Современные технологии контроля безопасности в микроэлектронике

Анатолий БЕЛОУС,
д. т. н.
ABelous@integral.by
Виталий СОЛОДУХА,
к. т. н.
VSaladukha@integral.by

Задачи обеспечения информационной безопасности давно и хорошо известны специалистам. Однако обеспечение контроля безопасности в микроэлектронике — проблема новая для российских инженеров, и пока на страницах научно-технической печати она, за редким исключением, не обсуждается. В статье рассмотрены основные пути решения этой проблемы за рубежом, а именно концепции, средства и методы обеспечения безопасности каналов поставок импортной ЭКБ для комплектации радиоэлектронных систем ответственного назначения.

Введение

Цель данной работы — анализ зарубежного опыта в области обеспечения безопасности каналов поставок микросхем, изготовленных на иностранных полупроводниковых производствах и предназначенных для комплектации радиоэлектронных систем ответственного назначения. В публикации будут рассмотрены основы государственной политики США и стран НАТО, концепции, методы, нормативные требования и основные технические средства обеспечения безопасности (достоверности) в современном микроэлектронном производстве.

Вопросы обеспечения безопасности в микроэлектронике начали активно обсуждаться за рубежом в открытой научно–технической печати более 20 лет назад. Интерес иностранных исследователей, и особенно военных специалистов, к этой сфере обусловлен следующими объективными факторами:

1. Экономическими причинами и глобализацией мировой полупроводниковой индустрии, процессами слияний и поглощений полупроводниковых фирм.
2. Процессом переноса полупроводниковых производств из высокоразвитых индустриальных стран (США, Англия, страны НАТО) в развивающиеся страны Юго-Восточной Азии (Китай, Тайвань, Южная Корея, Япония).
3. Результатами теоретических и экспериментальных исследований феномена появления проблем аппаратных троянов в микросхемах.
4. Эволюционным изменением парадигмы проектирования (разработки) микросхем.
5. Появлением нового вида оружия — информационно-технического оружия (за рубежом принят термин «кибероружие»), существенно расширяющего возможности и снимающего существенные ограничения «классического» современного оружия (атомного, биологического, СВЧ оружия, климатического, сейсмического и других видов).

В основе вышеуказанных процессов глобализации лежит тот очевидный факт, что при уменьшении проектных норм количество используемых в современных технологиях новых материалов растет по экспоненте, и обычно одна, даже «очень богатая» полупроводниковая компания не может найти требуемые дополнительные миллиарды долларов, а потому «полупроводниковые гиганты» вынуждены объединять финансовые и людские ресурсы [1].

Необратимый процесс переноса полупроводниковых производств в страны ЮВА обусловлен чисто экономическими причинами: например, еще в 2005–2010 гг., чтобы построить новый полупроводниковый завод в Китае, инвестор тратил на $2–3 млрд меньше, чем в США, причем разрешение на строительство в Поднебесной можно было получить чуть ли не в течение месяца, тогда как в США эта процедура занимает годы.

Зарубежные исследователи показали, что без ведома разработчика в каждую микросхему можно внедрить аппаратный троян практически на любой стадии маршрута — от проектирования до изготовления. По команде своего «хозяина» троян способен выполнять самые различные несанкционированные действия — изменять режимы функционирования, передавать по сторонним (неконтролируемым) каналам любую внутреннюю (секретную) информацию, изменять электрические режимы работы микросхемы вплоть до ее разрушения (отказа) по внешнему сигналу злоумышленника.

Впервые факт внедрения такого трояна в микросхему был документально зафиксирован в «лихие 90-е» Сергеем Скоробогатовым, выпускником московского вуза, нашедшим работу в одном из университетов США. Эта микросхема рекламировалась и разработчиком, и Министерством обороны США как абсолютно безопасная, с многоуровневой защитой. Поэтому она много лет широко использовалась в военных системах (подводные лодки, самолеты, высокоточное оружие).

Эволюция классической парадигмы проектирования микросхем ответственного назначения

Следующий фактор, существенно изменивший «парадигмы проектирования», хорошо известен зарубежным разработчикам микросхем. Отечественные разработчики пока проектируют «по старинке», поскольку и государственные заказчики таких микросхем, похоже, сами не знают об этом крайне неприятном факте.

Как известно, для любого разработчика современной микросхемы «руководящим документом» является техническое задание (ТЗ) на микросхему или общее техническое задание (ОТЗ) для комплекта разрабатываемых микросхем.

