Кому нужна электронная индустрия?

Алексей Галицын (a.a.galitsyn@gmail.com),
Андрей Железнов (zhelandr@mail.ru)

В статье рассматриваются различные аспекты безопасности России перед лицом экономических санкций со стороны ведущих мировых экономик. Обосновывается необходимость срочного обеспечения технологической независимости в ключевых направлениях развития микроэлектроники, телекоммуникаций, а также в сфере финансов.

Введение

Данная статья основана исключительно на проверенных с точки зрения Закона РФ № 538-ФЗ фактах, которые авторы могут подтвердить документально, и является последней из серии статей [1–6] коллектива авторов Консорциума «Физико-техническая корпорация», все проекты которого были отвергнуты Департаментом радиоэлектронной промышленности (ДРЭП) Минпромторга РФ. Что характерно, именно этот департамент несёт ответственность за импортозамещение, осуществляемое в целях безопасности электронного оборудования государства. В этой связи нам хотелось бы обратить внимание чиновников ДРЭП Минпромторга РФ, создающих крючкотворные законы о «балльной» оценке «отечественности» электронного оборудования, на то, что безопасность электронной техники – это не диссертация по экономике, безопасность не измеряется в процентах – она или есть, или её просто нет! А вот «безнадёжность» сложных, причём невосстанавливаемых электронных устройств (то есть вероятность их отказа: $Q(t) = 1 - P(t)$, где $P(t)$ – вероятность безотказной работы устройства) будет практически обратно пропорциональна произведению вероятностей $P_i(t)<1$ безотказной работы всех (n) его отечественных компонент: $P(t)= P_1(t)\times P_2(t)\times...\times P_n(t)$. Именно так, с гарантированной государством (при отсутствии конкуренции Pi=0,9) вероятностью отказа Q=0,999974, «погиб» ремонтопригодный советский гражданский автопром (при P_i=0,9 и n=100 $Q=1-0{,}9^{100} = 0{,}999974$).

Чтобы напомнить читателям, о чём, собственно, шла речь в отвергнутых Департаментом проектах, перечислим некоторые из них:

1. «Зонт» от сверхманёвренного гиперзвука» позволил бы создать реальную защиту от сверхманёвренного гиперзвукового оружия и сделать российское сверхманёвренное гипероружие (простой заменой электронного блока!) на порядок более точным;
2. «Настольная» ядерная энергетика» позволила бы сделать холодный ядерный синтез «настольным», а ионные двигатели – компактными;
3. «Интернет Вещей Будущего» – спасти и вывести на мировой рынок полупроводниковую индустрию страны, открыв ей (за счёт интеллектуальных преимуществ) мировой рынок Интернета Вещей (IoT) (рынок $7,0...10,0 трлн/год, четверть бюджета США);
4. «Российская рентгенолитография и РФА-спектрометрия»: первая – создать рентгенолитографию с кратно большей радиационной светосилой пучков наноразмерной ширины, вторая – обеспечить чувствительность рентгенофлуоресцентного анализа (РФА) на уровне масс-спектроскопических и атомно-абсорбционных методов анализа при себестоимости на порядок меньшей;
5. «Невидимая» и «неубиваемая» военная радиосвязь взамен смертоносной (для собственной армии) «китайской» радиосвязи – дать армии массовую дешёвую развед- и помехозащищённую радиосвязь, принципиально недоступную для кибератак и обладающую уникальной живучестью;
6. «Цифровая трансформация предприятий» – создать технологическую платформу интернет-коммуникаций повышенного качества («сеть поверх сети», в том числе сервис IP-TV и защищённая телефония) на базе сетевой технологии «IPv17» с ассоциативной маршрутизацией, гарантированной доставкой пакетов и исключением возможности организации дестабилизирующих воздействий на сетевую инфраструктуру;
7. «Аппаратная криптозащита киберсистем» – на недоступном для конкурентов уровне защитить информационные ресурсы, национальную цифровую валюту (см. далее), киберфизические системы, критическую инфраструктуру, а также осуществлять сертификацию и защиту товарного рынка при помощи криптосредств нового типа.

На основе именно таких проектов, базирующихся на так называемых «предельных технологиях» – технологиях, обладающих новыми качествами и опережающих современные научные достижения в своей области (в которых получается то, что считается невозможным), и должно давным-давно начаться возрождение новой полупроводниковой индустрии страны (загрузка полупроводниковых фабрик и рентабельное производство массовой конкурентоспособной продукции даже на отсталой технологической базе), а главное, создание и загрузка десятков дизайн-центров целенаправленным проектированием на кристаллах качественно новых криптосистем, электронных финансов, систем управления, систем телекоммуникаций, телефонии и связи для гражданских и военных применений.

Впрочем, сейчас об экономике электронной индустрии даже и вопрос не стоит – электронную индустрию надо просто спасать любой ценой и расплачиваться за 30 лет реального физического уничтожения отрасли, продукция которой (пока) априори неконкурентоспособна, но жизненно необходима для будущего страны, что наглядно показано в настоящей статье.

К сожалению, по этому вопросу у разных людей существуют совершенно разные и даже диаметрально противоположные мнения. Существует, например, суждение «в народе», что микроэлектронная индустрия в России погибла навсегда, восстановить её невозможно, а возрождать бессмысленно, ведь у народа и так есть и смартфоны, и телевизоры, и компьютеры.

Есть и суждение, что теперь у всех технических специалистов страны и у всех российских учёных в области микроэлектроники одномоментно изменилось сознание, и что они в результате этого «за

год» наверстают наше 30-летнее отставание от мировой цивилизации [7], при том что от электронных технологий (Cadence, Synopsys, Agilent, TSMC и SoC-комплектующих, etc.) российских разработчиков теперь, скорее всего, просто-напросто отключат [8-10].

Авторы уверены: чтобы публиковать оценочные суждения по тому или иному предмету, надо иметь и профессиональные знания в обсуждаемой предметной области, и моральное право на это (иначе люди будут считать тебя, мягко говоря, «чудаком»). Существует, например, суждение о «шпионских закладках» в «чайниках и утюгах» китайского производства. Как это ни смешно для подавляющего большинства людей, такое суждение (если все правильно понимать) имеет право на существование. И далее в статье будет показано, что ничего удивительного в этом нет!

Причины, побудившие авторов написать данную статью

Так почему же и на каком таком основании авторы осмелились и не смогли не сказать публично, может быть в последний раз и хотя бы кратко, эти несколько слов правды? Да потому что, к сожалению, подавляющее большинство специалистов в области микроэлектроники – это сотрудники госструктур, вынужденные молчать под давлением своего руководства.

К сожалению, российские чиновники и раньше, и сейчас, по-видимому, недооценивают то, что электронная индустрия, в отличие, например, от гражданского автопрома, это реальное глобальное оружие, стратегически не менее серьёзное, чем атомное. Поэтому очень важно, кто-же реально им (ей) управляет.

Теперь атомное оружие – это даже не оружие сдерживания, а способ бессмысленного возмездия и, гипотетически, полного уничтожения цивилизации. А вот реальное сдерживание и удушение нашей страны будет вестись совершенно другими средствами.

Представим локальные конфликты по всему периметру России, реально поддержанные деньгами и тактическим оружием НАТО, наряду с запретом на передачу технологий, одномоментной парализацией средств связи и управления, приостановлением всех финансовых транзакций. Это то, что реально и в кратчайшие сроки может экономически и политически уничтожить Россию, сохранив для будущих победителей в целости и сохранности (в том числе от радиации) все её природные ресурсы. И это вполне реальный сценарий. И к нему уже всё готово, а первый удар в этом сражении примут на себя гражданские и военные средства управления и связи, а также электронная платёжная и финансовая системы страны.

Но главное, почему авторы были вынуждены написать эту последнюю заключительную статью (специалисты всё и без того понимают), так это потому, что в то время, когда между США и Китаем развернулась жёсткое противостояние и жестокая борьба за лидерство в области электронной индустрии и индустрии телекоммуникаций, когда абсолютно всем стало совершенно очевидно, что именно этой отраслью будет определяться лидерство в будущей мировой цивилизации, оказалось, что для российского чиновничества даже самой этой проблемы целых 30 лет не существовало, да и теперь как бы не существует. Выходит, эта проблема должна «рассосаться» как бы сама собой в мутной воде министерств и институтов развития страны.

Несколько слов об авторах данной статьи

Авторы осмелились написать эту заключительную статью на том простом основании, что несколько десятилетий тому назад научным руководителем дипломного проекта одного из них (Алексея Галицына) был самый авторитетнейший специалист отрасли, д.т.н., профессор Игорь Павлович Степаненко, заведующий кафедрой микроэлектроники МИФИ, основоположник полупроводниковой техники и микроэлектроники СССР, автор фундаментальной монографии «Основы теории транзисторов и транзисторных схем» [11](впоследствии при переиздании результаты, полученные в дипломной работе автора данной статьи, вошли в эту монографию). Научным руководителем кандидатской диссертации автора статьи был основоположник отечественной микро- и наносхемотехники [12-14], д.т.н., профессор Андрей Геннадьевич Алексенко (награждён звездой Героя Социалистического Труда за получение фотографий с поверхности планеты Венера и кометы Галлея), по инициативе которого, направленной в Политбюро ЦК КПСС, был построен город микроэлектроники Зеленоград и создано советское микроэлектронное производство.

