МИР электроники

В.Н. Федорец,

Е.Н. Белов,

С.В. Балыбин

ТЕХНОЛОГИИ ЗАЩИТЫ МИКРОСХЕМ ОТ ОБРАТНОГО ПРОЕКТИРОВАНИЯ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕХНОСФЕРА
Москва
2019

УДК 621.374
ББК 32.85
Ф33

Рецензенты: *д.т.н., профессор Колковский Ю.В. (АО НПП «Пульсар»),*
д.т.н., доцент Сазонов К.В. (ВКА им. А.Ф.Можайского)

Ф33 Федорец В.Н., Белов Е.Н., Балыбин С.В.
Технологии защиты микросхем от обратного проектирования в контексте информационной безопасности
Москва: ТЕХНОСФЕРА, 2019. – 216с. ISBN 978-5-94836-562-6

В книге рассмотрены вопросы обеспечения информационной безопасности современной электронной компонентной базы, используемой при разработке радиоэлектронной аппаратуры различного назначения. Особое внимание уделено вопросам уязвимости, возникающим при разработке и изготовлении микросхем, создаваемых по fabless-технологии.

Авторами рассмотрены инженерно-технические и организационно-методические решения по защите от обратного проектирования современных микросхем.

Книга может быть полезна специалистам в области микроэлектроники, разработчикам отечественной элементной базы, а также студентам, обучающимся по специальностям, связанным с разработкой микросистем и информационной безопасностью.

УДК 621.374
ББК 32.85

ISBN 978-5-94836-562-6

Памяти Евгения Николаевича Белова

СОДЕРЖАНИЕ

Предисловие **6**
Список использованных сокращений **10**
Введение **12**

РАЗДЕЛ 1
Вопросы информационной безопасности и обратное проектирование микросхем **14**

1.1. Глобализация в микроэлектронике – основная тенденция ее развития 18
1.2. Могут ли содержать угрозы изделия микроэлектроники? 27
1.2.1. Проблема контрафактных изделий микроэлектроники в России 28
1.2.2. Практические шаги к выявлению контрафакта 31
1.3. Угроза снижения безопасности изделий микроэлектроники злоумышленниками 38
1.4. Роль «доверия» при анализе информационной безопасности микросхем 46
1.4.1. «Доверие» и защищенность систем 46
1.4.2. Особенности угроз в области модулей доверенной загрузки и связь с обратным проектированием микросхем 47

РАЗДЕЛ 2
Обратное проектирование микросхем и защита от него 52

2.1. Цели и задачи обратного проектирования изделий микроэлектроники 54
2.2. Обратное проектирование микросхем и его возможности 55
2.2.1. Основные этапы обратного проектирования микросхем 55
2.2.2. Оценка возможностей обратного проектирования применительно к микросхемам, используемым в аппаратуре ответственного применения, разрабатываемой в России 59

2.3. Защита от анализа структуры микросхемы 63
2.3.1. Защита от удаления корпуса и защитного покрытия..... 63

2.3.2. Защита микросхем от послойного восстановления топологии 64
2.3.3. Защита микросхем от обратного проектирования с помощью разрушения объекта исследования 70
2.3.4. Защита микросхем от обратного проектирования с помощью экранирования и камуфлирования 78
2.4. Защита от анализа функций микросхемы 82
2.5. Экономический аспект обратного проектирования 85

РАЗДЕЛ 3
Информационная безопасность в контексте защиты интеллектуальной собственности в микросхемах 89

3.1. Общие вопросы идентификации микросхем 90
3.2. Кремниевая фабрика как потенциальный нарушитель 92
3.3. Специализированные блоки идентификации 94
3.4. Использование обфускации при защите микросхем 103
3.5. Идентификация и аутентификация изделий микроэлектроники на основе физически неклонируемых функций 106
3.5.1. Краткая характеристика ФНФ 108
3.5.2. Подход к использованию ФНФ в случае недоверия к кремниевой фабрике 115
3.6. Скрытые метки для защиты собственной продукции 121

РАЗДЕЛ 4
Контроль однородности партий микросхем и радиоэлектронной аппаратуры путем измерения s-параметров (радиопортрета) четырехполюсника 129

4.1. Исследование s-параметров усилителя в корпусе 131

4.2. Исследование s-параметров микросхемы ПЛИС 140

РАЗДЕЛ 5
Аппаратно-программная целостность программируемых логических интегральных схем в контексте обратного проектирования 145

