На правах рукописи

Калинин Максим Олегович

АДАПТИВНОЕ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ

Специальность 05.13.19 — "Методы и системы защиты информации, информационная безопасность"

Автореферат
диссертации на соискание ученой степени
доктора технических наук

Санкт-Петербург — 2011

Работа выполнена в Государственном образовательном учреждении высшего профессионального образования "Санкт-Петербургский государственный политехнический университет"

Научный консультант:	доктор технических наук, профессор Зегжда Петр Дмитриевич
Официальные оппоненты:	доктор физ.-мат. наук, профессор Грушо Александр Александрович
	доктор технических наук, профессор Присяжнюк Сергей Прокофьевич
	доктор технических наук, профессор Хомоненко Анатолий Дмитриевич
Ведущая организация:	ОАО "Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте" (ОАО "НИИАС")

Защита состоится 14 сентября 2011 года в 14 часов
на заседании диссертационного совета Д 212.229.27
ГОУ ВПО "Санкт-Петербургский государственный
политехнический университет"
195251, г. Санкт-Петербург, ул. Политехническая, 29, Главное здание, ауд. 175

С диссертацией можно ознакомиться в библиотеке
ГОУ ВПО "Санкт-Петербургский государственный
политехнический университет"

Автореферат разослан " " 2011 г.

Ученый секретарь
диссертационного совета (Платонов В.В.)

Общая характеристика работы

Актуальность. Уровень безопасности информационных технологий, обеспечивающих хранение, доставку, обработку и представление информации, определяет надежность системы национальной безопасности. Стратегия развития информационного общества в РФ (Пр-212, 07.02.2008) к основным задачам государства относит противодействие использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам. В рамках государственных программ информатизации создаются мультитехнологичные комплексы безопасности информационных систем (ИС), интегрирующие нормативные, аппаратные и программные элементы защиты. Активное расширение областей информатизации, особенно в сегменте мобильных, распределенных и беспроводных технологий, сопровождается появлением новых угроз информационной безопасности, о чем свидетельствует статистика инцидентов, которая показывает, что ИС чрезвычайно подвержены агрессивным программным воздействиям независимо от качества и сложности применяемых мер и средств защиты. Наносимый ущерб определяется значительными экономическими потерями, связанными с простоями оборудования, непредсказуемыми нарушениями в производственных процессах, необходимостью восстановительных процедур, последствиями реализации угроз в отношении ценной информации, объектов информатизации и, в итоге, общества. Эта проблема характерна для всех критических ИС, эксплуатируемых на всех уровнях информатизации национальных институтов: от автоматизированных систем управления технологическими процессами и обработки персональных данных до электронного правительства и госуслуг.

В этих условиях становится невозможным трактовать обеспечение безопасности ИС как сохранение фиксированного состояния, безопасность которого формально доказана или подтверждена экспериментально. Потребность обеспечивать и контролировать безопасность в сложных ИС с учетом гетерогенности сред, прогнозировать поведение комплексных средств защиты и оперативно выявлять нарушения безопасности обуславливает необходимость формирования нового подхода к обеспечению безопасности как к задаче адаптивного управления динамическим процессом изменения

состояний ИС и среды ее функционирования, направленного на предотвращение выхода ИС из области состояний, удовлетворяющих требованиям безопасности. Для такого подхода актуальна проблема обеспечения устойчивой безопасности ИС, т.е. необходимость постоянно поддерживать выполнение предъявляемых к ИС требований, касающихся обеспечения стабильного функционирования (функциональной целостности ИС) и информационной безопасности.

Решение указанной проблемы заключается в создании новых методов и средств обеспечения устойчивой безопасности ИС. При этом наиболее перспективным направлением является разработка технологии управляемой информационной безопасности, согласно которой ИС и их характеристики рассматриваются как объект технического управления (далее — управления), когда состав, структура и параметры такого объекта могут контролироваться и изменяться в зависимости от воздействий. В данной области известны научные труды российских и зарубежных ученых: Будзко В.И., Гайдамакина Н.А., Герасименко В.А., Грушо А.А., Котенко И.В., Малюка А.А., Соколова И.А., Ухлинова Л.М., Маклина Дж., Самарати П., Сандху Р. В настоящее время необходимость разработки систем управления информационной безопасностью обусловлена признанием в РФ международных стандартов (например, ГОСТ Р ИСО/МЭК 13335, 17799, 27000). Известны отечественные разработки по контролю и оценке безопасности, например, средства автоматизации статического анализа защитных характеристик программ (НКВД, АИСТ), сканирования безопасности (XSpider, "Ревизор Сети"), оценки рисков (ГРИФ). Существуют зарубежные системы централизованного анализа параметров ИС (Symantec Enterprise Security Manager, MS System Center Configuration Manager, HP Open View Operations). Однако перечисленные разработки не решают обозначенную проблему в полном объеме, в частности нерешенными остаются задачи учета совокупного влияния множества факторов на работу защитных механизмов ИС, автоматизации расследования инцидентов и адаптации ИС к нарушениям безопасности. Данная работа, опираясь на указанные достижения, развивает их в следующих направлениях:

– моделирование безопасности ИС в части описания характеристик

и поведения ИС и предъявляемых к ним требований безопасности;

– автоматизация оценки безопасности и функциональной целостности ИС путем верификации предъявляемых к системам требований на множестве параметров в заданных и прогнозируемых достижимых состояниях ИС;

– выявление состава и последствий нарушений безопасности, а также активное реагирование на инциденты путем адаптации параметров ИС в соответствии с установленными причинами нарушений.

Теоретической базой для решения этих задач является построение моделей, позволяющих автоматизировать этапы управления безопасностью ИС, включая контроль, оценку и адаптацию параметров, с целью постоянного поддержания информационной безопасности и функциональной целостности ИС. Это позволяет обеспечить выполнение требований безопасности в существующих ИС и построить такие ИС, которые противостоят целенаправленным угрозам, действующим в целевых условиях эксплуатации, и при этом сохраняют постоянное соответствие предъявляемым требованиям безопасности. Тем самым, решаемая в работе задача, развивая перспективное направление по созданию принципов управления безопасностью ИС, представляет собой разновидность более общей задачи обеспечения информационной безопасности и в этой связи является актуальной в эпоху построения в РФ информационного общества, а внедрение разрабатываемых решений вносит значительный вклад в развитие экономики и повышение обороноспособности страны.

Целью работы является создание методов и средств поддержания в ИС требований безопасности в заданном диапазоне воздействий (устойчивой безопасности) с помощью разработки теоретических основ и реализации адаптивного управления безопасностью на основе логического моделирования ИС.

Для достижения данной цели в работе решались следующие задачи:

1. Определение пространства параметров, задающего представление управляемого объекта при поддержании устойчивой безопасности ИС, путем построения объектных моделей операционных сред ИС на основе анализа моделей контроля и управления доступом и механизмов защиты, реализуемых в современных операционных средах.

2. Разработка подхода к адаптивному управлению безопасностью ИС, включающему анализ параметров и выявление существующих и возможных нарушений в текущем и достижимых состояниях ИС, что позволяет определить область обеспечения устойчивой безопасности ИС.

3. Разработка теоретических основ обеспечения функциональной целостности ИС в части установления параметрической взаимосогласованности компонентов.

4. Разработка универсальной логической среды моделирования ИС, включая ее состояния, предъявляемые к ней требования, среду функционирования и работу средств защиты, позволяющей автоматизировать процедуры управления безопасностью, а именно описание всех моделируемых характеристик, верификацию требований безопасности, выявление и устранение нарушений безопасности.

5. Построение архитектуры системы адаптивного управления безопасностью ИС и реализация функций настройки, анализа, контроля и изменения параметров ИС в виде программной системы, автоматизирующей централизованное управление безопасностью для распределенных многомашинных комплексов, развернутых на платформах Windows и Unix.

Методы исследования. Для решения поставленных задач использовались теория множеств, теория графов, теория алгоритмов, теория автоматов, теория автоматического управления, теория вероятностей, методы системного анализа, анализа рисков, математической логики.

Научная новизна диссертационной работы состоит в следующем:

1. Построены объектные модели операционных сред семейств Windows и Unix, позволяющие сформировать пространство параметров, которое образует область определения требований безопасности, предъявляемых к ИС, и задает представление объекта управления безопасностью ИС.

2. Предложен и обоснован подход к адаптивному управлению безопасностью ИС, базирующийся на анализе и выявлении нарушений в текущем и достижимых состояниях ИС, что позволяет определить для ИС область устойчивого выполнения предъявляемых к ней требований безопасности.

3. Предложены интеллектуальные методы выявления нарушений безопасности в ИС на основе контроля выполнения предъявляемых к ИС требований в заданном состоянии системы и в прогнозируемом множестве достижимых состояний, оценки уровня риска информационной безопасности, вычисляемого на множестве параметров ИС, и контроля последовательностей запросов доступа.

4. Обосновано расширение понятия целостности ИС путем введения взаимосогласованности параметров как оценки безопасности ИС и разработан метод контроля функциональной целостности ИС.

5. Систематизированы методы моделирования безопасности ИС и разработана универсальная среда моделирования ИС, позволяющая посредством логических предикатов описывать функционирование ИС и предъявляемые требования, а также полностью автоматизировать адаптивное управление безопасностью ИС, включая этапы верификации требований и выработки управляющих воздействий.

