**127106 Россия, Москва**
**Алтуфьевское шоссе, 5/2**
**Тел**.: +7 (095) 9671451
**Факс**: +7 (095) 9671452
**e-mail**: director@random-art.com

Random Art Labs LTD
Annis Komninis Street 29A, Nicosia, Cyprus

# БИЗНЕС-ПЛАН
## внедрения стохастических систем в сферу высоких технологий

Бизнес-планом представляется новое направление развития высоких технологий, на основе прорыва, совершенного в области построения динамических систем с заметно выраженным недетерминированным, хаотическим поведением, именуемых ***стохастическими системами*** и их применения в криптографических приложениях и сфере абстрактных искусств.

В качестве темы первого плана внедрения решений компании, выбрано одно из наиболее актуальных и социально значимых направлений развития криптографии и технологий ***радиочастотной идентификации*** (**RFID**), связанное с решением задач повышения экономической и финансовой отдачи товарного рынка, обеспечением действенной и рентабельной защиты интеллектуальной собственности, товарной продукции и изделий от клонирования, фальсификации и поделки.

Руководство компании выражает особую благодарность **Московскому комитету по науке и технологиям** за предоставленную возможность проведения научно-технических исследований, а также ОАО **Ангстрем**, **МИФИ**, фирме **ЛанКрипто** и ОАО **Анкад**, российским представительствам компаний **Intel**, **Philips** и **Hewlett-Packard**, принявшим участие в обсуждении материалов приложений и представленные замечания.

**Содержание**



Компания **Random Art Labs Limited** ***(RA-Labs)***, создана 18 декабря 2002 года. Поводом создания компании послужила подготовка и подача заявки на изобретение «Способ придания реальному объекту рандомизационных свойств и рандомизационная система». Заявка на международный патент PCT/RU03/00141, 7 апреля 2003 года. Подана заявка на Евро-Азийский патент.

Компания принадлежит автору изобретения – Кулакову Игорю Анатольевичу, являющегося одновременно директором Компании и которому предоставлено право на ведение переговоров и заключения лицензионных договоров по существу использования изобретения.

**Персонал компании**: директор, научный секретарь и стажер.

## 1. Направления научно-технической деятельности компании

Компания специализируется в области теории и практики построения стохастических систем, включая внедрение в научную сферу и сферу высоких технологий следующих результатов:

1. Исследование систем в *неполной арифметике* и порождаемых ими алгебраических структур, допускающих строгое научное обоснование и практическое подтверждение, простое программное и техническое исполнение, с возможностью достижения предельно высокой, соизмеримой с выполнением *одной логической операции*, скорости организации вычислений.
2. Изучение существенно выраженных недетерминированных и гармоничных, линейных и нелинейных, *взаимно двойственных свойств*, присущих стохастическим системам и природному Хаосу.
3. Развитие новых научных направлений приложений линейных и нелинейных стохастических систем – ***стохастической криптографии*** и ***"гармоничного" хаоса***.

Выбранное направление подтверждается многолетним опытом практической разработки и характеризуется фундаментальным характером, новизной и большим потенциалом используемой теоретической базы.

Продвижение научных и технических разработок компании, производится посредством

- подготовки и публикации научных и методических материалов по теории стохастических систем и ее приложений,
- разработки методик оценки качества стохастических систем, математического и машинного моделирования предполагаемых решений,
- представления и обсуждения результатов на различных научно-практических форумах и конференциях.

В этом направлении проделана следующая работа:

1. Накоплен фактический материал, по основам построения стохастических систем. Готовится публикация первой части, охватывающей класс линейных систем. Отработаны правила и механизмы перехода от класса линейных, в класс нелинейных систем.
2. Заложены основы линейной и нелинейной стохастической криптографии, отвечающих классам линейных и нелинейных систем. Линейным системам присущ ряд недостатков, устраняемых на основе более сильных в криптографическом отношении нелинейных систем. Получены новые результаты в практике построения и применения управляемых операций.
3. Подготовлены полнофункциональные библиотеки алгоритмов и программ, охватывающие все разделы симметричной криптографии, рассчитанные на всевозможные практически значимые вычислительные платформы и уровни криптографической стойкости.
4. Разработаны методики имитационного статистического моделирования, адаптированные под известные **NIST**, **DIEHARD**, **СОК/МИФИ** и другие дополнительные пакеты статистических тестов, позволяющие оценить качество криптографических алгоритмов и эффективность известных криптографических атак.
5. Проведено комплексное тестирование алгоритмов и программ. Отобраны решения оптимальные с точки зрения их практической реализации.
6. Отработаны протоколы управления ключами, идентификации, проверки целостности и поточного шифрования информации, односторонней и взаимной аутентификации элементов систем.
7. Проведена независимая предварительная системно-аналитическая, криптографическая и техническая экспертиза, предназначенных для всеобщего обсуждения типичных (в большинстве своем – линейных), не имеющих весомой коммерческой ценности решений.

По заключениям экспертов и результатам сравнительного анализа, выбранное направление деятельности Компании оценивается как весьма перспективным и продуктивным, а достигнутые результаты теоретически и практически значимыми, отвечающими высокому научно-

техническому уровню, особенно в области симметричной криптографии. Что подтверждается большими потенциальными возможностями выбранного подхода и заметными, подавляющими преимуществами полученных технических решений перед существующими аналогами.

## 2. Порядок продвижения решений компании на рынок

Для реализации своих корпоративных и коммерческих интересов, деятельность Компании направлена на ***оказание услуг в сфере высоких технологий***, связанных с научно-технической специализацией компании, повышения отдачи, расширения масштабов распространения и ускорения продвижения технологий на рынок и включает в себя следующие этапы:

- создание благоприятных условий выхода на рынок,
- закрепление на рынке,
- занятие доминирующего положения на рынке.

Оценивая работу, проведенную Компанией и состояние развития высоких технологий, представляемые компанией разработки отличаются от предлагаемых на рынке решений

- отсутствием конкурентных аналогов, рассчитанных на среды с крайним дефицитом ресурса с одной стороны (например, печатные радиочастотные метки RFID) и сверхскоростную обработку значительных по объему потоков данных (например, сверхширокополосные системы передачи информации), с другой,
- эффективными высокоуровневыми механизмами управления ключами,
- заметным превосходством программных решений и подавляющими преимуществами аппаратных средств перед существующими аналогами.

Все это и возможность всестороннего обоснования действующих прототипов, гарантирующее высокое качество и надежность производимых на их основе программных средств и технических устройств, позволят заполнить существующие капиталоемкие ниши и создать наиболее ***благоприятные условия выхода на рынок***.

