планируется переход на 0,5 мкм уровень. Ликвидация такого отставания требует колоссальных затрат. Так современный завод-мегафаб на проектные нормы 0,13 мкм стоит 1,5–3,0 млрд. долларов.

Очевидно, что наше государство не может позволить себе такие затраты, а поиск зарубежных инвесторов оказался безуспешным.

Поэтому для изготовления изделий, требующих уровня глубокого субмикрона, придется ориентироваться на зарубежные "кремниевые мастерские", мирясь с необходимостью передачи им разработок наших дизайн-центров. В этом случае необходимо разработки доводить до уровня топологии, не останавливаясь, как принято сейчас у системщиков, на модели RTL-уровня. В противном случае нет гарантий защиты наших дизайн-центров от несанкционированного использования представленной модели, ее самого ценного — идеи. Кроме того, возникают опасения – не будут ли при изготовлении ИС встроены в них так называемые "закладки", в частности, взрывающийся пористый кремний, которые в час "Ч" способны нарушить нормальное функционирование систем, нанося значительный ущерб государству.

Разработку, выполненную на уровне топологии, а еще лучше представленную комплектом фотошаблонов, изготовленным в соответствии с требованиями выбранного производства ИС, проще защитить, она не воспроизводится. После изготовления пластины должны обязательно тестироваться у себя. Тогда изготовителю даже сложно узнать, что за функциональное устройство он сделал, все ноу-хау остаются у разработчика, становится трудно вписать "закладки".

Тем более, что изготовление фотошаблонов даже для глубоко субмикронной технологии можно организовать в республике. Концерн "Планар" производит для этого самое современное оборудование.

Для полного обеспечения секретности, сокращения сроков разработок таких, как "система на кристалле", "система на пластине", требующих глубокого субмикрона, рассмотрена технология, использующая функционально законченные, многократно используемые IP-блоки в сочетании с элементами собственных, имеющих ноу-хау блоков, которые изготавливаются на пластинах в зарубежных кремниевых мастерских. Данные блоки не соединены металлизацией в систему, что исключает понимание ее функционирования. Специализация выполняется на своем относительно недорогом гибком производстве — минифабрике, с использованием бесшаблонной фотолитографии для формирования 1–2 уровневой металлизации, соединяющей эти блоки в систему. Для этого достаточно 0,5–1,0 мкм технологии, которая реализуется лазерным генератором изображений ЭМ-5299 концерна "Планар".

Исключение фотошаблонов и малые сроки (3–4 часа) программирования одного слоя снижает до минимума утечку информации о разрабатываемых устройствах.

МОДЕЛЬ ОЦЕНКИ ПОСЛЕДСТВИЙ АТАК НА ЦЕЛОСТНОСТЬ И ДОСТУПНОСТЬ ИНФОРМАЦИОННЫХ РЕСУРСОВ

В.И. НОВИКОВ

В информационном обществе доминирующим катализатором и движущей силой социально-экономического развития становятся информационные ресурсы ***(R).***. Более того, в информационном обществе они выступают как интегральный вектор направления его развития. Развивающиеся информационные ресурсы порождают позитивное развитие общества, а их деградация приводит к застою в обществе, социально-экономическим потрясениям и кризисам.

Поэтому в комплексе задач создания, получения, хранения, использования и передачи информационных ресурсов как важнейшей социально-экономической категории информационного общества проблема доступа и защиты выдвигается на первый план.

Информационный ресурс ***R*** не изменяется сам по себе. Проблемный ресурс общества ***P***, постоянно взаимодействуя с информационным ресурсом, всегда как при воздействии внешней среды, так и вне зависимости от внешней среды создает новые знания и реструктурирует информационный ресурс в результате процессов объединения и трансформации, отрицания и старения.

Механизмом и средством взаимодействия ресурсов является информационная среда общества ***S***.

Под интеллектуальным потенциалом общества ***I*** будем понимать способность общества в соответствии с проблемным ресурсом ***P,*** средствами и механизмами информационной среды общества ***S,*** в том числе за счет "живого" знания, путем активизации и всестороннего анализа информационного ресурса ***R*** находить решения проблемных ситуаций в соответствии с целями общества в направлении его развития, создавая новые знания ***R****, новые цели и проблемы ***P****, информационную среду ***S**** и интеллектуальный потенциал ***I****[1].

Классификация всех видов ресурсов может быть выполнена по ряду признаков.

По признаку отношения к определенным общественным группам такая классификация в нисходящей последовательности включает ресурсы: мировые; национальные; государственные; общественные; отраслевые; профессиональные ресурсы личности, команды.