6. Предложена архитектура системы автоматизированного адаптивного управления безопасностью ИС и на ее основе разработана система, реализующая инструментарий поддержания устойчивой безопасности.

Инновационный характер работы подтвержден 5 патентами РФ на изобретения.

Практическая ценность работы определяется возможностью использования полученных в ходе работы результатов для автоматизации процессов управления безопасностью ИС, включая настройку безопасности, проведение анализа безопасности, верификацию предъявляемых к ИС требований, мониторинг безопасности ИС, выявление причин нарушений безопасности и реагирование на инциденты.

Разработанные методы и средства адаптивного управления безопасностью ИС использованы в системе "Декарт" автоматизации деятельности администраторов безопасности больших вычислительных комплексов (серебряная медаль премии "За укрепление безопасности России-2008"), в программно-аппаратном комплексе управления визуализации, моделирования и мониторинга безопасности (акт ООО "НеоБИТ"). Методы

автоматизации адаптивного управления безопасностью защищенных ИС, логического моделирования, верификации политик безопасности и выработки защитных мер на основе логических моделей использованы при создании системы оперативного контроля и управления разветвленными комплексами аппаратного и программного обеспечения (акт ЗАО "Голлард"), при построении системы автоматизации настройки, анализа и управления безопасностью информационно-телекоммуникационных комплексов (акт ООО НПП "НТТ").

Теоретические и практические результаты работы используются в процессе подготовки специалистов в области информационной безопасности по дисциплинам: "Основы информационной безопасности" и "Средства обеспечения информационной безопасности в сетях передачи данных" (специальность 210403 "Защищенные системы связи", акт ГОУ ВПО "СПбГУТ"), "Безопасность операционных систем", "Основы искусственного интеллекта", "Теория и системы управления информационной безопасностью" (специальности 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем", акт ГОУ ВПО "СПбГПУ").

Результаты работы использованы в проектах ГОУ ВПО "СПбГПУ" по целевым программам Министерства образования и науки РФ (№2.1.2./3849 "Исследование влияния настроек безопасности на предоставление доступа в операционных системах семейства Windows" аналитической ведомственной целевой программы "Развитие научного потенциала высшей школы (2009-2010 годы)"; №02.740.11.0659 "Создание информационно-телекоммуникационных систем высокой доступности и защищенности" ФЦП "Научные и научно-педагогические кадры инновационной России").

Апробация работы. Основные теоретические и практические результаты диссертационной работы представлены и обсуждены на Российской научно-технической конференции "Методы и технические средства обеспечения безопасности информации" (С.-Петербург, 1998-2010 гг.); на С.-Петербургском семинаре "Информационная безопасность-99" (СПбГТУ, 1999 г.); на ведомственной конференции "Проблемы обеспечения информационной безопасности на федеральном железнодорожном транспорте" (Внедренческий центр ГУП "Аттестационный центр Желдоринформзащита МПС РФ", 2001 г.);

на Межрегиональной конференции "Информационная безопасность регионов России" (Институт информатики и автоматизации РАН, 2001-2003, 2007, 2009 гг.); на Российской научно-технической конференции "Проблемы информационной безопасности в системе высшей школы" (НИЯУ МИФИ, 2002-2004, 2006-2008 гг.); на международной научно-практической конференции "Информационная безопасность" (Таганрог, 2006-2008 гг.), на Всероссийской научно-практической конференции "Методы и средства технической защиты конфиденциальной информации" (ГОУ "ГЦИПК" Минатома РФ, 2004 г.); Межвузовском конкурсе-конференции студентов и молодых ученых Северо-Запада "Технологии Microsoft в теории и практике программирования" (С.-Петербург, 2004, 2005, 2007 гг.); на всероссийской межвузовской научно-технической конференции студентов и аспирантов "Неделя науки СПбГПУ" (СПбГПУ, 2008-2009 гг.); на международной научной конференции по проблемам безопасности и противодействия терроризму (МГУ, 2008 г.); на научном форуме "Наука и общество. Информационные технологии. Петербургская встреча Нобелевских лауреатов" (С.-Петербург, 2009 г.); на международных конференциях "State-of-the-art in Scientific Computing (PARA'04)" (Дания, 2004 г.), "Security in Information Systems" (США, 2005 г.), "Enterprise Information Systems and Web Technologies" (США, 2007, 2008, 2010 гг.), "Information Security and Privacy" (США, 2009-2010 гг.), "Mathematical Methods, Models, and Architectures for Computer Networks Security (MMM-ACNS)" (С.-Петербург, 2003, 2005, 2007, 2010 гг.).

Публикации. По теме диссертации опубликовано 136 научных работ, в том числе 1 монография, 8 учебных пособий, 1 свидетельство об официальной регистрации программы для ЭВМ, 3 заявки на выдачу патентов РФ, 5 патентов РФ на изобретения.

Основные положения, выносимые на защиту:

1. Подход к адаптивному управлению безопасностью ИС.

2. Метод контроля функциональной целостности ИС.

3. Универсальная среда моделирования ИС на основе логических предикатов.

4. Интеллектуальные методы выявления нарушений безопасности в ИС.

5. Реализация управления безопасностью ИС в виде программной системы.

Объем и структура. Диссертация состоит из введения, четырех глав, заключения, списка литературы, изложенных на 220 страницах, и приложений.

Содержание работы

Во введении сформулирована и обоснована задача разработки методов и средств адаптивного управления безопасностью ИС.

В первой главе рассмотрены основные аспекты обеспечения и поддержания безопасности современных ИС, на их основе определен объект устойчивой безопасности и обоснован подход к адаптивному управлению безопасностью ИС.

Для создания методов и средств поддержания в ИС требований безопасности в заданном диапазоне воздействий (устойчивой безопасности) необходимо сформировать пространство параметров, которое образует объект поддержания устойчивой безопасности ИС.

Исследование показало, что управление безопасностью ИС в настоящее время основано на двух подходах:

1. Нормативный подход — определение требований безопасности, предъявляемых к ИС, на базе стандартов, руководящих документов, технических условий и правил политик информационной безопасности.

2. Эксплуатационный подход — исполнение требований безопасности, предъявляемых к ИС, средствами имеющихся защитных механизмов.

Будем считать ИС безопасной в том случае, когда она соответствует определенному набору условий информационной безопасности и функционирования (требований безопасности) и противостоит целенаправленным угрозам безопасности, действующим в конкретной среде.

Нормативные документы (например, ГОСТ Р ИСО/МЭК 15408, 27000, 17799, РД Гостехкомиссии, правила политик информационной безопасности) позволяют сформировать множество требований, но не определить область их задания и объект поддержания устойчивой безопасности. Поэтому нормативный подход дополняется эксплуатационным, согласно которому требования реализуются с учетом особенностей среды эксплуатации ИС.

Анализ теоретических и практических аспектов обеспечения безопасности, связанных с базовыми моделями контроля и управления

доступом, реализуемыми в защитных механизмах операционных сред семейств Windows и Unix, которые служат платформами для развертывания современных ИС любого масштаба, позволил установить чрезвычайную сложность задачи безопасной эксплуатации ИС и постоянного соблюдения требований в заданном диапазоне воздействий. Например, в среде Windows определено порядка 30 различных типов защищаемых сущностей, для каждого экземпляра которых задается список прав доступа из 32-разрядных записей. Помимо этого существует множество уникальных атрибутов, определяемых типом объекта (например, владельцы, члены групп, привилегии). В результате, мощность пространства задействованных параметров — 10^{18}-10^{19}. Это количество многократно увеличивается в распределенных ИС. Сложность оперирования "вручную" таким пространством подтверждается тем, что ошибки, допущенные при эксплуатации ИС, в т.ч. вследствие невыполнения рекомендаций экспертов, требований производителей и регулирующих органов, неточностей в реализации правил, заданных в корпоративной политике информационной безопасности, несоблюдения единой настройки компьютеров типовых конфигураций (типовых АРМ), приводят по статистике к нарушениям безопасности, составляющим в зависимости от вида операционной среды 20-40% от общего числа инцидентов.

Анализ факторов, влияющих на безопасность ИС, показывает, что независимо от их размещения в структуре ИС (рис. 1), область задания требований связана с элементами объектной модели ИС.

<table>
<tr><td rowspan="11">Информационная система</td><td rowspan="10">Программное обеспечение</td><td rowspan="8">Операционная среда</td><td>Инициализация (загрузка)</td></tr>
<tr><td>Управление памятью</td></tr>
<tr><td>Управление процессами</td></tr>
<tr><td>Управление устройствами</td></tr>
<tr><td>Управление файловой системой</td></tr>
<tr><td>Средства идентификации и аутентификации</td></tr>
<tr><td>Контроль и управление доступом</td></tr>
<tr><td>Другие размещения</td></tr>
<tr><td rowspan="2">Сервисы и утилиты</td><td>Сервисные службы (привилегированные утилиты)</td></tr>
<tr><td>Утилиты</td></tr>
<tr><td colspan="2">Прикладные программы</td></tr>
<tr><td colspan="3">Аппаратное обеспечение</td></tr>
</table>

Рис. 1. Размещение факторов, влияющих на безопасность, в структуре ИС

Объектная модель ИС — представление ИС в виде множества характеризующих ее параметров, а именно системных сущностей (субъектов и объектов доступа), их атрибутов и значений. Например, к системным сущностям относятся пользователи, группы, процессы, файлы, каталоги, к атрибутам — привилегии, права доступа, опции безопасности приложений. С учетом этого обеспечение безопасности ИС состоит в определении состава и значений параметров, влияющих на конфиденциальность, целостность и доступность системных и пользовательских информационных ресурсов, функционирование программных компонентов, средств защиты и ИС в целом. Параметры и их значения, зафиксированные в некоторый момент времени, назовем состоянием ИС, а совокупность действий по их заданию или изменению параметров — настройкой ИС.