5.1. Обратное проектирование ПЛИС: история и угрозы 145
5.1.1. Обратное проектирование конфигурационного битового потока ПЛИС..... 146
5.1.2. Защита от обратного проектирования конфигурационного битового потока ПЛИС 151
5.2. Технические параметры П ЛИС и особенности объектов, для которых необходим контроль целостности 152
5.3. Особенности обеспечения контроля целостности для высокоскоростных и многоядерных решений на базе ПЛИС 159
5.4. Перспективы применения криптографии для контроля целостности 160
5.5. Определение необходимых для реализации механизмов контроля аппаратной целостности конфигурационных данных 166
5.6. Система оценок для определения уровня контроля целостности конфигурационных данных ПЛИС 170

Заключение..... 173

Список рисунков 175
Список таблиц 180
Список литературы..... 181

Приложение А
«Иностранное» и «отечественное» производство: от диалектической борьбы к словесной казуистике..... 200

Приложение В
Полезные термины и определения 204

ПРЕДИСЛОВИЕ

Настоящее время применительно к радиотехнике и микроэлектронике характеризуется стремительным усложнением электронных систем, переходом к наноразмерным структурам и широкой глобализацией производства – в частности, территориальным, а часто и государственным разделением разработчиков элементной базы и заводов-изготовителей пластин со структурами и (или) кристаллов интегральных схем. Несмотря на пропагандируемую и внедряемую политику импортозамещения, этот процесс будет продолжаться для микросхем уровня сложности «система на кристалле» и «система в корпусе» при топологических нормах менее 50 нм. Разделение на разработчиков микроэлектронных систем (дизайн-центры) и производителей пластин и кристаллов (кремниевые фабрики) установилось на межгосударственном уровне и, по-видимому, будет только усугубляться. При этом возникает ряд проблем, связанных с надежностью, качеством и безопасностью продукции, в частности проблема контрафакта в самом широком его понимании. Зафиксированы злоупотребления правом на защиту интеллектуальной собственности, которые приводят к негласному внедрению подсистем с полицейскими и шпионскими функциями в изделия (ограничивающих права добросовестного пользователя).

Исторически попытка сбыта некачественной (бывшей в употреблении или контрафактной) продукции (например рыцарских доспехов) могла быть чревата для мастера-изготовителя. В настоящее время деперсонализация ответственности на фоне существенно возросшей номенклатуры выпускаемой продукции играет на руку производителям подделок. Соответственно, совершенствуются и методы борьбы с ними.

Вопросы борьбы с подделками, затрагиваемые в книге, известны широкому кругу читателей (все наслышаны о контрафактных лекарствах, напитках, продуктах питания и других товарах широкого потребления).

Про рынок микроэлектронных изделий написано не так много. Однако от качества продукции специального и двойного назначения зависят вопросы здоровья и безопасности как людей, так и государства в целом. Здесь отмечаются факты перемаркировки изделий, сбыта использованной и устаревшей продукции и другие разнообразные мошеннические приемы. Отчасти это связано с бы-

стрым обновлением рынка электронных устройств и недостатками в организации их утилизации (так, по данным [1], в США ежегодно выбрасывается порядка ста миллионов мобильных телефонов).

В мире ежегодно выходит не менее десяти сборников и монографий, посвященных в той или иной степени вопросам обратного проектирования. Большая часть такой литературы на английском языке и мало доступна российскому читателю. В России можно отметить выпущенные СПбГЭТУ в своем издательстве учебные пособия [2], но этого явно недостаточно. Поэтому выпуск русскоязычной книги, затрагивающей основные моменты обратного проектирования (что это такое, как это реализовать и как от этого защититься) давно назрел и стал необходимостью.

Естественно, в мире не обходится без некоторого преувеличения таких угроз и опасностей со стороны борцов с контрафактом в целях получения дополнительного финансирования работ в этой несомненно интересной как в научном, так и практическом плане области.

В значительной степени монография носит обзорный характер и затрагивает в основном именно иностранные литературные и патентные источники. Это отражает соотношение объемов исследований по данной тематике за рубежом и в России. Исключением являются некоторые параграфы главы 2, главы 3 и глава 4, в которых рассматриваются технические решения, предложенные авторами этой книги и защищенные патентами Российской Федерации, направленными на способы противодействия обратному проектированию. Предложены способы защиты (в частности скрытой маркировки), которые авторы рассматривают как вполне реальные, а также способы, которые выглядят как сомнительные (использование материалов с памятью формы для разрушения кристалла микросхемы при вскрытии пластмассового корпуса при повышенной температуре).