Дадим общее для этих уровней определение интеллектуального потенциала в терминах ресурсов.

Интеллектуальный потенциал ***Ii(t)*** некоторого иерархического уровня ***i*** общества в данный момент развития ***t*** определим как способность этого уровня общества к объединению средствами информационной среды ***Si(t)*** информационного ***Ri(t)*** и проблемного ***Pi(t)*** ресурсов для создания (развития) ***Ri(t+t*), Pi(t+t*), Si(t+t*), Ii(t+t*)*** в процессе разрешения проблемных ситуаций из ***Pi(t)*** в соответствии с целями развития данного иерархического уровня общества.

Или **I** есть отображение

$$I: (R,S,P) \rightarrow R^*,S^*,P^*,I^*. \quad (1)$$

Таким образом, ***R,P,S*** *и* ***I*** составляют основу национального достояния общества в информационной стадии развития и, как следствие, представляют предмет атак, производимых с экономической, политической и другими целями.

Атака на доступность информационных ресурсов предполагает нарушение временных характеристик доступа (отказ, частичный доступ), искажение целей доступа (нарушение алгоритма поиска), подставка неадекватной информации. Атака на целостность ресурсов предполагает искажение (снижение) их точности и достоверности, разрушение структуры баз и т.д.

В модели развития ресурсов эти процессы можно представить как искажение информационного ресурса **R**

$$\Delta R = R^a - R, \quad (2)$$

где $\mathbf{R^a}$ – искаженный в результате атаки информационный ресурс.

Разность ΔR определяет меру внесенных в результате атак искажений, последствия которых могут быть оценены только в результате выполнения отображения (1), где исходным является искаженный ресурс R^a

$$I: (R^a,S,P) \rightarrow R^a*,S^a*,P^a*,I^a*. \quad (3)$$

Рассмотрим частный случай, когда отображение (1) может быть представлено в стандарте IDEF0 описания бизнес процессов [2]. Методология IDEF0 предполагает построение иерархической системы диаграмм, описывающих бизнес процессы. На верхнем уровне строится контекстная диаграмма, описывающая взаимодействие бизнес процессо й.

Семантика IDEF0 применительно к йствия ресурсов трактуется следующим образом. Отображение ***I*** представляет содерж (activity), искаженный информационный ресурс R^a - как входные да t), проблемный ресурс ***P*** - как функциональные задачи, правила, стандарты на входе управлен обесп ode механизмы (рис. 1).

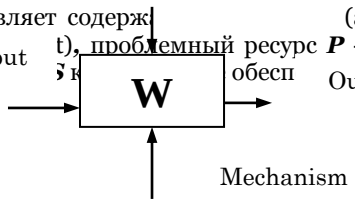

Рис. 1. Базовый блок IDEF0

Упростим модель, исключив влияние среды ***S*** . Тогда (3) может быть представлено в виде

$$I: (R^a,P) \rightarrow R^a*,P^a*,I^a, \quad (4)$$

а выход IDEF0 модели описан как $C=W(R,P)$ в идеальном случае, и как $C^a = W(R^a,P)$ в случае атаки на входной ресурс.

Рассмотрим, каким образом механизм декомпозиции контекстной модели влияет на последствия атаки на информационный ресурс.

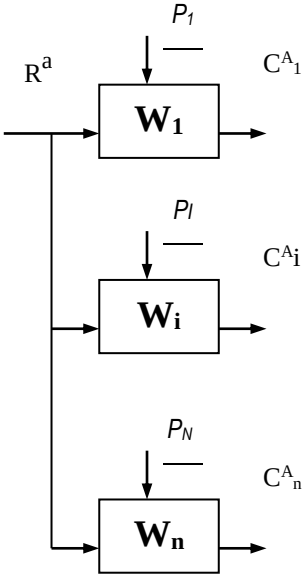

Рис. 2 Несвязные функциональные задачи

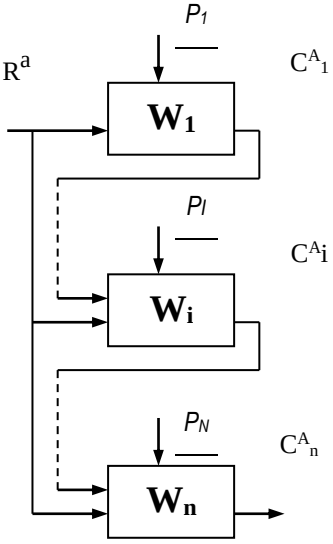

Рис. 3. Доминирование функциональных задач

Если задача P может быть представлена множеством несвязанных функциональных задач $P=(P_1 P_2 \ldots P_N)$, то декомпозиция работ может быть представлена N несвязными работами $W=(W_1W_2\ldots W_N)$ (рис.2).

