DOI: 10.22184/1992-4178.2020.201.10.10.16

Для обеспечения КИИ отечественными доверенными решениями объективных препятствий нет. Нужна только воля к победе

Рассказывает президент Ассоциации разработчиков компьютерных технологий доверия и безопасности «Доверенная платформа» А. И. Тихонов

Ассоциация «Доверенная платформа» была образована в 2015 году. В то время она была сосредоточена на создании доверенных и безопасных мобильных решений, построенных на основе открытых международных стандартов. Со временем сфера деятельности ассоциации расширилась, перекрыв практически все вопросы разработки доверенных решений в области как программного, так и аппаратного обеспечения.

В настоящее время ассоциация плотно взаимодействует с Департаментом радиоэлектронной промышленности Минпромторга России и принимает активное участие в реализации Стратегии развития электронной промышленности РФ на период до 2030 года в качестве технологического консорциума. Одной из важнейших задач, которые перед собой ставит эта организация, является обеспечение критической информационной инфраструктуры (КИИ) российскими доверенными решениями на отечественной ЭКБ.

О том, насколько это реализуемо и какие имеются возможности и препятствия на пути решения данной задачи, мы поговорили с президентом Ассоциации разработчиков компьютерных технологий доверия и безопасности «Доверенная платформа» Андреем Ивановичем Тихоновым.

Андрей Иванович, за последнее время в электронной и радиоэлектронной отрасли было создано несколько ассоциаций, что является частью реализации отраслевой стратегии, принятой в начале года. Однако ассоциация «Доверенная платформа» существует уже пять лет. Что побудило к ее созданию и что легло в ее основу?

Всё верно: в этом октябре нашей ассоциации исполнилось пять лет. Изначально она была организована как сообщество разработчиков технологий безопасности, производителей оборудования, софта, платформенных решений, системных интеграторов и нашей научной элиты и сосредоточена на создании доверенных и безопасных мобильных решений, построенных на основе открытых международных стандартов.

В качестве ее учредителей выступили 11 компаний, среди которых был Институт системного программирования имени В. П. Иванникова Российской

академии наук (ИСП РАН), ведущие разработчики решений в области информационной безопасности, такие как «Инфотекс», разработчики ПО, системные интеграторы и другие компании.

Но достаточно быстро стало очевидно, что тема доверия намного шире и главное – глубже. Уже на втором-третьем году существования ассоциации мы начали работать в направлении средств интегрированной безопасности. Эта тема стала своеобразной визитной карточкой ассоциации.

В чем заключается глубина доверия? Почему вы употребили именно это слово?

Фактически, всё, что касается доверия и безопасности в рамках устройств, систем и сервисов, начинается с того, что называется корень доверия. Совершенно очевидно, что, например, смартфоны, которыми мы пользуемся ежедневно, – это часть сервисов, которые предоставляют такие компании, как Google, Apple и т. п. Чтобы такой аппарат мог гарантировать нам, как потребителям, безопасность при использовании приложений, доступе к облаку и т. п., необходим некий фундамент доверия, который был бы максимально защищен от возможных атак злоумышленников и который даже мы сами не могли бы скомпрометировать. Ведь каждый из нас может ошибиться: кликнуть на вредоносную ссылку, поверить фейковому сообщению, пришедшему по электронной почте, установить ненадежное приложение... Любая подобная ошибка может привести к тому, что на устройстве появится троянская программа, которая дальше уже сама, без нашего участия, будет пытаться получить доступ к нашим ресурсам, паролям и т. п. И чтобы этому противостоять, безопасность должна базироваться на механизмах, до которых ни подобная вредоносная программа, ни сам пользователь не сможет добраться.

Поэтому чем глубже и надежнее «запрятан» корень доверия, тем выше будет уровень доверия и безопасности всей системы. Самое лучшее, если корень доверия располагается внутри чипа, куда добраться сложнее всего, хотя по-прежнему возможно.