И ещё потому, что диссертационная работа самого автора данной статьи в 1982 году была посвящена разработке программируемых в условиях эксплуатации матричных схем (FPGA или по-русски – ПЛИС). В настоящее время добрая половина электронного оборудования в мире и 90% оборудования в России проектируется именно с применением таких СБИС. К сожалению, иностранного производства – фирм Altera и Xilinx, учреждённых в США в 1984 году, а ныне гигантов мировой электронной индустрии. Только в последние годы в стране, наконец-то, появились аналоги устаревших импортных FPGA производства КТЦ «Электроника» (г. Воронеж). Также автор данной статьи участвовал в разработке первых советских микроЭВМ («Электроника-60» – полный аналог микро-ЭВМ «LSI-11» фирмы DEC), он же написал и первую в СССР техническую книгу о микропроцессорах никому в то время неизвестной фирмы Intel [15] (технический бестселлер 80-х) или, как теперь оказалось, книгу о технических основах информационной эры. Кроме того, его подписи стоят на кальках аппаратуры космического сегмента системы ГЛОНАСС, который был запущен в эксплуатацию ещё в середине 80-х, тогда как наземный сегмент страна стала создавать только в 10-х годах нового тысячелетия, навсегда потеряв при этом мировой рынок гражданских навигационных систем и неся всё это время десятки, если не сотни миллиардов рублей расходов на поддержание в рабочем состоянии спутниковой группировки, в то время как США (за GPS-приёмники) ежегодно получали сотни миллиардов долларов прибыли.

Осмелились ещё и потому, что второй автор данной статьи Андрей Железнов имеет не менее серьёзный технический бэкграунд: в своё время закончил физматшколу-интернат при МГУ им. Ломоносова; закончил МФТИ (Московский физико-технический институт), факультет управления и прикладной математики, специальность «Системы автоматического управления», кафедра «Управление и эффективность спецсистем» (стратегические и тактические системы авиационного вооружения); работал (с 3-го курса МФТИ) 10 лет в головном институте авиационных вооружений НИИАС; был (с 25 лет) руководителем группы НИИАС по исследованию и оптимизации облика стратегической крылатой ракеты Х-90, имевшей уже тогда (по данным

открытых публикаций в СМИ и книгам о гиперзвуковых системах) высоту полёта 30 000 м, скорость – 4,5...5 Махов (скоростей звука), два самонаводящихся ядерных блока.

Далее был (с 28 лет) начальником лаборатории перспективных комплексов бортового оборудования (включая пилотажно-навигационный комплекс, комплекс обороны, комплекс вооружения и др.) КБ УВЗ им. Н. И. Камова (соосные боевые вертолёты «Ка-50» «Чёрная акула», «Аллигатор» и др.), занимавшейся разработкой облика скоростного боевого перспективного вертолёта.

В 2006–2007 годах руководил разработкой и внедрением цифровых систем циркулярной связи для ЦУП (Центра управления полётами «РОСКОСМОСА» (г. Королев)). Именно эти системы обеспечивали взаимодействие операторов ЦУП при управлении МКС и другими космическими аппаратами в 2008–2020 годах.Этот человек, будучи сторонником реальных реформ, гораздо раньше, чем многие, ещё в 1989 году, смог осознать, к чему может привести перестройка при неправильном управлении экономикой, и даже лично попытался предостеречь М. С. Горбачёва и предупредить надвигающуюся на страну экономическую катастрофу. К тому времени реальные преобразования в СССР действительно назрели. И начатые Горбачёвым реформы были совершенно необходимы.Но при этом большинство ведущих экономистов СССР обосновывали целесообразность «псевдореформ» на основе вашингтонского консенсуса, в которых невидимая рука рынка должна была всё в экономике исправить и расставить по местам (и «расставила», как теперь оказалось).В 1990 году Андрей Железнов подготовил «Программу регулируемого перехода к рынку» и в 1990–1991 годах был создателем и руководителем-координатором рабочей группы, которая продвигала эту Программу [16]. Правда под рынком в ней подразумевалась конкуренция, а не «базар». Программа регулируемого перехода к рынку сделала бы СССР лидером мировой экономики.

В состав рабочей группы входили несколько генералов КГБ СССР (кстати, один из них закончил МИФИ и начинал работать в научной лаборатории Института атомной энергии им. Курчатова), несколько членов-корреспондентов АН СССР (в том числе по экономике), зам. председателя Госкомиссии СССР по реформе, начальник отдела Госплана СССР, депутат ВС СССР, доктора наук по социологии и политологии.

У группы весной 1991 года появился прямой выход на Президента СССР М. С. Горбачёва и Председателя ВС СССР А. И. Лукьянова.

8 мая 1991 года (в Кремле, в субботу, за день до Дня Победы) состоялась встреча участников группы с М. С. Горбачёвым. Это была непротокольная беседа, длившаяся 3,5 часа: 1,5 часа в диалоге с Горбачёвым был автор данной статьи, 1,5 часа – член-корреспондент РАН Львов, 0,5 часа – общая дискуссия.

Кроме членов группы присутствовали только Председатель Верховного Совета СССР А. И. Лукьянов и Президент Научно-промышленного союза СССР А. И. Вольский.

Так или иначе, программу и работу группы одобрили. В мае-июне 1991 года даже реализовали разработанные группой срочные меры, и Горбачёв не только избежал втягивания его в программу «Согласие на шанс», но и принял решение провести реальное реформирование экономики, отвергнув программы, навязанные из-за рубежа, т.е., по сути, СССР получил реальную возможность реформирования, резкого роста и усиления экономики.

Если бы не ГКЧП и его последствия, с осени 1991 года в СССР должна была реализовываться «Программа регулируемого перехода к рынку». СССР сейчас имел бы самую мощную в мире экономику и один из самых высоких в мире уровней жизни. Однако история не терпит сослагательных наклонений. СССР был разрушен.

Но вернёмся к технике. Так уж заведено, что технику создают люди, а она, в свою очередь, или защищает, или уничтожает людей. В любом случае, от качества электронной техники в итоге зависит жизнь людей, а её качество зависит от тех, кто, в каких условиях и под чьим руководством эту технику создаёт. В данной статье мы в основном будем рассматривать технические проблемы, но, увы, вынуждены будем затронуть и вопросы того, как создаётся электронная техника в нашей стране – одно без другого не бывает.

Что же можно сказать о безопасности электронных средств управления, связи и обеспечения финансовых транзакций с точки зрения их уязвимости и перспектив противостояния разного рода угрозам по оценке разработчиков радиоэлектронной аппаратуры, этих странных людей, несмотря ни на что не покинувших Родину и занимающихся «лженаукой» кибернетикой?

Безопасность электронного оборудования

Микроэлектроника развивается стремительно и непрерывно. Нравится нам или нет, но согласно Закону Мура стоимость микроэлектронных ресурсов (стоимость миллиона операций в секунду, мегабайта оперативной памяти, гигабайта долговременной памяти) соответственно непрерывно снижается: каждые 10 лет информационные ресурсы дешевеют в ... 100 (!) раз.Следовательно, если комплект «стандартного оборудования для шпионажа», например для передачи информации на пролетающий шпионский спутник, в 1980 году стоил немыслимые 1 млн долларов, то он мог стоить 10 тыс. долларов в 1990 году, 100 долларов – в 2000 году, 1 доллар – в 2010 году и... 0,01 доллара – в 2020 году.

И цена определяла «тактику» его внедрения: можно предположить, что в 1990 году оно уже было серийно встроено во все комплекты оборудования ценой 1 млн долл. (тогда речь шла уже о дополнительных электронных узлах). В 2000 году оно было, как можно предположить, встроено во все комплекты стоимостью 10 тыс. долларов (речь шла уже о «шпионских закладках», сделанных на кристалле микросхем), в 2010 году оно могло быть встроено в оборудование стоимостью 100 долларов, а в 2020 году – уже везде.

Начиная с 2000 года, «шпионский канал» активизируют только по мере необходимости, посредством передачи извне соответствующего управляющего кода. Причём можно предположить, что все «шпионские» устройства давно встроены в микроэлектронные кристаллы серийных микросхем, потому что их самих просто дешевле выпускать массово, активизируя «шпионский канал» извне по мере необходимости, а российские чиновники иногда неожиданно узнают и даже потом людям в прессе зачем-то сообщают, что ими обнаружены «шпионские закладки» в чайниках и утюгах китайского производства.

Вопрос: как можно с помощью традиционных «спецпроверок» (рентгеноскопии) и «специсследований» (контроля RF-спектра) в современных условиях обнаружить «шпионские закладки» (и даже какой в этом смысл?) при современном уровне микроэлектронных технологий и количестве серий микросхем? Тем более что акти-

визируются они и выходят на связь только по команде «сверху».

Ответ: практически никак! То же самое можно сказать и о незадекларированных возможностях сложной вычислительной техники, подключаемой к Интернету, которую тоннами закупают почти все режимные структуры. При современном уровне сложности однокристальных и других устройств, содержащих сотни миллионов транзисторов, при современном уровне сложности системного программного обеспечения обнаружить незадекларированные возможности в импортных микропроцессорах практически невозможно. И поверьте, авторы этих строк знают, о чём говорят. Это теперь даже теоретически невозможно, т.к. по уровню сложности такая задача не проще, чем заново разработать и изготовить процессор!

В плане шпионских закладок очень интересен вопрос об информационной безопасности при применении на спецсетях силовых структур импортного или российского оборудования, реально спроектированного на базе иностранных спецмикросхем связи, потенциально имеющих шпионские закладки на кристалле, более того, являющегося системной копией импортного оборудования. Оно собрано в России, но по зарубежным рекомендациям, на импортном оборудовании.К сожалению, такие случаи имеют место и совсем не редки даже в аппаратуре ФСО, и оптимизм ведомства в том плане, что сети ФСО выхода в открытые сети не имеют, не вполне оправдан, поскольку всего один шпион может поставить всю эту сеть под контроль. И касается это не только силовых структур, а всех электронных устройств и сетей так называемой критической инфраструктуры. В этой ситуации достаточно вспомнить печальную (для России) историю завербованного зарубежными спецслужбами генерал-лейтенанта ГРУ СССР Полякова, сдавшего ЦРУ целое поколение (8000 человек) советской резидентуры за рубежом.

TCP/IP и IP-телефония

Особенное удивление вызывает российская мода на использование в наземных военных и аэрокосмических системах связи и управления протоколов TCP/IP (Transmission Control Protocol – Internet Protocol), тем более что они были разработаны в DARPA (Агентство перспективных оборонных исследований) в США в 1972–1982 годах.

