На правах рукописи

МИНАЕВА ЕЛЕНА ВЯЧЕСЛАВОВНА

РАЗРАБОТКА АЛГОРИТМОВ МОДЕЛИРОВАНИЯ И АНАЛИЗА ПРОГРАММНЫХ РЕАЛИЗАЦИЙ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

05.13.19 — "Методы и системы защиты информации, информационная безопасность"

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук

Автор:_____

Москва – 2000

Работа выполнена в Московском Государственном инженерно-физическом институте (техническом университете)

Научный руководитель: Кандидат технических наук, доцент Малюк А. А.

Официальные оппоненты:

Доктор технических наук, Щербаков А. Ю.
Кандидат физ.-мат. наук, Юров И. А.

Ведущая организация: ЦНИИАТОМИНФОРМ

Защита состоится "5" декабря 2000 г.
в 10 часов 00 мин. на заседании диссертационного совета К.053.03.09 в МИФИ по адресу: 115409, Москва, Каширское ш., 31.

С диссертацией можно ознакомиться в библиотеке МИФИ
Автореферат разослан "27" октября 2000 года

Просим принять участие в работе совета или прислать отзыв в одном экземпляре, заверенный печатью организации.

Ученый секретарь
диссертационного совета
кандидат технических наук Горбатов В. С.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы.. Широкое использование вычислительных систем в повседневной жизни сделало их привлекательными для различного рода информационных атак. В связи с этим значительно повысилась актуальность задачи сохранения за информацией ее основных свойств как в процессе хранения и обработки, так и при передаче по открытым каналам связи. Одним из эффективных решений данной задачи на сегодняшний день является применение современных методов криптографии.

Среди требований, предъявляемых к современным массовым средствам защиты информации (СЗИ), значительную роль играет требование "прозрачности" – система должна быть удобна в эксплуатации и не снижать производительности работы конечных пользователей. Последнее предполагает, что все процессы преобразования информации с целью ее закрытия должны выполняться в режиме реального времени. Частая смена программно-аппаратных платформ и непрерывное повышение производительности вычислительных систем ставят задачу быстрого проектирования и оперативной доработки криптоалгоритмов в соответствии с изменившимися условиями эксплуатации. Актуальность задачи моделирования и анализа программных реализаций криптографических преобразований обусловлена необходимостью автоматизации процедуры проектирования эффективных программных реализаций криптоалгоритмов и соответствует текущим потребностям прикладной криптографии на современном этапе ее развития.

Методология и теоретическая база изучения проблем, возникающих при проектировании и создании программных реализаций криптографических преобразований, в настоящее время только формируется. Данная работа опирается на результаты исследований как российских, так и зарубежных специалистов в области защиты информации, таких как Герасименко В.А., Зегжда Д.П., Малюк А.А., Щербаков А.Ю., C.Adams, E.Biham, J. Daemen, L. Knudsen, B. Preneel, B.Schneier и др. и развивает их отдельные положения применительно к задаче формализации методов моделирования и анализа программных реализаций криптопреобразований, представляющей одно из направлений

исследований в области развития и совершенствования средств криптографической защиты в рамках решения общей проблемы обеспечения информационной безопасности.

Процесс синтеза и анализа моделей криптопреобразований в настоящее время недостаточно формализован и не имеет необходимой программной поддержки, что приводит к неоправданно высоким временным и стоимостным затратам. Поэтому разработка системных основ и методов синтеза и анализа моделей симметричных блочных шифров (СБШ), а также разработка соответствующего инструментария моделирования является актуальной проблемой, имеющей большое научное и практическое значение.

Предложенный в работе интегрированный подход, заключающийся в объединении в рамках единого инструментария различных средств поддержки разработки программных реализаций криптопреобразований, позволит решить целый ряд задач, имеющих важное практическое значение, а именно:

- разработки и анализа различных свойств новых криптоалгоритмов,
- модификации и усовершенствования существующих криптоалгоритмов в связи с изменившимися условиями эксплуатации,
- генерации эталонных решений для тестирования программных реализаций криптоалгоритмов на соответствие формальной спецификации,
- выработки рекомендаций по выбору средств криптографической защиты, наиболее полно отвечающих потребностям конкретной прикладной задачи.