Задача корня доверия платформы – защитить корневые (исходные) ключи аутентификации, гарантировать то, что они не будут несанкционированно считаны или модифицированы. Физически он представляет собой аппаратный блок, который надежно хранит необходимые ключи и производит вычисления, нужные для подтверждения аутентичности и целостности программного обеспечения платформы, импортируемой и экспортируемой информации. Он может быть реализован в виде СФ-блока в центральном процессоре или как отдельная ИС.

Корень доверия – это точка отсчета. А далее необходим ряд подсистем, которые обеспечивают наследование свойств доверия и безопасности от уровня к уровню, начиная от корня доверия, включая ОС, приложения и заканчивая всей платформой, системой, сервисом. Это и есть интегрированная безопасность.

Таким образом, основа доверенности – по сути, кристалл. Означает ли это, что в стране может существовать собственная доверенная платформа, только если у нее есть производство таких кристаллов?

Вообще говоря, чем бóльшая часть жизненного цикла доверенной платформы реализована на территории страны, тем более высокий уровень доверия может быть достигнут.

В потребительской сфере, если честно, тех корней доверия, которые встроены в наши смартфоны и ПК их производителями, для повседневных нужд более чем достаточно. Достаточно их и для большинства промышленных применений.

Чем бóльшая часть жизненного цикла доверенной платформы реализована на территории страны, тем более высокий уровень доверия может быть достигнут

Но если мы говорим о критической информационной инфраструктуре, там ситуация иная. Дело в том, что взлом защищенной системы требует определенных ресурсов, тем больших, чем лучше система защищена, и будет ли злоумышленник тратить соответствующие ресурсы зависит от того, насколько для него важно взломать эту систему. Когда мы говорим о целевых атаках, злоумышленник будет использовать все возможности, которые у него есть. Если он может на этапе производства чипа корня доверия тем или иным образом в него вмешаться, возможно, он это сделает. А последствия такой атаки на КИИ могут быть катастрофическими. Не зря же эту инфраструктуру называют критической.

Поэтому, если корень доверия производится за рубежом даже на основе российского дизайна, это – риск. Да, вероятность связанных с этим негативных последствий в ряде случаев может составлять считанные проценты, может быть даже доли процента, но их цена для некоторых применений настолько высока, что эту вероятность нельзя игнорировать.

Какой необходим уровень полупроводникового производства, чтобы изготовить чип корня доверия? Можно ли это сделать на российской фабрике уже сейчас?

Если корень доверия входит в качестве интегральной части в СБИС, например центрального процессора, то, само собой, необходимый уровень технологий будет определяться уровнем технологий этой СБИС.

Однако есть и другой вариант: корень доверия может быть реализован и в виде отдельной микросхемы. Сам по себе он не такой требовательный в плане производительности и количества элементов, для его производства не требуются самые передовые технологии. Примером реализации подобного подхода может служить аутентификация терминалов мобильной связи, когда корнем доверия является отдельная микросхема – процессор SIM-карты.

Наша роль четко коррелирует с ролью консорциумов, как ее определяет Минпромторг России в соответствии со Стратегией развития электронной промышленности РФ на период до 2030 года

Реализуя вариант внешнего исполнения, можно сделать отечественный центральный процессор на зарубежной фабрике по той технологии, которая для этого необходима, например 16 или 7 нм, не прибегая к тотальной проверке кристалла, а усилия по обеспечению максимального уровня доверенности сосредоточить на отдельном кристалле. При этом кристалл корня доверия может также изготавливаться за рубежом, но для него в обязательном порядке производится глубокая постпроизводственная верификация, накладывающая некоторые ограничения на выбор технологии изготовления, а по мере наработки базы необходимых компонент (СФ-блоков и библиотек) для отечественных фабрик, производство может организовываться в России с теми топологическими нормами, которые у нас есть, – 90 или 180 нм. Таким образом, корень доверия будет обладать максимальным уровнем доверенности. И этот подход последовательно реализуется лидирующими участниками нашего консорциума.

