На правах рукописи

БЕЛОМОЙЦЕВ ДМИТРИЙ ЕВГЕНЬЕВИЧ

РАЗРАБОТКА МЕТОДИКИ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ КАНАЛОВ ПЕРЕДАЧИ ЗАЩИЩЕННЫХ СООБЩЕНИЙ В БЕСПРОВОДНЫХ СОЕДИНЕНИЯХ МОБИЛЬНЫХ УСТРОЙСТВ

Специальность 05.13.12 – Системы автоматизации проектирования

АВТОРЕФЕРАТ

на соискание ученой степени кандидата технических наук

Москва - 2009

Работа выполнена на кафедре систем автоматизированного проектирования Московского Государственного Технического Университета им. Н.Э.Баумана.

Научный руководитель:	доктор технических наук, профессор Норенков И.П.
Официальные оппоненты:	доктор технических наук, профессор Буланова Т.А.
	кандидат технических наук, доцент Филиппов М.В.
Ведущая организация:	Общество с ограниченной ответственностью «Центр исследований экстремальных ситуаций»

Защита диссертации состоится « 17 » декабря 2009 года в 14^{30} на заседании диссертационного совета Д 212.141.10 в Московском государственном техническом университете имени Н.Э.Баумана по адресу: 105005, г. Москва, 2-я Бауманская ул., д.5

С диссертацией можно ознакомиться в библиотеке МГТУ им.Н.Э.Баумана.
Ваши отзывы в двух экземплярах, заверенные печатью, просим выслать по указанному адресу.
Автореферат разослан « » 2009 г.

Ученый секретарь
Диссертационного совета,
к.т.н., доцент С.Р. Иванов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Проектирование большинства сложных технических систем и устройств основано на блочно-иерархическом подходе, предполагающем расчленение моделей и процедур проектирования на иерархические уровни с поблочной разработкой составных частей на каждом из уровней. Известным недостатком поблочного проектирования является синтез параметров очередного блока при фиксированных значениях параметров остальных блоков системы, что ведет к необходимости завышенного числа итераций и, следовательно, к росту сроков и затрат на проектирование. Поэтому разработка методик проектирования систем иерархической структуры, позволяющих выполнять совместный синтез структуры и параметров подсистем, является весьма актуальной проблемой.

К числу систем иерархической структуры относятся многие вычислительные и связные системы, в частности, системы мобильной связи. Потребность современного общества в обмене информацией между различными видами вычислительной техники достаточно высока. Способность технического обеспечения различных сфер деятельности человека выполнять поставленные задачи и при этом не быть жестко привязанным к своему местоположению (мобильность) становится определяющей. Для успешного выполнения задач мобильным электронным устройствам необходимо взаимодействовать друг с другом, в том числе обмениваться данными. Как показывает проведенный в работе анализ имеющихся решений, задачи локального соединения могут быть обеспечены применением технологий по стандартам IEEE 802.11 и 802.15. Однако описываемые в этих стандартах методики проектирования рассчитаны на фиксированный состав требований и потому не обеспечивают должной гибкости при необходимости адаптировать каналы передачи сообщений к конкретным условиям.

Наиболее сложной для формализации является задача структурного синтеза проектных решений. Известные прецеденты их постановки и решения в системах автоматизированного проектирования относятся к отдельным частным случаям и не устраняют недостатки поблочного проектирования.

Вопросы автоматизированного блочно-иерархического проектирования сложных систем разрабатывались многими учеными в различных приложениях, например, в области радиоэлектроники известны труды Баталова Б.В., Бусленко Н.П., Иловайского И.В., Сигорского В.П., Топоркова В.В., Calahan D., Rohrer R., Zwicky F. и др.

В работах ряда авторов, например, Батищева Д.И., Курейчика В.М., Норенкова И.П., Baker J., De Jong, Eiben A. Goldberg D., Spears W., обращается внимание на перспективность решения проблемы структурного синтеза иерархических систем на основе эволюционных методов.

В диссертации решается проблема разработки методики автоматизированного проектирования сложных систем с иерархической структурой на примере каналов передачи сообщений в сетях мобильной связи.

Под каналом передачи данных (КПД) в диссертации принято понимать часть коммуникационной сети, состоящую из технических средств передачи и

приема данных, включая линию связи, а также из средств алгоритмического обеспечения и протоколов взаимодействия, предназначенную для трансляции определяемого передаваемыми данными набора сигналов между пользователями канала. В модели канала отражается влияние внутренних шумов системы на узлы передатчика и приемника, а также приложение внешних шумов в виде атак активного и пассивного типов.

Существующие методики проектирования КПД не обеспечивают необходимую гибкость для оперативного реагирования на возникающие факторы воздействия на сообщения в каналах при их эксплуатации. При возникновении факторов, непредусмотренных существующими методиками проектирования, практически невозможно внести изменения в работу канала для устранения последствий внешнего воздействия. Оперативное «перепроектирование» канала и изменение параметров преобразования сообщений невозможны вследствие жесткого ограничения методик проектирования с учетом требований стандартов. Существует необходимость в разработке методики проектирования каналов, которая бы позволяла учитывать динамически изменяющиеся условия передачи во внешней по отношению к сообщениям в канале среде. Тем самым будет достигнута несвойственная существующим методикам проектирования гибкость в вопросах учета новых внешних факторов воздействия на сообщения в каналах.