В отличие от обычных для отечественных разработчиков стандартных требований к микросхеме, предусматривающих описание функций, временных диаграмм протокольного обмена, быстродействия, рабочей частоты, максимальной величины потребляемой мощности, уровней стойкости к ионизирующим излучениям, помехам по входам и цепям питания, устойчивости к разрядам статического электричества, надежностным характеристикам (безотказность, наработка на отказ, срок активного функционирования в космосе и т. п.), уже более 10 лет зарубежный разработчик получает от заказчика (обычно

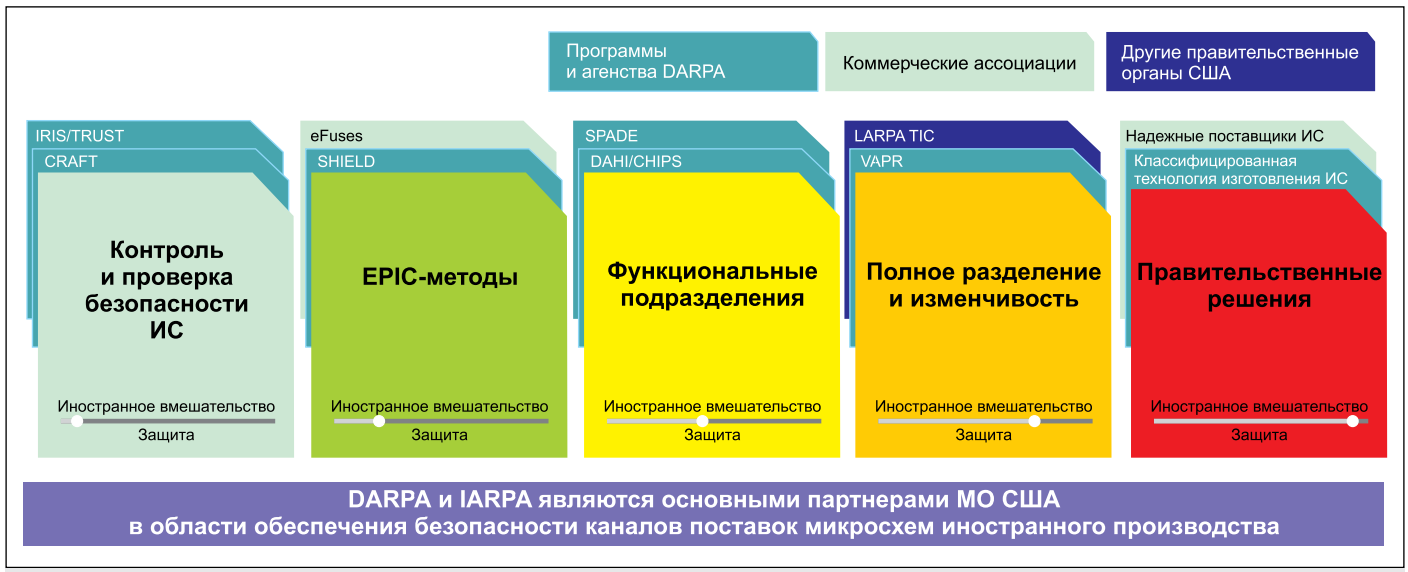

Рис. 1. Американская «золотая пятерка безопасности» — основные направления разработки комплексов нормативно-технических мероприятий, директив и программ обеспечения безопасности каналов поставки микросхем

от Министерства обороны США или NASA) стандартный дополнительный «пункт». Этот достаточно объемный «пункт» (раздел ТЗ) называется: «Методы, средства и порядок применения технологии контроля безопасности разрабатываемой микросхемы».

Небольшое, но важное «отвлечение от темы». С уменьшением проектных норм существенно возрастает стоимость разработки иностранных микросхем. Отечественные разработчики, как российские, так и белорусские, используют эти официальные статистические данные для обоснования увеличения стоимости своих НИОКР при защите финпланов (затрат) на разработку микросхемы перед финансовыми ведомствами своих стран (в основном, когда речь идет о государственном бюджетном финансировании мероприятий Гособоронзаказа). Простодушные и доверчивые чиновники Минпрома, Минэкономразвития и т. п. обычно весьма далеки от мирских «микроэлектронных» проблем и не могут знать истинной причины столь высокой стоимости импортных изделий.

Но сегодня зарубежные финансисты хорошо знают, что в многомиллионной стоимости разработки субмикронных микросхем 25–75% составляют затраты на реализацию и обеспечение методов технологической безопасности микросхем. Термин «технология контроля безопасности в микроэлектронике» впервые появился в научно-технической литературе после 2005 года, когда по результатам расследования Министерство юстиции США опубликовало полный судебный отчет, известный у нас, к сожалению, только узкому кругу специалистов и содержащий сведения о том, как контрафактные микросхемы попадают в военные и коммерческие системы США и их союзников. Исходной точкой в этом многотомном судебном расследовании стала полученная от глубоко внедренной на китайских полупроводниковых заводах агентуры ЦРУ информация о методах, средствах и каналах поставок в США и страны НАТО фальшивых «супернадежных» микросхем. В вышедшей в 2018 году в издательстве «Техносфера» нашей книге [2], посвященной столь непростой теме (фактически это первая в мире техническая энциклопедия по проблемам программных и аппаратных троянов) данные вопросы рассмотрены более детально и аргументировано. Основная цель технической энциклопедии — не только обобщить и систематизировать уже имеющийся опыт борьбы с этой реальной угрозой (программными и аппаратными троянами), но и дать возможность разработчикам микросхем ответственного (военного и космического) назначения и руководителям компетентных министерств и ведомств, наконец, оценить и осознать эту суровую реальность (уже давно известную из американского опыта!) и предпринять все необходимые меры по ее нейтрализации при формировании каналов поставки иностранных микросхем в Россию.

