На правах рукописи

Коршиков Сергей Борисович

МЕТОД РЕЗУЛЬТАТИВНОГО ИСКАЖЕНИЯ ГЕОМЕТРИЧЕСКИХ ДАННЫХ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ МОДЕЛЕЙ МАШИНОСТРОИТЕЛЬНЫХ ИЗДЕЛИЙ

Специальность 05.13.01
Системный анализ, управление и обработка информации
(Авиационная и ракетно-космическая техника)

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Москва – 2008 год

Работа выполнена на кафедре «Прикладная информатика» Аэрокосмического факультета Московского авиационного института (государственного технического университета, МАИ)

Научный руководитель:	доктор технических наук, профессор Падалко Сергей Николаевич
Официальные оппоненты:	доктор технических наук Осин Михаил Иванович
	кандидат технических наук Давыдов Юрий Васильевич
Ведущая организация:	Федеральное государственное унитарное предприятие "Центральный аэрогидродинамический институт им. проф. Н.Е Жуковского"

Защита состоится «___» _____ 2008 г. в __ часов на заседании диссертационного совета Д 212.125.12 в Московском авиационном институте (государственном техническом университете, МАИ) по адресу: 125993, г.Москва, А-80, ГСП-3, Волоколамское шоссе, д.4.

С диссертацией можно ознакомиться в библиотеке Московского авиационного института (государственного технического университета, МАИ).

Отзывы, заверенные печатью, просьба высылать по адресу: 125993, г.Москва, А-80, ГСП-3, Волоколамское шоссе, д.4, МАИ, Ученый совет МАИ.

Автореферат разослан «___» _____ 2008 г.

Ученый секретарь диссертационного совета Д 212.125.12,
кандидат технических наук, доцент

В.В.Дарнопых

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы.

Разработка и внедрение современных систем информационной поддержки изделий на протяжении всего их жизненного цикла требует решения ряда актуальных задач, одной из которых для систем машиностроительного профиля является обеспечение конфиденциальности данных о геометрии изделия. При этом требуется обеспечить конфиденциальность как при их хранении, так и при обмене этими данными между различными предприятиями и/или их подразделениями, участвующими в реализации жизненного цикла.

Объектом защиты в данном случае является полная, характерная для CAD/CAM/CAE-систем двухкомпонентная геометрическая модель изделия. Связано это с тем, что современные технологии интегрированного решения задач жизненного цикла изделий, в частности технологии параллельного проектирования, предполагают работу на паритетной основе, т.е. изменения в конструкцию до принятия окончательных решений могут вносить, в пределах полномочий, все участники процесса, выступающие при обмене информацией как передающей, так и принимающей сторонами. В этих условиях использование каких-либо упрощенных форматов при передаче данных о геометрии изделия (JT, STEP и др.) ограничено, и передаваться должна двухкомпонентная геометрическая модель изделия в полном объеме, размерность которого может достигать нескольких Гб.

Основным способом обеспечения конфиденциальности при обмене информацией в общем случае является использование криптографических алгоритмов. Данные алгоритмы, как правило, носят универсальный характер, но применительно к защите данных о геометрической модели изделия им присущи две группы недостатков:

1) экспоненциальный рост трудоемкости операций шифрования/ расшифрования;
2) уязвимость шифра из-за формулярности документа модели.

Более того, использование методов конфиденциальной передачи данных (SSL, PGP) не позволяет их применять для защищенного хранения, т. к. их использование подразумевает наличие определенных протоколов передачи данных.

Учитывая сказанное, проведенное в предлагаемой диссертационной работе исследование возможностей использования специфики представления геометрических данных о машиностроительных изделиях в CAD/CAM/CAE-системах в интересах обеспечения конфиденциальности как при хранении этих данных, так и при обмене ими является актуальным.

Целью работы является разработка и теоретическое обоснование схемы обработки информации с использованием методов системного анализа в процессе хранения и обмена данными электронных моделей машиностроительных изделий, существенно сокращающей объем подлежащей защите информации при сокрытии самого факта защиты.

Достижение данной цели в работе включает решение следующих задач:

1) разработку схемы обработки информации для защищенного хранения и обмена данными о изделиях, состоящую из предпроцессной обработки модели с целью выделения ограниченного набора оригинальных значений искажаемых параметров, передаваемых далее в шифроблоке параллельно с документом искаженной модели, и результативного искажения исходной модели, передаваемого далее без криптообработки;
2) анализ специфики представления электронной модели изделия, характерного для современных систем геометрического моделирования и хранимого в формулярных документах CAD/CAM/CAE систем;
3) определение правил выделения искажаемой информации и условий обратимости параметрических преобразований модели (компонент и модели в целом), выполняемых при её искажении;
4) формулировку задачи результативного искажения модели и разработку алгоритма её решения;
5) разработку структурно-логической схемы интеграции результативного искажения геометрической модели машиностроительных изделий с CAD/CAM/CAE системами и системами криптообработки данных.

Объект исследования: процесс обработки геометрической информации при хранении и передаче электронных моделей изделий.

Предмет исследования: информационная поддержка изделий на различных этапах жизненного цикла.

Методы исследования: основаны на топологическом и конструктивном представлении электронных моделей, методах обработки, хранения и обмена геометрической информацией об изделиях, методах оптимизации и методах организации взаимодействия информационных систем.

Научная новизна работы состоит в том, что в ней для решения задачи защиты геометрических данных электронных моделей машиностроительных изделий предлагается использовать специфику представления информации в формулярных документах современных CAD/CAM/CAE–систем, что позволило разработать метод результативного искажения, обеспечивающий максимизацию изменения объема геометрической модели при условиях, обеспечивающих восстановимость искаженных моделей.

Практическая значимость полученных в работе результатов заключается в том, что решена задача обеспечения конфиденциальности хранимой и передаваемой по отрытым каналам данных проектной информации с использованием специфики представления проектных данных, что позволило существенно повысить устойчивость криптоалгоритмов и снизить временные затраты на шифоропреобразование.

Научные результаты, выносимые на защиту:

1. Метод результативного искажения геометрической модели (компонент и сборки) машиностроительных изделий с целью её защиты при передаче по открытым каналам связи, который обеспечивает следующие преимущества:
   1) существенное сокращение объема криптоблока, передаваемого параллельно с искаженной моделью, по сравнению с криптоблоком геометрии изделия в целом;
   2) сохранение у искаженной модели всех признаков «правдоподобия», и тем самым сокрытие факта наличия системы защиты, при максимальном отличии физических свойств изделия-оригинала от искаженного изделия;
   3) формируемый криптоблок не содержит информацию о стандартных и/или известных компонентах, что исключает раскрытие шифра путем выделения соответствующих фрагментов криптоблока.
2. Формальные ограничения на искажения исходной модели машиностроительных изделий - как отдельных компонент (деталей), так и сборочных связей - обеспечивающие возможность выполнения обратного преобразования (восстановления) искаженной модели, основанные на двухкомпонентной геометрической модели и механистическом представлении сборочных зависимостей.
3. Формализация задачи результативного искажения геометрической модели машиностроительных изделий в виде задачи максимизации разности объемов исходного и искаженного изделий, что трактуется как максимальное отличие их физических свойств, при ограничивающих условиях, обеспечивающих восстановление искаженной модели.
4. Алгоритм построения результативного искажения геометрической модели сборочного машиностроительного изделия, базирующийся на методологии генетических алгоритмов. Алгоритм позволяет получить условно-оптимальное решение задачи обратимого искажения модели за ограниченное число шагов.

