DOI: 10.22184/1992-4178.2020.201.10.18.22

Новая комплексная научно-техническая программа по развитию микро- и радиоэлектронной промышленности

Рассказывает советник АО «НИИАА», ФГУ ФНЦ НИИСИ РАН В. В. Симонов

Госкорпорацией «Ростех» недавно было подготовлено предложение по разработке новой комплексной научно-технической программы (КНТП), направленной на создание программно-аппаратных платформ для обеспечения безопасности систем с критической миссией.

О том, почему такая программа особенно актуальна в текущих условиях, какие основные направления работ она включает, а также о том, как она сможет способствовать развитию российской микроэлектронной промышленности, мы поговорили с первым генеральным директором Российского агентства по системам управления (РАСУ), ныне советником АО «Ордена Трудового Красного Знамени научно-исследовательский институт автоматической аппаратуры имени академика В. С. Семенихина» (АО «НИИАА»), ФГУ «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук» (ФГУ ФНЦ НИИСИ РАН), к. т. н. Владимиром Валентиновичем Симоновым.

Владимир Валентинович, Госкорпорацией «Ростех» подготовлено предложение по разработке КНТП «Комплексная разработка и производство приоритетных доверенных интеллектуальных программно-аппаратных платформ на основе отечественных электронных компонентов и программного обеспечения». Почему эта идея появилась именно сейчас?

В настоящее время в отрасли часто можно услышать фразу: «Государство повернулось лицом к электронике». Она неоднократно звучала и на недавно прошедшей в Ялте Отраслевой научно-технической конференции радиоэлектронной промышленности. И это действительно так.

Во многом это связано с цифровизацией, с исполнением программы «Цифровая экономика РФ». Важность этого процесса в современном мире уже можно считать очевидной. Однако цифровизация обязана быть связана с развитием отечественной электроники и микроэлектроники. И это прекрасно понимает Председатель Правительства РФ Михаил Владимирович Мишустин, поэтому наша отрасль стала получать существенную поддержку от государства. А двигателем этого процесса, безусловно, выступает заместитель Председателя Правительства РФ Юрий Иванович Борисов, курирующий, в частности, направление радиоэлектроники и микроэлектроники и обладающий богатым собственным опытом работы в этой сфере.

За последние несколько десятилетий были предприняты попытки развивать отрасль разными путями. Один из таких путей – передать всё в частные руки, на откуп рыночной экономике. Однако это не сработало. Нужно отдать должное Юрию Ивановичу: он открыто признал ошибочность этого подхода. Электронная отрасль очень ресурсоемкая и низкомаржинальная, частные инвесторы просто не могут «потянуть» такие вложения и развивать отрасль без поддержки государства. Слово «инвестиции» повторяется

сейчас, как мантра. Но полагаться на частные инвестиции при такой низкой доходности и несформированном рынке сбыта бессмысленно.

С другой стороны, что можно сделать на те деньги, которые выделяются государством на развитие отрасли? В общенациональном плане восстановления экономики России на это заложено порядка 150 млрд руб. в год, то есть немногим более 1,5 млрд евро. Этого не хватит даже на то, чтобы построить современную микроэлектронную фабрику со средними топологическими нормами. О передовых нормах – 7, 5, 3 нм – я даже не говорю. Более того, рынок оборудования для микроэлектроники сильно монополизирован, а учитывая санкции, нам просто не дадут это оборудование приобрести, равно как и лицензии на технологические процессы, продуктовые лицензии, специалистов. Но приоритетность и критическая важность микроэлектроники в развитии страны бесспорны. На мой взгляд – сейчас появилась последняя возможность не остаться в глубоких сателитах мирового хай-тека.

Теоретически, мы можем создать собственные технологии совместно с партнерами, допустим, из Азии. Но здесь мы возвращаемся к вопросу о рынке сбыта. «Рынок» – еще одна отраслевая «мантра». На текущий момент следует констатировать, что как такового рынка для отечественной электроники нет. Конкуренция между немногочисленными дизайн-центрами идет не за долю рынка, не за клиента, а за бюджет. Завод «Микрон» – практически единственная действующая у нас серийная фабрика – достоин уважения за то, что им удалось сохранить производство. Но в то же время «Микрон» по мировым меркам – очень маленькое производство, и они тоже ориентированы преимущественно на регулируемые рынки: RFID-метки для отслеживания товаров, транспортные карты, электронные документы. И даже эти рынки дают загрузку порядка 1–2 тыс. пластин в месяц, тогда как любая рентабельная фабрика должна выпускать в месяц минимум 30 тыс. пластин.

