КОНЦЕПЦИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. ПРОБЛЕМЫ И РЕШЕНИЯ*

«Безопасность – это категория неизмеримо
более высокая, чем величие».
Кардинал Ришелье

Развитие и интеллектуализация логического уровня обработки, становление Интернет, зарождение Интернет «Вещей» и начатое массированное наступление на освоение физического уровня 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. В связи с нарастанием угроз безопасности и вызываемым ими существенным торможением развитию и распространению электронных систем, задачи обеспечения безопасности приобретают особо важную роль. В свою очередь, вследствие заметного отставания технологий обеспечения безопасности от уровня развития техники, электронные системы, представляемые технологиями RFID и микросенсорными технологиями, пошли по эволюционному пути развития. Для устранения вызываемых этим негативных процессов и выхода на новый качественный уровень, предсказанный экспертами, требуются новые подходы и прорывные решения.

Кулаков Игорь Анатольевич, www.random-art.ru

Оглавление

Литература

1. Salil Pradhan, Geoff Lyon, Ian Robertson and others.
RFID and Sensing in the Supply Chain (Challenges and Opportunities).
HP Laboratories Palo Alto HPL-2005-16, February 9, 2005.
www.hpl.hp.com/ techreports/2005/HPL-2005-16.pdf
2. Jin Mitsugi, Tatsuya Inaba and others.
Architecture Development for Sensor Integration in the EPCglobal Network.
Auto-ID Labs White Paper WP-SWNET-018, July, 2007.
3. И. А. Кулаков.
Инновационный прорыв в области микросенсорных (RFID) и кибер-сетевых технологий.
22 страницы, Random Art Labs, Москва, май 2010.
3. **The EPC Global**, website (www.epcglobalinc.org).
4. **The Auto-ID Labs**, website (www.autoidlabs.org).
5. Thomas Kelepouris, Samuel Bloch Da Silva, Duncan McFarlane.
Automatic ID Systems: Enablers for Track and Trace Performance.
Auto-ID Lab, University of Cambridge, UK Embraer S.A., Brazil,
Auto-ID Labs White Paper WP-BIZAPP-037 May 2, 2007. http://autoid.mit.edu

6. The RFID Global Forum **The Internet of Things**. www.rfidglobal.eu
7. Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Engels.
   Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems.
   In Security in Pervasive Computing, 2003.
8. Martin Feldhofer.
   Strong Crypto for Tiny RFID Tags (Challenges and Design Issues).
   IAIK –Graz University of TechnologyMartin.11-13 July 2007, Malaga, Spain.
   Workshops on RFID Security 07, www.iaik.tugraz.at
9. **Building Radio frequency Identification for the Global Environment** (BRIDGE).
   www.breadge-project.eu
10. **Stop Tampering of Products** (SToP project). www.stop-project.eu
11. **Ecrypt I, II**. European Network of Excellence in Cryptology. www.ecrypt.eu.org
12. Sanjay Sarma.
    RFID and Security.
    MIT and CTO of OATSystems, 2006.
13. Divyan M. Konidala, Woan-Sik Kim, and Kwangjo Kim.
    Security Assessment of EPCglobal Architecture Framework.
    Auto-ID Labs White Paper WP-SWNET-017, 2006.
    www.autoidlabs.org/single-view/dir/article/6/255/page.html
14. Mikko Lehtonen.
    Applying Auto-ID to Anti-Counterfeiting
    (Lessons Learned from SToP and BRIDGE Projects).
    Institute of Technology Management (ITEM), University of St. Gallen (HSG)
    Department of Management, Technology, and Economics (D-MTEC),
    ETH Zurich EAP Meeting, Paris / February 26th, 2009.
15. **Workshops on RFID Security** (RFIDSec) 2005-2008,
    www.cosic.esat.kuleuven.be/rfidsec09
16. И. А. Кулаков.
    Предарифметика. Стохастические технологии.
    «Инициатива 2011», Москва, январь 2011,
    www.random-art.ru
17. И. А. Кулаков.
    Дихотомические последовательности и их свойства.
    Статья, представленная на 3-ю Центрально-европейскую конференцию,
    TATRACRYPT 2003, Братислава, 28 июня 2003.
18. И. А. Кулаков.
    Дихотомические генераторы и их свойства.
    Статья, представленная на 6-ю Международную конференцию по информационной безопасности и криптологии, ICISC 2003, Сеул, 27 ноября 2003.
19. И. А. Кулаков.
    Рандомизационные генераторы.
    Статья, представленная на Международную конференцию по быстрым программным средствам шифрования, FSE 2004, Нью-Дели, 5 февраля 2004.
20. И. А. Кулаков, С. Н. Куксов, А. В. Дятленко, Н. В. Филиппов.
    Система контроля сертификационных меток промышленных товаров.
    НИР, 243 страницы, Московский комитет по науке и технологиям, Москва, апрель 2005.
21. А. Г. Иванов, М. А. Иванов, Д. А. Дударев, И. А. Кулаков.
    Анализ алгоритма односторонней аутентификации.
    Экспертные заключения, 40 страниц.
    Московский комитет по науке и технологиям, Москва, июль 2006.
22. И. А. Кулаков.
    Система защиты от клонирования, фальсификации и подделки.
    Обеспечение безопасности технологий RFID.
    41 страница, Random Art Labs, Москва, март 2006.
23. И. А. Кулаков.
    Стохастические системы и криптография.
    42 страницы, материалы конференции РусКрипто 2006, Москва, февраль 2006.
24. И. А. Кулаков.
    ***RA*-технологии. Обеспечение безопасности систем RFID**.
    14 страниц, материалы конференции РусКрипто 2006, Москва, февраль 2006.
25. И. А. Кулаков.
    Материалы конференций RusCrypto 2004, 2005, 2006,
    www.ruscrypto.org