Апробация работы и публикации.

Основные результаты доложены и обсуждены на 6-ой международной конференции «Авиация и космонавтика 2007» (г. Москва, 2007 г.); третьей всероссийской научно-практической конференции «Компьютерная интеграция производства и ИПИ-технологии» (г. Оренбург, 2007 г.); 7-ой международной конференции «Авиация и космонавтика 2008» (г. Москва, 2008 г.).

Основные результаты работы опубликованы в двух отчетах о научно-исследовательских работах, трех статьях, две из которых в издании из рекомендованного ВАКом перечня.

Структура и объем работы.

Диссертация состоит из четырех глав, заключения, списка литературных источников из 83 наименований. Работа изложена на 133 страницах машинописного текста, содержит 33 рисунка и 9 таблиц.

СОДЕРЖАНИЕ РАБОТЫ

В первой главе диссертационной работы рассматривается современное состояние систем автоматизированного проектирования как элемента систем поддержки жизненного цикла изделий, приводятся характеристики современных предприятий, одной из которых является распределенность (географическая и организационная). Выявляется основной объект информационного обмена – электронная геометрическая модель (ГМ) изделия, являющейся формулярным, то есть построенным по определенному формату, документом. Рассматриваются методы и способы организации защиты информации, содержащейся в ГМ, приводятся их достоинства и недостатки. На основе анализа современных методов защиты информации и правил построения ГМ предлагается схема защиты информации об изделии, устраняющая основные недостатки применяемых методов. Формулируются требования к такой схеме и ставятся задачи исследования.

Наиболее интенсивно ГМ изделия используется на этапах проектирования, инженерных расчетов, подготовки производства. При этом, в зависимости от организации процесса движения по жизненному циклу и назначенным ролям, для обмена геометрическими данными применяются различные форматы ГМ.

В случае, если от принимающей стороны не требуется внесение изменений в конструкцию изделия, то достаточным является использование облегченных форматов хранения данных ГМ, например STEP, JT и др. Основным достоинством таких форматов является малый объем, а недостатком – невозможность их использования для внесения изменений в модель. При разработке модели на паритетной основе несколькими предприятиями (этап проектирования) или внесения изменений в модель на последующих этапах ЖЦИ для учета различных требований (технологических и др.), то есть, если доступ на запись к модели должны иметь несколько субъектов, использование облегченных форматов хранения не представляется возможным. В этом случае требуется хранить и передавать полную ГМ. Наиболее часто в современных системах геометрического моделирования (СГМ) в качестве ГМ используется двухкомпонентная параметрическая модель (ДПМ).

Исходя из того, что задача защищенного хранения информации отличается от задачи защищенной передачи только тем, что в качестве канала передачи данных используется дисковый накопитель или другое устройство хранения информации, а адресантом и адресатом является один и тот же принципал, то в дальнейшем рассматривается только схема защищенной передачи. При этом подразумевается, что все рассуждения, относящиеся к этой схеме, будут справедливы и для схемы защищенного хранения.

В главе рассмотрены основные типы сред передачи данных, исследованы возможности организации защиты проектной информации (на основе открытых каналов передачи данных, на основе секретных каналов передачи данных). Создание секретного канала связи является сложным и затратным организационно-техническим мероприятием, и не всегда гарантирует защищенность передаваемой информации. Поэтому рассматриваются только применение программно-аппаратных средств защиты для передачи информации по открытым каналам данных.

Фактически применяемые средства защиты информации от несанкционированного доступа разделяются на два типа: криптографический и стеганографический. Первый заключается в организации шифропреобразования открытого текста, второй – в скрытии открытого текста в некотором стороннем документе.

Стеганографическое преобразование сложно применить для организации защиты данных ГМ, во-первых, из-за ее значительного информационного объема, во-вторых, из-за отсутствия подходящих контейнеров. Более того, до сих пор нет четких критериев для анализа стойкости стеганографических алгоритов.

Криптографическая защита позволяет осуществлять защищенную передачу данных по открытым каналам связи. Приводится обзор систем защиты информации, изучается их ресурсоемкость и применимость для организации защиты геометрической информации, хранимой в документах ГМ, на основе чего рассматривается широко распространенная схема, заключающаяся в комбинированном использовании открытых каналов передачи данных и криптографической защиты информации

При этом возможно использование нескольких подходов. В первом случае криптографическая защита используется непосредственно в момент передачи сообщения (SSL, PGP). Данная схема имеет существенный недостаток, а именно, невозможность использования для защищенного хранения информации. Второй подход заключается в использовании криптосистемы для формирования шифротекстов непосредственно до передачи сообщения, то позволяет осуществлять как защищенное хранение, так и передачу данных по открытому каналу.

Основные недостатки этого подхода заключаются, во-первых, в экспоненциальном росте трудоемкости шифропреобразования при увеличении объема передаваемой информации (что является характерным при обмене ДПМ); во-вторых, в уязвимости полученного шифротекста к некоторым видам криптоатак из-за наличия в нем латентного ключа, что вызывается формулярностью открытого текста.

Рассматривается параметризация в современных СГМ, и на ее основе изучается возможность сокращения объема информации, подлежащей защите для формулярного документа СГМ. Предлагается схема защиты проектных данных, называемая схемой результативного искажения, которая базируется на искажении реальных значений параметров геометрической модели, выделении

из модели изделия некоторого малого набора параметров и использовании его в качестве открытого текста. Формулируются требования к такой схеме:

1) правдоподобность искажения, заключающаяся в сходстве формы исходной и искаженной моделей;
2) обратимость искажения, заключающаяся в возможности восстановления исходной модели по искаженной заменой значений искаженных параметров на исходные;
3) сохранение структуры модели, то есть безошибочное преобразование исходной модели в искаженную.

Предлагаемая схема защищенной передачи данных дополняет типовую специальной обработкой модели до передачи, заключающейся в выделении ограниченного набора параметров модели и дальнейшей их передачи в зашифрованном виде параллельно с файлом ДПМ, значения параметров которого заменены искаженными значениями, и восстановлением исходного файла ДПМ на стороне адресата (рис. 1). Для разработанной схемы характерно снижение трудоемкости благодаря формированию блока ключевых параметров, объем которого, в зависимости от модели, может быть меньше в тысячи раз объема файла модели (рис. 2).