Итак, возникает следующий вопрос: «Как обеспечить рынок сбыта?» На зарубежные массовые рынки нас никто не пустит: они уже поделены. Их не хватает даже глобальным игрокам: мы видим постоянные слияния и поглощения среди производителей компонентов.

Остается рынок внутренний. Вообще говоря, эти выводы совпадают с мировой практикой: все страны, которые хотят развивать и защищать свою промышленность, начинают с внутреннего рынка.

Чтобы понять, что именно имеет смысл разрабатывать и производить в первую очередь для внутреннего рынка, чтобы это стало основой для дальнейшего развития отрасли, можно вспомнить историю. В начале-середине 1990-х, когда отрасль находилась в тяжелом положении, в какой-то мере выйти из этой ситуации помогла программа в области специальной вычислительной техники. Это был оборонный проект. Было принято решение создать вычислительные системы для различных видов и родов войск на основе унифицированного ряда процессоров «Эльбрус» и «Комдив» (знаменитая серия специализированной вычислительной техники «Багет»). Были разработаны процессоры на основе, подчеркну, отечественных СФ-блоков, на их базе была создана соответствующая аппаратура, которая, конечно, в дальнейшем модернизировалась, но до сих пор используется в различных системах вооружения: от подводных лодок до истребителей. Эта комплексная программа оказалась вполне успешной.

Исходя из этого, у группы руководителей и специалистов радиоэлектронного кластера ГК «Ростех» и РАН возникла идея сделать что-то подобное сейчас для внутреннего гражданского рынка. В программе «Цифровая экономика РФ» большое внимание уделяется критической инфраструктуре, есть Федеральный закон «О безопасности критической информационной инфраструктуры РФ», есть программа ГосСОПКА, направленная на защиту критической инфраструктуры. Но почему речь только об инфраструктуре? Ведь нужно защищать и сами стратегические объекты, сбои в функционировании которых или выход которых из строя могут приводить к тяжелым последствиям.

Так и материализовалась идея разработать программу, направленную на создание программно-аппаратных доверенных платформ для управления системами с критической миссией (СКМ), чтобы, с одной стороны, свести к минимуму риски, касающиеся правильного их функционирования, а с другой – максимально задействовать ресурсы отечественной промышленности в разработке всех компонентов этих платформ, включая ЭКБ, аппаратуру и ПО, обеспечив им гарантированный рынок сбыта.

Что понимается под системой с критической миссией?

Определение этого термина дается в заявке на разработку КНТП. Это система, нештатное функционирование которой может привести к масштабным неблагоприятным последствиям для стратегически важных объектов, таким как прекращение функционирования, высокие финансовые потери, разрушение объектов управления, травмы или гибель людей, экологический ущерб.

В документе также конкретизируется, какие именно системы относятся к классу СКМ. Это цифровые системы управления сложными комплексными техническими объектами, такими как тепловые, атомные и гидроэлектростанции, железнодорожные узлы, аэропорты, электросети, предприятия нефтехимической промышленности, газонефтетранспорта; тепловыми, газовыми и гидравлическими турбинами, энергогенераторами, электроподстанциями, системами функционирования на железнодорожном транспорте, насосами и компрессорами для добычи, транспортировки и переработки нефти и газа, атомными энергетическими установками, а также

цифровые системы управления специального и двойного назначения.

То есть здесь речь идет о самих объектах, вокруг которых построена критическая информационная инфраструктура. Те методы, которые направлены на защиту информационной инфраструктуры, призваны прежде всего противодействовать таким угрозам, как хакерская атака или непреднамеренный сбой в передаче данных. Но есть угрозы, возникающие на базе локальных преднамеренно или не преднамеренно созданных уязвимостей, приводящих к нештатному функционированию СКМ.