26. И. А. Кулаков.
Идентификация в системе RFC, **разрешение коллизий и аутентификация**.
89 страниц, Random Art Labs, Москва, май-август 2006.
27. И. А. Кулаков.
Электронные технологии в системе регулирования и защиты товарного рынка от нелегальной продукции.
Доклад на второй Международной выставке программных продуктов CIS 2006, Нанкин, 2 сентября 2006.
28. И. А. Кулаков. **Экосистемы. Угрозы безопасности**.
53 страницы, Российский научный центр «Курчатовский институт», Москва, август 2007.
29. И. А. Кулаков, А.И. Сухопаров, П. Р. Машевич, А.С. Лакаев, Б.Ю. Богданович, Л.Н. Кривошеин.
Адаптивные логистические сети государственного (международного), отраслевого и корпоративного уровней управления в системах обеспечения экологической безопасности, защиты товарных рынков и сегментов экономики от контрафактной продукции.
Тематическая заявка в Федеральное агентство по науке и инновациям № 5008, программное мероприятие 2.4, 2007.
30. И. А. Кулаков, П. Р. Машевич, С.М. Ларионов.
Обоснование и разработка модели базовой интеграционной платформы автоматизированной обработки информации о состоянии материальной среды и ее элементов, поддержки высокоуровневых приложений и обеспечения безопасности.
Тематическая заявка в Федеральное агентство по науке и инновациям № 5670 и 5733, программное мероприятие 1.4, 2008.
31. И. А. Кулаков, А.П. Ананьев, Ю.В. Гуляев, В.А. Конявский.
Реализация и проведение анализа бесповторных генераторов (псевдо) случайных чисел высокой криптографической стойкости систем управления ключами, предотвращения несанкционированного доступа и защиты информации.
Тематическая заявка в Федеральное агентство по науке и инновациям, программное мероприятие 1.4, 2008.
32. И. А. Кулаков, П. Р. Машевич, М. А. Иванов и другие.
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.
Тематическая заявка в Федеральное агентство по науке и инновациям, программное мероприятие 2.4, 2008.
33. В. Г. Ларионов, М. Н. Скрыпникова.
Как защититься от подделки?
Московский государственный университет прикладной биотехнологии (МГУПБ).
www.cfin.ru/press/marketing/2001-3/index.shtml
34. Р. Лидл, Г. Нидеррайтер.
Конечные поля.
М.: Мир, 1988.
35. К.Шеннон.
Работы по теории информации и кибернетике.
М.: Иностранная литература, 1963.
36. Б. Шнайер.
Прикладная криптография.
Изд. ТРИУМФ, Москва, 2002.
37. М.А. Иванов.
Криптографические методы защиты информации в компьютерных системах и сетях.
КУДИЦ-ОБРАЗ, Москва 2001.
38. Д. Кнут.
Искусство программирования. Получисленные алгоритмы.
т.2, Москва, 2003.
39. Г. Шустер.
Детерминированный хаос. Введение.
Мир, Москва, 1988.
40. Н. В. Карлов, Н. А. Кириченко.
Колебания, Волны, Структуры.
ФизМатЛит, Москва, 2003.

41. Н. Птицын.
Приложение теории детерминированного хаоса в криптографии.
МГТУ им. Н. Э. Баумана, Москва, 2002.
42. **Математическая энциклопедия**.
Изд. Советская энциклопедия, т.1 - 5, Москва, 1977 - 1985.
43. М.А. Иванов, И.В. Чугунков.
Теория, применение и оценка качества генераторов псевдослучайных последовательностей.
КУДИЦ-ОБРАЗ, Москва 2003.
44. Marsaglia G.
Пакет статистических тестов DIEHARD.
1997, geo@stat.fsu.edu
45. **A Statistical Test Suite for the Validation of Random and Pseudorandom Number Generators**.
NIST Special Publication 800-22, (FIPS PUB 140-1,2). NIST, 2001.
http://csrc.nist.gow
46. Sarma S., Weis S. and Engels D.
Radio-Frequency Identification: Security Risks and Challenges.
RSA Laboratories Cryptobytes, Volume 6, No.1 – Spring 2003.
47. Mikko Lehtonen, Nina Oertel, Harald Vogt.
Features, Identity, Tracing, and Cryptography in Product Authentication.
Auto-ID Labs White Paper WP-BIZAPP-040, 2008.
www.autoidlabs.org
48. **The NXP Semiconductors**, website (www.nxp.com, www.mifare.net).
49. Auguste Kerckhoffs.
La Cryptographie Militaire.
Journal des Sciences Militaires IX, 5–38 (January 1883).
50. Andrey Bogdanov.
Attacks on the KeeLoq Block Cipher and Authentication Systems.
3rd Conference on RFID Security, Malaga, 2007.
www.crypto.rub.de
51. Karsten Nohl, David Evans, Starbug and Henryk Pl¨otz
Reverse-Engineering a Cryptographic RFID Tag.
USENIX Security Symposium. San Jose, CA. 31 July 2008.
52. Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijrers,
Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs.
Dismantling MIFARE Classic.
Springer-Verlag, Berlin, Heidelberg, 2008.
53. ООО “АНГСТРЕМ”.
Описание микросхемы AN5505 (аналог MIFARE Classic).
54. **The Hitachi µ-solutions**, website (www.hitachi-eu.com)
55. **Near Field Communication (NFC)**, website (www.nfc-forum.org/home),
http://ru.wikipedia.org/wiki/Near_Field_Communication
56. J. Morak, D. Hayn, P. Kastner, G. Schreier.
Near Field Communication (NFC) technology.
Med-e-Tel Luxembourg, April 16-18, 2008.
57. Mohammad Khan (President & Founder).
Near Field Communications (NFC) Mobile Payments & Promotions.
ViVOtech, December 3, 2008 (Nokia World).
http://events.nokia.com/nokiaworld08/assets/pdf/Mohammad_Khan.pdf
58. Ernst Haselsteiner and Klemens Breitfuß,
Security in Near Field Communication (NFC), Strengths and Weaknesses.
Philips Semiconductors, Mikronweg 1, 8101 Gratkorn, Austria
http://events.iaik.tugraz.at/RFIDSec06/Program/papers/
59. Постановление правительства РФ № 957, от 29 декабря 2007,
Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами.
www.garant.ru/hotlaw/mon/109485.htm
60. Б.Н. Кузык, Ю.В. Яковец.
Россия –2050. Стратегия инновационного прорыва.
Москва «Экономика» 2005, www.h2club.mirea.ru/sources/Russia_2050.pdf
61. **Создание Кибернетического командования США**, 24 июня 2009.
www.mk.ru/politics/306719.html

Часть 1. Обеспечение безопасности в контексте развития технологий RFID

«За безопасность платят – за пренебрежение
расплачиваются!».

Народная мудрость

Объективно, с развитием физического уровня обработки на основе технологий RFID [1], а с ними и сенсорных технологий [2], знаменуется переход информационно-коммуникационных систем, информиндустрии и общества в целом, на качественно новый уровень [3].

В этом процессе следует отдать должное компании Philips (NXP Semiconductors) [48], Auto-ID Labs [3] и компании EPCglobal [4]. Благодаря их активной и новаторской деятельности получили развитие и промышленное освоение системы автоматической идентификации [5], «Интернет Вещей» [6]. Между тем, как показали исследования, ***развитие и масштабное распространение представляемых ими систем существенно сдерживается высокой стоимостью и энергопотреблением технологий защиты*** их элементов (радиочастотных меток и микросенсорных устройств) от клонирования и подделки [7].

