УДК 519.6

Д. М. Ненадович, Б. И. Шахтарин

ПОСТАНОВКА ЗАДАЧИ ДЕКОМПОЗИЦИИ СИСТЕМ ПОКАЗАТЕЛЕЙ КАЧЕСТВА БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Рассмотрена возможность синтеза системы показателей качества безопасности информации, циркулирующей в инфокоммуникационной сети специального назначения, на основе методов теории декомпозиции. Представлен алгоритм параметрической декомпозиции глобальной системы показателей качества безопасности информации на локальные системы.

Одна из основных составляющих национальных интересов Российской Федерации в информационной сфере — обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России [1].

Это актуально в свете угроз, связанных с разработкой рядом государств концепций информационных войн, в которых предусмотрено создание средств опасного воздействия на информационные и телекоммуникационные системы (инфокоммуникационные системы) [2].

В таких условиях важнейшими задачами становятся оценка реального состояния существующих угроз, своевременное и достоверное выявление фактов возникновения новых угроз информационной сфере РФ.

Особый интерес представляют инфокоммуникационные сети (ИС), разворачиваемые в интересах обеспечения государственного управления — ИС специального назначения (ИС СН).

Под информационной безопасностью ИС СН понимается состояние защищенности процесса функционирования и элементов телекоммуникационной сети от внутренних и внешних угроз. В этом случае основными задачами обеспечения информационной безопасности ИС СН являются:

— оценка внутренних и внешних угроз ИС СН;

— выработка оптимального управляющего воздействия, позволяющего обеспечить максимальную эффективность функционирования ИС в условиях дестабилизирующих факторов различной природы;

— выработка оптимального управляющего воздействия, позволяющего максимально противодействовать дестабилизирующим факторам.

Решение этих задач должно быть возложено, по мнению авторов, на систему обеспечения безопасности информации (СОБИ) ИС СН, являющуюся подсистемой системы управления ИС СН в целом.

При решении поставленных задач разработчики систем СОБИ на начальном этапе проектирования неизбежно сталкиваются со следующими вопросами:

— какие параметры показателей качества (ПК) объекта управления, когда и как надо наблюдать и оценивать?

— какие ПК функционирования противоборствующей системы подлежат наблюдению и оценке?

— какими ПК и с использованием каких методов надо управлять?

Оставляя за рамками рассмотрения этого, далеко не полного, перечня задач начального этапа разработки СОБИ вопросы методологии оптимального наблюдения, оценивания и управления, сосредоточимся на вопросах формирования оптимальных систем ПК, обеспечивающих безопасность информации (БИ) ИС СН.

Этап формирования систем ПК (СПК) БИ важен, поскольку никакие удобства математического и методологического аппарата, используемого для управления БИ ИС СН, заключительным этапом которого служит принятие информационного решения о ее состоянии, не смогут компенсировать последствий неадекватно сформулированных пространства состояний БИ и обобщенного критерия оценивания состояния БИ ИС СН.

Одним из подходов к формированию состоятельной и адекватной условиям и задачам управления БИ системы ПК ИС СН, отвечающей критерию минимальной избыточности, является подход, ориентированный на использование методов структурной и параметрической декомпозиции, методов эволюции и редукции компонентов векторного ПК.

Основы теории декомпозиции сложных систем, к которым относятся и ИС СН, были заложены в работах [3–8], где было рассмотрено, каким образом задачи управления (ЗУ) сложными системами можно декомпозировать на совокупность подзадач (ПдЗУ) в целях распараллеливания задач анализа и синтеза АСУ сложными системами. При этом декомпозиция ЗУ сложной системой позволяет вскрыть структуру АСУ, связанную с ЗУ, внешними условиями функционирования сложной системы и ее элементами. Кроме того, ЗУ сложной системой формулируются как оптимизационные задачи, результатом решения которых являются лучшие с точки зрения выбранных ПК значения управляемых переменных.

Классификация математических методов теории декомпозиции проведена на основе анализа работ [3–8] и отражена на рис. 1.

Использование математического аппарата теории декомпозиции как инструмента распараллеливания процессов анализа — оценивания ПК БИ ИС СН и синтеза, — разработка и обоснование ОТТ к ПК БИ