Диссертация посвящена разработке методов и алгоритмов моделирования и анализа программных реализаций криптографических преобразований на примере симметричных блочных криптосхем.

Цель исследования. Разработка и реализация методов синтеза и анализа моделей программных реализаций криптографических преобразований с целью создания, модификации и тестирования криптоалгоритмов, применяемых в современных средствах криптографической защиты информации (СКЗИ).

Для достижения поставленной цели были **решены следующие задачи:**

- Разработана обобщенная структурная модель СБШ, позволяющая синтезировать произвольный СБШ из унифицированных структурных компонент с применением операций композиции и задания рекурсивного определения.
- Разработан формальный язык описания структурных моделей СБШ, позволяющий формировать описание модели в виде, приближенном к формальным спецификациям.
- Автоматизирована процедура преобразования формального описания модели шифра в программный код на языке высокого уровня и набор команд гипотетической ЭВМ.
- Реализован интерпретатор модели гипотетической ЭВМ, позволяющий получить теоретические оценки эффективности программной реализации моделируемого криптоалгоритма на выбранной аппаратной платформе.
- Предложена методика построения семейства интегральных оценок качества симметричных блочных криптопреобразований.

Методы исследования. Структурный анализ, теория формальных грамматик и языков, теория информации, статистический анализ, векторная алгебра, методы оптимизации.

Научная новизна. Основным научным результатом работы является разработка методологического базиса синтеза и анализа широкого класса симметричных блочных криптопреобразований.

В ходе исследований были получены следующие новые результаты:

- предложен принципиально новый подход к классификации СБШ в соответствии с методологией проектирования;
- построена обобщенная структурная модель СБШ;
- разработан формальный язык описания структурных моделей СБШ;
- разработан алгоритм преобразования формального описания структурной модели СБШ в соответствующую программную модель;

- разработана формальная модель гипотетической ЭВМ, позволяющая учитывать последние достижения в области создания аппаратного и программного обеспечения вычислительных систем;
- предложена систематизация критериев оценивания криптографических преобразований;
- разработана методика получения интегральных оценок качества криптопреобразований в соответствии с требованиями конкретной прикладной задачи.

На защиту выносятся основные положения диссертации:

- совокупность алгоритмов и средств синтеза структурных моделей криптопреобразований;
- формальный язык описания структурных моделей криптопреобразований;
- совокупность алгоритмов и средств моделирования аппаратной платформы реализации криптопреобразований;
- методика формирования семейства интегральных оценок качества моделируемых криптопреобразований.

Практическая ценность исследования определяется следующими основными результатами:

- универсальность формального языка описания структурных моделей криптопреобразований позволяет использовать его для описания широкого класса симметричных блочных криптосхем;
- строгое соответствие построенной программной модели шифра формальной спецификации дает возможность использовать ее для получения эталонных решений;
- разработанный инструментарий моделирования и анализа программных реализаций криптопреобразований является универсальным и имеет широкие возможности наращивания и модификации компонент;
- предложенная методика интегрального оценивания позволяет проводить сравнительный анализ эффективности применения различных криптопреобразований в рамках конкретной прикладной задачи.

Обоснованность результатов и выводов. Обобщенная модель симметричного блочного криптопреобразования построена на основе анализа широкого класса СБШ. Методы формирования интегральных оценок получены использованием известного математического аппарата и согласуются с практикой. Конструктивность методов проверена реальным использованием для построения криптосхем и их элементов с заданными характеристиками. Универсальность и гибкость инструментария подтверждена большим объемом моделирования.

Публикации и апробация работы. По теме диссертации опубликовано 8 работ. Полученные результаты докладывались на конференциях регионального, всероссийского и международного уровня.