Необходимость в обеспечении постоянного выполнения требований безопасности в заданном диапазоне воздействий обуславливает разработку адаптивного управления безопасностью ИС, суть которого заключается в поддержании такого состояния ИС, представленного параметрами, в котором ее объектная модель согласуется с предъявляемыми требованиями.

Для обоснования подхода к адаптивному управлению безопасностью ИС, представим ИС в виде конечного автомата $\Sigma = (S^{\Sigma}, tr, s^{\Sigma}_{init}, Q)$, где S^{Σ} — множество системных состояний, $S^{\Sigma} = P \times T \times A^{T} \times V^{T}$. Состояние ИС — объектная модель, образованная множеством параметров: системных сущностей P определенных типов T с соответствующим набором атрибутов A^{T} и их значений V^{T}; Q — множество запросов, обрабатываемых ИС; $tr: Q \times S^{\Sigma} \to S^{\Sigma}$ — функция перехода из состояния в состояние, которая под действием запроса $q \in Q$ переводит систему Σ из состояния s^{Σ}_{x} в последующее состояние $s^{\Sigma}_{x+1} = tr(q, s^{\Sigma}_{x})$; s^{Σ}_{init} — начальное состояние системы. Состояние s^{Σ} назовем достижимым тогда и только тогда, когда существует последовательность $< (q_0, s^{\Sigma}_{0}), \dots, (q_n, s^{\Sigma}_{n}) >$, в которой $s^{\Sigma}_{0} = s^{\Sigma}_{init}$, $s^{\Sigma}_{n} = s^{\Sigma}$, $s^{\Sigma}_{x+1} = tr(q_x, s^{\Sigma}_{x})$, $0 \le x < n$.

Модель контроля и управления доступом M, реализованная в системе Σ, в общем случае, — кортеж $M = \{S, R\}$, где S — множество состояний модели

(состояний безопасности), R — множество правил контроля и управления доступом, имеющих форму предикатов вида $r(q,s,s')$, где $q \in Q$, $s,s' \in S$. Определим функцию pr проекции состояний, $pr: S^{\Sigma} \to S$, которая определяет соответствие между состояниями системы и состояниями безопасности. Предикаты $r(q,s,s')$ осуществляют проверку того, что в результате запроса q переход из состояния s в состояние s', т.е. срабатывание функции $s^{\Sigma\,\prime} = tr(q,s^{\Sigma})$, $s' = pr(s^{\Sigma\,\prime})$, $s = pr(s^{\Sigma})$, разрешен правилами модели контроля и управления доступом. Иными словами, переход системы Σ из состояния $s^{\Sigma} \in S^{\Sigma}$ в следующее состояние $s^{\Sigma\,\prime} \in S^{\Sigma}$ по запросу $q \in Q$ разрешен тогда и только тогда, когда для этого запроса все предикаты $r(q,s,s')$ истинны.

Требования безопасности представляют собой логически связанную совокупность критериев безопасности (КБ). Тогда свойство безопасности Λ системы Σ представляет собой кортеж $\Lambda = \{\Sigma, M, Cr\}$, где Cr — множество КБ, представленных в виде предикатов $cr(s)$, определенных на множестве состояний S и осуществляющих проверку безопасности состояния $s \in S$. Состояние $s \in S$ безопасно тогда и только тогда, когда для каждого КБ $cr \in Cr$ истинны все предикаты $cr(s)$.

Утверждение 1: В ИС Σ, реализующей модель контроля и управления доступом M, обеспечено выполнение требований безопасности в заданном диапазоне воздействий, т.е. ИС устойчиво безопасна согласно КБ, тогда и только тогда, когда выполняются оба условия:

– в ИС Σ реализованы правила модели M:

$$\forall s^{\Sigma}, s^{\Sigma\,\prime} \in S^{\Sigma}\ \exists s, s' \in S:\quad s = pr(s^{\Sigma}),\ s' = pr(s^{\Sigma\,\prime}),$$

$$\forall r \in R:\quad r(q,s,s') = \text{"ИСТИНА"};$$

– множество значений параметров заданного и любого достижимого из заданного системного состояния удовлетворяет системе КБ:

$$\forall s^{\Sigma} \in S^{\Sigma}\ \exists s \in S: s = pr(s^{\Sigma}),\quad \forall cr \in Cr:\ cr(s) = \text{"ИСТИНА"}.$$

Проверка соблюдения этих условий позволяет оценить безопасность ИС по выполнению КБ в каждом достижимом состоянии. Нарушение, в т.ч. и неизвестное, выявляется по невыполнению КБ, заданных на пространстве параметров ИС, что позволяет идентифицировать и изменить те

параметры, которые приводят к нарушению в текущем и в любом прогнозируемом достижимом состоянии ИС (пат. №2379754, №2394271). Состояние ИС, образованное множеством параметров, задает представление объекта управления при поддержании устойчивой безопасности ИС, а сформированные текущее и достижимые состояния ИС образуют область устойчивого выполнения предъявляемых к ИС требований.

Во второй главе представлены подход к адаптивному управлению безопасностью ИС и метод контроля функциональной целостности ИС.

Проверка выполнимости требований безопасности, представленная в форме утверждения 1, составляет суть адаптивного подхода, который дополняет нормативный и эксплуатационный подходы введением управления безопасностью ИС. В соответствии с утверждением 1 при осуществлении управления безопасностью ИС выполняются процедуры:

– верификация КБ в заданном состоянии;

– генерация множества достижимых состояний по заданным правилам модели контроля и управления доступом;

– рекурсивная верификация КБ в достижимых состояниях.

Выполнение этих действий гарантирует построение полного множества достижимых состояний ИС, прогнозирование изменения свойства безопасности по состояниям системы в будущем и цельную доказательную безопасность системы согласно КБ. Верификация КБ позволяет установить пространство достижимых состояний, в котором гарантированно выполняются требования безопасности, предъявляемые к ИС. Совокупность указанных процедур замыкается, образуя цикл управления безопасностью ИС по схеме с обратной связью (пат. №2399091), в которой адаптация к нарушениям безопасности осуществляется путем идентификации и изменения необходимых параметров ИС в зависимости от причин нарушений, установленных по невыполнению КБ (рис. 2). Совокупность факторов, учитываемых при этом, приведена на рис. 3.

По факту доступа субъекта к объекту, т.е. при оказании воздействия на текущее состояние безопасности ИС, выполняется фиксация параметров, состав и значения которых определяются объектной моделью операционной среды ИС. Затем выполняется оценка показателя безопасности ИС. Если его значение

индицирует нарушение безопасности, то определяется управляющее воздействие на параметры. Для этого путем сопоставления множеств текущих параметров и параметров, заданных в КБ, выявляются недостающие элементы этих множеств по каждому из требований и/или некорректно заданные/недостающие значения параметров.