Свою основную задачу авторы видят в ознакомлении разработчиков электронных систем с данной проблемой, преследуя цель сориентировать их на использование отечественной продукции, тем самым внеся посильный вклад в процесс реального импортозамещения. Книга может быть полезна и разработчикам отечественной элементной базы в плане указания на проблемные вопросы, с которыми они могут встретиться в настоящее время при существующей глобализации производства микросхем. Кроме того, ряд методов, предложенных авторами, может (по их мнению) найти применение при контроле качества продукции микроэлектроники и радио-

электроники. Книга может быть полезна студентам, обучающимся по специальностям, связанным с разработкой микросистем и с информационной безопасностью.

Метод (способ – при использовании патентной терминологии) применения радиопортрета, заключающийся в сравнении s-параметров изделий может быть применен и как метод скрытой маркировки при контроле подлинности, и как метод контроля качества отечественной продукции. При наличии ручного труда при сборке радиотехнических блоков радиопортрет можно в ряде случаев рассматривать как одну из физически неклонируемых функций (ФНФ), применению которых для защиты микросхем от обратного проектирования посвящена отдельная глава книги. Физически не клонируемая функция фактически является обобщенным параметром изделия, точное знание которого позволяет судить о подлинности (аутентичности) самого изделия. Ряд таких параметров, которые можно использовать при контроле подлинности и которые, тем не менее, не являются ФНФ, упомянут авторами в описании меток контроля подлинности (глава 2) при внесении специальных добавок, известных только изготовителю, в маркировку изделия или в состав материала корпуса.

Следует отметить появление работ по контролю микросхем на основе временных параметров – параметров задержек сигналов [1] – временной радиопортрет изделия (circuit timing signature). В этом случае предложенный и рассмотренный авторами настоящей книги метод точнее называть внутренним радиочастотным портретом, понимая под внешним радиопортретом картину электромагнитного излучения в непосредственной близости от изделия. Соответственно, результаты, полученные упомянутым выше методом исследования задержек, можно назвать хронопортретом микросхемы.

Заметим, что в настоящее время не устоялась и терминология в данном направлении исследований, поэтому ряд терминов, которые в настоящее время используются, дан в приложении В в том виде, как это понимают авторы. Также нет общего мнения о том, какую продукцию в настоящее время и с какой точки зрения (разработчика, потребителя, контролера) можно считать отечественной. Этот вопрос авторы также рассматривают и выносят на обсуждение (приложение А).

Авторы не рассматривают в деталях собственно процесс обратного проектирования, это было сделано коллективом авторов,

работающих под руководством В.В. Лучинина [3–9], и опубликовано в Петербургском журнале электроники в 2009–2010 гг. Также не затрагиваются вопросы надежности, которые, тем не менее, достаточно крепко связаны с рассматриваемой темой в части методик контроля изделий.

Данная работа состоит из введения, 5 глав, двух приложений, списков рисунков, таблиц и использованных сокращений.

В главе 1 рассмотрены вопросы информационной безопасности при применении современных микросхем в радиоэлектронной аппаратуре, что подтверждает мнение авторов об опасности изделий микроэлектроники. Во второй главе приведены вопросы, касающиеся собственно процесса обратного проектирования микросхем и «физико-механические» способы защиты от обратного проектирования. В главе 3 рассмотрены факторы уязвимости при fabless (foundry) процессе изготовления микросхемы. Глава 4 посвящена вопросу измерения S-параметров как предлагаемому авторами методу контроля однородности партий изделий. Глава 5 посвящается вопросам обеспечения аппаратной целостности ПЛИС, которые представляют собой удобную модель для исследования вопросов подлинности и доверительности.

В приложение В вошли термины, понятия и определения, которые, по нашему мнению, требуют объяснений, и даже простое знание этих терминов может способствовать лучшему пониманию предмета книги. Авторы считают, что понятие «отечественная продукция» в настоящее время не является однозначным, и выносят свою позицию для обсуждения в приложении А.

Хотелось бы, чтобы таких проблем в отрасли было меньше.

