DOI: 10.22184/1992-4178.2018.181.10.80.86

Надежность закупаемых ИС: опыт Министерства обороны США

М. Макушин[1], А. Фомина, д. э. н.[2]

УДК 621.38 | ВАК 05.27.06

Сфера государственного регулирования включает в себя такой специфический сегмент как обеспечение надежности ИС, закупаемых в интересах оборонных и специальных ведомств. Политику в этой области проводят все страны, которые в значительных объемах производят военную радиоэлектронную аппаратуру. Отказ одной из ИС, особенно в боевых или предвоенных условиях, может иметь тяжелые, а иногда и непредсказуемые последствия. Наиболее интересным опытом обеспечения надежности закупаемых ИС военного назначения обладают США.

ОБЩИЕ ТЕНДЕНЦИИ РАЗВИТИЯ В ОБЛАСТИ ИС ВОЕННОГО НАЗНАЧЕНИЯ В США

В 1960–1970-е годы спрос подрядчиков Пентагона был одним из главных факторов развития рынка ИС наряду с запросами изготовителей больших и универсальных ЭВМ, а также поставщиков средств связи. Министерство обороны США признало, что передовая технология микроэлектроники имеет большое значение для обеспечения военного превосходства страны с момента зарождения этой отрасли. При этом спектр требований ведомства варьируется от дорогих, узкоспециализированных, унаследованных* и почти устаревших компонентов до современных технологий, лежащих в основе будущих возможностей.

С тех пор динамика рынка полупроводниковых приборов кардинально поменялась. Появление в 1980-х годах персональных ПК резко стимулировало развитие рынка ИС гражданского назначения. За ПК последовали сотовые телефоны. По мере расширения продаж ИС гражданского назначения доля ИС военного назначения сокращалась. Сейчас в общей структуре спроса на ИС доля приборов военного назначения составляет 1–2%. В США этот показатель несколько выше, но правительство все равно не имеет рыночных рычагов влияния на поставщиков. В целом же мировой рынок ИС для военных / аэрокосмических систем в 2017 году достиг 2,9 млрд долл., что на 8% превысило уровень 2016-го (табл. 1).

В выполнении военных заказов заинтересовано небольшое количество фирм. Более того, многие видят в них помеху своему развитию – объемы производства ИС для военных / аэрокосмических систем малы, отличаются длительными циклами проектирования и жесткими требованиями. Кроме того, рынок фрагментирован, так как в отрасли разрабатываются разнообразные системы: авионика, средства РЭБ, РЛС и т. п. Тем не менее между этими сегментами есть общее. Военная система, как правило, представляет собой сложную платформу, требующую времени для интеграции и тестирования. Большая часть подобной электроники – практические разработки, достигающие уровня зрелости за несколько поколений. В значительной части это унаследованные технологии, что, впрочем, не исключает применения современных технологий.

Малая емкость рынка, измеряемого партиями от сотен до тысяч ИС, – одна из причин, по которой в оборонной промышленности так популярны вентильные матрицы, программируемые пользователем (FPGA). Также большим спросом пользуются специализированные ИС (ASIC) и радиоприборы на основе GaN, которые обычно изготавливаются на территории США.

Таблица 1. Динамика мирового рынка ИС для военных / аэрокосмических систем. *Источник: Databeans*

Год	2014	2015	2016	2017
Объем продаж, млрд долл.	3,0	3,1	2,8	2,9

[1] Главный специалист АО «ЦНИИ «Электроника».

[2] Генеральный директор АО «ЦНИИ «Электроника».

* **legacy systems (= legacy database, legacy software, legacy device)** – унаследованные системы (приложения, базы данных, ПО, устройства), переставшие удовлетворять потребностям, но все еще находящиеся в эксплуатации из-за трудностей их замены, так как при проектировании таких систем не были заложены возможности их перестройки. Это наглядно проявилось в связи с так называемой проблемой 2000-го года.