Цель работы

Целью диссертационной работы является разработка методики автоматизированного проектирования систем с иерархической структурой на примере каналов передачи защищенных сообщений в беспроводных соединениях мобильных устройств.

В работе показано, что для достижения данной цели необходимо последовательно решить следующие взаимосвязанные **задачи**:

1. разработка и обоснование методики проектирования систем с иерархической структурой на основе использования блочно-иерархического подхода и генетических методов синтеза;
2. создание математической модели канала передачи защищенных сообщений и способа кодирования проектных решений;
3. разработка метода кодирования сообщений при передаче по каналам беспроводных соединений мобильных устройств;
4. разработка программно-аппаратного комплекса для моделирования канала передачи данных на базе предлагаемой методики проектирования;
5. экспериментальная проверка предложенной методики проектирования каналов передачи данных.

Объекты и предметы исследования

В работе принято, что объектами исследования являются методы, средства и процессы проектирования систем с иерархической структурой.

Исследование проводится на примере каналов передачи защищенных сообщений, разрабатываются методики и алгоритмы выработки проектных решений задачи синтеза каналов беспроводных соединений мобильных устройств.

Научная новизна работы

1. Методика проектирования систем с иерархической структурой на основе генетических алгоритмов поиска оптимального решения;
2. Метод кодирования проектных решений в виде хромосомы с переменной длиной, отражающей неоднородность структур проектируемых объектов;
3. Критерий оптимальности в виде величины предотвращаемого воздействия помех на передачу и прием сообщений в канале;
4. Метод кодирования сообщений для передачи и приема в каналах беспроводных соединений, подверженных внешним помехам;
5. Метод автоматизированной синхронизации генераторов числовых последовательностей при потере их когерентности.

Практическая значимость работы

Результаты работы могут найти применение при проектировании и программно-аппаратной реализации систем с иерархической структурой. Предложенный метод кодирования сообщений может использоваться для обеспечения защиты сообщений в действующих каналах беспроводных локальных соединений мобильных устройств в экстремальных условиях автономной работы.

Реализация результатов работы

Результаты работы в виде программного комплекса проектирования и верификации каналов передачи защищенных сообщений были внедрены в процесс проектирования системы для съема информации в компонентах инфраструктуры аэродромного обеспечения фронтовой авиации, разрабатываемой совместно с ЗАО НПО «ФОМОС» по заказу МО РФ.

Основные положения, выносимые на защиту

1. Методика проектирования систем с иерархической структурой на основе генетического метода с автоматически настраиваемой структурой хромосомы при модификациях состава подсистем;
2. Метод кодирования проектных решений в виде хромосомы переменной структуры;
3. Критерий максимума предотвращаемого воздействия помех на сообщения в канале, метод кодирования сообщений на числовых последовательностях от когерентных генераторов и метод автоматизированной синхронизации генераторов при потере их когерентности.

Апробация результатов работы

Результаты работы докладывались и обсуждались на конференциях:

1. Международная конференция «Образование через науку». Москва, 17-19 мая 2005 г.
2. Всероссийский конкурс инновационных проектов аспирантов и студентов по приоритетному направлению «Информационно-телекоммуникационные системы». Москва, 12-15 октября 2006 г.
3. XII Всероссийская научно-техническая конференция «Новые информационные технологии в научных исследованиях и в образовании». Рязань, 19-21 апреля 2007 г.

Публикации

Основные результаты диссертационной работы опубликованы в 7 печатных работах [1, 2, 3, 4, 5, 6, 7]. Из них в рекомендованных ВАК изданиях – 1 [6].

Объем и структура работы

Диссертация состоит из введения, трех глав, заключения, приложения и акта о внедрении результатов работы, списка использованных источников. Объем диссертации 163 страницы, включает 62 рисунка, 12 таблиц, список литературы из 104 наименований. В приложение вынесены акты об использовании и внедрении результатов диссертационной работы.

Во введении обоснована актуальность темы, определены цели и задачи исследования, охарактеризована научная новизна и практическая значимость работы.

В **первой** главе рассмотрены основы блочно-иерархического подхода к анализу структуры сложных объектов на примере КПД. Проведен анализ преимуществ и недостатков основных методик проектирования каналов беспроводных соединений. Выделены общие принципы синтеза оконечного оборудования КПД.

Анализ состояния проблемы показал, что применяемые в настоящее время методики синтеза каналов передачи защищенных сообщений (по стандартам IEEE 802.11 и 802.15) не обладают необходимой гибкостью при возникновении новых факторов воздействия в силу невысокой мощности рассматриваемых множеств альтернативных вариантов. Методики проектирования по данным стандартам допускают изменение параметров каналов в узком диапазоне. Количество варьируемых параметров также невелико. Исследование круга потенциальных факторов воздействия показывает, что параметры канала, которые допускают варьировать существующие методики, могут использоваться для предотвращения воздействия лишь ограниченного количества факторов. В частности, известные методики не обеспечивают возможности синтеза каналов, устойчивых к возникновению активных шумов и атак с заданными параметрами. В работе поставлена задача создать методику проектирования, которая бы позволяла расширять множество альтернатив за счет добавления новых элементов, учитывающих воздействие новых внешних факторов.