Эти протоколы являются идеальным средством шпионажа против России (поскольку позволяют «подготовленным» серверам дублировать и передавать любую проходящую через них информацию в любом «нужном» направлении), а системы на основе этих протоколов могут быть легко парализованы, так как в них заложена эта возможность. Как следствие, они могут «зависнуть» в любой самый неподходящий момент, в чём заинтересованы потенциальные враги России.

Тем не менее протокол TCP/IP активно используется в критической инфраструктуре. Зарубежные спецслужбы это устраивает, поскольку упрощает и удешевляет шпионаж. Да и российские коррупционеры довольны, поскольку эти протоколы можно бесплатно скачать из Интернета, сделав при этом вид, что ты заплатил за их разработку огромные деньги.

Но если вдруг неожиданно в не самый подходящий момент произойдёт потеря управления космическими аппаратами, и при этом произойдёт авария, да ещё не дай бог с гибелью людей, что тогда?

Вместе с тем сами США и Европа применяют в своих новейших авиационно-космических разработках протоколы совсем другой группы. Называется эта группа протоколов TTP (Time-Triggered Protocol).

В числе авиационно-космических изделий, на которых применили эту новую группу протоколов TTP: Global-7500; F-16; Boeing-787; A-380 и др.Более того, за рубежом этот TTP-протокол принят как стандарт протоколов для критически важных систем, это так называемый стандарт SAE AS6003.

Сейчас в России повсюду внедряется IP-телефония. Повторим, что это идеальное средство для шпионажа против России со стороны зарубежных спецслужб.

Между тем интересно, что дальность по проводам до ближайшего концентратора в IP-телефонии – 100 м (причём четыре провода специального высокочастотного сетевого кабеля). А в обычной цифровой телефонии – 5000...7000 м (причём два провода обычного телефонного кабеля). Как говорится, почувствуйте разницу!

Всё это, а главное – возможность внешнего управления «живучестью» таких сетей связи, говорит о том, что IP-телефония хороша как некое дополнительное средство, но отнюдь не как основное. При помощи IP-телефонии можно легко снять секретную информацию и транспортировать её за рубеж из любого учреждения или предприятия России, в котором она присутствует. Как снимается информация? Очень просто!

Техника «съёма» информации

Дело в том, что в современных системах цифрового кодирования речи применяется так называемый «комфортный шум». В ситуации, когда абонент молчит, возникает эффект так называемого «ватного уха». И слушающий абонент испытывает дискомфорт, поскольку постоянно думает, что связь прервалась. Чтобы этого избежать, в моменты, когда абонент молчит, в канал добавляется так называемый «комфортный шум». В то же время особенности человеческого слуха таковы, что человек не слышит шумовых помех, которые маскируются громко звучащей речью. И именно это позволяет реализовать передачу на любые расстояния снятой с объекта «секретной информации» посредством сигнала [1]. При этом в канале возникнет «псевдокомфортный шум». На фоне речи он будет незаметен, а при отсутствии речи роль его будет даже положительна (правда, не с точки зрения информационной безопасности, а с точки зрения «комфорта» слушающего). Таким образом, на фоне одного открытого разговора можно снимать и транспортировать один секретный разговор (ведущийся через АТС или в других организациях).

Обычный цифровой телекоммуникационный канал между АТС Е1 (2 Мбит/с) является носителем 30 цифровых речевых каналов. Таким образом, мы приходим к интересному выводу о том, что, имея всего один цифровой канал Е1 между АТС (а меньше не бывает, только больше), можно «увести» в сторону 30 секретных речевых каналов. Очевидно, используя нехитрые (скорее даже примитивные) цифровые методы, можно транспортировать снятую секретную информацию за рубеж или (и) в посольства зарубежных стран.

Стоит это при современном уровне развития микроэлектроники малые доли цента! Согласитесь, учитывая, что годовой бюджет зарубежных спецслужб исчисляется огромными суммами, можно ли предположить, что они не воспользовались такой очевидной копеечной возможностью? Вряд ли...

Тем временем в России процветает массовая сборка якобы собственных

цифровых АТС. Производятся они на базе зарубежных спецмикросхем связи, несомненно, содержащих на уровне кристаллов шпионские закладки. Более того, они повторяют архитектуру зарубежных цифровых систем связи (конкретно – АТС производства SIEMENS, Германия). Но при этом спроектированы-то они в России (!).

Вопрос тогда в том, а что же, собственно, спроектировано в России? – А в России спроектирован дизайн. То есть внешне АТС не похожа на импортную АТС, а внутри она вся импортная. И она уже получила сертификат информационной безопасности! И дан сертификат такой солидной структурой как ФСБ России. Опираясь на этот сертификат безопасности связи, её уже успешно внедряют во все силовые структуры! В их числе ФСБ, Министерство обороны России и др.! На самом деле, это, конечно, несомненный успех разведки, правда, не российской, а BND (немецкой разведки).

Россия на современных импортных сборочных линиях сама массово собирает цифровые АТС из зарубежных (потенциально содержащих шпионские закладки на кристалле) спецмикросхем связи, по архитектуре повторяющие известную импортную АТС, а потом сама же внедряет их в силовых и других жизненно важных структурах, например американские цифровые АТС Avaya внедрены даже в концерне воздушно-космической обороны «Алмаз-Антей».

Отказ на линии «ЮГ» Ростелекома

Зимой 1998–1999 годов в ТЦМС-22 (Территориальный центр междугородной связи 22), отвечающем за связь на направлении «ЮГ» Ростелекома (Москва, Тула, Орёл, Курск, Белгород и т.д.), один из авторов данной статьи, Андрей Железнов, вместе со специалистами его предприятия и Ростелекома проверяли, как будет работать разработанная и производимая его компанией цифровая АТС с кольцом АТС, расположенных вокруг Москвы, на тот самый не самый приятный случай. В процессе проверки специалисты ТЦМС-22 решили показать, как качественно это сделано у них на других системах. Речь зашла не об ЦАТС на «кольце», а о цифровых каналах связи, идущих на «ЮГ».

Они с гордостью показали рабочую станцию Hewlett-Packard. Показали на экране в графической форме трассу, идущую на ЮГ. Андрей Железнов посмотрел на это и задал всего один вопрос: «А кто писал эту прекрасную программу?». Они ответили: «Специалисты SIEMENS!». «Значит, специалисты SIEMENS контролируют вашу сеть лучше, чем вы, и они могут выключить её в любой момент, когда сочтут нужным?» – спросил Андрей Железнов. Специалисты ТЦМС-22 тогда подняли его на смех, сказав, что «этого не может быть, потому что этого не может быть никогда».

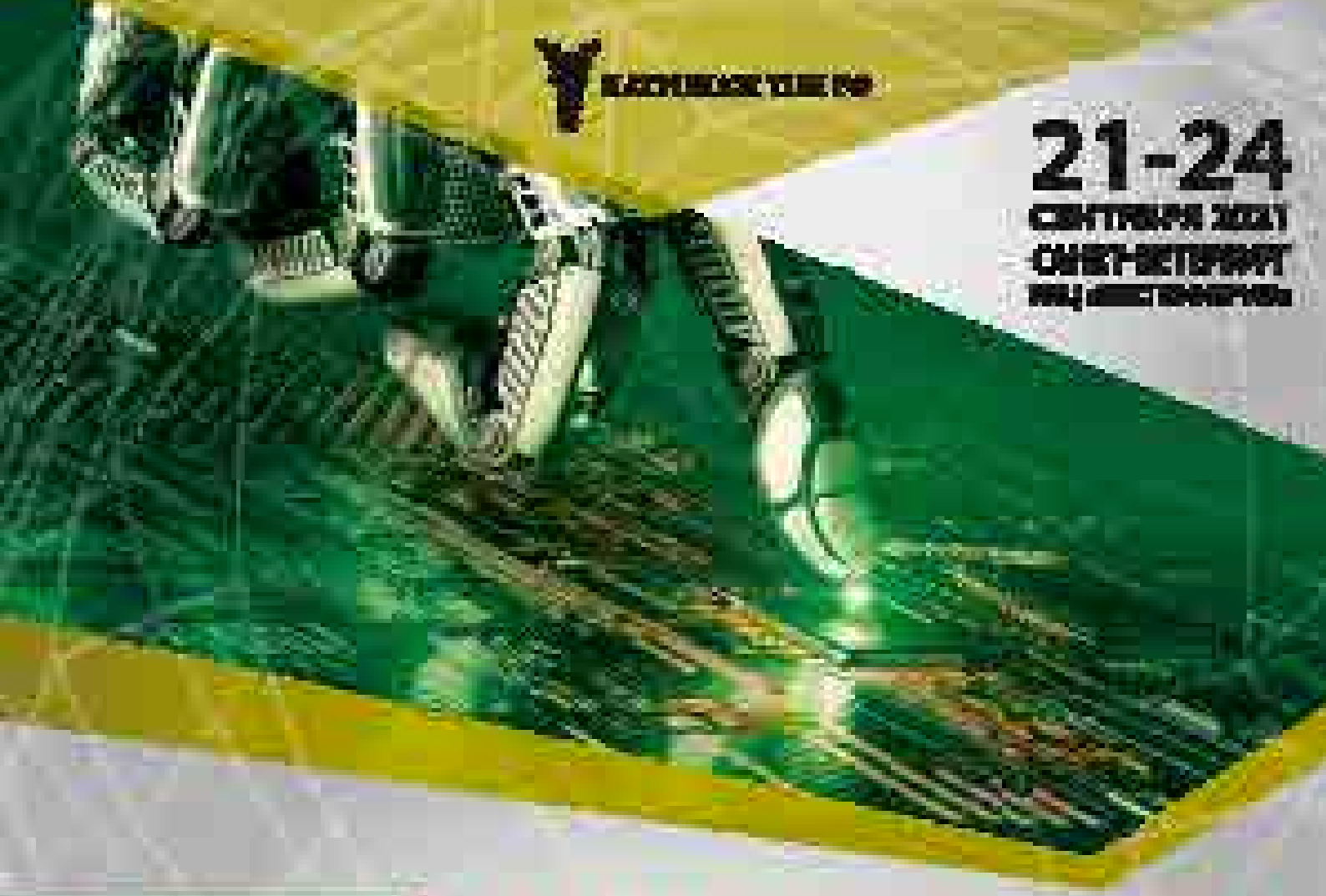
Год спустя (как раз началась 2-я чеченская война) вдруг вырубилось всё направление «ЮГ» Ростелекома. Вдруг ли? Попытки перезапустить оборудование оказались безуспешными. Попытки применить ЗИП не помогли. Призвали на помощь специалистов SIEMENS из Москвы, но и они ничего не смогли сделать. Тогда руководители Ростелекома связались с руководством SIEMENS в Мюнхене и сказали: «Сами понимаете, началась война, поэтому, если связь в ближайшее время не заработает, то руководство Ростелекома уволят (это в лучшем случае) или посадят (в худшем случае)». Руководители SIEMENS успокоили: «Всё нормально, всё будет хорошо!». И через полчаса связь заработала! Но главный и самый важный факт заключается в том, что российские специалисты не смогли восстановить связь самостоятельно!