Причины появления программных и аппаратных троянов

В технической энциклопедии [2] показано, что детальный анализ поистине огромных возможностей и столь же очевидных ограничений всех существующих сегодня видов «классических» вооружений (атомного, биологического, космического, СВЧ-оружия нелетального и летального действия) и пока таких «экзотических» видов оружия, как климатическое, сейсмическое, психологическое, нейронное и т. д., приводит к очевидному выводу, что их реальное применение на Земле станет не чем иным, как достаточно изощренным «способом самоубийства». Именно поэтому в недрах военных и разведывательных ведомств индустриально развитых стран и появилась идея разработки совершенно нового вида оружия, по замыслу его идеологов применение которого позволит реально «победить и выжить» нападающей стороне. Это и есть так называемое научно-техническое оружие, или кибероружие, как именуют его западные журналисты.

Своеобразной технической платформой этого нового вида оружия являются программные и аппаратные трояны, которые несанкционированно от владельцев, внедряясь в соответствии со злой волей «хозяина» в современные информационно-коммуникационные системы, системы телекоммуникаций, системы противоракетной обороны, системы энерго- и жизнеобеспечения мегаполисов, системы управления высокоточным оружием и т. д., способны не только организовывать передачу «хозяину» секретной информации, но и перехватывать управление этими объектами, вплоть до приведения их в полностью неработоспособное состояние.

Специалистами Министерства обороны США, а также входящих в его структуру разведывательных сообществ (ФБР, АНБ — аналоги российского ФСБ, кстати, многие читатели до сир пор наивно полагают, будто все эти ведомства подчиняются чуть ли непосредственно сенату или президенту США — это совсем не так) в повседневной практике очень часто используется термин «технологии контроля безопасности в микроэлектронике».

Что же это означает«по американским понятиям»? (Для отечественной технической литературы это пока «малопонятный» термин, как и все, что за ним стоит.) В основе данного определения лежит известное сегодня только западным разработчикам микросхем выражение: «Контроль безопасности в микроэлектронике абсолютно необходим, если у вас нет надежного фаундри».

