ОСНОВНЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ, ПРОБЛЕМЫ И УГРОЗЫ СОВРЕМЕННОЙ МИКРОЭЛЕКТРОНИКИ

Анатолий Белоус,
член-корреспондент НАН Беларуси,
д. т. н.
ABelous@integral.by
Виталий Солодуха,
к. т. н.
VSaladukha@integral.by

В данном аналитическом обзоре с использованием методов форсайта рассмотрены основные тенденции, направления и новые драйверы развития, проблемы и угрозы как мировой, так и отечественной микроэлектроники, проблемы глобализации, экономические особенности субмикронного производства, основные решаемые исследователями технологические проблемы, троянские и троллинговые угрозы, анализ новой стратегии кибербезопасности США и вытекающие из нее новые киберугрозы.

ВВЕДЕНИЕ

Для подготовки концепций и стратегий развития на средне- и долгосрочный периоды руководителям и техническим специалистам любого современного предприятия, а также сотрудникам маркетинговых и сбытовых подразделений необходимо хорошо понимать не только механизмы и тенденции, но и проблемы, риски и потенциальные угрозы мирового рынка. Это в полной мере относится и к полупроводниковой индустрии, причем не только к разработчикам и производителям данных изделий, но даже в большей степени к потребителям продукции полупроводниковой отрасли — проектировщикам различной радиоэлектронной аппаратуры, включая системы вооружений и военной техники.

Основная цель настоящей аналитической статьи — провести системный анализ вышеперечисленных тенденций, проблем и угроз на основе изучения информации, опубликованной в научно-технической литературе, размещенной на интернет-ресурсах, собранной в процессе работы над созданием монографий для зарубежных издательств, а также полученной авторами во время участия в международных конференциях, форумах и симпозиумах, личных переговорах с техническими специалистами и руководителями иностранных полупроводниковых компаний.

Еще одной целью является рассмотрение важных особенностей, очевидных проблем и угроз применения ЭКБ иностранного производства в отечественных системах ответственного назначения. Авторы решили оформить результаты этого системного анализа в виде настоящей статьи, полагая, что она будет полезна как руководителям, так и техническим специалистам других предприятий полупроводниковой отрасли и потребителям ЭКБ.

Учитывая достаточно широкий спектр рассматриваемых вопросов, материалы этого системного анализа было решено оформить в виде цикла из двух взаимосвязанных статей с общим названием. В первой части, опубликованной ранее в журнале «Компоненты и технологии» (№10’2019, стр. 6-14 [1-27]), на основе использования методов форсайта были рассмотрены основные тенденции и направления развития современной микроэлектроники, проблемы глобализации полупроводникового бизнеса, проблемы экспоненциального роста номенклатуры используемых в технологии материалов, новые драйверы развития, экономические особенности организации эффективного субмикронного производства, основные решаемые исследователями технологические проблемы, усиление деструктивного действия эффекта YieldKiller в субмикронной области, состояние и перспективы развития технологии FinFET на примере КНР, тенденции развития космической микроэлектроники, интегральной и радиофотоники, основ квантовой микроэлектроники.

Материалы второй части аналитического обзора в большей степени ориентированы на читателей не научно-технического, а делового издания (журнала). Здесь мы рассматриваем такие «не технические» вопросы, как реакция полупроводникового бизнеса на последствия торговой войны США и КНР, в том числе санкций США против Huawei, причины и следствия изменений парадигмы проектирования современных микросхем, неочевидные пока многим специалистам взаимосвязи микроэлектроники и кибербезопасности, принципиальные отличия отечественных и зарубежных концепций разработки и применений ЭКБ при создании РЭА, возможные пути решения проблемы зависимости предприятий ОПК от иностранной ЭКБ, угроза троллинговых атак на российские предприятия и многое другое. Впервые в отечественной печати будут рассмотрены и основные положения новой стратегии кибербезопасности США, в которой Штаты официально, устами президента Трампа, объявляют кибервойну всему остальному мировому сообществу, взяв на вооружение уже известный нам термин «сохранение мира путем принуждения». Сравним эту стратегию с российской Доктриной обеспечения информационной безопасности.

РЕАКЦИЯ ПОЛУПРОВОДНИКОВОГО БИЗНЕСА В СТРАНАХ ЮВА НА ПОСЛЕДСТВИЯ ТОРГОВОЙ ВОЙНЫ США И КНР

В послевоенное время практически все развивающиеся государства стремились защитить своих производителей и завоевать новые рынки, используя тактику торговых войн (автомобильные, нефтяные, рыбные, сигаретные, стальные и т. д.). В итоге в большинстве случаев эти войны портили отношения между государствами и наносили значительный ущерб экономикам конфликтующих стран.

Сегодня типовым примером таких войн служит торговое противостояние США и Китая. Чтобы понять истинную причину этого

явления, достаточно посмотреть статистику внешней торговли и прямых инвестиций. Ежегодный объем прямых иностранных инвестиций американской экономики в китайскую можно оценить на уровне $50 млрд. Удивительно, но те же прямые инвестиции Китая в США в десятки раз меньше — всего около $0,8 млрд в год. А вот в торговле ситуация зеркально противоположная. Если ежегодный объем экспорта американских товаров в Китай можно оценить в $92 млрд, то у КНР в отношении США этот показатель составляет $365 млрд — очевидно, пока китайские власти рассматривали Штаты исключительно как рынок сбыта. Однако торговая война между обеими странами привела к появлению новых неожиданных тенденций в сложившейся структуре мирового полупроводникового бизнеса. В качестве примера приведем ряд фактов, связанных только с Южной Кореей и Японией.

В поисках выхода из ситуации санкционных ограничений США на поставки в КНР высокотехнологичных микроэлектронных изделий, китайские руководители радиоэлектронной промышленности приняли ряд оперативных стратегических решений, в том числе начали искать замену американским партнерам в регионе Юго-Восточной Азии, прежде всего в Японии и Южной Корее, обладающих мощной полупроводниковой индустрией, в том числе осуществляющих поставки ЭКБ в США и ЕС. Эта тенденция в свою очередь породила конкуренцию между японскими и корейскими полупроводниковыми компаниями в борьбе за потенциальные заказы КНР.

Среди таких потенциальных заказов и проектов присутствует и импортозамещение — имеется в виду знакомая нам ситуация с воспроизведением американских аналогов, поставки которых в КНР были прекращены в соответствии с санкционными предписаниями американским изготовителям ЭКБ.

Южная Корея сохраняет за собой статус четвертой экономики Азии, ВВП на душу населения которой впервые в 2018 году преодолел отметку в $30 тыс. Экономическую ситуацию в стране во многом определяет конъюнктура рынков полупроводников и автомобилей в ключевых странах — импортерах указанной корейской продукции.

С конца 2018 года наблюдается замедление темпов экономического роста Республики Корея, связанное со снижением спроса на основные статьи корейского экспорта на мировом рынке вследствие торгового противостояния между КНР и США.

Сегодня набирает обороты новая локальная торговая война, которая происходит между Республикой Корея и Японией. Началась она с июля 2019-го, когда японские власти ввели ограничения на поставку в Южную Корею ряда химических веществ и комплектующих (фторированный полиимид, фтористый водород, резисты), широко применяющихся при выпуске дисплеев для смартфонов и телевизоров, а также для изготовления полупроводниковых приборов.