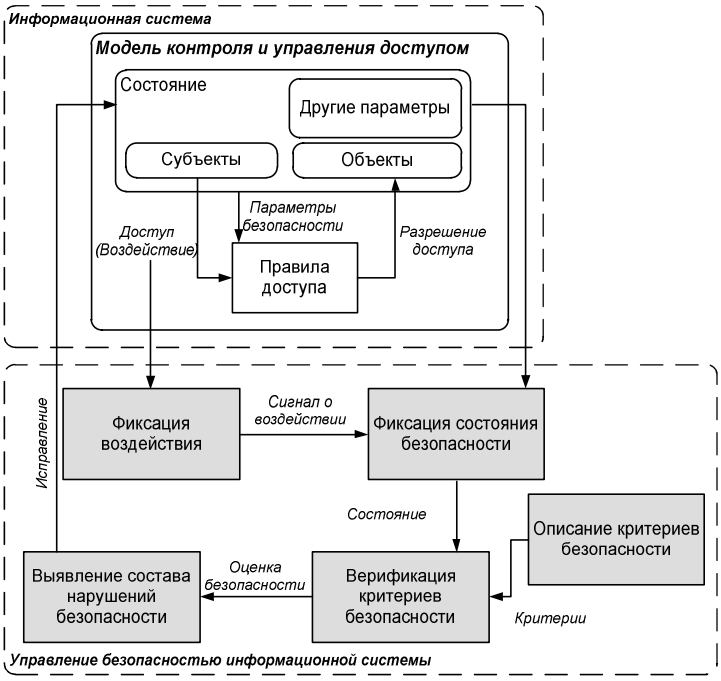

Рис. 2. Схема адаптивного управления безопасностью ИС

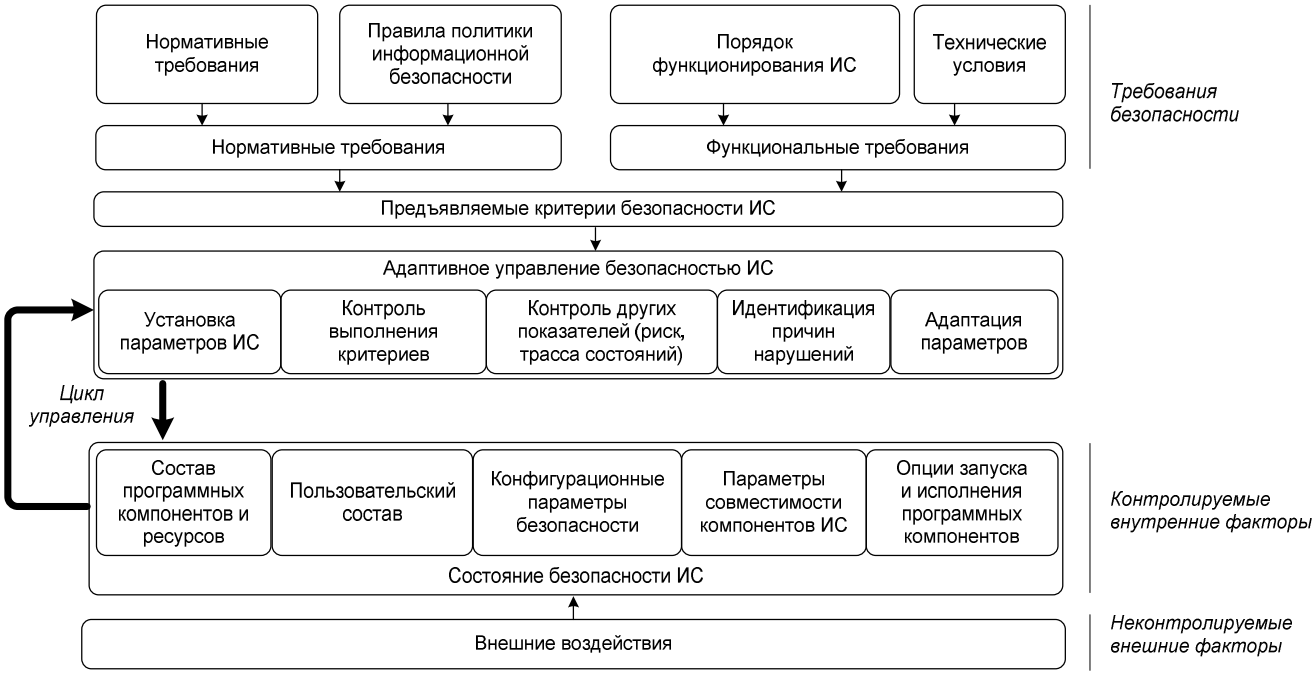

Рис. 3. Факторы адаптивного управления безопасностью ИС

Сопоставление выполняется в режимах прямого сравнения множеств (например, списков пользователей) или сопоставления эффективных множеств (например, полномочий пользователей), вычисленных с учетом иерархии и взаимного влияния параметров (пат. №2379752). После этого оказывается управляющее воздействие на текущие параметры ИС с целью устранения выявленных отклонений от КБ.

В качестве показателя безопасности ИС, по срабатыванию которого выполняется управляющее воздействие на параметры ИС, используются:

– общая индикаторная функция — статический бинарный показатель соблюдения критериев в заданном состоянии и в прогнозируемом множестве достижимых состояний ИС;

– оценка риска нарушения информационной безопасности — статический численный показатель вероятного ущерба от нарушения безопасности, рассчитанный на множестве параметров ИС;

– траектория системных состояний — показатель близости последовательностей эталонных и фактических изменений параметров (переходов состояний), характерных для нарушений безопасности.

Общая индикаторная функция, по которой выявляются нарушения в заданном системном состоянии, представляет собой логическую функцию $F(C) = C_1 \vee C_2 \vee \ldots \vee (C_k \wedge C_{k+1} \wedge \ldots)$, построенную на множестве логических индикаторных функций нарушений КБ $C = \{C_i\}$, где $i \in [1, n]$, n — количество КБ и C_i = "ИСТИНА", если КБ не выполняется. Каждой функции C_i соответствует степень $W_i \in W$, $i \in [1, n]$ критичности нарушения соответствующего КБ. В простейшем случае вид функции $F(C)$ согласован с введенными степенями критичности нарушений КБ: условия с малой критичностью составляют конъюнкцию $C_k \wedge C_{k+1} \wedge \ldots)$. Критичность нарушения КБ определяется по шкале степеней критичности. Граница между критичными и некритичными нарушениями КБ (индекс k в формуле $F(C)$) определяется путем ранжирования степеней критичности по указанной шкале.

Согласно требованиям ГОСТ Р ИСО/МЭК семейств 27000 и 17799 управление безопасностью ИС должно учитывать оценки рисков. Анализ современных методик (например, CRAMM, по ГОСТ Р ИСО/МЭК 17799)

и средств автоматизации оценки рисков (например, ГРИФ, Babel Enterprise) показал, что в них ИС рассматривается с обобщенных позиций. В современных ИС высокоуровневое описание компонентов является недостаточным, т.к. не учитывает сложную параметрическую структуру ИС и информационных ресурсов. С учетом объектной модели разработан метод оценки риска информационной безопасности на основе параметров ИС. Согласно системному подходу выполняется декомпозиция ИС на множество ее составляющих программных компонентов. Коэффициент значимости для безопасности i-го компонента, влияющего на оценку риска, рассчитывается по формуле $K_{O_i} = \frac{K_{p_i}}{K_{p_{max}}} K_{f_i}$, где K_{p_i} — коэффициент значимости, задаваемый экспертом, $K_{p_{max}}$— максимальное значение коэффициента K_{p_i}, K_{f_i} — уточняющий коэффициент, рассчитанный на основании атрибутов объектов, входящих в состав компонента. Экспертами создается база объектов и их атрибутов, а также сопоставленных с ними значений весовых коэффициентов. Эти значения сравниваются с текущими параметрами, на основании чего вычисляются уточняющие коэффициенты, которые позволяют произвести более точную оценку с учетом атрибутов каждого объекта. Уточняющий коэффициент рассчитывается по формуле $K_{f_i} = 1 - \frac{n}{\sum_{j=1}^{n}(K_{c_{i,j}} + K_{ext})K_u}$, где n — количество объектов, входящих в состав i-го компонента, $K_{c_{i,j}}$ — коэффициент значимости j-го объекта, входящего в i-й компонент. K_{ext} — коэффициент значимости типа объекта, который показывает увеличение влияния для наиболее значимых объектов (например, исполняемых файлов, драйверов) и уменьшение — для наименее значимых (например, файлов изображений, временных файлов), K_u — коэффициент значимости полномочий субъектов относительно j-го объекта, $K_u = \frac{m\sum_{h=1}^{m}(K_{u_h}\sum_{l=1}^{p}K_{pr_l})}{k}$, где m — количество полномочий, отличающихся от эталонных, k — общее количество полномочий, заданных относительно данного объекта, K_{u_h}— коэффициент значимости субъекта, заданный экспертом, K_{pr_l} — коэффициент значимости привилегии (в случае ее наличия у субъекта). Учет значимости привилегий отражает возможность получения субъектом

суперполномочий. p — общее количество учитываемых привилегий. Если интерпретировать нарушение конфиденциальности как несоответствие между эталонным и фактическим распределением прав на чтение объектов, целостности — прав на запись, доступности — прав на выполнение, то общая оценка риска для ИС представляет собой совокупность трех оценок рисков нарушений конфиденциальности, целостности и доступности, рассчитанных независимо по формуле $R = 1 - \prod_{i=1}^{g}(1 - K_{O_i})$, где g — количество анализируемых компонентов системы. В ИС не требуется изменения параметров компонентов, если полученная оценка риска не превышает допустимое граничное значение.

Поведение ИС представляется в виде траектории достижимых состояний. ИС, безопасная в одном состоянии, может оказаться небезопасной в результате последовательного изменения параметров ИС при работе пользователя, т.е. при выполнении запросов на доступ. Задача обнаружения такого рода активности состоит в том, чтобы, анализируя последовательность запросов, определить, присутствуют ли в ней признаки, характерные для той или иной атаки (разрешима и обратная задача — в случае уже произошедшей атаки, выявить траекторию изменений в параметрах ИС). В работе представлен метод обнаружения аномалий в траектории состояний ИС на основе алгоритма сопоставления генетических последовательностей. В качестве входных параметров сопоставления используются две последовательности запросов, в результате которых ИС изменяет состояние: $a = < q_{a_1}, q_{a_2}, \dots, q_{a_n} >$ и $b = < q_{b_1}, q_{b_2}, \dots, q_{b_m} >$. В качестве меры при сопоставлении отдельных запросов используется функция близости $\omega: (q_a, q_b) \to Z$, значения которой устанавливаются экспертами согласно степени опасности для ИС. Функция $R(a, b) = \sum_{i=1}^{n-1} \omega(q_{a_i}, q_{b_i})$ — общая мера сходства последовательностей запросов. Алгоритм заключается в выравнивании последовательностей запросов путем построения матрицы идентичности H размером $(m + 1) \times (n + 1)$, где m и n — длины последовательностей.

$$H(i, 0) = 0, \qquad 0 \le i \le m;$$

$$H(0, j) = 0, \qquad 0 \le j \le n;$$

$$H(i,j) = max\begin{cases} 0 \\ H(i-1,j-1) + \omega(q_{a_i}, q_{b_i}) \\ H(i-1,j) + \omega(q_{a_i}, -) \\ H(i,j-1) + \omega(-, q_{b_i}) \end{cases}, \ 1 \le i \le m, 1 \le j \le n.$$

Матрица H позволяет выравнивать последовательности запросов и сопоставлять с эталоном неполные (по части эталона) и модифицированные (с "маскирующими" запросами) последовательности, выявляя в результате отклонения в траекториях состояний ИС. В отличие от сигнатурного подхода, применяемого в настоящее время, предложенный метод контроля не зависит от ограниченного и известного множества используемых эталонов.

