М. О. Калинин, Д. А. Москвин
Санкт-Петербургский государственный политехнический университет

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ АДМИНИСТРИРОВАНИЯ С ПОМОЩЬЮ АВТОМАТИЗИРОВАННОГО ПРОФИЛИРОВАНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

В статье представлен метод автоматизированного создания профилей безопасности информационных систем (ИС), который позволяет добиться соблюдения принципов эффективного администрирования с учетом особенностей и требований, предъявляемых к различным системам.

Средства защиты любой информационной системы должны быть настроены в соответствии с требованиями политики безопасности (ПБ). Современные ИС обладают большим количеством настроек безопасности (НБ), поэтому автоматизированное применение ПБ существенно экономит время настройки системы и предотвращает возникновение ошибок администрирования. Автоматическая настройка безопасности ИС требует знания однозначного способа настройки. Однако в большинстве ИС существует множество вариантов предоставления пользователям одних и тех же полномочий.

Для определения способа настройки, наиболее подходящего для реализации ПБ, автором предлагается метод профилирования ИС. Под термином «профиль» понимается совокупность следующих характеристик ИС:

- назначение;
- сетевое окружение;
- состав и свойства программного обеспечения;
- состав и свойства аппаратного обеспечения.

Профилирование, являясь процессом сбора и анализа указанных характеристик ИС, позволяет выбрать оптимальные НБ, что упрощает дальнейшее администрирование и эксплуатацию ИС, сводит к минимуму риск возникновения ошибок администрирования, связанных с человеческим фактором.

В результате профилирования ИС составляется набор критериев соответствия профилю, выполнение которых позволит эффективно управлять системой. Например, критерий «Минимальное время настройки» актуален для систем с низкой производительностью. Характеристика «производительность» определяется автоматически по аппаратному обеспечению в процессе профилирования. Для выполнения каждого критерия необходимо использовать определенные множества НБ. Для вышеуказанного критерия при настройке ОС Windows следует использовать минимальное количество записей контроля доступа и большее количество привилегий. Тогда в процессе выбора способа настройки каждого правила ПБ необходимо проверять его непротиворечивость остальным правилам ПБ и соответствие профилю.

Поскольку каждому профилю соответствует несколько критериев, для выбора способа настройки, соответствующего профилю, целесообразно использовать методы многокритериальной оптимизации. Анализ данных методов [1, 2] показывает, что наиболее пригодным для решения данной задачи является метод последовательных уступок, поскольку он позволяет упорядочить критерии и учесть приоритет каждого из них [3].

Таким образом, метод автоматической настройки безопасности ИС включает в себя следующие этапы:

- автоматическое профилирование ИС;
- генерация критериев настройки;
- анализ ПБ;
- генерация множества способов настройки, удовлетворяющих ПБ;

• выбор способа настройки, наиболее удовлетворяющего профилю ИС;

• автоматическая реализация выбранного способа настройки.

Разработанный метод позволяет автоматически профилировать и настраивать произвольные информационные системы при применении политик безопасности.

В Специализированном центре защиты информации СПбГПУ разработанный метод используется в рамках практического курса «Безопасность операционных систем» для обучения принципам эффективного администрирования, грамотного применения политик безопасности, автоматизации управления безопасностью сложных вычислительных комплексов.

СПИСОК ЛИТЕРАТУРЫ:

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.

М. Ю. Киреев, Н. С. Шимон, Е. С. Агеев
Концерн «Созвездие», Воронеж

ПРИНЦИПЫ МОДЕЛИРОВАНИЯ МЕХАНИЗМОВ ВРЕДОНОСНОГО ВОЗДЕЙСТВИЯ НА ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ В ИНТЕРЕСАХ ОЦЕНКИ УГРОЗ ИХ БЕЗОПАСНОСТИ

Формулируются основные принципы моделирования механизмов вредоносного воздействия на информационные процессы в результате противоправных действий в информационной сфере. Рассматривается возможность оценки угроз информационной безопасности, вызванных подобного рода действиями

Основополагающими гипотезами при решении задачи моделирования механизмов вредоносного воздействия на информационные процессы в интересах оценки угроз их безопасности являются гипотеза об идентифицируемости вредоносных воздействий на информационные процессы и гипотеза о многоэтапности совершения противоправных действий в информационной сфере [1].

В соответствии с первой гипотезой, несмотря на применяемые злоумышленниками способы маскирования своих противоправных действий, существуют способы идентификации вредоносных воздействий на информацию. Это дает возможность поставить в соответствие каждому вредоносному воздействию его идентифицирующие признаки, что, в свою очередь, дает возможность использовать эти признаки в качестве исходных данных для моделирования механизмов вредоносного воздействия на информационные процессы в интересах оценки угроз их безопасности.

В соответствии со второй гипотезой вредоносные воздействия реализуются в рамках многоэтапных стратегий противоправных действий. Многоэтапность этих стратегий обусловлена необходимостью преодоления (вскрытия) механизмов защиты информации.