Более активно в производственные цепочки корейских компаний стали проникать и китайские поставщики ЭКБ, использующие их зависимость от поставок отдельной конечной продукции на китайский рынок, режим свободной торговли (с 2015 года) и периодически возникающие сложности в отношениях с японскими партнерами.

В целях стимулирования диверсификации и модернизации полупроводниковых производств южнокорейским правительством разработана долгосрочная стратегия поддержки затрагиваемого корейского бизнеса и исследовательских учреждений, для финансирования которой при участии Министерства торговли, промышленности и энергетики и Министерства науки и ИКТ Республики Корея предполагается выделить около $1 млрд. Для аккумулирования заявленных средств предусматривается образование целевого государственного фонда, из которого будут финансироваться разработка и освоение оригинальных и прикладных технологий производства новых типов и поколений полупроводников.

Аналогичные мероприятия реализованы и в Японии, как реакция правительства на торговую войну США и КНР.

И еще один важный момент китайской стратегии на фоне торговой войны с США. В этом году завершилась трехлетняя компания по созданию в странах ЕС целой сети дизайн-центров, которые формально возглавляют граждане ЕС. Эти фирмы участвуют в различных тендерах на разработку ЭКБ, как правило, выигрывая их за счет более низких цен на выполняемые услуги. Здесь действует специальная преференция — в случае заключения контракта с иностранной фирмой дизайн-центр получает 50% от стоимости контракта (правительство КНР фактически оплачивает половину стоимости контракта).

Отметим и еще одну тенденцию — предложенные правительством КНР трехкратные оклады и бонусы. Стимулируется новое явление — тайваньские микроэлектронщики уезжают в Китай целыми коллективами. Материковые компании предлагают таким специалистам в два и даже в три раза большую заработную плату, чем получают инженеры в тайваньских компаниях. Кроме этого, предусмотрены многочисленные бонусы, например, оплата образования детей тайваньских инженеров в частных учебных заведениях. Тайваньские компании пытаются оградить себя от подобной напасти повышением зарплат на острове, но конкурировать в этом направлении с китайцами они уже не могут.

Китайские компании не просто переманивают высших руководителей и инженеров с Тайваня, что происходит достаточно давно (за последние годы Тайвань покинуло свыше 3000 инженеров из имеющихся там 40 000 специалистов), но и приглашают уже целые рабочие коллективы.

Торговая война и санкции против Huawei ударили и по американским разработчикам чипов

Аналитики компании Trend Force опубликовали отчет о выручке 10 крупнейших в мире разработчиков микросхем в третьем квартале 2019 года. Для американских компаний результат оказался «разнонаправленным»: положительная динамика наблюдалась только у компаний, не затронутых торговой войной между США и Китаем и не имеющих отношения к Huawei и смартфонам. Приведем только два примера.

Лидер рынка проектировщиков микросхем, компания Broadcom, которая вынуждена была сменить «сингапурскую» прописку на «американскую» после ввода новых налогов Д. Трампом, из-за торговой войны теряет выручку третий квартал подряд. Китайская Huawei является самым крупным клиентом Broadcom, что привело к сокращению дохода компании после того, как Huawei была внесена в черный список компаний, с которыми американцам запрещено работать. В третьем квартале выручка Broadcom показала годовое падение на уровне 12,3%, что стало самым большим снижением за последние три квартала.

Второй по величине дизайнер чипов, компания Qualcomm, также стала жертвой торговой войны и пострадала сильнее всех среди самых крупных в мире разработчиков. Падение выручки Qualcomm в третьем квартале достигло 22,3% в годовом отношении. Реальный спрос на 5G пока не столь велик, чтобы Qualcomm начала зарабатывать на этом направлении достаточно много денег.

Вследствие снижения дохода лидеров отрасли в лице американских проектировщиков чипов, по нашему прогнозу, в 2019 году вся отрасль покажет снижение выручки. Да и в следующем, 2020-м

рост будет только в том случае, если разработчики микросхем смогут обойти санкции против Китая.

ИЗМЕНЕНИЕ ПАРАДИГМЫ ПРОЕКТИРОВАНИЯ МИКРОСХЕМ

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

В отличие от обычных для отечественных специалистов 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 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» [26].

Как показано выше, с уменьшением проектных норм существенно возрастает стоимость разработки иностранных микросхем. Зарубежные финансисты хорошо знают, что в многомиллионной стоимости разработки субмикронных микросхем 25–75% составляют затраты на реализацию и обеспечение методов технологической безопасности микросхем. Для удовлетворения этого дополнительного «пункта» зарубежный разработчик должен представить заказчику и затем реализовать на всех этапах жизненного цикла изделия (проектирование, анализ, измерение, корпусирование, организация выпускного контроля, производство) применение соответствующих методов, средств и технологий обеспечения безопасности. Такой большой разброс процента затрат на обеспечение безопасности обусловлен как широким спектром угроз (видов аппаратных троянов), так и фактором используемых проектных норм: чем меньше значение проектной нормы, тем дороже обеспечить безопасность и определить факт несанкционированного включения трояна в микросхему [29–44].

Современная микроэлектроника и кибербезопасность

Следует отметить и ряд очевидных угроз, появившихся сравнительно недавно в процессе развития как мировой, так и отечественной микроэлектроники и логически вытекающих из этой новой для нас парадигмы проектирования микросхем. Образно говоря, «угроза» — это нерешенная «проблема».

На первое место здесь необходимо поставить троянскую угрозу. Она стала следствием еще одной очевидной тенденции развития микроэлектроники — продолжающимся процессом переноса полупроводниковых производств из США в страны Юго-Восточной Азии — Китай, Тайвань, Южную Корею [4].

Зарубежными исследователями [31, 33] еще в 2005 году было теоретически и экспериментально показано, что в любую микросхему, без ведома ее разработчика, можно внедрить так называемый аппаратный троян практически на любом этапе создания — от стадии проектирования до момента изготовления и сборки. Этот троян может выполнить по команде своего «хозяина» самые различные несанкционированные и скрытые от наблюдателя функции — передавать «хозяину» любую информацию, изменять режимы функционирования, электрические режимы работы микросхемы (вплоть до ее частичного или полного отказа). Попадая в платы электронных блоков современных информационно-коммутационных устройств, систем энергообеспечения мегаполисов, систем управления высокоточным оружием, систем обеспечения безопасности атомных станций и т. п. эти «заряженные» микросхемы способны не только организовать передачу «хозяину» секретной информации, но и полностью перехватывать управление подобными объектами, вплоть до приведения их в неработоспособное состояние. Поэтому на Западе появилось новое направление в микроэлектронике — обеспечение безопасности микросхем. В развитие этого нового направления министерства обороны США, Англии, Франции и других стран НАТО разработали и с 2010 года полностью ввели в действие комплекс нормативно-технических мероприятий по защите и противодействию данной угрозе (рис. 1) [26, 31–42]. Важная составная часть указанного комплекса — объединенный федеральный центр обеспечения безопасности микросхем (JFAC), который создан как структурное подразделение Министерства обороны США. Аналогичные центры функционируют и в других развитых странах.

