Россия, «Инициатива 2011»

(ПРОЕКТ)

Стохастические технологии.
Инновационный прорыв в криптографии и обеспечении безопасности

Развитие и интеллектуализация логического уровня обработки, освоение технологий радиочастотной идентификации (**RFID**), бесконтактных микросенсорных технологий, становление систем расширенного Интернет и зарождение его разновидностей – Интернет «Вещей», «Медицинский», «Экологический» Интернет и представляемых ими «Облачных» технологий, начатая с ними и с выходом на нано уровень обработки глубокая системная трансформация, направленная на ***качественное обновление и завоевание физического уровня обработки*** – процесс новый, обладающий неисчерпаемым потенциалом, стремительно развивающийся и сопровождающийся, независимо от системных кризисов и потрясений, неизмеримо высокой отдачей во всех сферах деятельности человека [1]. В этих условиях привносимые в этот инновационный процесс прорывные решения и технологии, на примере Китая, стран ЕС, США, Ю. Кореи, Японии, Австралии, Индии и других, интенсивно развивающихся в технологическом отношении стран, являются предметом особой, ревностно оберегаемой гордости и заботы, приоритетной и полноценной поддержки и финансирования со стороны государства, создания наиболее привлекательных и благоприятных условий для развития бизнеса и вложения капитала.

Между тем, как показывает опыт и практика, освоение физического уровня обработки – это крайне сложный, взаимосвязанный с логическим уровнем, внутренне противоречивый процесс. С одной стороны, развитие физического, а с ним и логического уровня обработки, ведет к глубокой, взаимно обусловленной, качественной перестройке научно-технического, экономического и социального базиса, а с другой, к резкому обострению, оказывающих существенно сдерживающее влияние на эти процессы, непредсказуемых по последствиям и масштабам угроз безопасности, идущих по нарастающей с падением нравов и пренебрежительным отношением к природе. В этом отношении поучителен и показателен факт, когда, несмотря на развернутую по всему миру мощную рекламную акцию, процесс внедрения и распространения технологий RFID, в некотором смысле отражающим нравственное лицо современного общества, пошел по экстенсивному, эволюционному пути развития, а не по интенсивному, революционному, как полагали эксперты в начале тысячелетия.

Обращаясь к истории, по замечанию кардинала Ришелье, «***Безопасность*** – ***это категория неизмеримо более высокая, чем величие***», о чем в угоду скоропалительной выгоде беззастенчиво забывают, либо решение проблем обеспечения безопасности безответственно откладывают на потом, либо, руководствуясь политическими или меркантильными интересами, этими проблемами пренебрегают, либо отказываются от решения этих вопросов, прикрываясь оправданиями о непомерно высокой стоимости и существенном отставании средств обеспечения безопасности от уровня развития техники. И это притом, что в условиях проходящей в системной области научно-технической революции, особенно в информатике, электронике и сетевой обработке, задачи своевременного и адекватного противодействия идущим с ними угрозам и вызовам безопасности играют решающую, все более значительную и важную роль. Иное, как прозорливо и дальновидно учит практика и история, ведет к деструктивным и крайне негативным, фатальным последствиям и потерям, затрагивающим жизненно важные интересы, благополучие и социальное здоровье всех слоев общества.

Иными словами, ***задачи обеспечения безопасности приобретают все возрастающую, особо важную роль***, обусловленную такими доминирующими факторами, как:

- беспрецедентный рост производства и распространения фальсифицированной продукции, рост масштабов реализации недоброкачественной, не сертифицированной и нелицензионной продукции, увеличение числа противоправных действий в информационном и коммуникационном пространстве, а также числа финансово-экономических преступлений, краж, грабежей и угонов,
- вхождение в норму приобретающей все более угрожающие масштабы порочной практики жульничества, мошенничества, манипуляций и обмана в цепи производства и реализации продукции и услуг, обусловленное неуклонным падением эффективности существующих механизмов и отсутствием отвечающих вызовам действенных и рентабельных инструментов контроля товарного рынка со стороны инспекционных органов и потребителей,