Надо полагать, что проверка незадекларированных возможностей в оборудовании, поставленном фирмой SIEMENS, прошла успешно. «Успешно» с точки зрения немецкой разведки. Понятное дело, что Ростелеком имеет несколько глобальных линий цифровой связи («ЮГ», «СЕВЕР», «ЗАПАД», «ВОСТОК» и др.). На самом деле, по крайней мере в тот период, разные направления были сделаны на импортном оборудовании разных производителей. Правда, это распределение было довольно странным, скорее подозрительным: направление «ЮГ» построено на оборудовании немецкой SIEMENS; направление «СЕВЕР» построено на оборудовании американской AT&T; направление «ЗАПАД» построено на оборудовании французской ALCATEL; направление «ВОСТОК» построено на оборудовании японской NEC. Интересно, что это поразительно совпадает с военной активностью упомянутых стран в годы Первой мировой войны, Гражданской войны и Второй мировой войны.

Современные технологии шпионских закладок в современных цифровых АТС позволяют прослушивать телефонные разговоры и разговоры в помещениях и передавать их в штабы, расположенные на расстоянии в десятки тысяч километров. Во время войны в Ираке и Югославии связь в этих странах вообще отключили по команде извне, а ракеты на административные объекты наводились по пеленгу заранее установленных в них (закупленных их администрациями) средств радиосвязи стандарта Tetra. Кстати, а какой стандарт беспроводной связи используется российским Министерством обороны?

Несколько лет назад в США объявлено о создании кибервойск (нового рода вооружённых сил армии США, который должен вести войну в информационном пространстве) и объявлена задача: выведение из строя систем управления и связи в любой стране мира в любой необходимый момент времени. При этом было объявлено, что вся предварительная работа на территории главного потенциального противника уже проведена:

- Агентство национальной безопасности США (АНБ) (с бюджетом в несколько раз больше, чем ЦРУ) контролирует фактически все каналы телефонной связи в мире, полностью накапливает, систематизирует и анализирует все данные, циркулирующие в сети Интернет;
- Администрация Президента РФ, центральный аппарат ФСБ используют телефонную связь, базирующуюся на цифровой АТС HiCom, произведённой фирмой SIEMENS, теснейшим образом связанной с немецкой разведкой;
- большинство предприятий ракетно-космической промышленности России установили цифровые АТС DEFINI TY, произведённые американской компанией Avaya (ранее она называлась LUCENT, а ещё ранее – AT&T), которая теснейшим образом связана с ЦРУ и другими спецслужбами США;
- вся инфраструктура связи в России (сети Ростелекома и базовая сеть областных филиалов СВЯЗЬИНВЕСТА) полностью переведена на импортное оборудование;
- вся мобильная связь России поколения 5G (базовые станции и телекоммуникационное оборудование) на несколько лет вперёд законтрактована аппаратурой китайской (радует, что не американской!) компании Huawei.



21-24
СЕНТЯБРЯ 2021
САНКТ-ПЕТЕРБУРГ
ЛЕНЭКСПО

XXII МЕЖДУНАРОДНАЯ ВЫСТАВКА

РАДИОЭЛЕКТРОНИКА & ПРИБОРОСТРОЕНИЕ

- ЭЛЕКТРОННЫЕ КОМПОНЕНТЫ И КОММУТИРУЮЩИЕ
- ПЕЧАТНЫЕ ПЛАТЫ И ДРУГИЕ НОСИТЕЛИ СХЕМ
- СВЕТОДИОДНЫЕ ТЕХНОЛОГИИ
- РАЗРАБОТКА И ПРОИЗВОДСТВО ЭЛЕКТРОННЫХ УСТРОЙСТВ
- РОБОТОТЕХНИКА
- КОНСТРУКТИВЫ
- МАТЕРИАЛЫ
- ТЕХНОЛОГИИ
- ПРОМЫШЛЕННОЕ ОБОРУДОВАНИЕ И ИНСТРУМЕНТЫ
- КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И ЛАБОРАТОРНОЕ ОБОРУДОВАНИЕ

Может быть, в Администрации Президента РФ, Совете безопасности РФ, Минобороны РФ, ФСБ РФ, Военно-промышленной комиссии просто не знают об этом?

Безопасность микропроцессоров

В годы застоя в СССР был запущен грандиозный проект «ЕС-ЭВМ» («Единая система ЭВМ», копия семейства ЭВМ IBM-360/370, фирма IBM, США). Ради этого огромного проекта – «ЕС-ЭВМ» – в СССР прекратили, а по сути «убили» (вместо того, чтобы воспроизвести в интегральном исполнении), дальнейшее развитие советских ЭВМ семейства БЭСМ, вполне классных машин с массой наработанного собственного серьёзного программного обеспечения (включая системы трассировки 20-слойных печатных плат, разработки и трассировки матричных СБИС, моделирование разного рода процессов и т.п.). И это была самая крупная и (по мнению авторов) самая успешная экономическая диверсия против СССР, сравнимая по своим экономическим и историческим последствиям разве что с «антиалкогольной компанией» М. С. Горбачёва.Затем в СССР решили развивать «СМ-ЭВМ» («Серия малых ЭВМ», копий семейства PDP-11/70 фирмы DEC, США). Хотя разработчикам вычислительной техники уже было понятно, что, как только ты начинаешь копировать что-либо, ты заведомо обрекаешь себя на отставание, и хорошо, если на годы, а не навсегда, т.к. развивать чужие системы невозможно, а потому бессмысленно! Безответственность и тупость чиновников (которых отбирали из неудавшихся инженеров) привели к тому, что в СССР тогда было выработано ошибочное решение о том, что все перспективные бортовые вычислители (включая работающие в режиме реального времени (!) бортовые вычислители боевых самолётов и ракет) должны были быть программно совместимыми с СМ-4 (медлительная микропоследовательностная машина, в которой каждая команда выполняется посредством выполнения десятков микрокоманд). Под эту, «благородную» на первый взгляд, идею «единения», «зарезали» фактически все собственные перспективные разработки Минэлектронпрома СССР, который как раз в это время начинал выпуск микроЭВМ «Электроника НЦ-80», фактически не уступавшей американским. У неё, правда, был один очевидный «недостаток»: она была самостоятельной отечественной разработкой.

Получилось всё это в виду недооценки руководством СССР (но не специалистами! [12-15]) роли микроэлектроники и микропроцессорной техники для страны в целом (о кибербезопасности тогда вообще никто не задумывался), отсутствия единого центра координации работ в области микропроцессорной техники и её программного обеспечения, отраслевого «разделения труда», ведомственной раздробленности заказчиков, стремления одних министерств развиваться за счёт других и постоянных «оглядок власти на Запад». Но главное, потому что в то время большинство тем Минэлектронпрома (производившего микросхемы и транзисторы) финансировалось на вторичной основе. Тогда деньги выделялись первично профильным министерствам (Минавиапрому, Минобщемашу, Минрадиопрому, Минпромсвязи и т.д.), а уже потом эти ведомства, если считали нужным (!), выделяли часть из этих средств Минэлектронпрому, который по их заказу делал то, что им нужно.

А в США тем временем не «клали все яйца в одну корзину», а работали системно, развивая конкуренцию. Так, на рынке ЭВМ все эти годы работали следующие фирмы: в области ЭВМ для автоматизации медленно текущих операций работала DEC; в области ЭВМ для финансовых операций конкурировали IBM и NCR; в области ЭВМ для реального времени – Hewlett-Packard и Perkin Elmer; в области суперЭВМ – Cray, Control Data и Convex; в области рабочих станций – Hewlett-Packard и Silicon Graphics; в области персональных ЭВМ – IBM и Apple и т.д.Зато в СССР в области ЭВМ и большинства других изделий электроники конкуренции не было. Только вот сам СССР «почему-то» развалился.

Но вернёмся в современную российскую реальность. Изготовить отечественный микропроцессор теперь можно, но только за рубежом (fablessпроизводство, и то «до поры – до времени»), т.к. собственная микроэлектронная промышленность России разрушена. То, что есть, устарело. В лучшем случае мы имеем устаревшие импортные производственные линии. Производить микропроцессоры современного уровня сложности на них не только не рентабельно, а просто физически невозможно. Все расходные материалы этих линий импортные. А если нам перестанут их поставлять?

Вся обеспечивающая подотрасль для микроэлектроники тоже разрушена, её не существует!

Ещё одним «проколом» как отечественных (в том числе и авторов данной статьи), так и зарубежных разработчиков первых микропроцессоров было то, что они не могли даже предположить, что кто-нибудь когда-нибудь покусится на их детища и помимо их воли и воли пользователей начнёт запускать в микропроцессорные системы вирусы и прочие злонамеренные программы. В то время разработчики честно боролись за повышение производительности, снижение себестоимости, а решение всех проблем, связанных с безопасностью кибернетических систем, было (ошибочно, как теперь оказалось!) отдано на откуп программистам.Как результат, теперь мы имеем то, что имеем: весь мир неустанно борется с вирусами и киберпреступностью, а сама она превратилась в ужасную напасть для одних и в отдельную прибыльную отрасль техники, сделавшую долларовыми мультимиллиардерами других.

