Для достижения этой цели в работе решались следующие основные задачи:

- исследование нарушений безопасности и определение источников возникновения уязвимостей, построение формальной модели явления уязвимости, позволяющей нормализовать набор причин их появления;
- анализ моделей безопасности и методов управления доступом;
- разработка методов и средств анализа моделей безопасности и автоматического доказательства безопасности;
- разработка феноменологического подхода к построению защищенных систем обработки информации, основанного на устранении причин возникновении уязвимостей и обеспечении толерантности ограничений на доступ к информации;
- разработка принципов построения защищенных систем обработки информации в соответствии с феноменологическим подходом;
- разработка универсальных методов и средств контроля и управления доступом, предотвращающих появление широкого класса уязвимостей и обеспечивающих толерантность ограничений доступа к НСД;

- реализация защищенной ОС на основе предлагаемого подхода, предназначенной для использования в качестве базы защищенных информационных технологий;
- разработка методов применения защищенной ОС для построения защищенных систем обработки информации различного назначения.

Методы исследования. Для решения поставленных задач использовались теория множеств, аппарат реляционной алгебры, методы объектно-ориентированного моделирования и проектирования, объектно-ориентированное и логическое программирование, методы искусственного интеллекта и представления знаний.

Основные научные результаты и их новизна.

1. Проведено исследование причин нарушений безопасности автоматизированных систем обработки информации и осуществлен анализ источников возникновения уязвимостей, проведена их нормализация.
2. Впервые формализовано определение феномена уязвимости и построена формальная модель, позволяющая установить связь между уязвимостью и безопасностью.
3. Предложен феноменологический подход к построению защищенных систем обработки информации, реализующий опережающую стратегию защиты путем устранения источников возникновения уязвимостей и обеспечивающий толерантность ограничений на доступ к информации, и сформулированы его базовые принципы, определяющие основные свойства архитектуры защищенных систем и методы их построения.
4. Разработан универсальный язык описания моделей безопасности, выражающий правила управления доступом и критерии безопасности состояния системы в виде логических предикатов.
5. Предложено решение задачи автоматического доказательства безопасности системы методом оценки всех достижимых состояний в виде разработанного логического процессора моделей безопасности, позволяющего моделировать поведение системы и являющегося интерактивным инструментом разработки новых моделей безопасности и оценки безопасности систем.
6. Впервые разработан универсальный механизм контроля и управления доступом, основанный на представлении объектов защиты в виде абстрактных информационных ресурсов, унификации способов взаимодействия с помощью модели клиент-сервер и операций доступа с помощью универсального интерфейса, позволяющий обеспечить толерантность средств защиты к НСД и их инвариантность по отношению к модели безопасности.
7. На основе предложенного подхода и методологии разработана защищенная ОС «Феникс», реализующая универсальный механизм контроля и

управления доступом и включающая все функции защиты, необходимые для соответствия требованиям Гостехкомиссии РФ по второму классу защиты средств вычислительной техники от несанкционированного доступа, предназначенная для использования в качестве основы защищенных информационных технологий.

8. Разработаны типовые решения защищенных систем обработки информации, построенных на основе защищенной ОС, в том числе: терминальный комплекс обработки конфиденциальной информации, защищенный информационный сервер и защищенная система хранения и обработки данных, использующая СУБД Oracle.

Положения, выносимые на защиту:

1. Результаты исследования нарушений безопасности и анализа механизмов их осуществления, таксономия причин появления уязвимостей и их нормализация.

2. Формальное определение понятия «уязвимость» и формальная модель, позволяющая установить связь между уязвимостью и безопасностью.

3. Феноменологический подход к построению защищенных систем, состоящий в устранении источников возникновения уязвимостей и обеспечении толерантности ограничений на доступ к информации, и определяемые им принципы построения защищенных систем обработки информации.

4. Язык описания моделей безопасности, позволяющий выражать правила управления доступом и критерии безопасности состояния системы в виде логических предикатов.

5. Принцип работы логического процессора моделей безопасности, заключающийся в построении пространства достижимых состояний системы и оценке их безопасности.

6. Универсальный механизм контроля и управления доступом, основанный на абстракции представления объекта защиты, унификации модели взаимодействий и универсальном интерфейсе доступа.

7. Архитектура защищенной операционной системы «Феникс», разработанная в соответствии с предложенным феноменологическим подходом и реализующая универсальный механизм контроля и управления доступом.

8. Модель управления доступом защищенной ОС «Феникс», обеспечивающая управление распространением полномочий для иерархии пользователей, и ее доказательство с помощью логического процессора моделей безопасности.

Практическая ценность работы.

В основу диссертационной работы положены результаты, полученные автором в научно-исследовательских работах и практических разработках

защищенных информационных систем, проводимых в СЦЗИ СПбГТУ в период с 1994 по 2002 год:

- по программе Министерства образования РФ в ходе выполнения межвузовских комплексных программ "Методы и средства защиты информации"(1995-2002 гг.) и "Наукоемкие технологии в образовании" (1997-2002 гг.) в рамках научно-исследовательских работ по исследованию безопасности информационных технологий и созданию средств защиты информации;

- в рамках научно-исследовательских и опытно-конструкторских работ по исследованию безопасности различных операционных систем и разработке защищенной локальной сети «Феникс-ЛВС», работающей под управлением защищенной ОС «Феникс».

Полученные лично автором научные результаты были положены в основу ряда практических работ, в частности:

1. На основе предложенной модели управления доступом и языка описания политик безопасности создан процессор политик безопасности, решающий задачи анализа моделей безопасности.

2. Разработанные в диссертации принципы архитектуры защищенных систем, дискреционная модель иерархического управления распространением полномочий, обобщенная схема мандатных моделей использовались в СЦЗИ СПбГТУ при разработке под руководством и при личном участии автора защищенной ОС «Феникс».

3. На основе разработанного подхода созданы опытные образцы защищенных комплексов обработки информации, построенных на основе ОС «Феникс», позволяющих осуществлять иерархическое управление распространением полномочий, поддерживающих мандатную политику безопасности и соответствующих требованиям Гостехкомиссии РФ к защищенности автоматизированных систем по классу 1В.

Внедрение результатов. Результаты проведенных исследований нашли практическое применение в разработках, в которых автор принимал личное участие в качестве научного руководителя или ответственного исполнителя.

1. Разработанные в диссертации принципы технологии построения защищенных систем использовались при построении защищенной ОС «Феникс» и работающей под ее управлением локальной вычислительной сети «Феникс-ЛВС»(акт в/ч 43753 от 23 марта 2001 года). Комплекс «Феникс-ЛВС» прошел государственные испытания в в/ч 43753 в августе 2000 года (решение N2/59/3-595).

2. Результаты исследования нарушений безопасности и причин возникновения уязвимостей использовались в ходе выполнения правительственных научно-технических проектов по исследованию и оценки информационной безопасности ОС Novell NetWare, UNIX и Windows NT, выполненных СЦЗИ СПбГТУ (акт в/ч 43753 от 16 апреля 1996 года).

3. Разработанная в диссертации дискреционная модель безопасности, обеспечивающая иерархическое управление распространением полномочий, обобщенная схема мандатных моделей безопасности и язык описания моделей безопасности, а также логический процессор политик безопасности использовались при разработке защищенных комплексов обработки информации в НИИ Квант и в/ч 43753 (акт НИИ Квант от 17 апреля 2001 г. и акт в/ч 43753 от 16 мая 2001 года).

4. Разработанный автором феноменологический подход к построению защищенных систем и предложенные типовые решения защищенных систем обработки информации, построенных на основе защищенной ОС, в том числе защищенная система хранения и обработки данных, использующая СУБД Oracle, применялись для защиты распределенных вычислительных комплексов, предназначенных для обработки и хранения специальной информации (акт в/ч 45187 от 23 июля 2002 г.).

5. Написанная в соавторстве с А. М. Ивашко по результатам проведенных исследований книга "Основы безопасности информационных систем" рекомендована учебно-методическим объединением ВУЗов Российской федерации по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем".

6. Основные теоретические положения диссертации легли в основу разработанных автором курсов лекций "Технология построения защищенных информационных систем", "Защищенные операционные системы", а также при создании лабораторного практикума "Исследование свойств математических моделей политик безопасности" для специальности 0752, 0755 на кафедре ИБКС в СПбГПУ.

Апробация результатов работы. Результаты научных разработок и исследований, выполненных автором по теме диссертации, обсуждались на следующих международных и российских конференциях и семинарах: третий всесоюзный семинар "Качество программного обеспечения" (Москва, СНПО Алгоритм 1991 г.), Республиканский научно-технический семинар “Методы и технические средства защиты информации"(СПбГТУ, 1993 г.), International Congress on Computer Systems and Applied Mathematics CSAM'93(St. Petersburg, July 19-23, 1993), "The Workshop on Information Protection" (Institute for Problems of Information Transmission, December 1993, Moscow), "European Simulation Multiconference" (June 1994, Barcelona, Spain), 2-я всероссийская научно-практическая конференция "Проблемы защиты информации в системе высшей школы"(Москва, 11-13 октября 1994 г.), Республиканская научно-техническая конференция "Теория и практика обеспечения безопасности информационных технологий"(СПбГТУ, 1994 г.), семинар "Информационная безопасность"(Санкт-Петербург, 1995 г.), Республиканская научно-техническая

конференция "Методы и технические средства обеспечения безопасности информации" (СПбГТУ, 1995-2002 гг.), Санкт-Петербургская международная конференция "Региональная информатика-95", международная конференция "Безопасность информации"(Москва, 1997 г.), научно-практический семинар "Сеть Internet для банков — возможности и опасности" (16-19 сентября 1997 г., Москва), конференция “Информационная безопасность автоматизированных систем” (Воронеж, 16-18 июня 1998 г.), Межрегиональная конференция "Информационная безопасность регионов России"(1999 г.), международная конференция «Математические методы, модели и архитектура безопасности компьютерных систем» (Санкт-Петербург 2001 г.), а также опубликованы в журнале «Проблемы информационной безопасности. Компьютерные системы», издание СПбГПУ 1999-2002 гг. .

Основное содержание научных материалов по тематике диссертации опубликовано: в книгах, статьях, докладах, учебных пособиях, наиболее существенные из которых приведены в списке литературы.

Публикации. Общее число публикаций автора составляет 84 наименования, из них теме диссертации посвящены 56 научных трудов, в том числе 4 монографии и 2 учебных пособия.

Структура и объем работы. Диссертация включает введение, пять глав, заключение, список литературы и приложения.

Содержание работы

Во введении обоснована актуальность задачи диссертации, обрисована специфика проблемы в отечественных условиях, сформулирована цель диссертационной работы.

В первой главе содержатся результаты исследований автора в области различных подходов к понятию защищенная система, и формализуется цель, которую преследует данная работа. Автором исследованы предпосылки кризисного положения, сложившегося в сфере обеспечения информационной безопасности, и представлены различные подходы к определению понятия «защищенная система обработки информации» и критериев оценки ее защищенности. Сделана попытка обобщения этих подходов и предложена общая формальная модель безопасных информационных систем.

