УДК 621.384. **Толюпа С.В.**

ПРОЕКТИРОВАНИЕ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ПРОЦЕССЕ ВОССТАНОВЛЕНИЯ И ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ ЗАЩИТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Проектирование систем поддержки принятия решений представляет собой сложный, трудоемкий процесс, который требует использования как определенного методологического аппарата, так и соответствующего методического обеспечения. Одной из основных задач при создании такой системы является выбор ее структуры, поскольку от того, как организована система во многом зависит эффективность ее функционирования и обеспечение информационной безопасности. Для решения этой задачи предложено использовать агрегативно-декомпозиционный подход, который включает последовательную декомпозицию выполняемых системой целей, функций и задач и их агрегирование на соответствующих уровнях детализации структуры для генерирования вариантов построения системы в целом.

Ключевые слова: информационная система, защита информации, данные, доступ, информационные технологии.

Одной из основных задач при создании сложной системы является выбор ее структуры, которая определяет внутреннюю организацию и относительно устойчивые взаимосвязи элементов системы. Задачи проектирования структуры тесно связаны с задачами оптимизации функционирования систем и обеспечения ее информационной безопасности. Структура считается оптимальной, если общая эффективность разрабатываемой системы максимальна.

В каждой информационной системе можно выделить самые слабые с точки зрения безопасности места. На них необходимо обратить внимание прежде всего. К таким местам, конечно, принадлежат хранилища данных, административная система, кабельная система, система доступа из внешних сетей. Злоумышленник, найдя доступ к хранилищу данных, сможет взять из него конфиденциальные данные, а зайдя в административную систему, он будет иметь доступ ко всем ресурсам системы. К кабельной системе благодаря ее разветвленности легко присоединиться, подслушать и проанализировать данные, которые передаются, или подменить их другими [1].

Обеспечение защиты информации в системах происходит в условиях случайного действия разных факторов, часть из которых является систематизированной в стандартах, а часть заранее неизвестны. Оценка эффективности систем защиты информации (СЗИ) должна обязательно учитывать как объективные обстоятельства, так и вероятностные факторы, а ее характеристики должны иметь вероятностный характер. Особенную важность на современном этапе развития информационных технологий (ИТ) имеет обоснование оптимальных значений показателей эффективности и целевое назначение системы.

Чем более конкретно сформулирована цель защиты информации, детально выясненные ресурсы, которые привлекаются для этого, а также определен комплекс ограничений, тем в большей степени можно ожидать получения желательного результата. Если цель обеспечения информационной безопасности простая и принципиально досягаемая, то оказывается достаточно сравнительно несложных по составу и структуре средств защиты информации.

Однако при расширении круга проблем обеспечения интегральной информационной безопасности, содержание целевого назначения системы на формализированном уровне будет иметь многомерный, векторный характер. При этом значимость свойств отдельных элементов средств защиты информации снижается, а на первый план выдвигаются общесистемные задачи - определения оптимальной структуры и режимов функционирования системы, организация взаимодействия между ее элементами, учет влияния внешней среды и т. др. При целеустремленном объединении элементов в систему последняя будет иметь специфические свойства, сначала не свойственные ни одной из ее составных частей. При комплексном подходе имеют первостепенное значение только те свойства элементов,

которые определяют взаимодействие друг из друга и оказывают влияние на систему в целом, а также на достижение поставленной цели [2].

Задача проектирования структуры системы состоит в таком отображении определенным образом сгруппированных функциональных задач по определенным образом сгруппированным элементам системы, при котором достигается экстремум критерия качества отображения $\Re$ при выполнении заданных ограничений как на безопасность так и на некоторые аспекты функционирования.