Поэтапное освоение ниш, развитие и совершенствование представленных в них технологий, позволит твердо ***закрепиться на рынке*** и охватить все решения компании в целом.

Охват решений компании в целом, особенно в области криптографии, будет способствовать вытеснению с рынка существующих ныне не столь эффективных, отстающих от современных требований традиционных решений и ***занятию доминирующего положения на рынке***.

Однородный, эффективный, легко масштабируемый и интегрируемый характер решений компании представленный на рынке, а также решения в области “гармоничного” хаоса, позволят наиболее полно раскрыть потенциальные возможности, как самих стохастических систем, так и их наиболее значимых коммерческих и прикладных приложений – ***сетевой криптографии*** и ***совершенствовании абстрактных искусств***.

## 3. Политика компании

Исходя из направлений своей научно-технической деятельности и порядка продвижения решений на рынок, Компания строит свою политику исходя из следующих приоритетов:

1. Проведение научных исследований, разработка и приобретение необходимых технических решений. Комплексирование решений и создание, так называемых ***R****andom* ***A****rt* технологий (***RA***-технологий), ориентированных на различные сегменты рынка и оказания необходимых услуг.
2. Участие в совместных проектах по развитию представленных на рынке и разработке высоких технологий, на основе принадлежащих компании ***RA***-технологий. Системная интеграция и адаптация технологий. Разработка и обоснование инструментальных средств.
3. Продажа лицензий на право использования принадлежащих Компании “ноу-хау” и патентов, технологий и инструментальных средств.
4. Оказание услуг типа “инжиниринг”.

5. Осуществление совместной, инновационной и инвестиционной деятельности по внедрению и использованию имеющихся и новых технологий, “ноу-хау”, патентов и разработанных на их основе инструментальных средств.

6. Создание собственных опытных и совместных производств, размещение заказов и реализация принадлежащей Компании продукции.

7. Участие в разработке, сертификация стандартных решений и механизмов их интеграции.

Компания определяет стоимость прав использования принадлежащей ей интеллектуальной собственности, оказываемых услуг и производимой продукции на договорной основе, исходя из конъюнктуры рынка.

## 4. Основные задачи компании. *RA*-технологии

1. Исследования в области стохастических систем, разработка и построение на их основе инструментальных средств и технологий (***RA***-технологий), направленных на более эффективное и качественное решение задач, в следующих областях:

– защита материальных объектов от клонирования, фальсификации и подделки, предотвращение попыток жульничества и воровства,
– регламентирование доступа к защищаемым объектам и информации, упорядочивание движения и учета материальных средств,
– обеспечение информационной и физической безопасности, контроль и поддержание целостности сложных систем,
– представление абстрактных образов и композиций, развитие и совершенствование абстрактных искусств, художественного творчества и мастерства, компьютерного дизайна, подачи и оформления рекламы.

2. Продажа лицензий, предоставляющих право использования инструментальных средств и технологий принадлежащих Компании.

3. Участие в совместных проектах по разработке и внедрению программных и аппаратных средств.

Ориентируясь на потребности рынка и приоритеты компании, криптографические разделы приложений стохастических систем разработаны наиболее полно. Из них, детально проработаны вопросы, связанные с разработкой ***RA-технологий*** и ***инструментальных средств***, а также входящих в их состав функционально законченных решений – ***криптографических примитивов***, необходимых для более эффективного и качественного решения задач симметричной криптографии и их внедрения в сферу высоких технологий (Приложение III).

Приложения, связанные с сильно выраженным детерминированным (гармоничным) характером поведения стохастических систем, способны осуществить качественный скачок в области дизайна и рекламы, рассчитано на перспективу, находится в стадии экспериментальных исследований и опытных разработок.

## 5. Первоочередные задачи реализации *RA*-технологий. Оценка рынка

Среди первоочередных задач внедрения ***RA***-технологий, как наиболее перспективных с точки зрения продвижения решений компании на рынок, отводится задачам защиты материальных объектов от клонирования, фальсификации и подделки, предотвращению попыток жульничества, воровства и других несанкционированных действий на основе технологий RFID:

- защита продукции от клонирования, фальсификации и подделки;
- осуществление мелких денежных расчетов и платежей;
- маркировка и контроль ресурса оборудования, устройств, узлов и деталей, снаряжения, оружия и боеприпасов;
- защита транспортных средств от хищений (угонов), дистанционное выявление похищенных средств;
- электронное клеймение растений, животных, скота и птицы;

- защита и заверение документов и ценных бумаг;
- защита национальной валюты**;**
- другие задачи, включая задачи предотвращения несанкционированного доступа и организации пропускного режима.

Защита продукции от клонирования, фальсификации и подделки может быть эффективно осуществлена в системе защиты товарного рынка от фальсифицированной и контрафактной продукции. Выбор Компанией решения этой задачи в качестве ***темы первого плана*** далеко не случаен и обусловлен следующими факторами:

**Во-первых**, задача защиты товарного рынка от фальсифицированной и контрафактной продукции, сама по себе актуальна и вместе с другими задачами ***в системе регулирования товарного рынка*** (Приложение II), способна совершить экономический переворот в сфере производства и реализации товаров на рынке. При этом, в отличие от существующих ныне непопулярных у населения ведомственных механизмов регулирования рынка, система может быть самоокупаемой, за счет небольшой части отчислений субъектов товарного рынка из получаемой ими дополнительной прибыли.

По данным **IdTechEx** и **HP**:

Увеличение продаж, оценивается в среднем

для продавцов – 3%, для поставщиков – 1%.

Снижение затрат в цепи поставок – 0,4-3%.

50-процентное предотвращение потерь от краж и иных сокращений – 0,9%.

К примеру, если ограничиться 3% приростом прибыли за счет увеличения продаж, ожидаемого снижения затрат и предотвращения сокращений, при 20% части охвата мирового товарного рынка, с оборотом 7 трл. USD, достигнутого за 2004 год, оценка дополнительной прибыли компаний в системе регулирования рынка, может составить:

7000 млрд.· 3% · 20% = 210 млрд.· 20% = 42 млрд. USD.

Если исходить из данных **Applied Business Intelligence**, предполагаемые затраты на систему регулирования рынка, могут составить:

- разработка системы и создание необходимой инфраструктуры – $360 млн.,
- развертывание системы – $1,3 млрд.,
- поддержание и развитие системы – $1,7 млрд. в год.