Когда ассоциация занялась темой интегрированной безопасности, включающей и аппаратный уровень, наверняка потребовалось расширение состава ее членов с включением в нее компаний из электронной и радиоэлектронной отрасли. Это так?

Безусловно. Сейчас в число членов ассоциации входят не только производители электронного оборудования, такие как АО «НИИ «Масштаб», ОАО НПП «Полигон», АО «Концерн «Созвездие», ООО «Т8», АО «НПП «Цифровые решения», ООО «Булат», ООО «Юзергейт» и др., но и разработчики и производители ЭКБ, включая АО «ВЗПП-С», ПАО «Микрон», АО НПЦ «ЭЛВИС», АО «ПКК Миландр», АО «Байкал Электроникс».

Само собой, в консорциум входят компании – лидеры в области безопасности, такие как АО «Лаборатория Касперского», АО «Инфотекс», ООО «Код Безопасности», АО «НПК «Криптонит», АО «НТЦ «Атлас», АО «Аладдин Р.Д.» и др. Практически все ключевые имена присутствуют в нашей ассоциации. Кроме того, среди членов ассоциации – поставщики различного рода платформенных решений. Это АО «ИВК», ООО «КНС ГРУПП» (YADRO), ООО «Группа Борлас», ООО «Новые Облачные Технологии» – разработчик ПО «МойОфис», ЗАО «НПФ «ДОЛОМАНТ» и многие другие.

Академическую сферу у нас представляет ИСП РАН, с которым мы работаем с самого начала. Недавно к нам присоединился НИУ МИЭТ, что отражает наш усиливающийся фокус на ЭКБ.

С началом работы по теме интегрированной безопасности наша роль постепенно начала меняться от точечных усилий для развития той или иной технологии в сторону провязывания индустрии с целью создания полноценных интегрированных отечественных решений. К настоящему времени наша новая роль полностью сформировалась, и она четко коррелирует с ролью консорциумов, как ее определяет Минпромторг России в соответствии со Стратегией развития электронной промышленности РФ на период до 2030 года.

В области интегрированной безопасности была проделана большая работа, в первую очередь с компаниями «Лаборатория Касперского», «ЭЛВИС» и «Инфотекс». Мы очень глубоко исследовали эту тему по всем новым классам угроз аппаратного характера, встроенного ПО и прочего. И эта работа продолжается до сих пор. В рамках этой деятельности мы начали плотно работать с ФСТЭК России.

Следующий этап, который у нас начался примерно 2,5 года назад и выполнялся совместно с ПАО «Ростелеком», был связан с доверенными телекоммуникационными системами. Мы сделали упор на создание и применение доверенного сетевого оборудования российского производства. Совместно с J'son & Partners Consulting – одной из ведущих аналитических компаний, в частности, в области рынка телекоммуникаций,

мы в инициативном порядке провели исследование рынка КИИ в первую очередь с точки зрения применения ИКТ. В этом исследовании приняли участие ключевые члены нашей ассоциации.

Следует отметить, что тогда многим ставка на российские решения казалась нереалистичным подходом, практически никто не верил в саму возможность существования достойного отечественного сетевого оборудования, а Реестр ТОРП считался инструментом, который не может заработать в принципе.

Мы же, наоборот, считали сами себя недостаточно радикальными и говорили, что нужно идти дальше вплоть до ЭКБ отечественного производства.

Здесь нужно сказать огромное спасибо Олегу Евгеньевичу Бочарову, заместителю министра промышленности и торговли РФ, который тогда прислушался к нашим доводам, поддержал их, и дальше мы пошли по пути создания решений для интегрированной безопасности на основе российского оборудования и ЭКБ вместе с Минпромторгом России.

Видно, какие изменения произошли за эти два с небольшим года. Было принято Постановление Правительства РФ от 10 июля 2019 года № 878, которое определило правила формирования и ведения Единого реестра российской радиоэлектронной продукции. Этот реестр уже стал основой для защиты отечественных производителей оборудования.