На основании проведенного анализа сделан вывод о необходимости разработки новых методик и алгоритмов проектирования сложных иерархических систем типа каналов передачи защищенных сообщений, удовлетворяющих требованиям по устойчивости к атакам и активным помехам.

Во **второй** главе сформулирована задача разработки метода автоматизированного синтеза структуры и параметров проектируемых систем, являющегося основой методики проектирования систем типа канала передачи защищенных сообщений в беспроводных соединениях мобильных устройств. Проектирование систем с иерархической структурой должно осуществляться путем определения состава и значений подмножества параметров взаимосвязанных подсистем. Применительно к КПД определению подлежат состав и параметры оконечного оборудования обработки данных, линии связи и алгоритмов подсистем обработки данных.

Задача синтеза формулируется как задача принятия решения, в которой требуется выбрать наиболее подходящий вариант из множества альтернатив *А* при заданном множестве *К* критериев, модели *Мод* и способе *П* сведения *К* к скалярному критерию:

$$ЗПР = \langle A, K, Мод, П \rangle,$$

Множество альтернатив целесообразно представлять в форме И-ИЛИ графа, в котором учитывается зависимость подсистем различного типа как от общих управляемых параметров, так и от частных, специфичных для конкретных подсистем (см. Рис. 1). Канал (алгоритмическая реализация) представляется в виде совокупности подсистем S_i, $i = \overline{1, N^S}$, N^S - количество подсистем. Множество управляемых параметров алгоритмической реализации канала состоит из подмножеств типов подсистем и параметров подсистем $X = X^T \cup X^P$. Мощности множеств X^T, X^P составляют N^T, N^P, соответственно. У *i*-й подсистемы существует N_i^T альтернативных типов $X_k^{Ti}, k = \overline{1, N_i^T}$. Каждому типу X_k^{Ti} соответствует набор из N_k^{Pi} параметров $\{X_j^P\}$, где $j \in \{I_q^{Pi}\}$ -

совокупность индексов элементов $\left(0 < I_q^{Pi} \le N^P, q = \overline{1, N_k^{Pi}}\right)$. Каждый параметр X_j^P может принимать значение из набора C_r^j, где $r = \overline{1, N_j^V}$, N_j^V - количество допустимых значений параметра X_j^P.

Различные подсистемы имеют общие параметры, равно как и различные типы одной подсистемы. Поэтому невозможно отдельно вычислить оптимальные значения управляемых параметров для каждой подсистемы в отдельности.

Следует отметить отличия предложенного способа представления множества альтернатив от способов, применяющихся в стандартизованных методиках проектирования:

- для представления применен И-ИЛИ граф,
- обеспечена возможность добавления новых элементов и формирования новых альтернатив за счет расширения И-ИЛИ графа,
- обеспечена возможность учета зависимости различных типов подсистем от общих параметров подсистем.

При введении в рассмотрение новых типов подсистем канала необходимо учесть, что количество альтернативных вариантов может экспоненциально возрастать. Поэтому задача синтеза каналов принадлежит к классу **NP-сложных**. Следовательно, применение метода полного перебора будет невозможно с точки зрения эффективного использования временных ресурсов.