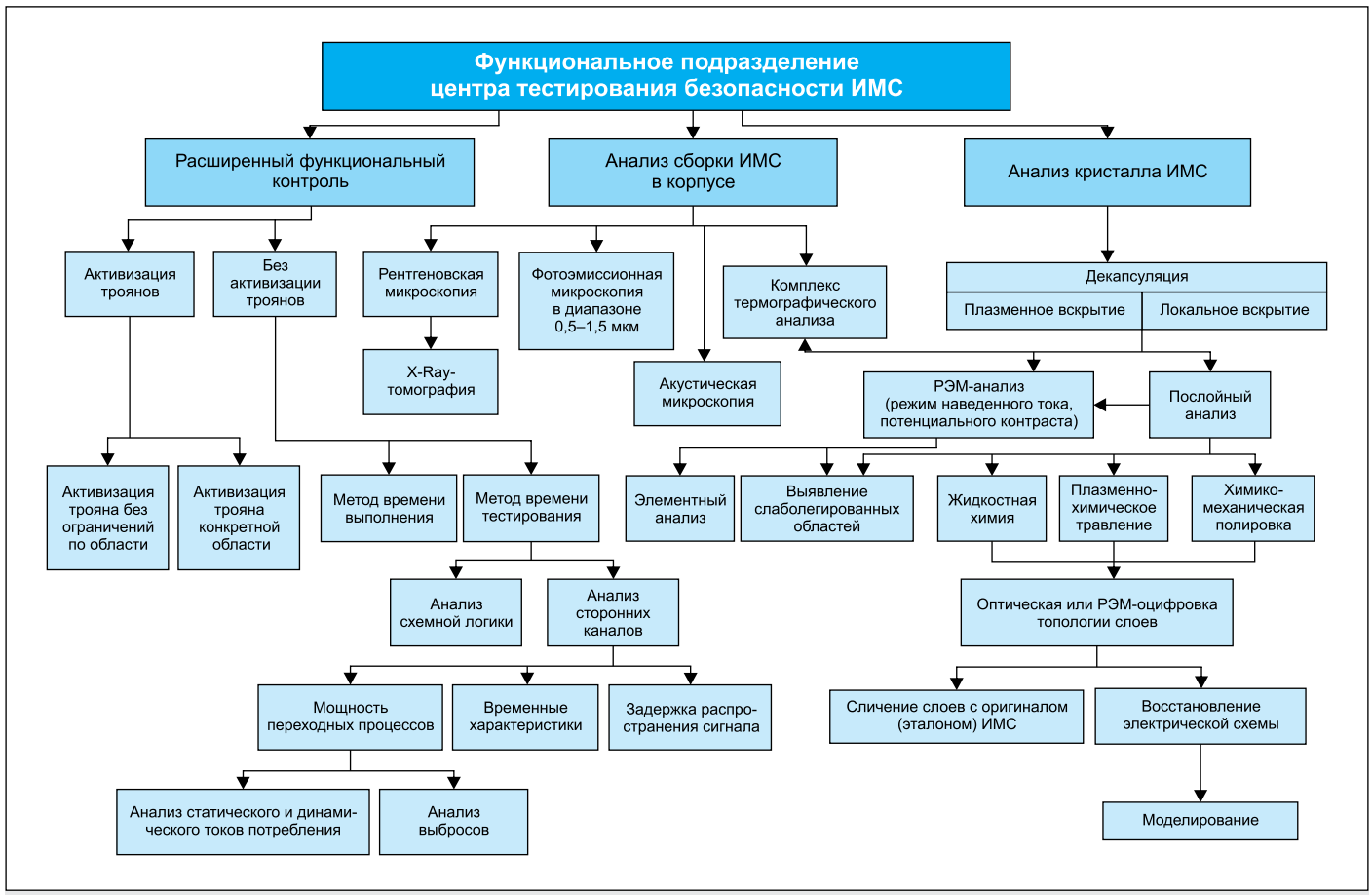

Рис. 2. Минимальный состав функциональных подразделений (лабораторий) центра тестирования безопасности микросхем

Место и роль технологий контроля безопасности в современной микроэлектронике

Как было показано в [2], в основе функционирования американской системы контроля безопасности микроэлектронных изделий лежит принцип «золотой пятерки безопасности». Эта «золотая пятерка безопасности» была сформирована в США в результате многолетней скоординированной деятельности военных, разведслужб, промышленных и правительственных органов США в области обеспечения каналов поставок так называемых «достоверных» микросхем иностранного производства (рис. 1).

Американская «золотая пятерка безопасности» — свод «толстых» комплексов нормативно-технических документов, различных правительственных (!) директив и постоянно действующих программ, конкретных мероприятий по обеспечению безопасности каналов поставки микросхем для Министерства обороны США, НАСА и стран НАТО, спроектированных в США, но изготовленных за пределами страны, в основном на полупроводниковых фабриках ЮВА. Эти пять базовых направлений, предусматривающих обеспечение защиты безопасности каналов поставок микросхем «иностранного» производства, оформлены в виде соответствующих «томов» комплексов директивных, нормативно-технических и «правительственных» документов с единым (общим) подзаголовком, который в непрофессиональном авторском переводе на русский язык можно сформулировать так: «Иностранное вмешательство. Защита».

Ниже перечислим эти комплексные направления контроля безопасности микроэлектронных изделий:

- методы контроля и проверки безопасности микросхем (IRIS, TRUST, CRAFT);
- методы контроля иностранных производств (EPIC, eFuse, SHIELD);
- методы функционального контроля аппаратных троянов в микросхемах (SPADE, DAHI/CHIPS и др.);
- методы искусственного разделения компонентов функционального контроля (LARPA TIC, VAPR и др.);
- решения правительства США в области утверждения перечня «надежных» поставщиков микросхем (надежных сертифицированных технологических линий, надежных сборочных производств).

В свою очередь, все методы контроля и проверки безопасности (первое направление «пятерки») можно разделить на три большие группы:

- анализ кристаллов микросхем;
- расширенный функциональный контроль с целью активации возможных скрытых аппаратных троянов в микросхемах;
- углубленный анализ собранных в корпус микросхем, систем в корпусе и систем на кристалле (SoC).

В структуре Министерства обороны США в итоге был создан ряд специальных подразделений, основные функции которых подобны функциям их российских аналогов: 18 ЦНИИ МО РФ, 46 ЦНИИ МО РФ, филиал ЦНИИ МО РФ (бывший 22 ЦНИИ).

Надо сказать, что наиболее известное из открытых источников подобное «антитроянское» подразделение — это специальное подразделение МО США — JFAC (Объединенный Федеративный Центр обеспечения надежности микросхем).

На рис. 2 представлена упрощенная основная (известная экспертам) информация об основных функциональных подразделениях этого центра, составленная авторами статьи в результате посещения ими целого ряда международных конференций по «троянским проблемам».