События развиваются очень быстро, и в этом большая заслуга нынешнего руководства Департамента радиоэлектронной промышленности Минпромторга России. Оно методично и достаточно твердо довело до всей отрасли простое сообщение: «Мы серьезно. Всё российское оборудование будет на российской ЭКБ». И сейчас даже самые тертые и циничные участники индустрии, которые пережили большое количество разных стратегий, поняли и приняли этот посыл.

Нам посчастливилось быть в центре происходящего. Департаментом проводится очень грамотная политика в области нормативного регулирования, а мы, как отраслевое сообщество, видим коммерческие и технические аспекты и стараемся максимально содействовать их деятельности.

Какое из недавних изменений в нормативном поле вы назвали бы наиболее полезным?

Это уже упомянутое постановление № 878. Но как только оно было принято, возникло два важных вопроса.

Первый – применение оборудования, включенного в реестр. Здесь всё понятно. У этого оборудования есть два пути: закупка для государственных и муниципальных нужд в соответствии с Федеральным законом № 44-ФЗ и государственными корпорациями и компаниями с госучастием – по Федеральному закону № 223-ФЗ. В этом отношении определены жесткие правила, и хотя некоторые проблемы и риски остаются, в целом это, на мой взгляд, самое лучшее, что было сделано за последнее время.

С другим вопросом сложнее. Как оборудование вносится в реестр, каким требованиям оно должно удовлетворять?

В отношении балльной системы оценки степени локализации оборудования мы занимаем позицию, что баллы должны начисляться строго за применение российской ЭКБ и других комплектующих

Здесь еще нужна более детальная проработка, которая потребует активного участия индустрии. Но ориентиры уже жестко проставлены. Объявлено, что с середины следующего года телекоммуникационная аппаратура будет включаться в реестр оборудования российского производства только при условии, что в ней используются российские микросхемы. Это очень важно, в частности, потому, что условием субсидирования в соответствии с Постановлением Правительства РФ от 17 февраля 2016 года № 109 является включение соответствующего оборудования в данный реестр. Если гарантии, что это произойдет, у компании нет, как она будет в дальнейшем отчитываться по использованию субсидии?

Помимо условий включения продукции в реестр оборудования российского производства, сейчас активно обсуждается балльная система оценки степени локализации. Какую позицию вы занимаете в этом вопросе?

Действительно, в отношении балльной системы разные группы отстаивают различные интересы.

Мы занимаем достаточно радикальную позицию: баллы должны начисляться строго за применение российской ЭКБ и других комплектующих. Всё должно быть абсолютно линейно. Мы считаем, что ключевым фактором является именно компонентная база, потому что именно она определяет основу локализации всей цепочки. Ведь если ЭКБ российская, то это подразумевает и разработку, и производство самого оборудования в России.

Наше мнение – что система должна быть в целом одинаковая для всех областей радиоэлектронной промышленности. Конечно, должны быть определенные

различия, отражающие особенности конкретного вида изделий, потому что очень трудно создать единую балльную систему, например, для светотехники и для телекоммуникационного оборудования. Но базовый принцип должен быть одинаковый, нужен общий знаменатель.

Главное, что хотелось бы со стороны Минпромторга России, чтобы начатое было продолжено с той же уверенностью в каждом движении

Это наш взгляд на данный вопрос. Но я вполне допускаю, что в каждой области могут существовать свои представления, свой здравый смысл.

Наша задача – внести предложения, довести свою точку зрения до Минпромторга России, а он, как регулятор, уже примет решение. И очень важно, что министерство прислушивается к нашим предложениям. В частности, именно так развивалось обсуждение этого вопроса на недавно прошедшем заседании Координационного совета разработчиков и производителей ЭКБ, РЭА и продукции машиностроения, где свои точки зрения высказали как сам Департамент радиоэлектронной промышленности, так и различные отраслевые ассоциации.

Какие у вас есть пожелания в отношении мер в области нормативного регулирования со стороны Минпромторга России?