В первую очередь ***это связано с отставанием криптографических технологий от уровня развития техники*** [8].

1.1. Состояние развития физического уровня обработки

Несмотря на предпринимаемые мировым сообществом усилия в решении ключевых проблем обеспечения безопасности [9,10], все ***попытки осуществления действенной, рентабельной и энергоэкономичной защиты элементов систем на физическом уровне обработки от клонирования и подделки***, ***в первую очередь радиочастотных (RF) меток типа EPC и Mifare, не увенчались успехом*** [11,12,52,53]. А это вынуждает возложить бремя организации противодействия на логический уровень обработки и логистические протоколы [13].

Дисбаланс между физическим и логическим уровнем обработки, вызываемый существенной деформацией в сторону логистичекой обработки, ведет к серьезным негативным последствиям, к абсолютизации ограничений на целостность цепей поставок, глобализации и сверхцентрализации системы. В свою очередь, это ведет к непреодолимым трудностям в решении проблем обеспечения информационной безопасности, особенно на высших (государственных) уровнях управления, непомерной нагрузки на линии связи, за счет астрономического роста числа транзакций аутентификации товаров и изделий, а также к заметному увеличению стоимости периферийного оборудования и обслуживания системы. Идущие с этим, ***связанные с обеспечением информационной безопасности общие накладные расходы растут, многократно превышают стоимость средств маркировки и возлагаются на рядовых потребителей***.

Кроме того, неопровержимо доказанные факты свидетельствуют [14,15,20,47], что на основе одних логистических протоколов, включая организацию строгой системы учета и контроля на всех уровнях логической обработки, ***обеспечить полноценную защиту элементов систем от клонирования, фальсификации и подделки не представляется возможным***. Игнорирование этого положения рано или поздно ведет к ощутимым потерям, вплоть до фатальных. В подтверждение этого следует указать на провалы, предпринятых в России попыток учета алкогольной продукции и защиты рынка от ее фальсификации и подделки. Эксперты утверждают, что прямые убытки от внедрения не оправдавшей себя системы (**ЕГАИС**), составили более 500 млн. рублей. Сами же производители говорят про 500 млн. долларов (вероятно, с учетом простоя предприятий и недополученной прибыли). Похожий обвал происходит в системе оплаты проездов в Московском метро, построенной на основе незащищенных от клонирования и подделки талонов RFID, построенные на основе RF-микрочипов NXP **Mifare Ultralight.** По скромным оценкам, ущерб от первой волны подделки талонов составил около 150 млн. рублей. ***Пренебрежение элементарными нормами обеспечения безопасности обходится очень дорого***.

Ко всему, ситуация усугубляется взломом криптозащиты наиболее распространенных RF-чипов NXP **Mifare Classic** [50-53], используемых в системах единой оплаты проезда, удостоверяющих документах, в социальных и медицинских электронных картах, пропусках, противоугонных системах и пр. Для решения этой проблемы, компания NXP предлагает перейти на более дорогие RF-чипы **Mifare Plus** высокой криптографической стойкости. При этом, компания **NXP** не несет никакой ответственности за последствия взлома потенциально слабой криптозащиты RF-чипов, рассматривая переход к Mifare Plus для себя, как наиболее прибыльное и перспективное развитие бизнеса. ***Во что обойдутся невосполнимые ошибки монополии NXP и навязываемый ею, не оставляющий выбора переход на более дорогие RF-чипы, еще предстоит оценить***.

В условиях беспрецедентно высокого нарастания угроз безопасности, ситуация потенциально опасна и непредсказуема по масштабам последствий [28,29,30]. Особенно, если учесть, что

потерпевшие неудачу вполне совершенные по современным меркам системы в полной мере охватывают подходы и логистические протоколы обеспечения безопасности, положенные в основу развития информационно-коммуникационных систем, включая и концепцию EPCglobal [13,14]. ***Ситуация усугубляется отсутствием должных выводов из полученных уроков, ведущим к бессмысленным расходам, порождаемых многократным дублированием разработок и постоянством повторения старых ошибок***. Причины возникновения такого рода явлений в основном обусловлены узковедомственной ограниченностью и межведомственной разобщенностью научно-технических разработок.

Аналитические прогнозы, опирающиеся на данные факты, указывают, что без полноценной системы обеспечения безопасности на физическом уровне обработки не избежать вызываемого нарастающими угрозами безопасности существенно выраженного торможения развитию и распространению систем RFID/EPC и им подобных систем [22,24,25]. Такое торможение ведет к тому, что системы данного типа, прорывные по началу, вырождаются в элитарно корпоративные, привлекательные исключительно для обустройства торговли и небольшого числа других узкоспециализированных приложений, не несущих видимых позитивных результатов главному субъекту товарного рынка и экономики – Потребителю.

В связи с нарастанием угроз безопасности и вызываемым ими существенным торможением развитию и распространению электронных систем, ***задачи обеспечения безопасности приобретают особо важную роль***. В свою очередь, вследствие заметного отставания технологий обеспечения безопасности от уровня развития техники [11,15], электронные системы, представляемые технологиями RFID и микросенсорными технологиями, пошли по эволюционному пути развития. Для устранения вызываемых этим негативных процессов и выхода на новый качественный уровень, предсказанный экспертами, требуются новые подходы и прорывные решения.

1.2. Перспективы развития физического уровня обработки

Кардинально ***изменить ситуацию обеспечения безопасности на физическом уровне обработки можно только на основе качественно новых криптографических технологий***.

В полной мере удовлетворить требованиям, предъявляемым к системам обеспечения безопасности способно новое, имеющее под собой фундаментальную алгебраическую базу, быстро развивающееся направление – ***стохастическая криптография*** [16,23,25]. Построенные на ее основе криптографические примитивы рассчитаны на перспективу, обладают подавляющим превосходством по всем показателям перед известными аналогами [15,52] и позволяют снять существующие проблемы обеспечения безопасности элементов систем и систем в целом [10].

Принимая как должное малые аппаратные затраты и энергопотребление, на порядок меньшие лучших аналогов, высокую производительность и регулируемую в сколь угодно широких пределах стойкость криптографических примитивов (см. раздел 3.4), высочайшую эффективность генераторов систем управления ключами, согласно с результатами проведенных исследований на протяжении последних 4-х лет, ***имеющийся на сегодня физический, а с ним и логический уровни обработки претерпевают качественную трансформацию***. Разгружаются линии связи, снимаются ограничения на целостность цепей поставок, неизмеримо возрастают функциональные возможности обработки, устраняются бреши в системе обеспечения безопасности, существенно уменьшаются затраты на периферийное оборудование и обслуживание.

