На правах рукописи

Москвин Дмитрий Андреевич

АВТОМАТИЗАЦИЯ НАСТРОЙКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ НА ОСНОВЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Специальность:

05.13.19 – Методы и системы защиты информации, информационная безопасность

Автореферат диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург — 2010

Работа выполнена в ГОУ ВПО "Санкт-Петербургский государственный политехнический университет"

Научный руководитель:

кандидат технических наук, доцент

Калинин Максим Олегович

Официальные оппоненты:

доктор технических наук, профессор

Саенко Игорь Борисович

кандидат технических наук

Трифаленков Илья Анатольевич

Ведущая организация:

ГОУ ВПО "Санкт-Петербургский университет телекоммуникаций им. проф. М.А. Бонч-Бруевича"

Защита состоится "___" _____ 20__ г. в __ часов
на заседании диссертационного совета Д 212.229.27 ГОУ ВПО "Санкт-Петербургский государственный политехнический университет" 195251, Санкт-Петербург, ул. Политехническая, 29, Гл. здание, ауд. ____

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

Автореферат разослан "___" _____ 20__ г.

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

Общая характеристика работы

Актуальность. Обеспечение безопасности компьютерных систем (КС) в наши дни становится все более актуальным в связи с постоянным развитием информационных технологий и появлением новых способов хищения, искажения информации, нарушения работоспособности КС. При этом штатное функционирование государственных и коммерческих КС становится невозможным без постоянного поддержания их конфиденциальности и целостности. Наряду с развитием информационных технологий растут и требования к поддержанию безопасности. Одновременно статистика свидетельствует о росте количества инцидентов, основными причинами которых являются недостатки в разработке и эксплуатации средств защиты. Эта проблема особенно остро стоит в критических КС: в системах управления производством, движением, финансовыми операциями, обработки категорированной информации.

Настройка безопасности КС "вручную" влечет множество проблем. Количество конфигурационных параметров защиты в современных операционных системах (ОС) (пользователей, файлов, каталогов, ключей реестра и др.) исчисляется сотнями тысяч, а при настройке безопасности локальной сети — ещё многократно возрастает. Поэтому для задания всех необходимых параметров "вручную" администратору требуется очень большое количество времени. Также в этом случае не существует механизма гарантии того, что администратор настроил систему в соответствии с предъявляемыми требованиями по безопасности (например, согласно корпоративной политике безопасности (ПБ)). Даже при высокой квалификации администратора безопасности сохраняется высокая вероятность возникновения ошибок, связанных с "человеческим фактором". Поэтому актуальна задача автоматизации процесса настройки безопасности КС.

Настройке безопасности КС посвящено множество исследований российский и иностранных ученых, таких как А. И. Щеглов, Д. П. Зегжда, Л. М. Ухлинов, В. И. Будзко, Ф. Шнейдер, М. Сломан, Р. Сандху, В. Клиффорд. Также существуют различные программные средства для автоматизированного применения ПБ и проверки её выполнения (Microsoft Baseline Security Analyzer, Symantec Enterprise Security Manager, Positive

Technologies MaxPatrol и др.) при настройке безопасности ОС. Основными недостатками существующих решений являются неполная (частичная) настройка ПБ и отсутствие комплексного подхода, учитывающего взаимоувязанность различных конфигурационных параметров защиты. Как правило, существующие средства лишь копируют настройки безопасности из собственных предустановленных шаблонов.

Таким образом, необходим автоматизированный подход к настройке безопасности ОС, применение которого позволит взаимоувязано настроить все правила ПБ и при этом исключить ошибки "человеческого фактора", существенно ускорить процесс настройки, сократить затраты на обслуживание и поддержание безопасности.

Целью работы является разработка подхода к автоматизации процесса настройки безопасности КС на основе моделей, обеспечивающих взаимосвязь требований по безопасности и конфигурационных параметров защиты ОС.