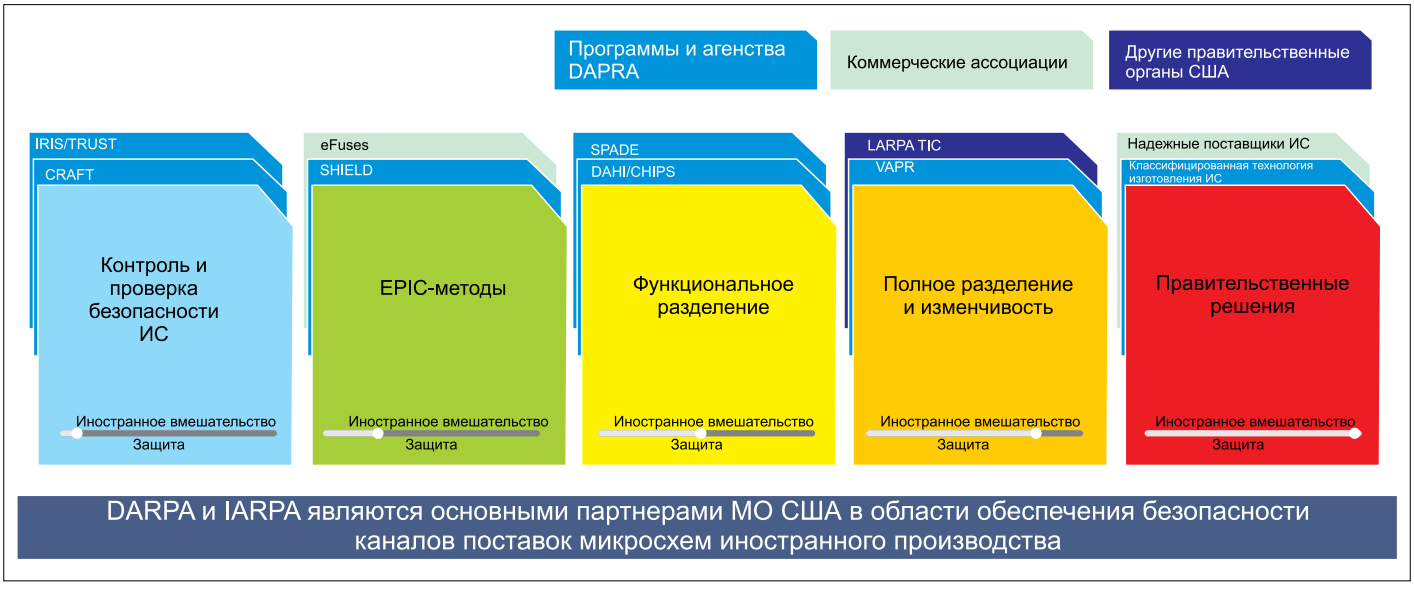

Рис. 1. Американская «золотая пятерка безопасности» — основные направления разработки комплексов нормативно-технических мероприятий, директив и программ обеспечения безопасности каналов поставки микросхем

Абсолютное большинство микросхем ответственного назначения, изготовленных как США, так и в странах ЮВА, проходят полную проверку (сертификацию) в лабораториях этого центра перед поставкой для комплектации систем ответственного назначения. И конечно, это далеко не та «сертификация», которая сегодня проводится аналогичными по названию структурами, например Роскосмосом или МНИИРИП. Кроме микросхем военного и космического назначения, через такие центры проходят микросхемы для коммерческих и промышленных применений (для банковской сферы, навигации, мобильной связи, наземного и воздушного транспорта, топливно-энергетического комплекса и т. п.).

К сожалению, в РФ на текущий момент отсутствуют как нормативно-технические мероприятия, программы типа американской «Безопасность микросхем», так и подобные центры безопасности. Сегодня это становится основным видом угроз и для отечественного радиоэлектронного комплекса, где по-прежнему доля импортных микросхем превышает 70%, и такое положение по объективным причинам будет сохраняться и в последующие годы. Надо отметить, что и наши китайские партнеры оказались в аналогичной ситуации, и у них, несмотря на мощную собственную полупроводниковую промышленность, более 30% микросхем для РЭА закупалось за рубежом, а введенные США в ходе торговой войны дополнительные санкции еще больше обострили ситуацию. Кстати, китайские товарищи весьма серьезно отнеслись к троянской угрозе (аппаратные трояны в микросхемах) и создали свою эффективную систему противодействия, используя «американский опыт». В отличие от США, в Китае пока не сняты цензурные ограничения на публикацию по данной тематике, хотя ряд институтов Министерства обороны КНР сегодня занимается исключительно проблемами контроля безопасности импортных микросхем.

Прежде чем перейти к рассмотрению следующих проблемных вопросов, необходимо уделить внимание американской стратегии кибербезопасности, поскольку именно микроэлектроника неожиданно становится одним из главных инструментов в арсенале современного и перспективного кибероружия.

Сохранение мира путем принуждения — основной принцип стратегии кибербезопасности США

К сожалению, ни в отечественных СМИ, ни в открытой отечественной литературе пока этот вопрос не нашел адекватного отражения, хотя последствия этого «иностранного» документа, как станет ясно читателю, касается буквально каждого из нас.

Надо отметить, что в последнее десятилетие США уделяет вопросам кибероружия и кибербезопасности исключительное внимание, рассматривая эти направления в качестве наивысшего приоритета государственной политики как на текущий момент, так и на ближайшую перспективу. С приходом к власти в США президента Трампа его администрация существенно пересмотрела основные положения и содержание ранее утвержденной стратегии.

В сентябре 2018 года на сайте Белого дома был опубликован текст Обращения президента Трампа к соотечественникам, объясняющий причины появления, цели и задачи этого документа. Данный факт лишний раз подчеркивает его важность — никогда ранее президенты США не комментировали такие документы, более того, в открытой печати никогда ранее не публиковали полный текст подобных документов, непосредственно относящихся к вопросам обеспечения национальной безопасности. Комментируя этот прецедент, абсолютное большинство независимых экспертов полагает, что таким образом Америка как «сверхдержава» официально объявляет кибервойну всему остальному мировому сообществу, открыто взяв на вооружение известный нам ранее «русский» термин «сохранение мира путем принуждения».

Этот факт подтверждает и нижеследующая цитата из обращения Трампа: «Нынешняя администрация признает, что исключительно технократического подхода в отношении киберпространства недостаточно для решения появляющихся проблем. Соединенные Штаты также должны обладать широким инструментарием эффективных мер принуждения, которые обеспечат сдерживание структур, осуществляющих хакерские атаки, и позволят предотвратить дальнейшую эскалацию».

Если перевести этот абзац текста с дипломатического «официального» языка на простой «человеческий» язык, то это действительно означает, что в сентябре 2018 года США устами своего президента объявили о начале «войны в киберпространстве». Против кого они объявили эту тотальную кибервойну? Здесь же указаны и конкретные, уже не «потенциальные» противники: Россия с «примкнувшими» к ней Ираном и Северной Кореей. Хотя Китай прямо не упоминается в этой группе стран-врагов, но из формулировок документа ясно следует, что все меры по «сохранению мира методом принуждения» в полной мере распространяются и на эту страну.