В общем случае задача построения защищенных систем обработки информации может быть формализована следующим образом:

U – множество лиц-участников информационного процесса (потенциальных пользователей компьютерной системы), осуществляющих доступ к информации и ее обработку и обменивающихся информацией.

I – множество информационных объектов-контейнеров(документов, книг, папок, файлов и т. д.), хранящих информацию. Информация не может существовать сама по себе — она хранится в каком-либо контейнере.

С точки зрения безопасности информационные процессы моделируются с помощью отношений информационных потоков, определенных на этих базовых множествах. Под информационным потоком понимается событие, приведшее к появлению в точке назначения потока информации, находящейся перед этим событием в точке исхождения потока. С точки зрения безопасности алгоритмы обработки информации не имеют значения, важен только информационный обмен между пользователями и системой.

Существуют два вида потоков:

$F^W \subseteq U \times I$ – отношение, описывающее потоки от пользователей к контейнерам;

$F^R \subseteq I \times U$ – отношение, описывающее потоки от контейнеров к пользователям.

Для того чтобы судить о безопасности системы должны быть определены базовые положения, характеризующую предметную область с точки зрения безопасности. Эти положения должны быть сформулированы в виде следующих *аксиом безопасности*:

1. Для каждой информации существует по крайней мере один пользователь являющийся ее *доверенным источником*. Доверенные источники описываются функцией $\mathrm{TrustSrc} : I \to U$.

2. Для каждого пользователя известен набор информации, для которой он является *уполномоченным потребителем*. Эти полномочия описываются функцией $\mathsf{Authority}:U\to I$.

В каждый момент времени распределение информации в системе характеризуется следующими отношениями между пользователями и информацией:

1. $\mathsf{Know} \subseteq U\times I$ – отношение известности, которое определяет какой пользователь знает какую информацию.
2. $\mathsf{Create} \subseteq U\times I$ – отношение порождения, которое определяет какой пользователь поставляет какую информацию.

В общем случае задача обеспечения безопасности может быть сформулирована следующим образом:

Состояние системы является безопасным, если выполняются следующие *критерии безопасности состояния*:

1. Отношение известности не противоречит функции авторизации $\mathsf{Know} \subseteq \mathsf{Authority}$;
2. Отношения порождения не противоречит функции доверенного источника $\mathsf{Create} \subseteq \mathsf{TrustSrc}$.

Система в целом является безопасной, если выполняются следующие *критерии безопасности для системы*:

1. Текущее состояние системы безопасно;
2. Транзитивное замыкание отношений Know и Create не противоречит аксиомам безопасности.

В компьютерной системе пользователи не могут обрабатывать информацию непосредственно и вынуждены использовать инструменты-посредники — программные средства обработки информации, которые представляют их интересы в системе. Для того чтобы отразить это, в модель вводятся следующие понятия:

S – множество субъектов;

O – множество объектов.

P, $\mathsf{P}\subseteq \mathsf{O}$ - множество программ-приложений, с помощью которых пользователи работают с информацией, находящейся в объектах.

Id – отношение идентификации, которое сопоставляет пользователю по крайней мере одного субъекта $\mathsf{Id} \subseteq \mathsf{U}\times \mathbb{P}(\mathsf{S})$.

Imp – отношение имперсонализации, которое для каждой программы определяет субъект, интересы которого она представляет $\mathsf{Imp} \subseteq \mathsf{P}\times\mathsf{S}$.

Sem – отношение семантики, которое устанавливает связь между объектами и информацией, которая в них содержится $Sem \subseteq O \times I$.

Набор операций, осуществляемых программами над объектами обозначается Op и представляет собой множество отношений вида $x \subseteq P \times O$, где x – тип операции(чтение, запись и др.) Тип операции зависит от природы объекта и возможностей программы.

Связь между операциями и информационными потоками описывается функцией $InfFlow: Op \rightarrow F$.

Доступ описывается отношением $A \subseteq P \times Op \times O$, которое определяет возможности программ по осуществлению операций в отношении объектов.

Модель безопасности $SM=\{R, A^A\}$ представляется в виде совокупности множества прав доступа R и отношения авторизованного (санкционированного) доступа $A^A \subseteq S \times O \times \mathbb{P}(R)$, определяющего права субъектов на доступ к объектам.

Средства контроля доступа опираются на модель безопасности и запрещают операции, которые противоречат правилам модели. Функционирование средств контроля доступа описываются следующими отношениями:

$Map \subseteq Op \times R$ – устанавливает соответствие между операциями и правами доступа;

$A^S \subseteq P \times Op \times O$ — определяет множество операций программ над объектами, контролируемых средствами защиты.

Можно выделить два устоявшихся подхода к понятию «безопасность информационных систем": нормативный и ноуменологический.

Нормативный подход состоит в том, что защищенной считается система, соответствующая требованиям выбранных критериев или стандартов. При этом степень защиты определяется классом или уровнем, требованиям которого отвечает система. Требования безопасности регламентируют как функциональные возможности средств защиты — контроль и управление доступом, идентификацию/аутентификацию, целостность и аудит, так и процесс разработки и качество функционирования системы. В терминах предложенной общей модели этот подход может быть выражен следующим образом:

Система является безопасной, если все отношения доступа находятся под контролем средств защиты(1), реализующих модель безопасности(2):

1. $A^S=A$

2. $(p, op, o) \in A^S \rightarrow \exists (s, o, R) \in A^A$, что $(s,p) \in Imp$ и $(op, R) \in Map$

Ноуменологический, или теоретический, подход сводится к формальной математической модели, которая представляет реальную систему и ее поведение. В этом случае под безопасностью понимается подчинение поведения реальной системы условиям, заданным формальной моделью. В этом

случае степень безопасности определяется тем, насколько сильны утверждения, доказанные для используемой модели безопасности.

Система считается безопасной для заданной модели $SM=\{R,A^A\}$, если удается доказать, что в любом состоянии системы $\forall (s,o,r) \in A^A$.

Автор предлагает новый *феноменологический* подход к построению защищенных систем и к оценке их защищенности, основанный на результатах исследования феномена уязвимости и предложенных критериях безопасности. В соответствии с этим подходом безопасность системы определяется с одной стороны отсутствием в ней т. н. уязвимостей, использующихся в качестве механизма нарушения безопасности, а с другой — способностью средств контроля и управления доступом реализовать требуемые ограничения на доступ к информации и обеспечивать их безусловное выполнение, т.е. их толерантностью к НСД.

Предлагаемый критерий безопасности формулируется следующим образом:

1. Средства контроля доступа реализуют модель безопасности: $(p, op, o) \in A^S \rightarrow \exists(s, o, R) \in A^A$, что $(s,p) \in Imp$ и $(op, R) \in Map$.
2. Реализация модели безопасности соответствует аксиомам безопасности:
   для $\forall (s,o,R) \in A^A$ выполняются следующие условия:
   $\exists$ u и i, такие что $(u,s) \in Auth$ и $(i,o) \in Sem$, что
   $(u,i) \in Authority$, если $InfFlow(op) \in F^R$ для всех op, для которых $(op,R) \in Map$, и $(u,i) \in TrustSrc$, если $InfFlow(op) \in F^W$ для всех op, для которых $(op,R) \in Map$.
3. Все функциональные возможности программ находятся под контролем средств защиты: $A^S \supseteq P \times Op \times O$.

Отличие предложенного подхода к безопасности состоит в том, что он может быть положен в основу технологии разработки защищенных систем, поскольку его критерий может быть использован в качестве целевой функции процессе проектирования и разработки защищенной системы.

На основе предложенного феноменологического подхода и критерия безопасности автор постулирует следующие базовые принципы технологии построения защищенных систем:

1. *Принцип толерантности* - средства защиты должны действовать в строгом соответствии с формальной моделью безопасности для всех без исключения взаимодействий в системе.
2. *Принцип абсолютности* — средства защиты должны быть встроены в систему обработки информации таким образом, исключить возможность любого взаимодействия, не попадающего под их контроль.
3. *Принцип инвариантности* — средства защиты должны функционировать исходя из представления всех типов информационных взаимодействий в виде операций доступа субъектов к объектам и контролировать их с помощью универсальных алгоритмов,

инвариантных к типу взаимодействий. Средства защиты должны быть независимы от особенностей реализации прикладных программ и логики их функционирования.

4. *Принцип унификации* — должно существовать однозначное соответствие между контролируемыми операциями доступа субъектов к объектам и отношениями доступа, описываемыми моделями безопасности. Это позволяет придать средствам защиты универсальность и использовать их без изменения как для реализации различных моделей безопасности, так и для контроля доступа к объектам различной природы.
5. *Принцип разрешимости* — безопасность системы должна быть формально доказана в рамках используемой модели. Должен существовать механизм, позволяющий решить вопрос о безопасности настоящего состояния системы и оценить ее безопасность в будущем.

Остальные главы работы посвящены методам реализации этих принципов и описанию применения предложенного подхода для решения практических задач.

Вторая глава содержит результаты исследований автора в области нарушений безопасности и анализа причин появления уязвимостей. Задача данной главы — определить причины успешной реализации угроз безопасности, дать определение понятию "уязвимость", выявить обстоятельства, которые приводят к их появлению, систематизировать их и определить источники появления уязвимостей в современных информационных системах.

Поскольку с точки зрения автора причины успеха атак на системы обработки информации предопределены свойствами самих систем обработки информации, анализ случаев нарушения безопасности должен основываться не столько на исследовании методов, используемых нарушителем, сколько на выявлении свойств системы, позволивших ему успешно осуществить атаку.

Количество нарушений безопасности, несмотря повышенный интерес к этому вопросу и принимаемые меры, направленные на усиление защиты, постоянно растет, о чем свидетельствует, например, статистика международной организации CERT(Computer Emergency Response Team), на которую опираются исследования автора.

Статистика свидетельствует, что в абсолютном большинстве случае нарушители используют определенные особенности архитектуры системы, детали ее реализации или просчеты администрирования, которые в определенных обстоятельствах сводят на нет все возможности средств защиты или создают механизмы, позволяющие действовать в обход контроля с их стороны. Для обозначения таких особенностей информационных систем, влекущих за собой неспособность системы противостоять определенному

воздействию, используют уже достаточно устоявшийся термин "уязвимость", пришедший из рабочего жаргона хакеров. Использование уязвимости нарушителем в тех или иных целях называется атакой. С каждым годом количество узявимостей возрастает, и именно в этом росте заключается наибольшая угроза для информационных технологий будущего.

В работе приведены примеры, демонстрирующие характерные черты различных видов уязвимостей и типовые механизмы их происхождения. В частности рассмотрены: получение хэша пароля пользователя Microsoft Windows NT из резервной копии базы Security Access Manager, сохранение прав владельца в Windows 2000, переполнение буфера в стеке, подделка подписи апплета в JDK 1.1.1 и HotJava 1.0, неконтролируемый доступ к памяти при сборке фрагментированных IP-пакетов.

Для того чтобы дать определение феномену уязвимости предлагается рассматривать систему как совокупность прикладных программ и средств защиты. Программы реализуют определенные функции доступа к информации и ресурсам системы. Средства защиты контролируют доступ и могут его разрешить или запретить. В том случае, когда доступ разрешается, система переходит в новое состояние, которое в соответствии с политикой безопасности является либо безопасным, либо небезопасным. Все средства защиты спроектированы таким образом, что все разрешаемые ими виды доступа должны переводить систему только в безопасные состояния.