СПИСОК ИСПОЛЬЗОВАННЫХ СОКРАЩЕНИЙ

АЦ – аппаратная целостность
БИС – большая интегральная схема
ВИМС – вторичная ионная масс-спектроскопия
ГСЧ – генератор случайных чисел
ДЦ – дизайн-центр – организация – разработчик ИМС, как правило, без собственного прозводственного цикла
ЗИП – запасные части и принадлежности
ЗМ – заказные микросхемы
ЗУ – запоминающее устройство
ИМС – интегральная микросхема
ИМЭ – изделие микроэлектроники
ИП – иностранное производство (см. приложение А)
ИС – интегральная схема
КД – конфигурационные данные
КМ – кремниевая мастерская – завод по изготовлению ИМС по представленной документации разработчика
КМОП – компланарные технологии металл – окись – полупроводник или полупроводниковые структуры
КП – ключевые параметры
КСВН – коэффициент стоячей волны по напряжению
КЦ – контроль целосности
МДП (TPM, trust platform module) – модуль доверенной платформы
МО США – министерство обороны Соединенных Штатов Америки
МЭ – микроэлектроника
НДВ – недекларированные возможности
НСД – несанкционированный доступ
ОВА – ответственные виды аппаратуры (медицинская, специальная, военная, космическая)
ОП – обратное проектирование
ОС – операционная система
ПЗУ – программируемое запоминающее устройство
ПК – персональный компьютер
ПЛИС – программируемая логическая интегральная схема
ПО – программное обеспечение
ПЭМИН – побочное электромагнитное излучение и наводки

РЭА – радиоэлектронная аппаратура
СБИС – сверхбольшая интегральная схема
СнК (SoC – англ.) – система на кристалле
СПбГЭТУ – Санкт-Петербургский Государственный электротехнический университет
СФ (IP – англ.) – сложно-функциональные блоки
ТРИЗ – теория решения изобретательских задач
УВЧ – ультравысокие частоты
УФНФ – управляемая ФНФ
ФНФ – физически не клонируемая функция
ФЧХ, АЧХ – фазочастотная и амплитудно-частотная характеристика
ЦОС – цифровая обработка сигнала
ЭК – электронные компоненты (комплектующие)
ЭКБ – электронная компонентная база
ЭМС – электромагнитная совместимость
ЭПП (eFUSE – англ.) – электрически программируемые перемычки
ЭСППЗУ – электрически стираемое запоминающее устройство
BNF (Backus-Naur Form либо Backus Normal Form) – БНФ, нормальная форма Бэкуса-Наура
СвК (SiP – англ.) – система в корпусе
FPGA – field programming gate array
HDL (Hardware Description Language) – язык описания аппаратных средств, язык HDL
JTAG – интерфейс программирования микросхем
RFID (radiofrequency identification, англ.) – радиочастотная метка
RTL (Register Transfer Level) – уровень регистровых передач, схема [модель] уровня RTL
XDL (Xilinx Description Language) – язык низкоуровневого описания конфигурационной битовой последовательности фирмы XILINX

ВВЕДЕНИЕ

И вот он изобретал целые узлы, агрегаты, сложные и нелепые с точки зрения его настоящих задач. Потом заваливал мастерские Вейнтрауба заказами на эти химерические детали. А получив готовое изделие, вынимал из него, как ядрышко из ореха, одну нужную ему часть и вставлял ее в свою схему. Остальное шло в ящик с «барахлом», как называл он все до времени ненужное, что попадало в этот ящик. Следуя хорошо продуманной системе, Мюленберг заказывал и обычные радиотехнические детали, порой несколько усложненные, — лампы, конденсаторы, сопротивления, электронно-оптические линзы, большая часть которых непосредственно отправлялась в тот же ящик, даже без осмотра. Все это нужно было для того, чтобы увести мысль вейнтраубовских инженеров, несомненно изучающих его головоломки, подальше от правильного пути.

Ю.А. Долгушин «Генератор чудес», журнал «Техника молодежи», 1939–1940 гг. — Дет. лит., 1960, с. 496.

Собственно обратное проектирование существует много лет. Первые законодательные акты, закрепившие за обратным проектированием право на существование в качестве инструмента для защиты от плагиата и защиты конкуренции, появились в США. Вопросы обратного проектирования в автомобильной, авиационной и других «крупногабаритных» отраслях промышленности достаточно подробно рассмотрены, например, в работе Vinesh Raja and Kiran J. Fernandes [10]. В качестве примеров обратного проектирования можно назвать широко известное копирование образцов вооружения и военной техники, а также промышленных изделий гражданского назначения.

Применительно к микроэлектронике законодательным актом, легализовавшим обратное проектирование как средство за-

щиты интеллектуальной собственности, явился Semiconductor Chip Protection Act, принятый в США в 1984 году.