Читателю следует обратить особое внимание — это совсем не фейковые сообщения СМИ или заявления отдельных «ястребов-сенаторов», это утвержденный главой государства официальный документ, определяющий политику, стратегию и тактику государства на текущий и перспективный период! Надо ясно понимать, что эта кибервойна объявлена не просто виртуальной России — она объявлена каждому из вас, читатели. Поэтому вы должны понимать, какое оружие может быть использовано против вас и как можно если не защититься, то по крайней мере хотя бы уменьшить уровень опасности путем использования простейших средств защиты.

Из анализа полного текста многостраничной Стратегии (http://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy_USA_2018.pdf) следует, что в ее основу положено всего лишь четыре приоритета (базовых принципа): защита американского народа и американского образа жизни, обеспечение процветания Америки, распространение американского влияния на весь мир, сохранение мира методом принуждения. Основным средством достижения (инструментом) этих благородных приоритетных задач развития США объявлено именно кибероружие (четвертый названный приоритет), а не ожидаемые читателем иные разнообразные инструменты и достижения научно-технического прогресса человечества. Американские политики, генералы и чиновники фактически на законодательном уровне присвоили себе право «без суда и следствия» принимать и реализовывать решения — кого, когда, за что и каким образом наказывать (принуждать) силой кибероружия. А как уже очевидно многим экспертам, технологической платформой (базой) современного кибероружия становятся программные и аппаратные трояны, которые в кибероперациях действуют солидарно с вирусами, шпионскими программами и прочими «цифровыми тварями», помогая и защищая друг друга.

Как обстоят дела в России с подобными стратегиями?

Как мы уже отмечали, в России сами понятия «кибероружие» и «кибербезопасность» пока считаются «иностранными», а наиболее широко на официальном уровне используются термины «доверенные системы», «информационная безопасность», «научно-техническое оружие».

Поэтому в РФ нет документа с названием «Киберстратегия», но в декабре 2016 года была наконец утверждена Доктрина информационной безопасности Российской Федерации.

Здесь мы должны дать краткие определения основных используемых терминов «стратегия», «концепция» и «доктрина» (http://vmest.ru/nuda/o-doktrinah-koncepciyah-i-strategiyah/main.html).

Концепция — модель целевых устремлений, где должны присутствовать не только декларации, но и обоснования необходимости и достаточности контента.

Стратегия определяет систему взаимосвязанных по задачам, срокам и ресурсам целевых программ, отдельных проектов и мероприятий.

Доктрина — целостная совокупность принципов, используемых в качестве основы для реализации программы действий.

Обычно концепция и стратегия тесно взаимосвязаны. Эта связь проявляется прежде всего в том, что первая без второй превращается в мало что значащую «декларацию о намерениях», а вторая без первой — в ни на чем не основанную «авантюру». И только дополняя друг друга, они способны стать эффективным руководством к конкретным действиям.

При таком подходе любая стратегия понимается как совокупность планов, программ, методов и механизмов достижения сформулированных и обоснованных глобальных и локальных целей.

Говоря простым языком, современная доктрина национальной кибербезопасности должна состоять из научно обоснованной концепции кибербезопасности и проистекающей из нее стратегии обеспечения кибербезопасности.

Если принимать во внимание эти юридические тонкости, можно говорить о том, что российская «доктрина» по уровню проработки должна находиться «выше» американской «стратегии».

Отвлечемся от этой юридической казуистики и посмотрим только на основные отличия российской Доктрины от американской Киберстратегии.

Изучив многостраничный текст этого документа, находящегося в открытом доступе, читатель сделает для себя выводы:

1. Здесь нет заявлений о желании быть лидерами в киберпространстве или на планете.
2. Здесь не используются термины «принуждение к миру», «противники» и никого не объявляют противником.
3. Признается наличие в мире равноправных партнеров по переговорам и соглашениям с отличающимися интересами, но с равными правами на переговорах.
4. Россия не объявляет о своем праве на проведение активных операций в киберпространстве против «противников» и не собирается вмешиваться в Интернет на их территориях.
5. Россия объявляет о своем желании построить прочный мир и обеспечивать сотрудничество в глобальном киберпространстве с любыми партнерами.

Итак, российская стратегия — оборонная, в отличие от атакующей американской. Хорошо это или плохо — на заданный вопрос пусть ответит сам читатель.

ПРОБЛЕМА ИСПОРТОЗАМЕЩЕНИЯ ЭКБ И ПУТИ ЕЕ РЕШЕНИЯ

Здесь необходимо более детально рассмотреть некоторые особенности проблемы закупок импортных микросхем военного, космического, промышленного и коммерческого назначения. В основе этой проблемы лежит очевидный специалистам тезис: полупроводниковая промышленность любой одной страны (даже США) сегодня не может полностью обеспечить потребности своего радиоэлектронного промышленного комплекса.

Например, МО США только за один 2017 год, по данным независимых экспертов, использовало для проектирования и производства радиоэлектронных устройств по разным источникам от 120 до 150 тыс. типономиналов микросхем и дискретных полупроводниковых приборов, в том числе более 25% ЭКБИП из стран Юго-Восточной Азии: китайского, японского, тайванского производства [5]. И это притом, что только на территории США в 2017 году находилось 24 самых современных полупроводниковых производств, сертифицированных МО США. В 2015-м доля полупроводниковой промышленности США в общем объеме мирового валового производства составляла всего 25%, а на момент выхода настоящей статьи эта доля по разным источникам составляет 20–23%.

Из ежегодно разрабатываемых в мире 9–10 тыс. новых микросхем 7–10% создается в интересах МО США. Это означает, что каждый год МО США получает от 600 до 1000 новых типов ЭКБ, что позволяет разрабатывать самое передовое оружие и военную технику. Отметим, что абсолютное большинство этих изделий является специализированными, а не универсальными (как в РФ) — предназначенными для решения конкретных задач, требующих обеспечения максимальной производительности (в современном бою победит тот, кто первым «увидит» противника и первым «выстрелит»).

При формировании российской программы разработки ЭКБ на 2017–2022 гг. Минпромторг (в отличие от США и всего мира в РФ военную электронику заказывают не военные, а гражданское ведомство) из заявленных МО РФ более 50 тыс. типономиналов отобрали для включения только 8900 типов, из которых, как официально подтверждают эксперты МНИИРИП, могут быть воспроизведены лишь 7100 типов, а 1800 даже в ближайшее время не могут быть разработаны (https://elibrary.ru/item.asp?id=35119938).

Почему только 8900 типономиналов? Потому что якобы больше российские предприятия не могут разработать за пять лет. Но реальная статистика показывает, что ведущие предприятия РФ ПАО «Микрон» и ОАО «Ангстрем» могут брать в год от 50 максимум до 100 проектов (в зависимости от сложности изделия). Простая логика показывает, что для выполнения планов госзаказа потребуется намного более 10 лет, а не пять заявленных. Один ОАО «Интеграл» также может выполнить в год от 50 до 100 проектов. Следовательно, только если подключить ОАО «Интеграл» — управляющую компанию холдинга «Интеграл» — теоретически возможно выполнить российскую программу обеспечения ЭКБ военного назначения в утвержденные правительством РФ сроки. Но на текущий момент это невозможно из-за отсутствия политической воли (решения) руководства РФ.

