



## Россия, «Инициатива 2007»

Современный мир, рассматриваемый в единстве физических и информационных процессов, высоко динамичен и крайне противоречив. Рынок информационных технологий и услуг поделен, мировые супер-бренды созданы и раскручены. На пороге новая эра.

**Развернута острейшая борьба за высокотехнологичные сектора**, связанные с завоеванием превосходства на физическом уровне обработки. В первую очередь к ним относятся сектора, охватываемые технологиями радиочастотной идентификации (RFID), сенсорными, широкополосными и сверхширокополосными (UWB) технологиями передачи данных, способными качественно изменить глобальную сеть Интернет, линии связи, системы автоматизированного сбора и обработки информации о материальных объектах и состоянии внешней среды.

**Информационный рынок упущен, государственный анахронизм в области развития отечественной электроники продолжается.** При наличии в стране свободных денег радиоэлектронная отрасль, как одна из ключевых в становлении и развитии «Информационного Общества», находится в состоянии стагнации, «задыхается» из-за отсутствия массовой конкурентоспособной продукции и не имеет видимых перспектив, если судить по состоянию научных исследований и содержанию принятых на 2008-2015 годы программ.

Подогреваемые нашей беспомощностью имперские амбиции некоторых государств, идущие с их стороны политические провокации, цинично прикрываемые «благими» намерениями, ведущиеся изощренные попытки навязывания выходящих из употребления бесперспективных решений, практикуемое внесение в них скрытых закладок – нацелены на завоевание господства и осуществление диктата в информационном пространстве, а также, как видим не без успеха, в научно-технической и производственной сфере.

Положение усугубляется процветающей коррупцией и правовым беспределом, а также разрушительной по последствиям проводимой политикой, ориентированной на импорт стратегических технологий и высокотехнологической продукции, вместо развития собственных технологий и высокотехнологических производств.

**Происходящее беспрецедентное нарастание внешних и внутренних угроз безопасности, послужило мотивом нашего обращения «к единомышленникам, ко всем, кто хочет сделать Россию сильной и благополучной страной» (В. Путин, 2007), с предложением присоединиться к инициативе, направленной на защиту национальных интересов и достижение прорывных результатов в области информационных, электронных, сенсорных, коммуникационных, био- и нанотехнологий, технологий автоматизированной обработки и обеспечения безопасности.**

Технологий, на основе которых этого можно достичь, единицы. По прогнозам аналитиков CNN, сделанных в 2004 году, технологии UWB и RFID, поставлены на первых два места, как одни из прорывных технологий XXI века, способных принести отдачу, соизмеримую с отдачей высоко развитых секторов экономики.

До недавнего времени казалось, здесь все, что только можно утрачено, но это не так. Получены новые, рассчитанные на массового потребителя и опережающие мировой уровень результаты в области помехоустойчивой и многоканальной обработки радиочастотных сигналов, работы в этой области продолжаются. Технологии RFID, не подкрепленные обеспечением должного уровня безопасности, не смогли выйти за корпоративные рамки и вопреки прогнозам аналитиков не оправдали надежд революционного преобразования мирового товарного рынка.

С открытием алгебраических систем неполной арифметики, введением стохастических систем и динамического хаоса дискретного времени, а также с имеющимися и существенно превосходящими мировой уровень разработками в теории сигналов, помехоустойчивой обработки и стохастической криптографии, сложились условия для осуществления прорыва и достижения реального превосходства в области информиндустрии и стремительного продвижения на мировые рынки отечественных технологий.

Создание условий для технологического прорыва необходимо, но недостаточно. Без перевода в практическое русло полученных научно-технических результатов, все наши призывы останутся на бумаге, а достижения уйдут за границу и будут заимствованы оборотистыми предпринимателями, как это уже было не раз.

**Так, что же мы можем сделать в ближайшие несколько лет ?** Проведенные исследования и уроки, полученные из внедрения автоматизированных систем электронной идентификации на базе платформ, типа EPC System Network, показали наличие серьезных тактических и стратегических просчетов в архитектуре построения и элементной базе систем RFID, в форматах представления данных и подходах обеспечения безопасности.

Имеющиеся на сегодня заделы и достигнутые результаты позволят осуществить разработку не имеющих аналогов в мире высокоэффективных, конструктивно и функционально гибких микросенсорных функциональных модулей (микросенсорных устройств) – радиочастотных меток и других средств маркировки, платежных талонов и карт, сенсор-датчиков и других надежно (криптографически) защищенных от клонирования и подделки миниатюрных устройств, по ценам, соизмеримым с дешевыми серийными метками RFID (3-7 центов и менее, против \$0.5-2.5), наладить их широкомасштабное производство.

Микросенсорные устройства будут способны функционировать как за счет энергии внешнего поля, так и за счет экономичных микро-топливных элементов, приобретут уникальные свойства с внедрением помехоустойчивых радио-интерфейсов, с оснащением экономичными и дешевыми мини-датчиками с многопрофильными чувствительными (чувствительными, смарт) элементами.

Устранение выявленных недочетов и создание прогрессивной технологической базы позволит добиться качественно нового, существенно выраженного мультипликативного взаимодействия физического и логического уровней обработки, положит основу для разработки и освоения технологий построения безопасных высокоэффективных сетей и систем, способных к высокоуровневой интеграции в сети Интернет, поддержке информационных, логистических и прикладных приложений.

Все это вместе позволит, **на недоступном для конкурентов качественном уровне** и значениях технико-экономических показателях, осуществить решение следующего комплекса задач:

1. Защита товарного рынка и сегментов экономики от нелегальной и недоброкачественной продукции на основе микросенсорных средств маркировки, их комплексирования с производственно-технологическими средствами защиты, сенсорными устройствами и мини-датчиками.

2. Проведение денежных расчетов и платежей на основе дешевых и более удобных в обращении бесконтактных микросенсорных талонов и карт. Регламентирование доступа, организация пропускного режима.

3. Обеспечение экологической, биологической и физической безопасности на основе микросенсоров, беспроводных сетей и глобальной сети Интернет.

4. Создание на основе сочетания микросенсорных и UWB технологий инструментальной базы необходимой для построения безопасных интеграционных платформ и сетей высокой помехозащищенности, развития и производства нового поколения бытового, офисного и специального беспроводного High-Tech оборудования, систем связи и телевидения.

5. Технологии выйдут на новый глобальный уровень интеграции с развитием спутниковых систем, систем позиционирования и навигации, отличающихся высоким уровнем безопасности.

Все это, в сочетании с возможностью достижения качественно нового уровня системной интеграции, управления и прозрачности товарного рынка и смежных с ним отраслей, позволит **осуществить качественный прорыв в следующих жизненно важных сферах:**

- Производство и реализация продукции, с предоставлением всем слоям населения индивидуальных карманных и мобильных средств проверки подлинности и качества продукции, перенос “центра тяжести” с малоэффективного ведомственного государственного надзора, на широкомасштабный действенный гражданский контроль.

- Мониторинг инженерно-технической инфраструктуры, отличающийся высокой эффективностью и надежностью, функциональностью и рентабельностью, устойчивый к деструктивным воздействиям и нерегламентированному управлению.

- Обеспечение безопасности граждан, организация и проведение мероприятий по борьбе с террористическими действиями и криминогенными проявлениями в обществе, вызываемыми ими социальными угрозами и экономическими деформациями.

Представляемые Инициативой информационные и электронные технологии допускают последующее масштабное распространение на задачи защиты удостоверяющих документов и национальной валюты, маркировки почтовых отправлений, архивных документов, выставочных экспонатов и содержимого библиотечных фондов, идентификации домашних животных, охраны и интеллектуализации не только особо жизненно-важных объектов, но и не менее важных для наших людей, их жилищ и строений, а также на другие приложения в сфере обеспечения безопасности.

Логическим итогом проводимых в рамках Инициативы работ, станет разработка на основе стохастических технологий параллельного криптографического сопроцессора и его программной поддержки, в целях решения задач обеспечения информационной безопасности в реальном масштабе времени, ликвидации отставания криптографических технологий от современного уровня развития техники. В этих условиях стохастическая криптография, в отличие от узкоспециализированной традиционной, как естественная и неотъемлемая часть стохастических систем, а не скрытых закладок спецслужб, встанет на защиту каждого добропорядочного гражданина.

Оценивая в целом существующее состояние и перспективы развития мирового информационного и электронного рынка, с реализацией в предлагаемой Инициативой постановке перечисленных

выше задач, **России представляется уникальный исторический шанс для достижения паритета, стремительного выхода на передовые рубежи и завоевания технологического превосходства**, особенно в сфере обеспечения безопасности, придания нового импульса инновационному развитию отечественной науки и экономики, опережающей разработке и промышленному освоению био- и наноматериалов, новых способов передачи данных и электроники. **Если этот шанс будет упущен, то вероятней всего, преодолеть проблемы связанные с этой бурно развивающейся сферой, в первую очередь в части обеспечения безопасности, будет практически невозможно.**

По всем объективным показателям настала пора действовать решительно, стремительно и твердо, поставить точку на безудержном копировании западных технологий, повторении прошлых ошибок, распылении государственных средств и интеллектуальных ресурсов России.

Наши попытки решить через Федеральное агентство по науке и инновациям даже малую часть выдвигаемых Инициативой проектов, из представленной ниже Комплексной программы, не увенчались успехом. Причин тому много, начиная, на удивление, от отсутствия финансовых средств, до серьезных претензий к организации отбора материалов и проведения конкурсов, с идущим захватом чиновниками руководства наукой, плодородных с этим непомерных объемов инструкций, указывающим что и как делать. Особенно от этого страдают именно новаторские разработки, выходящие за установленные ими в своих интересах элементарные процедурные рамки. Не иначе, как новой волной чиновничьего беспредела, ведущего к идейному банкротству агентства, это не назовешь.