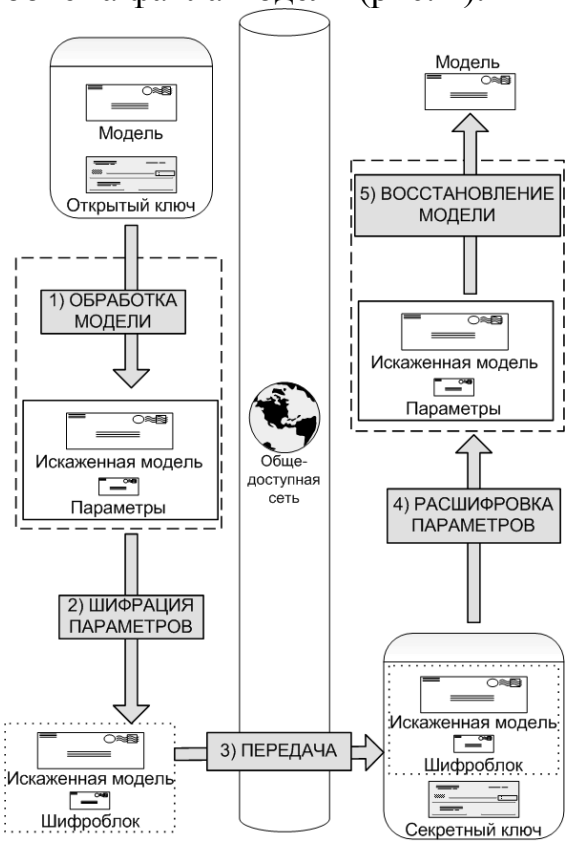

Рис. 1. Предлагаемая схема передачи данных

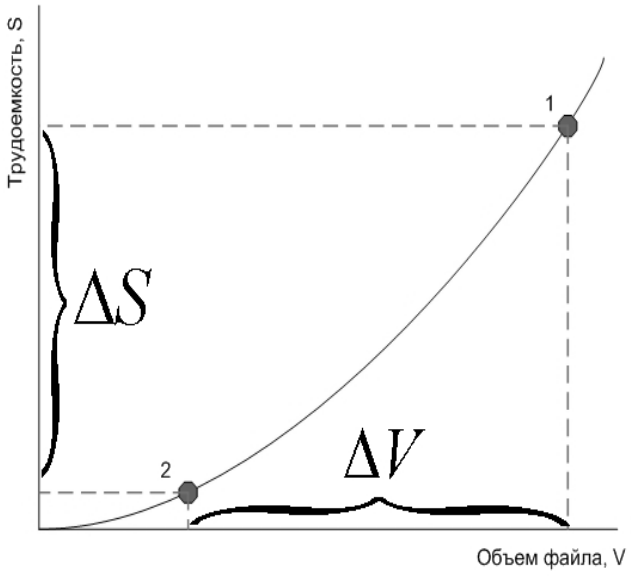

Рис 2. Снижение трудоемкости обработки при применении схемы результативного искажения

В основе данной схемы лежит решение задачи обеспечения максимального искажения исходной ГМ при условии возможности ее

однозначного восстановления, учитывая специфику представления геометрической информации в электронных моделях изделий. Формализации и решению данной задачи посвящены следующие главы диссертационной работы.

Вторая глава работы посвящена исследованиям применяемых в СГМ геометрических моделей и схем параметризации, а также формулировке условий обратимого искажения параметров геометрической модели. Приводится исторический обзор реализаций ГМ в системах геометрического моделирования.

Известно, что ГМ изделия может быть представлена в различных видах, например, каркасном, поверхностном и твердотельном. В современных CAD/CAM/CAE–системах, как правило, используется ДПМ, состоящая из граничного (поверхностного) и конструктивного (твердотельного) представлений. При этом граничное представление модели используется для вычисления габаритно-массовых характеристик модели и выполнения операций моделирования (например, построения границы пересечения тел и т. п.). Однако оно не удобно для работы конструктора, так как требует от него специальных знаний топологии оболочек. Для непосредственной работы конструктора используется конструктивное представление, которое, к тому же, содержит историю построения модели. На конструктивном представлении вводится параметризация. Но вычисление характеристик модели на основе конструктивного представления значительно сложнее, чем на основе граничного представления. Поэтому современные СГМ используют два взаимодополняющих представления, актуализируемые относительно друг друга в процессе моделирования.

Таким образом, на представление модели в виде ДПМ задаются параметры формы, определяемые в модели детали (компонента сборки) и параметры положения, определяемые в модели сборки (сборочного изделия).

В работе анализируется ДПМ детали, которая представляется в виде пары:

$$M = \{B, G\}, \qquad (1)$$

где B - граничное представление, G - конструктивное представление.

Граничное представление (ГП) содержит описание оболочек модели, состоящее из граней, ребер, циклов ребер, вершин и формируемое обычно для удобства вычислений в виде трех таблиц:

$$B = \{T_F, T_E, T_V\}, \qquad (2)$$

где T_F - таблица граней, содержащая уравнения граней и ссылку на граничные ребра граней; T_E - таблица ребер, содержащая уравнения ребер и ссылку на вершины, инцидентные ребру; T_V - таблица вершин, содержащая перечень вершин.

Конструктивное представление (КП) содержит историю построения модели в виде дерева операций построения и параметрические зависимостей:

$$G = \{G', \Upsilon\} \qquad (3)$$

Здесь G' - дерево построения, представляющее собой совокупность операций построения и неявных булевых операций:

$$G' = \bigcup_{i=1}^{n} G_i, G_i = G_{i-1} \cup O_i, \quad (4)$$

где i - номер яруса дерева построения, G_i - частичное дерево построения по i -ый ярус включительно, O_i - операция построения i -го уровня.

Аналогично частичному КП введено понятие частичного ГП, как структуры данных, эквивалентной частичному КП: $B_k \approx G_k$.

Параметрические зависимости Υ определяются набором:

$$\Upsilon = \{P, \Psi(P)\}, \quad (5)$$

где P - множество параметров модели, а функции вида Ψ описывают зависимости между параметрами:

$$p_{a1} = \psi(p_{b1},..,p_{bc}), p_{b1},..,p_{bc} \in P \setminus p_{a1}, c < |P|. \quad (6)$$

В этом случае параметры p_a, стоящие в левой части формулы (6), являются зависимыми параметрами, а параметры p_b, стоящие в правой части формулы (6), являются управляющими параметрами.

На основе выше изложенного, для модели (1) явно выделяется набор параметров формы:

$$M = \{B, G', \Upsilon\}, \quad (7)$$

В виде (7) может быть представлена модель детали (компонента сборки). Сборочные модели (модели сборочных изделий) состоят из набора моделей (7) и условий их взаимного расположения относительно друг друга, определяющих параметры положения. Таким образом, модель сборки A представима в виде:

$$A = \{M_s, \Pi_k\}, s = 1\ldots n, k = 1\ldots d, \quad (8)$$

где M_s - это модель компонента сборки, Π_k - позиционная связь, задающая расположение компонент сборки относительно друг друга.

Каждую из связей Π_k можно записать в виде:

$$\Pi_k = \{F_{M'}, F_{M''}, r_k, q\}. \quad (9)$$

Здесь $F_{M'}$ $F_{M''}$ - соответственно грани моделей компонентов сборки M', M'', r_k - параметр, а q - тип связи, задающей взаимное расположение граней $F_{M'}$ и $F_{M''}$ относительно друг друга (например, под определенным углом, совмещено, параллельно на расстоянии и т. п.).

Исходя из выше изложенного, каждой модели вида (8) ставятся в соответствие наборы параметрических зависимостей Υ_s, $s = 1\ldots n$, где n - количество компонентов сборки, и Π_k, $k = 1\ldots d$, где d - количество позиционных связей.

Таким образом, параметрическое преобразование модели компонента осуществляется изменением значений управляющих параметров, определенных связями вида Υ_s.