Структура и объем работы. Диссертация состоит из введения, пяти глав, заключения, списка литературы из 130 позиций. Объем: 180 страниц, из них основного текста — 160 с., 7 таблиц, 20 рисунков.

СОДЕРЖАНИЕ РАБОТЫ

Во введении на основе анализа общих тенденций в применении криптографических средств защиты в современных СЗИ обосновывается актуальность разработки методов моделирования и анализа программных реализаций криптографических преобразований. Определяется перечень требований к криптографическим алгоритмам, ориентированным на реализацию программными методами, формулируется задача автоматизации процедур синтеза и анализа программных моделей криптопреобразований, аннотируется содержание работы по главам.

В первой главе определяется класс СБШ и его роль в обеспечении защиты данных, приводится обзор известных на сегодняшний день методов построения СБШ и формулируется задача по разработке общего алгоритма синтеза структурных моделей СБШ.

В результате анализа различных подходов к классификации СБШ был предложен усовершенствованный метод классификации, отражающий генетические зависимости между различными подклассами СБШ, возникающие в процессе проектирования. Для

каждого из выделенных подклассов СБШ изучены основные свойства, указаны преимущества и недостатки полученных решений. Предложена обобщенная структурная модель СБШ на основе композиции унифицированных структурных компонент (УСК). В рамках данной структурной модели были определены основные конструктивные элементы СБШ. На их основе было сформировано полное множество УСК.

Существует ряд различных подходов к классификации СБШ. Для задач моделирования криптопреобразований наибольший интерес среди них представляет группа классификаций, основанных на методологии проектирования. В данном случае под методологией проектирования понимается набор утверждений о степени влияния тех или иных шифрующих преобразований (и их композиций), на результирующие характеристики полученной криптосхемы.

При создании новых архитектур шифров всегда наблюдается генетическая преемственность между различными методологиями проектирования. Учет этой зависимости приводит к принципиально новому подходу к классификации СБШ. На основе анализа обширного фактического материала автором диссертационной работы был предложен генетический подход к классификации блочных шифров, результаты которого представлены на рис. 1.

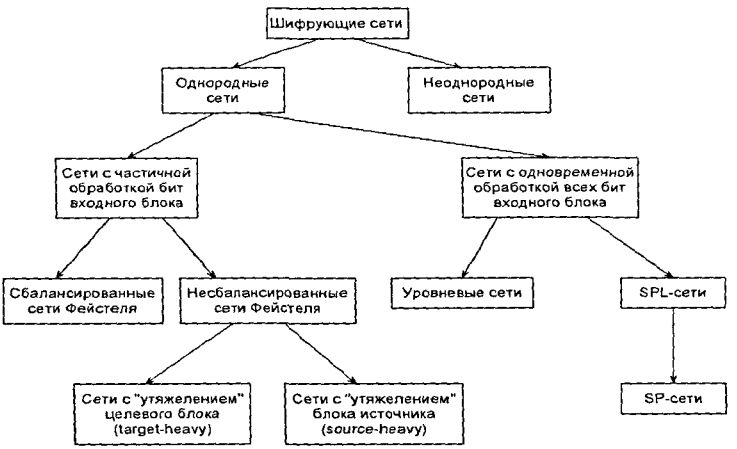

Рис. 1. Генетическая классификация симметричных блочных криптосхем.

Полученная классификация позволяет разработчику уже на этапе выбора базовой архитектуры шифра заранее "планировать" некоторые характеристики будущей криптосхемы.

Следующим этапом процесса моделирования после выбора базовой архитектуры, формирующей "каркас" моделируемого криптоалгоритма, является построение структурной модели криптопреобразования из УСК.