В настоящее время сложилась критическая зависимость отечественной радиоэлектроники от зарубежной ЭКБ. Доля микроэлектронных комплектующих иностранного производства в отечественных радиоэлектронных системах управления превышает 70%, а в телекоммуникационном оборудовании – 90%. Какие риски это несет? В первую очередь вспоминается такое понятие, как «закладки», то есть преднамеренно внедренные в аппаратные или программные средства недокументированные возможности, с помощью которых можно собирать информацию об объекте, влиять на его функционирование или даже полностью вывести его из строя. Но, помимо преднамеренных вредоносных «закладок», существуют и просто ошибки. В документе компании Intel № 326767-004 говорится: «...корпорация Intel снимает с себя всякую ответственность, которая может возникнуть при ненадлежащем функционировании продуктов корпорации в системах с критической миссией», а в документе № 324209-012 той же компании есть такие слова: «корпорация Intel официально заявляет, что продукты, описанные в документации, могут содержать дефекты или ошибки, которые могут вызвать отклонения реального поведения продуктов от поведения, описанного в опубликованных спецификациях...». И такая осторожность компании вполне понятна. Современные процессоры, системы на кристалле, микроэлектронные модули настолько сложны, что выявление и устранение ошибок в них – очень долгая и дорогая процедура, а в коммерческих продуктах крайне важны цена и скорость вывода на рынок. Исправлять ошибки может быть просто нецелесообразно. Произошел сбой в ноутбуке, «завис» смартфон – неприятно, конечно, но ничего жизненно важного не случилось. Совсем другое дело, когда речь идет о цифровой системе управления, например, атомной станцией, самолетом.

Всё дело в том, что в отечественных радиоэлектронных средствах применяется зарубежная микроэлектроника именно коммерческого класса, правильность функционирования которой, как мы видим, производитель не гарантирует.

Те же соображения справедливы и в приложении к программным средствам.

Другой риск связан с поставками зарубежных комплектующих, лицензий, ПО, в особенности в нынешней политической обстановке. Недавний пример – то, что произошло с проектом МС-21, когда в одночасье санкциями были перекрыты поставки в Россию для этого самолета, и сейчас разрабатываются в том числе бортовые системы на отечественной ЭКБ. Конечно, в этом есть и положительный аспект, но хотелось бы, чтобы разработка аппаратуры выполнялась на российской компонентной базе системно, а не в срочном порядке под давлением обстоятельств.

Поэтому, когда речь идет о системах с критической миссией, необходимо весь процесс разработки держать под контролем, использовать только проверенные и прежде всего отечественные комплектующие, созданные на базе отечественных СФ-блоков, и доверенное ПО, контролировать процессы изготовления от СФ-блоков и ПО до доверенных аппаратно-программных платформ (АПП).

И, вообще говоря, мы здесь не открыли ничего нового. Программа по обеспечению безопасности СКМ давно существует в США, есть такая программа и в Китае, и в других странах. И нам она тоже необходима.

Вы упомянули Федеральный закон «О безопасности критической информационной инфраструктуры РФ». Каким законом регулируется безопасность СКМ?

Есть несколько федеральных законов, область применения которых охватывает обеспечение безопасности отдельных видов объектов, например объектов ТЭК или опасных производств. Однако закона, посвященного безопасности СКМ, на данный момент нет.

Его разработка – одна из задач, которую планируется выполнить в рамках реализации программы.

Давайте перейдем к содержанию предлагаемой программы. Что именно планируется реализовать, чтобы противостоять упомянутым рискам?

В программе определены 14 направлений работ, направленных на решение этой задачи, которые разделили на шесть проектов.

Первый проект сосредоточен на фундаментальных исследованиях и включает в себя четыре направления:

- исследования в области специфики методов проектирования, производства и контроля доверенной ЭКБ;
- исследования в сфере создания доверенных АПП СКМ, включая основные модели угроз и атак для АПП различных классов СКМ и возможности их парирования;
- исследования оптимальных путей создания семейства доверенных СФ-блоков для отечественных универсальных микропроцессоров с развитыми средствами самоконтроля и диагностики для интеллектуальных АПП;
- исследования по оптимизации семейства электронных модулей, сопроцессоров, технологий создания приложений, средств статистического анализа программ, обеспечивающих отслеживание

и интеллектуальный анализ, выявление, самолечение и ликвидацию уязвимостей в режиме реального времени.