Таким образом, при отчислениях субъектов товарного рынка из получаемой ими дополнительной прибыли в 10%, т.е. 42 млрд.· 10% = 4,2 млрд. USD, вложения в систему окупаются в течение года и в дальнейшем, могут приносить ощутимую прибыль. Полученная прибыль в $2,5 млрд. и более в год, может направляться на стимулирование развития систем RFID и защиты товарного рынка от фальсифицированной и контрафактной продукции, путем целевых компенсаций затрат на маркировку продукции (50%), считывающие устройства индивидуального назначения (10%) и специальные криптографические модули проверки подлинности радиочастотных меток (40%), прилагаемых к ним.

**Во-вторых**, в основе защиты лежит идея привлечения широких слоев населения к контролю товарного рынка, на основе общедоступных в пунктах продажи и недорогих индивидуальных устройств проверки подлинности приобретаемого товара. По сути, в отличие от предпочитаемых ныне силового давления и сдерживающих властных ограничений, тем самым подключаются дополнительные сильные механизмы, позволяющие осуществить последовательный и взвешенный переход от малоэффективного ведомственного государственного контроля, ***к широкомасштабному действенному общественному контролю товарного рынка***.

По данным компании **HP**, в настоящее время, доля поддельной продукции колеблется от 5% в сфере производства товаров широкого потребления, 8% в сфере реализации лекарственных препаратов и до 12% от проданных в Европе игрушек, что составляет в среднем около 7% всей мировой торговли на западных рынках, при резко наметившимся 50% приросте в год.

В 2004 году, объем поддельной продукции на мировом рынке составил около $800 млрд. При этом, по разным оценкам, прямые потери товаропроизводителей составляют около 3%, а

налоговых органов порядка 10%, от этой суммы. Принимая снижение доли поддельной продукции на рынке в два раза, предотвращаемый ущерб товаропроизводителей от фальсифицированной и контрафактной продукции может составить (800 млрд.· 3%) / 2 = 12 млрд. USD. Учитывая интересы производителей, 50% часть этой суммы, с суммой целевых компенсаций в 2,5 млрд.· 50% = $1,25 млрд., а именно 12 млрд. · 50% + 1,25 млрд. = $7,25 млрд., вполне способна оправдать расходы предприятий на маркировку производимой ими продукции.

**В-третьих**, по общему мнению специалистов, без прорыва в области производства дешевых (печатных, пластиковых, кремниевых) радиочастотных меток и недорогих устройств проверки подлинности меток, а также достижений Компании в области ***минималисткой криптографии***, предполагающей реализацию в условиях крайнего дефицита ресурсов устойчивых к "взлому" криптографических устройств, действенное и рентабельное решение задачи защиты продукции от клонирования, фальсификации и подделки, не представляется возможным.

Исходя из суммы (1 млрд. + 7,25 млрд.) · 60% = 8,25 млрд.· 60% = 5 млрд. USD, от 60% всех меток RFID, отводимой на маркировку товаров на основе пассивных дешевых печатных, пластиковых, кремниевых радиочастотных меток (RF-меток), защищенных от клонирования и подделки по ***RA***-технологии, при первоначальной стоимости 2, 4 и 15 центов, в пропорции 60%, 30% и 10%, соответственно, можно ожидать следующие объемы производства:

- печатные RF-метки – (5 млрд.· 60% · 100) / 2 = 150 млрд. штук;
- пластиковые RF-метки – (5 млрд.· 30% · 100) / 4 = 37 млрд. штук;
- кремниевые RF-метки – (5 млрд.· 10% · 100) / 15 = 3 млрд. штук.

В итоге, данным объемом радиочастотных меток, можно промаркировать и защитить от клонирования, фальсификации и подделки около 200 миллиардов единиц товара.

По самым общим оценкам, можно ожидать, что с введением системы регулирования рынка, общая сумма, затрачиваемая на производство пассивных радиочастотных меток и специальных криптографических модулей проверки их подлинности, может составить

2,5 млрд.· 40% + 5 млрд. = 6 млрд. USD.

Если следовать прогнозам **IdTechEx**, годовой прирост этой суммы может составлять 20%, который предполагает ее удвоение за первые 5 лет. При планируемом уменьшении стоимости RF-меток в два раза, это позволит защитить от подделки более 800 миллиардов единиц товара.

### 6. Развитие *RA*-технологий. Расширение рынка

Обращаясь к ***задачам второго плана***, определяющих по существу расширение рынка, центральное место отводится достижениям Компании в области построения систем управления ключами и генераторов ключевого потока, становления минималисткой криптографии и развития ***RA***-технологий. А именно:

**Во-первых**, от эффективности решения задач регулирования товарного рынка на основе разработанных Компанией инструментальных средств, необходимых для обеспечения безопасности технологий RFID, решающим образом зависит эффективность решения и других, не менее актуальных, по архитектуре построения во многом схожих между собой задач, связанных с защитой материальных объектов от клонирования, фальсификации и подделки.

По самым общим оценкам, задачи осуществления мелких денежных расчетов и платежей, маркировки и контроля ресурса оборудования, узлов и деталей, электронного клеймения растений и животных, защиты транспорта от хищений, заверения документов и ценных бумаг, защиты национальной валюты и другие задачи, включая задачи предотвращения несанкционированного доступа и организации пропускного режима, по капиталоемкости все вместе могут составлять порядка 20% от капиталоемкости рынка пассивной защищенной RFID, т.е.

6 млрд.· 20% = 1,2 млрд. USD

с годовым приростом порядка 15%.

**Во-вторых**, минималистская криптография допускает естественное аналитическое обобщение и прозрачность обоснования, а ***RA***-технологии масштабирование и распространение на любые другие, включая сверхбольшие вычислительные платформы, производительностью более 1 Гбайт/сек, и при этом отличаются простотой технической реализации и позволяют обеспечить необходимый высокий уровень криптографической стойкости.

На этом этапе представляет интерес по решению задач обеспечения безопасности мобильных и стационарных систем связи, сетей спутникового и кабельного телевидения, защиты вычислительной техники, ее информационных носителей и периферийных устройств на основе электронных ключей и замков, криптографических сопроцессоров или встраиваемых в процессоры апробированные элементы криптозащиты.

В целом, капиталоемкости этого рынка, может превосходить капиталоемкости рынка пассивной защищенной RFID, в 2 раза и составлять

5 млрд.· 2 = 10 млрд. USD

с годовым приростом порядка 10%.

**В-третьих**, развитие стохастической криптографии и ***RA***-технологий, их более разностороннее практическое, глубокое теоретическое и методически совершенное обоснование с охватом все большего числа приложений, позволят придать разработкам законченный, научно и технически грамотный, всесторонне исследованный и изученный, общедоступный для различных категорий и широкого круга специалистов и разработчиков, индустриальный характер.

