Многоуважаемые коллеги,

Развитие и интеллектуализация логического уровня обработки, освоение технологий радиочастотной идентификации (RFID), становление Интернет и зарождение его разновидностей – Интернет «Вещей», «Медицинский» и «Расширенный» Интернет, начатое с ними массированное наступление на освоение физического уровня обработки, а также намечаемая их глубокая системная трансформация с выходом на нано уровень обработки – процесс сложный и внутренне противоречив.

С одной стороны, это ведет к глубокой качественной перестройке экономических и социальных отношений, а с другой, к нарастанию и резкому обострению угроз безопасности.

Задачи обеспечения безопасности приобретают все возрастающую, особо важную роль, обусловленную следующими факторами:

- беспрецедентный рост производства и распространения фальсифицированной продукции, рост масштабов реализации недоброкачественной и несертифицированной продукции, увеличение числа краж, грабежей и угонов,
- продолжающаяся глобализация информационного пространства и передача ключевых функций контроля и управления автоматизированным и роботизированным системам,
- ведущиеся попытки завоевания односторонних преимуществ, осуществляемых посредством технологического давления, прямых и скрытых кибер-угроз, внесения скрытых закладок, активного продвижения и усиленной пропаганды ущербных решений,
- опережающий рост технической оснащенности криминальных элементов,
- совершенствование способов взлома криптозащиты систем и их составляющих элементов, расширение масштабов и возможных направлений проведения деструктивных атак.

На качественно новом и действенном уровне, высоко рентабельно и эффективно ***решить ключевые проблемы в области обеспечения безопасности стало возможным*** благодаря новаторской деятельности Auto-ID Labs, развитию концепции EPCglobal, достижениям в радиотехнике и микроэлектронике (Hitachi, NXP Semiconductors), в системном анализе и прорыву, совершенному на основе открытий в области алгебры (И. А. Кулаков, 2005), развитию нового инновационного направления – ***стохастических технологий***.

С введением секретных ключей, ***стохастические технологии, равно, как и создаваемые на их основе продукты (аппаратные, программные), переходят в криптографические***. Стохастические технологии охватывают все разделы современной симметричной криптографии, рассчитаны на перспективу и открывают новые возможности в области теории систем, статистического моделирования и обеспечения безопасности, имеют подавляющее *превосходство по всем показателям перед существующими аналогами*.

Предоставляемая на основе стохастических технологий действенная, рентабельная и энергоэкономичная защита элементов систем от клонирования и подделки (меток RFID/EPC и микросенсоров, кремниевых и органических, фактически не приводящая к увеличению их себестоимости и энергопотреблению), позволит последовательно, на имеющейся технологической базе и в сжатые сроки 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 smart-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 несанкциониро-

ванных действий в условиях индустриальных и преднамеренных электромагнитных помех.

5. Системная интеграция с передовыми высокоуровневыми решениями организации бизнеса, 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).

Как видится в перспективе, с развитием и всесторонней апробацией стохастических технологий станет возможным ***создание высокоэффективного параллельного криптографического сопроцессора***. Внедрение сопроцессора позволит, без заметного уменьшения производительности компьютерных, телекоммуникационных и телевизионных систем, средств связи, позиционирования и навигации, на качественно новом уровне решить задачи

- информационной безопасности, предотвращения 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, выработанной ведущими российскими учеными и инженерами, подкрепленной новейшими фундаментальными и прикладными научно-техническими разработками.

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 высокоуровневыми приложениями организации бизнеса, выводе технологий RFID (радиочастотных меток EPC, Mifare и µ-Chip), а вслед за ними микросенсорных технологий 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 и развития электронных систем.

Заглядывая в ближайшее будущее, неотвратимо, с развитием элементной базы наделенной интеллектуальными функциями и технологий их адаптивной сетевой интеграции, ***на смену технологиям RFID идут микросенсорные технологии и кибер-сети***.

Кибер-сети покроют и закономерно завоюют весь мир, от жилищ, кошельков и валюты, до технических 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, разрастания терроризма и высокой технической оснащенности криминала, ***решения положенные в основу Концепции, ко всему, способны стать надежным гарантом обеспечения государственной безопасности стран и безопасности граждан***.

Готов ответить на интересующие Вас вопросы. Приложения – «**Концепция обеспечения безопасности**» и «**Обоснование инновационного прорыва России**», предоставляются отдельно.

С наилучшими пожеланиями,
координатор, ответственный исполнитель научно-исследовательских работ

Игорь А. Кулаков, http://randon-art.ru/