С введением эффективных аппаратных решений и централизованной системы управления ключами, с предоставлением на этой основе всем категориям потребителей штатных и индивидуальных (карманных автономных и мобильных прямого контроля, локальных и высокоуровневых сетевых) средств проверки подлинности и качества продукции и изделий, становится возможной организация тотальной защиты и контроля сегментов товарного рынка и экономики с перспективой глобального мирового охвата [55,56,57]. ***В такой постановке минимизируются риски приобретения недоброкачественной продукции, включаются ранее недоступные мощные государственные и общественные механизмы противодействия нелегальному производству***, причем, в этих процессах Потребителю отводится главенствующая роль, а не роль заложника рынка, с чем устраняются негативные факторы, препятствующие широкомасштабному распространению систем RFID/EPC.

Решение указанных выше задач предполагается на основе Концепции обеспечения безопасности, подкрепленной фундаментальными и прикладными научно-техническими разработками [16-32].

Часть 2. Концепция обеспечения безопасности

«Мир нужно изменять, иначе он неконтролируемым образом начнет изменять нас самих».

Станислав Лем

Обеспечение безопасности – задача комплексная, неотделимая от систем, представляемых неразрывно связанными между собой логическим и физическим уровнями обработки, информационными, коммуникационными, сетевыми, электронными и сенсорными технологиями.

Для решения проблем обеспечения безопасности в виду их чрезвычайной сложности, потребовалось привлечение экспертов и специалистов международных компаний **Philips**, **HP**, **Intel**, **Siemens** и **SAP**, а также представителей более 25 ведущих российских предприятий и организаций разных профилей:

ОАО «**Ангстрем**» и «**Ангстрем-М**» – ведущий производитель и разработчик микроэлектронной продукции в России и странах СНГ.

ИРЭ РАН – Институт радиотехники и электроники Российской Академии наук;

МИФИ – крупнейший Российский университет, располагающий передовой научно-технической базой, имеющий высшую международную репутацию;

ряда других крупных организаций, включая высшие органы государственного надзора, отвечающие за состояние Российского рынка.

Работы проводились, начиная с марта 2004 года.

Результатом является выработка Концепции обеспечения безопасности.

Проведена экспертиза Концепции на предмет ее практической реализации.

Краткий аналитический обзор Концепции

Формулировка Концепции, как и решение проблем обеспечения безопасности в целом, основана на открытиях и достижениях в области алгебры и стохастических систем и отвечает требованиям времени [16,23].

Разработанные на их основе стохастические и криптографические технологии не имеют себе равных по эффективности и потенциальным возможностям [24] и позволят преодолеть существенное отставание технологий обеспечения безопасности от уровня развития техники, ***особенно в части обеспечения высокоэффективной, действенной и рентабельной электронной защиты элементов систем*** [20,27].

2.1. Решения, положенные в основу Концепции обеспечения безопасности

Основу Концепции обеспечения безопасности составляют следующие инновационные решения и подходы:

1. ***Использование передовых достижений и мирового опыта*** в области автоматической идентификации, в первую очередь широкомасштабных апробированных решений EPCglobal, закладываемых в основу построения техносистем нового поколения – «Расширенный Интернет».

2. ***Переход от глобальной, несущей угрозы безопасности, к многоуровневой архитектуре построения системы***, предусматривающей мультипликативно выраженную интеграцию информационных, электронных, сенсорных, коммуникационных технологий и технологий обеспечения безопасности.

Глобальная системная интеграция, интеллектуализация и минитюаризация элементов систем, несут в себе серьезные угрозы информационной и физической безопасности.

3. ***Внедрение прорывных решений в области обеспечения безопасности***, полученных на основе развития алгебры, стохастических систем и предоставляемых ими стохастических технологий [16], взамен малоэффективных криптографических, в особенности построенных на основе полей Галуа GF(2) [36,37], включая и их нелинейные модификации [50,51,52].

Полноценное, не сказывающееся на эффективности и стоимостных показателях, наделение элементов электронных систем, вплоть до особо критичных печатных органических, высоконадежными функциями обеспечения безопасности. Осуществление комплексирования электронных способов защиты с простыми и дешевыми производственно-технологическими способами, начиная с номерных бумажных идентификационных меток [33].

4. ***Введение компактных сертификатов и супердинамичной системы управления ключами***, для обеспечения системной интеграции физического и логического уровней обработки, организации глубоко эшелонированной действенной системы обеспечения безопасности и защиты.

Организация тотальной защиты и контроля сегментов товарного рынка и экономики с перспективой глобального мирового охвата, за счет предоставления всем категориям потребителей индивидуальных (карманных автономных и мобильных прямого контроля, локальных и высоко-

уровневых сетевых) и штатных средств проверки подлинности и качества продукции и изделий [57,58].

5. ***Вывод элементной базы на качественно новый уровень***, посредством последовательного перехода к технологически гибким, дешевым, высокорентабельным и экономичным микросенсорным модулям (взамен функционально ограниченных меток RFID/EPC и энергоемких процессорных микрочипов), защищенным от несанкционированных действий, клонирования и подделки, снабженных многопрофильными смарт-датчиками и помехоустойчивым интерфейсом внешнего взаимодействия.

Предполагаемый **общий срок реализации Концепции составит около 3 лет** [32],

Результатом проводимых работ станет создание элементной базы и прототипов систем защиты от нелегальной (контрафактной), фальсифицированной и недоброкачественной продукции (потребительского, фармацевтического и авиационно-технического рынков), создание заделов для распространения решений на другие сегменты экономики и задачи обеспечения безопасности.

Для исключения рисков, **в первый год на основе создаваемого консорциума планируется проведение трех НИР**,

первая относится к разработке концепции и совершенствования протоколов обеспечения безопасности систем, охватываемых решениями EPCglobal,

вторая – к изложению алгебраической теории построения стохастических систем и разработки инструментальных средств, необходимых для наполнения протоколов обеспечения безопасности,

третья НИР относится к разработке технологических принципов построения и совершенствования элементной базы электронных систем.

Состав консорциума, объемы и источники финансирования работ является отдельной темой для обсуждения заинтересованными сторонами.