При адаптивном управлении безопасностью ИС для решения задачи выбора варианта управляющего воздействия с целью изменения параметров ИС разработан аналитический подход к поиску оптимального варианта безопасной настройки ИС, основанный на методе многокритериальной (векторной) оптимизации (пример критериев для операционных сред приведен в таблице, данный набор критериев может быть расширен в зависимости от назначения и типа ИС). Оптимальной является такая настройка ИС, которая максимально удовлетворяет всем перечисленным критериям.

Таблица

Соответствие критериев и способов настройки операционной среды

Критерий	Способ настройки
Сложность начальной установки параметров	Установка привилегий пользователей, настройка локальной политики безопасности
Сложность модификации параметров в связи с изменением множества объектов	Задание прав доступа непосредственно к каждому объекту
Сложность групповой настройки объектов	Установка прав доступа с включенным наследованием (распространение прав доступа по иерархии объектов)
Сложность модификации параметров в связи с изменением множества субъектов	Установка привилегий пользователей, назначение прав доступа к объектам группам пользователей
Сложность настройки сетевого взаимодействия	Настройка локальной политики безопасности

Каждый критерий представляется в виде целевой функции $f_i(x_i) = F_i$, $i \in [1,5]$, где $x_i \in X$ — множество параметров ИС, определяющих сложность настройки ИС согласно соответствующему критерию, $F_i \in R$ — показатели

сложности настройки. Задача многокритериальной оптимизации представима в виде системы $min\{f_i(x) = F_i\}, \quad i \in [1,5]$. Проведенное исследование различных методов многокритериальной оптимизации позволило обосновать применимость метода свертки векторного критерия в суперкритерий $\Phi(X) = \sum_{i=1}^{5} \alpha_i f_i(x_i)$, где $\alpha_i \in N$ — весовые коэффициенты критериев. В работе изложены способы вычисления показателей сложности настройки:

– сложность начальной установки $f_1(x_1) = \frac{\sum_{j=1}^{N_O} Perm(o_j)}{N_O}$, где x_1 определяется параметрами N_O — количеством объектов ИС, $Perm(o_j)$ — количеством пользователей, которым назначены разрешения на доступ к объекту o_j, $j \in [1, N_O]$;

– сложность модификации параметров в связи с изменением множества объектов $f_2(x_2) = Exter(O)$, где x_2 определяется множеством объектов O. $Exter(O)$ — среднее количество сторонних параметров, которое необходимо изменить при смене полномочий доступа субъекта к объекту. Под сторонними понимаются общесистемные (действующие на все объекты) параметры и параметры, которые устанавливаются на объекты, отличные от модифицируемого;

– сложность групповой настройки объектов $f_3(x_3) = \frac{N_S \sum_{j=1}^{N_O} A_{ni}(o_j)}{N_O}$, где x_3 определяется параметрами N_S — количеством субъектов, N_O — количеством объектов ИС, $A_{ni}(o_j)$ — количеством прямых полномочий, установленных к объекту o_j, $j \in [1, N_O]$;

– сложность модификации параметров в связи с изменением множества субъектов $f_4(x_4) = Exter(S)$, где x_4 определяется множеством субъектов S. $Exter(S)$ — среднее количество сторонних настроек, которое необходимо поменять при добавлении/удалении субъекта. Под сторонними понимаются настройки, которые не требуется выполнять непосредственно при создании/удалении субъекта, но которые необходимы для полноценной работы нового субъекта или для нормальной работы ИС после удаления субъекта;

– сложность настройки сетевого взаимодействия $f_5(x_5) = \frac{N_{net}}{N_S}$, где x_5 определяется параметрами N_{net} — количеством сетевых настроек, значения которых определены в ИС, и N_S — количеством субъектов.

При решении задачи настройки безопасности ИС выбор весовых коэффициентов α_i производится, исходя из назначения системы и практики ее использования, на основании таких факторов, как частота обновлений и установки программного обеспечения (ПО), создания/удаления пользователей, изменения их полномочий.

Устойчивую безопасность в ИС невозможно рассматривать в отрыве от функциональной целостности ИС. Установка новых компонентов в ходе эксплуатации ИС, изменение параметров при управлении безопасностью обуславливает необходимость в расширении понятия целостности до фиксации допустимого диапазона варьирования среды, в котором одновременно выполняются КБ и сохраняется необходимый функционал ИС. В дополнение к нормативному пониманию целостности как свойства сохранения правильности и полноты информационных активов (согласно ГОСТ Р ИСО/МЭК 13335-1) в работе введено понятие функциональной целостности ИС, т.е. взаимосогласованности параметров компонентов ИС, включая параметры системного и прикладного ПО, а также средств защиты информации (СЗИ).

Все компоненты ИС разделяются на два класса: стабильные и изменяемые. К стабильным компонентам относятся функциональные модули, которые создавались при разработке ИС. Их изменение требует дополнительного проектирования и связано с модификацией ИС, повторными испытаниями, настройками и т.д. К изменяемым компонентам относятся модули, которые могут быть произвольно модифицированы или внедрены в ИС, и этот процесс осуществляется в результате управления системой. Применение криптографических методов позволяет решить проблему целостности стабильных компонентов. В то же время в ходе управления ИС проявляются изменения, которые серьезно влияют на безопасность и стабильность функционирования ИС, но для которых криптографические методы неприменимы.

Примеры таких изменений:

– настройка безопасности установленных приложений (например, изменение опций безопасности прикладного ПО или применение пакета обновлений);

– изменение пользовательского состава, приводящее к модификации операционной среды и ее настроек (например, задание прав доступа или нового профиля пользователя).

Для обеспечения контроля функциональной целостности ИС, учитывающей параметрический состав ИС и его изменчивость в ходе функционирования системы, в работе представлен следующий метод. Состояние системы характеризуется совокупностью системных сущностей $p_i \in P$, каждая из которых задана типом $T_n \in T$ (например, на самом высоком уровне типы сущностей: операционная среда, прикладное ПО, СЗИ), множеством параметров $A^{T_n} = \{a_j^{T_n}\}$, множеством текущих значений параметров $V^{p_i,T_n} = \{v_k^{p_i,T_n}\}$, где $v_k^{p_i,T_n} = var(p_i, T_n, A^{T_n})$. Функция $var: P \times T \times A^T \to V^T$ ставит в соответствие сущности $p_i \in P$ типа $T_n \in T$, обладающей параметрами $A^{T_n} \in A^T$, их значения $V^{T_n} \in V^T$. Для формализации взаимосогласованности параметров введем функцию отображения $ref: P \times T \times A^T \times V^T \to P \times T \times A^T \times V^T$, которая для перечня параметров $a^t \in A^T$, проинициализированных значениями $v^{p,t} \in V^{p,t}$, заданной сущности $p \in P$ типа $t \in T$ указывает перечень согласующихся с ними параметров $a^{t'} \in A^T$, проинициализированных значениями $v^{p',t'} \in V^{p',t'}$, сущности $p' \in P$ типа $t' \in T$. В общем случае, для данной функции ограничение $p \neq p'$ отсутствует, так как в сложных ИС существует взаимное влияние параметров в рамках сущности одного типа (например, в операционной среде одни параметры могут отменять действие других).

Каждому значению параметров одной сущности может соответствовать не одно, а множество значений параметров другой сущности, т.е. $ref: P \times T \times A^T \times V^T \to P \times T \times A^T \times V_{\Leftarrow}^T$. Введем обратную функцию $ref^{-1}: P \times T \times A^T \times V_{\Leftarrow}^T \to P \times T \times A^T \times V_{\Rightarrow}^T$, определяющую область отображения $V_{\Rightarrow}^T$ для каждой точки из области $V_{\Leftarrow}^T$. Существование областей $V_{\Leftarrow}^T$

и $V_{\Rightarrow}^{T}$ позволяет формально определить условие функциональной целостности ИС через взаимосогласованность параметров.