Для достижения поставленной цели в работе решались следующие задачи:

1. Разработка имитационной модели подсистемы контроля доступа современных КС, связывающих значения конфигурационных параметров защиты ОС и установленных требований по безопасности.
2. Построение алгоритма автоматизированной настройки безопасности КС, результаты которой удовлетворяют требованиям по безопасности.
3. Разработка подхода к оценке эффективности настройки безопасности КС путем вычисления сложности изменения конфигурационных параметров защиты, обеспечивающих выполнение требований по безопасности.
4. Разработка методики автоматизированной настройки КС с соблюдением заданных требований по безопасности и показателей эффективности на основе решения оптимизационной задачи.
5. Построение архитектуры и разработка прототипа системы, реализующей предложенную методику автоматизации настройки безопасности КС.

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

Научная новизна диссертационной работы состоит в следующем:

1. Построена имитационная модель подсистемы контроля доступа КС на базе ОС семейства Microsoft Windows, связывающая и формализующая представление значений конфигурационных параметров защиты ОС и заданных требований по безопасности.

2. Предложен подход к автоматизации процесса настройки безопасности современных КС на основе имитационных моделей подсистем контроля доступа ОС.

3. Предложен подход к оценке эффективности настройки безопасности КС путем вычисления сложности изменения конфигурационных параметров защиты.

4. Разработан алгоритм и предложена методика автоматизированной настройки КС, обеспечивающая нахождение области устойчивых решений в отношении безопасности путем решения оптимизационной задачи.

Практическая ценность работы определяется возможностью использования полученных результатов для автоматизированной настройки современных ОС, согласно действующей ПБ и с учетом показателей качества настройки. Разработанные средства автоматизации используются во ФГУП "НИИ "Квант" и ЗАО "Голлард" для администрирования корпоративных сетей. Теоретические и экспериментальные результаты работы используются для подготовки специалистов в области защиты вычислительных систем по дисциплине "Безопасность современных информационных технологий" в ГОУ ВПО "СПбГПУ".

Апробация работы. Основные теоретические и практические результаты диссертационной работы доложены и обсуждены: на Российской научно-технической конференции "Методы и технические средства обеспечения безопасности информации" (СПбГПУ, 2004-2010 гг.), на Санкт-Петербургской межрегиональной конференции

"Информационная безопасность регионов России (ИБРР)" (Институт информатики и автоматизации РАН, 2003-2009 гг.), на Межвузовской конкурс-конференции студентов, аспирантов и молодых ученых Северо-Запада "Технологии Microsoft в теории и практике программирования" (СПбГПУ, 2005-2009 гг.), на Всероссийской научной конференции "Проблемы информационной безопасности в системе высшей школы" (МИФИ, 2007-2009 гг.), на Международной научно-практической конференции "Информационная безопасность" (ТТИ ЮФУ, 2007, 2008 гг.), на Первой молодежной конференции по проблемам информационной безопасности "ПЕРСПЕКТИВА-2009" (ТТИ ЮФУ, 2009 г.), на Всероссийской межвузовской научно-технической конференции студентов и аспирантов (СПбГПУ, 2007 г.), на Седьмой общероссийской научной конференции "Математика и безопасность информационных технологий" (МГУ, 2008 г.), на международной конференции "Региональная информатика" (СПИИРАН, 2008, 2010 гг.). Результаты работы использовались при выполнении аналитической ведомственной целевой программы "Развитие научного потенциала высшей школы (2009-10 гг.)".

Публикации. По теме диссертации опубликовано 43 научные работы, в том числе заявка о выдаче патента РФ.

Основные положения, выносимые на защиту:

1. Имитационная модель подсистемы контроля доступа ОС семейства Windows, позволяющая связать конфигурационные параметры защиты ОС и заданные требования по безопасности.

2. Решение оптимизационной задачи, позволяющей определить область конфигурационных параметров защиты, удовлетворяющих заданным требованиям по безопасности.

3. Методика автоматизированной настройки КС, обеспечивающая нахождение области устойчивых решений в отношении безопасности путем оптимизации значения показателя эффективности настройки безопасности КС.

4. Прототип системы автоматической настройки безопасности КС.

Объем и структура. Диссертация состоит из введения, четырех глав, заключения и списка литературы из 72 наименований.