Местоположение завода по обработке пластин – только один из факторов. Гражданские и военные заказчики разрабатывают приборы в сложных цепях поставок с использованием различных инструментальных средств САПР, СФ-блоков и производственных технологических процессов. При этом в настоящее время ИС и конечные системы могут проектировать подрядчики, расположенные иногда в разных странах, а результаты работ передаются в электронном виде по сетям связи, разработчики имеют доступ к закрытым секторам баз данных друг друга. Интеграторы систем обеспокоены возможностью кибератак. Например, злоумышленник может внести вредоносное изменение в последовательность технологических операций, открывающее возможности кражи интеллектуальной собственности или использования контрафактных приборов. Для предотвращения этого Министерство обороны США создало программу «Надежные кремниевые заводы» (Trusted Foundry) и предприняло ряд других действий, призванных на аппаратном уровне гарантировать невозможность преднамеренного или случайного «подрыва» технологического процесса по всей цепочке поставок.

ПРОГРАММА «НАДЕЖНЫЕ КРЕМНИЕВЫЕ ЗАВОДЫ»

На протяжении многих лет оборонная промышленность США была обеспокоена проблемой приобретения надежных приборов, что стало особенно актуальным с 1990-х годов, когда американские технологии и производственные мощности по выпуску ИС начали выводиться за рубеж. Пытаясь избежать негативных последствий для национальной безопасности, правительство США построило собственный завод, чтобы обеспечить поставку надежных ИС военного назначения. Расположенное в Форт-Миде (штат Мэриленд) предприятие находилось под управлением Агентства национальной безопасности (АНБ). Однако издержки на его модернизацию постоянно росли, и завод в конце концов закрыли.

В результате Министерство обороны США в начале 2000-х годов разработало новую стратегию, предусматривавшую передачу производства ИС военного назначения на мощности американских заводов, расположенных только на территории страны. В 2003–2004 годах отделение микроэлектроники (Microelectronics Group) корпорации IBM, выигравшее контракт на поставку ИС для Министерства обороны США, стало **единственным поставщиком передовых и надежных услуг** кремниевого завода для этого ведомства. Таким образом появилась программа «Надежные кремниевые заводы», которая первоначально охватывала два завода IBM по обработке пластин – в г. Эссекс-Джанкшен (штат Вермонт) и Ист-Фишкилл (штат Нью-Йорк). В рамках этой программы разрешение на допуск к работе выдается службой безопасности, как правило, после проверки биографии руководства и персонала предприятия. При таком условии завод получает право обрабатывать пластины как для гражданских, так и для военных заказчиков. Однако существуют определенные этапы технологического процесса, ориентированные только на военных заказчиков и обособленные от остального предприятия.

В 2007 году программа была расширена и теперь охватывает все фирмы, входящие в цепочку поставок ИС для Министерства обороны США – fabless-фирмы (проектирование ИС), поставщики шаблонов, кремниевые заводы и фирмы, специализирующиеся на корпусировании (рис. 1). Все это надежные поставщики, которые для получения данного статуса обязаны пройти процесс аккредитации, включающий проверку анкетных данных и мер обеспечения безопасности своих производственных мощностей (и иных объектов). В отличие от сделки с IBM «надежные поставщики» не получают ежегодные контракты с гарантированными объемами закупок. Но они могут использовать свой статус и претендовать на государственные заказы.

Сложный процесс аккредитации в качестве «надежного поставщика» доступен не всем фирмам, а окупаемость иногда ограничена, объемы заказов ИС военного назначения невелики. В программе «Надежный поставщик» задействованы различные кремниевые заводы, использующие как КМОП, так и специализированные процессы. Наиболее передовым для подобных поставщиков является 90-нм процесс. В качестве самого современного поставщика услуг кремниевого завода в рамках программы «Надежные кремниевые заводы» выступала корпорация IBM. Однако в 2015 году она продала свое отделение микроэлектроники корпорации GlobalFoundries и больше не рассматривает полупроводниковые приборы в качестве одного из основных направлений деятельности. Это вызвало беспокойство