Второй проект – разработка и серийное производство доверенной ЭКБ – перекрывает следующие три направления:

- исследования применяемых в отечественной ЭКБ лицензионных СФ-блоков на предмет возможности их использования в АПП СКМ;
- адаптация и локализация лицензируемых архитектур и вновь разрабатываемых СФ-блоков, определение типоряда доверенных СФ-блоков, рекомендованных для использования в ЭКБ для АПП СКМ;
- разработка и освоение серийного производства ключевой ЭКБ с развитыми средствами самоконтроля, диагностики и самокоррекции, обеспечивающими контроль соответствия штатному функционированию как отдельных, так и всех узлов универсального микропроцессора в целом.

Два направления относятся к третьему проекту – разработке и серийному производству доверенного ПО. Это разработка технологий и инструментальных программных средств для поддержки жизненного цикла разработки и эксплуатации доверенного ПО и для проверки ограничений на время выполнения фрагмента программы, задания последовательности действий и контроля порядка их выполнения, анализа других динамических характеристик и поиска аномалий.

Четвертый проект – разработка и серийное производство доверенных АПП – включает три направления:

- разработка унифицированного семейства серийных доверенных интеллектуальных АПП для цифровых систем управления различных классов СКМ;
- создание интеллектуальных компонентов для систем управления СКМ с развитыми средствами самоконтроля, отслеживания и самокоррекции ключевых параметров управления, сформированных на основе моделей угроз и их парирования;
- разработка технологии доверенного комплексирования серийных аппаратно-программных компонентов, обеспечивающей создание доверенных интеллектуальных АПП, моделей их «штатного» функционирования и соответствующих этой модели профилей на различных уровнях.

Тринадцатое направление – создание доверенных интеллектуальных проблемно-ориентированных аппаратно-программных комплексов, в том числе с интеллектуальной реконфигурацией архитектуры – выделено в пятый проект.

Наконец, последнее четырнадцатое направление – это организация обучения, переобучения и подготовка кадров для программы. Здесь задействована элита наших университетов во главе с МГУ им. М. В. Ломоносова.

Работа разбита на два этапа, первый из которых представляет собой параллельно-последовательную разработку доверенных аппаратных и программных решений, а второй – доработку полученных решений и формирование полного цикла производства доверенных комплексов. Первый этап предполагается завершить к 2025 году, а второй – к концу 2027-го.

В рамках работы предполагается разработать 15 базовых доверенных АПП, 100 СФ-блоков, 50 специализированных СБИС. Целевое количество поданных патентных заявок, связанных с выполнением программы, составит 180; количество продуктов и услуг на базе доверенных АПП, СФ-блоков и модулей, внедренных в сфере цифровой экономики при реализации программы, – 250, включая 60 программных изделий.

В программе предусмотрена разработка не менее 16 образовательных программ по доверенным АПП, СФ-блокам и модулям, подготовка не менее 390 специалистов в данной области.

В чем, по вашему мнению, основное отличие данной программы от тех ФЦП, которые существовали ранее?

В определенном смысле, эта программа – систематизация и структуризация тех средств, которые выделяются государством на развитие отрасли. Она конкретизирует цели, а не только способы освоения части из них, привязку к конкретным, а не возможным потребителям.

В отличие от ФЦП, выполнявшихся в течение прошлых лет, в ней делается акцент на комплексность и конкретный результат – под заказчика. Это не завуалированная финансовая помощь отдельным предприятиям с тем, чтобы они «пережили трудные времена», а затем за них всё сделает рыночная экономика. Не сделает. Мы уже в этом убедились.

В отечественной электронике и радиоэлектронике всегда было сложно усадить за один стол переговоров и производителей ЭКБ, и разработчиков конечных изделий. Комплексность этой программы позволит преодолеть эту проблему для решения конкретной задачи – обеспечения безопасности адресных систем с критической миссией.

Это – комплексный проект с понятным финансированием и результатом, который сформирует долгосрочный рынок для отечественной микроэлектроники – доверенных СБИС, СФ-блоков, модулей, а также для специализированных аппаратных и программных средств, аппаратно-программных платформ и систем.

Руководители программы считают, что мы должны начинать с внутреннего рынка, но ее реализация в перспективе может открыть возможность освоения и зарубежных рынков – конечно не массовых, потребительских, а рынков доверенных систем, к которым у ряда стран есть достаточно высокий интерес.

Какие предприятия будут задействованы в выполнении программы? Планируется ли привлечение к данной работе отраслевых ассоциаций – консорциумов?