В этом плане очень перспективными выглядят задачи обеспечения экологической безопасности и защиты от терроризма на основе миниатюрных сенсорных устройств – интеллектуальной пыли.

Заглядывая в ближайшее будущее, еще большие возможности могут быть достигнуты при переходе на ***наноэлектронные технологии***. Это обусловлено простой топологией и линейной архитектурой ***RA***-технологий, что может быть весьма привлекательным для первых практически значимых конструкторских разработок в области наноэлектроники и организации опытных производств.

В общем итоге, ***емкость рынка*** охватываемого ***RA***-технологиями и предполагаемой патентной защитой, может оцениваться суммой, от $15 млрд., с 10% годовым приростом.

## 7. Состояние *RA*-технологий. Предупреждение рисков

Объективно, ***RA***-технологии характеризуются малой известностью и своей относительной молодостью, если судить исходя из даты регистрации заявка на международный патент, а это 2003 год, когда открытая публикация не коммерчески значимой части материалов стала возможной. На самом деле, технология не так уж и молода, если принять во внимание более чем десятилетний период разработки, предшествующий оформлению и подаче международной заявки.

С внедрением ***RA***-технологий, а также разрабатываемых на их основе устройств и систем, по мнению специалистов по системной аналитике, схемотехническим решениям и криптографии связаны следующие ***риски***:

1. Неосуществимость механизмов интеграции элементов систем и протоколов защиты.
2. Невозможность аппаратной реализации решений и достижения их надлежащих технических и стоимостных показателей. Уязвимость устройств к сторонним атакам.
3. Компрометация статистической надежности и криптографической стойкости предлагаемых инструментальных средств.

Для обоснования и подтверждения практической реализуемости ***RA***-технологий, в 2004-2005 г., совместно с **Московским комитетом по науке и технологиям** была проведена промежуточная НИОКР, по теме ***Система контроля сертификационных меток промышленных товаров***, на основе технологий RFID (Приложение IV). Система получила свое дальнейшее развитие в ***Концепции регулирования товарного рынка*** (Приложение II) и исследовательской работе проведенной Компанией по ***Обеспечению безопасности технологий RFID*** (Приложение I).

В дополнение к этому, обращаясь к ***Аналитическому обзору RA***-технологий, приведенному в Приложение III, заключениям экспертов и дополнительным решениям по устранению замечаний, отраженным в Приложение IV, а также к результатам разработки, рассчитанного на различные вычислительные платформы набора инструментальных средств и их машинного моделирования, по представленным *типичным открытым решениям*, можно сделать следующие общие выводы:

1. Разработанные на основе ***RA***-технологий генераторы ключевого потока и многоуровневые протоколы управления ключами, позволяют организовать сетевую обработку, необходимую для построения сложных распределенных систем, интеграции и защиты ее элементов.
2. Инструментальные средства представляемые Компанией допускают эффективную аппаратную реализацию в условиях крайнего дефицита ресурсов. Построенные на их основе устройства, фактически обладают предельно высокой производительностью и требуют малых аппаратных затрат, не сказывающихся на рентабельности их производства.
3. Устройства, разрабатываемые на основе ***RA***-технологий, за счет параметризации и полного параллелизма не уязвимы к сторонним атакам. Зависимость секретных ключей от существенных внешних признаков защищаемых объектов и многоуровневые протоколы защиты мастер ключей, делает их устойчивыми и к физическому взлому.
4. Инструментальные средства обладают статистической надежностью, подтверждаемой на основе проверенных пакетов статистических тестов, достаточной для их практического использования.
5. Имитационное статистическое моделирование линейных, дифференциальных и корреляционных атак, представленных инструментальными средствами криптографических примитивов, дает основание предполагать о возможности достижения необходимого уровня криптографической стойкости построенных на их основе устройств.

Как следует из представленных положений, в зону рисков попадают инструментальные средства, к которым предъявляются высокие требования к их криптографической стойкости, а имитационное моделирование не дает гарантий выполнения этого требования.

Результаты имитационного моделирования подтверждаются на примере криптографического анализа 32-х разрядного алгоритма односторонней аутентификации, проведенного экспертом фирмы **ЛанКрипто** (раздел 3, Приложения IV). Результаты анализа допускают масштабирование и распространение, на другие криптографические платформы и примитивы односторонней и взаимной аутентификации, псевдослучайные функции и операторы, а также, при введении соответствующих усилений и на генераторы гаммы, хеш-функции и операторы выработки показателей контроля целостности информации. А это, без учета генераторов ключевого потока, фактически вся и значительная часть инструментальных средств стохастической криптографии, причем часть, находящаяся в зоне особо сильных криптографических рисков.

Не смотря на полученные вполне достаточные для практической реализации результаты, представленный алгоритм аутентификации предполагает ряд усилений, не учтенных в атаке, позволяющих существенным образом улучшить его статистические и криптографические показатели (раздел 4, Приложения III). Из них, особенно эффективна замена алгоритма его нелинейным аналогом, позволяющая устранить присущие линейным системам серьезные недостатки.

Обращаясь к представленным результатам, ***в условиях минимальных рисков и технической готовности для практической реализации*** инструментальных средств, представляется целесообразным перевод лабораторных исследований Компании в стадию подготовки технического проекта, изготовления прототипа и его стендовых испытаний.

В качестве первой, наиболее приоритетной задачи предполагающей развитие минималисткой криптографии, предлагается реализация ***Проекта обеспечения безопасности технологий RFID***, представленного в (Приложении I). Центральным местом проекта, является реализация протокола проверки подлинности (аутентификации) меток RFID.

Для снятия рисков компрометации криптографической стойкости инструментальных средств ***RA***-технологий в этой части, считается целесообразным провести разработку ***программного обеспечения I-ой очереди*** по детальному анализу алгоритма аутентификации с учетом его усилений и переменным числом раундов, начиная с 1, для различных платформ, от 8 до 64 бит, а также соответствующего ему алгоритма генератора гаммы. При выборе состава атак для анализа, следует руководствоваться критериями сбалансированности и минимальной достаточности, т.к. иное может существенным образом сказаться на качестве и стоимости проводимых работ. Состав программного обеспечения (см. раздел 3.3, Приложения IV), исполнители, оплата и сроки проведения работ, согласуются сторонами и отражаются в задании на разработку.

Разработка более чем оправдана, если принять к сведению высокую квалификацию экспертов, положительные результаты криптографической экспертизы и общую оценку ***RA***-технологий. Общая оценка – перспективность, подавляющие преимущества и высокие потенциальные возможности ***RA***-технологий, нашла свое обоснование в Приложении III.