Вызываемое этим более чем призрачные надежды реализации через это ведомство представляемой Комплексной программой проектов, даже при всех их очевидных преимуществах, послужило поводом нашего прямого обращения 21 февраля 2008 года к министру образования и науки. Полученный 12 марта 2008 года за № 04-208 ответ, показал нежелание рассматривать по существу чиновниками возглавляемого им министерства представленных Инициативой задач. Последовала формальная отсылка в Федеральное агентство по науке и инновациям. Тем самым показано, что **наши претензии и беспокойство не лишены оснований – замкнулся известный многим порочный бюрократический круг. Теперь, когда истинные создатели интеллектуальной продукции отсечены, им некуда деться и только остается положиться на милость чиновников, коррупционеры могут делать все что захочется.**

Не меняет дела и принятая недавно Федеральная целевая программа по «Развитию электронной компонентной базы и радиоэлектроники на 2008 - 2015 годы», в которой изначально в связи с убогим пониманием сути предмета, фактически вычеркнуто развитие и финансирование представляемого Инициативой гигантского технологического направления, ведущее на заклятие запада информационное пространство России и в полную зависимость отечественной экономики от развитых государств. Одно говорим, а прямо противоположное делаем.

Если судить по решаемым задачам, такая политика идет в разрез коренных интересов Населения и других рядовых Потребителей, Инспекционных органов и Министерств (промышленности и энергетики, информационных технологий и связи, экономического развития и торговли, здравоохранения и социального развития, транспорта, сельского хозяйства, внутренних дел, обороны, культуры и массовых коммуникаций), а в целом, ставит под угрозу безопасность России.

Со всей очевидностью, предпринятая **Инициатива, как новый общественный инструмент решения сложных задач и прорыва выстроенных колониальных кордонов, по степени интеграции представляемых решений и их неизмеримо весомой социальной, экономической и научно-технической отдаче, не укладывается в устроенные государственными ведомствами рамки и требует исключительно индивидуального подхода к финансированию и организации проводимых работ.**

Опираясь на имеющиеся заделы и проведенный всесторонний анализ, мы сделали выбор и приложили все силы для доведения до общественности и государственных органов своего видения пути развития «Информационного Общества».

**Теперь судьба предпринятой нами инициативы в руках первых лиц и высших органов государственной власти.**

Беспрецедентные масштабы распространения поддельной и недоброкачественной продукции, засилье элементной базы иностранного производства в системах информационной защиты и предотвращения несанкционированного доступа, превращение операционной системы Windows и лицензионных программных продуктов в источники утечки конфиденциальной информации и опасных деструктивных воздействий, причем с созданием в США 25 тысячного контингента для ведения киберсетевых войн, такие угрозы уже приобретают глобальный характер, а также угрозы идущие с развитием nanoиндустрии требуют коренного пересмотра политики проводимой государством в области обеспечения безопасности.

**На нижних уровнях государственного управления проблемы обеспечения безопасности не разрешимы и требуют жесткого государственного надзора и централизованного управления, подкрепленного современными научно-техническими достижениями.**

**К инициативе присоединились и поддерживают ее в принятой постановке:**<sup>2</sup>

Руководитель Роспотребнадзора, профессор, д.м.н, академик РАН Г.Г. Онищенко	Зам. руководителя Роспотребнадзора Л.П. Гульченко
Руководитель Росздравнадзора, профессор, д.м.н, Заслуженный врач России Н.В. Юргель	Зам. руководителя Росздравнадзора А.Л. Младенцев
Президент Торгово-Промышленной Палаты РФ, профессор, д.э.н, академик РАН Е.М. Примаков	Главный эксперт Департамента экономической безопасности ТПП РФ А.К. Никитин
Генеральный директор ФГУП ГосНИИ Авиационных систем, профессор, д.т.н, член-корреспондент РАН С.Ю. Желтов	Начальник отделения Информационных управляющих систем ФГУП ГосНИИАС, к.т.н, старший научный сотрудник Ю.И. Буряк
Директор Центра информационных технологий и систем Органов исполнительной власти профессор, доктор технических наук, Заслуженный деятель науки и техники РФ А.В. Старовойтов	Первый заместитель директора, Главный инженер ЦИТиС В.М. Купцов
Директор Института радиотехники и электроники РАН, профессор, д.ф-м.н, академик РАН Ю.В. Гуляев	Зам. директора ИРЭ РАН, профессор, д.ф-м.н, член-корреспондент РАН С.А. Никитов
Директор ФГУП ВНИИ Проблем вычислительной техники и информатизации доктор технических наук, академик РАЕН В.А. Конявский	
Ректор Московского технического университета связи и информатики профессор, д.т.н, академик МАС и МАИ А.С. Аджемов	Начальник отдела Информационных ресурсов и Интеллектуальной Собственности МТУСИ, профессор, к.т.н, академик МАС и МАИ Е.П. Зелевич
Ректор Московского инженерно-физического института (государственный университет), профессор, доктор физико-математических наук М.Н. Стриханов	Зам. заведующего кафедры № 12 МИФИ "Компьютерные системы и технологии", профессор, доктор технических наук М.А. Иванов
Ректор Московского государственного института электронной техники (технический университет) профессор, д.т.н, член-корреспондент РАН Ю.А. Чаплыгин	Проректор по научной работе МИЭТ, профессор, доктор технических наук В.А. Бархоткин
Генеральный директор ЗАО Научно-технического центра «Модуль» А.А. Адамов	Вице-президент Лиги оборонных предприятий, академик МАИ А.Н. Шулунов
Генеральный директор ОАО «Ангстрем» А.И. Спирин	Начальник дизайн-центра ОАО «Ангстрем» В.И. Гуминов
Генеральный директор ОАО «Ангстрем-М», кандидат технических наук П.Р. Машевич	Главный конструктор ОАО «Ангстрем-М» В.М. Самохвалов
Генеральный директор Межрегионального некоммерческого партнерства «Отечественная электроника», кандидат экономических наук А.Н. Михайлова	Главный технолог МНП «Отечественная электроника», к.ф-м.н, член-корреспондент АТН РФ В.В. Минаев
Генеральный директор ООО НПП «НовСисТех», к.т.н, А.А. Галицын	
Генеральный директор ЗАО «Авионика-РТС» А.Ю. Ипатов	Главный конструктор ЗАО «Авионика-РТС», Член рабочей группы ИКАО Г.А. Николаев

<sup>2</sup> по результатам проведенной участниками предварительной экспертизы первичных материалов

Генеральный директор ООО «ОПФ ПИК», академик ВАНКБ С.М. Ларионов	
Генеральный директор ООО «Протекшен Технолоджи» Н.И. Беликова	Исполнительный директор ООО «Протекшен Технолоджи», кандидат физико-математических наук М.И. Калиниченко
Президент компании «ЛАН Крипто», кандидат физико-математических наук А.Н. Лебедев	
Генеральный директор ООО «Проблемная Лаборатория» А.П. Ананьев	Эксперт ООО «Проблемная Лаборатория», кандидат технических наук И.В. Чугунков Эксперт компании ЗАО «ИнфоВотч», кандидат физико-математических наук А.Г. Иванов
Директор, главный конструктор НИКИРЭТ филиала ФГУП «Произв. объединения Старт» В.А. Первунинских	Зам. директора по науке НИКИРЭТ, к.т.н, Заслуженный конструктор РФ Л.Е. Лебедев
Генеральный директор Типографии ОАО «Промис» (Центр упаковки, этикетки, дизайна) Е. Е. Слияков	Директор по внешнеэкономическим связям ОАО «Промис» М.М. Трофимов
<p><u>Согласуются вопросы о присоединении к Инициативе:</u> холдинги «Российская электроника» и «Ситроникс», ООО «Анкад», ФГУ Российский научный центр «Курчатовский институт», МО РФ.</p> <p>Институт программных систем РАН, готов присоединиться к Инициативе в перспективе, для решения конкретных задач, предусмотренных выдвигаемой ею Комплексной программы.</p>	
Директор ФГУ РНЦ «Курчатовский институт», профессор, д.ф-м.н, член-корреспондент РАН М.В. Ковальчук	Начальник Управления инвестиционных программ ФГУ РНЦ «Курчатовский институт» А.Е. Лысенко
Директор ИПС РАН, д.ф-м.н, член-корреспондент РАН С.М. Абрамов	Ученый секретарь ИПС РАН, кандидат технических наук С.М. Понамарева
Президент ОАО «СИТРОНИКС» С.Г. Асланян	Руководитель бизнес-направления «СИТРОНИКС Микроэлектронные решения» профессор, д.т.н, член-корреспондент РАН Г.Я. Красников
<p>Инициатива строится на добровольной и открытой основе, носит рекомендательный характер, отражающий здоровое стремление и возможность профессионалов изменить к лучшему явное неблагоприятное положение дел в сфере информационных, электронных и коммуникационных технологий, обеспечения безопасности.</p> <p>Для координации действий участников Инициативы в реализации выдвигаемой ею Комплексной программы, организации подготовки планируемых ею Пилотных и Комплексных проектов и материалов конкурсных заявок, оказания консультативной и научной поддержки исполнителям, а также определения состава работ и отбора их исполнителей, создан Координационный совет.</p> <p>В состав Координационного совета вошли руководители следующих организаций: ЦИТиС, НТС «Модуль», ОАО «Ангстрем», ФГУП ВНИИ ПВТИ, ФГУП ГосНИИАС.</p> <p>От имени членов совета 19 февраля 2008 года в адрес Министра образования и науки РФ направлено письмо, с предложением возглавить Координационный Совет и стать его Председателем. Известно, каким произволом это обращение обернулось.</p> <p>Предложение войти в состав Координационного совета, также подано руководству ИРЭ РАН, ФГУ РНЦ «Курчатовский институт», ОАО «СИТРОНИКС».</p>	
<p>На период консолидации сил, по всем вопросам и получению дополнительных материалов, пожалуйста, обращайтесь к инициатору программы, Кулакову Игорю Анатольевичу, по адресу</p>	

**Стратегическая цель** преследуемая «Инициативой 2007» – создание на основе передовых научно-технических достижений технологической и инструментальной базы, необходимой для придания нового качественного уровня развитию информационных, электронных, коммуникационных, сенсорных и криптографических технологий, формирования посредством них условий для широкомасштабного внедрения в производство достижений микроэлектронной, био- и nanoиндустрии, направленных на становление и интенсивное развитие «Информационного Общества» России, поддержание необходимого уровня обеспечения обороноспособности и безопасности.