Руководство работ – естественно, за Минпромторгом России. За реализацию КНТП в целом отвечает ГК «Ростех», его радиоэлектронные предприятия контура управления АО «Объединенная приборостроительная корпорация» (АО «ОПК»); за ее научную часть – институты РАН, прежде всего ФГУ ФНЦ НИИСИ РАН, ИСП РАН и др.

Всего в реализации программы будет задействовано более 100 предприятий и организаций, в том числе стратегически важных отраслей промышленности, транспорта, ТЭК.

Особенно важно, что все разработки – от программы научных исследований до прикладных ОКР – будут выполняться коллективами, состоящими из числа разработчиков и постановщиков задач, заказчиков. Именно это и будет гарантией внедрения результатов НИОКР. Ведь программы импортозамещения есть в каждой отрасли. Таким образом появляется возможность их неформальной реализации.

Что касается консорциумов, это очень полезные организации, но у них есть своя специфика. Состав консорциума – вещь по определению непостоянная. Компании могут присоединяться к нему, могут его покидать. Как следствие, консорциум сам по себе не может нести ответственность за выполнение программы. Это площадка для коммуникаций, экспертное сообщество, но не исполнитель.

Среди их представителей – молодые и очень активные люди. Некоторые из руководителей консорциумов высказали желание возглавить те или иные направления в рамках реализации КНТП. Руководители программы будут только за.

На какой стадии находится работа над программой на данный момент?

КНТП, как и комплексная программа научных исследований, создается под научным руководством академика РАН Владимира Борисовича Бетелина, внесена Минпромторгом России – Департаментом радиоэлектронной промышленности под руководством Василия Викторовича Шпака, и прошла совет по приоритетному направлению научно-технологического развития РФ «Переход к передовым цифровым, интеллектуальным производственным технологиям, роботизированным системам, новым материалам и способам конструирования, создание систем обработки больших объемов данных, машинного обучения и искусственного интеллекта» и еще ряд госэкспертиз.

Сейчас дорабатываются отдельные положения программы, она готовится к следующему этапу – защите проекта на Совете по науке и образованию при Президенте РФ.

В рамках работы над проектом определены необходимое финансирование и коллективы исполнителей, разработаны тематические карточки по всем направлениям, которые уже согласованы не только с исполнителями, но и потребителями, в частности из ТЭК, авиационной, атомной и других отраслей – всего 12 якорных заказчиков программы.

Работа идет по плану: со стороны ГК «Ростех», АО «ОПК» под руководством Сергея Степановича Сахненко, очень жестко следят за соблюдением установленных сроков. К сожалению, из-за эпидемии многие сейчас работают удаленно. Это затрудняет общение. Во всяком случае, всегда эффективнее обсуждать вопросы лицом к лицу, видеть, что с вами соглашаются не из вежливости.

Спасибо за интересный рассказ.

С В. В. Симоновым беседовал Ю. С. Ковалевский

ОБНОВЛЕННАЯ СЕРИЯ УСТАНОВОК ЭЛЕКТРОННО-ЛУЧЕВОГО НАПЫЛЕНИЯ ТОНКИХ ПЛЕНОК В СВЕРХВЫСОКОМ ВАКУУМЕ В ГЕОМЕТРИИ «LIFT-OFF»

SemiTEq
ОТ ЗАМЫСЛА ДО ВОПЛОЩЕНИЯ

- Максимальный размер обрабатываемых подложек – Ø200 мм или 150x150 мм для стеклянных и керамических пластин
- Возможность оптимизации расхода материала за счет изменения расстояния «испаритель-подложка» в пределах 350÷500 мм

STE EB71
Стандартное исполнение

STE EB71M
Исполнение с опцией резистивного испарения в шлюзовой камере

ЗАО «НТО»
пр. Энгельса, 27
Санкт-Петербург, 194156, Россия
Тел.: +7 812 601 06 05,
Факс: +7 812 313 54 29
sales@semiteq.ru

www.semiteq.ru

EXPO ELECTRONICA

23-я Международная выставка электронных компонентов, модулей и комплектующих

13–15 апреля 2021
Москва, Крокус Экспо

expoelectronica.ru

Получите Ваш
бесплатный билет
по промокоду **ee21print**

Hyve