Программное обеспечение позволит оптимизировать структуру генератора гаммы и алгоритм аутентификации по числу раундов и наращиваемым по эффективности усилениям, для всех супермалых платформ, длиной 8, 16, 24, 32 и 36 бит, рассчитанных на обеспечение защиты печатных, пластиковых и кремниевых меток RFID.

Представленный выше набор инструментальных средств ***RA***-технологий завершают генераторы ключевого потока. Генераторы ключевого потока подразделяются на ***равноповторные*** и ***бесповторные*** генераторы.

Равноповторные генераторы – это, по сути, генераторы гаммы с очень малой, присущей им вероятностью повторения формируемых на их основе ключей, вычисляемой по формуле:

$$P = N / 2^{n},$$

при длине платформы генерации $n$ бит и общем числе ключей $N$. На этот тип генераторов распространяются криптографические риски, рассмотренные чуть ранее.

Бесповторные генераторы имеют период повторения, равный $2^n$ и в пределах этого периода не имеют одинаковых ключей. Как правило, бесповторные генераторы используются в тех случаях, когда пусть даже ничтожно маловероятные коллизии, могут вызвать крайне нежелательные эффекты.

Из них в зоне рисков находятся генераторы с секретным ключом, предназначенные для генерации открытого или секретного ключевого потока, высокой криптографической стойкости и при этом способных функционировать в условиях крайнего дефицита ресурсов. Последнее требование исключает возможность использования адресуемой памяти по объему, соизмеримым с формируемым объемом ключевого потока, когда за счет известных механизмов недетерминированного назначения ключей из потока, достижение высокой криптографической стойкости становится потенциально возможным.

Следуя строгим криптографическим правилам и жестким техническим ограничениям, далее везде рассматриваются генераторы открытого ключевого потока, ориентированные на среды с крайним дефицитом ресурса, как наиболее критичные для реализации и уязвимые для различного рода атак.

Как показывает опыт, имитационное моделирование, проведенное Компанией, необходимо, но недостаточно для обоснования криптографической стойкости генераторов.

В данный момент, в рамках предлагаемого для реализации ***Проекта обеспечения безопасности технологий RFID***, это не является сдерживающим фактором. Действительно, если обратиться к технологиям RFID, то для создания полновесной системы управления ключами, необходимой для обеспечения работоспособности и безопасности технологий, требуются следующие генераторы ключевого потока, а именно:

- генераторы идентификаторов меток и считывающих устройств;
- генераторы транспортных ключей, используемые при транспортировке меток;
- генераторы секретных ключей аутентификации меток;
- генераторы ключей блокировки/разблокировки меток;
- генераторы идентификаторов ярлыков на элементы входящие в состав упаковки.

Из представленного выше списка, только первые два типа генераторов относятся к классу бесповторных. Рационально принять, что в качестве транспортных ключей используются идентификаторы меток. Не делая различий между генераторами идентификаторов меток и считывающих устройств, задача сводится к бесповторному генератору ключевого потока с секретным ключом. Учитывая централизованный уровень выделения ключей, для реализации генераторов этого класса могут быть выделены достаточные вычислительные ресурсы, путем их программной реализации на выпускаемых серийных персональных компьютерах. При использовании известных механизмов недетерминированного назначения ключей из потока, становится возможным достижение высокой криптографической стойкости генераторов.

С разработкой Программного обеспечения I-ой очереди, ***снимаются криптографические риски***, связанные с реализацией не только генераторов ключевого потока, но и предлагаемого для реализации ***Проекта обеспечения безопасности технологий RFID***, в части приложений, связанных с ***защитой товарного рынка от фальсифицированной и контрафактной продукции***.

Для снятия рисков компрометации криптографической стойкости инструментальных средств ***RA***-технологий в целом, считается целесообразным произвести доработку и адаптацию под бесповторные генераторы ключевого потока, упомянутого программного обеспечения.

В ***программное обеспечение II-ой очереди*** следует включить детальный анализ криптографической стойкости генераторов, включая корреляционную атаку, на младшие биты дихотомических последовательностей, используемых в качестве исходных для формирования бесповторного ключевого потока.

Данная разработка более чем оправдана, если принять во внимание отсутствие каких-либо известных конкурентных решений способных с такой же эффективностью использоваться в условиях крайнего дефицита ресурсов, включая упомянутые ранее дополнительные факторы, такие как перспективность и высокие потенциальные возможности ***RA***-технологий.

Программное обеспечение позволит оптимизировать алгоритм генерации по числу раундов, от малых платформ, длиной 16, 24, 32 (36), 48 и 64 бит, до очень больших, длиной 512, 1024, 2048 и 4096 бит, рассчитанных на обеспечение технологий RFID, системы связи и распространения открытых ключей, предотвращения несанкционированного доступа и другие приложения.

Ориентируясь на конкретные результаты, создание Программного обеспечения I и II-ой очереди, а также создание ***Программного обеспечения III-ей очереди*** рассчитанного на алгоритмы взаимной аутентификации, предназначенного для проведения анализа и подтверждения криптографической стойкости инструментальных средств ***RA***-технологий, создаст реальные предпосылки для занятия доминирующего положения Компании на рынке.

Кроме этого, проводимый на его основе анализ, позволит оптимизировать реализацию решений, повысить их качество и эффективность.

## 8. Организация сотрудничества

Исходя из фундаментального, не проходящего по времени, характера используемых результатов, объема реальных решенных задач и потенциальных возможностей технологий, организация сотрудничества с заинтересованными сторонами строится на долгосрочной, среднесрочной и краткосрочной основе.

Цели сотрудничества:

1. Научно-техническое обоснование и развитие технологий.
2. Опытное проектирование и промышленное внедрение технологий.
3. Ускорение продвижения технологий на рынок.
4. Получение максимальной финансовой отдачи от внедрения технологий.
5. Подготовка специалистов в области стохастических систем и их приложений.

В условиях минимизации взаимных рисков, в зависимости от глубины научно-технических разработок и объема проводимых работ, перспектив, а также масштабов охвата рынка и внедрения практических результатов, сотрудничество предполагает следующую динамику развития отношений сторон:

1. Совместная деятельность, нацеленная на конечный технический и экономический результат.
2. Долговременное сотрудничество по направлениям – микроэлектроника, системы безопасности, информационные системы и сети, телевидение, связь и другим техническим отраслям.
3. Стратегическое партнерство в промышленной, социальной, технической и академической сферах.