♦ продолжающаяся глобализация информационного пространства и передача ключевых функций контроля и управления автоматизированным и роботизированным системам, как данное системной интеграции и кумулятивных эффектов, создающих предпосылки утраты существенно значимой информации и лавинно распространяющегося разрушения сетевых и инженерно-технических коммуникаций и инфраструктур,

♦ ведущиеся попытки завоевания односторонних преимуществ, осуществляемых посредством достижения технологического превосходства в стремительно развивающемся и милитаризируемом киберпространстве, наращивание политического давления, прямых и скрытых кибер-угроз, внесения потаенных закладок, недобросовестной конкуренции, активного продвижения устаревших и усиленной пропаганды низкосортных и ущербных решений,

♦ опережающий рост технической оснащенности криминальных элементов, антисоциальных сообществ и террористических групп,

♦ совершенствование способов взлома криптозащиты систем и их составляющих элементов, расширение масштабов и возможных направлений проведения деструктивных атак и фатальных воздействий.

На качественно новом и действенном уровне, высоко рентабельно и эффективно ***решить ключевые проблемы в области обеспечения безопасности стало возможным*** благодаря решениям и заделам, полученным в результате новаторской деятельности развернутых в точках инновационного роста лабораторий и центров RFID, обязанному **Auto-ID Labs** становлению и развитию концепции **EPCglobal** и привносимых ею стандартов и архитектур интеграционных платформ, а также благодаря достижениям в радиотехнике, материаловедении и микроэлектронике (**NXP Semiconductors** - Philips, **Hitachi**, **PolyIC** - Siemens), в системном анализе и прорыву, совершенному на основе открытий в области алгебры [2], развитию нового, рассчитанного на необозримую перспективу инновационного направления – «***Стохастические технологии***» [3].

С введением секретных ключей стохастические технологии, тесно примыкающие к «идеальному» хаосу свойственному природе, как и создаваемые на их основе изделия и продукты, отличающиеся непомерно функционально сложным и статистически непредсказуемым поведением, переходят в криптографические. При этом следует различать специфику проблем обеспечения информационной безопасности на логическом уровне, обострившихся с внедрением автоматизированных информационных систем, и проблем обеспечения безопасности на физическом уровне обработки. Последнему, относящемуся к истокам развития и до сих пор мало изученному направлению, не только более сложному и проблематичному, но и чрезвычайно социально опасному, разрушительному и непредсказуемому по последствиям и масштабам охвата, отводится ведущая роль.

Стохастические технологии строятся на основе динамических систем дискретного времени, носят естественно научный, фундаментальный и открытый характер, рассчитаны на самый широкий круг технических исполнителей. Такая, опирающаяся на общие ценности постановка, позволяет со временем отказаться от существующих на сегодня порочных догматов, запретительных норм и заслонов, ведущих к научному застою и технологическому вырождению, бюрократическому и властному диктату и произволу, к присвоению особого права на непреложную истину и кастовую исключительность привилегированных научных и государственных институтов, спецслужб и представляющих их монополий. Стохастические технологии охватывают все разделы современной симметричной криптографии и связанные с ней приложения, рассчитаны на бессрочную перспективу, открывают безграничные возможности и новые направления в области теории систем, статистического моделирования и обеспечения безопасности, имеют подавляющее *превосходство по всем показателям перед существующими аналогами* [4].

Вопреки предостережениям специалистов по безопасности, предупреждениям социологов и заявлениям правозащитных организаций, угрозы, привносимые внедрением и развитием широко афишируемых технологий RFID, без соблюдения соответствующих мер безопасности, могут привести к самым печальным социальным последствиям. Об этом по корыстным мотивам умалчивают, либо кичатся, вследствие невежества или безграмотности, а чаще банально обманывают, заверяя, якобы технологии RFID не несут в себе угроз безопасности и более того, способны эффективно противостоять этим угрозам. В этом плане, общее мнение аналитиков таково – без встроенной защиты меток RFID от подделки, сколь совершенно не был бы устроен логический уровень обработки и связанные с ним логистические протоколы, устранить угрозы безопасности идущие с развитием физического уровня обработки – задача недостижимая.