Чрезвычайно бурное развитие микроэлектроники и соответствующее расширение областей ее применения привели к тому, что «внутри» современной микросхемы (по современной терминологии, в большой и сверхбольшой схеме (БИС и СБИС)) «спрятано» много интеллектуальной собственности. Поэтому конкуренты готовы потратить серьезные средства для изучения микросхем, в ряде случаев – копирования, но прежде всего для поиска «обходных путей» в целях создания конкурентоспособных изделий. Весьма важным фактором стало и то, что в современных БИС и СБИС, в аппаратуре на их основе хранится и обрабатывается гигантское количество информации. Она также имеет свою цену, следовательно, в ее получении или добыче заинтересованы очень многие. Перечисленные тенденции вкупе с истинно полной глобализацией техники и технологии микроэлектроники привели к зарождению следующих направлений исследований:

- достаточно интенсивное развитие техники и технологий обратного проектирования (ОП) в микроэлектронике;
- многочисленные попытки защитить «внутреннее содержимое» БИС и СБИС от процедур ОП в целях сохранения конкурентоспособности максимально продолжительное время;
- интенсивные исследования возможных путей «встраивания» в состав БИС и СБИС различного рода элементов (устройств, блоков, программ и т.д.), имеющих своей целью нарушить или исказить работу БИС, СБИС и устройств на их основе, в том числе дистанционно, но в любом случае без декларирования таких возможностей; в последнее время появились первые публикации об успешной реализации этого направления;
- интенсивные исследования путей защиты БИС и СБИС от различного рода несанкционированных вмешательств в процесс их производства (включая неконтролируемое владельцем интеллектуальной собственности распространение готового изделия).

К сожалению, большая часть обзорной литературы по данным направлениям издана на английском языке, что вполне объяснимо, если учесть объемы разработок и промышленного выпуска изделий микроэлектроники в зарубежных странах. На русском языке имеется ряд статей, посвященных процессу обратного проектирования,

из которых следует отметить цикл работ, опубликованных в «Петербургском журнале электроники» сотрудниками СПбГЭТУ [2–9].

Авторы полагают, что назрела необходимость объединить в одном месте информацию по кругу вопросов обратного проектирования. Так как «нельзя объять необъятное», то и рассмотрение будет ограничено прежде всего вопросами, связанными с применением электронной компонентной базы (точнее, сложными БИС и СБИС) в системах, связанных с обработкой и передачей важных информационных потоков, поддержание целостности и конфиденциальности которых принципиально важно для сохранения жизни и здоровья людей и/или безопасности государства. Мы попытаемся рассмотреть следующие вопросы:

- информационная безопасность ответственных видов аппаратуры (техники) при применении в них БИС и СБИС иностранного производства;
- собственно технологии обратного проектирования;
- физические (или, скорее, физико-механические) методы защиты от обратного проектирования;
- вопросы поставок контрафактной продукции;
- аппаратно-программные методы защиты от обратного проектирования и рассмотрение методов исследования содержимого памяти микросхем, от которых (методов) и применяется защита;
- контроль собственной продукции, ее применения и распространения;
- изменение точки зрения на обратное проектирование при существенном усложнении компонентной базы – система на кристалле, система в корпусе, 2.5D и 3D интегральные схемы.

Авторы приносят свои извинения тем специалистам, работы которых по различным причинам не отмечены в настоящей книге. Также авторы приносят извинения за в значительной степени фрагментарное изложение материала, а также за возможно излишне подробное изложение собственных работ по методам защиты микросхем от обратного проектирования. Авторы в этой книге пытаются показать, что в рассматриваемой области имеется широкое поле деятельности для активного читателя в плане предложения новых технических решений.

Авторы сознательно не рассматривают в деталях вопросы взаимодействия отечественных дизайн-центров с зарубежными фа-

бриками – изготовителями пластин со структурами, кристаллов микросхем и самих микросхем. Такое рассмотрение, по-видимому, значительно увеличило бы объем книги, хотя без упоминания этой проблемы обойтись не удалось. Также авторы не затрагивают в необходимой степени проблемы сертификации и безопасного использования сложно-функциональных блоков.

При рассмотрении методов обратного проектирования мы ограничили себя, если можно так выразиться, «классическим» подходом к обратному проектированию – простые неинвазивные методы (визуальный и рентгеновский контроль) и послойный анализ кристалла микросхемы. Мы лишь кратко затронули современные неинвазивные методы анализа микросхем – картографирование электромагнитной обстановки в ближнем поле, что также необходимо при анализе электромагнитной совместимости, и ее исследование в пространственной и временной областях, динамический анализ потребляемого тока, анализ оптического излучения из канала транзисторов при утонении кристалла микросхемы, исследование акустических шумов при работе таких устройств, как персональный компьютер. Именно последние методы позволяют получать ключевую криптографическую информацию из памяти микросхем. Детальное рассмотрение этих методов значительно увеличит объем книги. Кроме того, данные методы в целом аналогичны методам анализа отказов (производственный термин – анализ брака) в работе микросхем.