Тем не менее (даже значительно позднее, уже понимая весь драматизм ситуации по части кибербезопасности) весь мир упорно шёл проторённым, консервативным путём. Максимум, на что программисты (и то в целях самосохранения) поначалу «разрешили» пойти разработчикам классических зарубежных микропроцессоров, так это на введение NX-бита страниц памяти для борьбы с вредоносными программами (аналогичные, но значительно более глубоко продуманные комплексные средства защиты есть в процессорах «Эльбрус») [17].

В простейшем случае NX – атрибут страницы памяти (NX-бит: от англ. no execute – запрет исполнения кода на странице) в архитектурах x86 и x86-64 был добавлен для защиты системы от ошибок в непрофессионально написанных программах и от использующих эти ошибки вирусов, троянских коней и прочих вредоносных программ. А добавлен он был только потому, что для программистов это было просто «чёрной дырой» в безопасности программного обеспечения: ведь организация злоумышленниками преднамеренного переполнения программного стека в непрофессионально написанных программах с последующей передачей

управления в не предназначенную для исполняемых команд область памяти была классическим и самым массовым способом передачи управления вредоносным программам, в результате чего злоумышленники получали контроль над уязвимой системой.

Поскольку в современных компьютерных системах память разделяется на страницы, имеющие определённые атрибуты, разработчики процессоров добавили ещё один атрибут, обеспечивающий запрет исполнения кода на странице: такая страница может быть использована для хранения данных, но не программного кода. При попытке злоумышленников передать управление на страницу с запретом исполнения программного кода будет инициировано прерывание, ОС получит управление и завершит выполнение «подозрительной» программы. Смешно сказать, но на этой «ерунде» возникла целая индустрия киберпреступности и (соответственно) индустрия кибербезопасности.

К сожалению, и теперь, и тем более в будущем (после создания компиляторов, операционных систем и наработки колоссального количества прикладного программного обеспечения для стандартных архитектур) достаточно сложно внедрять в вычислительные системы, казалось бы, очевидные, простые, но требующие и аппаратной, и программной поддержки элементы безопасности, такие как защищённый прямой доступ к памяти с шифрованием данных для критически важных функций, защищённая загрузка и защищённое обновление кода, контроль доступа к защищённым ресурсам, аутентификация сеансов, защита наборов инструкций, на которые не должны выполняться переходы при ветвлениях, сохранение функции адреса возврата в отдельном «теневом» стеке после передачи управления и извлечение его перед выходом из функции, поддержка встроенного в накопитель оборудования inline-шифрования (Inline Encryption), осуществляющего прозрачное шифрование и расшифровку на основе заданных ключей и алгоритмов шифрования при вводе/выводе информации с дисков и т.д, и т.п.

Многое в части кибербезопасности, конечно, делается уже сейчас, причём максимальная эффективность защиты достигается как раз там и тогда, когда разработчики имеют как возможность модернизировать вычислительную систему на структурном уровне процессоров (модифицировать сам кристалл), так и возможность модифицировать (а зачастую создавать заново) её системное (OS, компиляторы) программное обеспечение.Например, в микропроцессорах «Эльбрус» уже используются защищённые вычисления, основанные на контекстной защите памяти на базе тегированной архитектуры, обеспечивающей стойкость к компьютерным вирусам и быструю отладку программ, а аппаратно поддерживаемая двоичная компиляция обеспечивает совместимость этой системы с другими платформами на уровне исполняемых кодов.

Для реализации всего этого потребовалась определённая поддержка и со стороны аппаратуры, операционной системы, и со стороны систем языкового программирования: компиляторов, редакторов связей, отладчиков. Предложенная разработчиками реализация обеспечивает полную и эффективную модульную защиту программного обеспечения (поддержанную аппаратурой и компилятором) и может служить основой для защиты системы от компьютерных вирусов, а достичь этого (а также обеспечить возможность дальнейшего развития этой «экосистемы») оказалось возможным исключительно благодаря тому, что и идеология, и архитектура, и структура микропроцессора, и его программное обеспечение (OS, компиляторы, компоновщики, загрузчики, отладчики) изначально разрабатывались в России, причём как всегда за копейки и «не благодаря, а вопреки». И всей этой истории около 50 лет.

Защита передаваемой информации

При передаче информации через открытые, незащищённые передающие среды важное значение приобретает её криптокодирование. Основной задачей криптографии является шифрование информации у источника её происхождения и дешифрования её в приёмнике при помощи ключей шифрования (не путать с квантовой «криптографией», используемой на волоконно-оптических линиях связи, которая не шифрует информацию, а делает её просто физически принципиально недоступной именно для несанкционированного «съёма»).

Формирование, распределение и защита от компрометации ключей осуществляется по-разному, в зависимости от области применения, среды передачи и класса проектируемых систем: системы массового обслуживания, спецсистемы и т.п. При передаче через незащищённую среду по открытым каналам связи любую информацию (текстовую, цифровую и т.п.) сначала преобразуют в двоичный поток бит, затем шифруют его (по тем или иным алгоритмам шифрования) двоичным кодом (ключом шифрования), передают зашифрованный двоичный поток по каналам связи, принимают и дешифруют этот поток при помощи двоичных же кодов (ключей дешифрования) с помощью соответствующих алгоритмов дешифрования, а затем восстанавливают исходную информацию в текстовом, цифровом или ином виде.

В системах массового обслуживания, передающих информацию через открытые (широковещательные) среды, совершенно отдельными проблемами являются передача (распределение) открытых ключей корреспондентам, принимающим зашифрованный поток информации, и формирование ими (на основе этих открытых ключей) ключей закрытых, при помощи которых осуществляется дешифрование цифрового потока на принимающей стороне, а также проблема защиты передаваемых ключей от компрометации [18].

Сам процесс шифрования и дешифрования осуществляется посредством примитивных логических операций в двоичном формате, над двоичной информацией, с использованием двоичных ключей, но для реализации криптоалгоритмов и алгоритмов работы с ключами (вычисление, аутентификация, верификация, генерация, распределение ключей, защита их от компрометации и т.п.) в настоящее время используют весьма сложные алгоритмы и весьма ресурсоёмкую процессорную «десятичную арифметику». Но разве не странно тратить вычислительные ресурсы и время на переход из одной системы счисления в другую и использовать ресурсоёмкие вычислительные процедуры в десятичной системе счисления, когда всё это можно сделать аппаратно (т.е. на несколько порядков быстрее) в двоичной системе на уровне булевых функций и двоичной арифметики?

Современные достижения в области дискретной стохастической криптографии позволяют создавать криптографические технологии совершенно нового типа, аппаратно (без потерь на про-

цессорную десятичную арифметику), в реальном масштабе времени решающие криптографические задачи на качественно новом техническом уровне и обеспечивающие информационную безопасность без снижения производительности компьютерных систем, что крайне актуально для обеспечения, а также ликвидации и в настоящем, и в будущем отставания технологий обеспечения безопасности от современного уровня развития техники. И такие технологии в стране есть.

Данные технологии, уничтоженные, помимо прочих [1-6], Департаментом радиоэлектронной промышленности Минпромторга РФ, могли бы обеспечить не только надёжный, эффективный и единый, универсальный (криптографического уровня стойкости) безбумажный и бесконтактный подход к маркировке, идентификации и сертификации товарной продукции во всех отраслях производства, что позволило бы не только обеспечить защиту товарного рынка и всех (!) сегментов экономики от контрафактной, фальсифицированной и недоброкачественной продукции, но и обеспечить загрузку полупроводниковых фабрик страны социально значимой продукцией, что, кстати, в своё время было принудительно сделано в Китае для подъёма его полупроводниковой индустрии.

При этом рутинный и малоэффективный «бумажный» ведомственный контроль за маркировкой и сертификацией товарной продукции был бы заменён эффективным электронным гражданским контролем, а взаимодействие средств электронной маркировки продукции со средствами электронного гражданского и государственного контроля за её качеством и продажей (реализацией) осуществлялось бы бесконтактно, радиочастотным способом. Помимо этого, возможно последующее масштабное распространение этой универсальной технологии на задачи защиты (с криптографическим уровнем стойкости) национальной цифровой криптовалюты, удостоверяющих документов, а также на другие приложения в сфере обеспечения безопасности как физических объектов, так и (что не менее, а даже более важно) информационных процессов.

Подобные технологии позволяют осуществлять на недоступном для конкурентов уровне решение огромного комплекса производственных, экономических и социальных задач: обеспечить вывод на качественно новый уровень безопасности цифровой техники и киберфизических систем, в первую очередь – устройств с дефицитом аппаратных ресурсов, где другие способы защиты просто неприменимы.

Выводы

Нет сомнений, что несмотря на все организационные (часто выдуманные чиновниками) и реальные технические трудности и аппаратная дискретная стохастическая криптография, и программно-аппаратные (реализованные на структурном уровне организации процессоров и компиляторов) средства противодействия киберугрозам постепенно внедряются и рано или поздно всё же будут внедрены в технику будущего во всём мире и позволят вычислительным комплексам и системам, поддерживающим безопасность не только на программном, но и на структурном и архитектурном уровнях, эффективно защититься от вредоносных программ и прочих киберугроз, создаваемых хакерами и киберпреступниками.

Другой вопрос: как защититься от закладок и незадекларированных возможностей потенциального противника, закупая у него технологии и электронное оборудование, с учётом усложнения всей этой техники с годами? Ведь по мере усложнения электронной техники (100-кратное усложнение каждые 10 лет) эта проблема будет только усугубляться и усугубляться, став в скором времени не только неразрешимой, но и необратимой. Существовать (что нам пока ещё разрешают США) на импортной технике стране ещё можно, а вот развивать саму эту технику – уже нет: это не только архисложно, но и бессмысленно, потому что бесперспективно. Как научиться её использовать, блокируя заложенные противником незадекларированные возможности и «шпионские закладки», да ещё не зная, кто из нынешних торговых партнёров (США или Китай) в будущем будет более опасен для России? По-видимому, никак!