Основной характеристикой качества отображения $\Re$ обычно является эффективность разрабатываемой системы. Поскольку информационные системы относится к системам реального времени, поэтому в качестве показателя эффективности (распределенной системы поддержки принятия решения) РСППР целесообразно взять оперативность выдаваемых решений. Учитывая это, рассмотрим постановку задачи проектирования структуры РСППР с учетом взаимосвязи ее задач и узлов в процессе функционирования и обеспечения безопасности. Для ее формализации введем следующие обозначения:

$i = \overline{1, I}$ – множество задач системы функционирования и обеспечения безопасности;

$j = \overline{1, J}$ – множество узлов системы;

t_{ij} – время выполнения i-й задачи, решаемой в j-м узле;

$t_{ij'}$ – время передачи единицы информации между узлами j и j';

$\alpha_{ii'}$ – средний поток информации между i-й и i'-й задачами в процессе функционирования системы и обеспечения безопасности;

K_{ij} – затраты на разработку i-й задачи решаемой в j-м узле;

K_l – стоимость технических средств l-го типа.

Задача проектирования оптимальной структуры РСППР, состоящая в определении уровней и узлов системы (в том числе и комплекса технических средств в узле) с учетом затрат на обмен информацией между задачами, решаемыми на различных уровнях, и затрат на эксплуатацию системы, обеспечения ее безопасности может быть записана следующим образом:

$$\min \sum_{ij} T_{iji'j'}, x_{ij}, x_{i'j'}, \tag{1}$$

где $T_{iji'j'} = \begin{cases} t_{ij}, \text{ если } ij = i'j', \\ a_{ii'}, t_{jj'} - \text{в противном случае.} \end{cases}$

$x_{ij} = \begin{cases} 1, \text{ если } i\text{-я задача решается в } j\text{-м узле,} \\ 0 - \text{в противном случае.} \end{cases}$

$x_{ij} = \begin{cases} 1, \text{ если } j\text{-й узел оборудован } l\text{-м техническим средством,} \\ 0 - \text{в противном случае.} \end{cases}$

при следующих ограничениях:

$$\sum_{j} x_{ij} > 1, \quad i = \overline{1, I}, \tag{2}$$

$$\sum_{ij} K_{ij} x_{ij} + \sum_{jl} K_l x_{jl} \le K. \tag{3}$$

Величина критерия (1) определяет временные затраты на функционирование системы и обеспечения ее безопасности. Ограничение (2) допускает решение i-й задачи в различных

узлах системы. Ограничение (3) учитывает тот факт, что ресурсы на создание системы не должны превышать заданной величины *K*.

Рассмотренная задача является нелинейной задачей математического программирования, решение которой аналитическими методами весьма затруднено. Это связано с тем, что на ранних стадиях проектирования параметры проектируемой системы в ряде случаев могут быть известны лишь приблизительно, с некоторым распределением вероятностей их значений или с некоторой степенью принадлежности значений параметров заданным интервалам, что приводит к неоднозначности определения оптимального (рационального) варианта структуры.

Кроме этого, учет динамики функционирования системы на этапе проектирования структуры приводит к необходимости совместного использования оптимизационных и имитационных моделей для получения оптимальных (рациональных) вариантов построения структуры системы.

Учитывая вышесказанное, для решения задачи в постановке (1) – (3) целесообразно использовать агрегативно-декомпозиционный подход [3-4]. Он включает два взаимосвязанных этапа: последовательную декомпозицию выполняемых системой целей, функций, задач и агрегирование функциональных задач на соответствующих уровнях детализации структуры для генерирования вариантов построения системы в целом и обеспечения ее безопасности.

На первом этапе исходя из целей, стратегий функционирования системы, ее функций определяется организационная структура системы и основные мереы информационной безопасности (ИБ) . В результате определяется число уровней иерархии и узлов системы, то есть определяется топологическая структура системы.

На втором этапе оптимизируется распределение выполняемых задач по уровням и узлам системы.

На третьем этапе выбирается комплекс технических средств. При этом учитываются затраты на оснащение узла техническими средствами и их эксплуатацию, а также учитываются ограничения на оперативную и внешнюю память, быстродействие этих средств.

И на заключительном этапе анализируется динамика работы узлов выбранного варианта структуры системы с использованием имитационной модели, по результатам которой происходит уточнение характеристик и параметров элементов структуры.