2.2. Комплексирование с высокоуровневыми приложениями

Комплексирование с высокоуровневыми приложениями, например, решениями SAP и HP, посредством компонент интеграции физического и логического уровней обработки, позволит осуществить ***создание единой интеграционной платформы*** [29,32], необходимой для решения следующего комплекса производственных, экономических и социальных задач:

1. **Организация** непрерывного учета и контроля, придание прозрачности товарному рынку и сфере услуг (государственной, общественной и маркетинговой).
2. **Планирование**, формирование и поддержание оптимально сбалансированных пропорций между спросом и предложением на товарную продукцию и услуги.
3. **Оптимизация** производственных и бизнес процессов, цепей поставок, хранения и реализации продукции, обеспечение проведения многопрофильных профилактических работ. Расширение спектра и качества предоставляемых лицензионных услуг.
4. **Защита** товарного рынка и сегментов экономики от нелегальной (контрафактной), фальсифицированной и недоброкачественной продукции.
5. **Обеспечение** экологической, биологической и физической безопасности.

Взаимно обусловленная и сбалансированная интеграция этих задач на всех уровнях обработки и управления, по мере развития, расширения масштабов и углубления сетевого охвата, ведет к весомой отдаче, уменьшению, нивелированию и конечному восполнению общих затрат, связанных с внедрением, обеспечением безопасности и обслуживанием систем.

2.3. Развитие элементной базы

Введение построенных на основе стохастических технологий двусторонних, по примеру смарт-карт, более совершенных протоколов защиты позволит осуществить ***плавный переход к элементной базе нового поколения, представляемой функционально и конструктивно гибкими электронными устройствами – микросенсорными модулями*** [26,27,28].

Как показывает проведенный анализ, в результате вносимых новых решений, особенно в части касающейся организации управления порядком исполнения командных инструкций и взаимодействия с внешней средой, такие устройства будут менее энергоемкими, более простыми, дешевыми, “дальнобойными” и устойчивыми к внешним воздействиям, чем существующие ныне аналоги. Они позволят более эффективно, качественно и рентабельно решить все известные на сегодня прикладные задачи, присущие технологиям **RFID**, а также задачи контроля за состоянием внешней среды и другие, включая осуществление денежных расчетов и платежей, взамен дорогих и энергоемких микропроцессорных чипов.

Ко всему этому, микросенсорные устройства допускают комплексирование с дешевыми производственно-технологическими способами защиты, от простых этикеток до лазерной гравировки [10,33]. Представляемые ими ***сетевые технологии позволят обеспечить высокорентабельную защиту составных и сложных объектов***, от простых упаковок и входящих в их состав элементов, до агрегатов, их узлов и деталей. В свою очередь это позволит существенно повысить эффективность решений в сфере логистики и торговли, осуществить распространение технологий на сектора экономики (фармацевтика, транспорт и др.).

2.4. Место био и нанотехнологий

Большие перспективы связаны с полномасштабным освоением промышленного производства более дешевых, защищенных от клонирования и подделки, органических микросенсорных электронных устройств.

Дальнейшее развитие включает ***безопасные печатные технологии*** на основе органических чернил, нано-радио-чипы и антивандальные чипы с аналоговыми элементами, функционирующим на принципах поверхностных акустических волн.

Неизмеримо большие возможности представляются с развитием био и нано сенситивных *(чувствительных*, ***smart)*** ***материалов***, наделенных элементарными интеллектуальными функциями, созданием на их основе пассивных био- и нано-датчиков различного назначения, от физического и химического, до биологического и экологического мониторинга и контроля состояния внешней среды.

Био и наноиндустрия стремительно развиваются. Растет номенклатура, функциональные возможности и эффективность смарт-материалов. Микросенсорные устройства и датчики, построенные на их основе, способны вывести системы контроля качества продукции, экологической, биологической, физической и инженерно-технической безопасности на качественно новый уровень.

Обеспечение безопасности микросенсорных технологий находится на начальной стадии своего развития, но, несмотря на это, способно ***стать своеобразным полигоном для решения проблем обеспечения безопасности нанотехнологий высокого уровня интеллектуализации***. Без преодоления новых вызовов угроз безопасности идущих с освоением наноуровня обработки, развитие наноиндустрии в целом без вызываемого ими существенного торможения, особенно с освоением производства нанороботов, выглядит весьма проблематично.

2.5. Перспективы развития

Представляемые Концепцией информационные и электронные технологии допускают ***последующее масштабное распространение на задачи*** защиты удостоверяющих документов и валюты ***(актуальных в особенности)***, маркировки почтовых отправлений, архивных документов, выставочных экспонатов и содержимого библиотечных фондов, идентификации домашних животных, а также на другие приложения в сфере обеспечения безопасности.

По мере развития беспроводных сетевых технологий, с масштабным освоением смарт-материалов, технологий на основе поверхностных акустических волн (ПАВ) и UWB технологий микросенсорные устройства станут многофункциональными, многоканальными и помехозащищенными. С этим ***станет возможным решения задач*** охраны жизненно-важных объектов, жилищ и строений, защиты распределенных инженерно-технических инфраструктур от несанкционированных действий в условиях индустриальных и преднамеренных электромагнитных помех.

Следующим очевидным шагом, рассчитанным на перспективу, станет ***дальнейшее распространение решений*** на системы:

– интеллектуальные здания, коммунальные хозяйства, комплексы;

– интеллектуальные жилища (умные дома), площадки, кооперативы;

– математическое моделирование, решение производственных, распределительных и потребительских сетевых оптимизационных задач;

– создание экспертных систем планирования, оценки состояния и развития районов, городов (селений), областей, регионов и федеральных образований.

С развитием и всесторонней апробацией стохастических технологий станет возможным ***создание высокоэффективного параллельного криптографического сопроцессора***, в целях решения на качественном новом уровне (без заметного уменьшения производительности компьютерных, телекоммуникационных и телевизионных систем, средств связи, позиционирования и навигации) задач информационной безопасности, предотвращения прямых и скрытых кибер-угроз [61], предотвращения несанкционированного доступа и нерегламентированных действий, защиты авторских прав, в частности на аудио- и видео-продукцию, программы и литературу, ликвидации отставания технологий обеспечения безопасности от современного уровня развития техники.

Часть 3. Аспекты реализации технологий обеспечения безопасности

«Если мы хотим создать новый мир,
материал для него готов.
Первый тоже был создан из хаоса».

Роберт Куиллен.

Развитие и интеллектуализация логического уровня обработки, освоение технологий RFID, становление Интернет, 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, ведущий к новой общественно-экономической формации – «Постиндустриальное Общество», взамен индустриального, весьма сложнен и внутренне противоречив [28,60].

3.1. Угрозы безопасности

Обратной стороной технологического развития общества является ***нарастание и резкое обострение угроз безопасности***. Высокие технологии становятся не только инструментом роста промышленного производства и повышения социального благополучия населения, а также инструментом осуществления противоправных действий и реализации корыстных интересов криминальных структур и элементов.

