ботка концепции исследования, то есть комплекса ключевых положений, определяющих общую направленность, архитектонику и преемственность исследования.

Информационный подход позволяет увидеть многие явления совершенно по-новому и выявить ранее не замеченные факторы, которые оказываются очень важными в управлении затратами.

Стратегическое управление затратами не является самоцелью, а должно обеспечивать разработку и выполнение деловой стратегии организации.

Сегодня топ-менеджеры столкнулись с проблемой, как добиться наибольшей эффективности от реализации выбранной стратегии, как реагировать на непрерывные изменения внешней среды. В связи с этим для эффективного управления затратами необходимо иметь критерии оценки эффективности этих решений и действий. Другими словами для стратегического управления затратами необходимо использовать систему интегральных показателей, учитывающую не только финансовые, но и нефинансовые критерии оценки видов деятельности.

Следовательно, чтобы система управления затратами была эффективной, она должна ориентироваться на реализуемую стратегию, а общая система учета должна основываться на альтернативных возможностях.

SPICE- МОДЕЛИ БИПОЛЯРНЫХ ТРАНЗИСТОРОВ СО СТАТИЧЕСКОЙ ИНДУКЦИЕЙ

Бичурин М.И., Букашев Ф.И., Петров В.М.
Новгородский Государственный Университет им. Ярослава Мудрого, Великий Новгород

В настоящий момент известно большое число типов биполярных транзисторов со статической индукцией (БСИТ). Современные БСИТ характеризуются рабочими напряжениями до тысячи вольт, токами коллектора порядка сотен ампер при частоте переключения до 10 кГц. Применение БСИТ экономически целесообразно в устройствах с рабочими напряжениями от 60 до 600 В.

Принцип действия и первые экспериментальные образцы приборов со статической индукцией (СИТ) были разработаны в Японии в начале 50-х годов непосредственно вслед за изобретением полевого транзистора с управляющим p-n переходом (ПТУП). По своей структуре СИТ похож на обычный ПТУП, отличаясь от него более высокой степенью легирования истока и более узким и коротким каналом. Это позволило получить прибор, который мог работать не только в режиме обеднения канала носителями, но и в режимах его обогащения, при этом в приборе достигается гораздо больший, чем в ПТУП, выходной ток. В результате в подобных режимах обогащения канала носителями СИТ становится подобен обычному биполярному транзистору. БСИТ по сравнению с СИТ имеет более сложный профиль легирования и более сложную геометрию затвора, что обеспечивает данному типу транзисторов закрытое состояние при нулевом потенциале на затворе.

С развитием и распространением основанных на языке SPICE схемотехнических систем автоматизированного проектирования (САПР) появилась потребность в разработке SPICE- модели БСИТ. Электрическая модель полупроводникового прибора должна удовлетворять следующим основным требованиям:

- обеспечивать адекватность функционирования в широком диапазоне рабочих напряжений, токов, внешних воздействий, отображать с требуемой точностью разнообразные электрические характеристики в заданных произвольных режимах;
- иметь физически обоснованное соответствие между электрическими параметрами модели и электрофизическими процессами в приборе;
- состоять из набора стандартных элементов электрических цепей, связывающих токи и напряжения (резисторов, конденсаторов, индуктивностей, зависимых и независимых источников тока и напряжения);
- включать аппроксимации и упрощения для снижения вычислительных затрат при использовании моделей в САПР.

Для описания БСИТ, ввиду сходности вольтамперных характеристик рассматриваемого прибора с вольтамперными характеристиками биполярных транзисторов, может быть использована одна из моделей последних, в частности, модель Гуммеля-Пуна. Преимущества такого подхода – очевидность и простота; недостатки – погрешность моделирования может достигать 20%, что не всегда приемлемо, а значения параметров модели не всегда физически обоснованы [1].

Близость физических основ функционирования БСИТ и ПТУП предполагает использование моделей ПТУП, например, модели Шихмана-Ходжеса, модели идеального полевого диода или зарядоуправляемой модели ПТУП. Преимущество подхода – физическая осмысленность получаемой модели. Стандартная SPICE- модель позволяет также полнее использовать ее потенциал, например, для воспроизведения технологического разброса параметров прибора или температурных зависимостей.

Третий подход состоит в разработке эквивалентной схемы замещения БСИТ, состоящей из набора стандартных элементов электрических цепей. Пример построения подробной схемы замещения с учетом технологического разброса и температурных зависимостей приведен в работе [2].

Следует отметить, что выбор того или иного способа описания модели БСИТ должен определяться требуемой точностью, ограничениями на вычислительные ресурсы и возможностями алгоритмов САПР. Модель БСИТ на основе модели Гуммеля-Пуна была использована при моделировании бесконтактных коммутирующих устройств с использованием БСИТ. Рассчитанная вольтамперная характеристика устройства хорошо согласуется с вольтамперной характеристикой, полученной экспериментально.

