УДК 621.382.049.77-049.5(045) DOI: 10.22184/NanoRus.2019.12.89.19.26

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ КОНТРОЛЯ БЕЗОПАСНОСТИ В МИКРОЭЛЕКТРОНИКЕ

MODERN TECHNOLOGIES FOR SECURITY CONTROL IN MICROELECTRONICS

БЕЛОУС АНАТОЛИЙ ИВАНОВИЧ
Член-корреспондент НАН Беларуси, д.т.н., заместитель генерального директора
ABelous@integral.by

СОЛОДУХА ВИТАЛИЙ АЛЕКСАНДРОВИЧ
К.т.н., генеральный директор
VSaladukha@integral.by

ОАО «ИНТЕГРАЛ» — управляющая компания холдинга «ИНТЕГРАЛ»
Республика Беларусь, 220108, г. Минск, ул. Казинца И.П., 121А, к. 327
www.integral.by

BELOUS ANATOLY I.
Corresponding Member of the National Academy of Sciences of Belarus, Doctor of Technical Sciences, Deputy General Director
ABelous@integral.by

SALADUKHA VITALI A.
Ph.D, General Director
VSaladukha@integral.by

JSC "INTEGRAL" — "INTEGRAL" Holding Managing Company
Room 327, 121A, Kazintsa I. P. St., Minsk, Republic of Belarus, 220108
www.integral.by

Проблемы обеспечения информационной безопасности специалистам давно и достаточно хорошо известны. Обеспечение контроля безопасности в микроэлектронике для российских инженеров — проблема новая, 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.
Problems of ensuring the informational security have long since been well known to specialists. The problem of ensuring the security control in microelectronics for Russian engineers is a new problem and so far it is beyond discussion, with rare exception, on the pages of the scientific-technical press. The article considers the main means of coping with this problem abroad, specifically — concepts, methods and means of ensuring safety of the delivery channels of the import element component base for completeness of the radio-electronic systems of sensitive application.

ВВЕДЕНИЕ В ПРОБЛЕМУ

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

Проблемы обеспечения информационной безопасности специалистам давно и достаточно хорошо известны. Обеспечение безопасности в микроэлектронике для российских инженеров — это проблема новая, и пока на страницах отечественной научно-технической печати она, за редким исключением, не обсуждается.

Но за рубежом эта проблема активно начала обсуждаться в открытой научно-технической печати более 20 лет назад. Интерес зарубежных исследователей и особенно военных специалистов к этой проблеме был обусловлен следующими *объективными факторами*:

1. Экономическими причинами и следствиями глобализации 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 (ЮВА) (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 (за рубежом принят термин «кибероружие»), существенно расширяющего возможности и снимающего существенные ограничения «классического» современного оружия (атомного, биологического, СВЧ-оружия, климатического, сейсмического и др. видов оружия).

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

Необратимый *процесс переноса полупроводниковых производств* в страны ЮВА был обусловлен чисто экономическими причинами: строительство нового полупроводникового завода, например, в Китае еще в 2005–2010 гг. инвестору обходилось

на 2–3 млрд долл. США дешевле, чем в США, причем разрешение на строительство завода в Китае можно получить чуть ли не в течение одного месяца, а в США эта процедура занимает годы.

Зарубежными исследователями было показано, что в любую микросхему без ведома разработчика можно внедрить *аппаратный троян* практически на любой стадии маршрута — от этапа проектирования до изготовления. Этот троян может по команде своего «хозяина» выполнять самые различные несанкционированные функции — 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 выпускником одного из вузов Москвы Сергеем Скоробогатовым, в «лихие 90-е годы» нашедшим себе работу в одном из университетов США. Эта микросхема рекламировалась как разработчиком, так 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 — существенное *изменение «парадигмы проектирования»*, хорошо известен зарубежным разработчикам микросхем. Отечественные разработчики пока проектируют «по старинке», поскольку и государственные заказчики этих микросхем, похоже, сами не знают об этом крайне неприятном факте.