Для решения этих задач выдвигается Комплексная программа. Комплексная программа предполагает реализацию объединенных единым замыслом, двух Пилотных и трех Комплексных проектов.

**Пилотные проекты** предназначены для подтверждения осуществимости Программы и создания задела, требуемого для реализации поздних этапов Комплексной программы. Темы проектов:

**Первый.** «Обоснование и разработка модели базовой интеграционной платформы автоматизированной обработки информации о состоянии материальной среды и ее элементов, поддержки высокоуровневых приложений и обеспечения безопасности».

**Второй.** «Реализация и проведение анализа бесповторных генераторов (псевдо) случайных чисел систем управления ключами высокой криптографической стойкости, предотвращения несанкционированного доступа и информационной защиты».

**Комплексные проекты** рассчитаны на формирование базы высокотехнологического сектора экономики «Информационного Общества» – *информиндустрии*.

**Первый Комплексный проект** – «Разработка адаптивной интеграционной платформы и компонентной базы систем электронной сертификации, логистического и информационного сопровождения, контроля состояния, регламентного обслуживания и обеспечения безопасности материальных объектов и их образований». Является итогом совместной деятельности компаний ОАО «Ангстрем», ОАО «Ангстрем-М» и Random Art Labs, начиная с сентября 2005 года, а также работ выполненных в июле-сентябре 2007 года координатором «Инициативы 2007» и РИЦ «Курчатовский институт», по конкретизации и выработке подходов к решению проблем обеспечения безопасности, отраженных в проекте доклада «Долгосрочный научно-технологический прогноз развития Российской Федерации на период до 2025 года». Ставит целью подготовку условий для осуществления качественного прорыва в области сенсорных технологий.

**Второй Комплексный проект** – «Создание технологии и компонентной базы для построения безопасных микросенсорных сетей высокой помехозащищенности». Предполагает осуществление прорыва в области построения безопасных интеграционных платформ и адаптивных сетей высокой помехозащищенности на основе развития технологий передачи радиочастотных сигналов, UWB технологий и заделов вносимых компанией ООО НПП «НовСисТех», динамического хаоса дискретного времени и результатов проводимых работ с ИРЭ РАН в рамках второго Пилотного проекта и микросенсорных технологий вышеупомянутого Комплексного проекта.

**Третий Комплексный проект** – «Разработка на основе стохастической криптографии технологии и технических средств обеспечения информационной безопасности компьютерных систем, включая реализацию параллельного криптографического сопроцессора и его программной поддержки». Направлен на достижение нового качественного уровня развития систем обеспечения компьютерной информационной безопасности. Подготовка документации необходимой для начала работ по проекту является предметом разработки второго Пилотного проекта.

В соответствии с порядком реализации Комплексной программы, выдвигаемой Инициативой, состав работ приводится ниже в таблице 1, в Федеральное агентство по науке и инновациям:

1. Подана тематическая заявка, предусмотренная первым Пилотным проектом, зарегистрирована 13 декабря 2007 года, под номерами 5670 и 5733, программное мероприятие (п/м) 1.4, исполнители ООО «Протекшен Технолоджи», ОАО «Ангстрем» и ООО «ОПФ ПИК».

2. Подготовлена тематическая заявка, предусмотренная вторым Пилотным проектом, п/м 1.4, исполнители МИФИ, ИРЭ РАН и ФГУП ВНИИ ПВТИ.

3. На стадии согласования находятся материалы, необходимые для подготовки тематической заявки по первому Комплексному проекту, объединяющему в рамках консорциума более 16 организаций, взамен устаревшей тематической заявки, зарегистрированной под № 5008 за 2008 год (п/м 2.4), поданной от имени ОАО «Ангстрем» 27 февраля 2007 года, а также материалов по Конкурсному проекту «Разработка интегрированной технологической платформы для мониторинга элементов и систем жизненно важной инфраструктуры на основе информационно-коммуникационных технологий расширенного Интернета» (Лот 5, 2007-4-2.4-00-03), поданного консорциумом во главе с ОАО «Ангстрем» 14 марта 2007 года и соисполнителями: ОАО «Ангстрем-М», МНИИ «Интеграл», МИФИ и ООО «Авиакомплект».

4. Начата подготовка тематической заявки по второму Комплексному проекту. В основу проекта положены материалы заявки, поданные ООО НПП «НовСисТех» 14 ноября 2006 года (п/м 2.4), по теме «С-UWB RFID технология (для государственного сектора применений)».

Таблица 1. Основной состав работ проводимых в рамках Комплексной программы и планируемые результаты

Наименование проекта	Этап I	Этап II	Примечание: Пилотные проекты получают свое развитие в Комплексных проектах, по следующим направлениям:	Коммерциализация и подтверждение результатов
<b>Первый Пилотный проект</b> Обоснование и разработка модели базовой интеграционной платформы автоматизированной обработки информации о состоянии материальной среды и ее элементов, поддержки высокоуровневых приложений и обеспечения безопасности	1. Разработка компактных электронных сертификатов материальных объектов. 2. Разработка архитектуры и программная реализация базовой интеграционной платформы на основе модернизации и развития решений компании EPCglobal, рассчитанной на государственный и корпоративный уровни управления.	1. Разработка программной и информационной поддержки авторизационных Протоколов контроля и логистического прослеживания целостности цепей прохождения объектов. 2. Разработка общесистемного интерфейса интеграционной платформы с высокоуровневыми приложениями.	- Создание безопасной адаптивной логистической сети в соответствии с развитием инфраструктуры EPC System Network и SAP. - Проведение комплексного анализа криптографических Протоколов авторизации, аутентификации, генерации и управления ключами в микросенсорных сетях. - Разработка принципов построения комплексной (сетевой) защиты сложных объектов, комплексирование производственно-технологических и электронных способов защиты.	Создание системы электронной идентификации материальных объектов на основе серийно производимых цифровых меток типа I-Code и перспективных аналоговых ПАВ-меток компании ООО «ОПФ ПИК».
<b>Второй Пилотный проект</b> Реализация и проведение анализа бесповторных генераторов (псевдо) случайных чисел систем управления ключами высокой криптографической стойкости, предотвращения несанкционированного доступа и информационной защиты	1. Подготовка отчета по основам стохастической криптографии и алгебраических систем неполной арифметики. 2. Обоснование принципов построения и программная реализация линейки типовых генераторов ключевого потока, регулируемой криптографической стойкости.	1. Разработка методик и проведение линейного, дифференциального криптографического анализа генераторов, включая имитационное, осуществление оценки нелинейности алгоритмов. 2. Проведение сравнительного анализа динамического хаоса дискретного и непрерывного времени.	<b>Этап III</b>	Создание систем динамического регламентирования доступа устойчивых к массированному сторонним атакам, на основе микрочипов динамической генерации паролей высокой криптографической стойкости, для систем коллективного пользования и банковских систем.
<b>Первый Комплексный проект</b> Разработка адаптивной интеграционной платформы и компонентной базы систем электронной сертификации, логистического и информационного сопровождения, контроля состояния, регламентного обслуживания и обеспечения безопасности материальных объектов и их образований	1. Разработка и реализация интерфейса взаимодействия микросенсоров со считывающими устройствами. 2. Разработка диспетчера команд и информационной поддержки микросенсоров. 3. Изготовление на кристаллах кремния прототипа микросенсора ID и считывающего устройства.	1. Разработка и изготовление прототипа логистического микросенсора (с разрешением коллизий) и считывающих устройств. 2. Разработка типовых функциональных блоков микросенсоров. 3. Разработка штатных устройств авторизации (подписи) объектов. 4. Разработка технологических принципов построения WB интерфейса микросенсоров.	1. Разработка и изготовление прототипа криптозащищенного микросенсора и считывающих устройств, включая мобильные. 2. Разработка типовых мини-датчиков систем обеспечения безопасности на основе смарт-материалов 3. Разработка и реализация программно-аппаратной многоуровневой подсистемы генерации и управления ключами.	1. «Защита Авиацнонно-технического рынка от нелицензионной продукции» 2. «Защита товарного рынка от фальсифицированной и недоброкачественной продукции» 3. «Автоматизированный учет, сопровождение, контроль состояния и регламентное обслуживание техники, оружия, боеприпасов и военного снаряжения»
<b>Второй Комплексный проект</b> Создание технологии и компонентной базы для построения безопасных микросенсорных сетей высокой помехозащищенности.  <b>Прим.</b> Здесь и далее, под аббревиатурой WB условно понимаются, как широкополосные, так и сверхширокополосные радиосигналы.	1. Подготовка аналитического отчета «Стохастические системы и WB технологии». 2. Разработка WB интерфейса микросенсоров. 3. Разработка имитационной модели WB интерфейса. 4. Разработка принципов построения микросенсорных сетей на основе развития технологий WB, Wi-Fi, Bluetooth и ZigBee.	1. Разработка и проведение комплексного анализа криптографических примитивов WB технологий. 2. Реализация имитационной модели WB интерфейса. 3. Оптимизация на имитационной модели параметров и схемотехнических решений построения WB интерфейса. 4. Реализация WB интерфейса микросенсоров.	1. Проведение комплексных испытаний WB интерфейса. Доработка по результатам испытаний WB интерфейса и его имитационной модели. 2. Реализация прототипа WB микросенсора, проведение испытаний 3. Разработка принципов построения микросенсорных сетей высокой помехозащищенности на основе WB технологий	1. Распространение решений на мобильные телефоны и другие беспроводные устройства. 2. Организация производства WB микросенсоров. 3. Построение инженерно-технических, офисных и бытовых беспроводных сетей. 4. Создание заделов для новейших систем связи, навигации и позиционирования.
<b>Третий Комплексный проект</b> Разработка на основе стохастической криптографии технологии и технических средств обеспечения информационной безопасности компьютерных систем, включая реализацию параллельного криптографического сопроцессора и его программной поддержки	Подготовка документации необходимой для начала реализации проекта.  <b>Прим. автора.</b> Среди работ проводимых в рамках Комплексной программы, <b>контрастным цветом</b> выделены пункты, не требующих привлечения стохастических способов обработки.	1. Программная реализация основных криптографич. примитивов. 2. Проведение комплексного статистического, линейного, дифференциального криптографического анализа и оценки нелинейности криптографических примитивов. 3. Разработка подсистемы управления ключами компьютерных систем.	1. Унификация криптопреобразований, стандартизация алгоритмов и оптимизация аппаратных решений. 2. Разработка прототипа параллельного криптографического сопроцессора и его программной поддержки, проведение комплексных испытаний. 3. Проведение экспертизы и получение заключений.	1. Проведение на базе персонального компьютера опытной эксплуатации сопроцессора. 2. Создание библиотеки стандартных программ. 3. Распространение решений на моб. телефоны, USB-ключи и средства аутентификации. 4. Организация производства сопроцессоров.