В связи с этим, ***задачи обеспечения безопасности приобретают все возрастающую, особо важную роль***. Это обусловлено 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.

Развитие информационно-коммуникационных систем, их интеграция и формирование глобального информационного пространства без надлежащей защиты может привести к очень серьезным последствиям. Так, деструктивные воздействия, вырабатываемые в системах большой степени интеграции, способны «запускать» лавинно нарастающие вещественно-энергетические процессы, по своим последствиям сравнимые с социально-экономическими потрясениями и экологическими катастрофами.

С развитием наноиндустрии идут новые угрозы, которые без принятия адекватных мер могут носить фатальный характер. Трудно даже представить к чему может привести только одно - бесконтрольное использование нанороботов.

3.2. Просчеты в обеспечении безопасности

В свете нарастания указанных угроз, очевидно, что без принятия должных мер обеспечения безопасности, торможение экономическому, социальному и технологическому развитию общества будет усиливаться, а масштабы и вероятность угроз, равно, как и вызываемые ими потери, будут только расти.

При этом в силу передачи высокоуровневых функций управления автоматизированным системам, эффективность административных и правовых мер, направленных на обеспечение должного уровня безопасности, будет падать.

Для примера, по результатам маркетинговых исследований и наблюдаемой общей отдаче, техносистемы, представляемые концепцией, проводимой компанией EPCglobal, опирающейся на незащищенные от клонирования и подделки RF-метки, пошли по эволюционному пути развития, а не так, как на то первоначально рассчитывали эксперты, ведущие системные интеграторы и производители микроэлектронной продукции.

Показательно, попытка, предпринятая в России для защиты рынка алкогольной продукции от фальсификации и подделки на основе подходов и логистических протоколов, подобных про-

токолам, положенных в основу концепции EPCglobal, усиленная защищенными от подделки на основе производственно-технологических способов защиты акцизными марками, в частности голографических знаков и двумерных штриховых кодов, оказалась провальной.

Одна из основных причин торможения развитию техносистем и провалов, обусловлено отставанием технологий обеспечения безопасности (прежде всего криптографических) от современных требований. Не выдерживает никакой критики подходы, нарушающие основные принципы, лежащие в основе технологий обеспечения безопасности и криптографии [49]. Даже такие гиганты микроэлектронной индустрии, как компании Philips [48] и Hitachi [54], в целях достижения высокой рентабельности производимой ими продукции, используют засекреченные криптографические протоколы и алгоритмы, в ущерб стойкости защиты, требующие малых аппаратных затрат. Наиболее распространенные RF-чипы NXP (Philips) Mifare Classic, используемые в системах единой оплаты проезда, удостоверяющих документах, социальных картах, пропусках, противоугонных системах и др., взломаны в 2008 году [50,51,52,53]. С этим, данные, хранящиеся в RF-чипах, становятся легкой добычей мошенников.

Несмотря на усилия, предпринимаемые мировым сообществом и проведенные в период с 1997 по 2010 годы международные конкурсы, завершившиеся отбором лучших из известных криптографических примитивов, изменить положение к лучшему в сфере обеспечения безопасности, так и не удалось, как и не удалось создать реальных заделов, рассчитанных на ближайшую перспективу и опережающие темпы развития техники [9,10,15]. Положение дел еще больше усугубляется давно изжившими себя запретительными барьерами [59], препятствующим проведению разработок и сертификации криптографических средств.

На сегодня, все попытки осуществления рентабельной аппаратной защиты дешевых RFID меток от клонирования и подделки оказались безуспешными. Стоимость и энергозатраты надежной аппаратной защиты сохраняются очень большими. Для выхода из столь сложного положения, требуются новые, прорывные решения в области криптографии.

Между тем, использование логистических протоколов не подкрепленных аппаратной защитой ведет к деформации и перегрузке логического уровня обработки, нарастанию связанных с этим серьезных угроз безопасности и ограничению областей применения, увеличению затрат на транзакции и обслуживание, а также к увеличению стоимости периферийного оборудования.

Ко всему, можно констатировать, что существующие производственно-технологические способы защиты, рассчитанные на массовое производство и применение, дискредитированы настолько, что не способны надлежащим образом обеспечить защиту от фальсификации и подделки. К этому, ***стоимость производственно-технологической защиты непрерывно растет, и уже вплотную приблизилась к электронной*** [10,33].

3.3. Имеющиеся заделы

Решению упомянутых выше проблем, начиная с марта 2004 года, посвящено четыре НИР, проведенных автором, одной совместно с Московским комитетом по науке и технологиям [20], а также трех самостоятельных [22-27] по итогам тесной работы с экспертами российских представительств международных компаний Philips, HP, Intel, Siemens и SAP, государственных и общественных организаций России.

Результаты исследований получили развитие в работе, проведенной в середине 2007 года, совместно с одним из мировых лидеров в области наноиндустрии, Российским научным центром «Курчатовский институт», по конкретизации и выработке подходов к решению проблем обеспечения безопасности экосистем [28].

С целью выработки программ и подготовки условий для осуществления качественного прорыва в области электронных и микросенсорных технологий, в конце октября 2007 года было создано неформальное объединение «Инициатива 2007» [32], объединившей на базе более 25 организаций лучшие силы российских специалистов в области RFID («Ангстрем», ИРЭ РАН и др.).

К настоящему времени выработана Концепция построения и реализации техносистем новой формации – «Расширенный Интернет». По ней подготовлены экспертные заключения [21], указывающие на реалистичность решения на имеющейся научной и технической базе перечисленных выше проблем.

3.4. Стохастические технологии

Открытия алгебраических систем неполной арифметики и предарифметики (состоявшиеся в конце 2005 года, I.Kulakov), по существу предшествующим известной всем классической арифметики, симбиоз и развитие теории алгебр и систем, следующие из этого достижения в области

стохастических систем дискретного времени [42] и создание стохастических технологий, на основе работ проводимых с начала 1993 года, позволили создать необходимые предпосылки для осуществления технологического прорыва в сфере обеспечения безопасности [16-32].

С введением секретных ключей, ***стохастические технологии, равно, как и создаваемые на их основе продукты (аппаратные, программные), переходят в криптографические***. Такое разделение позволяет снять многие догматы и запретительные нормы, вносимые особым статусом криптографии, а с этим, по аналогии с принятой практикой внедрения блочного шифра Advanced Encryption Standard (AES), осуществить последовательный, организационно-правовой переход от обязательного лицензирования деятельности по производству и распространению криптографических средств [59] к независимой экспертизе и добровольной сертификации разрабатываемых опытных образцов, предназначенных для последующего промышленного освоения.