Как известно, «Руководящий документ» для любого разработчика современной микросхемы — это техническое задание (ТЗ) на микросхему или общее техническое задание (ОТЗ) для комплекта разрабатываемых микросхем.

В отличие от обычных для отечественных разработчиков микросхем стандартных требований, кроме описания требуемых от микросхемы функций, временных диаграмм протокольного обмена, требуемого 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.) зарубежный разработчик получает от заказчика (обычно это или Министерство обороны США, или NASA) уже более 10 лет *стандартный дополнительный «пункт»*. Этот достаточно объемный «пункт» (раздел ТЗ) обычно 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 зарубежных микросхем. Отечественные разработчики (как российские, так и белорусские) используют эти официальные статистические данные для обоснования увеличения стоимости своих НИОКР при защите финансовых планов (затрат) на разработку микросхемы перед финансовыми ведомствами своих стран (в основном тогда, когда речь идет о государственном бюджетном финансировании мероприятий Гособоронзаказа). Простодушные и доверчивые чиновники этих ведомств (Минпром, Минэкономразвития и т. п.) обычно весьма далеки от мирских «микроэлектронных» проблем и не могут знать истинной причины такой высокой стоимости «у буржуев».

Но зарубежные финансисты сегодня хорошо знают, что в многомиллионной стоимости разработки субмикронных микросхем от 25 % до 75 % составляют затраты на реализацию и обеспечение методов *«технологической безопасности»* микросхем. Термин «Технология контроля безопасности в микроэлектронике» впервые появился в научно-технической литературе уже после 2005 г., когда Министерством юстиции США был опубликован известный у нас, к сожалению, только узкому кругу специалистов и соответствующим «кураторам ФСБ» полный *судебный отчет по результатам расследования путей попадания в военные и коммерческие системы США и их союзников контрафактных микросхем*. Исходной точкой в этом многотомном судебном расследовании являлась полученная от глубоко внедренной на китайских полупроводниковых заводах агентуры ЦРУ информация о методах, средствах и каналах поставок в США и страны НАТО фальшивых «суперналежных» микросхем. В вышедшей в этом году в издательстве «ТЕХНОСФЕРА» нашей книге [2], посвященной этой непростой теме (фактически это первая в мире техническая энциклопедия по проблемам программных и аппаратных троянов) с названием «*Программные и аппаратные трояны — способы внедрения и методы противодействия*» все эти вопросы рассмотрены более детально и аргументированно. Основная цель этой технической энциклопедии — не только обобщить и систематизировать уже имеющийся опыт борьбы с этой реальной угрозой (программными и аппаратными троянами), но и способствовать тому, чтобы и разработчики микросхем ответственного (военного и космического) назначения, и руководители компетентных министерств и ведомств наконец осознали эту суровую реальность и предприняли все необходимые (уже давно известные из «американского» опыта!) действия по ее нейтрализации при организации каналов поставки иностранных микросхем в Россию.

ИСТОРИЯ И ПРИЧИНЫ ПОЯВЛЕНИЯ ПРОГРАММНЫХ И АППАРАТНЫХ ТРОЯНОВ

Прежде чем говорить о многочисленных и уже известных из «американского опыта» методах защиты и противодействия программным и аппаратным троянам, необходимо буквально несколько слов сказать об истории и о причинах их появления.

Первыми в своей практической «деятельности» программные и аппаратные трояны начали использовать различные криминальные группировки (японские якудза, итальянские мафиози, американские гангстеры, русские «братки») для решения своих чисто криминальных проблем без применения «ножа и пистолета» — незаметного уничтожения улик в базах данных правоохранительных органов, похищения секретных и конфиденциальных сведений объектов их внимания, несанкционированного снятия наличных с банковских карт, махинаций в игорном бизнесе, отмывания «наркодоходов» и т. п.).