**Таблица 2. Характеристики ожидаемого результата Комплексной программы**

<p><b>Первый Пилотный проект</b> Обоснование и разработка модели базовой интеграционной платформы автоматизированной обработки информации о состоянии материальной среды и ее элементов, поддержки высокоуровневых приложений и обеспечения безопасности</p>	<p>Создаваемая в рамках проекта технология построения адаптивной логистической сети наследует все возможности присущие общепризнанной и доминирующей на мировом рынке инфраструктуре EPC System Network и SAP, но в отличие от нее, дополнительно позволит:</p> <ul style="list-style-type: none"> <li>- Устранить неоднозначность, избыточность и/или неполноту представления данных о материальных объектах, посредством перехода от специализированных кодов EPC, к полносистемным - компактным электронным сертификатам.</li> <li>- Устранить угрозы национальной безопасности, связанные с предоставлением стратегической информации и односторонних преимуществ отдельным государствам в системе EPCglobal, путем перехода от глобальной к многоуровневой архитектуре государственного, отраслевого и корпоративного уровней управления.</li> <li>- Устранить, с введением криптозащищенной среды и сертификатов, существенный перекос в сторону логического уровня обработки, а так же кардинально разгрузить линии связи, снизить стоимость обслуживания и привлекаемого оборудования, на новом качественном уровне решить задачи по обеспечению безопасности.</li> </ul>			<p>В представленной постановке, Пилотный проект позволяет отказать от продолжающейся практики плодирования доморощенных, провальных систем, кроме пустого расходования бюджетных финансовых средств, не несущих конкретного результата. Факт, для пользователей очевидный.</p>
<p><b>Второй Пилотный проект</b> Реализация и проведение анализа бесповторных генераторов (псевдо) случайных чисел систем управления ключами высокой криптографической стойкости, предотвращения несанкционированного доступа и информационной защиты</p>	<p>Как следует из состава работ, представленных в таблице 1, главное место в Проекте занимают стохастические системы, а в них малая часть с существенно выраженным недетерминированным поведением, получившая название стохастическая криптография. Стохастические системы строятся на получившем недавно признании алгебраических системах неполной арифметики и ее предшественнице - предарифметики. Именно, уникальные функциональные, системные и стохастические свойства этих систем, сделали постановку Комплексной программы возможной. Особое место в проекте отводится бесповторным стохастическим генераторам псевдослучайных чисел. На их основе строится система управления ключами.</p> <p>Система управления ключами реализуемая в рамках Комплексной программы носит многоуровневый, глубоководный характер и позволяет добиться тотального контроля товарного рынка на основе предоставления населению индивидуальных устройств проверки подлинности и качества продукции.</p>			<p>Реализация проекта позволит на более убедительной базе снять риски, связанные с достижением необходимой стойкости к криптографическим и сторонним атакам, а также показать безусловное превосходство стохастической криптографии перед другими подходами.</p>
<p><b>Первый Комплексный проект</b> Разработка адаптивной интеграционной платформы и компонентной базы систем электронной сертификации, логистического и информационного сопровождения, контроля состояния, регламентного обслуживания и обеспечения безопасности материальных объектов и их образований</p>	<p>Изготовление микросенсора ID (контактного, бесконтактного).</p> <p><u>Аналоги:</u> ПАВ или цифровые идентификационные RF-метки, типа 64-х битовых ID-меток компании ОАО «Ангстрем».</p>	<p>Изготовление логистических контактных и бесконтактных микросенсоров.</p> <p><u>Аналоги:</u> антиколлизционные RF-метки, типа I-CODE, UCODE, простейшие платежные талоны.</p> <p><u>Для расширения функциональных возможностей,</u> микросенсоры оснащаются функциональным блоком - внешней памятью любого объема, счетчиком транзакций и/или пр.</p> <p><u>Для работы в условиях сильных помех,</u> микросенсоры оснащаются WB интерфейсом.</p>	<p>Изготовление криптозащищенных пассивных, контактных и активных бесконтактных микросенсоров, с обычным и WB интерфейсом высокой помехозащищенности.</p> <p><u>Аналоги:</u> RF-метки и смарт-карты, типа MifareDES, считывающие устройства - штатные и мобильные, включая авторизационные (по проверке подлинности подписи списка признаков) и индивидуальные средства проверки подлинности и качества продукции.</p> <p><u>Расширения:</u></p> <ol style="list-style-type: none"> <li>1. Оснащение микросенсоров функциональными блоками различного назначения (электронные кошельки).</li> <li>2. Оснащение микросенсоров типовыми мини-датчиками систем обеспечения безопасности (смарт-пыль).</li> <li>3. Сопряжение с производствен.-технологич. способами защиты. Постановка сетевой защиты сложных объектов</li> </ol>	<p>Реализация проекта позволит:</p> <ol style="list-style-type: none"> <li>1. Создать технологическую и элементную базу по своим техническим и экономическим показателям существенно превышающую мировые аналоги.</li> <li>2. Достичь на этой основе технологического паритета и превосходства, особенно в области обеспечения безопасности.</li> <li>3. Развернуть широкомасштабное внедрение логистических систем, систем управления бизнесом и обеспеч. безопасности.</li> <li>4. Начать массовое освоение беспроводных WB сетей.</li> </ol>
<p><b>Второй Комплексный проект</b> Создание технологии и компонентной базы для построения безопасных микросенсорных сетей высокой помехозащищенности</p>	<p>Представляемая проектом сверхширокополосная технология строится на основе развития управляемой, так называемой C-UWB технологии, позволяющей отказаться от дорогостоящих, низкопроизводительных и энергоемких цифровых сигнальных процессоров (DSPs), в пользу набирающей силу, недорогой, высокопроизводительной и неэнергоемкой технологии «Систем на кристалле» (SoC). Радио-интерфейсы, построенные на основе технологий UWB, по отношению к остальным, обладают следующими важными свойствами:</p> <ol style="list-style-type: none"> <li>1. Высокая помехозащищенность, позволяющая работать в условиях сильных (индустриальных) помех.</li> <li>2. Отсутствие интерференц. эффектов и невосприимчивость к переотражениям в замкнутых пространствах.</li> <li>3. Способность интеграции со стохастическими технологиями, с вытекающим новым качественным уровнем.</li> </ol>			<p>Предусмотренное проектом комплексирование микросенсорных и WB технологий закладывают основу для реализации масштабных гражданских проектов, типа «автомобиль, транспорт будущего», «умный дом, хозяйство, комплекс» и т.п.</p>
<p><b>Третий Комплексный проект</b> Разработка на основе стохастической криптографии технологии и технических средств обеспечения информационной безопасности компьютерных систем, включая реализацию криптографического сопроцессора</p>	<p>Проектом предусматривается развитие стохастических систем и вывод на новый качественный уровень построенных на их основе криптографических технологий и протоколов защиты, в расчете на перспективу развития техники, достижение такой культуры работы, чтобы устанавливаемые протоколами правила информационной безопасности, стали такими же простыми и обыденными, как правила пользования мобильными телефонами. При этом на передний план выходят технологии и задачи автоматизированного управления ключами, обеспечения информационной безопасности, погружения компьютерных, операционных и пользовательских систем в криптозащищенную оболочку, предотвращения несанкционированного доступа и действий, высокоскоростного шифрования и контроля целостности потоков информации в реальном масштабе времени.</p>			<p>Реализация предусматриваемого проектом параллельного криптографич. сопроцессора, позволит решить недоступные на сегодня задачи, связанные с защитой от нелицензионной и контрафактной продукции, частной жизни и авторских прав</p>



**Рассмотрим более подробно содержание Комплексной программы.** В таблице 2 приведены характеристики результатов, ожидаемых от реализации программы и возможные их приложения.