Содержание работы

Во введении сформулирована и обоснована задача автоматизации процесса настройки безопасности КС.

В первой главе приведены результаты исследований по определению множества конфигурационных параметров защиты ОС семейства Windows, их взаимосвязи и взаимного влияния.

Для построения имитационных моделей подсистем контроля доступа КС, связывающих конфигурационные параметры защиты ОС и установленные требования по безопасности, необходимо провести анализ механизмов управления доступом, определить конфигурационные параметры, влияющие на безопасность КС, и значимость различных факторов доступа.

В работе приведены эксперименты для КС, построенных на базе ОС семейства Windows, в результате которых выявлены все факторы, влияющие на предоставление доступа к защищаемым объектам, и степень их влияния.

Все защищаемые сущности в ОС семейства Windows делятся на два вида:

– объекты — пассивные сущности, контейнеры информации;

– субъекты — активные сущности, осуществляющие различные виды доступа к объектам.

К субъектам ОС семейства Windows относятся учетные записи пользователей, групп пользователей, встроенных участников безопасности и компьютеров. Объектами ОС семейства Windows являются файлы, каталоги, ключи реестра, сервисы, принтеры, разделяемые ресурсы, объекты службы каталога Active Directory, объекты ядра (процессы, потоки, задания, каталоги ядра, мьютексы, семафоры, события, секции, сообщения и др.).

Доступ субъектов к объектам регулируется с помощью дискреционных списков контроля доступа. Каждый элемент списка содержит битовую маску прав доступа для определенного субъекта

(рис. 1). Значения битов в маске (соответствие битов правам доступа) определяется типом объекта.

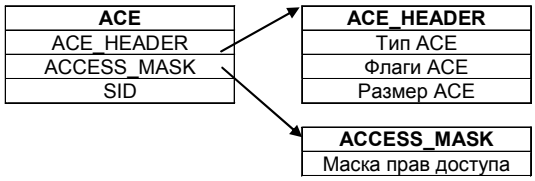

Рисунок 1 — Структура записи контроля доступа (ACE)

Помимо реализации дискреционной модели контроля доступа в ОС семейства Windows существуют и другие механизмы, влияющие на доступ субъектов к объектам. Например, у каждого объекта есть владелец — субъект, который может установить любые права доступа к этому объекту, независимо от действующих разрешений.

Механизмы, влияющие на контроль доступа в ОС семейства Windows, и алгоритмы их влияния документированы лишь частично. В рамках данного исследования определено, что все такие факторы образуют иерархию, которая представлена на рис. 2. Таким образом, при попытке осуществления субъектом доступа к объекту, механизмы защиты, использующие перечисленные факторы, работают в строгой последовательности.

Множество видов доступа к каждому объекту ограничено множеством прав доступа, специфичным для объектов этого типа. Действие всех других механизмов защиты можно спроецировать на множество прав доступа. Например, для объектов файловой системы проекцией привилегии "Архивирование файлов и каталогов" являются права доступа "Чтение данных", "Чтение атрибутов", "Чтение дополнительных атрибутов", "Чтение разрешений" и "Синхронизация".

Критериями безопасности будем называть формально описанные требования по безопасности, регламентирующие полномочия пользователей на доступ к ресурсам КС. Обычно такие требования составляются на основе действующей ПБ и профиля защиты системы.

Результат объединения множества прав доступа и множества проекций всех других факторов доступа будем называть эффективными правами объекта. Эффективные права позволяют определить реально имеющиеся полномочия на доступ у каждого пользователя.