Правоохранительные и судебные органы по своим каналам оперативно поставили в известность об этих фактах компетентные спецслужбы США, Англии, европейских стран (ЦРУ, АНБ, ФБР, БНД, МИ5 и др.), которые оперативно оценили уровень этих новых угроз и поистине неограниченные возможности,

предоставляемые им этим «криминальным феноменом». В этих спецслужбах были созданы многочисленные специальные подразделения, укомплектованные высокопрофессиональными военными и гражданскими специалистами и экспертами в области так называемых хайтек-технологий, которым были поставлены конкретные цели и задачи по организации тех процессов, которые потом в СМИ назвали «кибероперациями». В нашей книге [2] представлена подробная информация о составе и примерной численности «кибербойцов» в США, Северной Корее, Китае, России и других странах.

ПРОГРАММНЫЕ И АППАРАТНЫЕ ТРОЯНЫ — ТЕХНОЛОГИЧЕСКАЯ ПЛАТФОРМА ИНФОРМАЦИОННО-ТЕХНИЧЕСКОГО ОРУЖИЯ (КИБЕРОРУЖИЯ)

Как было показано нами в «предваряющих» главах вышеуказанной технической энциклопедии, 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., показал, что их реальное применение на Земле будет не чем иным, как достаточно изощренным «способом самоубийства». Именно поэтому в недрах военных и разведывательных ведомств так называемых индустриально развитых стран появилась идея разработки совершенно нового вида оружия, применение которого, по замыслу его идеологов, позволит реально «победить и выжить» нападающей стороне. Это и есть так называемое *научно-техническое оружие*, или «кибероружие», как называют его западные журналисты.

«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 полностью «перехватывать» управление этими объектами, вплоть до приведения их в полностью неработоспособное состояние.

Специалистами Министерства обороны США, а также входящими в его структуру разведывательными сообществами (Федеральное бюро расследований, Агентство национальной безопасности — аналоги российского ФСБ (кстати, многие читатели до сих пор наивно полагают, что все эти ведомства подчиняются чуть ли непосредственно Сенату или президенту США, но это совсем не так)) в повседневной практике очень часто используется этот термин — «технологии контроля безопасности в микроэлектронике».

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

МЕСТО И РОЛЬ ТЕХНОЛОГИЙ КОНТРОЛЯ БЕЗОПАСНОСТИ В СОВРЕМЕННОЙ МИКРОЭЛЕКТРОНИКЕ

Как было показано в [2], в основе функционирования *американской системы контроля безопасности микроэлектронных изделий* лежит так называемый принцип золотой пятерки безопасности. Эта «золотая пятерка безопасности» в США была сформирована 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» — это 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 этой страны, в основном на полупроводниковых фабриках ЮВА. Эти пять базовых направлений обеспечения защиты безопасности каналов

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

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 конкретно 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* в целях 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 аналогичны 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 (известная экспертам) информация об основных функциональных подразделениях этого центра, составленная авторами этой 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 превзошли ЦК КПСС времен Л. И. Брежнева с лозунгами той эпохи типа «Экономика должна быть экономной!». На входе в один из головных офисов этого федерального центра висит «слоган»: «*Безопасность не бывает бесплатной*». В этом коротком слогане скрыт большой смысл.

Если его «развернуть», то ситуация выглядит следующим образом. В многомиллионной «долларовой стоимости» разработки современных микросхем от 25 % до 75 %, по экспертным оценкам западных специалистов, составляют затраты на обеспечение надежности и этой самой технологической безопасности микросхем (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*