В работе рассматриваются ограничения, накладываемые на преобразование вида:

$$M \xrightarrow{\text{I}} \tilde{M}, \qquad (10)$$

где M - исходная модель, $\tilde{M}$ - искаженная модель.

Очевидно, что параметрическое преобразование I будет существовать в случае, если для модели $\tilde{M}$ сохранится дерево построения, т. е. $G = \tilde{G}$.

Для ДПМ, содержащих параметризованные сплайны, на параметрическое преобразование накладывается дополнительное условие отсутствия самопересечений сплайнов, образующих профили кинематических тел. При изменении такой модели, существование преобразования (10) проверяется с использованием поиска самопересечений сплайнов, что позволяет исключить из рассмотрения заведомо ошибочные варианты преобразования. Для поиска и устранения самопересечений используется алгоритм, построенный на критерии Лассера, заключающийся в том, что если $\sum_{i=0}^{n-2} |\alpha_i| < \pi$, то кривая самопересечений не имеет. Здесь α_i есть углы характеристической ломаной сплайна.

Довольно часто параметрическое изменение модели является необратимым. Обратимость параметрического изменения определяется порядком построения модели, используемой парадигмой параметризации («мягкая» или «жесткая»), наличием ассоциативных связей между операциями построения и другими факторами. Обратное преобразование, заключающееся в подстановке исходных значений параметров в модель, может привести к получению модели, не являющейся эквивалентной исходной, или даже к разрушению модели.

В работе формулируются ограничения, накладываемые на преобразование (10) для существования обратного преобразования $\tilde{M} \xrightarrow{\text{I}^{-1}} M$.

Как отмечено выше, в процессе моделирования каждый ярус дерева построения добавляет информацию об операции в КП, и изменяет ГП, добавляя или удаляя топологические объекты.

Известно, что при параметрическом изменении происходит модификация ГП, а КП остается неизменным с точностью до параметров. Изменение ГП может быть нескольких видов: удаление объектов, добавление объектов, изменение границ объектов. Исходя из того, что ГП не содержит журнала предыдущих состояний, можно заключить, что если при обратном параметрическом изменении от СГМ потребуется создать или удалить топологический объект, то возможна ситуация, при которой исходная и искаженная модели не будут эквиваленты. Отсюда следует, что обратимым будет параметрическое изменение, при котором не происходит добавление или удаление топологических объектов в граничное представление модели.

Таким образом, условием обратимости параметрического преобразования (10) модели компонента M является совпадение размерностей таблиц граней, ребер и вершин модели, т. е. если при преобразовании (10) выполняются условия:

$$\begin{cases} |T_F| = \left|\tilde{T}_F\right| \\ |T_E| = \left|\tilde{T}_E\right|, \\ |T_V| = \left|\tilde{T}_V\right| \end{cases} \tag{11}$$

то $\exists \tilde{M} \xrightarrow{\Gamma^{-1}} M$.

Условие (11) является условием обратимости параметрических преобразований модели компонента сборки.

Однако если модель используется в качестве одного из компонентов сборочной конструкции, то на его преобразование также накладываются ограничения, определяемые параметрами положения компонента. Очевидным условием, накладываемым на преобразование сборочной модели вида (8), является отсутствие пересечений компонент сборки, то есть:

$$\tilde{M}_{s1} \cap \tilde{M}_{s2} \neq \varnothing, s1 \neq s2;\ s1, s2 = 1 \ldots n \tag{12}$$

Другим условием, определяемым структурой сборочной модели, является условие сохранения сборочных связей между компонентами после преобразования, а именно, эквивалентность набора сборочных связей до и после преобразования:

$$\Pi_k = \tilde{\Pi}_k \tag{13}$$

Однако при изменении формы компонент может потребоваться изменить значения параметров формы R_k, определяемых связями Π_k, для чего используются пересчет значений параметров позиционных связей на основе измененных расстояний (углов) между компонентами сборки.

Таким образом, в формальной постановке задача получения результативного искажения может быть определена следующим образом.

Пусть дана модель сборки $A = \{M_s, \Pi_k\}, s = 1 \ldots n, k = 1 \ldots d$, где M_s - модели компонентов сборки, Π_k - позиционные связи между компонентами. Каждая модель компонента представима в виде $M_s = \{G_s, B_s\}$, с ГП $B_s = \{T_F, T_E, T_V\}$, и КП $G_s = \bigcup_{i=1}^{n} G_s^{\,i}, G_s^{\,i} = G_s^{\,i-1} \cup O_s^{\,i}, i = 1 \ldots q$. Параметризация КП ставит в соответствие каждой операции $O_s^{\,i}$ набор параметров P_s^{ij}, и позволяет представить модель M_s в виде совокупности частичных моделей и параметров операций $M_s = \{M_s^{\,i}, P_s^{ij}\}$.

Тогда задача результативного искажения сводится к максимизации разности объемов моделей при исходных и искаженных значениях параметров, где разность объемов является показателем эффективности искажения:

$$\Delta = \sum_s \left| V(P_s^{ij}) - V(\tilde{P}_s^{ij}) \right| \to \max \tag{14}$$

при условиях:

1)

$$\begin{cases} |T_F| = |\tilde{T}_F| \\ |T_E| = |\tilde{T}_E| \text{ для } \forall M_s \\ |T_V| = |\tilde{T}_V| \end{cases} \quad (15)$$

2)

$$\tilde{M}_{s1} \cap \tilde{M}_{s2} \neq \varnothing, s1 \neq s2;\ s1, s2 = 1 \ldots n \quad (16)$$

3)

$$\Pi_k = \tilde{\Pi}_k \quad (17)$$

В третьей главе работы рассматриваются способы сокращения размерности задачи результативного искажения на основе исследований предметной области; вводится понятие ключевых параметров модели; приводится алгоритм решения задачи генетического типа.

Исходя из доступности данных о модели в открытых источниках, проводится классификация моделей. Чтобы избежать появления в шифротексте известных значений параметров, что дает пары «открытый тест – шифротекст», требуется исключить их из множества искажаемых параметров. Предложенная классификация моделей проводится по времени разработки модели по отношению к текущему проекту.

При изучении множества параметров модели $P = P_K \cup P_A$, где P_A – подмножество общеизвестных параметров модели, P_K – подмножество искажаемых параметров модели, выявлены три основных типа моделей:

1) стандартные модели, для которых $P_K = \varnothing, P_A = P$;
2) модифицируемые модели, для которых $P_K \subseteq P \setminus P_A,\ P_A \neq \varnothing$;
3) разрабатываемые модели, для которых $P_K = P,\ P_A = \varnothing$.

Для стандартных моделей, к которым по данной классификации относятся модели, которые не разрабатывались в рамках текущего проекта, и используются без каких-либо изменений, например модели изделий, на которые есть государственный стандарт, стандарт предприятия или модели покупных изделий, проводить искажение параметров не требуется, так как они не представляют собой коммерческой тайны. Модифицируемые модели дорабатываются или изменяются в рамках текущего проекта, поэтому для них требуется проводить искажение только добавленных параметров. Для разрабатываемых моделей, как для вновь полученных объектов в процессе работы над текущим проектом, требуется проводить искажение всего множества параметров модели.

Таким образом, проведенная классификация моделей позволяет сократить размерность задачи, исключив из рассмотрения общеизвестные параметры моделей.