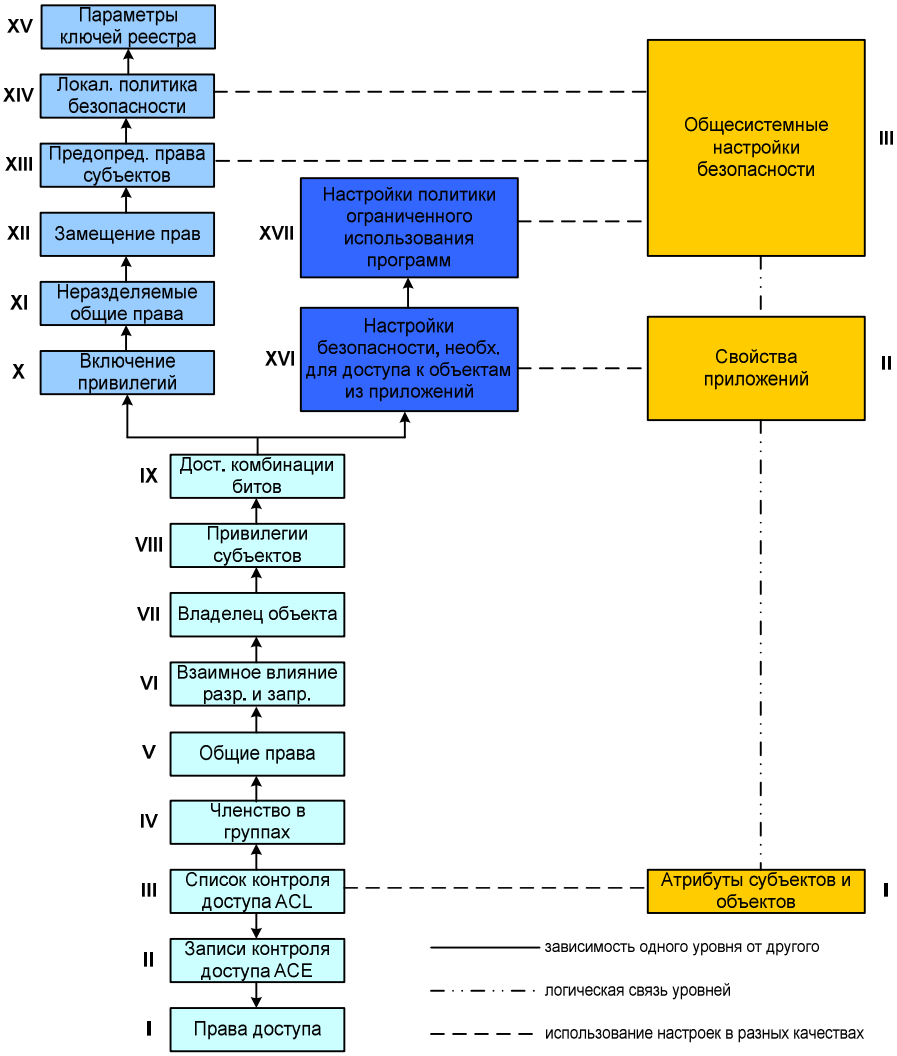

Рисунок 2 — Иерархия факторов имитационной модели подсистемы контроля доступа ОС семейства Windows

Множество видов доступа, задаваемое в критериях безопасности, также ограничено теми действиями, которые физически выполнимы с информационным ресурсом (объектом ОС). Таким образом, область определения критериев безопасности по видам доступа совпадает с множеством эффективных прав, как по числу элементов, так и по семантике.

Критерии безопасности представимы в виде логических функций следующего вида:

$$Criterion(S,O,R),$$

где S — пользователь (субъект),

O — информационный ресурс (объект),

R — разрешенный доступ (эффективные права).

Функция *Criterion()* имеет булеву область допустимых значений и принимает значение ИСТИНА, когда в КС субъект S имеет права R к объекту O, и ЛОЖЬ — в противном случае. КС настроена безопасно, т.е. находится в безопасном состоянии, когда все функции Criterion принимают значении ИСТИНА.

Исследование механизмов контроля доступа в КС на базе ОС семейства Windows позволило выделить конфигурационные параметры, влияющие на безопасность ОС, определить степень их влияния, разработать форму представления критериев безопасности и задать их область определения.

Во второй главе разработаны имитационная модель подсистемы контроля доступа ОС семейства Windows и подход к оценке эффективности настройки безопасности КС. Предложено формальное представление конфигурационных параметров защиты ОС и критериев безопасности.