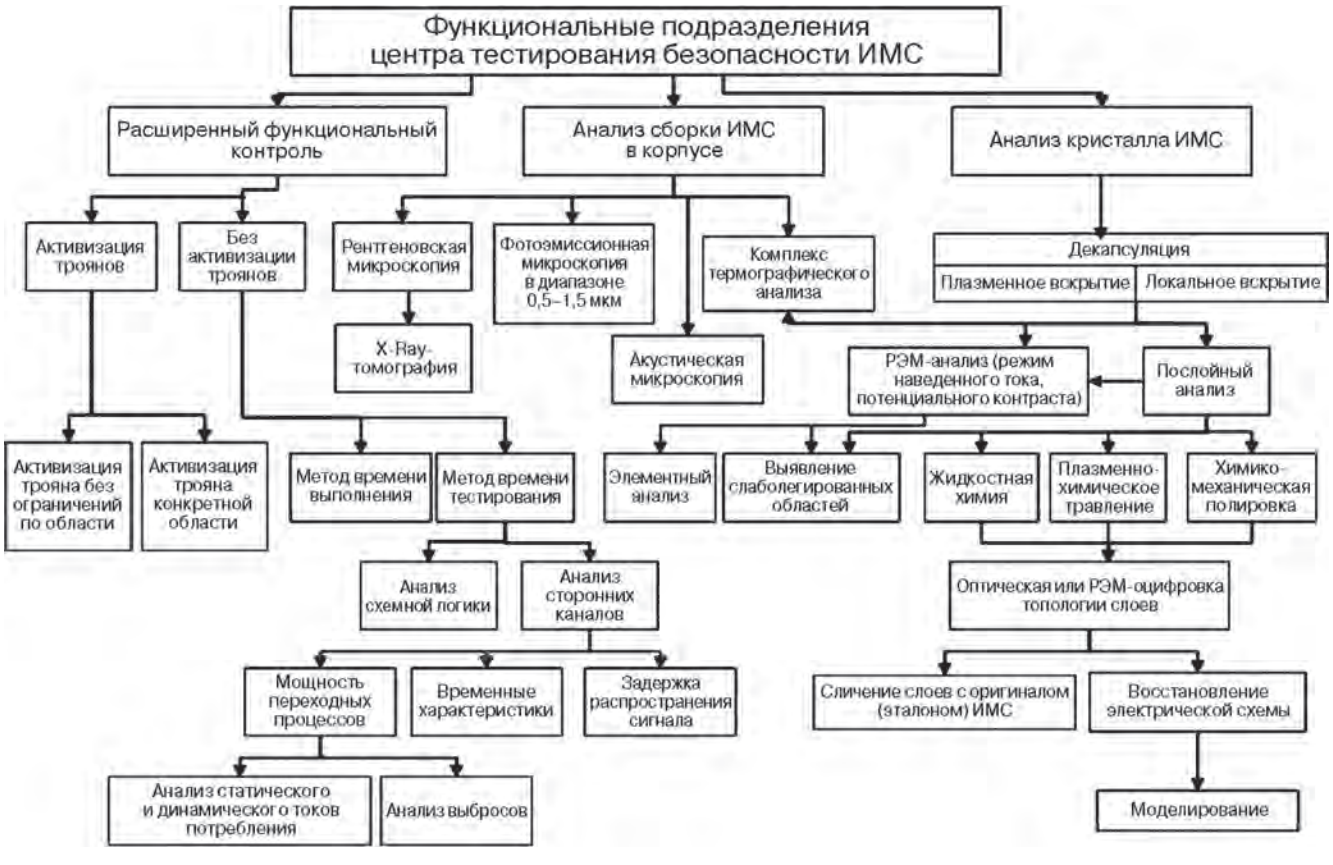

Рис. 2. Минимальный состав функциональных подразделений (лабораторий) центра тестирования безопасности микросхем

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 функциональной сложности исследуемой микросхемы, от ее целевого назначения. Как авторы показали в вышецитируемой технической энциклопедии, с увеличением степени интеграции, уменьшением уровня используемых проектных норм резко возрастают технические проблемы, связанные с применением разработанных аналитических методов типа анализа скрытых каналов, метода TESR, анализа тепловых излучений, анализа цепей питания, метода кольцевых генераторов и др. и с тем, что 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.), для обеспечения заданного заказчиком высокого уровня технологической безопасности необходимо будет 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, изготовленных 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 (утечки секретной информации, клонирования, 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, 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) применений регламентируется рядом нормативных актов. Так, российским предприятиям ОПК без ограничений разрешается применять только изделия,