А что делать предприятиям ОПК РФ — ведь есть указание Путина разрабатывать только современную и только на мировом уровне технику?!

Поэтому предприятия ОПК вынуждены закупать за валюту импортную ЭКБ. Посмотрите только официальную статистику таких закупок:

- 2014 год — $900 млн;
- 2015 год — $790 млн;
- 2016 год — $800 млн;
- 2017 год — $933 млн;
- 2018 год — $1010 млн.

Надо ясно понимать, что в любых из закупленных за рубежом микросхемах может находиться один из многочисленных типов закладок (троянов), выполняющих функции «временной бомбы».

За последние лихие десятилетия приобретение и перепродажа военным заказчикам импортных схем стало в России крупным и очень выгодным бизнесом. Его продвижением даже занимались чиновники российского государства на самом высоком уровне. Это идет еще от «младореформаторов», когда в 90-х годах Егор Гайдар, член правительства молодой независимой России, приехал в Зеленоград и говорил на встрече с жителями: «Кому нужны

эти ваши микросхемы? Мы все это можем быстро и дешево купить за границей» [26].

В России, как следует из официальных статистических данных [45], для продукции промышленного и оборонно-промышленного комплексов в 2017 году предприятиями было закуплено полупроводниковой ЭКБ всего на сумму $1,248 млрд, из которых $933 млн (75%) составляли закупки ЭКБ ИП, и только на $315 млн (25%) было приобретено отечественной ЭКБ (российского и белорусского происхождения) (рис. 2).

В 2018 году, невзирая на объявленные санкции (работает на практике американский слоган «бизнес есть бизнес»), возрос как общий объем закупок ($1,43 млрд), так и доля закупок ЭКБ ИП, которая уже перешагнула объем в $1 млрд ($1,02 млрд, или 71% от всех закупок) [45]. По нашему мнению, эта тенденция будет иметь нарастающий характер.

Обратная сторона этой проблемы заключается в принципиальных отличиях российской концепции создания и применения ЭКБ в РЭА от общепринятых мировых концепций.

ПРИНЦИПИАЛЬНЫЕ ОТЛИЧИЯ «ОТЕЧЕСТВЕННЫХ» И «ЗАРУБЕЖНЫХ» КОНЦЕПЦИЙ РАЗРАБОТКИ И ИСПОЛЬЗОВАНИЯ ЭКБ ПРИ ПРОЕКТИРОВАНИИ РЭА

Общеизвестно, что при разработке РЭА для военной и космической техники на Западе используют методы «системного проектирования», где основные требования к новой микросхеме (если имеющиеся на рынке не соответствуют тактико-техническим характеристикам проектируемой РАЭ) формируются уже на верхнем уровне иерархии проектируемой аппаратуры, детализируются по результатам системотехнического, алгоритмического и математического моделирования (не макетирования!) проектируемой системы (устройства) и затем направляются в соответствующие дизайн-центры в форме понятного разработчикам ТЗ [5]. В каждом из министерств и ведомств, при каждом роде войск министерств обороны США и стран НАТО функционируют десятки подобных институтов «системного проектирования» [26].

Со времен СССР в России в значительной степени была утеряна соответствующая компетенция разработчиков отечественной РЭА в части способности сформулировать такое системное и детальное ТЗ на ЭКБ. На общем фоне такие отечественные изделия, как настольные компьютеры «Эльбрус-801 М» на базе отечественного 8-ядерного процессора «Эльбрус-8 С» с 64-разрядной архитектурой четвертого поколения или «Бином-КА» на базе процессора МП16.2 (с усиленной киберзащитой) выглядят редчайшими исключениями из общего правила. Сегодня в абсолютном большинстве случаев разработчиками РЭА вместо «моделирования» используется «макетирование» — разработчики отечественных радиоэлектронных систем уже на этапе создания таких «макетных» образцов обычно используют импортные микросхемы, исходя из следующих основных соображений:

- сокращение сроков разработки и освоения РЭА (на 3–5 лет за счет исключения необходимости выполнения ОКР на разработку и освоение ЭКБ);
- наличие большого выбора функционалов ЭКБ (более сотни тысяч типов иностранных вместо отечественных сотен типов);
- высокое качество и существенно более высокий по сравнению с отечественными «техническими условиями» уровень детализации техдокументации на ЭКБ ИП: подробнейшие спецификации, «разжеванные» схемы включения и, особенно, многостаночное и детализированное для каждого конкретного случая руководство по применению (handbook).