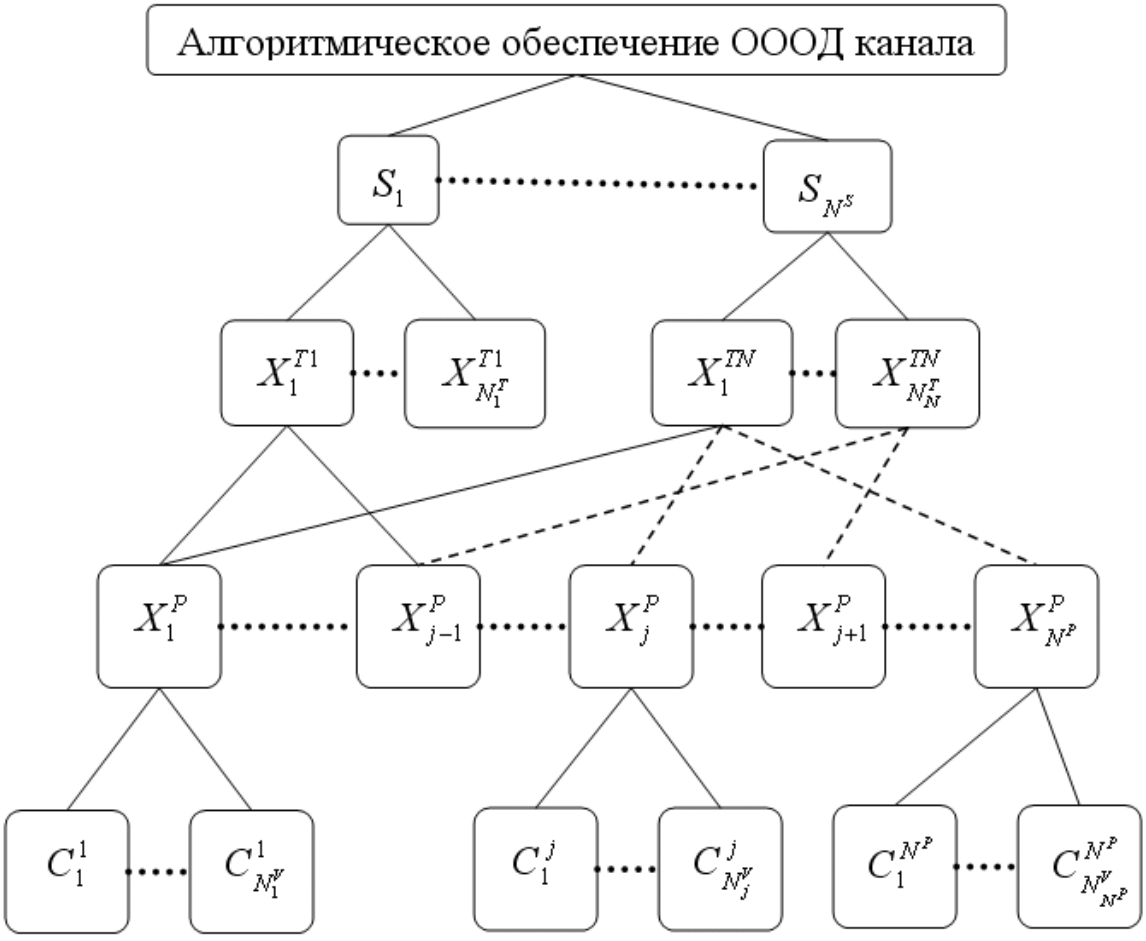

Рис. 1. Схема И-ИЛИ графа множества альтернативных вариантов

В соответствии с проведенными в работе исследованиями задача проектирования канала передачи защищенных сообщений формулируется, исходя из следующих положений:

- требуется синтезировать структуру канала из множества альтернативных составных элементов и определить их параметры;
- поскольку существует опасность компрометации сообщения в канале в результате приложения внешних помех и/или активных атак, степень предотвращаемого воздействия со стороны пассивных внешних помех и активных атак должна быть близка к возможному максимуму. Частичная компрометация сообщения свидетельствует о том, что приложенные помехи и/или атаки частично увенчались успехом, а их воздействие не было предотвращено.

Поэтому для задачи синтеза каналов передачи защищенных сообщений индивидуальные выражения для вычисления функций полезности $F_K^i\left(X^P\right)$ подсистем являются оценками степени предотвращаемого воздействия внешних помех на канал и получаются на основе обобщения экспертных мнений.

Задача проектирования канала формулируется как

$$\begin{aligned} X^* &= \arg\max_{X \in D_X} F\left(X\right) \\ D_X &= \left\{X \mid W\left(X\right) > 0, Z\left(X\right) = 0\right\} \end{aligned}, \qquad (1)$$

где X - вектор управляемых параметров,
$F(X)$ - функция полезности (целевая функция),
D_X - область определения вектора управляемых переменных,
$W(X), Z(X)$ - ограничения на область определения X.

Для решения задачи (1), прежде всего, нужно определить математическую модель канала передачи сообщений, включающую списки используемых параметров и алгоритмы вычисления функций полезности подсистем $\left\{F_{I_1}^1\left(\overline{X^P}\right),...,F_{I_{N^S}}^{N^S}\left(\overline{X^P}\right)\right\}$. Например, для различных типов подсистем шифрования данных выделены общие управляемые параметры K_{Lmax} - максимальная длина ключа, N_{fk} - частота смены ключа, M_{Lmax} – максимальная длина сообщения, N_{fm} - частота поступления сообщений. Параметры внешних факторов определяются на основании задания на проектирование:

$$\overline{V_i} = \left\{V_{i1},...V_{iN_i^{ext}}\right\},$$

где V_i – вектор параметров i-го внешнего фактора,
N_i^{ext} - количество параметров i-го внешнего фактора

В общем случае для альтернативных вариантов подсистем шифрования алгоритм вычисления значения функции полезности представлен на Рис. 2.

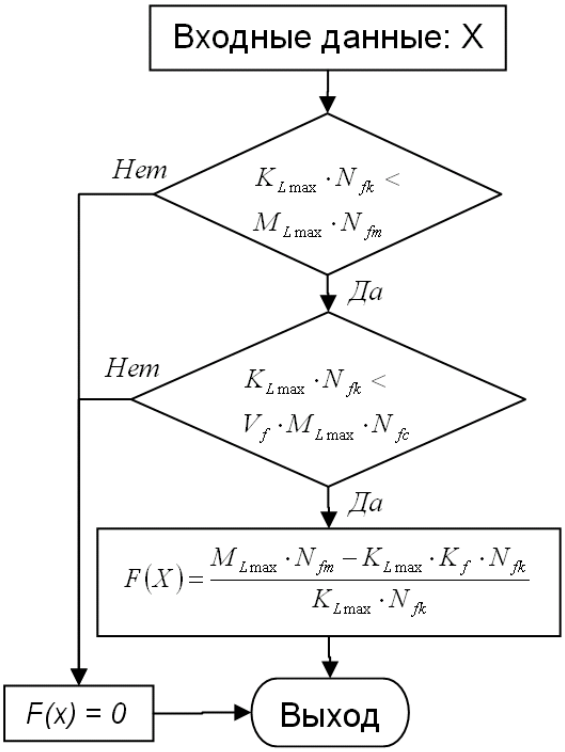

Рис. 2. Схема алгоритма вычисления целевой функции

Наличие специфических для каждого типа подсистемы управляемых параметров приводит к возникновению дополнительных условных блоков в структуре алгоритма вычисления значения функции полезности подсистемы.