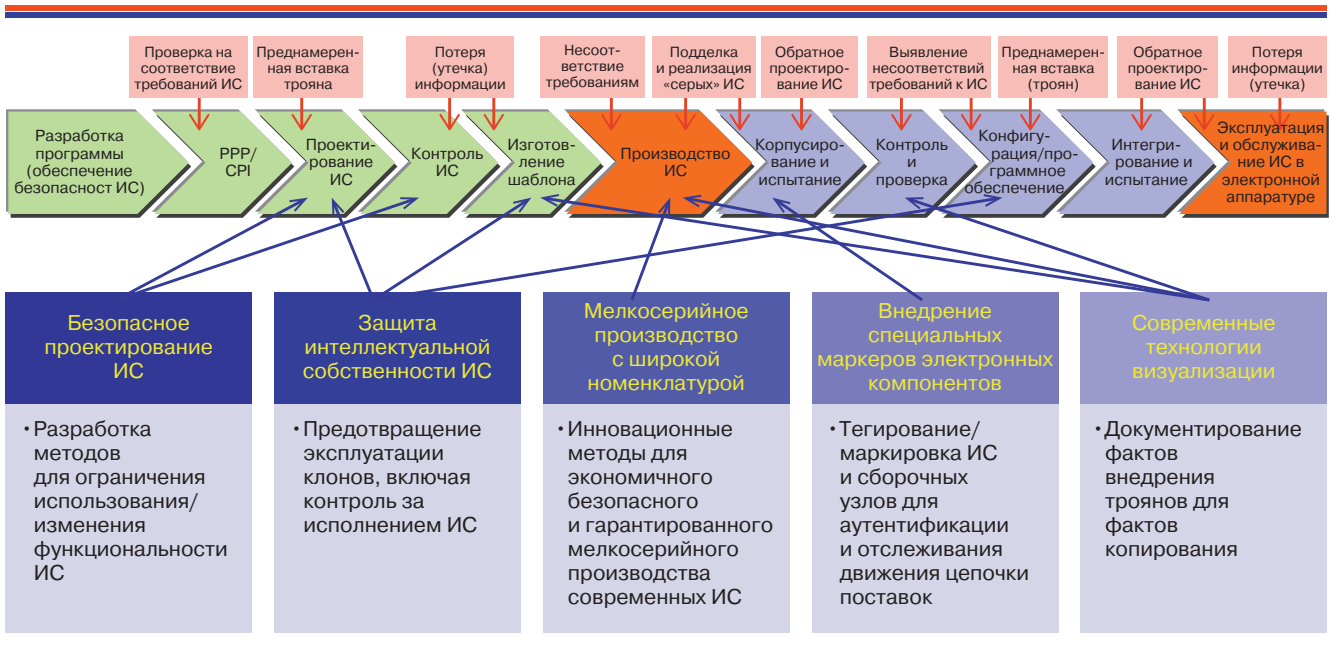

Рис. 3. Графическое представление последовательности основных этапов цикла изготовления и контроля микросхем на несертифицированной заказчиком (ненадежной) фабрике

включенные в ***«Перечень электронной компонентной базы, разрешенной 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, вместе с тем в последнее время в данный перечень стали включаться 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 дела, 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, изготавливаемых 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 фактически все известные нам сегодня современные технологии. Понятно, что с появлением любых новых микроэлектронных технологий они немедленно будут включены «дядей Сэмом» в этот 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 территории США. Надо ясно понимать еще один важный момент: для всех этих современных фабрик, расположенных вне территории США, в принципе, тоже не имеет особого значения, кто конкретно их «сертифицирует» (ведь за эту сертификацию они получают еще и 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 всего 30–50 % от проектной мощности. Более того, между этими фабриками постоянно идет ожесточенная конкурентная борьба за заказчиков: здесь будут рады каждому новому претенденту и никакие очередные «санкции» здесь не сработают.

Поэтому для достижения заданных заказчиком (Минпромторг или Минобороны РФ) тактико-технических характеристик радиоэлектронной аппаратуры из-за отсутствия отечественных аналогов разработчики аппаратуры зачастую 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, отсутствует жесткий контроль сборки и качества партии.

Гарантировать возможности безопасного применения 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, факт использования импортной ЭКБ для критических применений будет иметь место еще в течение длительного времени.