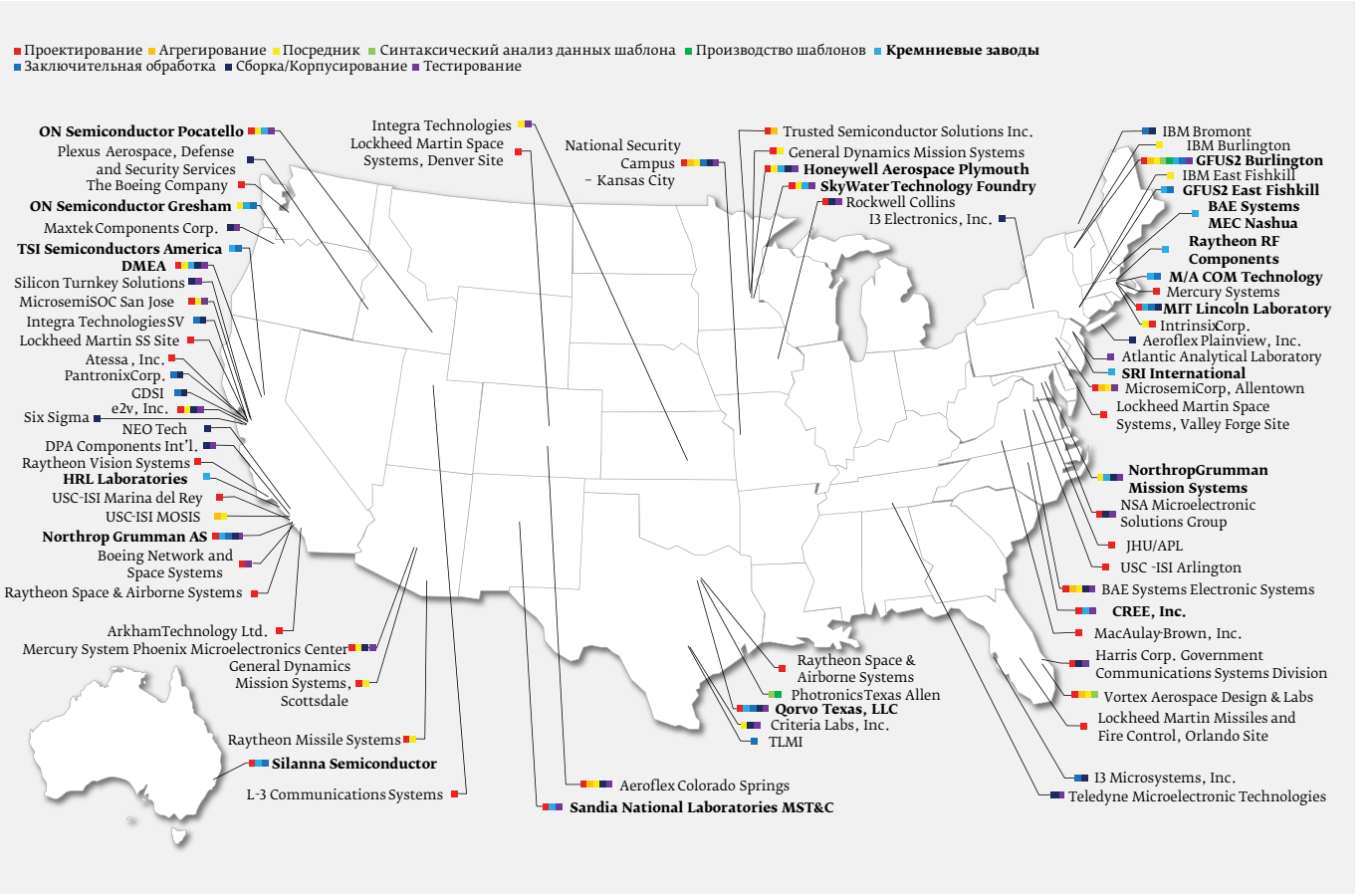

Рис. 1. Местонахождение доверенных кремниевых заводов/поставщиков Министерства обороны США. *Источник: МО США*

у руководителей оборонной промышленности США – **формально GlobalFoundries не является американской фирмой, поскольку принадлежит Фонду суверенного достояния (Mubadala Development Co.) эмирата Абу-Даби**. Этим государственным инвестиционным фондом владеют власти страны.

Тем не менее DMEA* передало контракт доверенного кремниевого завода GlobalFoundries. Таким образом, заводы по обработке пластин (в штатах Вермонт и Нью-Йорк) остались частью данной программы (с аттестацией Category-1A** и ITAR***). На предприятиях используются SiGe и радиочастотные процессы.

* **DMEA (Defense Microelectronics Activity)** – подразделение МО США в области микроэлектроники оборонного назначения.