Целевая функция *F(X)* является аддитивной сверткой целевых функций отдельных подсистем.

$$F(X) = \sum_{i=1}^{N^S} w_K F_K^i(X^P),$$

где X – искомый вектор проектного решения,

$K = I_i$ - выбранный тип подсистемы в множестве X^T,

$F_K^i(X^P)$ - частная функция полезности i-й подсистемы типа I_i,

w_K - весовой коэффициент $F_K^i(X^P)$,

$F(X)$ - целевая функция альтернативы

Аддитивный критерий выбран для преимущественного учета общего эффекта от системы, нежели выделяющегося эффекта от какой-либо одной подсистемы.

Задача (1) для систем иерархической структуры характеризуется рядом особенностей.

Во-первых, среди элементов искомого вектора управляемых переменных присутствуют предметные (лингвистические) переменные. Во-вторых, к ограничениям задачи относится наличие запрещенных комбинаций типов различных подсистем. Кроме того, целевые функции подсистем часто оказываются нелинейными и несепарабельными. В этих условиях большинство известных методов математического программирования

оказываются неприменимыми и зачастую применение эволюционных методов и, прежде всего, генетических алгоритмов становится безальтернативным. В-третьих, особенностью задачи является то, что при смене в проектном решении типа какой-либо подсистемы происходит смена не только состава управляемых параметров и их числа, но и алгоритма вычисления целевой функции. Эта особенность обусловливает переменность структуры проектных решений и затрудняет их представление в рамках генетических методов.

В диссертации представлены результаты .разработки генетического метода, учитывающего особенности задачи синтеза структуры иерархических систем. Отличительными чертами разработанного генетического метода являются: *n*-точечный кроссовер, в котором число разрывов хромосомы *n* определяется типами рекомбинируемых родительских особей; способ выравнивания длин хромосом; оператор мутации на уровне типов подсистем.

Кодирование проектного решения в виде хромосомы заключается в выделении участка генов, соответствующего общим для подсистем параметрам, и фрагментов, соответствующих специфическим параметрам подсистем. Каждый *i*-й фрагмент включает гены, соответствующие типу X_K^{Ti} и вектору управляемых параметров *i*-й подсистемы $\{X_j^P\}$. Для приведения хромосом к сопоставимости в условиях непостоянства числа значащих генов применен искусственный прием, заключающийся в дополнении числа генов в *i*-м фрагменте до величины $m_{i\max}$, где $m_{i\max} = \max\ N_k^{Pi}$, N_k^{Pi} - число параметров в векторе $\{X_j^P\}$ в случае подсистемы *k*-го типа (см. Рис. 3, на котором индекс *k* опущен). При этом позиции разрыва хромосомы в *i*-м фрагменте допустимы только в интервале [2, N_k^{Pi}] при условии совпадения значений X_K^{Ti} в хромосомах обоих родительских особей. При несовпадении этих значений *i*-е фрагменты родителей без изменений переходят в хромосомы потомков.

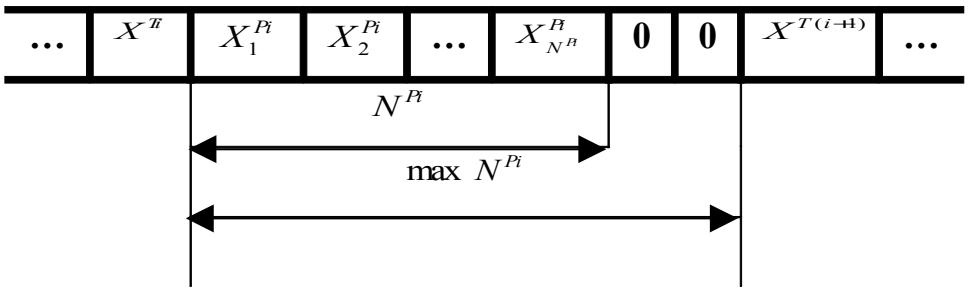

Рис. 3. Фрагмент хромосомы

Особенность оператора мутации на уровне типов подсистем заключается в том, что одновременно с заменой значения X_K^{Ti} в гене типа подсистемы на случайное значение *q* из $\{X_k^{Ti}\}, k = \overline{1, N_i^T}$, происходит также замена значений генов, соответствующих вектору $\{X_j^P\}$ (см. Рис. 4). Очевидно, что новый вектор $\{X_j^P\}$ должен отражать накопленные положительные изменения параметров, происшедшие в процессе эволюции. Для выполнения этого условия ведется база текущих «наилучших» значений векторов параметров, в

которой «наилучшее» значение $\{X_j^P\}$ соответствует хромосоме с наилучшим значением целевой функции *F(X)*, полученным при вхождении в *X* параметра X_K^{Ti} со значением *q*.

