УДК 004.056

Д.А. Москвин, М.О. Калинин

Перспективы использования многокритериальной оптимизации при управлении безопасностью информационных систем

Представлен перспективный подход к поиску оптимального варианта безопасной конфигурации информационной системы, основанный на методах многокритериальной оптимизации.

В процессе управления безопасностью информационных систем администратор сталкивается с задачей выбора способа реализации правил политики безопасности. Это обусловлено большим набором различных конфигурационных параметров безопасности и, как следствие, неоднозначностью методов назначения полномочий пользователей. Такая задача актуальна для информационных систем, построенных на базе операционных систем (ОС) семейства Microsoft Windows, так как для этих ОС характерно наличие множества параметров, влияющих на работу подсистемы контроля и управления доступом, и косвенного воздействия параметров безопасности друг друга.

В ходе управления безопасностью при решении задачи выбора способа настройки безопасности администратор руководствуется содержанием требований политик информационной безопасности, а также различными характеристиками системы, такими как ее назначение, производительность и т.д. Поэтому для автоматизации решения данной задачи авторами предложен аналитический подход к поиску оптимального варианта безопасной конфигурации информационной системы, основанный на методах многокритериальной оптимизации. В этом случае критериями являются требования к системе, параметрами критериев – характеристики системы, а результатом оптимизации – набор настроек, которые необходимо установить в системе.

Для многокритериальной оптимизации используются следующие аналитические методы:

1. *Метод весовых коэффициентов.* Позволяет свести задачу многокритериальной оптимизации к задаче однокритериальной оптимизации [1]. Основан на назначении каждому частному критерию весового коэффициента, определяющего его относительную важность. Все критерии, умноженные на свои весовые коэффициенты, складывают, образуя единый скалярный критерий оптимальности, по которому производят дальнейшую оптимизацию. Перед выбором весовых коэффициентов выполняют нормализацию частных критериев, чтобы их значения были сопоставимы [2]. Недостатком метода является сложность распределения весов [3].

2. *Метод эпсилон-ограничений.* Позволяет свести задачу к однокритериальной оптимизации. Основан на выделении наиболее важного частного критерия, по которому производится дальнейшая оптимизация, и ограничении остальных критериев константами [1]. При использовании данного метода необходимо знание значений констант, которые используют для ограничения критериев. Основными недостатками этого метода является сложность выбора максимально допустимых значений частных критериев и жесткость ограничений [4].

3. *Метод последовательных уступок.* Основан на расположении частных критериев в порядке убывания их важности и назначении уступок (т.е. максимальных отклонений от оптимального значения), допустимых для каждого критерия [1]. Метод позволяет контролировать, ценой какой уступки в одном частном критерии приобретается выигрыш в другом частном критерии. Метод применяют только для решения класса задач оптимизации, в которых частные критерии упорядочены по степени важности [1].

Результаты сопоставления проанализированных методов представлены в табл. 1.

Таблица 1

Сопоставление аналитических методов многокритериальной оптимизации

Критерий сравнения	Метод весовых коэффициентов	Метод эпсилон-ограничений	Метод последовательных уступок
Использование относительной важности критериев	+	–	+
Сводимость к однокритериальной задаче	+	+	–
Необходимость нормализации критериев	+	–	+
Обязательная упорядоченность критериев	–	–	+

При управлении безопасностью информационных систем наиболее применимым является метод весовых коэффициентов, так как он позволяет учитывать относительную важность частных критериев, не требуя их строгой упорядоченности, а также свести многокритериальную задачу к однокритериальной. Основным недостатком данного метода является сложность назначения весовых коэффициентов для частных критериев, однако он устраним путем определения весовых коэффициентов на основании характеристик системы [4, 5]. Часть этих характеристик (например, сведения о производительности системы) может быть получена автоматизированным путем, а другая часть (например, назначение системы) может быть запрошена у администратора системы.

Рассмотрим в качестве примера систему, для которой весовые коэффициенты критериев задаются в зависимости от назначения системы, и при этом используются частные критерии, перечисленные в табл. 2. Будем считать, что все частные критерии имеют одинаковый масштаб и потому не нуждаются в нормализации. Тогда весовые коэффициенты критериев для систем с различным назначением могут быть оценены в диапазоне, например, от 0 до 10. Пример такого распределения весовых коэффициентов приведен в табл. 3.

Таблица 2

Частные критерии эффективного администрирования системы

Частный критерий	Описание
Минимальная сложность начальной установки настроек безопасности	Первоначальное задание настроек безопасности должно осуществляться с помощью минимального количества действий
Минимальная сложность создания и удаления объектов системы (файлов, каталогов, ключей реестра и т.д.)	Изменения, вносимые в систему при создании и удалении объектов, для сохранения действия политики информационной безопасности
Минимальная сложность создания и удаления субъектов системы (пользователей, групп пользователей)	Изменения, вносимые в систему при создании и удалении субъектов, для сохранения действия политики информационной безопасности

Таблица 3

Типовое распределение весовых коэффициентов
частных критериев для систем различного назначения

Назначение компьютера	Весовой коэффициент		
	Кр. 1	Кр. 2	Кр. 3
Файловый сервер	4	10	9
Сервер баз данных	1	10	8
Рабочая станция секретаря	9	8	1
Рабочая станция тестировщика	2	9	7
Рабочая станция аналитика	7	8	4

Приведенное в табл. 3 распределение весовых коэффициентов показывает, что, например, для сервера баз данных более существенной является простота создания и удаления объектов, чем сложность первоначальной настройки, а создание/удаление нового субъекта на файловом сервере намного важнее, чем на компьютере секретаря. После получения значений весовых коэффициентов выполняется многокритериальная оптимизация, результаты которой определяют множество настроек безопасности, которые необходимо установить в системе.

Таким образом, использование предложенного подхода позволяет решить задачу выбора эффективного способа настройки безопасности. Применение многокритериальной оптимизации является перспективной технологией, которая позволяет автоматизировать процессы настройки, анализа и управления безопасностью.

Литература

1. Штойер Р. Многокритериальная оптимизация: теория, вычисления и приложения. — М.: Радио и связь, 1992.

2. Ларичев О.И. Теория и методы принятия решений. — М.: Логос, 2000.

3. Лотов А.В., Бушенков В. А., Каменев В.А., Черных О.Л. Компьютер и поиск компромисса. Метод достижимых целей. — М.: Наука, 1997.

4. Захаров И.Г. Обоснование выбора. Теория практики. — СПб: Судостроение, 2006.

5. Москвин Д.А., Калинин М.О. Нахождение оптимального варианта настройки параметров безопасности в ОС Windows // Проблемы информационной безопасности. Компьютерные системы. — 2007. — № 2.

Дмитрий Андреевич Москвин
ГОУ ВПО Санкт-Петербургский государственный политехнический университет, аспирант
Эл. почта: moskvin@ssl.stu.neva.ru.

Калинин Максим Олегович
ГОУ ВПО Санкт-Петербургский государственный политехнический университет, к.т.н., доцент
Эл. почта: max@ssl.stu.neva.ru.
Тел.: (812) 55 27 632.

D.A. Moskvin, M.O. Kalinin

The Perspectives of Multicriteria Optimization Use in IT-security Control

One of the main goals of the computer systems management is the effective administering of the security configurations settings. This paper discusses a perspective technique of searching the optimal security configuring algorithm with use of multicriteria optimization.