Однако на практике это получается не всегда, и системы, даже оснащенные средствами защиты, переходят в небезопасные состояния. Это происходит вследствие того, что система не всегда функционирует таким образом, как рассчитывали ее разработчики, поскольку при ее проектировании, реализации и в ходе эксплуатации допускаются ошибки, которые влекут за собой изменение ее функциональных характеристик. Однако далеко не каждая ошибка приводит к появлению уязвимости. В работе дано *определение уязвимости* как возникающее в результате ошибок или особенностей проектирования, программирования, эксплуатации, или постороннего вмешательства (модификации в ходе эксплуатации) расширение возможностей доступа либо за счет роста функциональных возможностей прикладных программ, которые не запрещаются средствами защиты, либо за счет сокращения функциональных возможностей самих средств защиты(рис. 1).

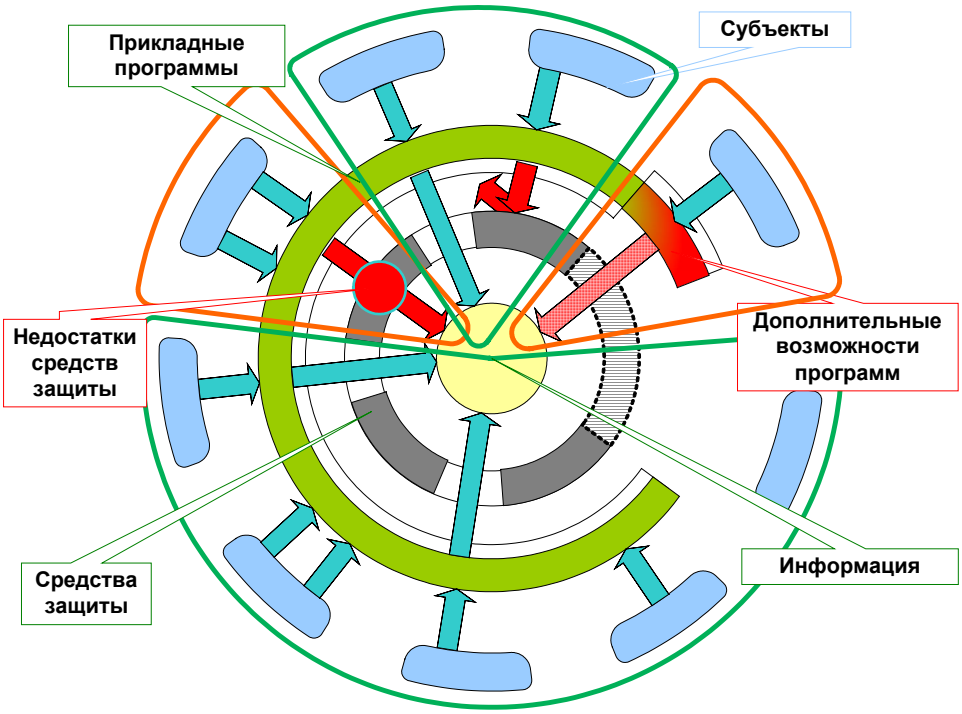

Рис. 1. Механизмы появления уязвимостей.

Возникшие благодаря уязвимости дополнительные возможности доступа не обязательно будут противоречить политики безопасности, поэтому назовем такой доступ нелегитимным, чтобы отличать его от несанкционированного. Нелегитимный доступ - это всегда результат нарушения баланса между функциональными возможностями прикладных программ и средств защиты. Нелегитимный доступ не контролируются средствами защиты поскольку либо осуществляются в обход них, либо игнорируется ими. Как и несанкционированный доступ нелегитимный доступ может привести к нарушению политики безопасности (если таковая имеется) или к утечке информации, нарушению ее целостности, к потере работоспособности всей системы.

В соответствии с предложенной общей моделью определение уязвимости формализуется следующим образом: система содержит уязвимость, если:

либо $\exists (p,op,o) \in A^S$, для которых $\exists s,r$ такие что $(p,s) \in Imp$, $(op,R) \in Map$, $(s,o,R) \notin A^A$

либо $\exists (p,op,o) \in A$ такое, что $(p,op,o) \notin A^S$.

От обычных ошибок программирования и проектирования уязвимости отличает то, что, во-первых, они проявляются в условиях, которые появляются вследствие преднамеренно созданного стечения обстоятельств, а вероятность их случайного появления ничтожно мала, и, во-вторых, их использование позволяет осуществлять действия, которые не пресекаются средствами защиты.

Уязвимости можно разделить на два класса - уязвимости в средствах защиты и уязвимости в прикладных программах. Для средств защиты уязвимость - это свойство терять способность осуществлять свои функции при наступлении определенных условий. Для прикладных программ уязвимость - это свойство при определенных условиях приобретать новые функциональные возможности, благодаря которым программа приобретает способность осуществлять одно из следующих действий: чтение, запись данных, исполнение кода и потребление ресурсов. Соответственно, уязвимостям первого типа соответствуют ошибки программирования средств защиты и недостатки администрирования безопасности, а уязвимостям второго типа — недостаточность средств защиты, заключающаяся в невозможности контролировать действия прикладных программ, и отсутствие защиты как таковой.

Проведенный автором анализ уязвимостей и их источников показал следующее:

1. Среди уязвимостей наиболее значительная часть приходится на ошибки программирования прикладных программ, средств защиты и администрирования безопасности(рис. 2.).

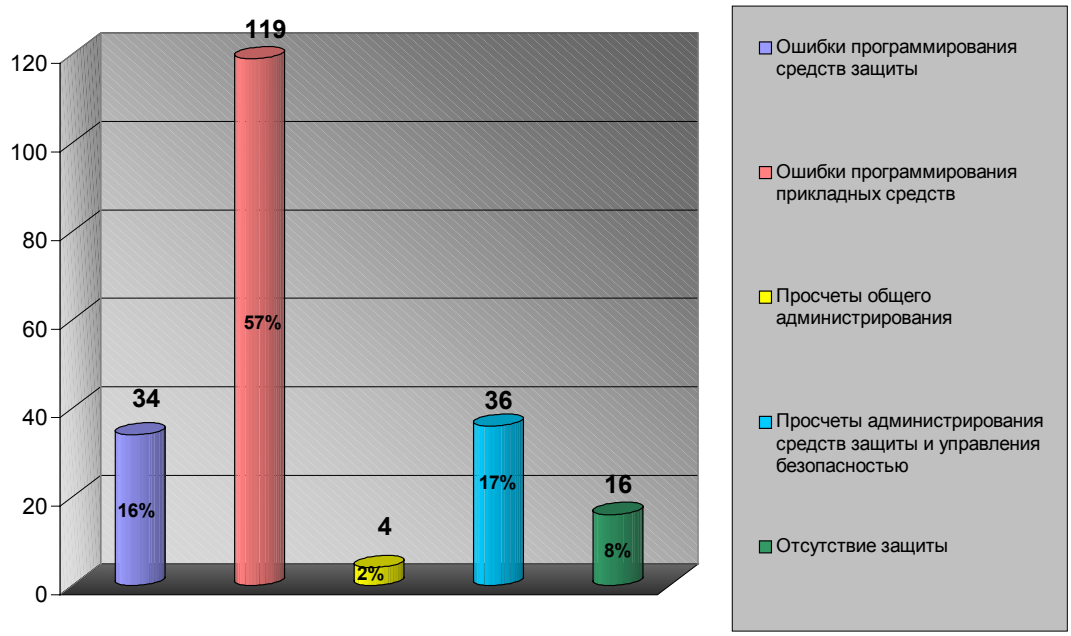

Рис. 2. Типы уязвимостей.

2. Автором проведена нормализация источников появления уязвимостей исходя из того, что в случае, когда непосредственным проявлением уязвимости является ошибка в прикладной программе или недостаток общесистемного администрирования, истинной причиной ее появления является недостаточность средств защиты, разработчики которых не предусмотрели возникшую ситуацию. В результате нормализации все причины возникновения уязвимостей были сведены к четырем, соответствующим различным стадиям жизненного цикла системы, на которых была допущена ошибка: отсутствие

защиты на этапе разработке требований, недостаточность защиты как результат ошибок проектирования, ошибки при реализации функций защиты, просчеты администрирования безопасности на этапе эксплуатации.

Среди источников появления уязвимостей первое место занимает недостаточность средств защиты, далее идут просчеты администрирования безопасности и ошибки программировании функций защиты (рис. 3).

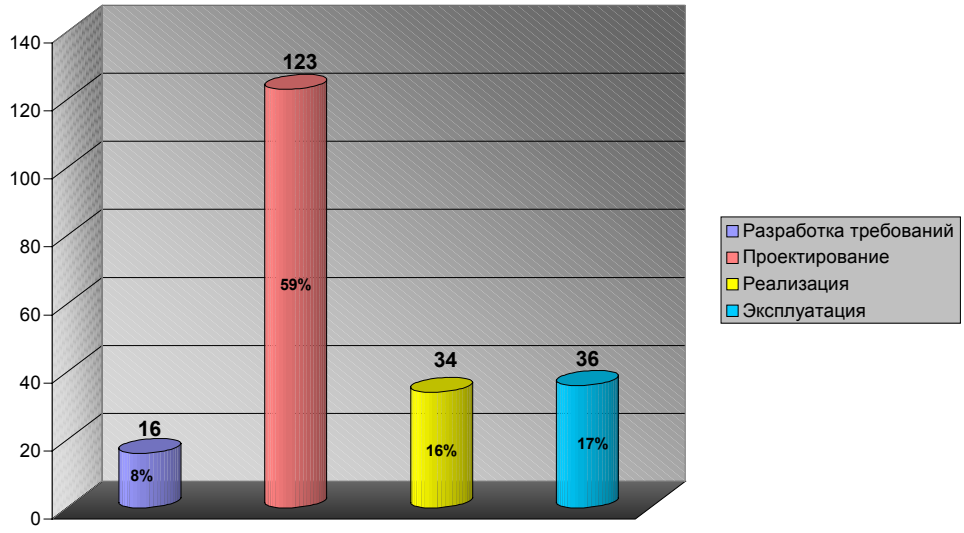

Рис. 3. Источники появления уязвимостей.

3. Подавляющее большинство недостатков средств защиты и ошибок их программирования связано с контролем доступа, а на идентификацию/аутентификацию и контроль целостности приходится лишь незначительная часть уязвимостей(рис. 4).