Имитационная модель подсистемы безопасности ОС состоит из следующих компонентов:

– субъекты и объекты ОС;

– ПБ — совокупность правил, определяющих полномочия доступа субъектов к объектам КС;

– профиль КС — совокупность свойств КС, отражающих ее назначение и особенности функционирования.

Введем формальное представление имитационной модели подсистемы контроля доступа КС:

$$OS = \{S_1, \ldots, S_n, O_1, \ldots, O_m, SecPol, Profile\},$$

где OS — ОС,

S_i — субъект ОС; O_j — объект ОС;

n — количество субъектов в ОС;

m — количество объектов в ОС;

SecPol — ПБ;

Profile — профиль КС.

Пусть $r(S, O)$ — правило отношения доступа субъекта S к объекту O,

$R^{SP} = \{r=r(S,O)\}$ — множество правил r из ПБ *SecPol* отношения доступа субъекта S к объекту O.

$R^{Pr} = \{r=r(S,O)\}$ — множество правил r из профиля *Profile* отношения доступа субъекта S к объекту O.

Безопасная настройка КС задана функцией *SecSet*(*OS*), которая принимает значение ИСТИНА при выполнении следующих условий:

1. $\forall S, O \in OS$

   $\exists\, r=r(S,O) \in R^{SP} \vee$

   $\exists\, r=r(S,O) \in R^{Pr}$.

2. $\forall S, O \in OS$ если

   $r_1 = r_1(S,O) \in R^{SP} \wedge$

   $r_2 = r_2(S,O) \in R^{Pr} \Rightarrow$

   $\Rightarrow r_1 = r_2$.

Таким образом, КС настроена безопасно, если отношения субъектов и объектов в ней полностью соответствуют требованиям ПБ и профиля, и эти требования не противоречат друг другу.

Предложим два варианта применения имитационной модели подсистемы контроля доступа ОС:

1. Модель используется, когда необходимо проверить, выполняются ли критерии безопасности (рис. 3). На вход модели подаются конфигурационные параметры защиты системы. На выходе — действующие полномочия пользователей. Их сравнение с предъявляемыми критериями безопасности позволяет сделать вывод о том, выполняются ли эти критерии.

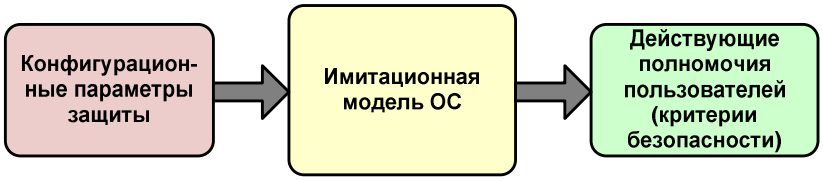

Рисунок 3 — Применение имитационной модели при проверке выполнения критериев безопасности

2. Модель используется, когда необходимо найти множество значений конфигурационных параметров защиты ОС, которые удовлетворяют заданным критериям безопасности (рис. 4). На входе модели — критерии безопасности и текущие конфигурационные параметры защиты (пользователи, файлы, ключи реестра, и т.д.), на выходе — множества (или векторы) значений конфигурационных параметров защиты, удовлетворяющих предъявляемым критериям безопасности. В общем случае таких векторов большое, но ограниченное число.

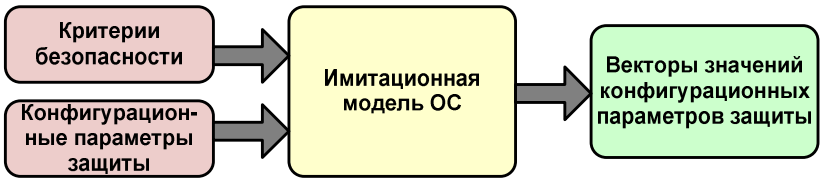

Рисунок 4 — Применение имитационной модели при настройке безопасности КС

Помимо выполнения критериев необходимо обеспечить эффективность выполняемой настройки безопасности КС. Наиболее эффективной назовём настройку, обеспечивающую наибольшее время нахождения КС в безопасном состоянии и наименьшее число необходимых изменений настройки впоследствии. Это достигается обеспечением устойчивости достигнутого безопасного состояния. Под устойчивостью понимается способность ОС сохранять безопасное состояние в ходе эксплуатации или под действием атак нарушителей.