В работе была предложена обобщенная структурная модель СБШ, отражающая перспективный подход к построению криптоалгоритма на основе криптографического ядра, окруженного уровнями некриптографического перемешивания. Данная концепция проектирования повышает стойкость шифра к дифференциальному и линейному методам криптоанализа, использующим свойства первого и последнего раунда шифрования. Была детализирована внутренняя структура криптографического ядра применительно к рассмотренным подклассам СБШ. По результатам детализации *i*-ый раунд шифрования итеративного преобразования, реализуемого в рамках криптографического ядра в обобщенной структурной модели СБШ, может быть представлен в виде последовательности следующих шагов:

- выбор подключа для *i*-го раунда шифрования,
- разделение входного информационного блока *i*-го раунда шифрования на шифрующую и шифруемую части,
- выполнение шифрующего преобразования над шифрующей частью входного информационного блока,
- обмен местами шифруемой и шифрующей частей входного информационного блока.

Структурный подход к моделированию криптосхем в настоящее время является наиболее распространенным среди разработчиков шифров. Это обусловлено следующим рядом причин:

- необходимостью оперативной доработки существующих криптоалгоритмов в связи с резким уменьшением стойкости к атакам полным перебором, обусловленной прогрессом в области средств вычислительной техники,
- трудоемкостью разработки криптографически стойких S-блоков,
- высокими требованиями к стойкости разрабатываемых криптосхем.

Известно, что одной из наиболее насущных потребностей модификации криптоалгоритма на сегодняшний день является адаптация к увеличению размера входного блока и секретного

ключа. Для некоторых подклассов СБШ структурная модель криптоалгоритма допускает простую модификацию путем дублирования УСК до получения преобразования требуемой размерности.

S-блоки являются ядром СБШ, во многом определяя их криптографические свойства. Значительное увеличение размеров подстановки является чрезвычайно сложной задачей, поэтому актуальным является использование в новых разработках S-блоков ранее созданных шифров.

Использовании в архитектуре криптоалгоритма УСК с исследованными криптографическими свойствами повышает уровень доверия общественности к дизайну шифра.

Наряду с вышеуказанными, построенная с помощью УСК структурная модель шифра обладает также рядом преимуществ, имеющих большое значение для разработчика шифра:

- простота модификации и замены УСК,
- наглядность описания,
- возможность изолированного тестирования криптографических свойств УСК.

Последнее свойство дает основания полагать, что полученная модель будет обладать свойством верифицируемости.

Полная совокупность УСК, с помощью которых может быть описан некоторый класс СБШ, составляет базис структурного проектирования для указанного класса криптосхем. Результатом структурного синтеза является выбор рациональной архитектуры криптоалгоритма. Процесс синтеза модели криптоалгоритма может быть описан пятеркой:

$$G_M(C, R, U_M, V_M, H),$$

где G_M (•) представляет собой функцию проектирования, C – базис проектирования, R – множество правил структурного синтеза, U_M – совокупность неварьируемых параметров, задающих формальное описание вычислительной среды реализации криптоалгоритма, U_M – совокупность варьируемых параметров, H – критерии синтеза.

Критерии синтеза представляют собой набор эксплуатационных характеристик y_i моделируемого криптоалгоритма

$$y_i = f_i(U_M, V_M), y_i \le h_i,$$
$$h_i \in H, i = 1, N$$

и соответствующих им ограничений h_i в виде числовых значений, которым должны удовлетворять указанные характеристики.

Общий алгоритм синтеза модели криптопреобразования представляет собой итерационный процесс, включающий последовательность следующих элементарных шагов:

- структурный синтез криптопреобразования, выполняемый разработчиком в элементах базиса проектирования на проблемно-ориентированном языке,
- автоматическое формирование программной модели криптопреобразования по описанию ее структуры.
- выбор системы варьируемых параметров и их начальных значений,
- определение значений эксплуатационных характеристик и удовлетворение их заданным ограничениям.

Перебором варьируемых параметров в итерационном цикле модель совершенствуется для удовлетворения заданным критериям синтеза.