Обращаясь к аналитической работе проделанной на протяжении последних пяти лет для подготовки представляемых материалов Комплексной программы, с учетом мнений и замечаний, представленным ведущими специалистами Инициативы, можно сделать следующие выводы:

1. Имеющиеся заделы, глубина проработки и квалификация исполнителей, привлекаемых для работ по проекту (может быть за исключением третьего проекта, который, как планируется, получит свое детальное обоснование в рамках второго Пилотного проекта), позволят в минимальные сроки добиться поставленного результата, но при этом потребуется строгая дисциплина проведения работ и максимальное напряжение сил.

2. Разрабатываемая в рамках работ по проекту элементная и инструментальная база с избытком перекрывает все известные на сегодня аналоги и перспективные разработки (пусть нам еще предстоит устранить провалы в органической и нанoeлектронике), обладает недоступной конкурентам высокой конструктивной и функциональной гибкостью, а также способностью к интеграции и с учетом вклада, вносимым стохастическими технологиями, неизмеримым потенциалом для своего развития, отличается существенно меньшей стоимостью, высокой производительностью и малым энергопотреблением.

3. Представленные проектом информационные, электронные и радиочастотные, включая сверхширокополосные, сенсорные и криптографические технологии, гармонично дополненные стремительно развивающейся отраслью смарт-материалов и производственно-технологическими способами защиты, сбалансированы между собой и позволяют добиться небывалых по силе мультипликативных эффектов. Такое объединение технологий между собой, в единой системе представления данных и управления ключами, позволит получить качественно новые, обладающие подавляющим превосходством решения.

Создание системы обеспечения безопасности – мероприятие не из дешевых, особенно в техническом обслуживании и сопровождении.

Оптимально, если такие системы целостно (гармонично) вписываются по всей вертикали в логистические системы, системы управления производством и бизнесом, мониторинга инженерно-технической инфраструктуры и другие высокоуровневые приложения. В этих случаях затраты, связанные с обеспечением безопасности сводятся к минимуму, нивелируются или восполняются с прибылью за счет возникающих мультипликативных эффектов. В таком сочетании, идущее развитие логического уровня обработки, влечет и развитие физического уровня обработки.

В представляемой постановке, подтвержденной детальным системным анализом и проведенной своими (достаточно высококомпетентными) силами экспертизой, реализация Комплексной программы позволит за три года достичь паритета в технологической и превосходства в элементной базе, а далее, на протяжении двух-трех лет, добиться, а в последующем осуществить наращивание общего технологического превосходства. Как показывает исторический опыт, такого шанса у России не было уже в течение последних 50 лет. Но, имея такой шанс, много зависит от того, как им распорядиться.

**Комплексная программа предполагает апробацию конечных результатов.** Для этого на завершающем этапе первого Комплексного проекта планируется создание адаптивной логистической сети высокого уровня криптографической стойкости, на примере разработки прототипа и подготовки демонстрационной модели - «Обеспечение безопасности Воздушных судов и защита Авиационно-технического рынка от нелегальной продукции». Исполнители: ГосНИИАС, с привлечением специалистов НПО «Модуль», более чем с 15-ти летним опытом работ в области технологий RFID, компании ОАО «Ангстрем» и ООО «Протекшен Технолоджи».

По итогам апробации сети, планируются работы по разработке принципов распространения результатов на задачи - «Защита товарного рынка от нелегальной (контрафактной), фальсифицированной и недоброкачественной продукции», «Сертификация, автоматизированный учет, сопровождение, контроль состояния и регламентное обслуживание техники, оружия, боеприпасов и военного снаряжения». В такой широкой, системной постановке процесс реализации технологических решений, как ожидается, будет носить интенсивный характер, за счет освоения охватывающих товарный рынок и сегменты экономики взаимно дополняющих направлений, в противовес экстенсивному процессу, ориентированному на сверх затратные в целом, узкоспециализированные приложения.

Интенсивный путь развития предполагает наличие надежной опоры – для отсталых в технологическом отношении стран, как Россия, в лице цивилизованных сил государства, подкрепленных открытой и честной позицией ученых и инженеров, а для развитых стран – в лице некоммерческих ассоциаций, таких как EAN International и EPCglobal, объединяющих более миллиона компаний во всем мире, коммерческих альянсов гигантов, таких как Wal-Mart и Metro, Philips и SAP.

Эволюционный путь развития, в ответ оппонентам, ни по времени, ни по масштабности, ни по эффективности решений не может составить конкуренцию интенсивному. Этот путь обречен

на вырождение, а для развивающихся стран еще и уязвим ко всякому роду злоупотреблениям и наиболее выгоден коррумпированным кланам.

Решения представленного Комплексной программой столь широкого и масштабного круга задач, далеко опережающих уровень развития западных технологий, не одноразовый акт. Теперь, когда необходимые заделы для начала и успешной реализации программы уже сделаны, он мало согласуется с работами по совместительству, требует рассчитанной на перспективу кропотливой работы и максимально полной отдачи, объединенного общими высокими целями коллектива.

Здесь стоит отметить, что без должного вознаграждения исполнителей за такие работы, не грабительским в угоду чиновников, а справедливого и строгого соблюдения государством их авторских прав, невозможно рассчитывать на получение полновесных конечных решений.

Учитывая чрезвычайно высокую социальную, экономическую и политическую отдачу представляемых технологий, многократно превышающую низкие по мировым меркам вложения государства, в условиях процветающей коррупции и непомерно большой массы желающих поживиться за чужой счет, в отношении вносимой и создаваемой интеллектуальной собственности, наша юридическая позиция твердая. Руководствуясь существующими международными нормами, мы оставляем за собой исключительное право распоряжаться ею по своему усмотрению и решительно отвергаем любое давление от имени государства, зная, кто и что за этим стоит, вплоть до одностороннего разрыва заключенных по работам договоров.

Все это, включая порочную политику, проводимую Федеральным агентством по науке и инновациям, делают невозможным реализацию в рамках Федеральных целевых программ, выдвигаемых Инициативой задач. В ряду этих причин следует выделить:

- строго лимитированный по годам характер бюджетного финансирования, не учитывающий закупки дорогостоящего оборудования необходимого для начала работ;
- непомерные и ничем не оправданные требования по внебюджетному финансированию, когда государство получает возможность решать свои задачи за малый по мировым рыночным ценам счет;
- абсурдность самой идеи конкурса, при отсутствии достойных конкурентов не только на отечественном, но и на мировом технологическом рынке;
- кабальные условия, навязываемые чиновниками под прикрытием высоких государственных интересов по использованию вносимой и создаваемой интеллектуальной собственности в период проведения работ, противоречащие всем международным правовым нормам;
- комплексный и высоко интегрированный характер проведения работ, требующий принятия и реализации нескольких, строго согласованных по времени и срокам финансирования проектов;
- скрытое противодействие чиновников высоких рангов, вызываемое опасениями потери "левых" источников дохода и ослаблением влияния на сегменты рынка и экономики.

Похоже, последнее стало одной из причин последовавшего после нашего обращения в Минобрнауки давления на сторонников Инициативы, вплоть до прямых указаний выхода из нее. И это, не смотря на то, что этот произвол существенно затрагивает их жизненно важные интересы. По всему, тем, кто отдавал такие приказы, либо не хватает ума и прозорливости, либо нет дела не только до государственных, но и до корпоративных интересов, низменные личные мотивы и корыстные интересы высокопоставленных особ оказываются выше.

По нашему убеждению, для исключения рисков связанных с подобного рода угрозами, характерной для отечественных исполнителей низкой ответственностью и качеством проводимых работ, а также в целях сохранения накопленного потенциала для последующего коммерческого внедрения и развития технологий, требуется создание Дизайн-центра схмотехнического профиля и его современное оснащение, достаточное и направленное исключительно для эффективной реализации поставленных Инициативой задач, внедрения передовых технологических разработок и представляемых ими аппаратных решений, как на отечественных, так и на зарубежных промышленных предприятиях.

**После завершения Комплексной программы**, как это регламентируется Федеральными целевыми программами, должна последовать коммерциализация представляемых ею технологий. Как это будет дальше после завершения Комплексной программы, во многом зависит от того, в чьи руки попадут результаты работы, как эффективно ими можно будет воспользоваться, как на отечественном, так и на зарубежных рынках.

На сегодня Россия не готова принять на себя такого рода технологии, у нас нет современной конструкторской базы (Chip&Software Design), подготовленных специалистов-интеграторов и специалистов-дизайнеров по системам обеспечения безопасности, у нас нет гарантий, что деньги, отпущенные на развертывание систем, не будут в очередной раз попусту израсходованы, но это не говорит о том, что новые кадры не надо готовить и поставленные нами задачи не надо решать. Вопрос только, как? Ясно одно, что для этого необходимо мощное централизованное ядро. Но это уже специальная для обсуждения финансово-организационная тема.