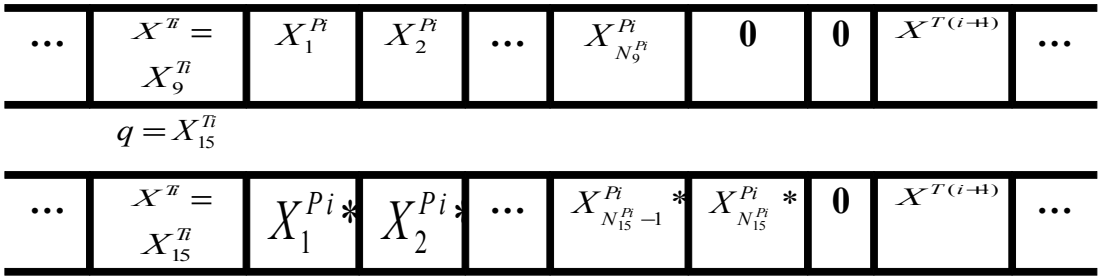

Рис. 4. Фрагменты хромосомы до и после мутации типа

Проведенные серии численных экспериментов подтвердили сравнительно высокую скорость сходимости генетического поиска к окрестностям финального решения с помощью разработанного метода. На Рис. 5 представлена зависимость целевой функции от числа смен поколений в одном из экспериментов. Различные траектории поиска, отличающиеся исходными значениями управляемых параметров, в одном из вариантов решения задачи (1) показали, что стагнация происходит на уровнях *F(X)*, различающихся не более чем на 2,1%, что можно считать оценкой точности определения локального экстремума.

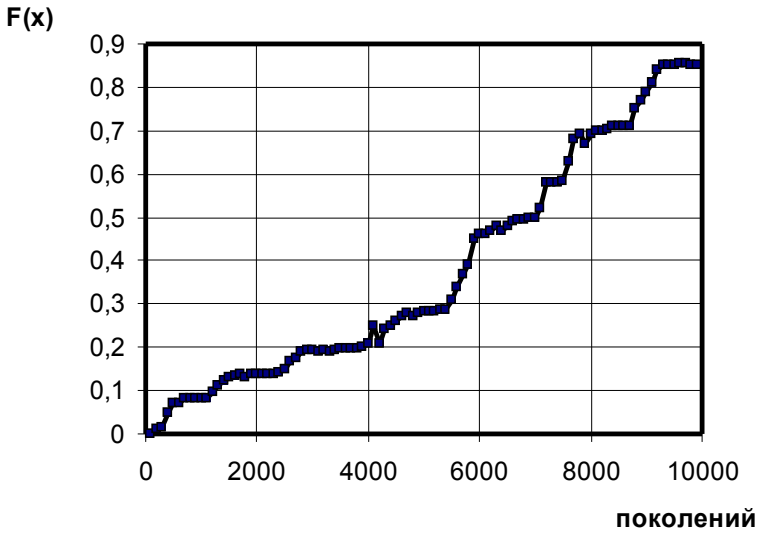

Рис. 5. Диаграмма изменения целевой функции

Важное значение для предотвращения негативного воздействия внешних факторов на сообщения в канале имеет метод кодирования сообщений, В диссертации предложен метод кодирования, основанный на особом способе шифрования сообщения передающей стороной и, соответственно, на расшифровании полученного сообщения принимающей стороной. Согласно предложенной методике, допускаются к применению схемы как с симметричным, так и с асимметричным шифрованием. Новизна метода

заключается в способе вероятностного определения ключа расшифрования принимающей стороной. Фактически, при передаче сообщения по каналу имеет место пара ключей. Один ключ используется на передающей стороне для зашифрования, а другой – на принимающей для расшифрования сообщения. Для каждого сообщения данная пара ключей определяется уникальным образом без непосредственного обмена данными между передающей и принимающей сторонами для генерирования ключей. Разработанный метод предлагает новый подход к синхронизации пар ключей между двумя сторонами канала передачи защищенных сообщений на основе оценки показателя автокорреляции псевдослучайных последовательностей.

В определенный момент времени T_0 объекты А и Б инициализируют генераторы псевдослучайных ключевых последовательностей. С использованием специфичных для данных объектов параметров темп работы генераторов синхронизируется, насколько это является возможным. Таким образом, объект Б способен с определенной долей вероятности в момент T_2 указать, какую ключевую псевдослучайную последовательность использовал объект А в момент T_1. Фактически, в данном случае определяется вероятность обнаружения объектом Б ключевой последовательности, на которой объектом А было осуществлено маскирование.

Таким образом, в отличие от известных методик симметричного и асимметричного шифрования, предложенный метод представления сообщений

- не требует изначального жесткого определения пар ключей,
- реализует принцип гибкого подбора масок и маркерных вставок на основе вероятностной характеристики,
- не предполагает использования временных ключей на этапе образования пары устройств,
- обеспечивает приближение к показателю криптостойкости методики «одноразовых блокнотов» благодаря возможности генерировать маски, соразмерные длине сообщения.

Испытания опытного образца относится к одному из заключительных этапов проектирования. Автоматизация этого этапа обычно требует разработки соответствующего стендового оборудования. В **третьей** главе диссертации приведены результаты разработки стенда и проведенных стендовых испытаний проектных решений задачи синтеза каналов. Предложена и обоснована методика экспериментальных исследований для реализации проектного решения на базе стенда. Создана программная реализация методики оценки качества проектного решения путем его моделирования на аппаратной базе стенда и экспериментального исследования показателей функционирования.

Экспериментальный стенд представляет собой программно-аппаратный комплекс для моделирования проектных решений задачи синтеза каналов передачи защищенных сообщений. Структура стенда включает:

- два передающих устройства, формирующих канал,
- дополнительные передатчики, моделирующие воздействие внешних факторов.