СПИСОК ЛИТЕРАТУРЫ

1. Букашев Ф.И., Бичурин М.И., Петров В.М. Математические модели биполярных транзисторов и полевых транзисторов с управляющим p-n переходом и оценка их применимости для описания биполярных транзисторов со статической индукцией. М.: Деп. ВИНИТИ, № 959-ВО2, 29.05.2002, 27 с.

2. Букашев Ф.И., Байбузов А.В., Смирнов А.Ю. Идентификация статических параметров SPICE-макромодели тиристора.//CAD/CAM/CAE Observer, №4, 2004, с 78-80.

СИСТЕМНЫЙ ПОДХОД К БЕЗОПАСНОСТИ ТЕХНОЛОГИИ ВЕРИФИЦИРОВАННОГО АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ ПРОГРАММ

Бочкарева Ю.Г., Клянчин В.К., Чижухин Г.Н.
Пензенский филиал ФГУП НТЦ "Атлас",
Пензенский государственный университет

Коротко о технологии верифицированного автоматизированного проектирования программ (ВАПП). Программное обеспечение (software) сегодня является необходимым и обязательным дополнением к техническим средствам (hardware), которые давно имеют и совершенствуют уже несколько десятилетий системы автоматизации их проектирования (САПР). Однако системы автоматизации *программирования* (проектирования software) по-прежнему находится в зачаточной стадии, хотя создание таких систем не только ускорил бы процессы программирования, но и позволил обеспечить большую безопасность создаваемого software.

Для верифицированного автоматизированного проектирования программ (ВАПП) предложена технология [1,2], основанная на использовании тензорной алгебраической системы (ТАС) [3] и Венского метода проектирования программ (VDM) [4]. Начало ее реализации представлено в работах, направленных:

- на создание специального глоссария [5], как конгломерата ТАС и VDM;
- на доказательство с использованием ТАС правильности перехода (верификации) с одного уровня представления программы на другой [6];
- на создание тензорной спецификации программы и на методику ее автоматического преобразования в программу на языке высокого уровня [7].

Однако, несмотря на эти, уже решенные при реализации ВАПП принципиальные вопросы, сегодня по-прежнему нет автоматизированного преобразования словесного описания (СО) алгоритма в его более четкий вид - «канонизированное» формализованное СО (ФСО), основанное на понятии «соответствие», а также дальнейшего автоматического преобразования ФСО в инверсную граф-схему алгоритма (ИГСА), необходимую для автоматического синтеза регулярного выражения алгоритма (РВА).

Кроме того, отсутствует системный анализ безопасности технологии ВАПП, который должен, на наш взгляд, состоять из следующих составных частей:

- системного анализа безопасности самой технологии программирования;
- системного анализа безопасности верификации программирования;
- системного анализа безопасности автоматизации программирования;
- комплексного системного анализа безопасности всей технологии ВАПП.

Общая постановка системного анализа информационной безопасности. Сначала рассмотрим системный анализ любой АСОИ (автоматизированная система обработки информации) как объекта информатизации с точки зрения информационной безопасности [8].

Для подобного анализа [9] необходимо представить, что такая АСОИ должна содержать в себе некоторую *подсистему информационной безопасности* (ПИБ), состоящую из *компонентов*, каждый из которых есть множество относительно однородных *элементов,* объединенных некоторыми функциями для обеспечения выполнения общих целей ее функционирования. Причем подсистема здесь не сводится к сумме компонентов, хотя в случае объединения их в подсистему они выступают и, соответственно, воспринимаются как единое целое. Для ПИБ АСОИ, на наш взгляд, имеют место следующие компоненты:

- стратегии (способы) *защиты* информации, стратегии (методы) прогнозирования *нападения* на рассматриваемый объект,
- стратегии (механизмы) принятия решения, основывающиеся на анализе возможных результатов суммарного действия двух предыдущих стратегий и представляющие собой *политику безопасности* (набор норм, правил и практических приемов, регулирующих такое управление и распределение ценной информации [10],которое обеспечивает ее безопасность).

Элемент. ПИБ - это условно неделимая, самостоятельно функционирующая ее часть, которая, например, для первой компоненты представляет собой одну стратегию защиты. Таких стратегий, как известно [11], может быть несколько. Из элементов ПИБ состоят все ее компоненты и элементы объединяются общей функциональной средой.

Функциональная среда - это характерная для ПИБ совокупность законов, алгоритмов и параметров, согласно которым осуществляется взаимодействие (обмен, взаимоотношение) между ее компонентами и функционирование (стабильность или деградация) ПИБ в целом.

И, наконец, *структура* ПИБ подразумевает совокупность связей, обеспечивающих этот информационный обмен между компонентами, определяющий функционирование ПИБ в целом, и способы взаимодействия ее с внешней средой.

Рассмотрим подробней компоненты и элементы ПИБ, из которых они состоят. Например, организация защиты информации в самом общем виде может быть сформулирована как задача поиска оптимального компромисса между *потребностями в защите* и *необходимыми ресурсами* для этих целей [12]. Потребности обусловлены важностью и объемами защищаемой информации, условиями ее хранения, обработки и использования. Ресурсы могут быть ограничены заданным пределом либо определяются условием