Исходя из того, что в качестве критерия оптимизации используется разность объемов исходной и искаженной моделей, то множество искажаемых параметров также можно сократить, изучив влияние изменения параметра на изменение объема модели. Для этого вводятся понятия слабо и сильно влияющих параметров. Каждому параметру модели, как непрерывному, так и дискретному, соответствует диапазон вариации. Если рассмотреть изменения объема модели, вызванного вариацией значения параметра, то можно выделить две группы параметров:

1) слабо влияющие параметры, для которых изменение объема модели много меньше куба изменения параметра, $\Delta V \ll (p_{\max} - p_{\min})^3$;
2) сильно влияющие параметры, для которых изменение объема модели сравнимо с кубом разности изменения параметра, $\Delta V \cong (p_{\max} - p_{\min})^3$.

Исходя из такой классификации параметров, основанной на критерии оптимизации, слабо влияющие параметры искажать не требуется.

Однако, в общем случае, диапазон вариации параметра неизвестен, более того, диапазон вариации параметра обычно неявно зависит от значений других параметров модели. Поэтому для определения слабо влияющих параметров используется следующая процедура. Пусть $P_b = (p_{b1},...,p_{bn})$ — множество управляющих параметров модели, а $\langle P_b \rangle = (\langle p_{b1} \rangle,...,\langle p_{bn} \rangle)$ - множество значений управляющих параметров. Выберем максимальное значение параметра $\langle p_b \rangle_{\max} = \max(\langle P_b \rangle)$. Тогда, если $\langle p_b \rangle_i \le \varepsilon \langle p_b \rangle_{\max}$, то параметр p_{bi} является слабо влияющим параметром.

Коэффициент ε, в зависимости от вида модели, может принимать значения в диапазоне $[0,05;0,2]$ (меньшие значения коэффициента характерны для моделей, ограничивающий параллелепипед которых близок к кубу).

На основе классификации моделей, параметров и типов параметров, вводится понятие ключевых параметров, являющихся исходными данными для задачи результативного искажения.

Ключевые параметры – ограниченный набор управляющих параметров геометрической модели, не находящихся в открытом доступе, изменение значений которых существенно изменяет геометрические характеристики модели.

Таким образом, *результативное искажение геометрической модели* − это обратимое, не разрушающее структуру модели изменение значений ключевых параметров этой модели, которое обеспечивает максимизацию разности объемов исходной и искаженной моделей.

Поставленная задача результативного искажения (14) относится к классу задач нелинейного программирования. Однако данная задача обладает спецификой, которая не позволяет применять классические методы решения таких задач. Несмотря на то, что ограничивающие условия являются числовыми, они существенно нелинейны и представлены в виде алгоритмического «черного ящика». Наряду с этим, даже сокращение размерности задачи, обусловленное классификациями моделей и параметров,

оставляет ее размерность достаточно высокой, что наряду со сложной системой ограничений, и требованием минимизации временных затрат, делает ее решение достаточно трудоемким. В то же время практическое применение результатов решения задачи позволяет ограничиться поиском одного из близких к оптимальному решений. В этих условиях наиболее рациональным является использование эвристических алгоритмов, например, алгоритма генетического типа.

Кодирование параметров осуществляется следующим образом: ключевой параметр модели κ_s^{ij} является геном, вектор параметров компонента K_s^{ij} является хромосомой, и множество параметров сборки $\{\mathrm{K}_s^{ij}\}$ составляет генотип. Схема кодирования приведена на рис.3.

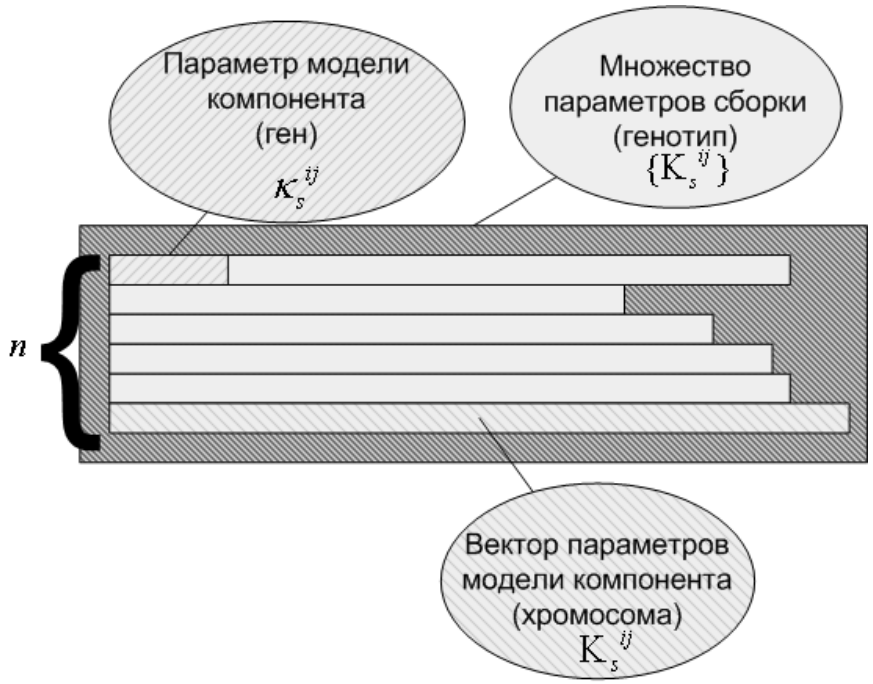

Рис. 3. Схема кодирования

Согласно методологии генетических алгоритмов требуется определить начальную популяцию, вычислить приспособленности каждой особи на основе условий (15-17); на основе наиболее приспособленных особей сформировать следующее поколение, с использованием генетических операторов кроссовера и мутации. Для каждого поколения проверяется функция приспособленности (т. е. критерий оптимизации). При стабилизации функции приспособленности (т. н. условие конвергенции, когда функции приспособленности текущего и предыдущего поколении отличаются не более чем на определенное значение) алгоритм завершается и выбирается особь с максимальным значение функции приспособленности.

Для инициации получим начальное искажение ($t = 0$, t - номер поколения) для каждого параметра, для чего потребуется установить диапазон вариации для каждого ключевого параметра. Пусть $\kappa_i^* \in \left[h_i \kappa_i, \frac{1}{h_i} \kappa_i \right]$, где h_i -

случайное число в диапазоне $[0,6;1]$, $i=1\ldots k$. Осуществив процесс начального искажения l раз, получим начальную популяцию из l особей. Обозначим особь как $A_j, j=1\ldots l$. Для вычисления начальной популяции ограничимся $l=25$, чтобы сократить количество ресурсоемких операций вычисления приспособленности (проверки граничного представления).

Проверим КП и ГП, и выявим, искаженные значения каких параметров вызывают их нарушения. Не нарушая общности, будем считать, что для операции мы имеем удовлетворяющие последующим моделям искаженные значения параметров $\kappa_1^*,\ldots\kappa_m^*$ и не удовлетворяющие значения параметров $\kappa_{m+1}^*,\ldots\kappa_k^*$. Вернем параметрам $\kappa_{m+1}^*,\ldots\kappa_k^*$ их исходные значения $\kappa_{m+1},\ldots\kappa_k$. Будем продолжать процесс до тех пор, не получим удовлетворяющий моделям набор $\kappa_1^*,\ldots\kappa_m^*$ и $\kappa_{m+1}^*,\ldots\kappa_k^*$, или не убедимся в том, что ни одно из искаженных значений не подойдет для модели. Отбракуем особи, идентичные исходным.