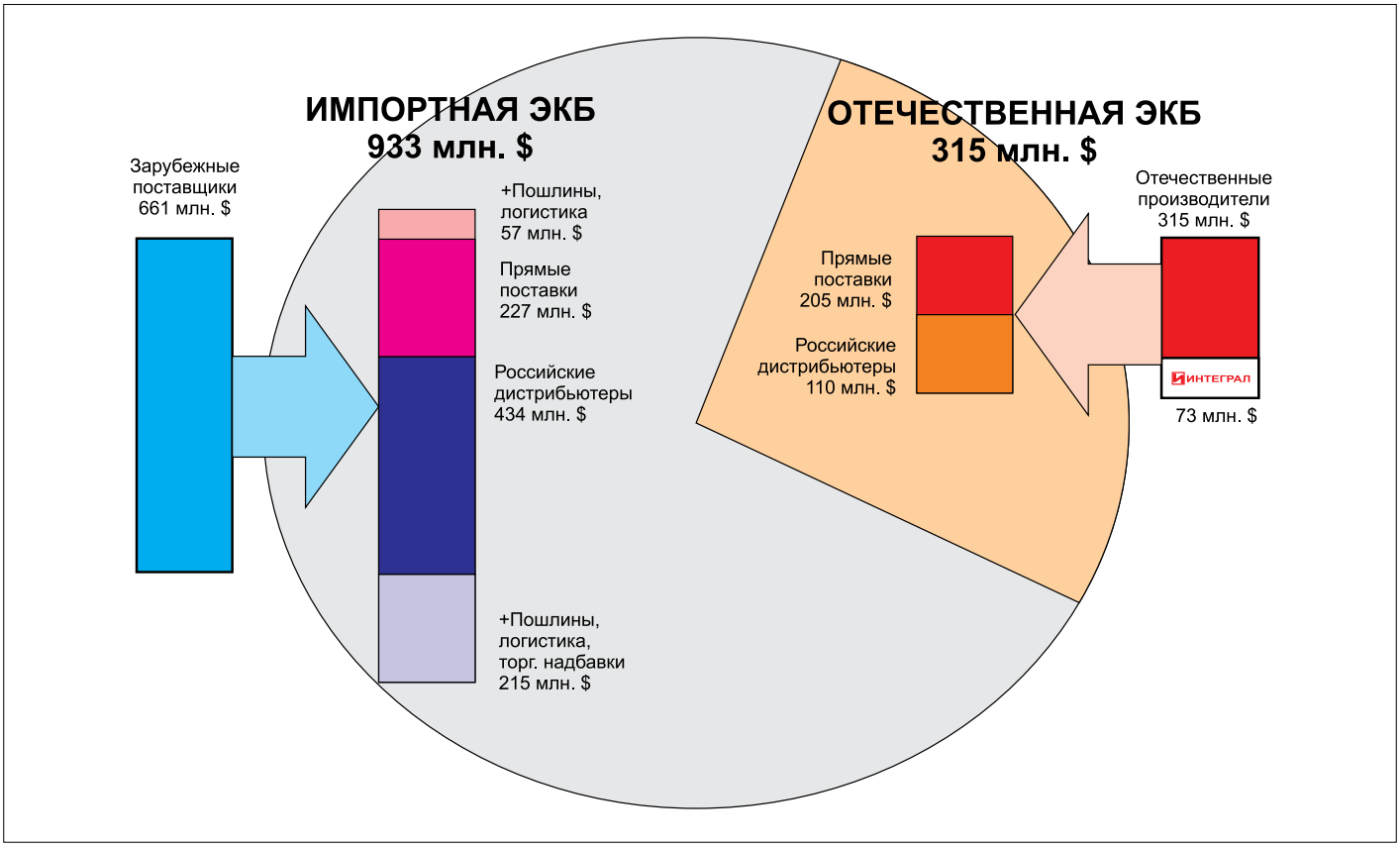

Рис. 2. Распределение рынка полупроводниковой ЭКБ Российской Федерации между поставщиками в 2017 г.

Сложившаяся на протяжении многих лет в России практика простого воспроизведения (клонирования, копирования) микросхем зарубежных аналогов для изделий коммерческой и военной электроники привела к существенному отставанию технического уровня российских изделий электронной техники от мировых стандартов. При этом сегодня необходимо учитывать и основные возможные риски, связанные с санкциями и геополитическими условиями: срывы соглашений, договоров и контрактов, запрет на применение (продажу) новейших технологий, экспортный контроль США и ЕС, а также неизбежное отставание в отечественных технологиях и продуктах и отсутствие потенциала роста компетенций отечественных инженеров-электронщиков [46]. Резко выросла вероятность появления изделий, содержащих различные незадекларированные функции («закладки», аппаратные трояны), которые практически невозможно (точнее — очень сложно) обнаружить входным контролем при закупке иностранной продукции.

Созданные за последние 5–7 лет в РФ в соответствии с ранее утвержденными концепциями национальных программ развития отечественной электронной промышленности десятки «центров системного проектирования» (дизайн-центры, фаблесс-компании) были ориентированы именно на реализацию восстановления утерянной после развала СССР компетенции проектирования радиоэлектронных систем по принципу «сверху вниз»: от алгоритма функционирования системы (устройства) к архитектуре, электрической схеме, топологии кристалла и собранному в конкретный корпус (модуль) устройству.

Как ясно следует из их названия, предполагалось, что эти исходные «алгоритмы функционирования» по аналогии с «западными стандартами» специалисты дизайн-центра будут получать от разработчиков перспективных радиоэлектронных устройств и систем, проектировать необходимые заказчику наборы микросхем с последующим их изготовлением либо на отечественных полупроводниковых фабриках, либо (в случае отсутствия требуемой технологии) на зарубежных продвинутых фабриках. Для этого даже были внесены соответствующие изменения в отечественную нормативно-техническую базу в части разграничения их классификации при включении в разрешительный перечень МНИИРИП.

Однако в итоге исходной цели достичь не удалось по причинам, основные из которых детально были исследованы нами в главах 9 «Основы государственной политики США в области обеспечения безопасности каналов поставки микросхем» и 10 «Особенности российской системы управления развитием военной электроники» [26]. В итоге решение об использовании импортной ЭКБ в отечественных системах военного, космического и двойного назначения было принято при условии организации последующего воспроизведения и освоения в отечественном серийном производстве их полных аналогов. Таким образом, в тематических планах ведущих российских и белорусских разработчиков и изготовителей ЭКБ специального и двойного назначения, прямо или косвенно участвующих в выполнении Гособоронзаказа РФ, появились соответствующие НИОКРы. Согласно информации, представленной соответствующими министерствами и ведомствами на официальных сайтах, на ближайшие 3–5 лет исключительно «воспроизведение» зарубежных аналогов с их освоением в отечественном серийном производстве будет основным направлением развития отечественной ЭКБ, для чего из бюджета РФ выделены значительные материальные и финансовые средства.

Помимо упомянутых очевидных недостатков, «данный подход требует прямого копирования очень большого количества изделий, что невозможно реально выполнить ни в разумные сроки, ни из-за ограниченного ресурса дизайн-центров, ни из-за высокой стоимости таких работ» [47].

Здесь необходимо сказать и о возникновении совершенно новой угрозы для отечественных изготовителей ЭКБ, фактически осваивающих аналоги микросхем зарубежных фирм, а именно — угроза троллинговых атак. Более детально этот механизм рассмотрен в [4], а также в разделе 8.2 «Защита прав интеллектуальной собственности на полупроводниковые микросхемы» в нашей работе [26]. На Западе все большее число даже добропорядочных производителей ЭКБ становится мишенью для «патентных троллей» — фирм или предпринимателей (иногда их называют «не практикующие организации» — non-practicingentity, NPE). NPE не производят продукции, не оказывают услуг (поэтому им юридически нельзя предъявлять встречные иски). Но эти фирмы скупают патенты компаний — разработчиков ЭКБ, активно мониторят рынок и предъявляют многомиллионные иски «нарушителям прав интеллектуальной собственности». А очевидные факты подобного «копирования аналогов» в явном виде легко можно прочитать даже на официальных сайтах Минпромторга, МНИИРИП т. д. Если раньше годовые объемы закупок ЭКБИП в РФ не превышали $ 1 млрд, то сегодня следует ожидать повышенное внимание «патентных троллей» к необъятному российскому рынку ЭКБ, что в итоге может привести к непрогнозируемым последствиям. Уровень этих угроз для отечественных изготовителей (и потребителей!) «клонированных» микросхем возрастает еще и в связи с тем, что во главе большинства NPE стоят эмигранты из бывшего СССР, хорошо знающие реальную ситуацию. Так, понимание этих угроз заставило белорусских производителей ЭКБ разработать ряд специальных защитных мероприятий.

Поэтому сегодня как никогда нужна мощная государственная программа восстановления и развития отечественной твердотельной электроники. По мнению В. Г. Немудрова, «без самодостаточности в этой сфере независимость России под вопросом или просто невозможна» [48]. В условиях все усиливающихся западных санкций и прочих ограничительных мер важно ликвидировать импортозависимость радиоэлектронной промышленности, прежде всего в сфере электронной компонентной базы, которая стала определяющей для современных вооружений, космической техники, гражданской радиоэлектронной продукции и цифровой экономики страны в целом.

У правительства РФ есть понимание того, что для достижения импортонезависимости России в части ЭКБ в первую очередь необходимо восстановить ее собственное производство в стране, а это подразумевает весь спектр ключевых средств проектирования и производства, включая аппаратные средства, САПР, технологии, специальные материалы и технологическое оборудование. По крайней мере об этом явно говорят заголовки и содержание публикаций по данной тематике отечественных руководителей и авторитетных специалистов, отвечающих за развитие российской электроники [49–53].

МЕЖПРАВИТЕЛЬСТВЕННЫЕ СОГЛАШЕНИЯ КАК ИНСТРУМЕНТ АКТИВИЗАЦИИ КООПЕРАЦИОННЫХ СВЯЗЕЙ

Как следует из первой части нашего аналитического обзора, в силу объективных причин во всем мире за последние 20 лет наблюдается тенденция глобализации мировой микроэлектроники.