Для оценки устойчивости безопасного состояния необходимо ввести показатель устойчивости каждого вектора настроек. В работе обоснован способ вычисления показателя устойчивости на основе подсчета

количества вызовов API-функций, которое необходимо для вывода системы из безопасного состояния, т.к. именно этими функциями пользуется нарушитель и они вызываются при использовании уязвимостей в ОС. Следовательно, для каждого вектора необходимо вычислить число шагов (вызовов API-функций) до выхода из безопасного состояния по каждой компоненте вектора настроек и по числу компонент, значения которых необходимо изменить. С этой целью для каждого конфигурационного параметра защиты требуется произвести подсчет количества вызовов API-функций, необходимого для смены состояния. При этом каждая компонента вектора обладает собственным показателем устойчивости. Затем необходимо вычислить устойчивость каждого вектора, сравнить их, и найти вектор с максимальной устойчивостью. Если максимальной устойчивостью обладают несколько векторов, то применяться для настройки безопасности КС может любой из них.

Таким образом, разработанная имитационная модель КС на базе ОС семейства Windows позволила связать конфигурационные параметры защиты ОС и критерии безопасности и предложить подход к оценке эффективности настройки безопасности КС.

В третьей главе выполнена постановка оптимизационной задачи, позволяющей определить область конфигурационных параметров защиты, удовлетворяющих критериям безопасности, разработаны алгоритм и методика автоматизированной настройки безопасности КС.

Задача оптимизации настройки безопасности ОС с учетом устойчивости в общем случае имеет следующий вид:

$$\begin{cases} SecSet(OS) = \text{TRUE} \\ Stable(r(S_i,O_j)) \to \max\limits_{\substack{i\in[1;n] \\ j\in[1;m]}} \end{cases}$$

где *Stable()* — функция вычисления показателя устойчивости, определенного в главе 2.

Для использования имитационной модели во втором варианте необходим алгоритм автоматизации настройки безопасности КС. Простейший вариант такого алгоритма — полный перебор подходящих

конфигурационных параметров защиты. Для повышения эффективности перебора применяется метод отсечения заведомо неверных вариантов. Для реализации предложенного алгоритма используется логическая машина вывода языка Пролог, что позволяет найти все решения за приемлемое время.

Тем не менее, результирующее множество векторов настроек, как правило, велико, что обусловливает необходимость в некотором дополнительном критерии. Такой критерий должен позволять оценивать и сравнивать эффективность настройки безопасности, выполненной по различным векторам настроек. Для этого предлагается использовать введенный в работе показатель устойчивости.

Для выполнения автоматизированной настройки безопасности КС разработана методика настройки системы по критериям безопасности с наибольшей устойчивостью. Данная методика включает в себя следующие основные этапы:

1. Задание критериев безопасности на основании ПБ и профиля КС.
2. Сбор информации о субъектах и объектах ОС.
3. Вычисление множества векторов конфигурационных параметров защиты ОС, удовлетворяющих критериям безопасности.
4. Вычисление показателя устойчивости для каждого из "безопасных" векторов.
5. Оптимизация — выбор вектора с наибольшим значением показателя устойчивости.
6. Выполнение настройки безопасности ОС по выбранному вектору.
7. Верификация (и затем периодическое повторение верификации) предъявляемых критериев безопасности на множестве установленных значений конфигурационных параметров защиты.

Таким образом, разработанная методика позволяет выполнять автоматизированную настройку безопасности КС, приводя её в устойчивое и удовлетворяющее критериям безопасности состояние.

В четвертой главе построена архитектура системы, реализующей предложенную методику автоматизации настройки безопасности КС, и представлены опытные результаты работы прототипа системы.

В основе разработанной системы лежит логический процессор, который на основании правил ПБ, профиля КС и описания текущих ресурсов ОС согласно имитационной модели подсистемы контроля доступа КС генерирует множество конфигурационных параметров защиты ОС (рис. 5). Работа логического процессора представлена на рис. 6.