Проведем выбраковку в популяции (для первого прохода алгоритма этот шаг пропускается). Вначале удалим из популяции те особи, для которых не выполняются условия обратимости искажения (15-17). Затем удалим из популяции особи, для которых число искаженных параметров m меньше количества искажаемых параметров $m_{\max}$. После этого рассчитаем для каждой особи функцию приспособленности как:

$$F(A_l)=\frac{\sum_{i=1}^{m_{\max}}\left|\kappa_i^*-\kappa_i\right|}{m_{\max}}$$

Затем вычислим среднее значение приспособленности популяции, как $F_{mid}=\frac{\sum_l F(A_l)}{l}$ и для каждой особи определим отношение $F(A_l)/F_{mid}$. Если отношение $F(A_l)/F_{mid}\geq 1$, то особь будет участвовать в скрещивании, в противном случае, вероятность этого события меньше единицы (т. н. стратегия пропорционального отбора), которая реализуется через дополнительный массив: геном особи помещается в этот массив $ent(F(A_l)/F_{mid})$ раз, после чего вычисляется случайное число в диапазоне $\xi\in[0,1]$. Если $\xi<\frac{F(A_l)}{F_{mid}}-ent\left(\frac{F(A_l)}{F_{mid}}\right)$, то геном добавляется в массив еще раз, иначе – не добавляется.

Так как значения параметров представляют собой вещественные числа, то в качестве оператора скрещивания используем SBX (Simulated Binary Crossover). Пусть u - случайное число, распределенное в диапазоне (0,1) по равномерному закону. Выберем из промежуточной таблицы 2 родителя - $A^y=(\kappa_1^y,\ldots\kappa_k^y), y=1,2$. На основании этих родителей создаются 2 потомка

$H^y = (h_1^y, \dots h_k^y), y = 1,2,$ где $h_j^1 = \frac{1}{2}\left((1-\beta_1)\kappa_j^1 + (1+\beta_1)\kappa_j^2\right),$

$h_j^2 = \frac{1}{2}\left((1+\beta_2)\kappa_j^1 + (1-\beta_2)\kappa_j^2\right),\ j = 1 \dots k$. $\beta_{1,2}$ - числа, вычисленные по формуле:

$$\beta = \begin{cases} (2u)^{\frac{1}{v+1}},\ u \le \frac{1}{2} \\ \left(\frac{1}{2(1-u)}\right)^{\frac{1}{v+1}},\ u > \frac{1}{2} \end{cases},$$

v - случайное число в интервале $[\kappa_j^1, \kappa_j^2]$.

Таким методом формируются все потомки для записей промежуточной таблицы, и формируется таблица потомков. Применение кроссовера SBX обеспечивает передачу потомкам "лучших" генов и не требует сохранения промежуточной популяции, в которой представлены особи-родители и особи-потомки. Чтобы избежать преждевременной сходимости алгоритма применяется оператор мутации, заключающийся в случайном инвертировании одного из битов двоичного представлении гена.

Условием останова является достижение конвергенции по большинству параметров, то есть при стабилизации значения критерия эффективности $\Delta(14)$. Будем считать, что конвергенция достигнута, когда значения суммарной функции приспособленности отличаются не более чем на 5%.

В случае не достижения конвергенции в 15 поколении останавливаем процесс и выбираем в качестве решения особь в максимальной функцией приспособленности из текущей популяции.

Таким образом, построенный для решения задачи результативного искажения алгоритм представляет собой совокупность классификаторов моделей, параметров и генетического алгоритма. Набор ключевых параметров шифруется с использованием системы защиты информации (СЗИ) предприятия и сохраняется в файле модели. Полученный ГА позволяет достаточно быстро получить необходимое искажение параметров модели, для которой гарантируется выполнения условий обратимости искажения. В результате экспериментов получено, что наиболее рациональными сочетаниями управляющих параметров алгоритма являются: размер начальной популяции – 25 особей, вероятность мутации – 0,01, значение конвергенции – 5%, ограничение на число поколений – 15. Такой набор характеристик позволяет быстро получить близкое к оптимальному решение, сведя к минимуму количество ресурсоемких вычислений функции приспособленности.

Общая схема алгоритма результативного искажения приведена на рис.4.