Монография подготовлена коллективом авторов (Белов Е.Н., Балыбин С.В., Пономарев А.А., Семенов А.В., Федорец В.Н., Швыдя О.В.) под общей редакцией доктора технических наук, старшего научного сотрудника Федорца Владимира Николаевича.

РАЗДЕЛ I

Вопросы информационной безопасности и обратное проектирование микросхем

– Пустыня – это бездарно! Но она существует. И с этим приходится считаться.
И. Ильф и Е. Петров «Золотой теленок»

Одной из принципиальных особенностей современного этапа развития радиоэлектронной аппаратуры (РЭА) является «массированное» использование различного рода вычислительных средств, позволяющих возложить на РЭА все большее количество интеллектуальных функций, ранее выполнявшихся человеком. Эта тенденция несомненно сохранится, а учитывая естественный рост объемов обрабатываемой информации и повышение ее ценности, проблемы обеспечения информационной безопасности создаваемой и эксплуатируемой техники различного рода и назначения постоянно усложняются. Естественно, что объединение различных видов и классов РЭА в сети усугубляет эти проблемы. Например, это коснулось аппаратуры медицинского назначения (от сбоев и отказов которой зависит жизнь пациентов, а информация медицинского характера может интересовать как физических, так и юридических лиц, например страховые компании). Поэтому «безопасность» здесь можно рассматривать как более общую категорию, например по ГОСТ Р 51898-2002 [11] – как «отсутствие недопустимого риска». Вполне логично, что при использовании ИМЭ вопросы информационной безопасности тесно связаны с надежностью и с функциональной безопасностью. Надежность технической системы определяется как свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования [12]. Проявление некоторых видов дефектов (в том числе умышленно внедряемых) как одной из угроз информационной безопасности в РЭА может приводить к отказам, так как вызывает факт нарушения работо-

способного состояния объекта. При этом критерии отказа должны совпадать с предварительно зафиксированными в технической документации. В ГОСТ 27.002-89 отмечается, что понятие критичности отказа и «классификация отказов по критичности (например по уровню прямых и косвенных потерь, связанных с наступлением отказа, или по трудоемкости восстановления после отказа) устанавливается нормативно-технической и (или) конструкторской (проектной) документацией по согласованию с заказчиком на основании технико-экономических соображений и соображений безопасности».

С позиций функциональной безопасности на надежность системы влияют только опасные отказы, которые приводят к человеческим жертвам, экономическому или экологическому ущербу [13].

В этой связи остро стоит проблема обеспечения информационной безопасности систем управления транспортом (включая как отдельные легковые авто, так и перевозку ценных или опасных грузов), проблемы безопасности (в том числе устойчивости, надежности и безотказности) систем связи, систем управления различными, в том числе опасными, производствами (объекты химической и атомной промышленности, например атомные электростанции).

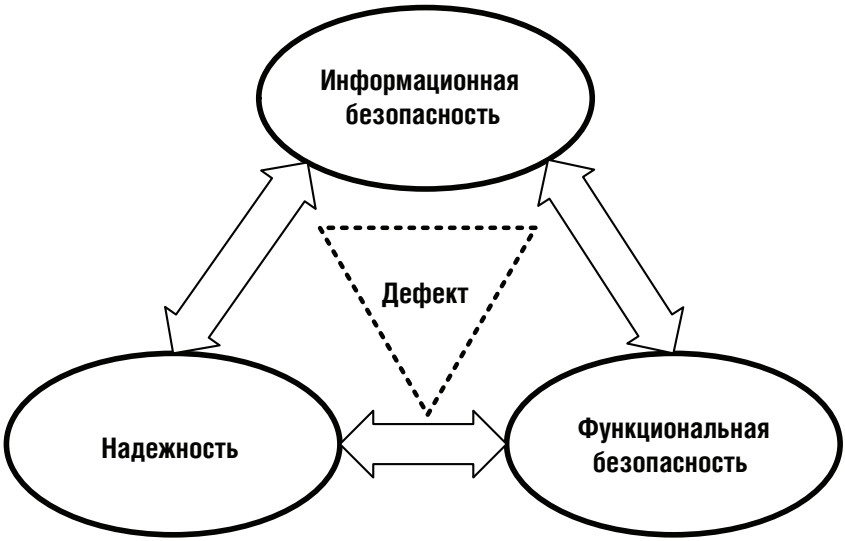

Рис. 1.1. Связь информационной безопасности с надежностью и функциональной безопасностью через понятие дефекта

Недопустимы сбои в системах энергоснабжения, газоснабжения и многих других инфраструктурных системах. Несколько обособленно (но не менее остро) стоят проблемы, связанные с обеспечением безопасности и обороноспособности государства.