В тоже время, несмотря на предпринимаемые усилия, в условиях крайнего дефицита отводимых ресурсов, *решить задачи полноценной защиты элементов систем от подделки*, таких как радиочастотные (**RF**) метки RFID, на сегодня и в ближайшей перспективе, даже с переходом на нано уровень обработки, ***не представляется возможным***. Определенно, в некоторой мере это является одной из причин, постоянно всплывающих и пропагандируемых мифов о безопасности технологий RFID. Собственно, это прямо и косвенно подтверждается информацией публикуемой на сайтах компаний и в прессе, экспертными группами, включая такие авторитетные, как **IDTechEx**, и, конечно, результатами масштабной, 13 миллионной (в евро) Европейской программы **BRIDGE**, всецело опирающейся на криптографические сообщества **RFIDSec** и **ECRYPT** и привносимые ими научные исследования и технические разработки. По всему, для преодоления столь нетривиальных проблем, требуются принципиально новые решения и подходы. В отличие от известных аналогов, такими исключительными возможностями сегодня обладают лишь базирующиеся на предарифметике стохастические технологии [3].

Предоставляемая на основе стохастических технологий действенная, эффективная и рентабельная ***защита элементов систем от клонирования и подделки*** (меток **RFID**/**EPC** и микросенсоров, кремниевых и органических, фактически ***не приводящая к увеличению их себестоимости и энергопотребления***), позволит последовательно, фактически на любой имеющейся технологической и промышленной базе (см. 3-х центовый прототип – RF-метка **I-Code** H4100, 1.2 μm, ОАО «**Ангстрем**»), при минимальных затратах (на порядок меньших 13 миллионов, израсходованных на так и не достигшую поставленных целей, сосредоточенную на перспективном, 5-ти центовом прототипе **EPC Gen2** 0,18μm, программу BRIDGE) и в сжатые сроки разрешить упомянутые выше проблемы [5]. Действительно, как показывает предварительная комплексная экспертиза [6], представляемая частными – общесистемными (МИФИ, МНИИ «Интеграл»), техническими (ОАО «Ангстрем», ООО «Анкад») и криптографическими («ЛАНКрипто», МИФИ) экспертными заключениями, опирающаяся на закрепленные в заявках на изобретения [7] общие методологические положения [3,8], и подкрепленные ноу-хау, полнофункциональные, предусмотренные для промышленной реализации результаты [4], стохастические технологии позволяют решить следующие прикладные задачи:

1. Защита продукции и изделий от фальсификации и подделки, распространение решений на задачи проведения денежных расчетов и платежей, дистанционной оплаты услуг, регламентирование доступа и организации пропускного режима, защиты удостоверяющих документов и валюты, маркировки почтовых отправлений, архивных документов, выставочных экспонатов и содержимого библиотечных фондов, идентификации домашних животных и прочие.
2. Осуществление высокорентабельной защиты составных и сложных объектов (от простых упаковок и входящих в их состав элементов, до агрегатов, их узлов и деталей), посредством комплексирования электронной защиты, с дешевыми производственно-технологическими способами, от простых номерных этикеток до лазерной гравировки, распространение технологий на сектора экономики (фармацевтика, транспорт и др.).
3. Вывод систем контроля качества продукции и мониторинга состояния внешней среды, а с ними и систем обеспечения экологической, биологической, физической и инженерно-технической безопасности на качественно новый уровень, за счет оснащения радиочастотных меток и микросенсоров многопрофильными чувствительными мини-датчиками, построенным на основе смарт-материалов, представляемых современной био- и наноиндустрией.
4. Создание, по мере освоения помехоустойчивых многоканальных широкополосных и акустических радиочастотных технологий, систем охраны жизненно-важных объектов, жилищ и строений, защиты распределенных инженерно-технических инфраструктур от несанкционированных действий в условиях индустриальных и преднамеренных электромагнитных помех.
5. Системная интеграция с передовыми высокоуровневыми решениями организации бизнеса, например, с такими как SAP и HP, освоение технологий нового поколения, идущих с развитием адаптивных технологий интеграции элементов систем, таких как, интеллектуальные здания, коммунальные хозяйства и комплексы, интеллектуальные жилища (умные дома), площадки и кооперативы.