Во второй главе описывается методика построения и анализа моделей программных реализаций криптопреобразований. В качестве формального описания структурной модели криптопреобразования была предложена денотационная модель, формирующая описание шифра в виде, приближенном к формальной спецификации. Разработан формальный язык для описания денотационных моделей криптоалгоритмов. Предложенное подмножество языка является полным. Разработана многоступенчатая процедура преобразования денотационной модели шифра в процедурную модель, соответствующую фон-неймановской модели вычислителя. Процедура включает проверки на целостность и непротиворечивость полученной модели.

Разработан алгоритм преобразования процедурной модели шифра в последовательность команд гипотетической ЭВМ. С этой целью была предложена модель гипотетического процессора, учитывающая особенности конвейерной и суперскалярной обработки, характерные для современных процессорных платформ. Разработан интерпретатор последовательности инструкций гипотетического процессора, моделирующий процесс вычислений на гипотетической ЭВМ. В процессе работы данного интерпретатора могут быть получены различные характеристики программной реализации криптосхемы, в частности, определена теоретическая

верхняя граница производительности алгоритма, компактность кода и эффективный параллелизм.

Денотационной моделью шифра называется формальное описание криптоалгоритма в виде последовательности утверждений о значении его различных параметров. Таким образом, полученная модель представляет собой набор полей описания. Каждое поле состоит из имени некоторого параметра шифра и его текущего значения. Понятие поля универсально – в качестве поля может рассматриваться как указатель на предопределенную (или внешнюю) функцию преобразования, так и различные параметры шифрования, такие, как размер секретного ключа или входного информационного блока.

Язык описания денотационных моделей криптопреобразований представляет собой формальный язык, грамматика которого может быть представлена в расширенной нотации Бэкуса-Наура. Грамматика языка относится к классу LR(1)-грамматик, реализующих метод восходящего разбора с чтением входных символов слева направо и использованием процедуры правостороннего вывода; при этом число предварительно просматриваемых лексических единиц равно 1. Для задания последовательностей и списков используются леворекурсивные правила подстановки. Грамматика языка разработана с учетом особенностей построения программных реализаций криптоалгоритмов, что предполагает наличие интерфейсной и реализационной части в описании шифра.

Преобразование денотационного описания шифра в программный код на выбранном языке программирования реализуется путем применения многоступенчатой процедуры компиляции. Автором работы был разработан универсальный компилятор, позволяющий преобразовывать исходное описание модели шифра в программный код на языке высокого уровня (язык С), а также в последовательность команд гипотетической ЭВМ. Компилятор построен по классической схеме, что предполагает наличие фазы лексического, синтаксического и семантического анализа. На этапе лексического анализа производится разбор входного потока на последовательность лексем, представляющих собой элементарные структурные единицы формального языка. На этапе синтаксического анализа строится дерево разбора и анализируется соответствие описания шифра заданной грамматике. Семантический анализатор проверяет баланс по входам и выходам в

каждой паре последовательных шифрующих преобразований. Сгенерированный программный код на языке С может быть обработан стандартным компилятором Borland C++ 5.02.

Моделирование программной реализации шифра на гипотетической ЭВМ включает определение параметров модели целевой ЭВМ, генерацию соответствующего набора инструкций и интерпретацию полученного кода для определения потенциальной эффективности криптоалгоритма на выбранной аппаратной платформе.

Моделирование аппаратной платформы реализации предполагает определение следующих характеристик целевой ЭВМ:

- тип ЭВМ (VLIW- или суперскалярная архитектура),
- набор команд,
- структура и состав регистров,
- методы адресации,
- размер кэша данных и кэша инструкций,
- глубина конвейера,
- количество дублированных функциональных элементов,
- особенности одновременного выпуска команд,
- время выполнения элементарных операций и задержки.

В ходе интерпретации псевдокода, представляющего собой последовательность команд гипотетической ЭВМ, для разрешения *конфликтов по управлению используются* различные методы динамической оптимизации.