** **Category-1A** – предприятие, предоставляющее услуги доверенного кремниевого завода (товары и услуги) изготовителям конечных электронных систем, являющимся подрядчиками МО США.

*** **ITAR (International Traffic in Arms Regulations)** – Правила международной торговли оружием, свод нормативных актов, разработанный госдепартаментом США в целях контроля за экспортом товаров и технологий, связанных с обороной и безопасностью.

Наиболее передовым КМОП-процессом является 32-нм технология «кремний-на-изоляторе». Недавно DMEA расширило сделку с GlobalFoundries, включив в нее новый завод корпорации в штате Нью-Йорк, обрабатывающий 300-мм пластины по 14-нм FinFET-технологии. Официально у него нет статуса надежного кремниевого завода, однако он аттестован по категории 2 (Category-2), то есть на предприятии принимаются все меры по обеспечению неприкосновенности интеллектуальной собственности и других секретов заказчиков. Тем не менее военные заказчики пользуются доступом к 14-нм процессу GlobalFoundries, а также шаблонам и услугам корпусирования. Корпорация предлагает комплексное решение, привлекая в качестве партнера завод IBM по корпусированию ИС в г. Бромон (Канада) [1].

В августе 2018 года, когда GlobalFoundries отказалась от работ над 7-нм процессом, ограничившись развитием технологий с топологическими нормами 14 нм и выше [2, 3], программа «Надежные кремниевые заводы» вышла на новый этап. Соответственно, военным подрядчикам приходится искать решения в области технологий с проектными

* reverse engineering – обратный инжиниринг, обратное проектирование/конструирование. Инженерный анализ технологии изготовления какого-либо товара с целью раскрытия технологических секретов фирмы-конкурента и последующего незаконного копирования.
** PPP/CPI – передача с использованием протокола связи точка-точка/стандартного программного коммуникационного интерфейса.

Рис. 2. Новые подходы Министерства обороны США к выбору надежных и гарантированных поставщиков. *Источник: МО США*

нормами 10/7 нм у других поставщиков. Такие решения понадобятся Министерству обороны США, но не в ближайшей перспективе. Сейчас большая часть военных платформ использует ИС, изготовленные по более зрелым технологиям. Однако по мере освоения технологий искусственного интеллекта, требующих значительных вычислительных мощностей, понадобятся самые передовые процессы. Считается, что они позволят значительно увеличить вычислительную мощность при сохранении или даже дальнейшем уменьшении габаритов конечных электронных систем. Выбор в области 10-/7-нм технологий невелик – корпорации Intel, Samsung и TSMC, и военные круги оценивают возможность работы с каждым из этих поставщиков.

ПЕРСПЕКТИВНАЯ СТРАТЕГИЯ МИНИСТЕРСТВА ОБОРОНЫ США

Сейчас Министерство обороны США разрабатывает новую стратегию в области надежных поставщиков. Ситуация рассматривается в контексте современного состояния кремниевых заводов, обслуживающих заказы на изготовление ИС военного/авиакосмического применения. Существует несколько вариантов:

- работать с GlobalFoundries, используя технологии с проектными нормами 14 нм и более;
- воспользоваться услугами любого кремниевого завода из перечня надежных поставщиков Министерства обороны США;
- разместить заказ на кремниевом заводе (как американском, так и неамериканском), не включенном в перечень.

У каждой фирмы есть стратегия. Так, например, корпорация Xilinx на протяжении многих лет заказывала

Таблица 2. Бюджетная заявка на 2019 финансовый год по микроэлектронике

Программа, статья расходов	Финансирование, млн долл.	
	2018	2019
Надежная микроэлектроника (PE604294D8Z)	83,6	233,1
Верификация и аттестация	41,5	41,7
Новые подходы к надежности	42,1	191,3
Надежная микроэлектроника (PE0605294D8Z)	61,0	56,1
Надежные шаблоны	2,0	2,0
Демонстрационная версия новых подходов к надежности	59,0	54,1
Итого	**144,6**	**289,2**

производство FPGA на тайваньском кремниевом заводе TSMC. Но эта корпорация не является частью программы «Надежный кремниевый завод» и не относится к надежным поставщикам, так как в программу не включены заводы по обработке пластин, расположенные в КНР или на Тайване. Тем не менее TSMC продолжает совершенствовать технологические процессы, и Xilinx не видит необходимости менять свою практику, ведь благодаря этому она получает доступ к мощностям с новейшими производственными процессами, на которых выполняются начальные этапы обработки пластин (формирование транзисторной структуры). Завершающие этапы (металлизация), а также программирование Xilinx осуществляет в США, то есть TSMC не получает доступ к реальным данным конечного заказчика о конфигурации / конструкции FPGA.