Утверждение 2: для ИС, состоящей из сущностей P, область существования всех парных отношений между параметрами ИС должна составлять непустое множество:

$$\forall p \in P, \forall t \in T\ \exists a \in A^{t}: \exists p' \in P, \exists t' \in T, \exists d_{\Rightarrow} = V_{\Rightarrow}^{p,T}$$
$$\text{и}\ \exists d_{\Leftarrow} = V_{\Leftarrow}^{p,T} : ref(p, t, a^{t}, d_{\Rightarrow}) =< p', t', a^{t'}, d_{\Leftarrow} >;$$
$$ref^{-1}(p', t', a^{t'}, d_{\Leftarrow}) =< p, t, a^{t}, d' >;\ d' \cap d_{\Rightarrow} \neq \emptyset\,.$$

Пересечение всех парных областей, удовлетворяющих такому условию, образует пространство целостности. Мерой целостности является мощность пространства целостности. При этом любые парные отношения в пространстве целостности являются толерантными, т.е. рефлексивными и симметричными. Указанное свойство показывает, что предложенная модель и мера целостности сохраняются при любой комбинации элементов ИС, для которых построено пространство целостности. В качестве примера на рис. 4 схематически изображен процесс установления целостности для ИС, состоящей из трех компонентов: операционной среды, прикладного ПО и СЗИ.

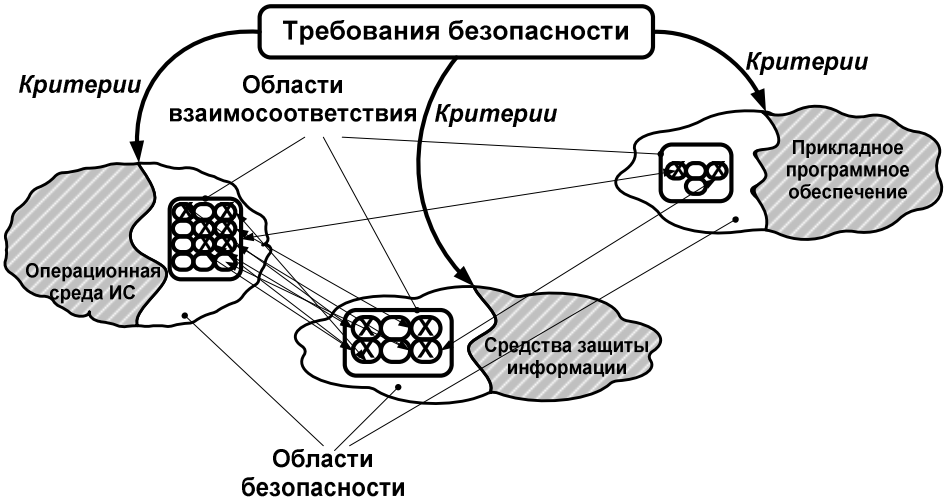

Рис. 4. Влияние параметров на целостность ИС

При одновременном соблюдении КБ в пространстве целостности образуется пространство безопасности ИС, что позволяет перейти от жесткого понимания безопасности как точечной характеристики к области параметров, в которой как соблюдаются требования информационной безопасности, так и обеспечена взаимосогласованность параметров компонентов ИС.

Если исходное множество параметров состоит из одного элемента, т.е. вся область взаимосоответствия проецируется в одну исходную точку, то ИС обладает устойчивой целостностью. Если такое условие не выполняется (существует область обратного отображения), возможны два случая:

– область обратного отображения попадает на множество параметров, не соответствующих КБ. Тогда ИС небезопасна, потенциально не целостна или несовместима;

– область обратного отображения не нарушает КБ. Тогда необходима рекурсивная проверка каждой точки из области обратного отображения в пространстве параметров одной сущности на область в пространстве параметров другой сущности для определения их пересечений. Когда область найдена, установлена область безопасности и функциональной целостности ИС.

Суть подхода продемонстрируем с помощью аппарата ориентированных трехдольных графов. Элементы трех множеств X, Y, Z (представление множеств параметров трех типов компонентов ИС на рис. 4) являются вершинами соответствующих долей графа. Направленные дуги соединяют только вершины различных долей графа. Дуга из x в y означает, что элемент $x \in X$ может давать безопасное состояние ИС только в сочетании с элементом $y \in Y$. Дуга из y в x означает, что элемент $y \in Y$ может давать безопасное состояние только в сочетании с элементом $x \in X$. Аналогичная ситуация с дугами между элементами множеств X и Z, Y и Z. Из вершины может выходить (в нее могут входить) ни одной, одна или несколько дуг.

Утверждение 3. Связь $x \to y$ существует тогда и только тогда, когда существует обратная связь $y \to x$. Поэтому трехдольный граф может быть неориентированным.

Клика в трехдольном графе — трехдольный подграф, в котором каждая вершина соответствующей доли связана со всеми вершинами двух других долей. Состояние (x, y, z) целостно, если оно — элементарная клика (треугольник в трехдольном графе). Обратно, любой треугольник дает целостное состояние ИС. Таким образом, описание безопасности ИС становится возможным не в точке, а в некоторой области так, чтобы некоторое

изменение изначально безопасного состояния по любой координате оставалось бы безопасным. Аналогом такой области в рассмотренной ИС является клика трехдольного графа. Чем больше вершин в клике, тем в большем диапазоне может изменяться состояние системы, оставаясь безопасным. Однако поскольку поиск такой клики, как и верификация КБ, является трудоемкой задачей, не выполнимой "вручную", то в работе она сводится к анализу параметров ИС на основе модели ИС.

В третьей главе проанализированы методы, используемые для моделирования безопасности ИС, и представлена универсальная логическая среда моделирования ИС, позволяющая автоматизировать цикл адаптивного управления безопасностью ИС.

Решение указанных в главах 2 и 3 задач заключается в автоматизации управляющего цикла на основе модели ИС в контексте правил контроля и управления доступом и предъявляемых требований с целью ее дальнейшей обработки в рамках верификации различного рода требований, выявления нарушений, установления и устранения их причин. С целью реализации модельной среды выполнен анализ методов моделирования безопасности ИС, в результате чего определены группы аналитических, графовых, объектных и логических методов, что позволило выделить логический метод как наиболее перспективный для представления ИС и автоматизации процедур управления безопасностью ИС.

В работе представлен логический язык описания безопасности ИС, интерпретируемый машиной вывода Пролог:

```
модель_системы::= описание_сущностей |
      описание_атрибутов_безопасности | правила_требований
описание_сущностей::=
     описание_сущности |описание_сущности, описание_сущностей
описание_атрибутов_безопасности::=
     описание_атрибута_безопасности |
     описание_атрибута_безопасности, описание_атрибутов_безопасности
правила_требований::= правило_требований |правило_требований, правила_требований
описание_сущности::=
     entity(имя_сущности, [ список_атрибутов_безопасности ]).
имя_сущности::=атом_Пролога
список_атрибутов_безопасности::=
     имя_атрибута(список_значений_атрибута) |
     имя_атрибута(список_значений_атрибута), список_атрибутов_безопасности
список_значений_атрибута::=
     значение_атрибута | значение_атрибута, список_значений_атрибута
описание_атрибута::= entityAttr(имя_атрибута).
имя_атрибута::= атом_Пролога
```

```
значение_атрибута::= атом_Пролога
правило_требований::= заголовок:-
     {проверка_атрибутов_безопасности},   другие_действия
заголовок::=
     чтение_объекта(имя_субъекта, имя_объекта) |
     запись_в_объект(имя_субъекта, имя_объекта) |
     выполнение_объекта(имя_субъекта, имя_объекта) |
     создание_объекта(имя_объекта, список_атрибутов_безопасности) |
     создание_субъекта(имя_субъекта,список_атрибутов_безопасности)|
     удаление_объекта(имя_объекта)|
     удаление_субъекта(имя_субъекта)|
     добавление_значения_атрибута_безопасности(имя_сущности,
                                имя_атрибута, значение_атрибута) |
     удаление_значения_атрибута_безопасности(имя_сущности,
                               имя_атрибута,  значение_атрибута) |
     другой_заголовок
проверка_атрибутов_безопасности::=
     checkAttr(Имя_сущности, Имя_атрибута, Значение_атрибута)
имя_субъекта::= имя_сущности
имя_объекта::= имя_сущности
другой_заголовок::= структура_Пролога
другие_действия::= предикаты_Пролога |
      элементарные_предикаты_языка_описания | предикаты_интерфейсного_уровня |
      пользовательские_предикаты.
```

В работе приведены примеры применения предложенного логического языка при моделировании всех аспектов безопасности ИС: состояний ИС, включая параметры программных компонентов (ОС, прикладного ПО и СЗИ), предъявляемых КБ, правил контроля и управления доступом, правил сопоставления состояний, правил поиска причин нарушения безопасности, правил выработки управляющих воздействий, что подтвердило применимость данного метода моделирования для широкого класса ИС.