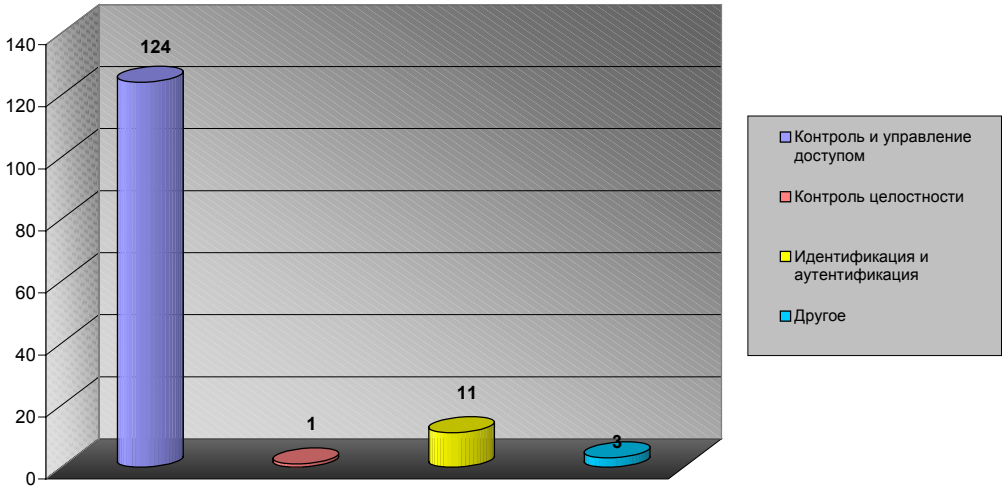

Рис. 4. Уязвимости и функции защиты.

4. Более детальный анализ уязвимостей средств контроля и управления доступом показал, что они обусловлены следующими причинами(рис. 5):

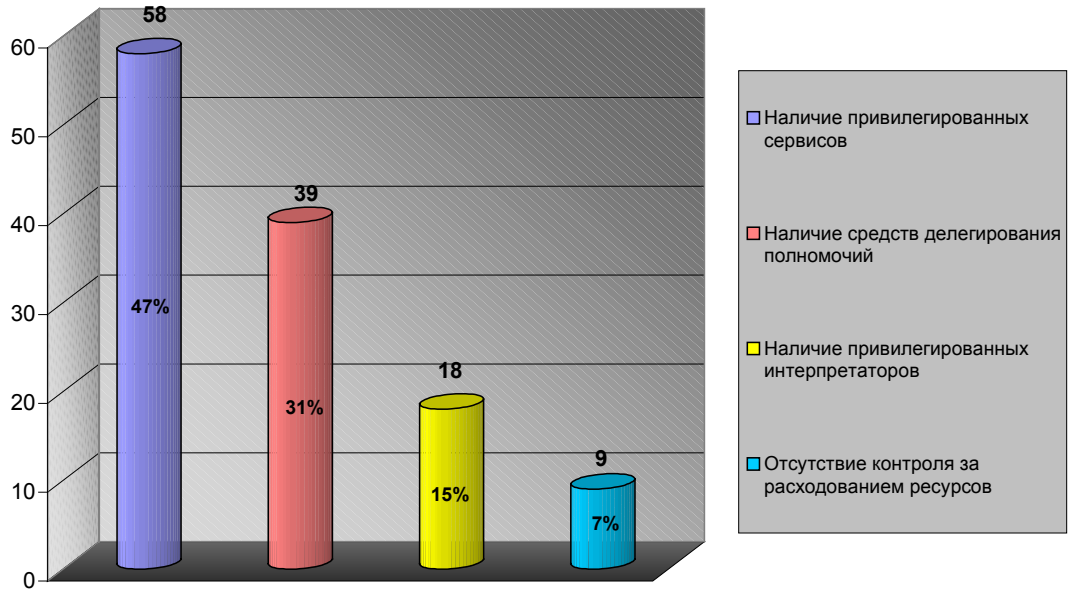

Рис. 5 Источники уязвимостей средств контроля и управления доступом.

- наличие привилегированных программ и сервисов. Нарушитель может воспользоваться ошибками, имеющимися в этих средствах и путем подбора параметров или последовательности вызовов заставить их выполнить желаемые действия вплоть до исполнения созданного им кода. Системы защиты не смогут его остановить, поскольку эти средства считаются привилегированными и работают вне контроля с их стороны.

- наличие механизма делегирования полномочий (типа SUID в UNIX). Эта причина по сути является частным случаем предоставления привилегий, но он гораздо более опасен поскольку предоставляет пользователю возможность запуска привилегированных процессов с произвольными функциональными возможностями.

- наличие привилегированных интерпретаторов. Этот механизм принципиально отличается от привилегированных средств тем, что в рамках интерпретатора порождается новая вычислительная среда, которая требует решения всех тех же проблем безопасности, что и первичная система, поскольку внутри нее уже не действуют системные средства защиты.

- отсутствие контроля за использованием ресурсов. Практически все существующие системы подвержены атаке отказа в обслуживании и не способны функционировать в ситуации, когда какое-либо приложение или сервис начинают активно потреблять системные ресурсы.

Основной вывод, который сделан на основании этого исследования, состоит в том, что главной причиной появления уязвимостей является отсутствие тотального контроля за доступом к ресурсам, реализующееся в виде различных механизмов делегирования полномочий и привилегий. Привилегии делегируются обычным прикладным программам и сервисам, в которых всегда

найдется ошибка, воспользовавшись которой нарушитель получает полномочия этих сервисов и выходит из под контроля средств защиты. Отдельную проблему представляют собой различные интерпретаторы, представляющие собой виртуальные машины, которые неподконтрольны средствам защиты базовой системы, и нуждаются в точно таких же средствах защиты, что и среда, в которой они функционируют. Следующей по значимости причиной появления уязвимостей является отсутствие в современных системах средств контроля за потреблением ресурсов, таких как процессорное время, память, пропускная способность каналов связи и т.д. Это объясняется тем, что такой контроль достаточно трудно реализовать и он не только будет потреблять определенную долю ресурсов, но главное скажется на эффективности их распределения.

Предложенная автором нормализация источников появления уязвимостей является первым этапом применения феноменологического подхода к решению задачи построения защищенных систем обработки информации, направленного на устранение причин нарушений безопасности. Знание природы этих источников позволяет оценить реальную способность систем противостоять угрозам безопасности, а также понять те недостатки в средствах защиты, которые привели к соответствующим нарушениям, и построить защищенную систему, лишенную этих недостатков.

Третья глава содержит результаты, полученные автором в области исследования и разработки математических моделей политик безопасности.

Автором разработана дискреционная модель безопасности, основанная на модели Харрисона-Руззо-Ульмана, обеспечивающая иерархическое управление распространением полномочий и устраняющая ряд недостатков базовой модели. Данная модель применяется в защищенной операционной системе «Феникс» для дискреционного контроля и управления доступом.

Рассмотрены шесть вариантов мандатной модели, которые различаются представлением взаимодействующих сущностей (индивидуальные или групповые субъекты), правилами контроля за изменением уровней безопасности (наличие/отсутствие уполномоченных субъектов), а также критериями безопасности (безопасные состояния или безопасные переходы). Все рассмотренные модели построены на одних и тех же принципах, поскольку все они применяют единый механизм представления атрибутов безопасности в виде решетки уровней безопасности и опираются на одни и те же методы доказательства. Автор предлагает обобщенную схему доказательства мандатных моделей, связывающую их отношениями обобщения/конкретизации, которая обобщает результаты всех теоретических исследований в этой области.

Обобщенная схема мандатных моделей позволяет выбирать для каждого конкретного применения наиболее подходящую по уровню ограничений модель, без необходимости проведения формального доказательства безопасности, и предоставляет возможность сравнивать системы, построенные

в соответствии с различными моделями. Например, при решении задачи анализа безопасности существующих систем предварительная проверка необходимых условий, сформулированных для моделей уполномоченных субъектов, модели Белла-ЛаПадулы и модели совместного доступа, в случае их невыполнения позволяет избежать трудоемкой проверки достаточных условий.

Автор развивает предложенную в первой главе модель защищенной системы в части общей модели функционирования средств контроля и управления доступом, обобщающей существующие модели безопасности.

В любой модели безопасности можно выделить три компонента: состояние, правила контроля доступа, критерии безопасности.

Состояния — это абстракция системы в терминах модели, например, представление учетных записей пользователей, выполняющихся программ, файлов, прав доступа и т.д. в виде множеств субъектов и объектов и отношений между ними. Правила контроля доступа задают ограничения, накладываемые на поведение системы. Критерии безопасности позволяют выделить защищенные состояния в полном множестве состояний.

Система считается безопасной в соответствии с моделью, если:

1) ее исходное состояние удовлетворяет критериям безопасности модели;

2) системный механизм контроля доступа реализует правила контроля доступа модели;

3) все состояния модели, достижимые из исходного, соответствуют критериям безопасности модели.

Вычисление множества достижимых состояний и оценку их соответствия критериям безопасности называется *разрешением проблемы безопасности*. Разрешимость мандатных моделей доказана для общего случая. Для дискреционных моделей Харрисон, Руззо и Ульман показали, что проблема безопасности в общем случае неразрешима, однако доказательство, может быть проведено для каждой конкретной системы, находящейся в заданном состоянии.

Поскольку абсолютное большинство систем реализуют дискреционные модели, разрешение проблемы безопасности является актуальной задачей для процесса оценки и верификации защищенности.

Проблема безопасности может быть формализована следующим образом:

Система Σ в общем виде представляет собой машину состояний: $\Sigma = \{S^{\Sigma}, T, s_{init}^{\Sigma}, Q\}$, где:

S^{Σ} — множество состояний системы;

Q — множество запросов, обрабатываемых системой;

T — функция перехода из состояний в состояние, T: $Q \times S^{\Sigma} \rightarrow S^{\Sigma}$. Функция T в ответ на запрос q переводит систему из состояния s_i^{Σ} в следующее $s_{i+1}^{\Sigma} = T(q, s^{\Sigma})$;

s_{init}^{Σ} — начальное состояние системы.

Состояние s^{Σ} достижимо в системе $\Sigma=\{S^{\Sigma}, T, s^{\Sigma}_{init}, Q\}$ тогда и только тогда, когда существует последовательность $<(q_0, s^{\Sigma}_0), ..., (q_n, s^{\Sigma}_n)>$, в которой $s^{\Sigma}_0=s^{\Sigma}_{init}$, $s^{\Sigma}_n=s^{\Sigma}$, а $s^{\Sigma}_{i+1}=T(q_i, s^{\Sigma}_i)$, $0\le i<n$.

Модель безопасности M — это кортеж множеств: $M=\{S, R, C\}$, где:

S — множество состояний для данной модели;

R — множество правил контроля доступа, сформулированных в форме логических предикатов, определенных на множестве S, вида $r(s_1, s_2)$, определяющих допустимость перехода из состояния s_1 в состояние s_2 в соответствии с правилами модели;

C — множество критериев безопасности, сформулированных в форме логических предикатов вида $c(s)$, определяющих безопасность состояния s с точки зрения модели.

Состояние $s\in S$ является безопасным тогда и только тогда, когда для него истинны все критерии $c(s)\in C$, т.е. $\forall c\in C$: $c(s)$=«истина».

Проблема безопасности представляется как $\Lambda=\{M, \Sigma, D\}$, где:

M — модель безопасности, $M=\{S, R, C\}$;

Σ — система, $\Sigma = \{S^{\Sigma}, T, s^{\Sigma}_{init}, Q\}$;

D — функция соответствия, D: $S^{\Sigma}\to S$, определяет соответствие между системными состояниями и состояниями модели.