Защититься от иностранного вмешательства в работу киберсистем в час «Ч» можно, только используя собственные процессоры (причём без использования в них чужих IP-блоков), собственные криптосистемы, собственные средства безопасности и собственные программные средства, «совместимые» с зарубежными разве что на уровне файловых систем, а также синтаксиса и семантики языков высокого уровня.

Электронные финансы – новый стимул развития российской электронной индустрии

При немыслимом (сотни триллионов долларов) размере внутреннего и внешнего госдолга США, во время пандемии их «печатный станок» вновь заработал и начал печатать новые доллары триллионами в месяц и «надувать» ими уже не какие-нибудь «доткомы» или «ипотеку», а свой последний (ничего другого уже не существует) оплот – финансовый сектор (попутно наводняя и мировой финансовый рынок «резаной зелёной бумагой»), что свидетельствует о неизбежности суверенного дефолта доллара (а соответственно, и резервных валют) в ближайшем обозримом будущем и перехода Человечества на новые, именно цифровые валюты (цифровой доллар, цифровой юань и т.п.), что сейчас уже является велением времени (технически апробировано на криптовалютах) и к чему и США, и Китай (в отличие от России) технологически уже готовы (у них есть системы-прототипы на уровне группы крупнейших банков).

И если раньше ЦБ России «не было позволено» даже думать о цифровых валютах, то в нынешней преддефолтной ситуации как с долларом, так и с самой государственностью США наличие хотя бы прототипа собственной национальной цифровой валюты – это уже вопрос жизни и смерти для России как государства. Но при этом следует понимать, что самое важное качество любой валюты – это её технологическая защищённость, причём как на данный момент, так и на исторически обозримую перспективу (!). Ведь в основном именно по этому признаку будет выбираться будущая мировая цифровая валюта.

Поскольку электронные криптоденьги намного эффективнее обычных выполняют роль универсального средства обращения (и не только его!), потребность экономики в них столь высока, что участники сферы обращения готовы были принять даже столь сомнительное средство, как Bitcoin. Но так как все существующие криптовалюты выполняют все пять функций «денег Маркса» (включая накопление капитала), то они обладают одинаковыми недостатками и имеют одинаковый печальный исход – нулификацию, т.е. финансовый крах. Но главным недостатком существующих криптовалют является отсутствие персонифициро-

ванного эмитента, что даже в будущем не позволит осуществлять целенаправленную эмиссию цифровых денег ни владельцам мировых валют, ни владельцам валют национальных, т.е. осуществлять ими осознанное и целенаправленное управление экономикой.

Такие возможности может предоставить стране национальная (государственная) цифровая валюта, технологический прототип которой обязательно должен быть создан и в России на случай дефолта доллара и резервных валют, на случай резкого ужесточения санкций (например, отключения транзакций SWIFT, VIZA, MasterCard и т.п.) или разрыва тех или иных международных договоров по независящим от России причинам.

Ведь в ту секунду (в тот день и час «Ч»), когда доллар да и все прочие фиатные валюты «вдруг» перестанут существовать (суверенный дефолт), главный «эмитент» мировых фиатных валют сможет защититься от владельцев валют с помощью военной силы, т.е. ракет (не потому ли отменен ДРСМД?), флота (не потому ли, казалось бы, бессмысленный американский флот по численности превосходит все остальные?) и кибервойск (а не для этого ли США и нужны кибервойска?).

Но что делать остальным странам, когда годом раньше или годом позже, но дефолт доллара все же произойдёт? Слишком огромен (приближается к триллиарду долларов) и несопоставим с размерами реальной экономики этот пузырь американского (и мирового) финансового рынка, и неизвестно, по какой именно причине и в какой момент он лопнет, и активы из финансового сектора экономики вдруг «низвергнутся» в реальный сектор и «затопят» его – слишком много в мире накопилось внутренних и межгосударственных противоречий. Не хотелось бы быть пророком, но, с грустью вспоминая анекдот про «коммунизм» и «Олимпиаду-80», мы опасаемся, как бы вместо ранее объявленной Зимней Олимпиады 2022 года в Пекине, в Китае не случился «коммунизм»: глобальный дефолт доллара, евро и других валют, т.е. «крах капитализма».

Во время глобального дефолта экономически одномоментно проиграют все (огромный финансовый пузырь лопнет, все «долги» будут списаны, коммерческие банки рухнут, накопленная населением «резанная зелёная бумага» аннулирована), и мир начнёт жизнь с «чистого листа».Но те (страны), чья экономика устоит, а технология государственных электронных финансов окажется прочнее, они и выйдут победителями из этой схватки и станут владельцами всех денег мира. После этого у победителя на мировой арене уже не будет никаких конкурентов долгие столетия, а вот остальные страны (проигравшие) будут вынуждены использовать финансовые технологии победителей, т.е. де факто станут их колониями, и история повторится сначала.

Как развивать экономику национальных государств «с нуля» (или не «с нуля»), «до дефолта» (или «после»), если каждое из них начнёт создавать свою национальную цифровую валюту и даже получит возможность «печатать» её в неограниченных количествах (пропорционально потребностям экономики)? Как вводить такие цифровые деньги в хозяйственный оборот?

В условиях открытой экономики, т.е. свободного обмена всех (в том числе и цифровых) валют и трансграничного движения капитала, все вброшенные, но невостребованные пустые «фантики» (в обмен на ресурсы) мгновенно «превратятся» в валюты более успешных и сильных государств, произойдёт очередной виток инфляции, рынок слабых стран заполнится дешёвыми иностранными товарами из более развитых государств, что дестабилизирует производство стран отсталых и замедлит рост их экономики. Опять всё пойдёт по тому же кругу: начнут развиваться сильные страны и эксплуатировать слабых. Всё это пройдено всеми и уже не раз.

Таким образом, мы приходим к выводу, что всё вернётся просто к аннулированию финансовых пузырей, законных и незаконных накоплений населения, переоценке ценностей и возвращению к основе основ – реальному производству. Так какой, спрашивается, смысл ждать глобального дефолта, очередного разрушения производства и как разорвать этот замкнутый круг?

Единственное разумное решение в данной ситуации (когда «невидимая рука рынка» явно уже с ней не справилась!) это заблаговременно, одновременно с переходом на национальную цифровую валюту встать на новый инвестиционный путь развития. Но инвестиционный совсем не в том упрощённом смысле, в котором его понимают финансисты и банкиры: «Вот вам деньги – вернёте в тройном размере, а ещё будете платить ренту... всю оставшуюся жизнь!».

Каким предлагается сделать российский цифровой рубль

Автор «финансового» раздела данной статьи (Алексей Галицын) заранее извиняется перед ЦБ РФ и Минфином за свою финансовую необразованность, а также за посягательство на святая святых –американский доллар и российский рубль. Но, видимо, время пришло и уже пора что-то делать, т.к. техническая подготовка к введению официальной национальной (государственной) цифровой валюты требует времени, но позволит России в критический момент, момент мировой паники, в час «Ч», когда произойдёт суверенный дефолт доллара и «вдруг» окажется, что под ним нет никакого обеспечения, а все финансовые транзакции (SWIFT, VIZA, MasterCard e.t.c.) будут остановлены, мгновенно запустить двух- или даже трёхконтурную систему электронного денежного обращения в стране.

К примеру, в СССР за две пятилетки мобилизационной экономики и индустриализации (по сути, подготовивших страну к Великой Отечественной войне) безо всяких там инвестиций было построено более 9000 (!) заводов, и не в последнюю очередь – благодаря введению в стране двухконтурной системы обращения. Да и сразу после войны (даже под угрозой ядерного нападения) СССР не поддался ни на какие уловки ФРС (в плане суверенитета советского рубля).

Тем не менее эмитируемые государством безналичные деньги обеспечивали развитие страны (фактически это было осознанное целенаправленное инвестирование), независимое от рыночного спроса-предложения. Наличные же деньги обеспечивали рыночные операции, а золото и валюта – внешнеторговые. Наличные и безналичные деньги были взаимно неконвертируемы: безналичными нельзя было дать взятку, а инфляции (без «ссудного процента») не могло быть в принципе.

Смысл нового государственного инвестирования в России должен заключаться в том, что эмиссия денег государством (вся или частично) должна осуществляться в развитие страны, а деньги должны вкладываться именно в это развитие посредством инвестирования цифровых денег (в трёх разных контурах) в перспективные инвестиционные (инновационные) проекты, создающие новые реальные ценности,

востребованные промышленностью и населением.

Причём инвестируемые цифровые деньги, будучи эффективным средством обращения, некоторое время (год, два, три) после их эмиссии не должны быть средством накопления, а должны стать средством, стимулирующим товарообмен, в цифровой форме это сделать достаточно просто. Таким средством и должен стать инвестиционный «российский цифровой рубль».

Формула российского цифрового рубля

Даже сейчас, соблюдая все «законы МВФ» (как это делает «законопослушный» Китай), т.е. вплоть до дефолта доллара, не увеличивая «незаконно» рублёвую денежную массу, а просто последовательно замещая «старые рубли» новыми «цифровыми рублями» (а после глобального дефолта денежную массу цифровых рублей можно будет в тот же день и увеличить... «сталинским» методом), можно и сейчас вводить в оборот «цифровой рубль». Более того, нужно обязательно убрать «функцию накопления» у распределяемых целевым образом, эмитируемых (инвестируемых – в указанном выше смысле слова) государством («бюджетных») цифровых денег «квазибезналичного контура» посредством введения по ним «отрицательной электронной» процентной ставки, что резко увеличит оборот денег и товаров (ускорит продвижение товаров) и кратно (что давно доказано) ускорит экономическое развитие страны. В то же время выбывающую (из-за отрицательной процентной ставки) общую стоимость всей цифровой валюты можно будет периодически восстанавливать осознанной целевой эмиссией новых цифровых денег (и запуском новых, востребованных обществом проектов) на вполне законных основаниях.