Третья глава посвящена разработке алгоритмов поиска рациональных решений на множестве синтезируемых программных моделей шифров. Предложена методика построения семейства интегральных оценок качества криптопреобразований, учитывающая особенности их конкретной реализации. Данная методика основана на построении вектора оценки на множестве независимых критериев и последующего применения процедуры линейной аддитивной свертки с весовыми коэффициентами, определяемыми методами экспертного оценивания. Результаты анализа могут быть использованы для определения множества допустимых решений, удовлетворяющих заданным ограничениям, а также для поиска оптимального решения.

К настоящему моменту отечественными и зарубежными криптографами разработано и применяется для решения различных исследовательских и практических задач несколько десятков СБШ.

В этих условиях для разработчика СКЗИ неизбежно встает проблема выбора шифра, наилучшим образом отвечающего требованиям конкретной прикладной задачи. Проведение длительной процедуры опытного тестирования для каждого из потенциальных алгоритмов-кандидатов может потребовать значительных затрат времени. По этой причине наилучшим решением является применение различных методов экспресс-оценивания, позволяющих прогнозировать поведение шифра в интересующих условиях на основе результатов моделирования.

При многокритериальном анализе моделей криптоалгоритмов для большинства известных методов поиска решений требуется обобщение выходных показателей в виде единого функционала. Наличие подобного функционала позволяет для каждой точки (вектора) рассматриваемого пространства свойств получать единую оценку и тем самым осуществлять поиск рациональных решений с использованием известных методов.

В качестве подобного функционала в данной работе была выбрана линейная композиция взвешенных критериев оценивания

$$F(X) = \sum_i k_i G_i(X),$$

где k_i – весовой коэффициент, $G_i(X)$ – критерий оценивания.

Для выбора G_i была проведена систематизация различных известных критериев, получивших отражение в открытой литературе. Исследовалась их функциональная и статистическая взаимозависимость, по результатам исследования было выработано множество независимых критериев. Полученный набор критериев является базисным.

Значения k_i определяются методами экспертного оценивания. Групповая оценка для i-го критерия формируется в количественном выражении по непрерывной шкале 0 – 1 с применением следующей реккурентной процедуры:

$$k_i^l = \sum_{i=1}^{m} e_{ij} T_j^{l-1}, j = 1,2,\ldots,n; l = 1,2,\ldots$$

$$T_j^l = \frac{\sum_{i=1}^{n} e_{ij} k_j^l}{\sum_{i=1}^{n}\sum_{j=1}^{m} e_{ij} k_i^l}, i = 1,2,\ldots,n; j = 1,2,\ldots m; T_0 = \frac{1}{m}$$

где e_{ij} $(i=1,2,...,n;\ j=1,2,...,m)$ есть оценка значимости i-го критерия j-м экспертом. Полученные значения для весов, определяют относительный вклад каждого критерия оценивания в общую интегральную оценку.

Четвертая глава содержит описание разработанного инструментария МАРК (Моделирования и Анализа программных Реализаций Криптографических преобразований). Рассматриваются составляющие его компоненты, интерфейсные функции и правила взаимодействия при выполнении системных операций. Предлагается методика применения разработанного инструментария для создании новых и модификации существующих криптоалгоритмов.

Главной задачей разрабатываемого инструментария является организация некоторого "каркаса", реализующего набор общих концептуальных принципов моделирования и анализа на примере СБШ, но при этом имеющего широкие возможности наращивания и модификации компонент.

Ядро системы состоит из диспетчера задач и трех функциональных модулей, осуществляющих управление ресурсами вычислительной системы в процессе моделирования.

Модуль интерфейса реализует графический интерфейс приложения с пользователем посредством развитой системы меню и диалоговых окон, а также предоставляет средства сопряжения с внешними по отношению к системе модулями. Взаимодействие с внешними криптографическими библиотеками осуществляется по специфицированному интерфейсу, с внешними приложениями – по технологии OLE. Менеджер памяти обеспечивает файловый ввод-вывод и работу с внутренними базами данных. Исполнительный модуль реализует набор сервисных функций необходимых разработчику криптоалгоритма в процессе моделирования и анализа. Передача управления между компонентами системы осуществляется посредством диспетчера задач.