Для прекращения идущих пустых пересудов и неконструктивных диалогов, **по поводу решаемых в рамках Комплексной программы задач**, хотелось бы сделать следующие, касающиеся специалистов и чиновников, пусть мало приятные и жесткие, но необходимые и вынужденные в условиях развернутого прямого давления на сторонников Инициативы, замечания:

**Во-первых**, вызывают недоумение и раздражение заявления, особенно звучащие с высоких трибун и исходящих от людей высокого ранга, при отсутствии достаточных знаний и понимания сути предмета, либо полученных понаслышке, либо высказанных по наитию и интуиции, без весомых на то оснований и имеющихся доказательств. Как вам нравится такое заявление, по отношению к радиочастотным меткам. “Вы что хотите, чтобы за вами следили?...”. После «промытия мозгов», что такие угрозы можно легко и просто технически устранить, следует более здравое заявление, что “Это дорого”. Теперь, если в этом формате обратится к тому, что происходит на мировом рынке, окажется дорого, даже очень, покупать за границей за рубли то, что у нас за копейки можно произвести. Самое страшное, что за лозунгами подобного рода чаще всего скрываются лица, готовые за мизерные дивиденды предать свою совесть и национальные интересы. И это не наказуемо и у чиновников, издевательски по отношению к своим соотечественникам, называется бизнесом. Здесь следует посоветовать всем честно и лучше делать порученную работу и воздержаться от, выходящих за рамки своей компетенции, советов другим.

**Во-вторых**, с завидным постоянством возникают «чудо аналитики», с «чудо решениями» утверждающим, что задачу защиты от не легитимной продукции можно решить на логическом уровне обработки, путем прослеживания цепей поставок. Анализ подобного рода решений по существу, показывает, что предлагаемые решения, есть с разным успехом «изуродованная» EPC System Network, с прибабасами. На какие чудеса рассчитывают горе-ученые, когда число транзакций в сети будет исчисляться миллионами, а число абонентов сотнями. Что делать, если на практике работа даже с десятью абонентами, большая проблема. Потеря и неполнота информации ведет к потере целостности цепей поставок. А, как известно из теории, системы такого рода даже в идеальных условиях, не говоря о последствиях вносимых низким качеством связи, не позволяют решить задачи защиты, а лишь выводят их на более высокий новый виток. Для полной картины осталось добавить позорный провал акции введения акцизных марок нового образца на спиртосодержащую продукцию, повлекший много миллионные потери государства и миллиардные потери законопослушных предпринимателей, за которые в очередной раз никто не ответил. (Относясь с большим уважением, в этом контексте, не постесняемся сделать предостережение на будущее компании EPCglobal). Кажущаяся простота подкупает, но нельзя забывать об уроках, о том, что “Плюшкина разорила жадность”, а своих граждан безответственное государство. Так позвольте ответить господа от науки, до каких же пор можно наступать на одни грабли и бесстыдно транжирить народные деньги. Ко всему этому представлен прекрасный сценарий для тех, кто намерится дискредитировать системы подобного рода и на этом еще хорошо заработать. Между тем, как показывают исследования, с введением криптозащищенной среды на физическом уровне обработки, система приобретает новое качество и подобного рода сценарии, уже не проходят.

**В-третьих**, еще не искоренено предубеждение, что среди производственно-технологических способов защиты (голографические, лазерные, смарт-этикетки и др.) найдутся такие дешевые, которые в течение долгого времени невозможно имитировать. Наука отвечает на этот вопрос, что это сродни созданию «вечного двигателя». Гонка продолжается, одни изобретают, другие дискредитируют. Стоимость защиты растет, время гарантированной стойкости падает. Это в полной мере относится к широко разрекламированной технологии микроточек австралийской компании DataDot, которые, как оказалось, даже в кустарных условиях легко имитируются. Тоже относится к двумерным штриховым кодам акцизных марок, которые еще, как ни крути, не читаются. Стоимость указанных средств, почти достигла стоимости меток RFID – электронных средств маркировки. Сама по себе, производственно-технологическая защита неэффективна, но может быть очень дешевой и эффективной в сочетании с электронной криптозащитой.

В продолжение этого можно упомянуть о проблемах криптозащиты, о насущности решения проблем безопасности, возможности организации тотального контроля товарного рынка со стороны населения, напомнив некоторым деятелям, радным покрасоваться на публике и подчеркнуть, на смех, свое высокое положение и административное превосходство, что задачи, решаемые при организации масштабной защиты, требуют индивидуального подхода, если хотите, своего рода искусства, а не «мобилизации населения на сбор стеклянной посуды, от защищенных от подделки вино-водочных изделий, в целях организации нелегального производства».

Если бы это было бы образовательным и воспитательным курсом, «вбивание гвоздей», в особенности в ученых пустословов и дельцов от науки, можно было и дальше продолжить. Здесь же ставилась совсем другая задача, на наиболее убедительных примерах показать, какие неприятные уроки способно преподнести нежелание учиться, недостаточно полное владение предметом и неподкрепленная знаниями интуиция, чтобы не выглядеть невеждой и не прослыть дураком, как и с каким уважением и доверием следует относиться к мнению и знаниям специалистов.

А теперь, **подошли к наиболее сложной и острой финансовой теме**, с постановкой которой, утихают фанфары и прекращают бить барабаны.

Все наши предпринятые усилия, действовать в рамках стандартных процедур, оказались напрасными, и рассчитывать на финансирование нечего.

Так, по нашим источникам, денег у Федерального агентства по науке и инновациям осталось не много и оно, со всеми вытекающими отсюда последствиями, не в состоянии профинансировать даже малую долю Комплексной программы. Нет их и в новых, принятых программах. По-видимому, нам остается надеяться на официально данные обещания, но, зная их низкую цену, больше на прозорливость и здравый смысл первых лиц государства, что на амбициозные, прорывные проекты деньги у государства найдутся.

К тому же, в очередной раз наши чиновники показали, чего они стоят. Федеральное агентство, 12 ноября 2007 года объявив о начале приема тематических заявок, по мероприятиям 1.4 и 2.4, плюнув на все и на все усилия исполнителей, вставших не дешево, толи ушло на каникулы, толи до сих пор занимается плодированием и так, непомерно больших объемов отчетных бумаг и только им понятных инструкций. Все возвращается. Развитие науки вновь диктуют чинуши, действуя как им угодно, да еще по недомыслию, неграмотности или расчету умудряются заявлять, что у нас нет прорывных решений и “нобелей”.

Теперь, если судить по несоответствующим действительности заявлениям высокопоставленных чиновников и по тому, что среди исполнителей одни и те же лица (что официально, сам же приложивший со своей командой к этому руку, подтверждает г-н А. А. Фурсенко), да и по мизерным срокам, отводимым на разработку, сравнимым с подготовкой груды ненужных отчетных бумаг, проводимые конкурсы все более превращаются в фарс, а научная новизна во внесение правок, малозначащих усовершенствований и переписывание. А что значит множество закладок, именуемых «формальными признаками», служащим не делу, а инструментом произвола чиновников, а также неполнота представляемой для исполнителей информации и практикуемые подтасовки. Позвольте зарвавшиеся господа, но это уже далеко не наука, а самое прямое выколачивание и проедание «кучкой избранных» незаслуженно выделенных денег.

В отличие от малопродуктивных подходов избранных чиновниками Минобрнауки, нами принят общесистемный подход, приносящий не эфемерный, а действительно значимый технический результат. Все проекты Комплексной программы связаны единым замыслом и предполагают строгий порядок выполнения работ и координацию планов, Учитывая не имеющий на сегодня равный, заметно превосходящими мировой, уровень разработок и планируемую отдачу, соизмеримую с отдачей высокоразвитого сегмента экономики, говорить о достойной конкуренции не только со стороны отечественных, но и со стороны лидеров мировой научно-технической школы и экономики не приходится.

В этих условиях возможны серьезные расхождения и противоречия с любыми проводимыми, превратившимися в очередной раз в фарс конкурсными мероприятиями, практикуемым внесением совместно с действительно ценными проектами, под предлогом якобы во благо развития науки, «проектов-пустышек», с равным финансированием, как одного из механизмов поборов и присвоения государственных денег, установками несоразмерно малой оплаты труда высококвалифицированных специалистов и не принимаемых в счет, вносимых ими заделов. Здесь **требуется строго индивидуальный подход**.

Если судить по решаемым задачам, то подавляющая их часть относится к компетенции государства. В этих условиях бессмысленно рассчитывать на финансирование со стороны отечественных коммерческих организаций (не в почете творимый произвол и жадность чиновников), а тем более на иностранных инвесторов.

На сегодня точки расставлены, не смотря на поступившие указания в ряд организаций о немедленном выходе из Инициативы, коренным образом противоречащих не только их собственным, но и государственным интересам. Мы не намерены торговать совестью и останавливаться. Воли и силы нам не занимать, иначе мы не взяли бы за решение столь масштабной задачи.

**Для наиболее полного понимания задач, стоящих перед участниками Инициативы, поступившим замечаниям и предложениям, требуются дополнительные пояснения.**

***Оценка состояния развития технологий, связанных с решением задач представляемых данной Инициативой, указывает на фрагментарный, функционально неполный, системно несбалансированный, противоречивый и в тоже время, явно и далеко отстающий от уровня современных требований характер решений.***

В этих условиях, не смотря на невиданную консолидацию грандов мировой экономики и поддержку торговых гигантов, привлекаемые научные силы и финансовые ресурсы, добиться революционного прорыва в области оптимизации процессов доставки и реализации продукции на

основе развития технологий RFID и их системной интеграции с информационными, логистическими и другими высокоуровневыми приложениями, как на то рассчитывали эксперты, не удалось.

Несмотря на первые всплески и последовавшей за ними на грани провала цепочка серии неудач, обусловленная, как выяснилось позже, недооценкой скрытых в технологиях RFID сложных негативных системных эффектов. Только благодаря исключительно высокой культуре организации работ (EPCglobal), достигнутого уровня развития информационных и электронных технологий и производственной базы (SAP, Symbol, Philips), это не стало препятствием устойчивому и поступательному развитию и наращиванию реальной отдачи от представляемых ими систем.