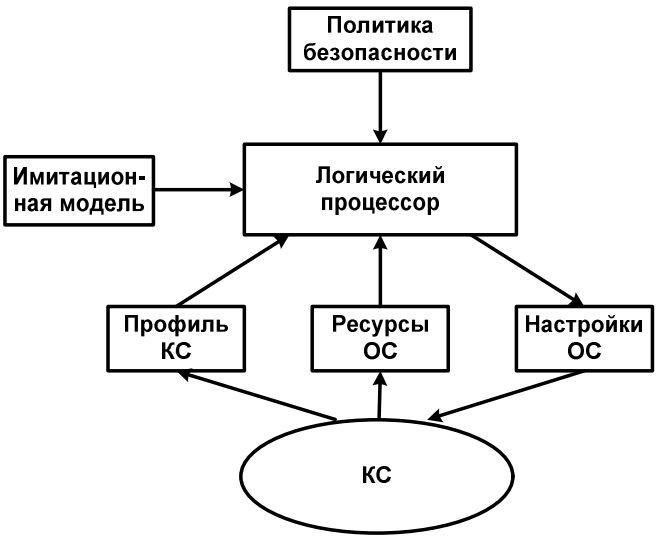

Рисунок 5 — Архитектура системы настройки безопасности ОС

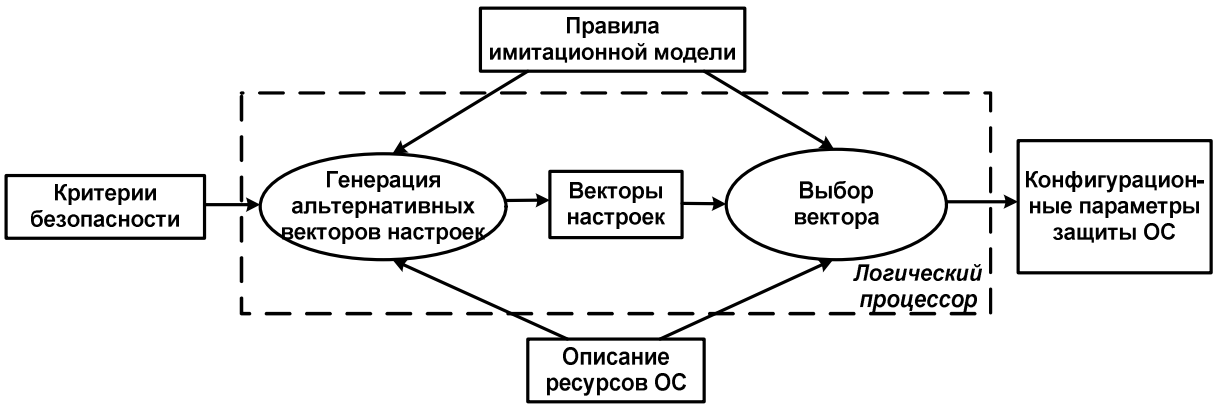

Рисунок 6 — Работа логического процессора

Применение предложенного подхода к построению множества конфигурационных параметров защиты ОС позволяет автоматизировать процесс настройки безопасности КС согласно действующей ПБ и с учетом устойчивости безопасного состояния.

Эффективность предложенного подхода и архитектуры системы автоматизированной настройки безопасности КС подтверждается полученными экспериментальными результатами. Тестирование выполнялось в корпоративной сети из 118 компьютеров, среди которых два файловых сервера, один Вэб/почтовый сервер и 115 рабочих станций. Полученные экспериментальные результаты приведены в таблице.

Таблица — Результаты применения системы автоматизированной настройки безопасности КС

Характеристика	**Настройка безопасности**		
	Разработанная система	**MS Baseline Security Analizer**	**"Ручная" настройка**
Время, затраченное на выполнение настройки безопасности	2,5 часа	1 день	1 неделя
Количество ошибок (несоответствий критериям безопасности)	0	5	11
Успешность проведения атак	2 из 50	24 из 50	18 из 50
Время до первой корректировки настройки безопасности	28 дней	2 дня	5 дней

Теоретические и экспериментальные результаты проведенных исследований использовались в рамках аналитической ведомственной целевой программы "Развитие научного потенциала высшей школы (2009-2010 годы)" и применяются для подготовки специалистов в области защиты вычислительных систем по дисциплине "Безопасность современных информационных технологий" в ГОУ ВПО "СПбГПУ".