Возвращаясь к проблеме «эволюционного изменения парадигмы проектирования микросхем», надо отметить следующий интересный для читателя факт. Как мы уже убедились, американцы тоже большие любители различных «лозунгов» и «слоганов». В этом они даже

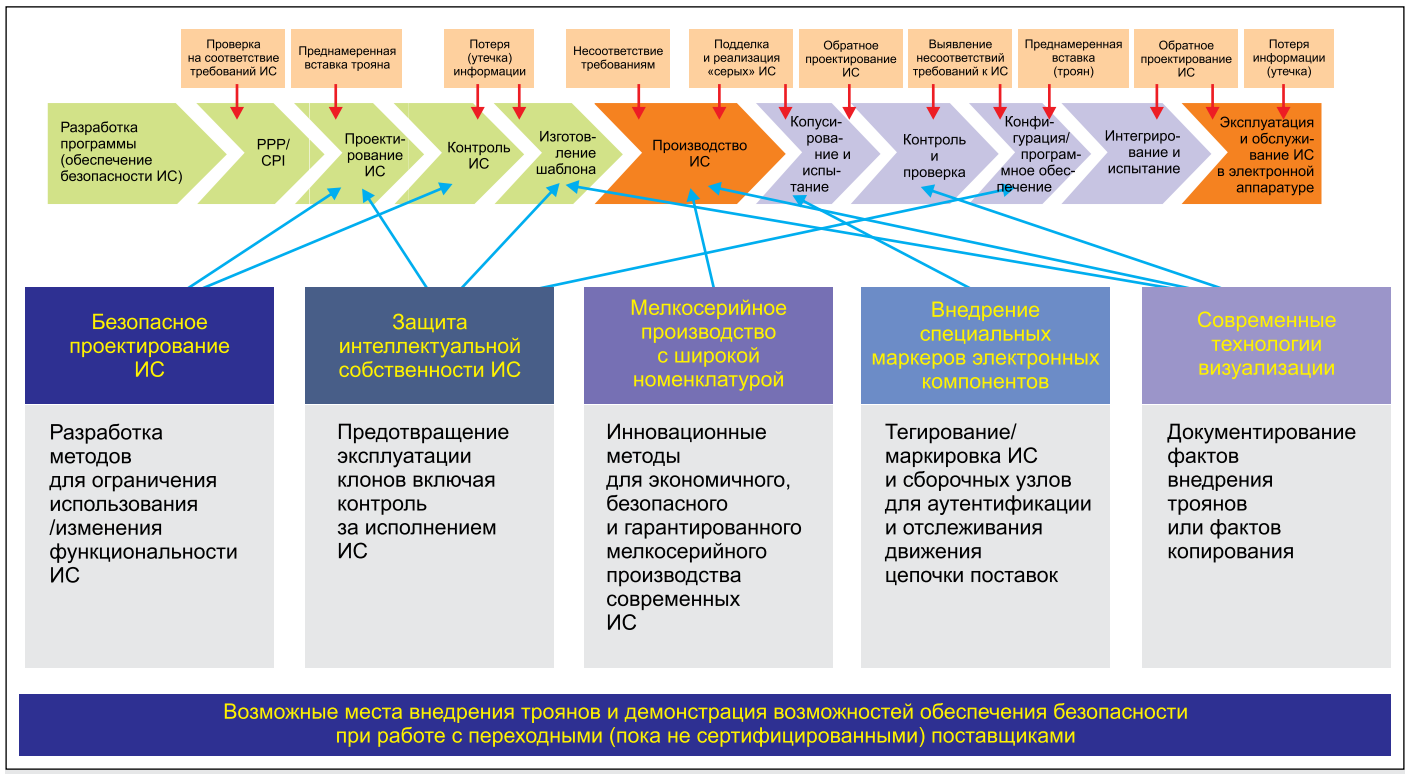

Рис. 3. Графическое представление последовательности основных этапов цикла изготовления и контроля микросхем на не сертифицированной заказчиком (ненадежной) фабрике

превзошли ЦК КПСС времен Л. И. Брежнева с лозунгами той эпохи типа: «Экономика должна быть экономной!». На входе в один из головных офисов Федерального Центра висит слоган: «Безопасность не бывает бесплатной». В этой короткой фразе скрыт большой смысл.

Если ее «развернуть», то ситуация выглядит следующим образом. По экспертным оценкам западных специалистов, в многомиллионной «долларовой стоимости» разработки современных микросхем 25–75% составляют затраты на обеспечение надежности и технологической безопасности (проверка на возможное наличие внедренных злоумышленниками аппаратных троянов). Смысл этого американского слогана прост: «Если ты пришел к нам с заказом на тестирование по одному или по всем трем направлениям нашей деятельности для проверки безопасности разработанных тобой и изготовленных в ЮВА микросхем, то ты должен понимать, что это будет стоить тебе «больших» денег».