Однако есть ряд проблем. Например, фирма Flex Logix изготавливает FPGA на мощностях TSMC. Сейчас фирма поставляет 16-нм встраиваемые FPGA, одновременно разрабатывает 7-нм приборы. Недавно корпорация Boeing, лицензировавшая технологию Flex Logix, приступила к изготовлению 14-нм ИС на мощностях GlobalFoundries в штате Нью-Йорк. Для обеспечения производства Flex Logix перенесла свою технологию на 14-нм процесс GlobalFoundries. Но проблема в том, что оборонный бизнес относительно невелик. Для получения прибыли Flex Logix использует свою технологию как для военных, так и для гражданских заказчиков. Однако и здесь не обходится без трудностей. GlobalFoundries только предоставляет доступ к своей технологии с топологиями до 14 нм. А оборонная промышленность желает получить доступ к технологиям с проектными нормами 10 нм и менее. Соответственно, ей нужно будет работать с такими поставщиками, как TSMC, не имеющими статуса надежного поставщика.

Проблема заключается в том, **что современные гражданские технологические процессы охватывают сложную цепочку поставок. Недоверенный и даже доверенный технологический процесс может подвергаться рискам на фоне растущего количества кибератак, что требует новых решений, обеспечивающих достаточную защиту**. В этих целях Министерство обороны США разрабатывает методологию поставок, получившую название «Программа надежной и гарантированной микроэлектроники» (Trusted and Assured Microelectronics program) (рис. 2). В рамках этих работ особое внимание уделяется методикам прослеживания всей цепочки поставок. В центре внимания – разработка и переход к новым методикам обеспечения надежности и гарантий, то есть отказ от прежних подходов в пользу производства на кремниевых заводах за счет расширения возможностей защиты процесса проектирования и цепочки обеспечения надежности всех технологических операций (от разработки ИС до эксплуатации и технического обслуживания) [1].

Реализация Программы надежной и гарантированной микроэлектроники началась в 2018 финансовом году, на эти цели было выделено 144,6 млн долл. На 2019 год запрошено уже в два раза больше (табл. 2) [4].

Существуют и другие решения. В прошлом году объединенная рабочая группа по надежной микроэлектронике предложила несколько методов противодействия попыткам несанкционированного вмешательства, а именно: функциональную дезинтеграцию, проектирование на основе доверенности и разделение заводов по обработке пластин. В случае функциональной дезинтеграции разработчики распределяют функциональность прибора, чтобы вновь объединить его функционал уже на системном уровне – на территории США. Примером функциональной дезинтеграции является программа CHIPS, реализуемая Управлением перспективного планирования оборонных научно-исследовательских работ Министерства обороны США (DARPA). Идея программы в том, что разработчику предлагается меню модульных кристаллов ИС (или чиплетов*), объединенных в библиотеку. Собранные в модуль чиплеты подключаются с использованием схемы межсоединений [5, 6].

Другой подход – «проектирование под надежность» (design-for-trust). Например, FPGA может предлагать в конструкции функцию «ДНК или отпечаток пальца»

* **chiplet** – чиплет, созданные в 2013 году в исследовательском центре Пало-Альто компании Xerox специализированные микросхемы, обладающие минимальной вычислительной мощностью и рядом других функций, что позволило их использовать в качестве малого микропроцессора, устройства хранения данных, сложной логической схемы или части MEMS, выполняющих функции датчиков различных параметров, например, освещенности, температуры, давления, движения и ускорения.

кристалла ИС (Physically Unclonable Function, PUF). Технология, разработанная специалистами Массачусетского технологического института, определяет для каждой ИС уникальное цифровое обозначение («подпись») кристалла.