Последствия атаки являются аддитивными и вычисляются как сумма погрешностей, вносимых в каждую конкретную работу

$$\Delta Ci = Ci^a - Ci. \quad (5)$$

Однако в большинстве случаев декомпозиция контекстной модели приводит к сильно-связанной модели доминирования работ (рис. 3)

Последствия атаки являются мультипликативными, так как конечный результат выполнения работ $C^A = C^A_n$ и воздействие атаки учитывается многократно.

$$\Delta Ci=Wi(R^A, C^Ai\text{-}1,Pi) - Ci. \quad (5)$$

Полученная модель положена в основу программного комплекса минимизации влияния атак на информационные ресурсы. В функции от последствий влияния атаки на конкретные работы ΔCi он позволяет синтезировать алгоритм декомпозиции работ с минимальными последствиями атаки.

Литература

1. Кривцов В.Н, Новиков В.И. Управление информационными ресурсами — перспективное направление образования // Тез. докладов IIV международной конференции "Комплексная защита информации" Мн, 2003.С. 186–188.
2. Маклаков С.В. Bpwin, Erwin. CASE-средства разработки информационных систем. М. 2000.

ОБНАРУЖЕНИЕ АКУСТИЧЕСКИХ СИГНАЛОВ НА ФОНЕ РЕЧИ

В.И. ВОРОБЬЕВ, Г.В. ДАВЫДОВ, Д.В. ЛЕЩЕНКО

Рассмотрены методы обнаружения сигналов на фоне речи, включая тональные сигналы, шумовые сигналы и частотно-манипулированные с использованием кодов Баркера. Такие методы применяются для автоматизации обнаружения несанкционированных технических средств съема акустических сигналов в выделенном помещении путем автоматического сканирования радиочастотного диапазона и анализа демодулированных сигналов.

Задача обнаружения заключается в принятии решения: в данном помещении присутствуют технические средства съема речевой информации и передачи ее по радиоканалу или указанные средства в помещении отсутствуют. При этом предполагается, что средства съема информации используют для её передачи радиопередающее устройство с амплитудной, частотной и другими видами модуляции и имеют ненаправленную антенну. Алгоритм обнаружения включает формирование и излучение в выделенном помещении тестового акустического сигнала и поиск этого сигнала в частотном спектре радио излучений в заданном диапазоне частот.

Для обнаружения технических средств съема речевой информации активным методом в качестве тестового сигнала представляется целесообразным использовать частотно-манипулированный сигнал со сменой частоты в соответствии с кодами Баркера. Корреляционная функция такого сигнала имеет четко выраженный пик, а спектральный состав обеспечивает борьбу с замираниями в условиях наличия в помещении явления акустической реверберации.

Рассматриваются наиболее распространенные критерии обнаружения и вопросы выбора оптимального критерия для решения поставленной задачи.

Для оценки эффективности представленного алгоритма обнаружения приводятся результаты моделирования. Оценены вероятность правильного обнаружения и вероятность ложной тревоги при различных значениях порога и отношения сигнал/шум. В качестве модели шума использовался случайно выбранный сигнал речи достаточно большой длительности.

ВИБРАЦИОННЫЕ ПРЕОБРАЗОВАТЕЛИ СИСТЕМ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

Г.В. ДАВЫДОВ, А.В. ПОТАПОВИЧ, В.А. ПОПОВ

В настоящее время для защиты речевой информации широко используются вибрационные преобразователи. Основные электроакустические параметры различных вибрационных преобразователей систем защиты речевой информации не нормируются и отсутствуют методики оценки их эффективности.

Целью работы является исследование амплитудно-частотных характеристик вибрационных преобразователей и разработка методики измерений и сравнение основных электроакустических параметров вибрационных преобразователей.

Вибрационные преобразователи систем защиты речевой информации преобразуют электрические колебания в силовые воздействия на присоединенные конструкции и являются устройствами инерционного принципа действия. Преобразователи, работающие в системах защиты речевой информации, должны иметь достаточно широкую частотную полосу, соответствующую полосе речевого сигнала. Кроме того, их параметры не должны существенно изменятся в рабочем или заданном диапазоне температур и во времени.

В работе излагается методика измерения выталкивающей силы вибрационных преобразователей, по которой можно сравнивать эффективность различных типов преобразователей и оценивать их