Разработка экспериментального стенда и реализация разработанной методики проектирования осуществлена на базе библиотек методов генетических алгоритмов на языках высокого уровня C++ (GAGS, GALib) и Java (GAJIT, GA Playground).

Экспериментальные исследования проводились в рамках ОКР «Концерт» совместно с ЗАО НПО «ФОМОС» по заказу МО РФ. Целью работы было получение надежного средства проектирования и верификации каналов передачи защищенных сообщений. В рамках работы экспериментально исследовалось качество проектных решений, полученных при помощи разработанной методики синтеза.

Принято, что в минимально необходимом составе стенда должны присутствовать передающее и принимающее устройство. Для исследования аспектов воздействия внешних помех и атак на сообщения в канале необходимо предусмотреть наличие в схеме стенда источника данных угроз.

Канал передачи данных образован из модулей оконечного оборудования обработки данных (которые входят в состав передатчика и приемника), а также линиями связи.

В качестве воздействия на процесс передачи сообщений внешних факторов рассматриваются результаты приложения к каналу помех и атак. Принято, что они представляют собой попытки несанкционированного использования передаваемых данных. Соответственно, санкционированное использование происходит только передатчиком и авторизованным приемником.

В результате исследований в работе был определен перечень помех и атак, влияние которых на сообщения должно быть предотвращено проектируемым каналом. В работе определено, что данный перечень использовался при формировании задания на проектирование и при определении требований, которые предъявляются к проектируемому каналу. В процессе выполнения этапов методики автоматизированного проектирования, требования к каналу применяются для определения значений функций полезности альтернативных вариантов подсистем канала.

На основе анализа экспертных оценок сформирован набор уровней вреда, который могут причинить сообщению в канале помехи и атаки. Состав набора уровней вреда соответствует перечню угроз, который может быть составлен на этапе предпроектных исследований. В работе показано, что вследствие различий подходов к проведению атак и помех могут будут отличаться и уровни вреда от них для сообщения в канале. Например, максимально возможный вред причиняется в случае компрометации сообщения в канале или после его подмены. Принято решение, что в соответствии с экспертными оценками серьезности доставляемого сообщению в канале вреда данным уровням необходимо назначить веса.

Выделены возможные уровни вреда сообщению в канале. Список данных уровней и поставленных им в соответствие удельных весов (перечень возможных атак при передаче сообщения по каналу) приведен в диссертации.

В ходе работ со стендом были выполнены два вида исследований:

- эксперименты по проверке адекватности установки, моделирующей работу канала,
- эксперименты по моделированию воздействия на сообщения в канале со стороны внешних помех и атак.

В первом случае измерялись временные затраты на выполнение операций с каналом, а также реализуемость всех необходимых операций в соответствии с графом конечного автомата. Результаты измерений показали, что каналы, создаваемые на базе стенда, соответствуют по своим характеристикам производительности и временным затратам аналогичных стандартных каналов.

Корректность параметров проектных решений подтверждается замерами, проводящимися при аттестации оборудования экспериментального стенда. Для данной процедуры генерируется проектное решение, которое соответствует стандартным каналам IEEE 802.11 и 802.15. В результате моделирования проектного решения, а также его реализации на базе экспериментального стенда получаются величины основных характеристик (производительности и пропускной способности) и воздействия внешних факторов. Эти величины отличаются от результатов аналогичных измерений для стандартных каналов не более, чем на 3%.

Эффективность проектных решений подтверждается сравнением экспериментально определенных величин воздействия внешних факторов (см. Табл. 1).

Таблица 1.

Результаты экспериментов по определению воздействия внешних факторов на каналы передачи защищенных сообщений

Тип канала	Величина воздействия фактора					
	1, %	2, %	3, %	4, %	1+3, %	1+2, %
канал по методикам стандартов 802.11/802.15	13,0	30,0	79,0	12,0	6,0	4,5
канал по разработанной методике проектирования	4,0	4,1	0,1	5,0	2,0	0

По результатам анализа результатов экспериментов путем моделирования воздействия помех и атак на канал сделан вывод, что степень воздействия внешних факторов на стандартные каналы значительно выше, чем на канал, который получен при помощи разработанной методики проектирования. Моделирование действия помех и атак на стандартные каналы показало, что уровень вреда для сообщений в каналах превышает допустимые пределы и означает компрометацию сообщений или потерю функциональности канала, что недопустимо. Испытание канала, полученного при помощи разработанной методики, показало, что степень воздействия внешних факторов не превышает

пределов, установленных требованиями на разработку. Таким образом, экспериментально установлено, что воздействие идентичных наборов внешних факторов на результаты применения стандартных и разработанной методик проектирования показывает преимущество последней. Данное преимущество заключается в возможности включать дополнительные средства предотвращения воздействия помех и атак в множество альтернатив в качестве возможных составных элементов при синтезе проектного решения. Стандартные методики проектирования каналов не обладают подобными возможностями по расширению множества альтернатив.

Разработанный экспериментальный стенд можно рассматривать, как самостоятельное научно-техническое решение, которое обеспечивает возможность моделировать каналы передачи защищенных сообщений, параметры которых были получены в ходе проектирования. Средствами стенда также моделируются воздействия внешних помех и атак на канал, оценивается степень деструктивного влияния. Таким образом, выполняется проверка качества проектного решения, а также аспектов его соответствия предъявляемым требованиям.