На основе предложенных определений сформулирована *обобщенная теорема безопасности* систем обработки информации:

Система Σ, реализующая модель безопасности M, является безопасной тогда и только тогда, когда выполняются следующие условия:

1. для $\forall c\in C$: $c(D(s^{\Sigma}_{init}))$=«истина»;

2. для $\forall s^{\Sigma}_i, s^{\Sigma}_{i+1}\in S^{\Sigma}$: $s^{\Sigma}_{i+1}=T(q, s^{\Sigma}_i)$ $\exists$ s_i, s_{i+1} такие, что $s_i=D(s^{\Sigma}_i)$, $s_{i+1}=D(s^{\Sigma}_{i+1})$ и для $\forall r\in R$ $r(s_i, s_{i+1})$=«истина»;

3. для $\forall s^{\Sigma}_i\in S^{\Sigma}$, достижимого из состояния s^{Σ}_{init}, $\exists$ s_i такое, что $s_i=D(s^{\Sigma}_i)$ и для $\forall c\in C$ $c(s_i)$=«истина».

Следствиями данной теоремы являются постановки трех задач, которые могут быть решены методом разрешения проблемы безопасности:

1. Проблема доказательства модели безопасности.

Для данной модели M требуется доказать, что любое достижимое состояние из множества состояний S соответствует критериям C, т.е. система на основе данной модели будет защищена в общем случае.

2. *Проблема построения защищенной системы.*

Для данной системы Σ, критериев C, безопасных состояний S требуется построить множество правил контроля доступа R таких, что система Σ,

реализующая модель контроля доступа *M*={C, S, R} была бы безопасной в соответствии с обобщенной теоремой безопасности.

3. *Проблема оценки защищенности системы.*

Для данной системы Σ в состоянии s_{init}^{Σ}, использующей модель безопасности *M*, требуется произвести оценку безопасности всех достижимых состояний.

В работе предложен и реализован метод автоматизации решения проблемы оценки безопасности. Чтобы разрешить данную проблему, необходимо:

- *оценить* заданное состояние системы на соответствие критериям безопасности;
- *доказать*, что механизм контроля доступа, реализованный в системе, соответствует правила контроля доступа;
- *вычислить* множество состояний, достижимых из заданного, и оценить их безопасность.

Выполнив указанные действия, можно доказательно гарантировать защищенность системы. В качестве механизма их осуществления в работе предложен процессор политик безопасности(ППБ), использующий язык описания моделей безопасности, основанный на логике предикатов.

Разработанный язык описания политик безопасности(ЯОПБ) позволяет описывать наборы субъектов и объектов доступа, их атрибуты, а также правила контроля доступа и критерии различных моделей безопасности.

В качестве примеров, демонстрирующих возможности использования предложенного языка, в работе приведены описания трех различных моделей безопасности: классической дискреционной, основанной на модели Харрисона-Руззо-Ульмана, производной от нее ролевой и классической мандатной Белла-ЛаПадулы.

Реализация ППБ позволяет промоделировать поведение системы, подчиняющейся заданной политике безопасности и оценить безопасность ее состояний. Разработаны программные средства, которые на основании описания политики безопасности, сформулированного с помощью предложенного языка, создают модель системы, подчиняющийся правилам этой политики, позволяют исследователю интерактивно изучать поведение системы в определенных ситуациях (попытки осуществления доступа, создание и уничтожение субъектов и объектов, изменение их атрибутов) и оценивать его корректность. Кроме того такое исследование может выявить сильные и слабые стороны исследуемой политики безопасности.

Исследуемая система описывается на ЯОПБ в виде *модельно-ориентированного описания системных состояний* (МСС-описание), *описания правил контроля доступа* (ПКД-описание) и *описания критериев безопасности состояния* (КБС-описание).

ППБ — это обрабатывающая указанные описания машина логического вывода, построенная на основе Пролог-ядра, которая позволяет автоматизировать процесс доказательства безопасности системы (рис. 6).

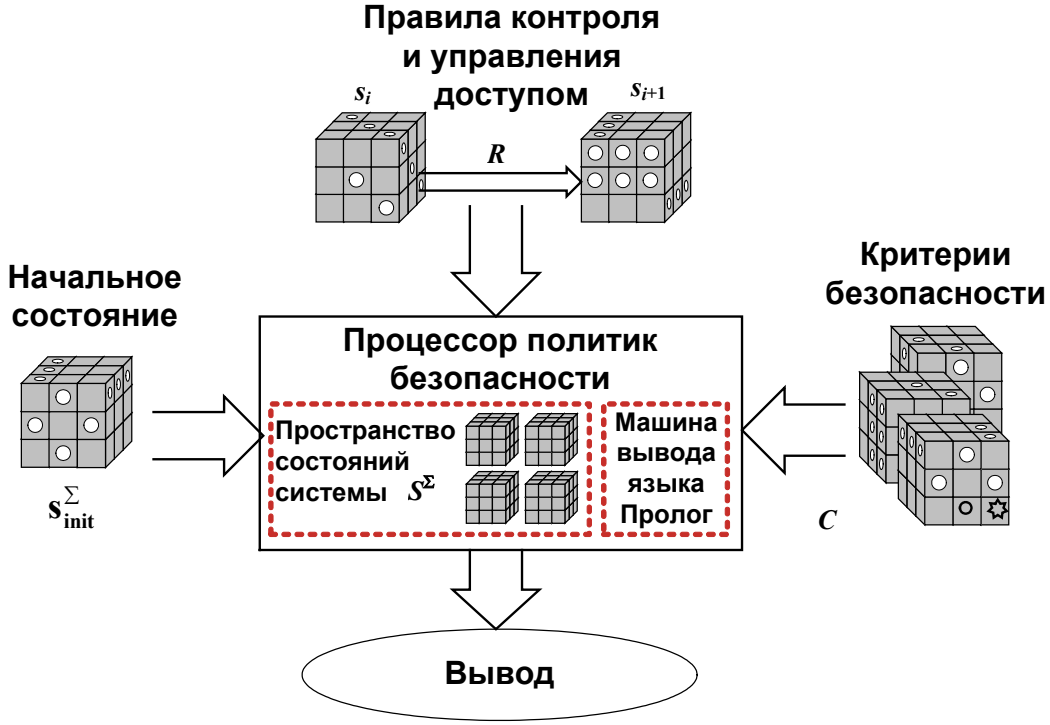

Рис. 6. Входные и выходные параметры процессора политик безопасности.

Можно отметить следующие направления применения ППБ:

Оценка заданного состояния системы на соответствие критериям безопасности. Входными параметрами ППБ являются описание состояния(МСС) и критерии(КБС), а выходом — оценка защищенности состояния.

Построение множества состояний, достижимых из заданного, и оценка их безопасности. Входными параметрами будут описание текущего состояния(МСС), правила контроля доступа(ПКД) и критерии безопасности(КБС), а на выходе получаются достижимые безопасные состояния.

Для полной автоматизации процесса разрешения проблемы безопасности разработан специальный инструментарий, функционирующий в комплексе с ППБ и включающий следующие утилиты (рис. 7):

1. Анализатор системных состояний, генерирующий МСС-описания.
2. Шаблон МСС-описаний.
3. Шаблон ПКД-описаний.
4. Шаблон КБС-описаний.
5. Интерактивное средство управления критериями безопасности.
6. Монитор нарушений безопасности.
7. Генератор отчетов.

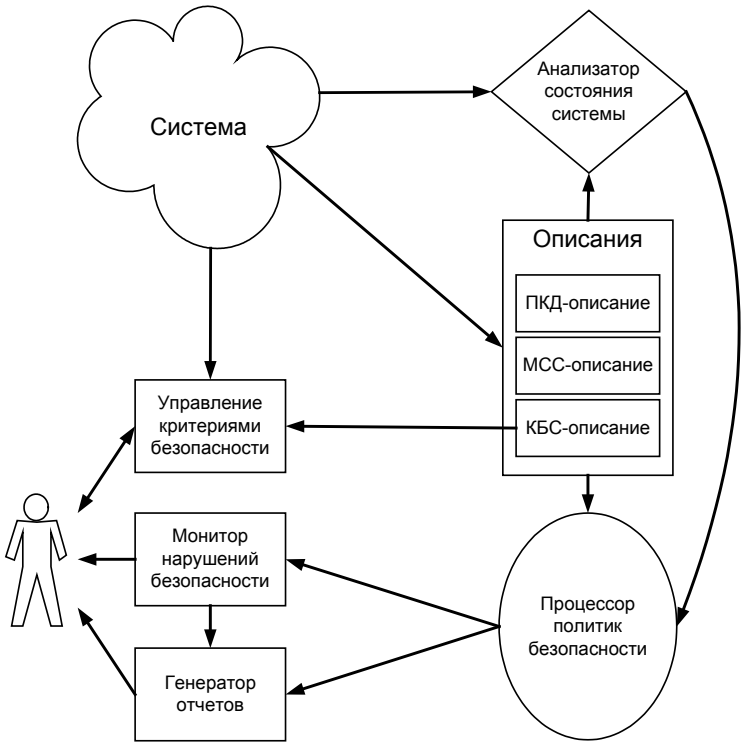

Рис. 7. Комплекс средств разрешения проблемы безопасности.

Исследуемая система и модель безопасности, реализованная в ней, описываются на ЯОПБ в виде МСС-, ПКД- и КБС-описаний на основе разработанных шаблонов. Анализатор состояния генерирует описание системы, ППБ получает на вход необходимые данные, производит анализ и выдает решение. Если он обнаруживает состояние системы, в котором не выполняются критерии безопасности, то монитор нарушений безопасности может продемонстрировать последовательность событий, приводящую систему в это состояние. Генератор отчетов формирует отчет, содержащий описания модели, системы, начальное состояние, правила контроля доступа, критерии безопасности, результаты оценки защищенности, трассу переходов в небезопасные состояния.

Полученные в данной главе результаты создают необходимую базу для построения основного средства защиты информационной системы – механизма контроля и управления доступом, позволяют сделать его инвариантным по отношению к политике безопасности и проанализировать его толерантность по отношению к НСД.

В четвертой главе рассмотрено применение предложенного автором подхода при разработке защищенной операционной системы «Феникс» (ЗОС «Феникс»). К основным научным результатам данной главы можно отнести системную архитектуру защищенной ОС, концепции информационного ресурса и универсального интерфейса доступа.

Защищенная операционная система «Феникс» является подлинной отечественной разработкой, в основе которой лежат результаты научных

исследований Центра защиты информации Санкт-Петербургского государственного технического университета.

ЗОС «Феникс» в целом удовлетворяет требованиям Гостехкомиссии РФ для второго класса защиты средств вычислительной техники от несанкционированного доступа и содержит в своем составе оригинальные средства контроля и управления доступом, идентификации и аутентификации, контроля целостности и аудита.

Функциональные возможности ЗОС «Феникс» позволяют использовать ее в среде современных локальных сетей и Интернет совместно с распространенными средствами обработки информации, а наличие интерфейса прикладного программирования, совместимого со стандартом POSIX, обеспечивает возможность портирования на платформу «Феникс» приложений ОС UNIX. Системная архитектура ЗОС «Феникс», опирающаяся на концепцию микроядра, технологию клиент-сервер и объектно-ориентированный подход, обеспечивает тотальный контроль всех взаимодействий в системе.