Таким образом, под проектированием структуры РСППР будем понимать процесс последовательного решения системно увязанных частных задач выбора его основных элементов и частей: выбора уровней и узлов и согласования их целей; оптимального распределения выполняемых задач (функций) по уровням узлам прототипа; выбора технических средств, обеспечивающих их своевременное решение.

Данные задачи решаются итерационно в силу их взаимосвязанности и необходимости корректировки получаемых решений. А это, в свою очередь, предполагает изначально построение базового (опорного) варианта структуры РСППР, а затем его последовательное уточнение.

Выбор структуры РСППР, как правило, осуществляется на ранних стадиях проектирования, на которых объективно присутствует значительная неполнота и неопределенность исходных данных. Неполнота и неопределенность исходных данных особенно проявляется в процессе построения опорного варианта структуры РСППР. Так, например, задача распределения задач по узлам и уровням системы должна решаться практически в условиях отсутствия основных характеристик решаемых задачах, так как этот этап осуществляется по времени значительно раньше их разработки. Отсутствие характеристик решаемых задач также усложняет и выбор необходимых технических средств для их эффективного решения. Неполнота и неопределенность исходных данных требуют для решения задач построения опорного варианта использования адекватных методов принятия решений, основанных на применении нечетких экспертных оценок для задания

исходных данных и представления результатов. По мере получения более точных исходных данных опорный вариант структуры уточняется более точными, количественными методами.

Задача определения числа узлов и уровней РСППР состоит в выборе такой его топологии, которая при прочих равных условиях обеспечивает эффективную реализацию функций и задач в процессе функционирования. Эта задача решается как при первоначальном определении количества узлов и уровней РСППР, так и итерационно по результатам имитационного моделирования с целью их уточнения.

Изначально топология системы должна формироваться согласно принципу соответствия структуры РСППР организационно-штатной структуре информационной системы. Данный принцип предполагает, что внедрение средств автоматизации не повлечет коренной перестройки структуры системы управления. Скорее наоборот, предполагается, что средства автоматизации должны мягко вписываться в существующую структуру управления без кардинальных изменений последней.

Кроме этого, в организационной структуре РСППР должны быть предусмотрены также технологические узлы решения функциональных задач управления. Исходя из этого задачу формирования топологии РСППР можно сформулировать следующим образом.

Пусть F – множество уровней управления, P – множество должностных лиц, обеспечивающих управление, а Q – множество операционно-технологических схем решения задач управления. Требуется построить отображение

$$\aleph : F \times P \times Q \to M \times N ,$$

где M, N – множество уровней и узлов РСППР соответственно.

Это отображение можно декомпозировать на два: $\aleph_1 : F \times P \to M \times N$ и $\aleph_2 : Q \to N$. Выбор организационной структуры в рамках отображения $\aleph_1$ характерен тем, что в этом случае отсутствуют достаточно обоснованные формализованные критерии, что индуцирует применение для этих целей экспертных методов анализа соответствия структуры РСППР организационно-штатной структуре системы диспетчерского управления.

Выбор узлов РСППР в рамках отображения $\aleph_2$ должен осуществляться на основе анализа оптимального варианта операционной технологии решения всей совокупности задач диспетчерского управления, обеспечивающего при заданных ограничениях по времени и объемам информации минимум затрат на ее обработку. В таком варианте выделяются функционально связные технологические операции, которые в совокупности будут составлять предметную направленность того или иного технологического узла. Суть такого подхода состоит в следующем [5].

Для каждой задачи РСППР формируется совокупность различных вариантов операционной технологии ее решения. Эти варианты представляются в виде графа, узлы которого соответствуют используемым техническим средствам и носителям информации, а дуги отражают взаимосвязи и последовательности операций. Время выполнения операции задается в виде оценки длины соответствующей дуги. Для любой задачи РСППР, рассматриваемой отдельно, оптимальный вариант технологии находится как путь минимальной длинны в вышеуказанном графе.