Одним из определяющих моментов решений является введение высокоэффективной (производительностью десятки млрд. ключей в секунду), централизованной системы управления ключами, а с ней, предоставление всем категориям потребителей штатных и индивидуальных средств проверки подлинности и качества продукции и изделий, а именно

- дешевых карманных и мобильных автономных устройств прямого контроля, а также локальных и высокоуровневых сетевых встраиваемых модулей и приставок, в частности, для компьютеров и телефонов.

С налаживанием широкомасштабного производства указанных средств становится возможным ***привлечение широких слоев населения к организации тотальной защиты сегментов национального и мирового товарного рынка и экономики от нелегитимной и недоброкачественной продукции***. В этом отношении показателен пример стремительного развития, освоения и отдачи мобильных технологий **NFC** (Near Field Communication, Nokia).

Ко всему этому, стохастические технологии допускают простую и эффективную реализацию ***физических неклонируемых функций*** (Phisical Unclonable Function, **PUF**), воплощаемых в физической структуре микросхем посредством случайных вариаций задержек в проводниках и затворах транзисторов. Такие функции могут быть полезны для реализации

- высококачественных генераторов истинно случайных чисел (**RNG**), используемых в составе сверхширокополосных устройств, микросенсоров и RF-меток для разрешения коллизий и поддержки вероятностных криптографических протоколов аутентификации, в отличие от известных на сегодня подходов, с гарантированно-доказуемой надежной статистикой и криптографической стойкостью, а также осуществления встроенной зашиты памяти микрочипов от прямого проникновения, постановки заградительных помех и прочих технических приложений.

Как видится в ближайшей перспективе, по мере апробации и освоения стохастических технологий, а также представляемых ими криптографических примитивов, как и подобает в случаях наличия безусловного превосходства привносимых ими решений, станет возможным ***создание дешевых, высокоэффективных, миниатюрных и энергоэкономичных криптографических средств и параллельного криптографического сопроцессора***, производительностью в тысячи и сотни Гбит в секунду, соответственно. Внедрение указанных средств ***позволит снять проблемы отставания криптографических технологий от уровня развития техники***, а с этим пойти дальше и при сравнительно меньших общих затратах и видимого уменьшения производительности компьютерных, информационно-коммуникационных, телевизионных и спутниковых систем, средств связи, позиционирования и навигации, на качественно новом уровне решить задачи

- обеспечения информационной безопасности, предотвращения массированных кибер-атак, прямых и скрытых кибер-угроз, несанкционированного доступа и нерегламентированных действий, защиты авторских прав, в частности на аудио- и видео-продукцию, программы и литературу.

Решение представленных выше задач предполагается на основе «***Концепции обеспечения безопасности***», исходящей из развития информационных и беспроводных технологий, микросенсорных (RFID) и кибер-сетевых технологий, выработанной при непосредственном участии иностранных компаний (EPCglobal, Philips, Intel, HP, SAP, Panda) российскими учеными и инженерами в рамках программы – «**Инициатива 2007**» [9], а также на основе полученных к настоящему времени результатов, отражаемых в данном документе обновленной и принимаемой для последующих действий и руководства программе – «**Инициатива 2011**», подкрепляемой мировым опытом и последними новейшими, далеко опережающими мировой уровень фундаментальными и прикладными научно-техническими исследованиями и разработками [10].

В целях перевода в практическую плоскость отраженных в Концепции научно-технических достижений и ликвидации просчетов вызывающих существенное торможение распространению и развитию электронных систем, ***предлагается объединение усилий*** в модернизации системы EPCglobal и интеграции с наиболее перспективными высокоуровневыми приложениями организации бизнеса, выводе технологий RFID, представляемых наиболее перспективными радиочастотными метками – **UCODE**, **EPC Gen2**, **µ-Chip**, а вслед за ними микросенсорных технологий, технологий производства смарт-материалов и технологий обеспечения безопасности в целом, как и предсказывают эксперты, на уровень, сравнимый с революционным.