Универсальность механизмов контроля и управления доступом ЗОС «Феникс» позволяет гарантировать соблюдение правил политики безопасности при выполнении любых операций доступа, независимо от способа его осуществления и природы защищаемых информационных ресурсов. Строгость специализированной системной архитектуры, ориентированной на обеспечение безопасности, в сочетании с ее открытостью позволяют использовать ЗОС «Феникс» при построении защищенных информационных систем в качестве базового компонента, обеспечивающего высокий уровень защиты и безусловную реализацию политики безопасности при сохранении совместимости с существующими технологиями обработки информации.

ЗОС «Феникс» является микроядерной, многопользовательской, многозадачной, многопоточной операционной системой класса UNIX. Средства обеспечения безопасности ЗОС «Феникс» не зависят от надежности работы каких-либо базовых программных средств, поскольку опираются непосредственно на аппаратные механизмы защиты, предоставляемые тридцатидвухразрядными Intel x86-совместимыми процессорами при работе в защищенном режиме.

Совместимость ЗОС «Феникс» с распространенными программными средствами обеспечивается поддержкой основных протоколов сетевого взаимодействия: TCP/IP, SMB, FTP, HTTP и др. Доступ к информационным ресурсам, находящимся под контролем ЗОС «Феникс», может осуществляться не только локально(с консоли системы), но и удаленно — с помощью стандартных клиентов сети MS Network, FTP-клиентов, Интернет-броузеров и прикладных средств, работающих по протоколам TCP/IP.

ЗОС «Феникс» может осуществлять удаленную загрузку операционных систем семейства MS Windows или Linux на рабочие места, оснащенные средствами загрузки по сети, обеспечивая неизменность состава и конфигурации их системного и прикладного программного обеспечения.

Открытость интерфейсов прикладного программирования ЗОС «Феникс» дает возможность пользователю не только расширять ее функциональные возможности, но и вводить в систему новые виды информационных ресурсов, включая их в сферу действия общесистемной политики безопасности, а также добавлять сетевые сервисы, делающие ресурсы «Феникс» доступными для приложений, использующих прикладные протоколы. Поддержка значительной части стандарта прикладного программирования POSIX позволяет портировать в среду «Феникс» прикладное программное обеспечение с платформы UNIX.

Средства защиты ЗОС «Феникс» реализуют следующие функции:

- идентификацию и аутентификацию пользователя на основе пароля с последующим предоставлением доступа к информационным ресурсам в соответствии с его полномочиями;
- контроль и управление доступом к информационным ресурсам в соответствии с дискреционной и мандатной политиками безопасности;
- регистрацию и аудит всех общесистемных событий, критических ситуаций, успешных и неуспешных попыток идентификации/аутентификации, осуществленных и отвергнутых операций доступа к информационным ресурсам, изменений атрибутов безопасности субъектов и объектов;
- локальное и удаленное администрирование, управление полномочиями пользователей в соответствии с политикой безопасности;
- контроль доступа к удаленно загружаемым автоматизированным рабочим местам;
- контроль целостности средств защиты и системных компонентов ЗОС «Феникс».

Функциональные возможности ЗОС «Феникс» позволяют использовать ее в системах обработки конфиденциальной информации не только в качестве базовой системы для автоматизированных рабочих мест, сетевой ОС для серверов хранения конфиденциальной информации и средства удаленной загрузки операционных систем на рабочие места пользователей, но и в качестве посредника между распространенными прикладными средствами и серверами, функционирующими на основе операционных систем семейства MS Windows и UNIX.

ЗОС «Феникс» может осуществлять удаленную загрузку операционных систем семейства MS Windows или Linux на рабочие места, оснащенные средствами загрузки по сети, обеспечивая неизменность состава и конфигурации их системного и прикладного программного обеспечения.

Основная задача ЗОС «Феникс» — защита систем обработки информации путем обеспечения безусловного выполнения правил системной политики безопасности для всех информационных взаимодействий с помощью средств контроля и управления доступом.

Главной архитектурной особенностью ЗОС «Феникс» является оригинальный подход к реализации контроля и управления доступом, основанный на концепциях «информационного ресурса» и «универсального интерфейса доступа», позволяющий распространить общесистемную политику безопасности на все операции доступа независимо от способа его осуществления и природы защищаемых информационных ресурсов.

Информационный ресурс — это любая обладающая уникальным идентификатором абстрактная сущность, способная участвовать в отношениях доступа в качестве источника либо приемника информации абстрактная сущность, доступ к которой осуществляется с помощью фиксированного набора операций, работающих с содержанием только одного ресурса и осуществляющих передачу информации только в одном направлении – либо от потребителя к ресурсу, либо от ресурса к потребителю.

В качестве защищаемых информационных ресурсов могут выступать файлы, html-страницы, документы, учетные записи пользователей, сетевые соединения и т.п.. Защищаемые ресурсы могут быть как локальными, так и сетевыми. Локальные ресурсы принадлежат непосредственно ЗОС «Феникс», тогда так защищаемые сетевые информационные ресурсы — это разделяемые ресурсы других систем, для работы с которыми ЗОС «Феникс» используется в качестве шлюза.

Универсальный интерфейс доступа определяет унифицированный для всех типов информационных ресурсов набор операций, включающий операции доступа к информационному содержанию ресурса, его создания, уничтожения и управления свойствами, в том числе атрибутами безопасности.

Представление защищаемой информации в виде информационных ресурсов позволяет контролировать все виды информационных взаимодействий, а благодаря использованию универсального интерфейса доступа механизмы защиты ЗОС «Феникс» инвариантны как по отношению к способам осуществления доступа, так и к различным типам информационных ресурсов.

Построенные на базе предложенных подходов механизмы защиты позволяют ЗОС «Феникс» решать задачи защиты информации от несанкционированного доступа и соблюдения правил политики безопасности для авторизованных пользователей.

Пользователи могут работать за консолями ЗОС «Феникс» или осуществлять доступ к ресурсам, находящимся под управлением ЗОС «Феникс», с помощью стандартных средств из состава других ОС. Независимо от способа осуществления доступа и используемых средств пользователь может осуществлять доступ только в рамках своих полномочий и действующих для

него ограничений. Администрирование ЗОС «Феникс» может осуществляться как локально с консоли, так и удаленно — с помощью специальных утилит, входящих в состав ЗОС «Феникс», но функционирующих на платформе Win32.

В основе системной архитектуры ЗОС «Феникс» лежат предложенные автором принципы феноменологического подхода применительно к операционной системе. Поскольку основной задачей ЗОС «Феникс» является обеспечение безопасности, все ее компоненты в той или иной степени участвуют в реализации функций защиты.

Наличие обоснованной архитектуры составляет принципиальное отличие ЗОС «Феникс» от традиционных защищенных систем, представляющих собой доработку систем общего назначения, но сохранивших при этом все недостатки, присущие их архитектуре.

Архитектура ЗОС «Феникс» является главным механизмом обеспечения безопасности, поскольку гарантирует всеобъемлющий и непрерывный контроль всех информационных взаимодействий, составляющий основу функционирования всех средств защиты.

Основу ЗОС «Феникс» составляет отвечающая принципу *абсолютности* микроядерная архитектура, предусматривающая единственный способ взаимодействия между компонентами системы с помощью механизма обмена сообщениями, реализованного в микроядре. Встроенные в этот механизм средств защиты пропускают через себя все потоки сообщений, что гарантирует тотальный контроль всех взаимодействий в системе.

В соответствии с принципом *инвариантности* все взаимодействия между компонентами ЗОС «Феникс» осуществляются на основе технологии клиент-сервер, четко регламентирующей роли взаимодействующих сторон не зависимо от его природы, типа и способа осуществления доступа.

В качестве инициатора взаимодействия выступает процесс-клиент, являющийся субъектом, а исполнителем операции является процесс-сервер. Для обозначения предмета осуществления операции используется понятие ресурса как абстрактного представления объекта доступа.

В зависимости от источника происхождения и способа осуществления доступа ресурсы разделяются на аппаратные и информационные.

Аппаратные ресурсы – это ресурсы оборудования вычислительной системы, непосредственно потребляемые процессами (оперативная память, процессорное время, порты ввода-вывода и т.п.) и предоставляемые в их распоряжение микроядром.

Под информационным ресурсом понимается реализованная программными средствами абстракция любого уровня(файл, каталог, сокет, пространство жесткого диска, учетная запись пользователя и т.д.), обладающая уникальным идентификатором, инкапсулированная в некоторый программный объект, предоставляющий фиксированный набор методов для доступ к ней. В ЗОС «Феникс» этот объект реализуется в виде процесса-сервера, который

представляет совокупность однотипных ресурсов. Информационные ресурсы, в отношении которых действует политика безопасности, называются объектами.

Процессы-серверы обслуживают запросы процессов-клиентов на использование ресурсов, представляющих средства и возможности системы, путем обслуживания исходящих от них запросов к этим ресурсам. В этой схеме все взаимодействия принимают форму обращения процессов-клиентов к ресурсам, которые обслуживаются процессами-серверами.

Поскольку все информационные ресурсы ЗОС «Феникс» находятся под контролем процессов-серверов, обрабатывающих запросы на использование этих ресурсов, поступающие от процессов-клиентов, субъектом доступа всегда является процесс-клиент, представляющий пользователя системы, а объектом — ресурс, поддерживаемый процессом-сервером. Существует единственный механизм взаимодействия — посылка сообщения, содержащего идентификаторы субъекта, объекта и запрашиваемой операции.

В соответствии с принципом *унификации* доступ к информационным ресурсам ЗОС «Феникс» осуществляется с помощью универсальных операций "Унифицированного интерфейса доступа к информационным ресурсам". УНИДИР определяет множество универсальных для всех типов информационных ресурсов операций доступа к содержащейся в них информации, создания, уничтожения ресурсов и управления их свойствами. Все операции УНИДИР однозначно отображаются на отношения доступа, регламентируемые моделями безопасности, используемыми в ЗОС «Феникс». Использование УНИДИР является единственным способом осуществления операций над объектами.

Микроядерная архитектура, взаимодействие по технологии клиент-сервер, концепция ресурсов и УНИДИР гарантируют всеобъемлющее и непрерывное функционирование средств защиты ЗОС «Феникс» реализуя принцип *толерантности*.

Средства аутентификации обеспечивают доступ к системе только авторизованных пользователей. Процесс, выполняющийся от имени пользователя и обладающий его полномочиями, осуществляет доступ к ресурсам ЗОС «Феникс» под обязательным контролем средств идентификации, которые определяют соответствующий ему субъект доступа.

Все обращения к информационным ресурсам осуществляется под контролем средств управления доступом, которые обеспечивают выполнение правил политики безопасности при доступе к тем информационным ресурсам, которые являются объектами.

Средства контроля за потреблением аппаратных ресурсов ограничивают их потребление в соответствии с полномочиями субъектов и обеспечивают работу остальных средств защиты.