В основу создания данного инструментария была положена объектно-ориентированная технология разработки программного обеспечения. Использование объектов и классов позволяет при проектировании структур данных оперировать непосредственно понятиями предметной области.

Пример объектно-ориентированной структуры представлен на рис. 2.

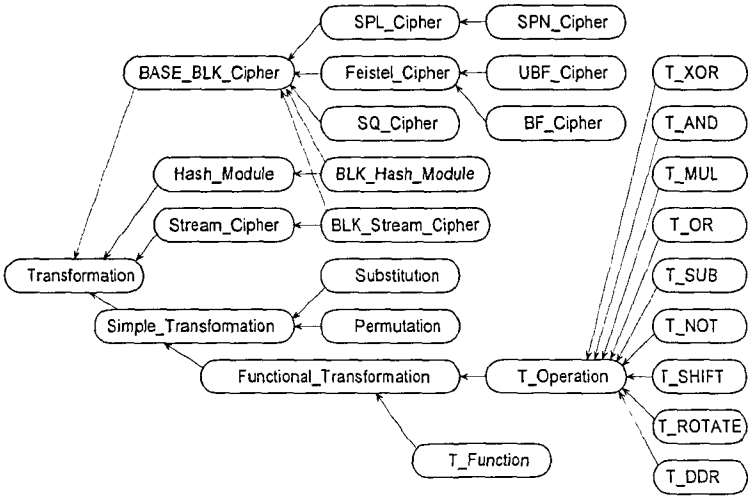

Рис. 2. Иерархия классов встроенной криптографической библиотеки инструментария МАРК.

Иерархия классов встроенной криптографической библиотеки инструментария МАРК отражает генетические зависимости между различными классами шифрующих преобразований. Реализация принципа множественного наследования предполагает наличие у класса-потомка набора свойств, характерных для нескольких классов-предков. Это имеет место в случае классов BLK_Hash_Module и BLK_Stream_Cipher.

Организация криптографической библиотеки в виде библиотеки классов упрощает разработку моделей, предоставляя разработчику шифра готовые шаблоны типовых архитектур.

В пятой главе описываются примеры практического применения разработанного программного комплекса для решения прикладных задач в двух проектах.

Первый проект представляет собой курс лабораторных работ по дисциплине "Криптографические методы защиты информации", реализованный в рамках учебного процесса на факультете "Информационная Безопасность" МИФИ. В лабораторный

практикум входит 4 лабораторных работы, освещающих следующие темы:

- методы проектирования СБШ;
- исследование свойств СБШ;
- определение теоретической верхней границы производительности СБШ методом измерения критического пути;
- построение интегральной оценки качества СБШ в соответствии с требованиями конкретной прикладной задачи.

Работы расположены в порядке, обеспечивающем проведение исследований по принципу "сквозного примера".

В задачу второго проекта входил выбор и верификация средств криптографической защиты при организации защищенного информационного обмена на базе корпоративной сети Департамента государственной аттестации научных и научно-педагогических работников Минобразования России. Работа проводилась в рамках проекта по созданию информационно-аналитического комплекса в системе послевузовского образования "аспирантура (докторантура) – диссертационный совет – ВАК России".

Понятие безопасности информации в корпоративной сети Департамента государственной аттестации научных и научно-педагогических работников Минобразования России включает:

- защиту информации от несанкционированного доступа, как со стороны, так и внутри Департамента. Должны быть исключены как несанкционированные получение и копирование информации, так и ее изменение (искажение, неправомерное уничтожение или внедрение).
- защиту информации от потери или искажения по аппаратным причинам (сбои, перегрузки и т.п.),
- поступление информации не по адресу.