В такой расширенной постановке, ***представляемые технологии по масштабам, отдаче и значимости становятся сравнимы с высокоразвитым сектором экономики***, по важности выходят на национальный и межгосударственные уровни, позволяя *занять лидирующее положение в мире* в сфере обеспечения безопасности, в первую очередь, в разработке и производстве криптографических средств, необходимых для устойчивого и динамичного развития физического и логического уровней обработки.

Ко всему, последующее развитие стохастических технологий ведет к совершенствованию методологической базы, предполагает развитие, унификацию и стандартизацию математических методов и подходов криптографического анализа создаваемых на их основе приклад-

ных приложений. В свою очередь это позволит достичь оптимального сочетания криптографической стойкости и дизайна программных и аппаратных решений, а также существенно уменьшить затраты на экспертизу, сертификацию и лицензирование промышленных образцов.

Очевидно, для решения представленных в документе первостепенных задач, налаживания связей и привлечения инвестиций, организации бизнеса, научно исследовательских и совместных работ, проведения рекламных компаний для вхождения в рынок и интеграции в мировое сообщество ***требуется создание, действуя на шаг впереди,*** **Российского центра** *«***Микросенсорных Технологий***», а с ним и лаборатории, типа* **Auto-ID**.

Заглядывая в ближайшее будущее, с развитием производства сенситивных (смарт) материалов и элементной базы наделенной интеллектуальными функциями, и технологий их адаптивной сетевой интеграции, неотвратимо, ***на смену технологиям RFID идут микросенсорные и*** «***Облачные***» ***технологии***, ***а вслед за ними локальные и глобальные кибер-сети***, построенные на основе помехоустойчивых сверхширокополосных (**UWB**) и беспроводных (NFC, Bluetooth, Wi-Fi, ZigBee) технологий, наземных (GSM, CDMA) и спутниковых (GPS, ГЛОНАСС, Galileo, Běidǒu) систем.

Как показывают исследования и прогнозы, кибер-сети покроют и закономерно завоюют весь мир, от систем мониторинга состояния внешней среды, жилищ, кошельков и валюты, до технических и инженерных систем, производственных комплексов, медицинских учреждений и земельных угодий, проникнут на более глубокие материальные уровни. В условиях вносимых ими потенциально опасных и прямых кибер-угроз, не изжитых великодержавных амбиций во взаимосвязанном мире, разрушения и загрязнения среды обитания живых организмов и нарастания масштабов распространения опасной для здоровья человека продукции, разрастания терроризма и высокой технической оснащенности криминала, ***решения положенные в основу упомянутой выше Концепции, ко всему, способны стать основой прорыва в области информационно-коммуникационных технологий***, ***а с ними, надежным подспорьем и действенным инструментом обеспечения государственной безопасности стран, безопасности граждан и безопасности ведения бизнеса***.

Более полную информацию по упомянутым в этой обширной программе, в первую очередь обязанной открытиям в области алгебры**,** обоснованию следующих из них стохастических технологий и прорыву в криптографии, а также по техническим вопросам и состоянию дел, можно найти в прилагаемых источниках информации и на тематическом сайте: random-art.ru

В расчете на долгосрочную перспективу и снятие рисков, сохраняя преемственность разработок при движении от простого к более сложному, ***в качестве первого шага*** реализации упомянутой выше Концепции и Программы, предлагается участие в коротком, относительно незначительным по инвестициям и отличающимся высокой отдачей, в сравнении с ведущимися сегодня в мире аналогичными разработками, паритетном проекте – «***Обоснование реализации минималистских протоколов аутентификации дешевых идентификационных радиочастотных меток***» [11].

Цель проекта. Обоснование реализации действенной, высоко рентабельной (без увеличения себестоимости производства) и энергоэкономичной (без уменьшения радиуса действия) встроенной электронной защиты от клонирования, имитации (эмуляции) и подделки дешевых кремниевых и органических, не перезаписываемых (типа **RO**), идентификационных радиочастотных меток (RF-меток **ID**).