Главное, что хотелось бы, чтобы начатое было продолжено с той же уверенностью в каждом движении. Индустрия – это большое количество разных людей, множество сообществ. Все пытаются так или иначе адаптироваться к существующим условиям, воспользоваться ими. И чтобы от этого была польза, со стороны регулятора необходима последовательная политика, ясность мышления и твердая рука.

Сейчас индустрия получила хороший формат взаимодействия с регулятором, он прислушивается к мнению отрасли, принимает решения и последовательно проводит их в жизнь. Хорошим примером этого служит то, что мнение индустрии было учтено при разработке Стратегии развития электронной промышленности РФ на период до 2030 года. Наша ассоциация также активно участвовала в этом процессе.

Что было сделано за последний год и какие задачи стоят перед вами в настоящее время?

На основе результатов совместного исследования с J'son & Partners Consulting, о котором я упомянул ранее, в этом году мы разработали дорожные карты по двум направлениям.

Первое направление отражает то, что мы можем сделать на базе уже существующей отечественной ЭКБ. К текущему моменту ведущие российские дизайн-центры, такие как «ЭЛВИС», «Байкал Электроникс», МЦСТ, уже создали очень интересные СБИС, на базе которых в ближайшие два года можно сделать весьма производительные решения в области телекоммуникаций и вычислительной техники, которые будут обладать повышенным уровнем доверия и безопасности.

Второе направление – что необходимо сделать в рамках решения задачи обеспечения доверия и безопасности. Здесь был обнаружен очень серьезный пробел. Оказалось, что у нас практически не уделялось внимание так называемым средствам традиционной коммутации – сетевым процессорам и всему тому, что связано с физическими каналами передачи данных: с оптикой и т. п.

Задачу устранения данного пробела придется решать с нуля, и это потребует времени. Мы это вписали в дорожную карту, представили ее в Минпромторге России и надеемся, что соответствующие работы будут в ближайшее время поставлены на уровне министерства.

Знаковым событием для нас стало состоявшееся 30 июня текущего года подписание соглашений об организации взаимодействия для выполнения стратегических задач реализации промышленной политики по развитию электронной промышленности Минпромторгом России и Минцифры России с пятью отраслевыми консорциумами, включая нашу ассоциацию. Подписанное соглашение еще раз подчеркивает нашу роль в содействии развитию отрасли, в том числе в отношении импортозамещения и расширения применения отечественной электронной продукции.

Собственно, этим мы сейчас и занимаемся. Спектр тем и задач растет. К ним прибавляются такие направления, как промышленный Интернет вещей – область, включающая множество решений, среди которых промышленные контроллеры, модульные системы, специализированные протоколы и т. п.

Одной из перспективных областей являются квантовые вычисления и криптография.

Конечно, нельзя объять необъятное. Поэтому по мере усложнения задач и увеличения их числа происходит определенное их разделение по разным ассоциациям в зависимости от их специализации. Так, мы взяли на себя в большей степени сетевое оборудование, а Консорциум «Телекоммуникационные

технологии» (АНО ТТ) – то, что связано с сотовыми сетями 5G и т. п.

В то же время все эти области взаимосвязаны, и это требует плотного взаимодействия с другими ассоциациями. Поэтому мы активно работаем и с АНО ТТ, и с Консорциумом «Вычислительная техника» (АНО «ВТ»), и с ассоциацией «Консорциум дизайн-центров и предприятий радиоэлектронной промышленности».

А как построено ваше взаимодействие с ФСТЭК России? Оно ограничивается консультациями по нормативной базе или этот регулятор тоже прислушивается к вашим рекомендациям?

Нужно сказать, что ФСТЭК – это очень открытый к взаимодействию и очень профессиональный регулятор. Их сотрудники, включая высшее руководство, являются экспертами в области безопасности. Я даже сказал бы, лучшими экспертами в индустрии. Они отлично знают все передовые технологии, трезво оценивают риски и по-настоящему открыты всему новому.