Компания планирует следующие источники финансовых поступлений от своей коммерческой деятельности:

1. Продажа лицензий на право использования принадлежащих Компании “ноу-хау” и патентов, технологий и разработанных на их основе инструментальных средств. Оказание по заключенным договорам дополнительных услуг типа “инжиниринг”.
2. Внедрение и использование принадлежащих Компании исключительно или на правах совместной собственности “ноу-хау”, патентов, технологий и инструментальных средств.
3. Продажа программных и аппаратных средств, ориентированных на решение конкретных технических задач.
4. Создание собственных опытных и совместных производств, размещение заказов и реализация принадлежащей Компании продукции.
5. Реализация совместных проектов по развитию и совершенствованию представленных на рынке высоких технологий.
6. Проведение совместных научно-технических исследований и разработок, ориентированных на различные сегменты рынка. Оказание необходимых услуг по разработке и внедрению специальных программных и технических средств.
7. Сертификация стандартных решений, предоставление механизмов их интеграции и оказание консультационных услуг.

Для инвесторов, технических разработчиков и других потенциальных потребителей, деятельность Компании может представлять следующий коммерческий интерес:

1. Приобретение лицензий или в исключительных случаях получение процентных отчислений от лицензий, на право использования принадлежащих Компании “ноу-хау”, патентов, технологий и инструментальных средств.
2. Получение процентных отчислений из прибыли от совместной деятельности сторон.
3. Приобретение в собственность программных и аппаратных средств, ориентированных на решение конкретных технических, коммерчески и социально значимых задач, а также на повышения эффективности и качества действующих систем.

Компания строит свою работу исходя из конъюнктуры рынка, на взаимовыгодной договорной основе.

## 8. Порядок внедрения и финансовая отдача *RA*-технологий

Следуя прогнозам аналитиков и опираясь на результаты проведенных исследований, в целях преодоления жесткой конкуренции, минимизации затрат на разработку, получения максимальной социальной и финансовой отдачи от внедрения ***RA***-технологий, Компания в своей деятельности исходит из нижеследующих приоритетов.

**Задачи первого плана**, связанные с вхождением в рынок.

**I этап**. «***Разработка дешевых защищенных радиочастотных меток и элементов совместимости со считывающими устройствами***».

Данный проект является неотъемлемой, базовой частью общего проекта «***Обеспечения безопасности технологий RFID***», представленного в Приложении I и включает в себя следующий комплекс работ:

1. Научно-техническое обоснование способов односторонней аутентификации объектов на основе ***RA***-технологий и выработки эффективных механизмов защиты.
2. Проведение статистического анализа аутентификаторов полихотомического типа, предназначенных для промышленной реализации и имитационно-статистического моделирования криптографических атак, с учетом возможных вариантов усилений защиты.
3. Разработка программного обеспечения I-ой очереди и проведение детального криптографического анализа типичного, открытого для анализа алгоритма аутентификации и соответствующего ему генератора гаммы, с учетом их усилений, на возможность "взлома".
4. Распространение результатов детального криптографического анализа типичных вариантов реализации на аутентификаторы предназначенные для промышленной реализации.
5. Оптимизация структуры и параметров аутентификаторов по числу логических элементов, производительности и энергопотреблению, не сказывающаяся на конечной криптографической надежности данных систем.
6. Выбор схемотехнических решений и разработка топологии аутентификатора RF-метки и верификатора считывающего устройства. Проведение стендового моделирования и доработка опытных образцов, из расчета реализации на кристалле кремния.
7. Изготовление на кристаллах кремния прототипа метки RFID и верификатора считывающего устройства. Проведение стендовых испытаний.
8. Подготовка технической документации необходимой для налаживания промышленного производства дешевых защищенных кремниевых RF-меток и верификаторов считывающих устройств.

Общая стоимость работ, проводимых на Российской научно-технической и производственной базе, составляет  USD. Затраты экономически оправданы, если учесть даже одно, что стоимость надежных в криптографическом отношении дешевых RF-меток производимых на основе беспроцессорных ***RA***-технологий, приблизительно в 4-7 раза меньше, чем стоимость выпускаемых ныне на основе процессорных технологий защищенных меток RFID. При этом производительность беспроцессорных меток может превышать в 10, а энергопотребление может быть ниже в 5 и более раз процессорных меток RFID.

Как показывают исследования, представленный проект масштабируется на печатные и пластиковые, очень дешевые защищенные RF-метки, стоимостью несколько, а в ближайшем будущем 1-2 евроцента. На основе процессорных технологий, обеспечение рентабельной защиты меток этого типа – не реалистичная задача. При наличии соответствующих технических условий, стоимость реализации каждого из этих проектов на зарубежной базе является предметом переговоров и главным образом зависит от стоимости изготовления прототипа печатной и пластиковой защищенной метки RFID.

**II этап**. «***Обеспечение безопасности технологий RFID в системе защиты товарного рынка от фальсифицированной и контрафактной продукции***».

Данный проект закладывает основу для решения актуальной и наиболее перспективной с точки зрения продвижения решений компании на рынок, задачи защиты материальных объектов от клонирования, фальсификации и подделки.

Проведенный анализ показывает, что наиболее эффективно и рентабельно эта задача может быть решена в системе регулирования товарного рынка, рассмотренной в приложении II.

В целом, система регулирования товарного рынка предполагает решение следующих задач:

1. Придание прозрачности товарному рынку (государственной, маркетинговой и общественной), достижение и поддержание оптимально сбалансированных пропорций между спросом и предложением на товарную продукцию.
2. Оптимизация цепей поставок, хранения и реализации товаров.
3. Защита товарного рынка от фальсифицированной и контрафактной продукции.

Первые две задачи образуют логический уровень системы, основу которой, как это предусмотрено концепцией **EPC**global, составляют распределенные базы данных и средства коммуникации с ними.

В отличие от них, задача защиты товарного рынка от фальсифицированной и контрафактной продукции решается на независимом от них физическом уровне, основу которого составляют дешевые защищенные метки RFID и считывающие устройства, объединенные в логическое целое централизованной системой управления ключами.