Такой большой разброс процентного соотношения стоимости работ зависит от конкретных требований конечного заказчика, от технологии изготовления микросхемы, от ее функциональной сложности и целевого назначения. Как показали авторы в цитируемой выше технической энциклопедии, с увеличением степени интеграции, уменьшением уровня используемых проектных норм резко возрастают технические проблемы, связанные с применением разработанных аналитических методов типа «анализ скрытых каналов, метод TESR, анализ тепловых излучений, метод анализа цепей питания, метод кольцевых генераторов и др.», и соответствующее аналитическое оборудование стоит десятки миллионов долларов.

Ну а если анализируемая микросхема предназначена для работы в составе особо важных, стратегических или военных электронных систем (атомная промышленность, высокоточное оружие, подводные лодки, космическая разведка и т. п.), то для обеспечения заданного заказчиком высокого уровня технологической безопасности необходимо проводить не один-два, а максимальный цикл исследований с использованием всех самых современных (и не всегда публикуемых в открытой научно-технической печати) методов анализа и дорогостоящего оборудования.

Понятно, что организационная структура подобных Центров, как и описание конкретных задач, входящих в их состав функциональных подразделений (лабораторий), описание типа и характеристик используемого оборудования и методик анализа являются служебными и техническими ноу-хау соответствующих служб и департаментов МО США. Это мировая практика. Действительно, что, например, «обычный читатель» может узнать о 18 ЦНИИ МО РФ, кроме самого факта его существования в структуре российского Министерства обороны?

На рис. 3 представлена последовательность основных этапов реализации цикла изготовления и контроля безопасности микросхем, выполненных по заказу МО США на несертифицированной (непроверенной, ненадежной) полупроводниковой фабрике. Здесь показан весь жизненный цикл изготовления микросхем для МО США с указанием как конкретных проверочных функций, так и возможных нежелательных последствий (утечка секретной информации, клонирование, поставки «серых» микросхем и т. п.).

Методы выявления аппаратных троянов в микросхемах

Следует отметить, что сегодня известно достаточно много методов выявления аппаратных троянов в микросхемах [2]. Здесь же мы приведем названия только наиболее популярных методов. Это, например, методы анализа по боковым (сторонним) каналам, на основе анализа спектра электромагнитного излучения микросхемы, метод автореференции (TeSP), метод кольцевых генераторов, функциональная валидация, метод design-for-trust, метод обфускации и многие другие.

К вопросу о порядке использования микросхем ответственного (критического) применения предприятиями российского ОПК

В настоящее время порядок использования микросхем для критических (ответственных) назначений регламентируется рядом нормативных актов. Так, российские предприятия ОПК могут без ограничений применять только изделия, включенные в Перечень электронной компонентной базы, разрешен-

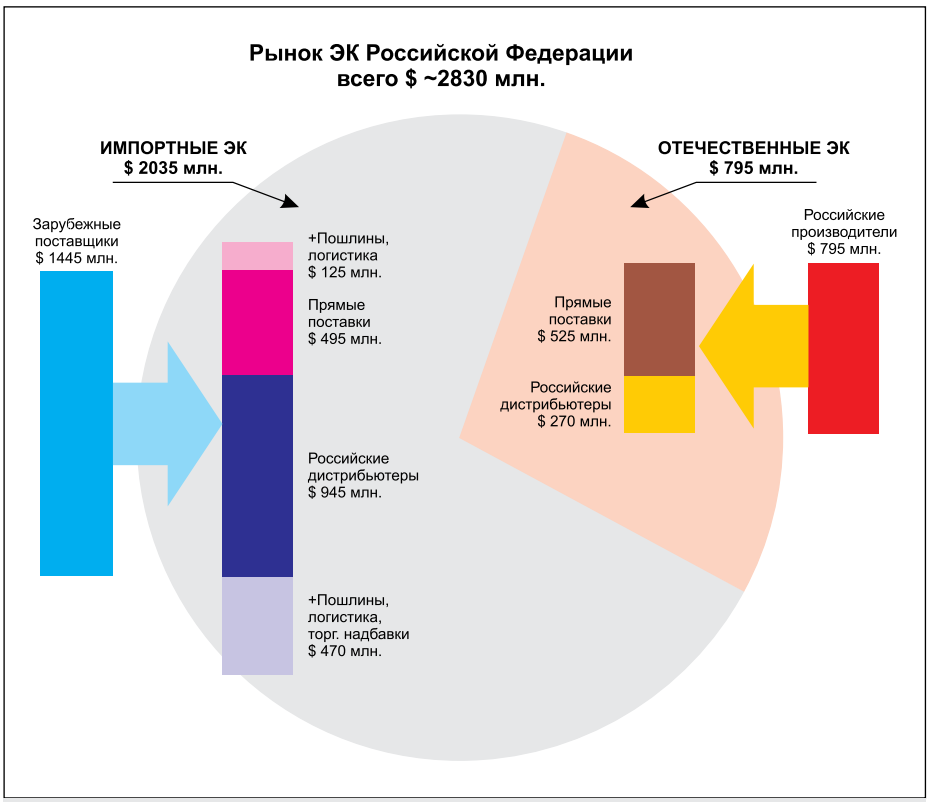

Рис. 4. Обобщенная структура каналов поставки ЭКБ в РФ [3]
Примечание. Здесь поставки через компании-комплектаторы приравнены к прямым поставкам

ной для применения при разработке, модернизации, производстве и эксплуатации вооружения, военной и специальной техники (Перечень ЭКБ 02).