На этом фоне, признавая существенное отставание России по всем ключевым технологическим и производственным показателям от мирового уровня, усиленным узковедомственным характером разработок и разобщенностью научно-технических кадров, как показали неоднократные неудачи, рассчитывать на практически значимый результат не приходится. В итоге, все сводится к использованию, подаваемых как благо, либо тиражированию устаревших решений, причем не лучшему, за счет вносимых сторонних дополнительных ограничений и очередному повторению прошлых ошибок, ведущих к отрицательному, эфемерному техническому результату.

По горькой практике использования подобного рода разработок, движение в таком направлении не только неперспективно, но и в ущерб перспективным отечественным разработкам и производству грозит превращением российского рынка в отхожее место отживших свое технологий и второсортных решений. А это, надо напомнить всем кто ведет такую политику, кроме прямого вреда, разбазаривания или пустой траты государственных средств и интеллектуальных ресурсов, нарастания угроз безопасности, все более и более усиливающегося отставания, ничего не несет.

Вместе с тем, следует отдать должное усилиям ученых, специалистов и их достижениям, позволившим получить решения и результаты, отличающиеся функциональной полнотой и отвечающие самому высокому научно-техническому уровню, большая часть из которых принята в качестве стандартов или рассчитана на такую перспективу, а также, что не менее важно, выявить тактические и стратегические просчеты, заметным образом сказывающиеся на конечных технико-экономических показателях и ведущие к существенному сдерживанию развития технологий, например, как это имеет место для технологий RFID.

Объективно обусловленный, эволюционный процесс развития представляемых технологий и открытый характер решений, очищенный от меркантильной и политической подоплеки, позволяет совершить переход на уровень, несущественно отличающийся от мирового. Для достижения паритета необходима работа на опережение. Достижение превосходства возможно, путем внедрения прогрессивных решений и устранения просчетов, оказывающих существенное торможение развитию и распространению технологий. Последнее из положений не тривиально и требует прорывных, качественно новых решений.

Проведенные многолетние исследования и имеющиеся заделы, в части и целом, указывают на теоретическую возможность достижения паритета и технологического превосходства на основе избирательного развития и частичной модернизации имеющихся информационных, электронных, криптографических, сенсорных и коммуникационных технологий, технологий передачи данных, в особенности сверхширокополосных, технологий создания чувствительных материалов, необходимых для производства сенсорных элементов, в свою очередь используемых для построения безопасных беспроводных сетей нового поколения.

По оценке состояния развития упомянутых технологий и заключению аналитиков, теоретические достижения давно бы получили практическое воплощение, а процесс развития представляемых ими сенсорных технологий, был бы, сравним с революционным, если бы не проблемы, связанные с обеспечением действенной и рентабельной встроенной аппаратной криптозащиты микросенсорных устройств от клонирования и подделки, а для продвинутых устройств, защиты от несанкционированного доступа, шифрования и контроля целостности информации.

С получившим в последнее время развитием стохастических систем, созданием на их основе стохастической криптографии и симметричных криптографических примитивов, рассчитанных как на среды с крайним дефицитом ресурсов, так и на высокую, сверхпроизводительную обработку, сложились все условия, необходимые для придания нового качественного уровня развитию сенсорных и коммуникационных технологий. Но не только.

Указанные криптографические примитивы допускают развитие и выход на недоступные ныне новые рубежи в построение систем безопасности, автоматизированного управления ключами и сверхскоростной обработки больших по объему информационных потоков. Это дает возможность не только преодолеть проблемы и торможения связанные с отставанием криптографических технологий от современных требований, но и более того, добиться их опережающего разви-

тия, даже с переходом на нано- и квантовые уровни обработки и вычислений.

Особенно это будет заметно с разработкой криптографического сопроцессора и оснащением им вычислительных устройств и персональных компьютеров, что, ко всему прочему, позволит решить недоступные на сегодня задачи, связанные с предотвращением несанкционированного доступа и нерегламентированных действий, утечкой и разглашением конфиденциальной информацией, действенной и рентабельной защитой товарного рынка от контрафактной продукции и авторских прав, в частности на аудио, видеопродукцию, программы и литературу.

Поистине качественный переворот в коммуникационно-информационной сфере несут за собой, применимые и для высококачественных объектов, рассчитанные на массового потребителя высокорентабельные системы сверхширокополосной передачи и доступа, обладающие высокой производительностью, скрытностью и помехозащищенностью передачи данных, а с внедрением стохастических криптографических технологий, высокими регулируемыми уровнями и уникальными функциональными возможностями по обеспечению информационной безопасности.

***Для решения комплекса столь разнообразных и взаимосвязанных между собою задач, необходима консолидация сил высококвалифицированных научно-технических работников многих профилей, опытных разработчиков программного и аппаратного обеспечения, ведущих производителей микроэлектронной продукции и современных композиционных материалов, весомой и авторитетной поддержки потенциальных заказчиков и потребителей предлагаемых интеграционных решений.***

Предлагаемая консолидация сил необходима, но недостаточна. Для того чтобы приступить к началу работ и добиться реальных практических результатов, по масштабам сравнимых с образованием и становлением нового высокотехнологического сектора экономики мирового уровня, требуется стройная и прозрачная система организации работ, опирающаяся на соответствующий решаемым задачам уровень финансирования.

Добиться этого без инициативы снизу, подкрепленной четкой обоснованной программой, без участия компетентных и авторитетных лидеров способных сплотить коллектив, убедить высшие органы государственной власти и инвесторов в актуальности данных направлений развития технологий и реалистичности их высокой отдачи, не представляется возможным.

На это направлена «**Инициатива 2007**» и выдвигаемая ею, упомянутая выше Комплексная программа. Состав, особенности и порядок проведения работ, планируемый Программой, а также предполагаемый состав исполнителей, предусматриваемый научно-технический уровень разработки и ее перспективы развития, приведены в **Приложении VII**.

Как видится в ближайшей перспективе, логическим продолжением Комплексной программы может стать участие (создание) в эффективной корпорации «Информационных технологий» – ведущей технологической, системно образующей и организационно-производственной силы, направленной на становление и развитие «Информационного Общества» Российской Федерации, поддержания необходимого уровня обеспечения обороноспособности и безопасности государства.

Как следует из заложенных в Комплексную программу и имеющихся результатов, основными задачами Корпорации может стать:

1. Мобилизация интеллектуальных, материальных и финансовых ресурсы страны, направленная на становление и развитие «Информационного Общества» Российской Федерации, поддержания необходимого уровня обеспечения обороноспособности и безопасности.

2. Объединение на честной и открытой основе усилий отдельных разработчиков, творческих коллективов и производств, в целях придания нового качественного уровня развитию информационных, электронных, коммуникационных, сенсорных и криптографических технологий.

3. Проведение комплексных мероприятий, направленных на создание технической базы необходимой для решения задач обеспечения экологической, биологической и физической безопасности, защиты товарного рынка и сегментов экономики от нелегальной (контрафактной), фальсифицированной и недоброкачественной продукции.

4. Развертывание и последующее материально-техническое обеспечение Сертификационной государственной службы, по электронной сертификации товарной продукции и услуг.

5. Содействие переносу «центра тяжести» с малоэффективного ведомственного государственного надзора, на широкомасштабный действенный гражданский контроль товарного рынка и смежных с ним отраслей, путем организации производства и предоставления всем категориям потребителей индивидуальных и штатных устройств проверки подлинности и качества продукции.

6. Оказание всесторонней поддержки разработке и внедрению широко доступных высокоуровневых приложений оптимизации производственных и бизнес процессов, цепей поставок, хранения и реализации продукции.

7. Осуществление глобального мониторинга товарного и финансового рынка и сегментов экономики.

8. Создание условий для интеллектуализации и качественного улучшения уровня безопасности инженерно-технических инфраструктур, коммунальных хозяйств и жилищ.

9. Координация работ по распространению решений на задачи защиты удостоверяющих документов и национальной валюты, маркировки почтовых отправлений, архивных документов, выставочных экспонатов и содержимого библиотечных фондов, идентификации домашних животных.

10. Стимулирование развития био- и наноиндустрии через широкомасштабное производство сенситивных (смарт) материалов для микросенсоров, включая производство био- и наноэлектронных микросенсорных устройств, микросенсоров типа смарт-пыли.

11. Выработка и проведение мероприятий по устранению угроз безопасности личной жизни и здоровью граждан, идущих с внедрением микросенсорных устройств и нанотехнологий.

12. Организация противодействия и контр противодействия внешним и внутренним угрозам информационной безопасности.

13. Демонопользации рынка и придания максимальной информационной прозрачности программным средствам, в первую очередь сетевого взаимодействия, посредством проведения ревизии поставляемой продукции, изъятие закладок или замена приложений, осуществление последовательного перехода на открытые программные коды.

14. Вывод на новый качественный уровень криптографических технологий и протоколов защиты, рассчитанный на перспективу развития техники, выработка и проведение технических мер, пропаганда высокой культуры работы в условиях несанкционированных действий и рисков деструктивных атак.

15. Координация работ по распространению решений на новейшие банковские системы, системы мобильной и стационарной связи, навигации и позиционирования, кабельного и спутникового телевидения, телекоммуникационные и радиолокационные системы, системы опознавания, радиоэлектронной борьбы, управления войсками и подразделениями на поле боя.

16. Реализация масштабных гражданских проектов, таких как «автомобиль, транспорт будущего», «умный дом, хозяйство, комплекс» и т.п.

17. Осуществление сертификации программного обеспечения и аппаратных средств.