Известно, что создание современных (а тем более перспективных) видов РЭА любого назначения возможно только на основе современной электронной компонентной базы (ЭКБ). Так как основой функционирования современных и будущих систем управления является получение, передача, накопление и обработка огромного объема информации, роль информационно-управляющих систем различного уровня трудно переоценить, причем эта роль в дальнейшей перспективе будет только возрастать.

Создание любых информационно-управляющих систем невозможно без соответствующих изделий микроэлектроники (ИМЭ), в первую очередь без больших и сверхбольших интегральных схем (БИС и СБИС), таких как микропроцессоры, микроконтроллеры, цифровые процессоры обработки сигналов и т. д. В дальнейшем все БИС и СБИС для информационно-управляющих систем условно будем именовать как БИС и СБИС для ответственных видов аппаратуры (ОВА), не забывая и о различиях в их реальном использовании (к примеру по срокам активной эксплуатации).

1.1. Глобализация в микроэлектронике – основная тенденция ее развития

Последние 20 лет ознаменовались революционными изменениями в микроэлектронике (МЭ). Прежде всего это масштабная глобализация в сочетании с глубокими изменениями структуры всей отрасли и радикальным ростом ее технологических возможностей. Рассмотрим эти изменения.

Технологический уровень развития МЭ характеризуется прежде всего величиной минимального топологического элемента ($d_{мин}$), формируемого на поверхности кристалла микросхемы. На момент написания данной работы в массовом производстве находятся микросхемы с $d_{мин} = 32$ нм (1 нм = 0,001 мкм $=10^{-9}$ м). Фирмы Intel и Samsung начали выпуск микросхем $d_{мин} = 22$ нм, а фирма AMD к 2015 г. освоила техпроцесс с $d_{мин} = 14–18$ нм [14, 15]. Фирма Samsung начала выпуск NANDFlash ЗУ емкостью 64 Гб по топологическим нормам 19 нм; с 2013 года начат выпуск таких ЗУ емкостью 128 Гб. Эта же фирма разработала ЗУ на фазовых пере-

ходах (типа PCM – phase-charge memory) емкостью 8 Гб. Фирма Intel разработала и презентовала опытный образец «ATOM-процессора» (шифр ROSEPOINT), содержащий процессор и WiFi-модуль на одном кристалле. Изделие выполнено по проектным нормам 32 нм, содержит несколько СФ-блоков, включая блок Intel On-chip System Fabric – коммутатор для тестирования с помощью внутреннего логического анализатора [16]. В перспективе планируется встроить в кристалл приемопередатчики 3G и 4G, а также антенну.

Еще в 2010 г. получены функционирующие элементы запоминающих устройств с $d_{мин} = 8$ нм (при $d_{мин} = 30–40$ нм на этом размере «укладывается» менее 100 атомов материала, например кремния). Серьезно обсуждается вопрос о транзисторах размером в несколько атомов.

Это традиционное направление развития МЭ, подчиняющееся закону Мура (удвоение числа транзисторов на кристалле приблизительно каждые 2 года), в перспективе [16–18] дополняется следующими:

- дальнейшее совершенствование традиционных направлений, в том числе обеспечение условий для встраивания радиочастотных трактов в типовые изделия, изготовленные по КМОП-процессу (в литературе встречается термин «за пределами КМОП»);
- «больше Мура»: рост сложности технологических процессов, поиск новых архитектур компонентов [19, 20], новых архитектур на системном уровне, новых методов в схемотехнике, новых материалов (диэлектрики, барьерные слои и др.). Данное направление весьма дорогостоящее и фактически обеспечивает сохранение действия закона Мура на ближайшие годы;
- «больше, чем Мур»: это интеграция различных технологий на кристалле и/или в корпусе (например сочетание микроэлектромеханических устройств и кристаллов с КМОП-микропроцессорами и другими элементами в одном корпусе).

Более детальное рассмотрение этих направлений выходит за рамки настоящей книги, однако само усложнение конечных изделий МЭ имеет прямое отношение к рассматриваемой проблеме – обеспечению защиты изделий микроэлектроники от обратного проектирования.