В данный Перечень включена вся отечественная (российская и белорусская) ЭКБ, разработанная и производимая под контролем Военных Представительств РФ и РБ. Хотя почти все изделия из этого Перечня действительно можно отнести к безопасным с высокой долей вероятности, в последнее время в этот документ стали включать изделия, к конструкции которых в процессе проектирования либо изготовления существует прямой или опосредованный доступ третьих лиц (сторон). Так, целый ряд изделий был создан с применением так называемых IP-блоков (библиотек) иностранного происхождения.

По сути разработка микросхем в этих случаях свелась фактически только к «сборке» структуры (архитектуры) микросхемы из нескольких составных частей без достаточно полного понимания и анализа их содержимого. Второй важный момент — изготовление таких разработанных в РФ изделий на «несертифицированном» российским заказчиком фаундри-производстве. Говорить о возможности полного контроля за процессом в данном случае, конечно же, не приходится.

Для сравнения, на конец 2017 года Министерство обороны США имело в своем распоряжении 23 сертифицированные фабрики, которые в итоге позволяли американцам размещать свои заказы на изготовление с последующей сертифицированной поставкой микросхем, выпускаемых по двадцати различным технологиям (количество технологических опций для каждой технологической платформы варьируется от трех до десяти):

- стандартный CMOS;
- NVRAM CMOSMixed Signal CMOS;
- NVRAM CMOSMixed Signal CMOS+SONOS NVM;
- RF CMOS;
- HV CMOS;
- RH CMOS;
- CMOS Image Sensor;
- SOI CMOS;
- Thin Film SOI CMOS;
- RH SOI CMOS;
- SOS;
- BICMOS;
- CCD Image Sensor;
- Bipolar;
- GaAs;
- GaN;
- inP;
- SiGe SOI;
- SiGe.

Как видим, это все известные нам сегодня современные технологии. Понятно, любые, вновь появившиеся микроэлектронные технологии немедленно будут включены в список сертифицированных поставщиков. Мы помним провозглашенную американцами стратегию достижения безусловного технологического превосходства США — здесь абсолютно не имеет значения, что эти фабрики в основном расположены не на американской территории. Надо ясно понимать еще один важный момент: для всех современных фабрик, расположенных вне территории США, в принципе тоже не имеет особого значения, кто конкретно их сертифицирует (за сертификацию они получают дополнительные дивиденды) — американский «дядя Сэм» или русский «Младший Брат» — ведь эти фабрики нужно загружать заказами, и сегодня очень немногие полупроводниковые фабрики работают на полную мощность, иногда загрузка их производственных линий составляет лишь 30–50% от проектной мощности. Более того, между фабриками постоянно идет ожесточенная конкурентная борьба за заказчиков: здесь будут рады каждому новому клиенту и никакие очередные «санкции» не сработают.

Поэтому, чтобы достичь заданных заказчиком (Минпромторг или Минобороны РФ) тактико-технических характеристик радиоэлектронной аппаратуры, из-за отсутствия отечественных аналогов разработчики нередко вынуждены ориентироваться на ЭКБ иностранного производства.

Здесь следует отметить два аспекта:

1. Для ЭКБ категорий MIL-grade и SPACE-grade возможность прямых поставок исключена, а при покупке через третьи руки серьезно возрастает опасность как поставки изделий с вредоносными аппаратными троянами и программными закладками, так и банального контрафакта.
2. Для ЭКБ категории INDUSTRIAL при умеренной опасности закладок статистические показатели качества и надежности имеют большие разбросы. Часто отсутствует конкретная информация по количественным показателям надежности, нет жесткого контроля сборки и качества партии.

Гарантировать безопасное применение ЭКБ импортного производства возможно только после проведения дорогостоящих операций скрининга, серии испытаний и исследований, позволяющих оценить надежность и стойкость к специальным факторам конкретной партии изделий, и реинжиниринга — анализа топологии, восстановления схемы электрической и поиска незадокументированных элементов.

К сожалению, использование импортной ЭКБ для критических применений будет иметь место еще длительное время.

На рис. 4 представлена обобщенная структура поставок в РФ ЭКБ в денежном выражении за 2017 год [3]. Как видим, из общего объема российского рынка, $2830 млн, объем приобретенной импортной ЭКБ составил $2035 млн, а отечественной — $795 млн.

В связи с этим крайне важно разработать действенные методы защиты от попадания в состав российской радиоэлектронной аппаратуры ЭКБ с вредоносными составляющими.