Распределение задач между уровнями и узлами иерархической системы является достаточно типичной задачей проектирования сложных технических систем. Эффективность функционирования РСППР во многом зависит от того, каким образом задачи будут распределены по его уровням и узлам. Поэтому задача состоит в таком распределении множества решаемых задач между уровнями и узлами РСППР, чтобы удовлетворить некоторый критерий эффективности и заданные ограничения.

Кроме функциональных задач РСППР включает также задачи общего назначения (вспомогательные задачи). Эти задачи могут решаться на различных уровнях и узлах, поэтому их требуется распределить по узлам системы таким образом, чтобы удовлетворить некоторому критерию эффективности и заданным ограничениям. В качестве критерия эффективности целесообразно использовать минимум временных затрат, связанных с

обменом информацией между уровнями и узлами системы. С целью минимизации временных затрат, связанных с обменом информацией между уровнями и узлами системы, в каждом узле должны быть сконцентрированы те задачи, которые имеют максимальную взаимосвязь.

Практика проектирования сложных систем свидетельствует о том, что функции любой сложной системы непосредственно зависят от специфики тех задач, которые она решает. Исходя из этого, задача определения функций узлов РСППР будет состоять в нахождении отображения $\Im : S \to F$, где S – множество задач управления сетью, а F – множество функций узлов.

Под отображением $\Im$ будем понимать механизм последовательного преобразования предметной направленности задач управления сетью в функции узлов. На первом этапе строится алгоритмическая модель системы управления сетью (СУС), которая дает возможность уточнить специфику решаемых задач. На втором происходит агрегирование элементов алгоритмической модели, в результате которого формируются функции узлов РСППР.

Понимая под РСППР совокупность различных взаимодействующих технических элементов и людей, объединенных для достижения общей цели, роль *интеграции* состоит в эффективном их взаимодействии и связях между элементами для получения максимума эффекта.

Рассмотренные концептуальные требования вытекают из более общего требования – *информатизации*, которое предполагает, прежде всего, высокое качество информационного обслуживания пользователей.

Требования к техническим характеристикам аппаратно-программных средств узлов РСППР вытекают из оперативно-тактических требований, предъявляемым к задачам управления и характеристик их программной реализации. В свою очередь оперативно-тактические требования к задачам управления определяются задачами ИС и условиями ее функционирования.

Уточнение технического варианта РСППР осуществляется по мере уточнения системных требований к техническим средствам с целью выбора наиболее рационального варианта. Учитывая тот факт, что системные требования могут быть как метрическими, так и качественными, а множество альтернативных АС, как правило, не велико, то эффективное решения данной задачи можно осуществить методом анализа иерархий [6], который является одним из эффективных методов системного анализа при решении задач, где необходимо взвешивать как метрические, так и качественные критерии в их иерархической структуре. Он состоит в декомпозиции проблемы на все более простые составляющие части и дальнейшей обработке последовательностей суждений лица, принимающего решения по парным сравнениям. В результате может быть выражена относительная степень (интенсивность) влияния элементов в иерархии.

В заключение отметим, что рассмотренный метод может эффективно быть использован для выбора СУБД совместно со схемой Захеди [7]. Это позволит создать когерентный механизм для структурированного процесса сравнения и выбора альтернативных СУБД по всему спектру аппаратной базы. Схема Захеди разработана на основе нисходящей структуры оценки, которая не зависит от принятой модели данных и включает два типа анализа: сравнение элементов альтернативных СУБД на одинаковых уровнях и объединение оценок на различных уровнях. Учитывая сказанное, выбор подходящей СУБД на основе схемы Захеди эффективно осуществляется рассмотренным методом анализа, так в этом случае эта схема будет представлять иерархическую декомпозицию задачи выбора.

В силу того, что средства безопасности любой ИС имеют ограниченные возможности относительно противодействия угрозам, всегда существует достоверность нарушения защиты, даже если во время тестирования механизмы безопасности не были обойдены или блокированы. Для оценки этой достоверности должны проводиться дополнительные исследования. В методическом плане определения эффективности СЗИ должно заключаться в выработке мысли относительно пригодности способа действий персонала или приспособленности технических средств к достижению цели защиты информации на основе измерения соответствующих показателей, например, при функциональном тестировании.