Все операции доступа к ресурсам (как успешные, так и неуспешные) заносятся в протокол аудита.

Средства контроля целостности обеспечивают целостность средств защиты и восстановление целостности информационных ресурсов.

Универсальные механизмы контроля и управления доступом ЗОС «Феникс» позволяют использовать ее как платформу для создания средств защиты и встроенного программного обеспечения защищенных программно-аппаратных комплексов.

ЗОС «Феникс» может использоваться в качестве:

- операционной системы не требующих графического интерфейса автоматизированных рабочих мест обработки конфиденциальной информации;
- сетевой операционной системы для файловых серверов, FTP-серверов, WWW-серверов, хранящих конфиденциальную информацию;
- средства контроля доступа пользователей к рабочим местам, обеспечивающего неизменность состава и конфигурации их системного и прикладного программного обеспечения с помощью механизма удаленной загрузки;
- сервера приложений, выполняющего функции шлюза доступа к серверам хранения конфиденциальной информации;
- платформы для работы средств защиты, опирающихся на базовые механизмы безопасности ЗОС «Феникс»;
- системного программного обеспечения защищенных программно-аппаратных комплексов или встроенных систем.

В пятой главе работы содержатся примеры использования ЗОС «Феникс» для построения защищенных систем на примере терминального комплекса, сервера локальной сети и информационной системы на основе СУБД Oracle.

В работе представлены результаты внедрения в ЛВС сервера безопасности терминальных станций на базе ОС «Феникс», обеспечивающего для станций безопасную среду ОС Windows NT при помощи технологии удаленной загрузки. Принудительная удаленная загрузка операционной среды терминальных станций позволяет обеспечить их безопасность в условиях использования на них ПО низкой степени доверия.

Предлагаемое решение позволяет обеспечить контроль информационных взаимодействий в системе, осуществляемых с терминальных станций, при помощи средств защиты, функционирующих на платформе «Феникс», обеспечивающих достаточные средства контроля доступа, аутентификации и аудита для удовлетворения предъявляемым к комплексу требованиям по защите от НСД.

В работе приведено обоснование достаточности предлагаемой системы защиты информации требованиям класса 1Б ГТК по НСД к

автоматизированным системам в отношении обработки информации на терминальных станциях комплекса.

Благодаря совместимости с протоколами SMB, FTP и HTTP ЗОС «Феникс» может использоваться как защищенный сервер в локальных сетях(рис. 8).

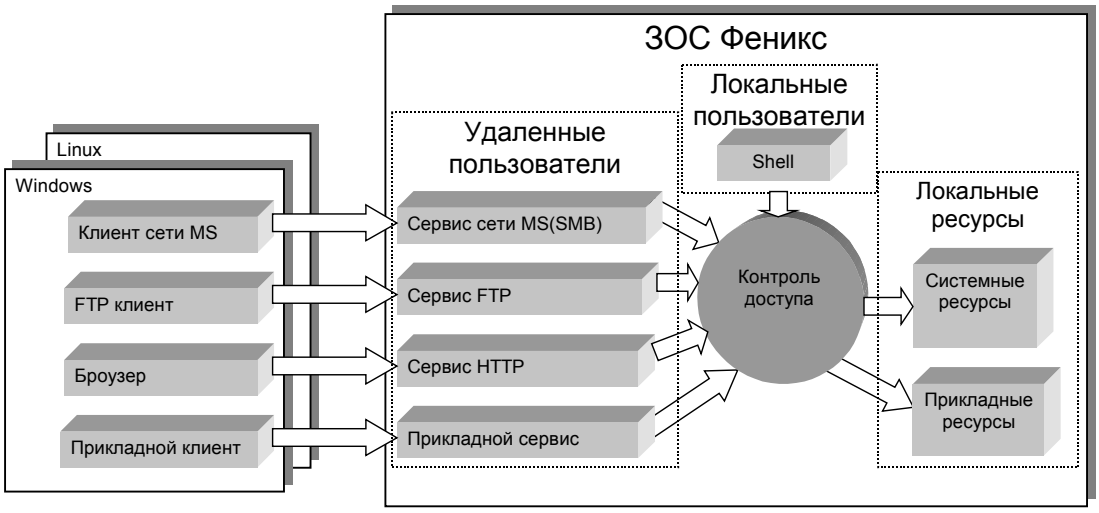

Рис. 8 Использование ЗОС «Феникс» в качестве сервера локальных сетей.

Вся защищаемая информация сосредоточена на сервере ЗОС «Феникс», который предоставляет к ней доступ для авторизованных пользователей посредством стандартных протоколов и средств удаленного доступа(клиенты сетей Microsoft, FTP-клиенты, броузеры).

В работе приводится описание защищенной распределенной информационной системы, построенной на базе СУБД Oracle8i/9i и ЗОС «Феникс», использующейся в качестве шлюза доступа к ресурсам СУБД Oracle, безопасность которой обеспечивается за счет использования специальной технологии доступа к БД (рис. 9).

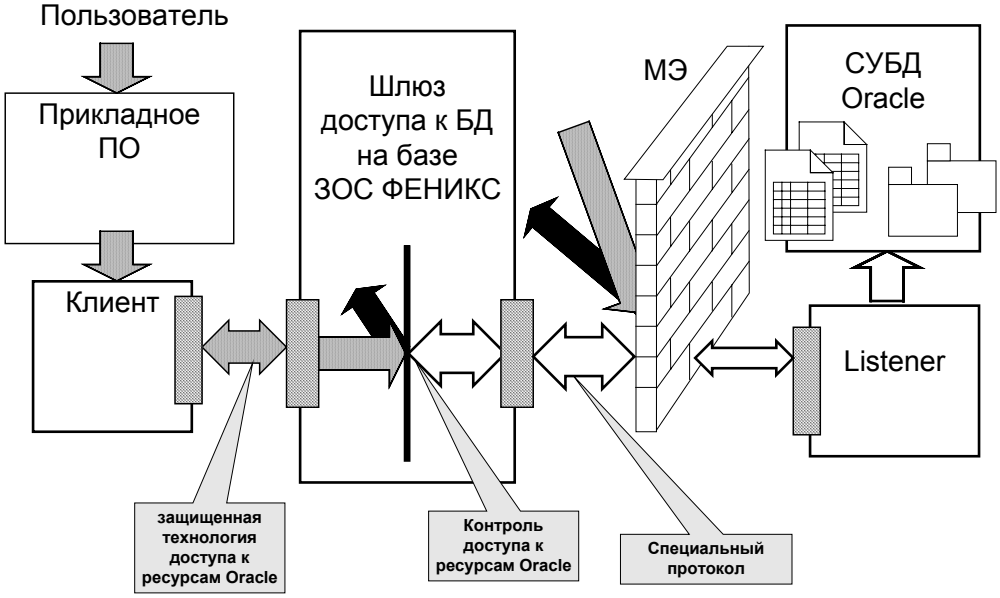

Рис. 9. Схема контроля доступа к ресурсам СУБД Oracle.

Средствами ЗОС «Феникс» обеспечиваются следующие функции:

- контроль и управление доступом к информации, хранимой в Oracle;
- управление доступом к ресурсам Oracle в терминах прикладного уровня;
- контроль целостности программных компонент схемы, отвечающих за безопасность;
- блокировка попыток нарушений безопасности;
- повышение отказоустойчивости на уровне технологии доступа к ресурсам БД и уровне средств обеспечения безопасности путем резервирования.

Представленный в работе новый подход к проблеме создания безопасных систем основан на последовательной реализации средств контроля и управления информационными потоками в соответствии с политикой безопасности, а также на практическом опыте анализа нарушений безопасности. Этот подход позволил автору предложить концепцию создания защищенных систем и технологию их разработки, что в совокупности составляет базу для развития безопасных информационных технологий и интеграции отечественных средств защиты в состав систем обработки информации.

Создание на основе предложенного подхода защищенной ОС «Феникс» на практике подтвердило правильность его принципов, а использование разработанных методов позволило достичь качественно нового уровня безопасности и получить ОС, изначально лишенную недостатков, присущих подобным системам. Создание на базе ОС «Феникс» защищенного сервера хранения информации, терминального комплекса и средства защиты информационных систем на базе Oracle подтверждает возможность ее интеграции с популярными средствами обработки информации и использования в качестве базы защищенных информационных технологий.

В приложениях содержатся документы, подтверждающие практическое использование полученных автором научных результатов, а также данные, полученные в ходе анализа уязвимостей.

Основные результаты. Совокупность сформулированных и обоснованных в диссертационной работе положений, а также ее практические результаты представляют собой основу технологии построения защищенных систем обработки информации, что имеет важное значение как для народного хозяйства, так и для повышения обороноспособности страны.

В работе получены следующие результаты:

1. Предложена и обоснована феноменологический подход к построению защищенных систем обработки информации, реализующий опережающую

стратегию защиты путем устранения источников возникновения уязвимостей и обеспечивающий толерантность ограничений на доступ к информации,

2. Разработана общая модель безопасности информационных систем и сформулированы критерии безопасности.

3. Предложены принципы технологии построения защищенных систем и методы их реализации.

4. Проведен анализ причин возникновения уязвимостей и источников их появления, дано определение понятию "уязвимость" и предложена его формальная модель. Выявлено, что основными источниками появления уязвимостей являются привилегированные программы и сервисы, в том числе средства делегирования полномочий и привилегированные интерпретаторы, а также отсутствие контроля за использованием ресурсов.

5. Разработана обобщенная модель управления доступом, позволяющая реализовать универсальные средства контроля и управления доступом, инвариантные к модели безопасности.

6. Разработан универсальный язык описаний правил моделей безопасности, основанный на логике предикатов и являющейся основой для построения процессора моделей безопасности.

7. Предложен механизм доказательства безопасности системы методом оценки достижимых состояний.

8. Реализован процессор моделей безопасности, позволяющий проводить анализ моделей безопасности путем построения полного пространства состояний системы и проверки выполнения условий моделей безопасности, автоматизирующий процесс анализа безопасности.

9. Предложенные в работе методы и принципы построения защищенных систем апробированы в ходе разработки специальной защищенной ОС.

10. Предложена технология построения безопасных систем обработки информации с использованием защищенной ОС в качестве базового компонента, обеспечивающего защиту ресурсов системы и безусловную реализацию политики безопасности при сохранении совместимости с приложениями.

Основные опубликованные работы по теме диссертации:

1. Зегжда Д. П., Семьянов П. В. Анализ средств противодействия исследованию программного обеспечения и методы их преодоления // Республиканский научно-технический семинар "Методы и технические средства защиты информации", 1993 г., тезисы докладов, СПбГТУ 1993, стр. 38.
2. Мешков А. В., Зегжда Д. П., Матвеев В. А., Семьянов П. В. "Автоматизация анализа безопасности программного обеспечения", Республиканский научно-технический семинар "Методы и технические средства защиты информации", 1993 г., тезисы докладов, Обнинск.