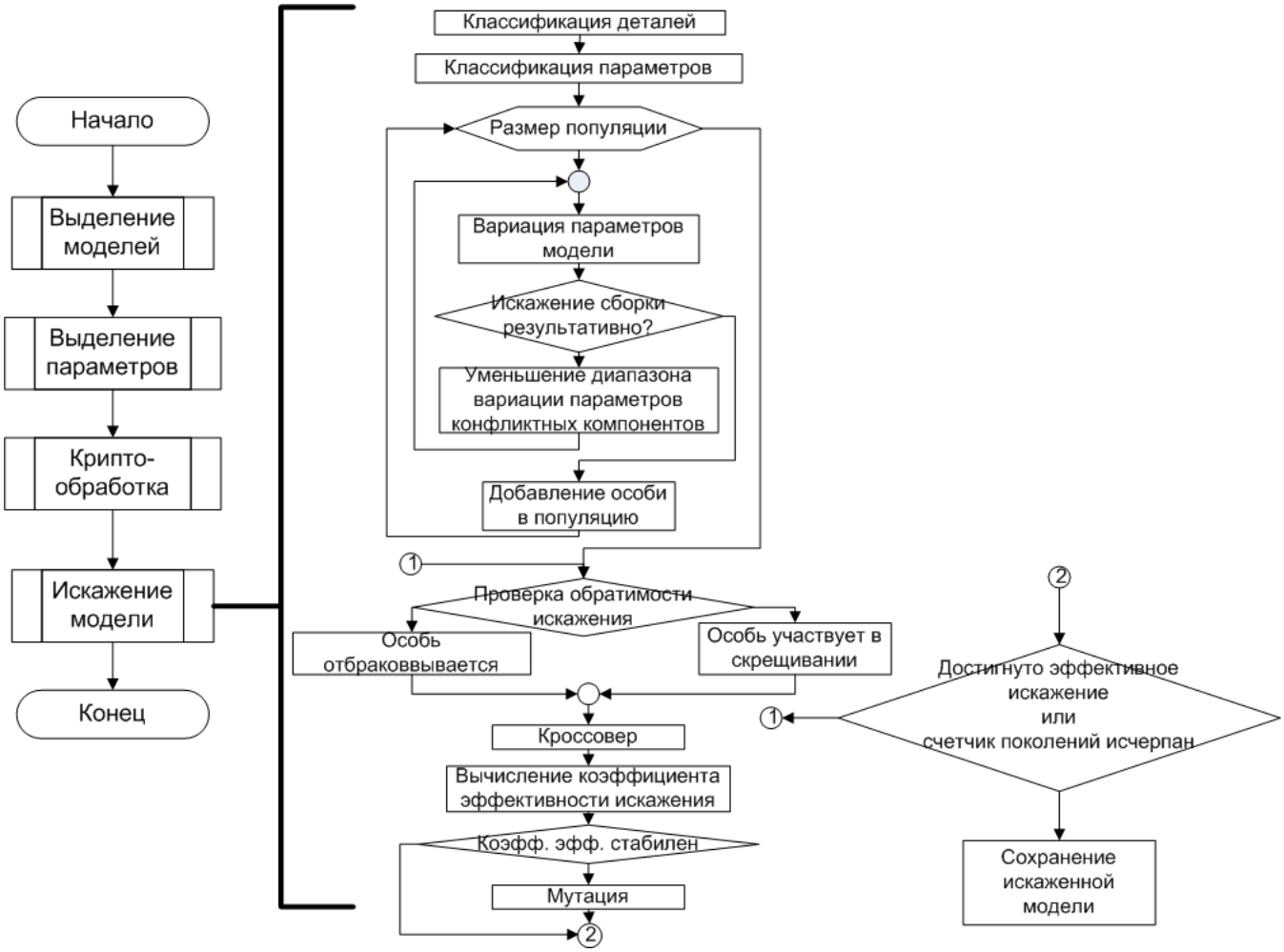

Рис. 4. Общая схема алгоритма результативного искажения

<u>В четвертой главе</u> работы рассматривается место подсистемы результативного искажения (ПРИ), реализующей соответствующий метод, в информационной среде предприятия, приводится пример работы метода.

ПРИ искажения состоит из двух частей – универсальной и настраиваемой. Универсальная часть реализует классификаторы моделей, параметров и генетической алгоритм, и может быть применена для работы с ДПМ. Для интеграции в информационную среду предприятия предназначена настраиваемая часть ПРИ, представляющая собой два интерфейса – интерфейс СГМ и интерфейс СЗИ. Интерфейс СГМ обеспечивает получение из файлов ДПМ набора ключевых параметров, проверку условий обратимости преобразования, осуществляемых ядром СГМ, и сохранение в файлах ДПМ искаженных значений параметров. Интерфейс СЗИ предназначен для передачи набора ключевых параметров в СЗИ и получения шифроблока ключевых параметров, сохраняемых далее в файле ДПМ.

Схема интеграции представлена на рис.5.

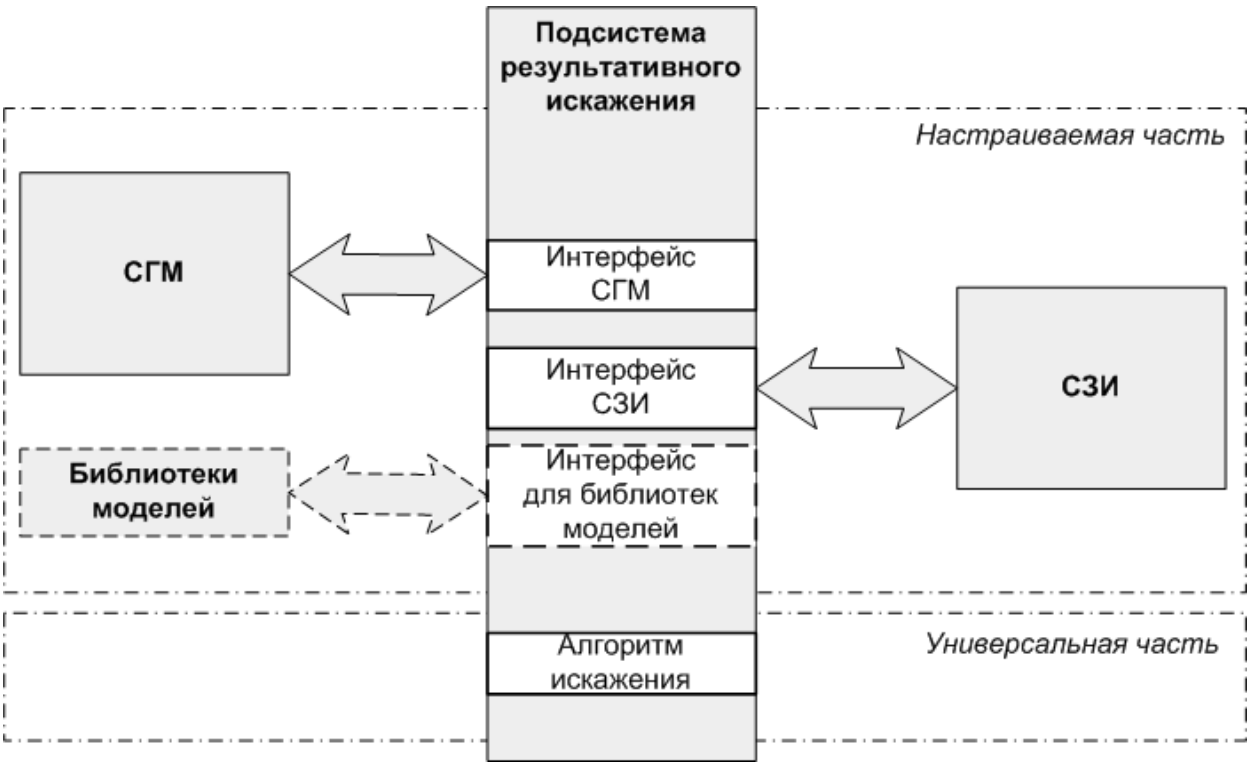

Рис. 5

Результаты работы и предложенный алгоритм апробированы на упрощенной модели обводов самолета «Меркурий» (компания «АвиаСТЭП», г. Москва). Модель построена с использованием глобальной контрольной структуры и содержит порядка 2000 параметров. Общий объем файлов модели 14 Мб. В результате работы классификаторов в качестве входных данных алгоритма определены 38 ключевых параметров, разделенных по трем областям искажения (ОИ): часть кабины (ОИ1* - 14 параметров), хвостовое оперение (ОИ2 - 14 параметров) и крыло (ОИ3 - 10 параметров). Виды модели до и после искажения приведены на рис. 6а и 6б, соответственно.

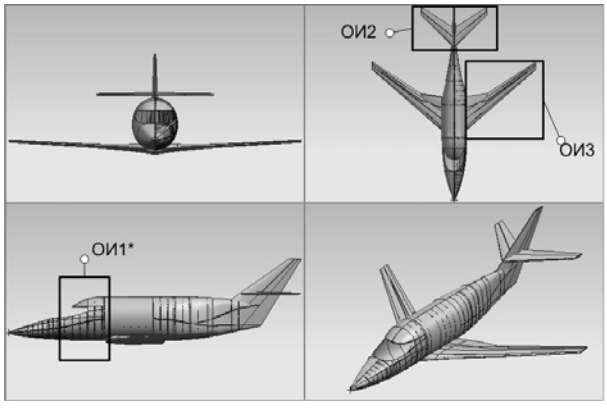

Рис. 6а

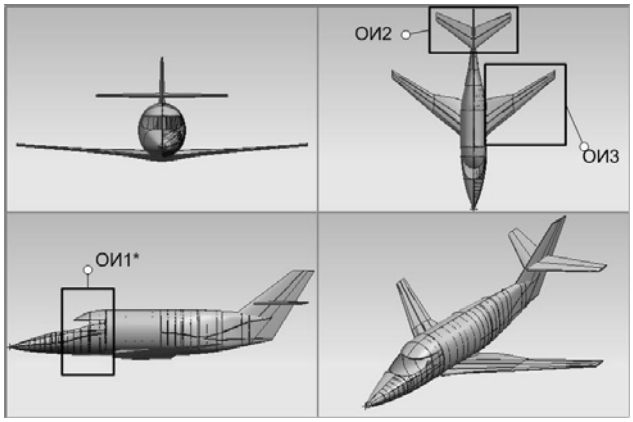

Рис. 6б

Исходные значения параметров и их искаженные значения приведены в табл. 1.