Современная полупроводниковая промышленность представляет собой глобальную многоуровневую систему кооперации различных исследовательских институтов промышленных предприятий, разработчиков технологического оборудования

и средств проектирования. При этом не имеет никакого значения ни национальность ученых и специалистов, ни географическое местоположение предприятия (института), главная цель — объединить финансовые, интеллектуальные, материальные ресурсы и различные технологические базы для получения новых знаний, компетенций, материалов и технологий в стремлении сохранить технологическое лидерство в своей завоеванной нише (сегменте) мирового рынка.

Упомянутые в первой части статьи полупроводниковые альянсы типа Sematech (в США) и IMEC (в Европе) — только наиболее известные среди десятков других, успешно функционирующих сегодня в мире.

За те же 20 лет существования Союзного государства России и Беларуси в процессе его развития были достигнуты многочисленные успехи в установлении взаимовыгодных прямых научных и кооперативных связей между профильными предприятиями аграрного, машиностроительного, военно-промышленного, транспортно-логистического, авиационного, нефтегазодобывающего, энергетического, атомного, космического и многих других секторов науки и промышленности. По основным из этих направлений за прошедший период были подписаны соответствующие межведомственные решения, протоколы, меморандумы и межправительственные соглашения.

Аналогичные меморандумы, протоколы, соглашения были подписаны и успешно реализованы и в области военно-технического сотрудничества, совместной охраны границ, борьбы с терроризмом и экстремизмом и многое другое.

Что касается микроэлектроники и ее многочисленных применений, здесь наблюдается несколько иная картина. Так, подготовленный по инициативе Министерства промышленности Республики Беларусь в далеком 2015 году проект «Соглашения между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области электронной и радиоэлектронной промышленности» «потерялся» где-то между двумя Министерствами в процессе длительного согласования, так и не вступив в законную силу.

Поэтому имеет смысл привести только некоторые основные фрагменты текста проекта этого Соглашения.

Цели Соглашения:

- Развитие научно-технической, производственной и промышленной кооперации в области электронной и радиоэлектронной промышленности.
- Координация работ, проводимых в Республике Беларусь и Российской Федерации в рамках государственных программ и программ Союзного государства в области электронной и радиоэлектронной промышленности Республики Беларусь и Российской Федерации.
- Координации работ, проводимых в Республике Беларусь и Российской Федерации в области электронной и радиоэлектронной промышленности Республики Беларусь и Российской Федерации в целях производства совместной продукции и ее поставок на рынки третьих стран.

Область сотрудничества:

- Разработки, производства и использования изделий электронной и радиоэлектронной промышленности.

Формы сотрудничества:

- Планирование и осуществление совместных программ и проектов.
- Взаимный обмен научной и технической информацией, специальными знаниями, экспериментальными данными и материалами в различных областях радиоэлектронной, электротехнической и оптико-механической промышленности.
- Взаимный обмен нормативными документами по стандартизации при выполнении работ (услуг) по разработке, постановке на производство, производстве и поставке изделий специального и двойного назначения для оборонно-промышленного комплекса и обеспечения национальной безопасности Республики Беларусь и Российской Федерации.

Как видно только из этих фрагментов, цели и задачи проекта подобного Соглашения в полной мере соответствовали вышерассмотренным мировым тенденциям интеграции полупроводниковой индустрии и создавали правовую основу для взаимовыгодной интеграции интеллектуальных, технологических, финансовых и материальных ресурсов двух стран и их концентрации на прорывных направлениях.

Принимая во внимание все изложенное выше, необходимость подробного межправительственного соглашения очевидна.

ЗАКЛЮЧЕНИЕ

Итак, в предложенных выше материалах, авторы предприняли попытку представить в упрощенном, по возможности систематизированном виде результаты своего субъективного анализа текущего состояния и обозримых перспектив развития одного из самых сложных и многообразных научно-технических направлений развития современного общества — микроэлектроники. Насколько это им удалось — судить читателю.

В отличие от традиционных для аналитических обзоров и научных статей заключительных разделов типа «выводы и предложения» авторы решили, что не будут формулировать здесь никаких «выводов» — пусть каждый читатель сам сделает свои выводы по результатам прочтения этого материала.

Обратившись к многочисленным ссылкам на цитируемые источники информации, читатель обнаружит и многие другие важные тенденции развития микроэлектроники, новые проблемы и угрозы, которые авторы не приводят здесь из-за естественных ограничений, связанных с объемом статьи.

В любом случае, авторы надеются, что представленная информация будет полезна читателю в его профессиональной деятельности и послужит источником последующих дискуссий, возможных новых идей о поисках путей развития действительно отечественной микроэлектроники.

ЛИТЕРАТУРА

1. Соколов А. В., Карасев О. И. Форсайт и технологические дорожные карты для наноиндустрии//Научно-техническая политика. Российские технологии. 2009. Т. 4. № 3, 4.

2. Шашнов С. Методы форсайт-исследований для оценки перспектив развития гражданского общества и третьего сектора. М.: Высшая школа экономики, 2016.

3. WSTS Semiconductor for Market Forecast Autumn 2018. November 27, 2018. www.wsts.org

4. Макушин М. Волна сделок слияния/поглощения в микроэлектронике: причины и последствия//Электроника: НТБ. 2018. № 1.

5. Belous A., Saladukha V. High-Speed Digital System Design: Art, Science and Experience. 1st ed. Springer, 2019.

6. Belous A., Saladukha V., Shvedau S. Space Microelectronics Volume 2: Integrated Circuit Design for Space Applications. London, Artech House, 2017.

7. Belous A., Saladukha V., Shvedau S. Space Microelectronics Volume 1: Modern Spacecraft Classification, Failure, and Electrical Component Requirements. London, Artech House, 2017.

8. Меликян В. Дальнейшее масштабирование интегральный схем: вызовы и решения. VIII Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем», МЭС-2018. Зеленоград, 2 октября 2018.

9. Красников Г. Я. Конструктивно-технологические особенности субмикронных МОП-транзисторов. Изд. 2-е, испр. М.: Техносфера, 2011.

10. Lu J.-C., Holton W. C., Fenner J. S., Williams S. C. et al. A new device design methodology for manufacturability//IEEE Transactions on Electron Devices. 1998. Vol. 45. No. 3.

11. Cunningham S. P., Spanos C. J. Semiconductor yield improvement: results and best practices//IEEE Transactions on Semiconductor Manufacturing. 1995. Vol. 8. No. 2.

12. Downs T., Cook A. S., Rogers P. G. A — partitioning approach to yield estimation for large circuits and systems//IEEE Transactions on Circuits and Systems. 1984. Vol. AS-31. No. 8.

13. Gaston G. J., Walton A. J. The integration of simulation and response surfacemethodology for the optimization of IC processes//IEEE Transactions on Semiconductor Manufacturing.1994. Vol. 7. No. I.

14. Sighal K. and Pinel J. F. Statistical design centering and tolerancing using parametric sampling//IEEE Transactions on Circuits and Systems. 1981. Vol. 13, No. П.-V.