Таким образом, все эмитируемые государством новые цифровые деньги пойдут не на кредитование банков-паразитов и разгон инфляции (посредством ключевой ставки ЦБ, ссудного процента коммерческих банков и банковского кредитного мультипликатора), а на скорейшее создание востребованной обществом продукции. При этом функцию средств накопления начнут выполнять не спекулятивные виртуальные финансовые, а реальные активы (товары, природные ресурсы, интеллектуальная собственность и даже... золото), которые будут свободно обмениваться на цифровую валюту «квазиналичного» контура. Цифровые деньги оставят нетронутым все финансовые институты прошлого (в т.ч. и «ссудный процент»), но, как это ни странно звучит, постепенно заставят все эти институты «служить добру» (реальным нуждам экономической жизни), а не «злу» (закабалению людей), т.к. коммерческим банкам придётся конкурировать с дешёвыми и быстрыми «короткими» и «длинными» цифровыми деньгами, разумно эмитируемыми государством, и самим, до минимума сокращать свой паразитический ссудный процент, и (вынужденно!) оказывать реально полезные людям финансовые услуги.

Цифровые валюты ближайших конкурентов

Вскоре после начала работы над цифровым юанем (2014 год) Центробанк Китая (НБК) объединил усилия с Банком международных расчётов (БМР) и Международным валютным фондом (МВФ): Европейский центральный банк, Банк Англии, ФРС США, Банк Канады, Банк Японии, а также ЦБ Швеции и Швейцарии совместно с Банком международных расчётов уже определили основные требования к национальным цифровым валютам. В декабре 2019 года ЦБК заключил партнёрство с семью крупными государственными компаниями и банками, чтобы начать масштабное тестирование цифрового юаня. Госбанки КНР уже конвертировали часть своих депозитов в НБК в цифровую валюту и определили секторы экономики для её продвижения.

Анонимность транзакций будет пониматься лишь в контексте транзакций контрагентов, а у НБК будет доступ к информации обо всех операциях. К концу 2020 года НБК завершил разработку необходимых норм и правил, а регулятор предложил поправки в законодательство, которые предусматривают легализацию цифрового юаня и запрещают выпуск привязанных к нему токенов.

Победа в этой гонке позволит Китаю укрепить позиции юаня на мировой арене и сломить доминирование доллара, создав лучший продукт. Если старый добрый USD работает на древней инфраструктуре, то цифровой юань изначально создан для новой, цифровой, а платёжная система на основе цифрового юаня способна заменить морально устаревшую систему SWIFT на базе доллара. Полномасштабный запуск цифрового юаня (и, соответственно, начало его распространения по всему миру) предположительно состоится на зимних Олимпийских играх в Пекине в 2022 году, откуда «электронные кошельки с цифровым юанем» разлетятся по всему земному шару.

В серьёзности намерений китайцев, а также в том, что они своей настойчивостью, сплочённостью и целеустремлённостью добьются лидерства в мире, сомневаться не приходится, ведь согласно уже принятому компартией Китая плану социально-экономического развития страны на 14-ю пятилетку задачей Китая на ближайшие 5 лет будет превращение его в технологическую супердержаву путём создания самодостаточной замкнутой технологической экосистемы, не оставив всем конкурентам на планете никаких шансов. Для этого ежегодное финансирование всех НИОКР в стране будет увеличено в 17,5 раз (!) по сравнению с предыдущей пятилеткой (когда по технологическому уровню Китай практически сравнялся с США).

Первостепенные задачи, стоящие перед российской электронной индустрией

Раньше России можно было печатать фиатные деньги на любом допотопном печатном станке. Работать с юридическими и физическими лицами тоже было можно на любой непонятно какой импортной технике через коммерческие банки, это был их коммерческий риск! Но вот строить новую валютно-финансовую систему страны, систему национальных цифровых денег (когда, по сути, каждая транзакция будет проходить через ЦБ), и любые (все) риски будут приходиться на ЦБ и его «кибернетику», строить такую национальную систему на иностранных процессорах с уязвимостями и незадекларированными возможностями (ведь это даже не система по учёту налогов) просто недопустимо!

Строить новую цифровую валютно-финансовую систему страны можно только на безопасном цифровом оборудовании, поэтому стране жизненно необходима не только собственная процессорная техника, но и новая цифровая, защищённая аппаратной и квантовой криптографией государственная облачная платформа хранения, обработки и передачи данных. И создавать её надо уже сейчас, заблаговременно и комплексно (наряду с цифровой национальной валютой), а не потом, когда доллара «вдруг» не станет (!).

Наиважнейшее качество любой национальной цифровой валюты – её технологическая защищённость. На сегодня это сложный комплексный вопрос создания целой экосистемы, который должна решить отечественная электронная индустрия. В первую очередь от возможного иностранного вмешательства должна быть защищена (посредством полной замены процессорных и телекоммуникационных средств на отечественные) внутренняя (цифровая электронная) транспортная инфраструктура (маршрутизаторы, серверы, ВОЛС – на квантовые ВОЛС и т.п.), кроме того, заменена вся управляющая электроника на объектах критической инфраструктуры, и ещё должна быть создана защищённая государственная цифровая облачная инфраструктура и, соответственно, собственные защищённые системы хранения данных. Но для этого все эти отечественные технические средства должны быть созданы именно как элементы единой защищённой технической системы (не путать с РАО ЕС).

И момент для создания подобной инфраструктуры (системы) в государственном масштабе (по крайней мере, для госсектора) к настоящему времени с технической точки зрения полностью назрел, поскольку:

- во-первых, именно сейчас, с появлением облаков, качественно изменяется глобальная архитектура систем, что приводит к отмиранию архаичных (т.е. исторически созданных совсем для другого) процессоров (x86 и x86-64) и операционных систем (типа Windows, где есть много ещё не найденных уязвимостей и изначально заложены незадекларированные возможности), причём у страны есть шанс сразу перейти на более простую и более адекватную новой архитектуре самих систем, причём отечественную операционную систему и на отечественную аппаратную платформу;
- во-вторых, в стране уже создана и активно развивается экосистема «Эльбрус», следующее поколение которой уже «не за горами», оно будет в 300 раз быстрее и по производительности практически догонит зарубежные платформы. Но главное в этом то, что эти машины не будут содержать «незадекларированных» возможностей и будут иметь программное обеспечение и операционную систему с поддерживаемой на аппаратном уровне защитой от вирусов и других вредоносных программ. Т.е. это будет полностью контролируемая отечественными разработчиками, а главное развиваемая экосистема, которая должна быть вписана в глобальную отечественную (!) облачную архитектуру;
- в-третьих, именно сейчас Россия (с её-то просторами) весьма далеко продвинулась в области практической квантовой криптографии, точнее в области создания принципиально недоступных для потенциального противника транспортных волоконно-оптических криптосистем, а кроме того, в РКЦ впервые в мире был даже разработан квантово защищённый блокчейн – инструмент для создания распределённой базы данных, в которой практически невозможно подделать записи. Методы квантовой криптографии позволили защитить блокчейн от угроз, связанных с появлением квантового компьютера, потенциального «убийцы» классического интернет-трафика и всех

известных на сегодня, основанных на нем информационных и банковских сервисов. Далеко продвинулись и методы аппаратной дискретной стохастической криптографии, необходимые для защиты как самих технических средств, так и информационных процессов;

- в-четвертых, мировая полупроводниковая индустрия вышла на уровень «систем на кристалле» (System on Chip – SoC). На этом уровне развития полупроводниковая фабрика, производя кристалл, фактически будет производить функционально законченное изделие (электронную часть вещи или системы). Поэтому сегодня не приходится надеяться на западный мир, который осознал, что производить (в ущерб себе) и поставлять в Россию даже микросхемы прошлого века (не говоря уж о SoC), значит, терять огромные рынки и вооружений, и гражданской техники. Поэтому других альтернатив, кроме как инициировать собственные разработки SoC, у России в общем-то и нет (и никакой Китай ей в этом не поможет!).

Технической основой национальной цифровой валютно-финансовой системы и современных систем управления критической инфраструктурой (как было показано ранее) могут быть только технические средства, разработанные отечественными разработчиками (в частности процессоры не должны иметь в своем составе иностранных IP-блоков). Поэтому чем раньше страна поймёт и чем раньше вложит именно в электронную индустрию весь свой интеллект и всю свою оставшуюся финансовую «мощь», тем больше шансов у неё останется сохранить свой суверенитет и в итоге не стать колонией и отсталой страной третьего мира несмотря на наличие у неё атомного оружия. И именно сейчас, именно в электронной отрасли для нашей страны будет решаться вопрос: «To be, or not to be».

Особая роль и вклад экономистов в обеспечение безопасности

Сегодня при наличии гигантских природных ресурсов, при наличии людей и неплохих мозгов у самих этих людей в России уже которое десятилетие не наблюдается никакого развития и экономического роста якобы потому, что нет каких-то инвестиций. Но что такое инвестиции, да и откуда им взяться, инвестициям, в планово убыточную российскую электронную индустрию? Тем не менее с деньгами на электронную индустрию у РФ как раз проблем никогда и не было: «Денег у нас очень много», – обмолвился однажды глава «Роснано» [19]. При желании, а также при наличии политической воли не только нанотехнологии, но и обыкновенная микроэлектроника в стране могла бы уже быть не хуже, чем, например, в Германии.

Но в России на основании утверждённых экономистами бизнес-планов 20 лет подряд, всеми институтами развития, массово, триллионами, финансировались национальные бизнес-проекты по разработке электронной техники на «безопасной» импортной элементной базе, а госпредприятия закупали импортное программное обеспечение и импортные процессоры. Именно так «осваивались» триллионы. Типичный пример этому – «разработка» гипер-процессора «Кристофари» и будущего «российского» искусственного интеллекта на его основе.