Полная стоимость производственной технологической «линейки» для производства ИМС с $d_{мин}$ = 60 нм может превышать 10 млрд долларов США, а для $d_{мин}$ = 20 нм оценивается в 50 млрд долларов США. Естественно, что такие затраты на организацию и освоение производства современных и перспективных ИМС доступны крайне ограниченному числу фирм. В настоящее время это фирмы Intel, Samsung, TSMC и, может быть, IBM. В свое время ожидание столь стремительного роста затрат на развитие и поддержание технологического уровня стимулировало организационную перестройку промышленности в мире (кроме СССР): появились фирмы, взявшие на себя решение проблем в области разработки, развития и поддержания на должном уровне технологических процессов. Естественно, что эти фирмы крайне заинтересованы в загрузке своих производственных мощностей, в том числе обеспечивая высокое качество продукции, осваивая новые технологические процессы и привлекая этим новых заказчиков. Полная загрузка мощностей – это необходимость, и она обусловлена рядом взаимозависимых и взаимосвязанных факторов, а именно производственными, экономическими, технологическими – стабильность технологических процессов и управляемость технологических процессов. К числу этих фирм относятся TSMC, UMC, Globalfoundries, PGC, X-FAB, IHP, SilTerra и др. Эти фирмы называются foundry, а в отечественной литературе встречается термин «кремниевые мастерские» (КМ). Особо необходимо отметить тот факт, что foundry-фирмы изготавливают микросхемы всех категорий (для потребителей с различными требованиями по стойкости к внешним воздействующим факторам): space, military, industrial, auto и т.д. Фундаментальными основами такой «многозадачности» являются: высокая стабильность технологических процессов на предприятиях – изготовителях кристаллов и значительная вариация объемов контрольно-измерительных операций в зависимости от категории микросхем. Именно объем контрольно-измерительных операций (включая стоимость специального корпуса и объем контрольно-измерительных операций после герметизации) и определяет в конечном итоге разницу в стоимости микросхем разных категорий, превышающую часто два порядка.

Несколько раньше появились фирмы, разрабатывающие микросхемы, но не имеющие производственно-технологической базы для их изготовления. Эти фирмы за рубежом называются fabless, а в отечественной литературе – «дизайн-центр» (ДЦ). К услугам

КМ обращаются такие фирмы, как AMD, TI, Intel, IBM и др. (имеющие собственное производство), а также ДЦ – фирмы Xilinx, ALTERA, российские UnikICs, «МЦСТ», «ЭЛВИС», «Миландр», «НИИМА Прогресс» и др. При этом продолжают существовать и развиваться фирмы, владеющие полным циклом «разработка – производство», особенно применительно к специальным случаям: радиационно-стойкие ИМС, ИМС на новых материалах, ИМС СВЧ-диапазона и т.д. [21–25]. Но для «массовых» изделий разделение на fabless и foundry (т.е. ДЦ и КМ) является однозначным, экономически и технологически эффективным и перспективным. Более того, выделились фирмы, разрабатывающие системы автоматизированного проектирования – САПР (Cadence, Mentor, Synopsys), развиваются фирмы, разрабатывающие различные «типовые» блоки и их модели для САПР (с учетом технологических норм и ограничений конкретного производителя). Эти блоки называются IP-блоками (Intellectual Properties), а в отечественной литературе – сложными функциональными блоки (СФ-блоки) [26, 27].

Производственно-технологические возможности вкупе с мощными системами проектирования стимулировали интенсивное развитие современных «заказных» БИС и СБИС, а также систем на кристалле (СнК или SoC – System-on-Chip). Для большинства фирм это направление интересно тем, что позволяет не только достичь предельных массогабаритных показателей при снижении стоимости сборочно-монтажных работ, но и какое-то время сохранить в тайне от конкурентов новые алгоритмы обработки информации или новинки в архитектуре (системо- и схемотехнике).

Типичным примером СнК «начального» уровня может служить приемник спутниковых навигационных систем – уже достаточно известная среди разработчиков РЭА микросхема RFIC02 (Беларусь) – радиоприемное устройство для систем GPS и GLONASS (рис. 1.2).

Последние 4–5 лет отмечены разработками систем в корпусе (СвК, system-in-package – SiP) – в определенной степени экономической и технологической альтернативе СнК, а также методов наиболее «плотной» компоновки самих СнК. Системы в корпусе по своей сути являются развитием существовавших ранее микросборок и гибридных интегральных схем и считаются перспективнейшим направлением современного развития микроэлектроники [17, 18, 28].