15. Kouleshoff A. A., Nelayev V. V. New approach for the response surface methodology//Proc. 4th Int. Workshop on New Approaches to High-Tech: Nondestructive Testing and Computer Simulations in Science and Engineering. Russia, St.-Petersburg, 2000.

16. Koskinen T., Cheung P. Y. K. Hierarchical Tolerance Analysis Using Statistical Behavioral Models//IEEE Transactions Computer-Aided Design of Integrated Circuits and Systems.1996, Vol. 15, Iss. 5.

17. Benkoski J.. Stroiwas A. J. A new approach to hierarchical and statistical timing simulation//IEEE Transactions Computer-Aided Design. 1987. Vol. CAD-6. No. 6.

18. KurkerC. M., Paulos J. J., Gyurcsik R. S., Lu J.-C. Hierarchical yield estimation of large analog integrated circuits//IEEE Journal of Solid-State Circuits. 1993. Vol. 28. No. 3.

19. Кулешов А. А., Малышев В. С., Нелаев В. В., Стемпицкий В. Р. Статистическое проектирование и оптимизация технологии производства интегральных микросхем//Микроэлектроника. 2003. Т. 32. № 31.

20. Belous A., Nelayev V., Syakerski V. End-to-end statistical proess/device/circuit/system design. 34th Euromicro Conference on Software Engineering Advanced Applications. SEEA and 11th Euromicro Conference on Digital SystemDesign — architectures, methods and tools. DSD, September 2008.

21. Белоус А., Солодуха В., Шведов С. Основы конструирования высокоскоростных электронных устройств. Краткий курс «белой магии». М.: Техносфера, 2017.

22. Tomioka K. et al. A III–V nanowire channel on silicon for high-performance vertical transistors//Nature. 2012. Aug.

23. Belous A., Saladukha V., Shvedau S. High Velocity Microparticles in Space//Springer Nature Switzerland AG, 2019.

24. Romanov I., Komarov F., Milchanin O., Vlasukova L., Parkhomenko I., Makhavikou M. Structural Evolution and Photoluminescence of SiO_2 Layers with SnNanocrystals Formed by Ion Implantation//Journal of Nanomaterials. 2019. Vol. 2019.

25. Romanov I. A., Parkhomenko I. N., Vlasukova L. A., Komarov F. F., Kovalchuk N. S., Milchanin O. V., Makhavikou M. A., Mudryi A. V. Blue and red light-emitting non-stoichiometric silicon nitride-based structures//Известия НАН Беларуси. Сер. физ.-мат. наук. 2018. Т. 54. № 3.

26. Белоус А., Солодуха В., Шведов С. Программные и аппаратные трояны. Способы внедрения и методы противодействия. Первая техническая энциклопедия. В 2-х книгах. М.: Техносфера, 2018.

27. Комаров Ф. Ф., Нечаев Н. С., Пархоменко И. Н., Ивлев Г. Д., Власукова Л. А., Пилько В. В., Вендлер Э., Комаров А. Ф. Формирование фотоприемных структур ИК-диапазона путем пересыщения кремния теллуром//Доклады НАН Беларуси. 2019. Т. 63. № 5.

28. Белоус А., Солодуха В. Современные технологии контроля безопасности в микроэлектронике//Компоненты и технологии. 2018. № 10.

29. U. S. Department of Commerce. Defense industrial base assessment: unterfeit electronics. 2010.

30. 112th Congress. Inquiry into counterfeit electronic parts in the department of defense supply chain. Senate Report of the Committee on Armed Services, 2012.

31. Belous A., Saladukha V. Viruse, Hardware and Soft ware Trojans — Attacks and Counter measures. 1-st ed. Springer, 2019.

32. Office of the Under Secretary of Defense For Acquisition, Technology, Logistics. Defense Science Board (DSB) study on high performance microchip supply, 2005. www.acq.osd.mil/dsb/reports/ADA435563.pdf

33. Skorobogatov S. Hardware assurance and its importance to national ecurity. 2012. www.cl.cam.ac.uk/sps32/secnews.html

34. Белоус А. И., Гайворонский К. В., Турцевич А. С. Программные и аппаратные трояны — технологическая платформа кибероружия. ГГУ им. Ф. Скорины, 2018.

35. Innovation is at risk as semiconductor equipment and materials industry' loses up to $4 billion annually due to IP infringement. SEMI, 2008. www.semi.org/en/Press/P043775

36. Rostami M., Koushanfar F., Rajendran J., Karri R. Hardware security: Threat models and metrics. Proc. of the International Conference on Computer-Aided Design, 2013.

37. Кузнецов Е., Сауров А. Аппаратные трояны. Часть 1. Новые угрозы кибербезопасности//Наноиндустрия. 2016. № 7.

38. Митчел С., Стефан Д.и Альменар С. Г. Атаки через аппаратные закладки, которые приводят к нарушению криптографической безопасности в системах шифрования fpga.

39. Becker G. T. et al. Stealthy dopant-level hardware trojans. Cryptographic Hardware and Embedded Systems-CHES 2013. Spring, Berlin Heidelberg, 2013.

40. Jin Y., Makris Y. Hardware Trojans in wireless cryptographic integrated circuits//IEEE Design & Test. 2013. Iss. 99.

41. Wolff F. et al. Towards Trojan-free trusted ICs: Problem analysis and detection scheme. Proceedings of the conference on Design, automation and test in Europe. ACM, 2008.

42. Jin Y. and Makris Y. Hardware Trojan detection using path delay fingerprint. Hardware-Oriented Security and Trast 2008, HOST-2008. IEEE International Workshop, 2008.

43. Ali S., Chakraborty R. S., Mukhopadhyay D., Bhunia S. Multi-level attacks. An emerging security concern for cryptographic hardware. Proc. Design, Automation & Test in Europe Conference & Exhibition (DATE), 2011.

44. Banga M., Hsiao M. S. Trusted RTL: Trojan detection methodology in pre-silicon designs. Proc. IEEE Int/Hardware-Oriented Security and Trust (HOST) Symp., 2010.

45. Покровский И. И. Отчет исследования российского рынка электронных компонентов/ООО «СОВЭЛ», 2019.

46. Шпак В. В. Микроэлектроника — основа национального суверенитета. Форум «Микроэлектроника-2018». Алушта, Крым, 2018.

47. Щепанов А. Развитие российской электронной компонентной базы: взгляд эксперта//Электроника: НТБ. 2019. № 7.

48. Немудров В. Г. Без самодостаточной отечественной микроэлектроники не сохранить политическую независимость России//Электроника: НТБ. 2017. № 6.

49. Красников Г. Я. Нужно двигаться вперед, а не ждать, когда будет подготовлена почва//Электроника: НТБ. 2017. № 9.

50. Красников Г. Я. В союзе с конструктором. www.rg.ru/2017/03/19/akademik-krasnikov-rasskazal-o-sudbe-rossijskoj-mikroelektroniki.html

51. Шпак В. В. Развитие отечественной электроники — не прихоть, а острая необходимость//Электроника: НТБ. 2019. № 6.

52. Шпак В. В. Российская микроэлектроника: не стоит догонять, надо стараться опережать//Экономические стратегии. 2018. № 12.

53. Шпак В. В. Микроэлектроника — основа национального суверенитета. Форум «Микроэлектроника-2018». Алушта, Крым, 2018.