На основе логического языка описания безопасности ИС построена универсальная среда моделирования ИС (рис. 5), которая позволяет решать следующие задачи:

– моделировать процессы, происходящие в ИС, включая процессы работы СЗИ, в виде последовательности смены состояний;

– автоматизировать процесс настройки безопасности ИС путем проецирования КБ на множество параметров ИС;

– осуществлять активный мониторинг безопасности ИС и прогнозировать нарушения безопасности, контролируя возникновение нарушений и выделяя области критических параметров;

– проверять корректность работы ИС путем определения множества контролируемых параметров и выявления небезопасных ситуаций;

– сопоставлять различные методы и средства защиты информации по их эффективности;

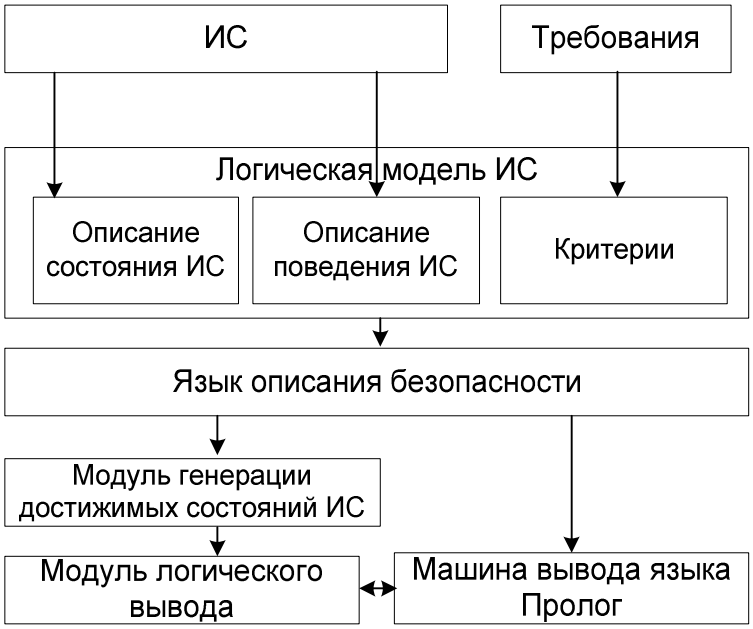

Рис. 5. Универсальная среда моделирования ИС

– анализировать риски нарушений безопасности по параметрам безопасности путем оценки критичности нарушений безопасности ИС при реализации различных угроз;

– моделировать взаимодействие систем нападения и защиты путем построения сценариев атак и мер противодействия.

Достоинства универсальной среды моделирования ИС:

– возможность экспериментальной проверки адекватности модели;

– возможность управления степенью адекватности за счет увеличения степени гранулярности при иерархическом представлении ИС;

– возможность распространения на информационно-телекоммуникационную среду при построении более сложной модели, учитывающей протоколы взаимодействия различных ИС, средств сетевой и аппаратной защиты;

– возможность реализации правил модели в виде ПЛИС для обеспечения высокой скорости принятия решений.

В четвертой главе представлено применение предложенных автором решений при разработке комплексной системы, автоматизирующей адаптивное управление безопасностью ИС.

Состав системы, реализующей инструментарий адаптивного управления безопасностью ИС и поддерживающей устойчивую безопасность

в распределенных многомашинных комплексах, развернутых на платформах Windows и Unix (пат. №2390839, №2399091) (рис. 6):

– агенты управления параметрами безопасности;
– редактор политик безопасности;
– логический процессор безопасности;
– модуль генерации отчетов;
– консоль управления;
– модуль сетевого взаимодействия и безопасности.

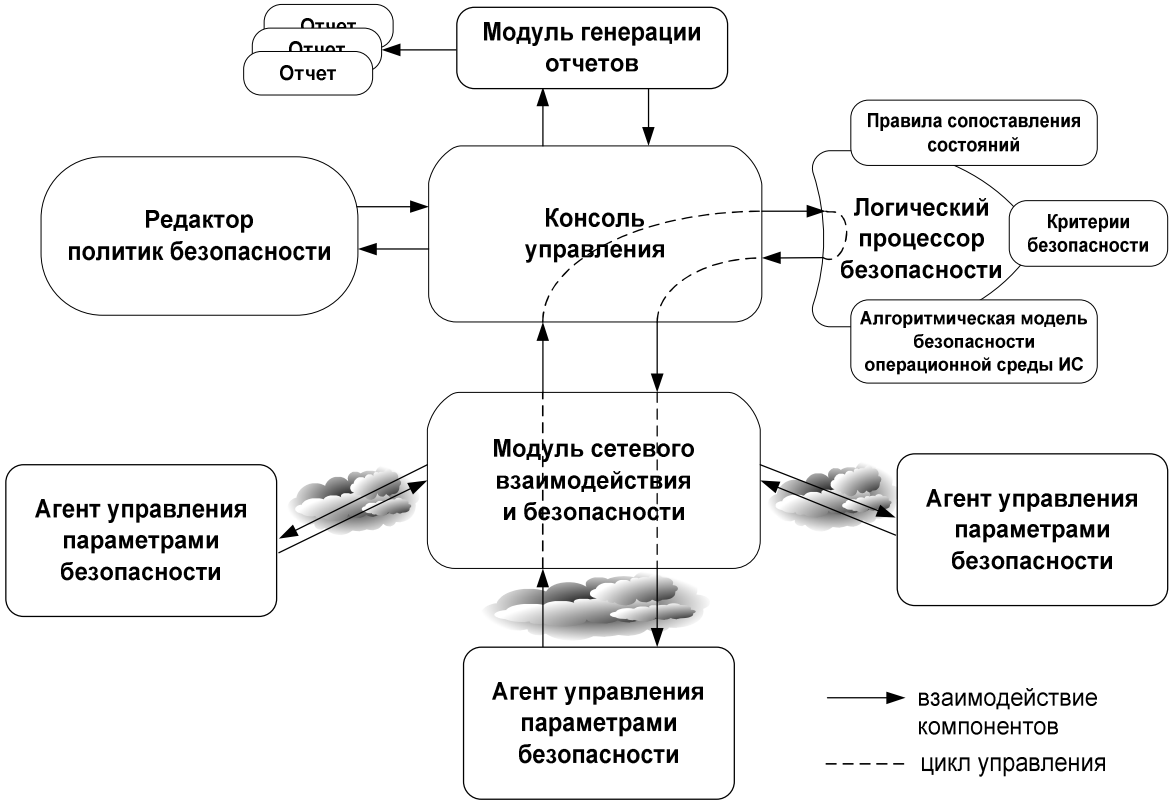

Рис. 6. Архитектура системы автоматизированного управления безопасностью ИС

Агенты управления параметрами безопасности выполняют функции настройки и фиксации значений параметров ИС. Агенты устанавливаются на удаленные компьютеры сети и взаимодействуют с консолью управления. Зафиксированное состояние безопасности представляет собой файл, который содержит информацию о собранных параметрах ИС, представленную в виде логических предикатов на языке описания безопасности ИС. Каждый предикат описывает определенный субъект или объект защиты, его атрибуты

безопасности и их значения. Например, в среде Windows агенты собирают информацию о пользователях, группах, файлах, каталогах, ключах реестра, процессах, объектах синхронизации и их атрибутах: учетных записях, правах доступа и т.д.

Модуль сетевого взаимодействия и безопасности обеспечивает установку/удаление агентов на удаленные компьютеры, поддерживает сетевое взаимодействие с ними, реализует каталогизацию и безопасность сохраняемых файлов состояний, файлов проверяемых КБ и создаваемых описаний правил политик информационной безопасности, отчетов с результатами работы и служебной информации. Описание проверяемых КБ создается в полуавтоматическом режиме. При помощи редактора политик безопасности эксперт составляет логическое описание правил путем задания КБ на множестве параметров ИС и требований безопасности ИС.

Файлы зафиксированного системного состояния и КБ обрабатываются в логическом процессоре безопасности. Он производит интерпретацию описаний, оценивает безопасность состояния ИС по ее параметрам в соответствии с КБ. Пространство перебора параметров определяется мощностью объектной модели и ограничивается областью определения КБ.

Если процессор безопасности выявляет нарушение безопасности в состояниях ИС, то система позволяет в терминах исследуемой ИС выявить и продемонстрировать набор параметров, который приводит к нарушению. Модуль генерации отчетов формирует описания уязвимых состояний ИС, проверенные КБ, результаты анализа безопасности. Выявленные причины нарушений безопасности устраняются путем установки новых значений параметров, соответствующих КБ.

Использование автоматизации придает объективный характер процессу управления безопасностью ИС, позволяет сократить издержки на восстановление ИС после сбоев и на администрирование. Разработанный инструментальный комплекс применим при создании новых защитных механизмов ИС, при верификации и исследовании СЗИ, при сертификации ИС и их классификации в соответствии с государственными нормативами, а также для выявления параметров ИС, не соответствующих требованиям.

Построенная система позволяет добиться значительного прироста производительности труда персонала, повышения качества обнаружения нарушений безопасности, тем самым обеспечивая экономический эффект от внедрения технологии адаптивного управления безопасностью ИС.

Результаты, полученные при реализации такой системы, и сама система неоднократно демонстрировались на различных конференциях и семинарах. Системе "Декарт" (св-во об офиц. рег. №2007613805), решающей указанную задачу в локальных сетевых комплексах, присуждена серебряная медаль премии "За укрепление безопасности России" (2008 г.).

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

В приложениях представлены описания объектных моделей современных операционных сред, алгоритмическая модель контроля и управления доступом, построенная для сред семейства Windows, алгоритм верификации правил политик информационной безопасности, реализованный в системе "Декарт".

В работе получены следующие основные результаты:

1. Проанализированы модели контроля и управления доступом и механизмы защиты, реализуемые в современных операционных средах ИС, что позволило построить объектные модели операционных сред ИС и, в свою очередь, определить пространство параметров, образующее область определения КБ и представление объекта управления при поддержании устойчивой безопасности ИС.