Когда мы заговорили о доверенной ЭКБ, ФСТЭК консолидировал усилия всех знаковых представителей индустрии безопасности. Мы первыми представили свои предложения по высокотехнологичным и внешним аппаратным угрозам, угрозам интегрированного ПО и др. Наши предложения были должным образом оценены и учтены.

Когда вы получаете новые знания, нужно гармонизировать с ними имеющуюся у вас картину. И такая работа началась. Таким образом тема интегрированных средств защиты информации начала выделяться в отдельный поток. Исходя из этого и на основании глубокого и детального анализа планов по локализации оборудования и ЭКБ, а также реальных возможностей индустрии ФСТЭК оперативно вносит изменения в свою нормативную базу и грамотно мотивирует отрасль.

На мой взгляд, уровень нормативной документации ФСТЭК может служить эталоном в России. Впрочем, учитывая работу Департамента радиоэлектронной промышленности в настоящее время, сейчас эталонов два.

Помимо изменений в нормативном регулировании, сейчас поддержка электронной промышленности выражается и в значительном увеличении государственного финансирования. В то же время говорится, что со временем должна расти доля частных инвестиций в отрасль. По вашему мнению, достаточны ли те условия, которые созданы, для того чтобы спустя определенное время запустить рыночные механизмы, перевести отрасль по крайней мере в самоподдерживающееся состояние?

Я думаю, что запуск рыночных механизмов достижим в том случае, если у нас просто будет исполняться законодательство. Например, условием выдачи субсидии по Постановлению Правительства РФ № 109 может быть обязательство компании реализовать установленное количество изделий. Это коммерческий риск компании. Но если компания не продаст заявленное количество, это будет не только недостаток выручки, но и нарушение условий субсидирования, и компания будет обязана субсидию возвратить. Иначе говоря, риски компании удваиваются, и она будет в большей мере мотивирована создать такое изделие, которое будет продаваться.

Мне видится, что сектора, регулируемого Федеральными законами № 44-ФЗ и № 223-ФЗ, вполне достаточно, чтобы рынок «схватился»

Безусловно, возможность сбыта тесно связана с гарантией рынка. Главная гарантия на сегодняшний день – это законы № 44-ФЗ и № 223-ФЗ, а также постановление № 878. Это очень хорошие гарантии, но необходимо, чтобы они работали.

Когда у нас началось импортозамещение в области ПО, первая реакция потребителей была закупить привычные импортные решения на пять лет вперед, пока есть возможность. Их можно понять. Но что они будут делать через пять лет, когда поддержка этих продуктов прекратится?

Поэтому нужны продуманные регламенты и твердые и последовательные действия регулятора, для того чтобы эта система заработала.

А что касается объема рынка, мне видится, что сектора, регулируемого Федеральными законами № 44-ФЗ и № 223-ФЗ, вполне достаточно, чтобы рынок «схватился».

В то же время нужно понимать, что тот бюджет, который обозначен в качестве поддержки электронной промышленности, недостаточен, чтобы сделать абсолютно всё. Поэтому нужна приоретизация.

Может быть, у меня некоторая профессиональная деформация, но мне кажется, что вперед нужно пропустить те вещи, которые входят в контур критической инфраструктуры и закрывают наибольшее количество рисков. Если мы сейчас сделаем упор на аппаратные и программные средства защиты информации, то это позволит нам создать огромное

количество оборудования и закрыть множество потребностей в КИИ.

Вы уже сказали о том, что у российских дизайн-центров есть хорошие решения в области ЭКБ. Но всё же, насколько реалистично достижение обозначенной вашей ассоциацией цели – 100%-ная доля защищенной отечественной ЭКБ в оборудовании к 2024 году?

Это возможно. Абсолютно точно.

Конечно, здесь речь не идет о резисторах и конденсаторах. Мы говорим о СБИС, в первую очередь о тех, в которые можно интегрировать свой корень доверия и в которых реализуется некая логика. Это ЦПУ, коммутационные чипы...

Уже дальше встанет вопрос о памяти, ПЛИС и т. п.