Еще одна идея – разделение технологического процесса по разным заводам по обработке пластин. Подразумевается, что начальные этапы обработки пластины (включая формирование транзисторной структуры) могут осуществляться за рубежом, но завершающие (включая металлизацию) – на территории США. Идея разделения заводов по обработке пластин не лишена ряда недостатков. Во-первых, требуются значительные ресурсы. Во-вторых, одному кремниевому заводу может понадобиться обмен конфиденциальными данными с другим. Известно несколько вариантов такого подхода. DMEA строит завод завершающих этапов обработки пластин (металлизация) в Калифорнии, но его технологии будут масштабироваться только до 90 нм. При этом не ясно, будет ли осуществлять масштабирование менее 90 нм какой-либо другой надежный кремниевый завод. Тем временем есть некоторые наработки на рынке шаблонов.

В настоящее время поставщиком наиболее современных шаблонов для программы «Надежные кремниевые заводы» Министерства обороны США является GlobalFoundries. При этом правительство США хочет получить резервный источник шаблонов с 14-нм топологиями. Недавно военное ведомство США опубликовало запрос на информацию (RFI*) о поставщиках шаблонов, способных поставлять эти изделия с 14-нм топологиями. В процессе отбора участвует корпорация Photronics, американский гражданский поставщик шаблонов. Эта корпорация была аккредитована в 2010 году как доверенный поставщик шаблонов с топологиями до 150 нм [7].

Все частные промышленные американские корпорации, работающие в секторе военной микроэлектроники, хотят быть уверенными, что программа «Надежные кремниевые заводы» будет продолжаться. Здесь кроется еще одна проблема. Количество кибератак растет, развитие технологий не замедляется. Например, КНР вкладывает в сегмент национальной микроэлектроники миллиарды долларов. Соответственно, правительство США пока не совсем понимает, какими могут быть оптимальные способы противостояния подобным вызовам [1].

* **RFI (request for information)** – официальный документ МО США, публикуемый в открытой печати в целях получения от заинтересованных фирм данных о технологиях, процессах, приборах и т. д., которые министерство могло бы использовать в своих целях.

* * *

Производство ИС военного назначения тесно связано с вопросами секретности и защиты информации о конструкциях микросхем, методах их проектирования и производства. Однако по мере развития научно-технического прогресса, масштабирования ИС и нарастания киберугроз действующие методики обеспечения защиты производства и разработки ИС военного назначения перестают отвечать современным реалиям. Министерство обороны США пытается сформировать новые подходы и методики обеспечения доверия ко всем заводам по обработке пластин, являющимся его подрядчиками. Среди этих мер можно выделить:

- новые методы организации цепочки поставок;
- новые методы проектирования, изготовления и корпусирования, включая чиплеты;
- использование метода разделения заводов-производителей, когда начальные этапы обработки пластин, включая формирование транзисторной структуры, выполняются на одном заводе, а завершающие (включая металлизацию) – на доверенном предприятии.

Для реализации последнего метода Министерство обороны США создает собственный завод по обработке пластин, использующий достаточно зрелые технологии.

Существование и развитие программы «Надежных кремниевых заводов» и другие меры МО США по обеспечению надежности закупаемых ИС показывают ошибочность распространенного в России мнения о том, что достаточно создать отечественную индустрию разработки современных и перспективных ИС, а производство передать на зарубежные кремниевые заводы. Такое мнение не просто ошибочно, а опасно с точки зрения интересов национальной безопасности.

ЛИТЕРАТУРА

1. **LaPedus M.** A Crisis In DoD's Trusted Foundry Program? // Semiconductor Engineering, October 22.
2. **Merritt R.** GF Grabs AI Wins with FD-SOI // EE Times. 09.26.18.
3. Mentor releases optimized flow, new fill automation for GLOBALFOUNDRIES' 22FDX IC manufacturing process // Solid State Technology. The Pulse. 2018. October 09.
4. Accounts of Interest in the Presidential Budget Request for Financial Year 2019 // NDIA.org, 2018.
5. **LaPedus M.** The Chiplet Race Begins // Semiconductor Engineering. 2018. August 06.
6. **Russell J.** DARPA's CHIPS Program Aims for Mix-and-Match Functionalities // HPC wire, August 29, 2017.
7. New Methods to Instill Trust in Commercial Semiconductor Fabrication // NDIA. Trusted Microelectronics Joint Working Group. Team 4. White Paper. 2017. July.