Как показывают исследования и заключения аналитиков, недостатки присущие системам, построенным на основе концепции **EPC**global, не являются сдерживающим фактором для внедрения технологий RFID для обеспечения рентабельной, эффективной и действенной защиты продукции от клонирования, фальсификации и подделки. Решению этой задачи составляет основную часть упомянутого проекта «***Обеспечения безопасности технологий RFID***» и включает в себя следующий комплекс работ:

1. Научно-техническое обоснование системы защиты материальных объектов от клонирования, фальсификации и подделки, на основе ***RA***-технологий и технологий RFID.
2. Разработка многоуровневой системы управления ключами и генераторов ключевого потока системы.
3. Разработка основных Протоколов изготовления, транспортировки, активации, деактивации и реактивации защищенных меток RFID и Протоколов обслуживания верификаторов считывающих устройств. Проведение криптографического анализа Протоколов.
4. Проведение статистического анализа генераторов ключей и имитационно-статистическое моделирование возможных криптографических атак.
5. Разработка программного обеспечения II-ой очереди и проведение детального криптографического анализа базового алгоритма генерации ключей, с учетом его усилений, на возможность “взлома”.
6. Распространение результатов детального криптографического анализа на другие типовые варианты реализации генераторов.
7. Оптимизация структуры и параметров генераторов по числу логических элементов, производительности и энергопотреблению, не сказывающаяся на конечной криптографической надежности данных систем.
8. Разработка конструкций элементов сопряжения генераторов ключей и верификаторов стационарных, мобильных и индивидуальных считывающих устройств.
9. Выбор схемотехнических решений и разработка топологии генератора ключей и верификатора мобильного считывающего устройства. Проведение стендового моделирования и доработка опытного образца.
10. Изготовление прототипа считывающего устройства на базе мобильного телефона выбранного образца. Проведение стендовых испытаний прототипа.
11. Подготовка технической документации необходимой для налаживания промышленного производства стационарных, мобильных и индивидуальных считывающих устройств и верификаторов к ним.

Общая стоимость работ, проводимых на Российской научно-технической и производственной базе, составляет [redacted] USD. Затраты более чем оправданы, если учесть социальную и финансовую отдачу в сотни миллионов долларов (раздел 5 бизнес-плана), лишь только от внедрения системы регулирования товарного рынка и защиты продукции от клонирования, фальсификации и подделки.

**III этап**. «***Инструментальные средства обеспечения безопасности технологий RFID***»

Реализация данного проекта, в отличие от Протокола односторонней аутентификации, используемого на I этапе для защиты меток RFID, предполагает введение Протокола взаимной аутентификации, используемого при осуществлении мелких денежных расчетов и платежей на основе дешевых радиочастотных смарт-карт (**RF/s**-карт).

Все рассмотренные выше криптографические примитивы, совместно с криптографически стойкими генераторами гаммы пригодными для поточного шифрования и генераторами ключевого потока, используемыми для предотвращения несанкционированного доступа, составляют инструментальные средства «***Обеспечения безопасности технологий RFID***».

Создание такого набора инструментальных средств означает полнофункциональную, значимую уже саму по себе, реализацию концепции ***минималисткой симметричной криптографии***, позволяющей наиболее полно раскрыть потенциальные возможности и в конечном итоге осуществить широкомасштабное внедрение и распространение технологий RFID (см. раздел 5 бизнес-плана).

Реализация данного проекта во многом аналогична проекту I-го этапа и включает в себя следующий комплекс работ:

1. Аналитический обзор инструментальных средств ***RA***-технологий и обеспечения безопасности технологий RFID.
2. Научно-техническое обоснование способов взаимной аутентификации объектов на основе ***RA***-технологий и выработки эффективных механизмов защиты.
3. Проведение статистического анализа двухсторонних аутентификаторов полихотомического типа и имитационно-статистического моделирования криптографических атак, с учетом оптимальных вариантов усиления защиты.
4. Разработка программного обеспечения III-ой очереди и проведение детального криптографического анализа типичного, открытого для анализа алгоритма взаимной аутентификации и соответствующего ему генератора гаммы, с учетом их оптимальных усилений, на возможность “взлома”.
5. Распространение результатов детального криптографического анализа типичных вариантов реализации на аутентификаторы предназначенные для промышленной реализации.
6. Оптимизация структуры и параметров аутентификаторов по числу логических элементов, производительности и энергопотреблению, не сказывающаяся на конечной криптографической надежности данных систем.
7. Выбор схемотехнических решений и разработка топологии аутентификатора RF/s-карты и верификатора считывающего устройства. Проведение стендового моделирования и доработка опытных образцов, из расчета их реализации на кристалле кремния.
8. Изготовление на кристаллах кремния прототипа RF/s-карты и верификатора считывающего устройства. Проведение стендовых испытаний.
9. Подготовка технической документации необходимой для налаживания промышленного производства дешевых кремниевых RF/s-карт и верификаторов считывающих устройств.

Общая стоимость работ, проводимых на Российской научно-технической и производственной базе, составляет [redacted] USD. Затраты экономически оправданы, если учесть даже только одно, что стоимость надежных в криптографическом отношении дешевых радиочастотных смарт-карт производимых на основе беспроцессорных ***RA***-технологий, приблизительно в 7-10 раза меньше, чем стоимость RF/s-карт выпускаемых ныне на основе процессорных технологий. При этом производительность беспроцессорных карт может превышать в 10-20, а энергопотребление может быть ниже в 5-7 и более раз процессорных карт.

Как показывают исследования, представленный проект также масштабируется на печатные и пластиковые, очень дешевые RF/s-карты, стоимостью 2-3 евроцента. При наличии соответствующих технических условий, стоимость реализации каждого из этих проектов является предметом переговоров и главным образом зависит от стоимости изготовления прототипа печатной и пластиковой радиочастотной смарт-карты.

**Задачи второго плана**, связанные с закреплением на рынке.

При решении задач второго плана, Компания ориентируется на сегменты рынка, связанные с высокоскоростной передачей и обработкой больших объемов информации, причем там, где обеспечение информационной безопасности на основе выбранных криптографических методов обходится очень дорого или существенно сказывается на качественных характеристиках, либо не отвечает требуемому уровню защиты или технически неосуществима.

Среди них можно выделить стационарные и мобильные (CDMA) системы широкополосной связи, радиолокационные системы, системы спутникового и кабельного телевидения, системы сверхширокополосного доступа (UMB), устройства обработки графической информации, системы распределения ключей и системы разграничения доступа на основе динамических ключей.

Проведенные Компанией исследования показывают, что эффективно и качественно решить эти задачи можно на основе минималисткой криптографии путем ее масштабирования на большие и сверхбольшие платформы, либо набирать платформы необходимых размеров из дешевых стандартных криптографических модулей.

**Задачи третьего плана**, связанные с занятием доминирующего положения на рынке.

В силу явного превосходства инструментальных средств ***RA***-технологий над существующими аналогами начиная с супермалых до супербольших платформ и их высокой, регулируемой в необходимых пределах криптографической стойкости, решение задач первого и второго плана, позволят естественным образом охватить всю симметричную криптографию и ее приложения в целом.

Иными словами, ***RA***-технологии предоставляют возможность существенного повышения эффективности и качества существующих систем, а также снимают серьезные барьерные ограничения, вызываемые заметным отставанием известных решений от современных требований.