Согласно расчетам [4], общие аппаратные затраты, требуемые для реализации Протоколов аутентификации построенных на основе стохастических технологий составляют порядка 150-200 GE, что в 15-20 раз меньше чем у аналогов, построенных на основе известных криптографических примитивов (AES-128/3400 GE, TEA/2633 GE, Trivium/3091 GE, Grain/3360 GE). Ко всему, предлагаемые сегодня ***легковесные криптографические примитивы аутентификации*** тоже не в состоянии оказывать сколь ни будь серьезную конкуренцию, так как для своей реализации, пусть и требуют в несколько раз меньше логических элементов, порядка 1000 GE (KTANTAN48/588 GE), но при этом требуют большое число раундов 48 и более, ведущих к ощутимым затратам энергии от внешних источников. К этому, для общей убедительности можно добавить, что широко распространенные, мало затратные примитивы аутентификации, такие как A3/A5 и Crypto-1, используемые в системе GSM и в бесконтактных картах Mifare Classic, как и их многочисленные предшественники, опирающиеся на поля Галуа, уже дискредитированы по криптографическим свойствам и показателям.

Потенциальные потребители результатов – ведущие российские и иностранные производители меток RFID (Ангстрем, Ситроникс, а также Hitachi, NXP Semiconductors, PolyIC) и крупные системные интеграторы (Систематика, РосНаноТех, а также EPCglobal, Symbol, IBM, HP, Philips, Siemens, Nokia, SAP, Microsoft) и др.

Игорь А. Кулаков

E-mail: art@istra.ru
Tel: 8-496-312-81-50
http://random-art.ru/

Источники дополнительной информации

1. И. А. Кулаков. **Предпосылки инновационного прорыва России**.
   Рукопись статьи, Москва, январь 2011,
   http://random-art.ru/?download=Predposylki_innovacionnogo_proryva_Rossii.pdf
2. И. А. Кулаков. **Гипотеза о природе Арифметики**.
   Рукопись статьи, Москва, октябрь 2011,
   http://random-art.ru/?download=gipoteza_o_prirode_arifmetiki.pdf
3. И. А. Кулаков. **Стохастические системы и криптография**.
   Рукопись статьи по материалам конференции «РусКрипо 2006», Москва, ноябрь 2011,
   http://random-art.ru/?download=DhSqn_Gen
4. **Аспекты реализации стохастических технологий**.
   Методические материалы, «Инициатива 2011» Москва, ноябрь 2011,
   http://random-art.ru/?download=RM_Tab.pdf
5. **Концепция построения и реализации «Расширенного Интернет»**.
   Методические материалы, «Инициатива 2007» Москва, ноябрь 2008,
   http://random-art.ru/?download=Koncepcija_IKT.pps
6. **Общее экспертное заключение**.
   Проект, «Инициатива 2007» Москва, август 2008,
   http://random-art.ru/?download=Akspertiza.pdf
7. **Рандомизационный способ**.
   Заявки на изобретения, октябрь 2011,
   http://random-art.ru/sitemap/randomizacionnii-sposob/
8. И. А. Кулаков. **Стохастическая криптография. Дихотомические последовательности**.
   Рукопись статьи, Москва, декабрь 2011,
   http://random-art.ru/?download=Dh_Sqn_New.pdf
9. «**Инициатива 2007**». Москва, апрель 2008,
   http://random-art.ru/?download=Iniciativa_2007.pdf
10. И. А. Кулаков. **Концепция обеспечения безопасности. Проблемы и решения**.
    Рукопись статьи, Москва, январь 2011,
    http://random-art.ru/?download=Koncepcija_obespechenija_bezopasnosti.pdf
11. **Обоснование реализации минималистских протоколов аутентификации RF-меток ID**.
    Пилотные проекты, «Инициатива 2007» Москва, февраль 2011,
    http://random-art.ru/?download=proect.pdf