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 долл. США объем приобретенной импортной ЭКБ составил 2035 млн долл. США, а отечественной — 795 млн долл. США.

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

В заключение надо отметить, что американцам с большим трудом удалось создать и внедрить в практику вышеописанную систему 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 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 г. в г. Спрингфилде, штат Вирджиния. Хотя основная часть доклада была посвящена описанию методологии работы

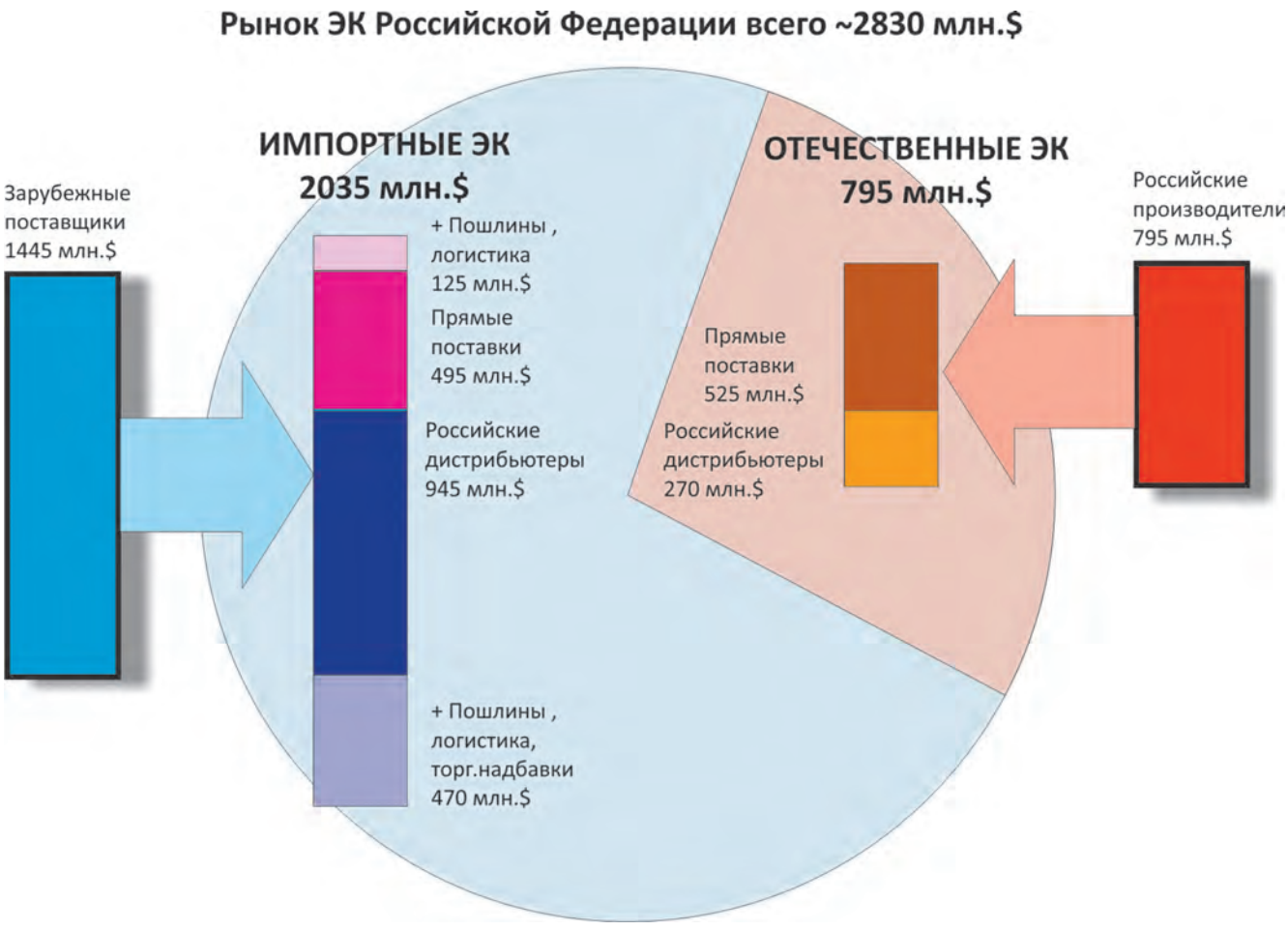

Рис. 4. Обобщенная структура каналов поставки ЭКБ в РФ [3] (здесь поставки через компании-комплектаторы приравнены к прямым поставкам)