Табл. 1

Область искажения 1		
Параметр	*Исходное значение*	*Искаженное значение*
_p686	2908 мм	2800 мм
_p689	3278 мм	3150 мм
_p692	3648 мм	3500 мм
_p22	3700 мм	3600 мм
_p817	4018 мм	4050 мм
_p820	4388 мм	4312 мм
_p25	4500 мм	4350 мм
_p823	4758 мм	4760 мм
_p826	5498 мм	5327 мм
_p829	5868 мм	5778 мм
_p832	6238 мм	6112 мм
_p835	6608 мм	6618 мм
_p838	6978 мм	6982 мм
_p28	7000 мм	7013 мм
Область искажения 2		
Параметр	*Исходное значение*	*Искаженное значение*
_p2077	9145 мм	9068 мм
_p2078	3300 мм	3378 мм
_p2103	11502 мм	11257 мм
_p2101	1950 мм	2194 мм
_p2116	13858 мм	13447 мм
_p2114	600 мм	1011 мм
_p2187	2500 мм	2700 мм
_p2161	11400 мм	11487 мм
_p2163	1 °	4 °
_p2164	1450 мм	1570 мм
_p2194	13900 мм	13580 мм
_p2193	1 °	5 °
_p2201	550 мм	600 мм
_p2156	2000 мм	2145 мм
Область искажения 3		
Параметр	*Исходное значение*	*Искаженное значение*
_p2338	4285 мм	4354 мм
_p2351	400 мм	500 мм
_p2721	2550 мм	2940 мм
_p2849	6250 мм	5980 мм
_p2612	826 мм	990 мм
_p2750	2217 мм	2433 мм
_p2878	5433 мм	5024 мм
_p3074	0 мм	50 мм
_p3075	0 мм	100 мм
_p3076	0 мм	130 мм

Объемы исходной и искаженной моделей приведены в табл. 2.

Табл. 2

Искажаемые области	Объем до искажения, м³	Объем после искажения, м³	Разность, %
ОИ1* (часть кабины)	5,5852	6,538	17,05
ОИ2 (хвостовое оперение)	1,4439	1,6031	11,03
ОИ3 (крыло)	1,7844	1,8977	6,35

Таким образом, искажение небольшого числа параметров, проведенное по предложенному алгоритму, существенно изменяет геометрические характеристики модели.

Общий объем файлов модели равен 14 Мб, объем ключевой информации (с необходимыми связями) 190 байт. Следовательно, количество подлежащей защите информации сокращено для рассмотренной модели примерно в 75000 раз.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. В работе показано, что использование специфики представления проектной информации в формулярных документах современных CAD/CAM/CAE-систем в виде двухкомпонентной модели, позволяет выделить набор параметров геометрической модели, по размерности отличающийся от модели в целом на порядки, которые могут быть искажены без нарушения правдоподобности исходной модели в пределах, обеспечивающих восстановление исходной модели [1, 4].
2. Введено понятие результативного искажения как обратимого изменения параметров модели для которого, при сохранении правдоподобия искаженной модели, исходная и искаженная модель отличаются максимально [1,3].
3. Предложен метод результативного искажения, сведенный к задаче максимизации разности объемов исходного и искаженного изделий при условии сохранения возможности обратного преобразования искаженной модели изделия. Данный метод является универсальным для большинства современных СГМ, так как базируется на двухкомпонентном представлении геометрической модели [1,3,4].
4. Получены условия, обеспечивающие обратимость искажения, разделенные на две группы:
   1) условие восстановления компонент (деталей) изделия, базирующиеся на совпадении размерности таблиц (ребер, вершин, граней) моделей до и после искажения [1,3];
   2) условия восстановления сборок, базирующиеся на совпадении наборов позиционных связей исходной и искаженной модели и отсутствии самопересечений компонент в искаженной модели [2].

5. Разработан и реализован алгоритм решения задачи результативного искажения генетического типа. Алгоритм обеспечивает поиск условно-оптимального значения за ограниченное число шагов [1].
6. Предложена схема системы, реализующей алгоритм результативного искажения, обеспеченная необходимыми интерфейсами и структурами данных, в рамках которой реализован регламент взаимодействия с СГМ и СЗИ [1,4].
7. На основе предложенной схемы реализовано взаимодействие системы, реализующей метод результативного искажения с СГМ. Показана эффективность реализованной схемы для решения поставленных задач: сокращения объема защищаемой информации, минимизации объема вычислений и максимизации отличия физических свойств искаженной модели от исходной [1,4].

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

в изданиях, рекомендованных ВАКом

1. Коршиков С.Б., Падалко С.Н. Метод результативного искажения параметров двухкомпонентной геометрической модели для обеспечения безопасности ее передачи по открытым каналам / Вестник Московского авиационного института.– Москва: МАИ, 2008. – Т. 15. – № 1. – с. 126–135.
2. Коршиков, С.Б. Алгоритмы восстановления сборочных связей при параметрическом изменении компонентов сборок / Вестник Московского авиационного института.– Москва: МАИ, 2008. – Т. 15. – № 3. – с. 212–218.

иные публикации

3. Коршиков, С.Б. Условия обратимости параметрических изменений двухкомпонентной геометрической модели // Третья всероссийская научно-практическая конференция «Компьютерная интеграция производства и ИПИ-технологии»: Сб. материалов, г. Оренбург 2007 г. – Оренбург: ИПК ГОУ ОГУ, 2007. – с. 143–146.
4. Коршиков С.Б. Использование специфики представления данных о геометрии изделия в современных СГМ для обеспечения конфиденциальности проектной информации // Авиация и космонавтика – 2008. Международная конференция, М. 2008: Тез. докл. – М.: МАИ, 2008. – с. 96.
5. Коршиков С.Б. Новые возможности Solid Edge v10 / САПР и графика.– 2002. – № 1’2002 (62). – с. 49–52.
6. Падалко С.Н., Коршиков С.Б., Корякин Л.А., Кулик Ю.П., Степаненко А.Ю. Разработка методик гармонизации нормативной

документации и формального описания процессов информационной поддержки жизненного цикла продукции: отчет о НИР. – г. Москва: МАИ, 2005, ГК № 032-0198/05 – 72 с.

7. Падалко С.Н., Коршиков С.Б., Макаров Д.А., Станкевич А.М. Рекомендации по организации работ по комплексной автоматизации этапов жизненного цикла аэрокосмической техники: отчет о НИР. – г. Москва: МАИ, 2007, ГК № 851-0434/06 – 63 с.
8. Коршиков С.Б. Электронные модели изделий аэрокосмической техники и их агрегатов: формирование, хранение, передача / Уч. пособ. каф. 609 МАИ.– М., 2008 (рукопись). – 71 с.