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

В работе получены следующие основные результаты:

1. Построены имитационные модели подсистем контроля доступа КС на базе ОС семейства Microsoft Windows, связывающие значения конфигурационных параметров защиты ОС и установленных требований по безопасности.

2. Разработан алгоритм автоматизированной настройки безопасности КС.

3. Предложен подход к оценке эффективности настройки безопасности КС путем вычисления сложности изменения конфигурационных параметров защиты.

4. Разработана методика автоматизированной настройки КС с соблюдением заданных требований по безопасности и показателей эффективности на основе решения оптимизационной задачи.

5. Разработаны архитектура и прототип системы, реализующей предложенную методику автоматизации настройки безопасности КС.

Основные результаты диссертационной работы изложены в 43 печатных трудах. Ниже приведены основные из них:

1. Москвин, Д. А. Методология оценки эффективности управления информационной безопасностью и оптимизации рабочей безопасной конфигурации для операционных сред [Текст] / Д. А. Москвин, М. О. Калинин // Проблемы информационной безопасности. Компьютерные системы. — 2010. — №1. — С. 27-31.

2. Москвин, Д. А. Автоматизация настроек безопасности информационных систем [Текст] / Д. А. Москвин, М. О. Калинин // Сборник материалов XII Санкт-Петербургской международной конференции "Региональная информатика (РИ-2010)". — 2010. — С. 42-43.

3. Способ определения показателя эффективности управления безопасностью операционных систем Windows и способ оптимизации настройки безопасности операционных систем Windows : заявка №2008111237/09 Рос. Федерация : МПК 7 G06F 21/22 / Д. П. Зегжда, М. О. Калинин, Д. А. Москвин – заявл. 17.03.2008 ; опубл. 27.09.2009, Бюл. №27. – 3 с.

4. Москвин, Д. А. Оптимизации применения политик безопасности в информационно-телекоммуникационных системах [Текст] // Сборник материалов XVIII научно-технической конференции "Методы и технические средства обеспечения безопасности информации". — 2009. — С. 64-66.

5. Москвин, Д. А. Перспективы использования многокритериальной оптимизации при управлении безопасностью информационных систем [Текст] / Д. А. Москвин, М. О. Калинин // Доклады Томского государственного университета систем управления и радиоэлектроники. — 2008. — №2 (18). Ч.1. — С. 128-129.

6. Москвин, Д. А. Применение многокритериальной оптимизации при администрировании безопасности Windows [Текст] / Д. А. Москвин, М. О. Калинин // Материалы Всероссийской научной конференции "Проблемы информационной безопасности в системе высшей школы". — 2008. — С. 103-104.

7. Москвин, Д. А. Автоматизированное профилирование и настройка информационных систем при применении политик безопасности [Текст] // Материалы Общероссийской научно-технической конференции "Методы и технические средства обеспечения безопасности информации". — 2008. — С. 34.

8. Москвин, Д. А. Нахождение оптимального варианта настройки параметров безопасности в ОС Windows [Текст] / Д. А. Москвин, М. О. Калинин // Проблемы информационной безопасности. Компьютерные системы. — 2007. — №2. — С. 32-38.

9. Москвин, Д. А. Метод оптимизации настройки безопасности ОС Windows [Текст] // Материалы всероссийской конференции "Методы и технические средства обеспечения безопасности информации". — 2007. — С. 27-28.

10. Москвин, Д. А. Алгоритмическая модель подсистемы контроля и управления доступом операционной системы Windows [Текст] / Д. А. Москвин, Д. П. Зегжда, М. О. Калинин, А. Г. Лысенко // Проблемы информационной безопасности. Компьютерные системы. — 2006. — №1. — С. 26-29.