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 философу, жившему целых пять веков тому назад (рис. 5), чтобы подчеркнуть всю сложность вечной проблемы «замены старых порядков новыми» в супердемократическом американском обществе, в котором армия является его неотъемлемой частью.

Суть доклада американского генерала сводилась к тому тезису, 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.

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 выше изложенного можно сформулировать краткие выводы и рекомендации.

1. 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

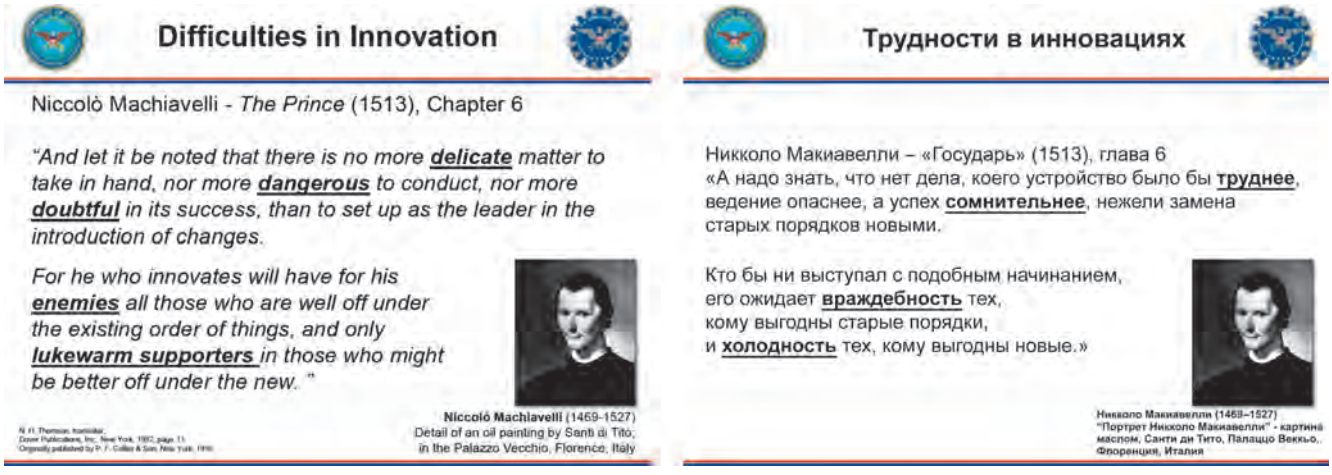

Рис. 5. Слайд доклада Д. Скотта Лусеро, посвященный проблеме внедрения в жизнь новых решений

в ближайшей и отдаленной перспективе будет сохраняться, именно здесь необходимо сконцентрировать усилия по созданию соответствующей инфраструктуры безопасности каналов поставок — от разработки комплекса нормативно-технической документации по «американским калькам» до создания соответствующих отечественных центров компетенции.

2. 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 трояном близка к нулю.

ЛИТЕРАТУРА

1. Макушин М. Волна сделок слияния/поглощения в микроэлектронике: причины и последствия // Электроника НТБ, 2018. — № 1. — С. 142.
2. Белоус А. И., Солодуха В. А., Шведов С. В. Программные и аппаратные трояны — способы внедрения и методы противодействия. Первая техническая энциклопедия / Под общ. ред. Белоуса А. И. В двух книгах. — М.: ТЕХНОСФЕРА, 2018. — 698+630 с.
3. Отчет исследования российского рынка электронных компонентов / Информационно-аналитический центр современной электроники // ООО «СОВЭЛ», 2018. — 138 с.