СТОХАСТИЧЕСКИЕ СИСТЕМЫ. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

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 потаенных закладок, недобросовестной конкуренции и пропаганды низкосортных и 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, 2010), развитию нового инновационного направления – ***стохастических технологий***.

С введением и сокрытием секретных ключей, не иначе, ***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* [1].

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 энергопотребления), 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 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, 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 высокоэффективных стандартных криптографических примитивов и параллельных криптографических сопроцессоров***, рассчитанных на терабитную в секунду, информационную обработку. Их освоение позволит, без заметного уменьшения производительности компьютерных, информационно-коммуникационных, телевизионных и спутниковых систем, средств связи, позиционирования и навигации, на качественно новом уровне решить задачи

- 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.

Ко всему, 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 использованы для реализации

- нелинейных высококачественных генераторов истинно случайных чисел и вероятностных криптографических протоколов аутентификации, в отличие от известных на сегодня подходов, с гарантированно-доказуемой надежной статистикой и криптографической стойкостью, а также встроенной зашиты памяти микрочипов от прямого проникновения и др.

Решение представленных выше задач предполагается на основе Концепции обеспечения безопасности, исходящей из развития интеграционных платформ, информационных и беспроводных технологий, микросенсорных (**RFID**) и кибер-сетевых технологий, выработанной ведущими Российскими учеными и инженерами, подкрепленной новейшими фундаментальными исследованиями, мировым опытом 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, μ-Chip, UCODE), 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, развития криптографии, био и наноиндустрии, электронных и информационно-коммуникационных систем.

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 технологии***, ***а вслед за ними локальные и глобальные кибер-сети***, построенные на осно-

ве помехоустойчивых сверхширокополосных (**UWB**) и беспроводных (**NFC**, **Bluetooth**, **Wi-Fi**, **ZigBee**) технологий, наземных (**GSM**, **CDMA**) и спутниковых (**ГЛОНАСС**, **GPS**, **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 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 представляемой в приложении Концепции способны стать надежным подспорьем и действенным инструментом обеспечения государственной безопасности стран и безопасности граждан***.

Приложения – «**Инновационный прорыв в области микросенсорных** (**RFID**) **и кибер-сетевых технологий**» и «**Концепция обеспечения безопасности**», предоставляются отдельно.

В расчете на долгосрочную перспективу, сохраняя преемственность разработок при движении от простого к более сложному, **в качестве первого шага** реализации упомянутой выше Концепции, предлагается участие в коротком, 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**».

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**).

За счет привносимых решений, аппаратная реализация радиочастотного интерфейса и одностороннего Протокола аутентификации характеризуется низким энергопотреблением, линейной и простой топологией и очень малым числом логических элементов (30 триггеров и 300 транзисторов – 75 **GE**, на ядро односторонней функции, 2 триггера и 40 транзисторов – 10 **GE**, на ее усложнение), при длине впечатываемого в микросхему секретного ключа 71 бит и криптографической стойкости не менее 2^{57}, достигаемой при 16-17 раундах (последовательных однобитовых опросов), что по критерию временных и финансовых затрат необходимых для взлома защиты, по крайней мере на ближайшее десятилетие, вполне достаточно для планируемых приложений на основе дешевых RF-меток **ID**. При реализации взаимных, двухсторонних Протоколов аутентификации, число логических элементов увеличивается незначительно, на 3 триггера и 14-16 **GE**, при неизменном ядре, исключительно за счет изменения функции усложнения.

В итоге, 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 наиболее известных криптографических примитивов (**AES-128**/3400 **GE**, **TEA**/2633 **GE**, **Trivium**/3091 **GE**, **Grain**/3360 **GE**). Ко всему, предлагаемые сегодня ***легковесные криптографические примитивы***, для своей реализации требуют порядка 1000 **GE** и очень большое число раундов, а также широко распространенные, мало затратные, такие как **A3**/**A5** и **Crypto-1**, используемые в системе **GSM** и в бесконтактных картах **Mifare Classic**, но дискредитированные, по имеющимся техническим и криптографическим показателям, не могут тоже оказывать сколь ни будь серьезную конкуренцию.

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.

---

[1] Развитие стохастических технологий ведет к совершенствованию методологической базы, предполагает развитие, унификацию и стандартизацию математических методов и подходов криптографического анализа создаваемых на их основе прикладных приложений. В свою очередь это позволит достичь оптимального сочетания криптографической стойкости и дизайна программных и аппаратных решений, а также существенно уменьшить немалые затраты на экспертизу, сертификацию и лицензирование промышленных образцов.