3. Зегжда Д. П., Семьянов П. В. Перспективные средства исследования программного обеспечения // "Безопасность информационных технологий", N 1 1994г., стр. 68.
4. Зегжда Д. П., Матвеев В. А., Молотков С. В., Мешков А. В., Семьянов П. В., под редакцией Зегжда П. Д. Основы верификационного анализа безопасности исполняемого кода программ // СПбГТУ 1994 г., 58 стр.
5. Зегжда Д. П. Объектный подход к моделированию разрушающих программ // Санкт-Петербургский семинар "Информационная безопасность", 1995 г., тезисы докладов, стр. 46-47.
6. Зегжда Д. П. Общие принципы и теоретические основы анализа безопасности программ. в сборнике "Проблемы безопасности программного обеспечения" // издание СПбГТУ, 1995 г., стр. 128-164.
7. Зегжда Д. П. Анализ безопасности программ на основе объектной модели вычислительных систем и понятия легитимности доступа // Республиканская научно-техническая конференция "Методы и технические средства обеспечения безопасности информации", СПбГТУ 1995 г., тезисы докладов, стр. 45-49.
8. Зегжда Д. П., Андреевский Н. А. Проблемы создания моделей безопасности компьютерных систем // Республиканская научно-техническая конференция "Методы и технические средства обеспечения безопасности информации", СПбГТУ 1995 г., тезисы докладов, стр. 61-63.
9. Зегжда Д. П., Ивашко А. М., Копылов Д. Ю. Анализ подходов к построению защищенных операционных систем // Республиканская научно-техническая конференция "Методы и технические средства обеспечения безопасности информации", СПбГТУ 1995 г., тезисы докладов, стр. 146-149.
10. Зегжда Д. П., Кузмич В. С., Фомин А.А. Реализация дискретной модели разграничения доступа // V Санкт-Петербургская международная конференция "Региональная информатика-96", тезисы докладов, стр. 128.
11. Зегжда Д. П. Основы технологии создания защищенных систем // Республиканская научно-техническая конференция "Методы и технические средства обеспечения безопасности информации", СПбГТУ 1996 г., тезисы докладов, стр. 68-76.
12. Зегжда Д. П. и др. Под ред. Зегжды П. Д. Теория и практика обеспечения информационной безопасности. // Издательство Агентства "Яхтсмен", М. 1996. 298 стр.
13. Зегжда Д. П. Устранение причин нарушений безопасности как метод создания защищенных систем, доклад на международной конференции "Безопасность информации", Москва 1997 г.
14. Зегжда Д. П., Ивашко А. М. Сравнительный анализ стандартов информационной безопасности // Материалы научно-практического семинара "Сеть Internet для банков — возможности и опасности" 16-19 сентября 1997 г. , г. Москва

15. Зегжда Д. П., Ивашко А. М. Как построить защищенную информационную систему. Том 1. Что такое защищенная система. // "Мир и семья 95", Санкт-Петербург, 1997г. 312 стр.
16. Зегжда Д. П. К созданию защищенных систем обработки информации // Конференция “Информационная безопасность автоматизированных систем”, Воронеж, 16-18 июня 1998 г.
17. Зегжда Д. П. Сравнительный анализ стандартов информационной безопасности. //"Проблемы защиты информации в системе высшей школы", МИФИ, Москва 1998 г.
18. Зегжда Д. П. Создание систем обработки закрытой информации на основе защищенной ОС и распространенных приложений // Республиканская научно-техническая конференция "Методы и технические средства обеспечения безопасности информации", СПбГТУ 1998 г., тезисы докладов, стр. 187-191.
19. Зегжда Д. П., Пантелеева Е. А. Применение темпоральной логики для моделирования безопасности реальных систем и оценки соответствия политике безопасности // Республиканская научно-техническая конференция "Методы и технические средства обеспечения безопасности информации", СПбГТУ 1998 г., тезисы докладов, стр. 40-43.
20. Зегжда Д. П., Калинин М. О. Реализация универсального языка описания политик безопасности // Республиканская научно-техническая конференция "Методы и технические средства обеспечения безопасности информации", СПбГТУ 1998 г., тезисы докладов, стр. 32-40.
21. Зегжда Д. П., Калинин М. О., Степанов П. Г. Теоретические основы информационной безопасности. Защищенные операционные системы. Руководство к практическим занятиям. СПбГТУ 1998 г. 70 стр.
22. Зегжда Д. П., Баранов А. П., Зегжда П. Д., Ивашко А. М., Корт С. С. Теоретические основы информационной безопасности. Дополнительные главы. Учебное пособие. СПбГТУ 1998 г. 174 стр.
23. Зегжда Д. П., Ивашко А. М. Как построить защищенную информационную систему. Том 2. // "Мир и семья", Санкт-Петербург, 1998г. 252 стр.
24. Зегжда Д. П. Анализ предпосылок нарушений безопасности в Internet // "Вестник связи", N 4, 1999 г., стр. 95-99.
25. Зегжда Д. П. Создание систем обработки закрытой информации на основе защищенной ОС и распространенных приложений // "Проблемы информационной безопасности. Компьютерные системы." N1 1999 г., стр. 106-108.
26. Зегжда Д. П., Ивашко А. М. Технология создания безопасных систем обработки информации на основе отечественной защищенной операционной системы // "Проблемы информационной безопасности. Компьютерные системы." N2 1999 г., стр. 59-74.

27. Зегжда Д. П. Использование микроядерной архитектуры для построения защищенной операционной системы. // "Проблемы информационной безопасности. Компьютерные системы." N3 1999 г., стр. 41-52
28. Зегжда Д. П., Тенихин А. Л. Применение формальных методов для доказательства безопасности и корректности программного обеспечения // Межрегиональная конференция "Информационная безопасность регионов России" "Методы и технические средства обеспечения безопасности информации", СПбГТУ 1999 г., тезисы докладов, часть 2, стр. 22-23.
29. Зегжда Д. П., Ивашко А. М., Баранов А. П. Защищенная операционная система «Феникс» //Межрегиональная конференция "Информационная безопасность регионов России" "Методы и технические средства обеспечения безопасности информации", СПбГТУ 1999 г., тезисы докладов, часть 2, стр. 172-175.
30. Зегжда Д. П., Фетисов В. А., Ухлинов Л. М. и др. Информационная безопасность таможенных технологий. Учебно-практическое пособие. Разделы 4.1-4.2. //"Синтез-Полиграф". Санкт-Петербург. 1999 г.
31. Зегжда Д. П. Общая схема мандатных моделей безопасности и ее применение для доказательства безопасности систем обработки информации // "Проблемы информационной безопасности. Компьютерные системы." N2 2000 г., СПбГТУ, стр. 89-97.
32. Зегжда Д. П., Калинин М. О. Моделирование политик безопасности для исследовательских и обучающих целей // "Проблемы информационной безопасности. Компьютерные системы." N2 2000 г., СПбГТУ, стр. 105-111.
33. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. //Горячая линия-Телеком, Москва, 2000г. 449 стр.
34. Зегжда Д. П., Калинин М. О. Моделирование защищенности компьютерных систем, основанное на множестве правил. // Республиканская научно-техническая конференция "Методы и технические средства обеспечения безопасности информации", СПбГТУ 2001 г., тезисы докладов, стр. 5-9.
35. Зегжда Д. П., Калинин М. О. Организация управления дискреционным доступом в ОС «Феникс». // II Межрегиональная конференция «Информационная Безопасность Регионов России-2001» Санкт-Петербург 2001 г., материалы конференции, стр. 101.
36. Зегжда Д. П., Калинин М. О. Тестирование дискреционного управления доступом в ОС «Феникс». // Республиканская научно-техническая конференция "Методы и технические средства обеспечения безопасности информации", СПбГТУ 2001 г., тезисы докладов, стр. 172-175.
37. Зегжда Д. П., Бундин Г.Г., Зегжда П.Д., Калинин М.О., Отавин А.Д., Степанов П.Г ОС «Феникс» – как основа построения защищенных информационных комплексов // II Межрегиональная конференция «Информационная Безопасность Регионов России-2001» Санкт-Петербург 2001 г., материалы конференции, стр. 88.

38. Зегжда Д. П., Тенихин А. Л. Использование ACL2 для доказательства соответствия функциональной спецификации средств управления доступом и модели политики безопасности на примере Trusted Mach // "Проблемы информационной безопасности. Компьютерные системы." N2 2001 г., СПбГТУ, стр. 89-97.
39. Peter D. Zegzhda, Dmitry P. Zegzhda Secure Systems Design Technology // Proceeding of International Workshop on Mathematical Methods, Models and Architectures for Network Security Systems. Information Assurance in Computer Networks. Springer 2001 pp. 63-71.
40. Dmitry P. Zegzhda, Pavel G. Stepanov, Alexey D. Otavin Fenix Secure Operating System: Principles,Models and Architecture // Proceeding of International Workshop on Mathematical Methods, Models and Architectures for Network Security Systems. Information Assurance in Computer Networks. Springer 2001 pp. 207-218.
41. Зегжда Д. П. Защищенная ОС «Феникс». Технология построения и развития. //сборник "Проблемы управления информационной безопасностью", Институт системного анализа РАН, Москва, 2002 г.
42. Зегжда Д. П., Калинин М.О. Универсальный механизм внедрения политик безопасности в защищенную информационную систему. //сборник "Проблемы управления информационной безопасностью", Институт системного анализа РАН, Москва, 2002 г.
43. Зегжда Д. П., Калинин М. О. Лабораторный практикум к дисциплине "Безопасность операционных систем" Безопасность операционных систем. Модели контроля и управления доступом. Часть I. Дискреционные модели. Издание СПбГТУ 2002 г., 104 стр.
44. Зегжда Д. П., Калинин М. О. Лабораторный практикум к дисциплине "Безопасность операционных систем" Безопасность операционных систем. Модели контроля и управления доступом. Часть II. Мандатные, информационные и комбинированные модели. Издание СПбГТУ 2002 г., 76 стр.
45. Зегжда Д. П., Калинин М.О. Математические основы построения и моделирования комбинированных политик безопасности // "Проблемы информационной безопасности. Компьютерные системы." N2 2002 г., СПбГТУ, стр. 7-14.
46. Зегжда Д. П., Гореленков А.П. Вопросы построения службы каталогов с использованием защищенной ОС «Феникс» // "Проблемы информационной безопасности. Компьютерные системы." N2 2002 г., СПбГТУ, стр. 22-30.
47. Зегжда Д. П., Таразевич С.А. Современное состояние безопасности компьютерных технологий и его причины // "Проблемы информационной безопасности. Компьютерные системы." N3 2002 г., СПбГТУ, стр. 36-47.
48. Зегжда Д. П., Калинин М.О. Алгебра составных политик безопасности // Республиканская научно-техническая конференция "Методы и технические

средства обеспечения безопасности информации", СПбГТУ 2002 г., тезисы докладов, стр. 6-8.
49. Зегжда Д. П., Калинин М.О. Оценка защищенности информационных систем // "Проблемы информационной безопасности. Компьютерные системы." N3 2002 г., СПбГТУ, стр. 92-94.
50. Зегжда Д. П. Защищенная операционная система – как ядро безопасности систем обработки информации // Республиканская научно-техническая конференция "Методы и технические средства обеспечения безопасности информации", СПбГТУ 2002 г., тезисы докладов, стр. 138-141.