Наиболее эффективным решением задачи обеспечения целостности и конфиденциальности данных, передаваемых по открытым каналам связи, на сегодняшний день является применение VPN-технологий. В качестве программного решения для организации виртуальной частной сети в Департамента государственной аттестации научных и научно-педагогических работников Минобразования России по соображениям стоимости и совместимости было выбрано программное решение на базе серии VPN-продуктов ЗАСТАВА компании "Элвис+". Особенностью VPN-продуктов ЗАСТАВА является отсутствие встроенных средств

криптографической поддержки. При этом для реализации различных функций криптографической защиты используются внешние по отношению к VPN ЗАСТАВА криптомодули, работающие по открытому интерфейсу OpenCryptoAPI.

При формировании перечня требований к криптографическим средствам защиты, применяемым во встраиваемых криптографических модулях VPN ЗАСТАВА, был проанализирован целый ряд конкретных показателей, параметров и характеристик обрабатываемых данных, включая их суммарный объем, внутреннюю структуру, методы обработки и требования к защищенности. Другим аспектом анализа являлась структура входящих и исходящих информационных потоков корпоративной сети.

На основе сформированного перечня требований средствами инструментария МАРК было произведено ранжирование различных СБШ с точки зрения пригодности для решения конкретных прикладных задач защиты. Для выбранного криптоалгоритма было произведено тестирование оптимизированной программной реализации на соответствие эталонному решению, выработанному с помощью средств моделирования криптопреобразований инструментария МАРК.

В Заключении дается оценка эффективности применения предложенных методов моделирования и анализа программных реализаций криптопреобразований и рассматриваются перспективы развития работ в данном направлении. Проведенные исследования и разработки позволяют сделать следующие выводы:

- Исследованы различные подходы к проектированию СБШ, проведен сравнительный анализ типовых архитектур СБШ.
- Построена обобщенная классификация СБШ, основанная на методологии проектирования.
- Разработан формальный язык описания структурных моделей криптопреобразований.
- Разработан алгоритм преобразования формального описания структурной модели криптопреобразования в программную модель.
- Разработана методика построения семейства интегральных оценок качества криптопреобразований.

- Разработан универсальный инструментарий моделирования, анализа и оценки программных реализаций криптопреобразований.

Публикации по теме диссертации

1. Минаева Е.В. AES — новый стандарт шифрования (обзор).//Безопасность информационных технологий, № 2, М.: МИФИ, 1999, с. 31 – 46.
2. Минаева Е.В. Причины ненадежности криптографического ПО. //Безопасность информационных технологий, № 3, М.: МИФИ, 1999, с.72 – 78.
3. Минаева Е.В., Петрова Т.В. Комплексный подход к решению задач обеспечения безопасности современных информационных систем. Труды семинара "Информационная безопасность – Юг России", Таганрог, 1999, с.25 – 27.
4. Минаева Е.В. Современные подходы к конструированию оптимальных алгоритмов генерации расширенного ключа в итеративных блочных шифрах. //Безопасность информационных технологий, № 2, М.: МИФИ, 2000, с.24 – 26.
5. Минаева Е.В. О методе построения интегральных оценок надежности симметричных блочных криптоалгоритмов. Труды семинара "Информационная безопасность – Юг России", Таганрог, 2000, с.161 – 169.
6. Минаева Е.В. Разработка инструментария моделирования программных реализаций симметричных блочных криптопреобразований. В сб. тезисов конференции "Методы и технические средства обеспечения безопасности информации" 29-30 октября, Санкт-Петербург, 2000, с.118 – 120.
7. Minaeva E.B. Using Numerical Methods for Non-Linear Approximation of Symmetric Block Ciphers. Proceedings of the CSIT'2000, v.2, USATU Publishers, 2000, pp.69 – 74.
8. Малюк А.А., Минаева Е.В., Петров В.А. Проблемы моделирования процессов и систем защиты информации. Тезисы докладов Международной конференции "Региональная информатика" РИ-98. С.-Петербург, 1998, с. .