Необходимо на самой ранней стадии обеспечить диалог между субъектами КИИ и промышленными консорциумами с целью формирования номенклатуры и дорожных карт импортозамещения

Мы очень последовательно отстаиваем развитие ПЛИС, потому что это крайне востребованный компонент среди разработчиков. Он гибкий, и в данной области существует множество наработок. И при этом ПЛИС у нас пока отстают.

По этому направлению мы очень плотно работаем с «ВЗПП-С» – предприятием, входящим в нашу ассоциацию.

Недавно ГК «Ростех» было подготовлено предложение по разработке комплексной научно-технической программы (КНТП) «Комплексная разработка и производство приоритетных доверенных интеллектуальных программно-аппаратных платформ на основе отечественных электронных компонентов и программного обеспечения». Планируется ли участие ассоциации в этой работе?

Еще на этапе разработки данной программы мы принимали достаточно активное участие в этом.

Мы предлагали такую программу еще примерно два года назад. Первые наброски мы делали вместе с ИСП РАН. Затем, около полугода назад, эта работа была структурирована в виде пяти ключевых направлений, первое из которых сосредоточено на фундаментальных исследованиях, а остальные четыре посвящены базовым технологиям ЭКБ, ПО, аппаратно-программных платформ и комплексов. Сейчас по каждому из них уже созданы экспертные советы.

Основная задача КНТП – обеспечить связь между академическими работами, которые у нас в основном относятся к Минобрнауки России, и промышленностью, то есть с деятельностью Минпромторга России. Думаю, нам надо еще поработать, чтобы эта взаимосвязь стала прямой и эффективной. Нам потребовалось три года, чтобы построить рабочую кооперацию между дизайн-центрами, поставщиками оборудования и программных платформ. Теперь необходимо включить в эту цепочку академические институты. При этом желательно избежать соблазна изобрести велосипед.

Что вы назвали бы главным препятствием для реализации обозначенных планов, обеспечения КИИ российскими доверенными решениями на отечественной ЭКБ?

Объективных препятствий нет. У нас имеется множество наработок, по многим направлениям достигнут паритет с зарубежными решениями. Препятствия могут возникать только из-за нежелания потребителей переходить на отечественные решения.

Так, сейчас на стадии обсуждения готовящийся Указ Президента РФ по переходу на преимущественное использование российского аппаратно-программного обеспечения в КИИ. Вокруг него развернулась настоящая битва: многие субъекты КИИ утверждают, что они к этому не готовы и не будут готовы в течение ближайших 5–10 лет.

Мы направили в Министерство цифрового развития, связи и массовых коммуникаций РФ наши предложения, в частности – придать первоочередной приоритет и ограничить целевые сроки импортозамещения средств защиты информации, которые являются основным барьером на пути злоумышленников. Необходимо подойти дифференцированно к теме импортозамещения программного и аппаратного обеспечения. А самое важное – на самой ранней стадии необходимо обеспечить диалог между субъектами КИИ и промышленными консорциумами с целью формирования номенклатуры и дорожных карт импортозамещения. Это позволит нам всем сосредоточить усилия отечественных производителей программного и аппаратного обеспечения на первоочередных нуждах российской критической информационной инфраструктуры.

Спасибо за интересный рассказ.

С А. И. Тихоновым беседовал Ю. С. Ковалевский.
Фото: О. Ф. Слепян

МЕЖДУНАРОДНЫЙ ВОЕННО-МОРСКОЙ САЛОН

INTERNATIONAL MARITIME DEFENCE SHOW

Организатор:

МИНПРОМТОРГ РОССИИ

При участии:

Министерство обороны

Министерство иностранных дел

Федеральная служба по военно-техническому сотрудничеству

Администрация Санкт-Петербурга

РОСОБОРОНЭКСПОРТ

IMDS 2021

23-27 июня

РОССИЯ

Санкт-Петербург

Устроитель:

ООО «Морской Салон»

www.navalshow.ru

"Через сотрудничество – к миру и прогрессу!"