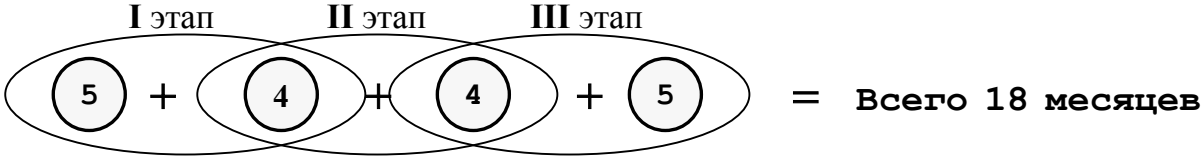
**Перспективы развития *RA*-технологий**

Исследования, проводимые компаниями **Hewlett-Packard** и **Siemens**, достижения других ведущих исследовательских групп в области био- и наноэлектроники, а также прогнозы компаний производителей микроэлектроники **Ангстрем, Intel** и **Philips**, дают основания полагать, что ассортимент и объемы предлагаемых на рынке радиочастотных меток будет расти, а стоимость неуклонно уменьшаться, при заметном росте их функциональных возможностей.

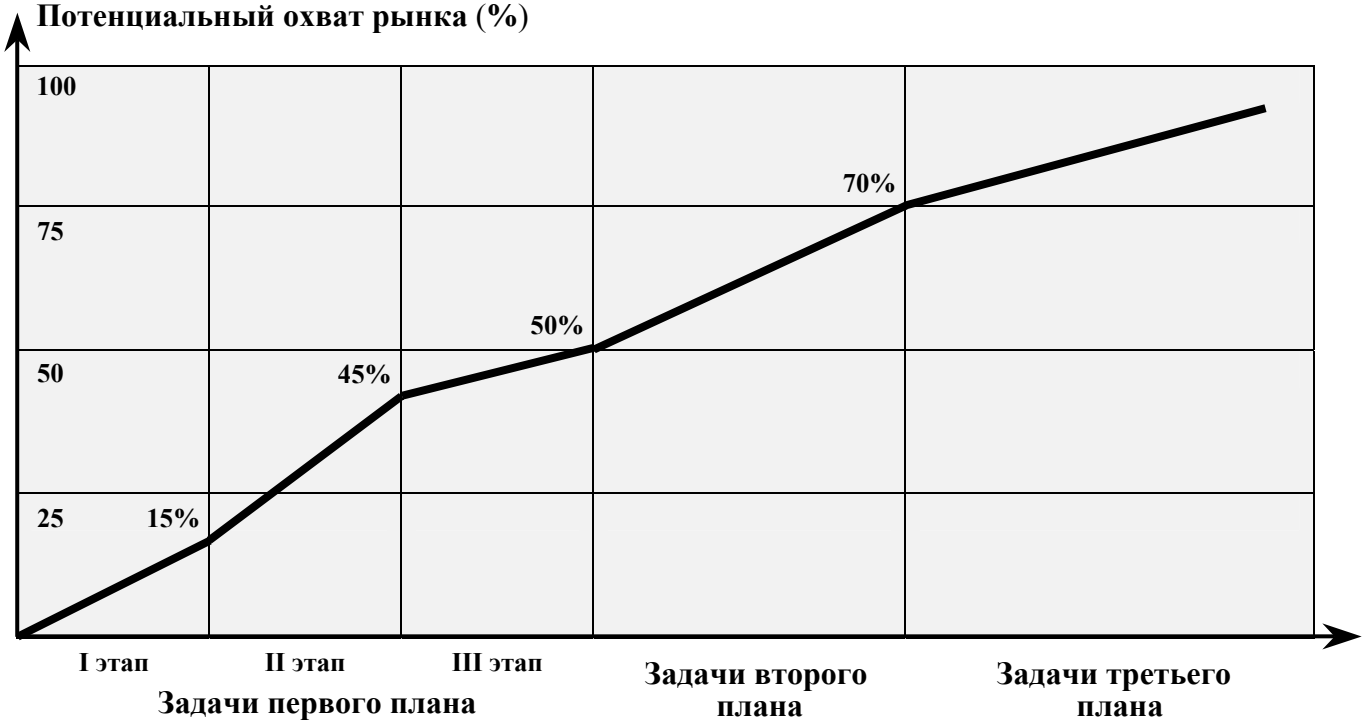
В свою очередь, новая физика параллельных вычислений заложенная в ***RA***-технологиях, их простая топология и линейная архитектура, позволят не только ускорить процесс практического внедрения био- и наноэлектроники, но и смогут послужить реальной основой, необходимой для создания сетевых технологий нового поколения - ***интеллектуальной кремниевой*** "***пыли***", ***интеллектуальных био***- и ***нанокремнеевых структур***.

Исходя из готовности разработок Компании, а также предварительных договоренностей с фирмой **ЛАН Крипто** (www.lancrypto.com), по созданию программного обеспечения и проведению детального криптографического анализа, а также договоренностей с компанией ОАО **Ангстрем** (www.angstrem.ru/english), по разработке топологии и изготовлении прототипов предусмотренных проектами микросхем, сроки реализации каждого из этапов задач первого плана составляют 9 календарных месяцев.

Работы допускают перекрытие, представленное ниже графом. В этом случае общий срок реализации трех представленных первым планом проектов, сокращается с 27-ми до 18-ти календарных месяцев.



На графике представлен предварительный прогноз потенциального охвата рынка, составленный по материалам открытой печати, в зависимости от полноты реализации ***RA***-технологий.




**Предполагаемая доля лицензионных отчислений Компании от стоимости производимой криптографической продукции, построенной на основе *RA*-технологий и решаемым ими задачам**

| Задачи первого плана | От всех поступлений, по задачам | |
|---|---|---|
| | второго плана | третьего плана |
| Производство защищенных радиочастотных меток, разных типов **5-12**%<br>Производство считывающих устройств и верификаторов **15-20**% | **10-25**% | **5-10**% |

**в среднем** [redacted] **от емкости рынка**

**Распределение общей прибыли от совместной деятельности, является предметом переговоров сторон**.

Оценивая в целом ***RA***-технологии и их общесистемный, универсальный характер, Компания, опираясь на единую теоретическую базу и преемственность разработки, в конечном итоге стремится выработать как для себя, так и для других компаний и специалистов, оптимальную формулу разработки и внедрения криптографических приложений:

от постановки задачи к конструированию и далее,
через лицензирование (сертификацию) к промышленному производству.

Приношу извинения, за столь объемное приложение. С благодарностью приму все Ваши замечания. Готов ответить на интересующие вопросы, в любое удобное для Вас время.

С уважением,
Президент компании **Random Art Labs**

Кулаков Игорь Анатольевич