В заключение надо отметить, что американцам удалось с большим трудом создать и внедрить в практику вышеописанную си-

стему контроля безопасности каналов поставки микросхем. Здесь будет уместно привести слова одного из идеологов и организаторов системы контроля — директора Центра исследований в области проектирования систем военного назначения (SERC) господина Д. Скотта Лусеро, начальника соответствующего отделения, заместителя министра обороны США по проектированию систем (примерный советский аналог названия должности — заместитель министра обороны СССР по радиоэлектронике; такая должность была введена решением правительства СССР, чтобы обеспечивать оперативную связь военных и разработчиков РЭА, и существовала вплоть до развала СССР), сказанные им на 19-й ежегодной Конференции по проектированию систем Национальной ассоциации оборонной промышленности США (NDIA), которая состоялась в октябре 2015 года Спрингфилде, штат Вирджиния. Хотя основная часть доклада была посвящена описанию методологии работы центра исследований в области проектирования систем военного назначения (SERC), в том числе защищенных и надежных систем — от револьвера до американского палубного истребителя бомбардировщика F/A-18 «Хорнет», нашлось в нем место и «троянским» проблемам. Господин Скотт обратился к словам философа, жившего целых пять веков назад, чтобы подчеркнуть всю сложность вечной проблемы «замены старых порядков новыми» в супердемократическом американском обществе, в котором армия является его неотъемлемой частью.

Конкретно он привел высказывание Николо Макиавелли («Государь», глава 6): 2 А надо знать, что нет дела, коего устройство было бы труднее, ведение опаснее, а успех сомнительнее, чем замена «старых» порядков «новыми». Кто бы ни выступал с подобным начинанием, его ожидает враждебность тех, кому выгодны старые порядки и холодность тех, кому выгодны новые».

Суть доклада американского генерала сводилась к тому, что какие бы эффективные методы организации безопасного микроэлектронного производства и методы противодействия троянским атакам ни предлагались техническими экспертами, их ожидает «враждебность» тех, кому выгодны старые порядки, и «холодность» тех, кому выгодны новые.

Заключение

Авторы считают, что в данной работе новыми являются следующие положения и результаты.

Впервые в отечественной научно-технической печати рассмотрены основные положения государственной политики США и стран НАТО в области обеспечения безопасности каналов поставок микросхем зарубежного производства, предназначенных для комплектации систем ответственного назначения — космической техники, систем вооружений и военной техники, систем управления энергетическими и транспортными потоками и т. п. Рассмотрены основные концепции, методы, нормативная и законодательная база и технические средства обеспечения безопасности в современной микроэлектронике.

Показано, что обеспечение технологической безопасности в микроэлектронике отнесено в США и странах НАТО к числу государственных задач с высшим приоритетом важности. Решением правительства США головная роль в обеспечении безопасности каналов поставки ЭКБ для систем ответственного назначения возложена на Министерство обороны США.

Рассмотрены экономические причины и следствия процессов глобализации полупроводникового производства, причины и следствия изменения парадигмы проектирования (разработки) современных микросхем, обусловленные появлением новых угроз безопасности — аппаратных троянов в микросхемах.

Показана роль и место программных и аппаратных троянов в создании нового типа оружия — информационно-технического (известного за рубежом как кибероружие), где эти трояны фактически являются так называемой технологической платформой кибероружия.

На основании вышеизложенного можно сформулировать краткие выводы и рекомендации:

- Наибольшие угрозы безопасности для предприятий российского ОПК имеют место для каналов поставок ЭКБ иностранного изготовления. Поскольку важное значение этого канала для развития современных электронных систем управления вооружения и военной техники по вышеуказанным причинам в ближайшей и отдаленной перспективе будет сохраняться, именно здесь необходимо сконцентрировать усилия на создании соответствующей инфраструктуры безопасности каналов поставок — от разработки комплекса нормативно-технической документации по «американским калькам» до создания отечественных центров компетенции.
- Необходимо также разработать и ввести в действие комплект нормативно-технической документации, разрешающей предприятиям ОПК РФ использовать в аппаратуре военного и космического назначения индустриальные компоненты, которые американцы уже более 30 лет успешно применяют как в военной, так и в космической технике. Более того, как показано выше, с точки зрения обеспечения безопасности каналов поставки для этого класса микросхем задача существенно упрощается: вероятность приобретения на мировом рынке индустриальной микросхемы с внедренным троянom близка к нулю.

Литература

1. Макушин М. Волна сделок слияния/поглощения в микроэлектронике: причины и последствия // Электроника НТБ. 2018. № 1.
2. Белоус А. И., Солодуха В. А., Шведов С. В. Программные и аппаратные трояны — способы внедрения и методы противодействия. Первая техническая энциклопедия. В 2-х книгах. М.: Техносфера, 2018.
3. Отчет исследования российского рынка электронных компонентов. Информационно-аналитический Центр Современной Электроники. ООО «СОВЭЛ», 2018.