В России вместо организации разработок систем на кристалле (SoC), т.е. формирования высокорентабельной добавочной стоимости, на народные деньги закупались планово убыточные полупроводниковые фабрики, с которыми теперь никто не знает что вообще и делать: фабрикам просто нечего производить, а затраты на их содержание огромны [20]. К счастью, «виноватый» во всём этом уже найден. Им оказался разработчик процессоров [21]. Но, как сказано в басне Крылова, по-видимому, он «виноват лишь в том, что хочется мне кушать...». Впрочем, какова истинная цель столь «жёсткой» скупки теперь «отечественных» и якобы безопасных процессоров и операционной системы, известно исключительно «экономистам»..., наука этого не знает.

Экономика и безопасность страны прочно связаны друг с другом. По текущему состоянию экономики России видно, что наши экономисты не в состоянии решить ни системные проблемы экономики, ни, соответственно, проблемы безопасности страны, потому что проблемы эти заключаются совсем не в том, от чего господа-экономисты предлагают страну «лечить» [16, 22]. Конечно, некоторые учёные-экономисты многое знают и что-то могут, некоторые даже очень многое, например, Андрей Рэмович Белоусов, 1-й вице-премьер Правительства России, но таких в стране немного.

Но даже лучшие учёные-экономисты могут решать только задачи параметрического анализа экономики в целом (на основе данных Росстата), а задачи параметрического и структурного синтеза (тем более, касающиеся конкретных технологических отраслей и их взаимодействия) они ни решать, ни решить принципиально не в состоянии). А ведь если допущены ошибки на структурном уровне, то никаким параметрическим анализом и управлением (в т.ч. законами и запоздалым латанием дыр народными деньгами) ситуацию уже не отрегулировать.

Если мы имеем проблемы в химической промышленности, то кого мы пригласим для обсуждения этих проблем и поиска решения? Пригласим химиков: теоретиков, практиков, организаторов. Если мы имеем проблемы в металлургии – пригласим металлургов. Если проблемы в обороне – пригласим военных и т.д. Так почему же такой сложнейшей технической, столь динамично развивающейся и комплексной отраслью, как нанотехнологии, электронная индустрия и вычислительная техника, были поставлены управлять вообще мало что понимающие во всём этом «ура-экономисты»?

Заключение

Реальные инновации, реальные системы, реальные прорывные и конкурентоспособные технологии создаются не чиновниками, не экономистами, а людьми совсем другого рода, в иной, научной и рыночной среде.

Но миллионы людей, среди которых сотни тысяч уникальных специалистов, покинули Россию. Только по официальной оценке РАН, если в 2013 году было 20 тыс. уехавших учёных, то в 2016 их стало уже 44 тыс., и это число к 2020 году лишь увеличилось.

Сотни перспективнейших проектов в области электроники, которые давно могли бы «поднять с колен» полупроводниковую индустрию страны (примеры тому – Китай, Южная Корея и т.п.), десятилетиями лежали, лежат и будут лежать «под сукном» у российских чиновников [1–6,23].

И главное, что теперь должна понять страна: отдавая последние деньги в руки новоявленных «ура-экономистов от электроники», ни по риторике ни по делам ничем не отличающихся от предыдущих [24], она проводит последний, причём смертельный экономический эксперимент. Пора, наконец, осознать,

что время глашатаев-болтунов, «ура-экономистов» и «ура-патриотов» закончилось. Началась Третья Мировая Электронная Война.

Литература

1. *Галицын А.* Неуправляемые боевые роботы и беспилотники. Современная электроника. 2020. № 9.
2. *Галицын А., Рождественский А., Рождественский Д.* Системы управления с «предвидением». Современная электроника. 2019. № 9.
3. *Галицын А.* Туманный Интернет вещей. Современная электроника. 2020. № 3.
4. *Егоров Е., Егоров В., Галицын А.* Явление и последствия волноводно-резонансного распространения и взаимодействия радиационных потоков. Часть 1,2. Современная электроника. 2020. № 1,2.
5. *Егоров Е., Егоров В., Галицын А.* Элементный анализ планарных нано-структур на базе рентгеновской эмиссии индуцированной высокоэнергетическим возбуждением. Современная электроника, 2021, №5
6. *Галицын А.* IoT-радиопроцессор с крипто-кодированием структуры радиосигнала. Современная электроника. 2019. № 7.
7. *Шпак В.* «О первом годе реализации Стратегии развития электронной промышленности до 2030 года». Интернет-портал YOUTUBE : https://www.youtube.com/watch?v=PK1vTyfmBJw&feature=share&fbclid=IwAR3f_O9AdopQUcz3sPC43IxfOHZUp_OV1wymBfBGLKQpXE_0N6d6IOHzulg.
8. В США пригрозили ответить России «не просто санкциями». Портал Лента.RU, Новости, 2021: https://lenta.ru/news/2021/02/21/ciber/.
9. *Андреев С.* Технологии под ударом. Зачем США ввели санкции против российской промышленности. Интернет-портал LIFE, 2019: https://life.ru/p/1359926.
10. *Королев И.* Российские электронщики объявлены врагами США: 119 имен и компаний. Интернет-портал CNEWS,2020: https://www.cnews.ru/news/top/rossijskie_elektronshchiki_obyavleny_vragami.
11. *Степаненко И.* Основы теории транзисторов и транзисторных схем. Издание 3-е, переработанное и дополненное, М. Энергия, 1973, 608 р.
12. *Алексенко А.* Основы микросхемотехники. М. Советское радио, 1971, 352 р.
13. *Алексенко А., Шагурин И.* Микросхемотехника: Учеб. пособие для вузов. Издание 2-е, переработанное и дополненное. М. Радио и связь, 1990, 496 с.
14. *Алексенко А. Графен, М.* Бином, 2014. 176 с.
15. *Алексенко А., Галицын А., Иванников А.* Проектирование радиоэлектронной аппаратуры на микропроцессорах. М. Радио и связь, 1984, 270 с.
16. *Железнов А.* Системные вопросы разрушения экономики СССР и России. Часть 1,2. Журнал «СВЕРХНОВАЯ РЕАЛЬНОСТЬ», 2008, №3, 2009,№4.
17. *Трушкин К.* Что такое «Эльбрус»? Официальный сайт компании МЦСТ, 2020: http://www.elbrus.ru/.
18. *Смоленцев С.* Информационные технологии. Защита информации в корпоративных сетях. Издательство ГМА им. Адмирала С. О. Макарова, 2009, 201 с.
19. *Чубайс А.* Выступление на собрании «Роснано». Интернет-портал YOUTUBE : https://www.youtube.com/watch?v=_lzr2UXAI1g
20. *Гатинский А.* Шувалов объявил о выделении заводу «Ангстрем-Т» почти 21 млрд руб. Интернет-портал РБК: https://www.rbc.ru/business/27/05/2019/5cebf51b9a79475a3786f801.
21. Baikal Electroniks. О компании. Официальный сайт компании «Байкал Электроникс»: https://www.baikalelectronics.ru/about/
22. *Ханин Г.* Как спасти от краха экономику России? Троицкий вариант. М. Наука, 2019, № 277, с. 15. Интернет-портал trv-science.ru: https://trv-science. ru/2019/04/23/kak-spasti-ot-kraxa-ekonomiku-rossii/.
23. *Галицын А.* Технология широкополосной высокозащищенной радиосвязи (C-UWB): что лежит «под сукном» у российских чиновников. М, Первая миля, Техносфера, 2008, № 1.
24. *Садыркин П.* «Роснано» создавали для технологического прорыва. Почему его не случилось даже через 13 лет. Интернет-портал LENTA.RU: https://lenta.ru/articles/2021/01/27/ rosnano/.

НОВОСТИ МИРА

К 2025 году число eSIM в мире достигнет 3,4 миллиарда

Исследование предполагает, что внедрение фреймворков eSIM от поставщиков потребительских устройств, таких как Apple и Google, ускорит рост ESIM. Исследование Juniper Research показало, что количество ESIM, установленных в подключённых устройствах, увеличится с 1,2 миллиарда в 2021 году до 3,4 миллиарда в 2025 году, что составляет рост на 180%. ESIM – это модули, встроенные непосредственно в устройства, которые обеспечивают сотовую связь и хранят несколько профилей операторов сети. Исследование независимо оценило внедрение eSIM и спрос в потребительском, промышленном и государственном секторе и прогнозирует, что к 2025 году на потребительский сектор будет приходиться 94% мировых установок eSIM. Исследование предполагает, что внедрение платформ eSIM от поставщиков потребительских устройств, таких как Apple и Google, ускорит рост ESIM в потребительских устройствах, опередив промышленный и государственный секторы. Глобальное развёртывание ESIM во всех потребительских вертикалях увеличится на 170% в течение следующих четырёх лет, а широкое внедрение будет зависеть от поддержки сетевых операторов. Чтобы помочь рынку, производители устройств должны оказать давление на операторов, чтобы они поддерживали платформы eSIM и ускоряли созревание рынка. Однако фрагментация поставщиков оборудования на рынке устройств сотовой связи IoT потребует от каждой вертикали принятия комбинации беспроводных технологий, оборудования и инструментов управления. В свою очередь, в отчёте прогнозируется, что появятся специализированные поставщики, которые обеспечат надёжные форм-факторы eSIM для промышленных сред. Разработка промышленных форм-факторов позволит поставщикам хорошо заработать на

рынке, поскольку установки eSIM в этих вертикалях вырастут с 28 миллионов единиц в 2021 году до 116 миллионов к 2025 году. Авторы исследования отметили, что обеспечение удобства для конечного пользователя должно оставаться главным приоритетом для поставщиков платформ управления eSIM. Для этого они должны обеспечить уровень обслуживания, сопоставимый с тем, который наблюдается при использовании традиционных SIM-карт.

www.eenewswireless.com

РОССИЙСКАЯ НЕДЕЛЯ ВЫСОКИХ ТЕХНОЛОГИЙ

СВЯЗЬ

Информационные и коммуникационные технологии

15–18 июня 2021

33-я международная выставка

Организатор

экспоцентр

12+ Реклама

Россия, Москва, ЦВК «ЭКСПОЦЕНТР»

www.svyaz-expo.ru