Проектирование, организация и применение СЗИ ИС фактически связано с неизвестными событиями в будущем и потому всегда содержат элементы неопределенности. Кроме того, присутствующие и другие причины неоднозначности, такие как недостаточно полная информация для принятия решений управления или социальнопсихологические факторы.

Объективной характеристикой качества СЗИ - степенью ее приспособленности к достижению уровня безопасности, который требуется, в условиях реального действия случайных факторов, может служить вероятность, которая характеризует степень возможностей конкретной СЗИ при заданном комплексе условий. Другими словами - достоверность достижения цели операции или достоверность выполнения задачи ИС. Эта достоверность должна быть установлена в основу комплекса показателей и критериев оценки эффективности СЗІ. Во время синтеза системы возникает проблема решения задачи с многокритериальным показателем. При этом рассматриваются показатели эффективности, какие назначенные при решении задачи сравнения разных структур СЗИ. Оценка оптимального уровня гарантий безопасности в определенной мере зависит от убытка, связанного с ошибкой в выборе конкретного значения показателя эффективности. Для получения численных оценок риска необходимо знать распределения ряда случайных величин. Это в определенной степени ограничивает количественное исследование уровней гарантий безопасности, которые предоставляются СЗИ, но во многих практических случаях такие оценки можно получить с помощью имитационного моделирования или по результатам активного аудита СЗИ.

Выводы. Таким образом анализ основных требований, предъявляемых к РСППР позволяет сделать вывод о том, что РСППР является сложной человеко-машинной системой, характеризуемой большим числом территориально распределенных элементов и выполняемых ими функций, высокой степенью связности элементов, сложностью алгоритмов выбора тех или иных управляющих воздействий и большим объемом перерабатываемой при этом информации. Проектирование такой системы представляет собой сложный, трудоемкий процесс, который требует использования как определенного методологического аппарата, так и соответствующего методического обеспечения. Одной из основных задач при создании РСППР является выбор ее структуры, поскольку от того, как организована система во многом зависит эффективность ее функционирования и обеспечение информационной безопасности. Поэтому при выборе структуры должны учитываться различные условия ее функционирования и степени угроз. Учитывая требования, предъявляемые к функционированию РСППР, задача выбора структуры сформулирована с учетом взаимосвязи его задач и узлов в процессе их решения. Для решения этой задачи предложено использовать агрегативно-декомпозиционный подход, который включает последовательную декомпозицию выполняемых системой целей, функций и задач и их агрегирование на соответствующих уровнях детализации структуры для генерирования вариантов построения системы в целом.

ЛИТЕРАТУРА

1. Ленков С.В. Методы и средства защиты информации / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. - К.: Техника, 2008. - Т. 1. - 465 с.
2. Власов О.М. Комплексний підхід оцінки ефективності систем захисту інформації в інфокомунікаційних мережах нового покоління / О.М. Власов, С.В. Толюпа // Наукові записки Українського науково-дослідного інституту зв'язку. Наук.-вироб. зб. – 2011 - №3(19). – С. 38-45.
3. Цвиркун А.Д. Основы синтеза структуры сложных систем / А.Д. Цвиркун. – М.: Наука, 1982. – 197 с.
4. Толюпа С.В. Застосування декомпозиційного методу для синтезу моделі контрольованої системи / С.В. Толюпа, С.С. Штаненко // Материалы IV-й международной молодежной научно-технической конференции "Современные проблемы радиотехники и телекоммуникаций РТ-2008", 21-25 апреля 2008 г. - Севастополь, 2008. – С. 112.
5. Саати Т. Принятие решений. Метод анализа иерархий. / Саати Т. – М.: Радио и связь, 1993. – 311 с.
6. Zahedi F. Data-Base Management System Evaluation and Selection Decision. – Decision Sciences. – 1985. – № 16. – P. 91–116.

Надійшла: 18.10.2012р.

Рецензент: д.т.н., проф. Олійник В.Ф.