18. Организация тесного международного сотрудничества, в первую очередь с ближайшими стратегическими партнерами, формирование новых секторов, наращивания присутствия на мировом рынке высокотехнологичной продукции и услуг.

***Идеи, заложенные в Комплексной программе, а именно, предарифметика, алгебраические системы неполной арифметики, стохастические системы и криптография, форматы представления данных, управление ключами, микросенсорные функциональные модули и их сопряжение с сенситивными элементами, управляемая сверхширокополосная технология (C-UWB) и планируемое ее развитие, подходы построения беспроводных сетей и их интеграция с системами высокоуровневой обработки, организации защиты товарного рынка и сегментов экономики от нелегальной и недоброкачественной продукции, а также решения других задач обеспечения безопасности, отличаются новизной, носят фундаментальный, реалистичный и мультипликативный, а преследуемые ими цели прорывной, высокорентабельный и социально направленный характер.***

Как видим, идей более чем предостаточно и каждая из них значима, а первые из них особо для последующего развития математики, физики и естествознания. По наивности помыслов и здравому смыслу смели надеяться, что идеи найдут понимание и финансовую поддержку и это несколько поможет поправить униженное положение, когда по выражению Виктора Зубкова на заседании правительства посвященному развитию наноиндустрии “денег больше чем идей”, а также позволит опровергнуть неоднократные укоры Андрея Фурсенко, что российские ученые топчутся на месте и не берутся за амбициозные проекты, хотя на них есть деньги.

На самом деле выяснилось, что «денег нет» в Федеральном агентстве по науке и инновациям. Нет их и в Федеральной целевой программе «Развитие электронной компонентной базы и радиоэлектроники на 2008 - 2015 годы». К тому же, при нашем прямом обращении к господину Фурсенко, ко всему этому еще оказалось, что нет денег не только в возглавляемом им министерстве, но и чиновникам министерства нет ни малейшего дела до подобных программ.

В этой связи, увлекшимся прокладыванием «светлого пути» чиновникам от науки, при этом далеких от сути предмета, на что указывают принимаемые ими решения и конкретные результаты, полезно будет напомнить, по мнению экспертов, сверхширокополосные технологии и технологии RFID в широком их понимании, поставлены на первых два места, как одни из прорывных техно-

логий XXI века. На 2008 год экспертами CNN уже заявлены нано-радио-чипы.

А что же мы видим в нашей реальной действительности. Сверхширокополосным технологиям не нашлось места. На идентификационные технологии, словно в насмешку для цифровых (см. таблицу), выделены средства, но только на узкоспециализированные, построенные на основе поверхностных акустических волн (ПАВ), и то благодаря героическим усилиям ИРЭ РАН.

Мероприятия		2008 - 2015 всего	В том числе: бюджет/внебюджет					Ожидаемые результаты
			2008	2009	2010	2011	2012 - 2015	
43	Разработка базовых технологий микроакусто-электромеханических систем	<u>155</u> 100	<u>110</u> 70	<u>45</u> 30				создание базовых технологий (2009 год) и комплектов необходимой технологической документации на изготовление микроакусто-электромеханических систем, основанных на использовании ПАВ (диапазон частот до 2 ГГц) и объемно-акустических волн (диапазон частот до 8 ГГц), пьезокерамических элементов, совместимых с интегральной технологией микроэлектроники
99	Разработка в лицензируемых и нелицензируемых международных частотных диапазонах 860 МГц и 2,45 ГГц ряда радиочастотных пассивных и активных акустоэлектронных меток-транспондеров, в том числе работающих в реальной помеховой обстановке, для систем радиочастотной идентификации и систем управления доступом	<u>120</u> 80		<u>21</u> 14	<u>48</u> 32	<u>51</u> 34		создание технологии и конструкции акустоэлектронных пассивных и активных меток-транспондеров для применения в логистических приложениях на транспорте, в торговле и промышленности (2010 год, 2011 год)  (так не пишут, <b>метка-транспондер...</b> )
137	Разработка базовых технологий создания рядов унифицированных электронных модулей процессоров, скоростного и сверхскоростного ввода-вывода данных, шифрования и дешифрования данных, интерфейсов обмена, систем сбора и хранения информации, периферийных устройств, систем идентификации и управления доступом, конверторов, информационно-вычислительных систем	<u>3285</u> 2190	<u>60</u> 40	<u>105</u> 70	<u>105</u> 70	<u>540</u> 360	<u>2475</u> 1650	создание на основе современной и перспективной отечественной электронной компонентной базы унифицированных электронных модулей широкой номенклатуры для применения в различных информационных системах, в том числе унифицированных электронных модулей шифрования и дешифрования данных; разработка базовых технологий и конструкций унифицированных электронных модулей на ПАВ систем радиочастотной и биометрической идентификации, систем идентификации личности, транспортных средств, электронных паспортов, логистики, контроля доступа на объекты повышенной безопасности, объектов атомной энергетики. В создаваемых унифицированных электронных модулях будет обеспечена скорость обмена и передачи информации до 30 Гб/сек.

В разделе программы «Обеспечение создания и производства средств радиочастотной идентификации» читаем, что с использованием подобных технологий можно выпускать менее сложные микросхемы, например электронные метки для товаров и грузов (по экспертным оценкам, потребность в них в 2007 году может достигнуть 250-400 млн. штук). Кто их видел у нас в 2007 году, да и какие метки имеют ввиду, крайне специализированные ПАВ-метки, по сравнению с цифровыми радиочастотными метками, мало пригодными как для логистики, так и торговли?...

По криптографическим средствам, ситуация еще более плачевная, в особенности если учесть, что операционная система Windows (и это уже не скрывается), превратилась в крупнейший вирус и создание с этим 18 сентября 2007 года Госдепартаментом США 25 тысячного контингента для ведения киберсетевой войны, и то, что основные вложения идут на 2011-2015 годы, в расчете, авось, там все переменится.

Ситуация еще больше осложняется тем, что на основе существующих стандартных симметричных криптографических примитивов, в силу их крайней ограниченности и низкой производительности, эффективную и рентабельную защиту от новых вызовов угроз безопасности, не построишь.

Последним аккордом в разъяснении нашей позиции, в ответ на дружественные поцелуи подсаженных в Массачусетс провокаторов, идеологов проводимого в интересах западных стран



глобализма, должно было стать разъяснение на накопленном опыте близорукой позиции, о возможности ощутимого и масштабно значимого для экономики развития технологий RFID, построенных не только на основе аналоговых ПАВ-меток, но и на основе других, незащищенных от клонирования и подделки средств маркировки, включая самые современные – радиочастотные метки Gen2. Как видится, такое будет возможно в перспективе для антивандальных систем, но только в сочетании цифровой и аналоговой обработки, когда, при разрушении встроенной электронной защиты, по очень дешевым и устойчивым к сторонним воздействиям ПАВ-элементам, успевают отработать логистические протоколы. При этом добиться низкой стоимости ПАВ-элементов можно будет на основе тонкопленочных материалов и печатных технологий, тем более что такие материалы уже разработаны, да и подобные принтеры уже существуют.

На просчетах надо учиться, требуется строгий системный анализ всех вариантов и выработка решений, очищенных от совершенных в прошлом ошибок. При этом следует помнить, особенно сторонникам узкоспециализированных ПАВ технологий, что условия диктует потребитель, а не поставщик, тем более не способный с необходимым качеством удовлетворить его требования, иначе все, какое бы оно не было в своей основе научно блестящим и технически замечательным, окажется выброшенным.

Здесь также необходимо отметить, что сложность утилизации и приведения в неработоспособное состояние отработанных ПАВ-элементов, как уже было с цифровыми, вступает в серьезное противоречие с требованиями правозащитников о недопустимости слежки. По опыту внедрения цифровых технологий, наличие такого рода угроз может привести к серьезному торможению развития аналоговых технологий, вплоть до запрета.

***Оценивая в целом положение дел, вот так бездарно и безответственно, а по некоторым позициям просто преступно, в угоду западным спецслужбам, политическим провокаторам и коррумпированным кланам планируем свои действия, стремимся в неизвестно какое «Информационное Общество», рискуем потерять контроль над своим информационным пространством и навсегда попасть в полную зависимость стран с высококоразвитой экономикой.***

На чем мы строим свою политику и на что мы рассчитываем? Так кто, за граница, быть может, компания Philips начавшая осваивать наш микроэлектронный рынок RFID, либо другие, несущие прямые или скрытые угрозы национальной безопасности государству, в беде нам поможет...

**Только в кошмарном сне может привидеться, что все системы безопасности в нашем «светлом будущем» будут иностранного производства, а все их жизненно важные элементы помечены иностранными марками.**

Будем надеяться, что чувства здравого смысла и самосохранения преобладают. Пока Инициатива еще действует и не разгромлена продажными чиновниками и ненасытными кланами, не все безвозвратно потеряно, и все можно поправить.

Заглядывая в будущее, с открытием предарифметики, предшествующей известной нам классической арифметике порождаемой в великой гармонии поведения систем, получают развитие алгебраические системы неполной арифметики и стохастические системы. Являясь предметом самостоятельных фундаментальных исследований, они способны выступать в качестве новой научной базы не только для криптографии, благодаря которой вообще стало возможной постановка представленных выше задач, но и для дальнейшего развития математики, физики и естествознания в целом.

***Если последовать изречению «Математика – царица наук. Арифметика – царица математики», то только с мудростью и чистыми помыслами откроется наш мир по другому. А то, что в этом есть огромная доля истины, уже сейчас указывают многие реалии и существующие аналогии. Проведение исследований в этой полной тайн зарождающейся и столь малоизвестной области – отдельная тема, которая ждет своих первопроходцев и «нобелей».***