Стохастические технологии охватывают все разделы современной симметричной криптографии [24.25] и знаменуют создание нового научно-технического направления – ***стохастической криптографии*** [16,21,23,25,31], позволяют придать новый импульс и преодолеть торможение развитию криптографии в целом.

Стохастические технологии рассчитаны на перспективу и отличаются подавляющим превосходством по всем показателям перед решениями, полученным на основе известных на сегодня криптографических технологий [36,37].

3.4.1. Теоретическая и инструментальная база стохастических технологий.

Формально, в качестве инструментальной базы стохастических технологий выступают линейные и нелинейные односторонние (иначе стохастические, псевдослучайные – **PR**) функции и операторы [7,42]. Много раундовые односторонние операторы (функции) именуются однонаправленными.

В общих чертах, ***теоретическую основу стохастических операторов составляют конечные поля*** [34], порождаемые в алгебраических системах неполной арифметики. Ближайшим аналогом таких полей, являются поля (доказано, именно поля, а не кольца вычетов, как это нередко трактуется) порождаемые линейным конгруэнтным методом по модулю степени 2 [38]. По сравнению с линейно выраженным характером полей Галуа GF(2) [36,37], представляемые поля носят сильно выраженный экспоненциальный характер [17,18,23,40], что предопределяет их высокую стойкость и эффективность.

При этом в предарифметике, производительность односторонних стохастических операторов в аппаратном исполнении, также как и регистров сдвига с линейной обратной связью (LFSR) в конфигурации Галуа, сравнима ***со скоростью исполнения одной логической операции XOR и не зависит от длины платформы генерации***. Присущая им параллельная архитектура по каждому биту платформы, делает их неуязвимыми к сторонним атакам [46], таким как анализ мощности и временной анализ.

Ко всему, как следует из анализа и имитационного моделирования, базирующегося на общепризнанных пакетах статистических тестов NIST и DIEHARD [43,44.45], прозрачность построения и уникальные (существенно выраженные лавинные, нелинейные и апериодические) свойства стохастических операторов [35,39,41], показывают ***возможность достижения устойчивости таких операторов ко всем видам аналитических атак***. При этом, что особенно важно для подтверждения состоятельности и последующего распространения стохастических технологий, существенно упрощается оценка их криптографической стойкости по А. Кирхгофу [49] – «Шифр не должен зависеть от способов защиты информации и тогда неважно, если он попадет в руки врагов.» (применительно к стохастическим технологиям, измеряемой в элементарных логических операциях, необходимых для полного перебора ключа), которая по существу сводится к оценке статистических свойств, мощности ключевого пространства и нелинейности описывающих их алгоритмов [21].

3.4.2. Технические показатели основных криптографических примитивов

Построенные на основе стохастических операторов криптографические (симметричные) примитивы обладают подавляющим превосходством по всем показателям перед известными аналогами, и позволяют снять существующие проблемы обеспечения безопасности элементов систем и систем в целом.

Математическая прозрачность алгоритмов криптографических примитивов и простота их программной реализации, надежность и стабильность статистических показателей, обязанная используемой алгебраической базе, универсальность и полнота методики оценки устойчивости ко всем видам аналитических атак [21], позволяют дать оценку криптографической стойкости, оп-

тимизировать и рассчитать аппаратные затраты, а также оценить возможное энергопотребление и производительность схем реализаций алгоритмов.

Далее по тексту, приведены показатели реализации основных криптографических примитивов планируемых для практического освоения, построенных на основе нелинейных стохастических технологий, полученные по результатам машинного моделирования и предварительного криптографического анализа.

Аутентификация. Согласно с новым разработанным Протоколом, односторонние и двухсторонние криптографические примитивы аутентификации по криптографической стойкости, аппаратным затратам и энергопотреблению фактически не отличаются между собой. Поэтому, приводимые ниже данные относятся к двухсторонним криптографическим примитивам, предусматривающим проверку подлинности (взаимной аутентификации), как носителей информации (RF-меток и микросенсоров), так и считывающих устройств.

Для реализации указанных примитивов достаточно высокой криптографической стойкости порядка $2^{57\boldsymbol{p}}$ (*1≤**p** ≤4)* на основе стохастических операторов (длина секретного ключа порядка 71***p***), требуется около 40***p*** триггеров и 480***p*** транзисторов (120***p*** логических элементов, GE), при скорости их функционирования в раунде соизмеримой со скоростью срабатывания триггера и выполнением одной логической операции. Для гарантированно надежной аутентификации, в разных случаях требуется 16-30 раундов. При этом, пиковые энергические затраты соизмеримы с затратами в одном раунде. А это, при достаточно высоком уровне криптографической стойкости, по аппаратным и энергозатратам, на порядок меньше, чем у лучших аналогов [8,15].

В оправдание ожиданий, столь малые аппаратные затраты на постановку защиты, в случае экономичного использования почти всегда имеющихся в микрочипе метки малых резервов, вообще не приводят к увеличению себестоимости RF-меток или это увеличение незначительно, в худшем случае на 5-10%, против в 10-15 раз, при использовании имеющихся на сегодня технологий защиты.

Идентификация. Кроме этого, стохастические технологии представляют возможность создания суперпроизводительных микросхем генерации ключей, с любой наперед заданной разрядностью n бит, не имеющих повторений, в пределах периода 2^n и при использовании 1.2 - 0.13μm CMOS технологий, способных генерировать от 0.9 до 27 млрд. ключей в секунду. Причем, для примера, при длинах ключа n, от 36 до 48 бит и криптографической стойкости 2^{2n} (длина секретного ключа 2^{4n} бит), для аппаратной реализации таких генераторов требуется от 1210 до 1370 GE.

Для заметки, использование столь высокоскоростных генераторов позволит, без видимой задержки обеспечить нормальное функционирование систем регламентирования доступа в условиях массированных сетевых атак.

Шифрование. Ко всему, стохастические технологии позволяют создать генераторы шифрования, путем наложения гамм, с периодом повторения сопоставимым с $2^{1.4n}$ и криптографической стойкостью, порядка 2^{2n}. При длинах блоков гаммы 64 и 128 бит, пропускная способность при использовании 1.2 - 0.13μm CMOS технологий составляет 57.6 – 1728 и 115.2 – 3456 Гбит/сек, что на порядки выше существующих аналогов [11] и далеко опережает уровень развития техники. Причем для аппаратной реализации генератора (длина секретного ключа 2^{4n} бит), при длинах блоков гаммы 64 и 128 бит, соответственно требуется около 832 или 1664 GE.

По идее, шифрование /расшифрование информации на основе таких быстродействующих генераторов, можно осуществлять под тактовой частотой процессоров, фактически без уменьшения производительности компьютеров.