Практическое применение разработанной методики проектирования, а также проектных решений произошло в ходе выполнения таких задач, как:

- модификация структуры существующих каналов локальных соединений для автономной работы в экстремальных условиях;
- программно-аппаратная реализацию канала передачи защищенных сообщений для съема информации в компонентах инфраструктуры аэродромного обеспечения фронтовой авиации.

Была разработана система автоматизированного проектирования каналов (имеется акт о внедрении), которая использовалась при проведении НИОКР по заказу МО РФ. На вход разработанного программного обеспечения подавались данные о возможных внешних факторах воздействия, которое должен предотвращать проектируемый канал. В результате проектирования был получен вектор параметров канала, в который вошли типы подсистем канала и значения их параметров. Данный вектор представляет собой настройки алгоритмического обеспечения, которое реализует функции по предотвращению воздействия внешних факторов на сообщения в канале. Вектор управляемых параметров был исследован путем его «занесения» в алгоритмическое обеспечение экспериментального стенда. Разработанный стенд обеспечивает выполнение двух функций:

- проверки качества проектных решений путем моделирования работы каналов,
- является частью оборудования, поставленного заказчику в рамках НИОКР.

В **заключении** изложены основные выводы и результаты диссертационной работы.

В **приложении** приводятся копии актов о внедрении результатов диссертационной работы.

Общие выводы и результаты

Разработанная методика проектирования обеспечивает возможность синтезировать каналы с учетом наиболее современных данных о возможных видах внешних факторов воздействия и средствах их предотвращения. Такой возможностью разработанная методика обладает благодаря следующему:

- проектируемый канал рассматривается в виде совокупности подсистем;
- у каждой подсистемы может быть несколько альтернативных вариантов;
- количество подсистем и их альтернативных вариантов не ограничено и формируется с учетом требований, предъявляемых к проектируемому каналу;
- выбор предпочтительного варианта компоновки канала осуществляется в ходе поиска проектного решения генетическим алгоритмом по критерию максимизации внешнего воздействия от помех и атак на сообщения в канале.

Основными результатами по данной диссертационной работе стали следующие положения:

1. Задача проектирования каналов передачи защищенных сообщений решается путем проведения синтеза структуры каналов и параметрического синтеза компонентов структуры. Разработана методика автоматизированного проектирования каналов, как частного случая систем с иерархической структурой, основой которой является решение NP-сложной задачи синтеза канала с помощью генетических методов.

2. Предложен способ представления проектных решений в виде хромосом, отражающий типы подсистем оконечного оборудования обработки данных канала и параметры функционирования алгоритмической составляющей подсистем.

3. Разработан генетический метод синтеза проектных решений, учитывающий непостоянство числа управляемых параметров и другие выявленные особенности задач проектирования систем иерархической структуры.

4. Предложена подсистема кодирования данных в канале на основе нового метода, который обеспечивает преобразование сообщений при подготовке к передаче по линиям связи. Новый метод кодирования данных использует симметричную систему выработки ключей с синхронным обновлением бинарных масок и обеспечивает когерентность генераторов псевдослучайных числовых последовательностей.

4. Предлагаемая методика проектирования и генетические операторы реализованы в виде программного комплекса и позволяет использовать различные реализации генетических алгоритмов в виде библиотек методов на языках программирования высокого уровня.

5. На основе разработанной методики выполнено проектирование каналов передачи защищенных сообщений для систем съема информации в аэродромном обеспечении фронтовой авиации.

6. Предложенная методика автоматизированного проектирования каналов в совокупности с методом кодирования сообщений в канале позволяет исправить недостатки существовавших ранее методик проектирования, которые были выявлены в процессе проведенных исследований.

Публикации по теме диссертационной работы

1. Беломойцев Д.Е. Методика проектирования процесса безопасной передачи данных в беспроводных соединениях мобильных устройств // Наука и образование. 2008. №5. http://technomag.edu.ru/doc/93258.html
2. Беломойцев Д.Е. Разработка методики проектирования защищенной передачи данных в беспроводных соединениях мобильных устройств // НИТ-2007: Тез. докл. Всеросс. конф. 2007. С. 143-145.
3. Беломойцев Д.Е. Разработка приложений на основе Bluetooth API // RSDN-Magazine. 2005. №1. С. 52-79.
4. Беломойцев Д.Е. Система контроля доступа по беспроводной связи для мобильных телефонов // Технологии Microsoft в теории и практике программирования: Тез. докл. Всерос. конф. Москва. 2005. С. 89-93.
5. Беломойцев Д.Е. Система параллельной обработки изображений в пикосетях мобильных устройств // Наукоемкие Технологии и Интеллектуальные Системы: Тез. докл. Межд. конф. 2005. С. 54-56.
6. Волосатова Т.М., Беломойцев Д.Е. Технологии и библиотеки методов построения пикосетей мобильных устройств // Информационные технологии. 2006. №4. 32 с.
7. Волосатова Т.М., Чичварин Н.В., Беломойцев Д.Е. GPS-навигация и контроль доступа в пикосетях мобильных телефонов // Образование через науку: Тез. докл. Межд. конф. 2005. С. 48-49.