2. Предложен и обоснован подход к адаптивному управлению безопасностью ИС, базирующийся на анализе и выявлении существующих и возможных нарушений безопасности на множестве параметров ИС.

3. Разработаны интеллектуальные методы выявления нарушений безопасности в ИС: на основе контроля предъявляемых к ИС требований в заданном системном состоянии и в прогнозируемом множестве достижимых состояний, оценки уровня риска информационной безопасности, рассчитанного на основе множества параметров ИС, контроля траекторий состояний на основе сопоставления последовательностей запросов доступа.

4. Расширено понятие "целостность" путем введения оценки

безопасности ИС с позиций взаимосогласованности параметров компонентов ИС. Это позволило разработать метод контроля функциональной целостности ИС, дополняющий функциональный базис системы управления безопасностью мониторингом параметрической совместимости компонентов. Метод контроля функциональной целостности ИС позволяет повысить надежность ИС в целом.

5. Исследованы методы моделирования безопасности ИС, что позволило разработать логический язык описания безопасности ИС. Язык положен в основу разработанной универсальной среды моделирования ИС, которая позволяет построить систему логических моделей и на базе этого автоматизировать этапы адаптивного управления безопасностью ИС.

6. Разработана архитектура системы адаптивного управления безопасностью ИС, включающей все функции управления от настройки параметров до реагирования на нарушения безопасности.

7. Разработанные методы управления безопасностью ИС реализованы в виде программного инструментария, автоматизирующего централизованное выполнение процедур адаптивного управления безопасностью для распределенных многомашинных комплексов, построенных на базе платформ Windows и Unix, и обеспечивающего поддержание в них устойчивой безопасности.

Результаты диссертационной работы изложены в 136 печатных трудах. Основные из них:

Монографии и учебные пособия

1. Калинин, М. О. Безопасность компьютерных систем / М. О. Калинин / СПб. : Изд-во Политехн. ун-та, 2010. – 220 с. (13,75 п.л.).

2. Калинин, М. О. Теоретические основы компьютерной безопасности. Применение методов искусственного интеллекта : лаб. практикум / М. О. Калинин. – СПб. : Изд-во Политехн. ун-та, 2010. – 97 с. (6,1 п.л.).

3. Калинин, М. О. Безопасность операционных систем. Модели контроля и управления доступом : лаб. практикум. Ч. 1. Дискреционные модели / Д. П. Зегжда, М. О. Калинин. – СПб. : Изд-во СПбГПУ, 2003. – 104 с. (6,5/3,25 п.л.).

4. Калинин, М. О. Безопасность операционных систем. Модели контроля

и управления доступом : лаб. практикум. Ч. 2. Мандатные, информационные и комбинированные модели / Д. П. Зегжда, М. О. Калинин. – СПб. : Изд-во СПбГПУ, 2003. – 76 с. (4,75/2,4 п.л.).

Статьи в журналах Перечня ВАК

5. Калинин, М. О. О решении проблемы выбора актуальных мер защиты на примере управления информационной безопасностью серверного программного комплекса / М. О. Калинин // Проблемы информационной безопасности. Компьютерные системы. – 2010. – №1. – С. 16-26. (0,7 п.л.).

6. Калинин, М. О. Методология оценки эффективности управления информационной безопасностью и оптимизации рабочей безопасной конфигурации для операционных сред / М. О. Калинин, Д. А. Москвин // Проблемы информационной безопасности. Компьютерные системы. – 2010. – №1. – С. 27-31. (0,3/0,15 п.л.).

7. Калинин, М. О. Парадигма параметрического управления безопасностью информационных систем / М. О. Калинин // Проблемы информационной безопасности. Компьютерные системы. – 2009. – №1. – С. 25-33. (0,6 п.л.).

8. Калинин, М. О. Автоматическое управление информационной безопасностью как технология обеспечения целостности защищенных информационных систем / М. О. Калинин // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2009. - №1(19). – Ч.2. – С.43-45. (0,18 п.л.).

9. Калинин, М. О. Параметрическое управление кибербезопасностью UNIX-систем / М. О. Калинин // Труды Института системного анализа Российской академии наук (ИСА РАН). Т. 41. Управление рисками и безопасностью. – М. : ЛЕНАНД, 2009. – С. 147-157. (0,7 п.л.).

10. Калинин, М. О. Обеспечение доверенности информационной среды на основе расширения понятия "целостность" и управление безопасностью / Д. П. Зегжда, М. О. Калинин // Проблемы информационной безопасности. Компьютерные системы. – 2009. – №4. – С. 7-16. (0,6/0,3 п.л.).

11. Калинин, М. О. Оценка киберрисков на множестве параметров безопасности ОС Windows XP/2003 / Р. А. Абдульманов, М. О. Калинин // Проблемы управления рисками и безопасностью: Труды Института системного анализа Российской академии наук (ИСА РАН). Т. 31. – М.: Изд-во ЛКИ, 2007. – С. 208-215. (0,5/0,25 п.л.).

12. Калинин, М. О. Нахождение оптимального варианта настройки параметров безопасности в ОС Windows / Д. А. Москвин, М. О. Калинин // Проблемы информационной безопасности. Компьютерные системы. – 2007. – №2. – С. 32-38. (0,4/0,2 п.л.).

13. Калинин, М. О. Структура и применение языка описания политик безопасности / М. О. Калинин // Проблемы информационной безопасности. Компьютерные системы. – 2002. – №1. – С. 18-26. (0,6 п.л.).

Патенты и свидетельства

14. Способ сопоставления состояний безопасности операционных систем семейства Windows : пат. 2379752 Рос. Федерация : МПК 7 G06F21/22 / Д. П. Зегжда, М. О. Калинин – №2008129212/09 ; заявл. 26.06.2008 ; опубл. 20.01.2010, Бюл. №2. – 11 с. (0,7/0,35 п.л.).

15. Способ автоматической оценки защищенности информационных систем и система для его осуществления : пат. 2379754 Рос. Федерация : МПК 7 G06F 21/22 / Д. П. Зегжда, П. Д. Зегжда, М. О. Калинин – №2008129213/09 ; заявл. 26.06.2008 ; опубл. 20.01.2010, Бюл. №2. – 17 с. (1,0/0,33 п.л.)

16. Способ прогнозирования и оценки безопасности достижимых состояний защищенных информационных систем : пат. 2394271 Рос. Федерация : МПК 7 G06F 21/00 / Д. П. Зегжда, П. Д. Зегжда, М. О. Калинин – №2008143299/09 ; заявл. 23.10.2008 ; опубл. 10.07.2010, Бюл. №19. – 15 с. (0,9/0,3 п.л.).

17. Способ централизованных автоматизированных настройки, контроля и анализа безопасности информационных систем и система для его осуществления : пат. 2390839 Рос. Федерация : МПК 7 G06F 21/22 / Р. А. Абдульманов, Д. П. Зегжда, М. О. Калинин – №2008143281/09 ; заявл.

23.10.2008 ; опубл. 27.05.2010, Бюл. №15. – 34 с. (2,1/0,7 п.л.).

18. Способ адаптивного параметрического управления безопасностью информационных систем и система для его осуществления : пат. 2399091 Рос. Федерация : МПК 7 G06F 21/00, H04L 9/32, G06F 12/14 / Д. П. Зегжда, П. Д. Зегжда, М. О. Калинин – заявл. 27.11.2008, опубл. 10.09.2010, Бюл. №25. – 18 с. (1,12/0,38 п.л.).

19. Система "Декарт" : свид. об офиц. рег. программы для ЭВМ №2007613805 / П. Д. Зегжда, Д. П. Зегжда, М. О. Калинин – зарегистр. 06.09.2007.

Другие публикации

20. Kalinin, M. O. IT Systems Security Monitoring and Control via Advanced Concern with Integrity Property / Maxim O. Kalinin, Dmitry P. Zegzhda, Peter D. Zegzhda // International Conference on Information Security and Privacy (ISP-10) : Proceedings of the conference ; Orlando, USA. 2010. – P. 74-79. (0,38/0,13 п.л.).

21. Калинин, М. О. Технология построения систем управления информационной безопасностью / М. О. Калинин // Общерос. науч.-техн. конф. "Методы и технические средства обеспечения безопасности информации" : мат-лы конф. – СПб. : Изд-во Политехн. ун-та, 2009. – С. 50-52. (0,18 п.л.).

22. Калинин, М. О. Контроль целостности операционной среды как необходимое условие обеспечения безопасности информационно-телекоммуникационных систем / П. Д. Зегжда, М. О. Калинин // СПб научный форум "Наука и общество": Информационные технологии (4-я Петербургская встреча Нобелевских лауреатов) : тез. докл. – СПб. : СПБГУТД, 2009. – С. 344-347. (0,25/0,12 п.л.).

23. Kalinin, M. O. A New Approach to Security Evaluation of Operating Systems / Peter D. Zegzhda, Dmitry P. Zegzhda, Maxim O. Kalinin // Computer Network Security: International Workshop on Mathematical Methods, Models, and Architectures for Computer Networks Security (MMM-ACNS-2007) ; St. Petersburg, Russia. – Springer-Verlag, 2007. – P. 254-259. – (Communications in Computer and Information Science (CCIS) ; vol. 1). (0,4/0,13 п.л.).