Длина платформы генерации, длина секретного ключа и, соответственно, криптографическая стойкость любого из примитивов могут быть сколь угодно увеличены, без потери их производительности и при несущественном увеличении аппаратных и энергозатрат.

Столь высокие показатели криптографических примитивов создают предпосылки, необходимые для осуществления технологического прорыва в сфере обеспечения безопасности, при этом легковесная криптография, как таковая, а тем более криптография с засекреченными нестойкими алгоритмами (Mifare Classic, Hitachi μ-Chip), утрачивает свое содержание, несущее недоверие и серьезные риски [12,15,52,53,54].

Фундаментальный научный и открытый характер решений предоставляемых стохастическими технологиями позволит устранить запретительные барьеры [59], обусловленные особой спецификой криптографической обработки, а также позволит избежать вносимых ими существенных организационно-технических ограничений и привносимых ими потерь.

В частности, стохастические технологии позволяют надежно, максимально эффективно, действенно и высоко рентабельно защитить промышленно освоенные на сегодня RFID метки. При этом ***дополнительные затраты очень малы, а чаще всего не потребуются***, за счет экономичного использования почти всегда имеющихся в микрочипе метки малых резервов.

3.4.3. Результаты апробации стохастических технологий

Результаты исследований были представлены на Братиславской 2003 года [17] и трех Российских 2004–2006 года международных криптографических конференций [25], 2-ой Китайской международной выставке программных продуктов CIS 2006 [27]. В 2006 году проведена предварительная криптографическая экспертиза [21], указывающая на практическую ценность и техническую реализуемость заявленных результатов, полученных на основе линейных стохастических систем.

В 2007 году получили развитие нелинейные стохастические системы, позволяющие существенным образом повысить качество и стойкость решений. На их основе (июнь 2007 года) разработан широкий класс генераторов системы управления ключами и остальные криптографические примитивы (аутентификации, хеширования и шифрования) необходимые для создания инструментальных средств обеспечения безопасности различного назначения и регулируемого уровня стойкости, вполне достаточного для известных практических приложений, ориентированные на среды с крайним дефицитом ресурсов, начиная с сотни логических элементов типа XOR, и сверхскоростную криптографическую обработку, достигающей на имеющейся элементной базе сотни и тысячи Гбит в сек.

На сегодня заложены алгебраические основы построения стохастических систем [16], созданы имитационные модели, необходимые для доказательства выдвинутых алгебраических положений, проведения комплексного статистического и криптографического анализа решений и перевода исследований в практическую плоскость.

Ядро стохастических систем и представляемых ими стохастических технологий, составляет разработанный на основе привносимой Предарифметиками новой алгебраической базы, так называемый, ***рандомизационный способ***. Рандомизационный способ, подлежит патентованию.

Подготовлены две заявки на изобретение, представляющие регулярный и нерегулярный рандомизационный способ, отражающие результаты 20-ти летней работы и исчерпывающе полно охватывающих все ключевые положения технической реализации стохастических технологий и современной симметричной криптографии [16].

Открытая публикация накопленных научных материалов и перспективных технических решений сдерживается недостатком финансирования и коммерческими интересами.

Заключение

«Оборона сильнее наступления».
Карл Клаузевиц

В результате положенных в основу Концепции проведенных работ, впервые, с общесистемных позиций, опирающихся на ***супераддитивную интеграцию физического и логического уровней обработки***, рассмотрена роль и место технологий обеспечения безопасности в развитии общества [28].

Проведенные исследования показывают, что с преодолением отставания современных технологий обеспечения безопасности от уровня развития техники, ***имеются все предпосылки перехода от эволюционного процесса развития информиндустрии, к революционному***.

В централизованной системе управления ключами, на основе предоставления всем категориям потребителей недорогих мобильных средств проверки подлинности и качества продукции, станет возможным осуществить последовательный переход с малоэффективного инспекционного надзора, на ***широкомасштабный, действенный гражданский контроль и защиту сегментов мирового товарного рынка и отраслей экономики от нелегитимных и недоброкачественных товаров и изделий*** [55,56,57]. Даже по самым осторожным оценкам экспертов это по масштабам распространения и отдаче, как и предполагалось в начале, будет означать выход информационно-коммуникационных систем на качественно новый технологический уровень.

Введение полноценной защиты на физическом уровне обработке позволит ***существенно повысить устойчивость и эффективность функционирования системы***, а также качественную информационную и логистическую обработку, за счет разгрузки каналов связи и освобождения логического уровня от несвойственных ему функций.

Ко всему этому ***создается грандиозная по масштабам область приложений био и нанотехнологий***, создаваемых на их основе смарт-материалов и изделий.

Закладывается база для широкомасштабного развертывания высокорентабельных микросенсорных беспроводных сетей, особенно эффективных с внедрением **ПАВ** и **UWB** технологий, ведущая к прорыву в области обеспечения экологической, биологической и физической безопасности, противодействия терроризму.

В итоге, 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 RF-меток и микросенсоров многопрофильными чувствительными мини-датчиками, построенным на основе smart-материалов, представляемых современной био- и наноиндустрией.
4. Создание, по мере освоения помехоустойчивых широкополосных и акустических многоканальных 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 клю-

чами, 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 ближнего действия **NFC** (Near Field Communication) [57,58].

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 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.

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***.

На это указывают проведенные аналитические исследования: «**Предпосылки инновационного прорыва России**», на основе развития микросенсорных технологий, смарт-материалов и технологий обеспечения безопасности. Результаты исследований также показывают, что реализация представленной в части 2 этого документа «**Концепции обеспечения безопасности**», позволит создать реальные условия для осуществления встречного, далеко идущего инновационного прорыва России, по силе превосходящего инновационное развитие стран ЕС и США.

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 [61], 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***.

В заключении следует отметить, что открытие предарифметики предопределяет прорыв не только в области построения систем с существенно выраженным хаотическим поведением и создании стохастической криптографии, по достигнутым результатам и потенциальным возможностям далеко опережающей существующие на сегодня подходы.

Начатые в 2007 году исследования показывают существование множества других предарифметик. ***Следующие из них алгебры способны придать новый импульс развитию математики, физики и естествознания в целом*** [16]. Идущие с этим феноменологические научные результаты и аналогии [40], согласующиеся с достижениями древних цивилизаций и современными экспериментальными данными, ведут к более глубокому и тонкому пониманию мира, созданию и освоению качественно новых технологий в сфере энергетики, радионики и акустики, связи и транспорта, материаловедения и геологии, в сельском хозяйстве, экологии, биологии и медицины.