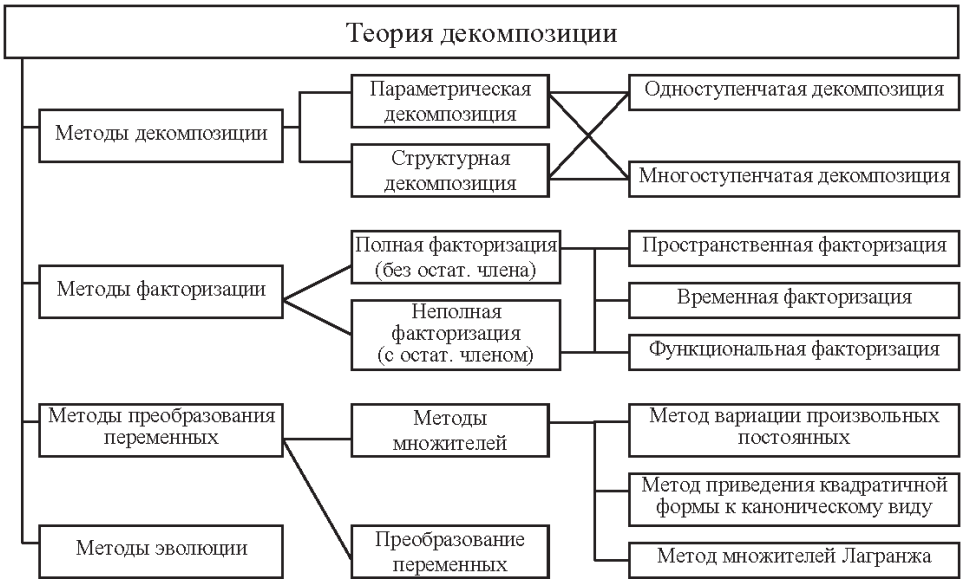

Рис. 1. Классификация математических методов теории декомпозиции

ИС СН позволят повысить оперативность и качество (точность) оценивания, а следовательно, своевременность и объективность принятия информационного решения по управлению БИ ИС СН.

Обоснуем использование теории декомпозиции для решения задачи синтеза иерархически связанной системы СПК БИ ИС СН. Декомпозиция глобальной СПК (ГСПК) БИ ИС СН предусматривает ее замену эквивалентным множеством локальных СПК (ЛСПК) БИ ИС СН. Это достигается путем поэтапной декомпозиции, при которой на первом этапе глобальная система ПК БИ ИС СН преобразуется в вид, удобный для реализации алгоритмов декомпозиции; на втором этапе осуществляется собственно декомпозиция ГСПК, а на третьем этапе – декомпозиция полученных ЛСПК БИ ИС СН.

Первые три метода из существующих шести ключевых методов математической теории декомпозиции (см. рис. 1), а именно факторизация, параметрическая и структурная декомпозиция, лежат в основе различных способов разделения ГСПК на несколько ЛСПК. При этом метод факторизации позволяет делить ГСПК БИ на независимые локальные системы ПК БИ, а два других метода позволяют реализовать разбиение ГСПК БИ ИС СН на пары взаимосвязанных локальных систем ПК БИ ИС СН. Методы преобразования переменных, преобразования Лагранжа и эволюции (развития) могут быть ориентированы на различные преобразования ГСПК БИ ИС СН, причем преобразование переменных позволяет вводить новые переменные состояния, метод Лагранжа позволяет устранить ограничения, налагаемые на локальные системы ПК (вследствие введения множителей Лагранжа в

целевую функцию), а метод эволюции позволяет преобразовать ГСПК БИ ИС СН за счет введения определенного рода допущений.

При выборе метода (группы методов) теории декомпозиции в интересах синтеза оптимальной СПК БИ ИС СН учитываются следующие основные положения [9]:

— в процессе декомпозиции необходимо вводить определенные ограничения, поскольку требуется декомпозировать ГСПК БИ ИС СН на совокупность иерархически связанных ЛСПК. Это обусловливает необходимость применения методов структурной и параметрической декомпозиции;

— поскольку взаимосвязь между отдельными процессами, являющимися объектами управления СОБИ ИС СН, должна быть изоморфна по отношению к взаимосвязи соответствующих ЛСПК, то структура (иерархия) наблюдаемых, оцениваемых и управляемых СОБИ ИС СН показателей зависит от того, каким образом ГСПК БИ сети декомпозируется на ЛСПК;

— чтобы применять рассмотренные методы декомпозиции в задаче синтеза СПК в интересах обеспечения БИ ИС СН необходимо поэтапно проанализировать весь процесс декомпозиции, учитывая то, что на каждом этапе применяется отдельный, предварительно обоснованный метод декомпозиции.

Наиболее привлекательным подходом к разработке СПК БИ ИС СН является, по мнению автора, подход, впервые предложенный в работах [7, 8], предполагающий формирование такого оптимального множества ПК БИ ИС СН, которое соответствует (адекватно) совокупности свойств сети, влияющих на обеспечение БИ ИС СН на данном этапе функционирования. Затем, если необходимо, синтезируются дополнительные ПК, позволяющие соединить исходные системы СПК в ГСПК, характеризующую в целом всю основную задачу функционирования (ОЗФ) СОБИ ИС СН.

С учетом основных постулатов данного подхода и рассмотренных ограничений сформулируем задачу декомпозиции в виде определения подзадач Y_i, на которые можно декомпозировать ОЗФ СОБИ ИС СН $W\{Y\}$, определения их содержания и взаимосвязи между ними при условии, что множество ограничений x, налагаемых на эти подзадачи, принадлежит множеству допустимых ограничений X:

$$\underset{x\in X}{W}\{Y\} = \underset{x\in X}{W}\{Y = R(Y_i)\}, \quad i = \overline{1,\ I}, \tag{1}$$

где $R(Y_i)$ — функция взаимосвязи между подзадачами.

Поскольку ОЗФ характеризуется ГСПК, а подзадачи, на которые эта цель может быть декомпозирована, — ЛСПК, то можно предположить, что ГСПК БИ ИС СН, определяющую общую цель функционирования (ОЗФ) СОБИ ИС СН, формулирует пользователь в виде

комплекса требований и допусков на ПК БИ сети. В этом случае формализация процесса синтеза СПК в интересах БИ ИС СН, состоящая в декомпозиции ГСПК на иерархическую совокупность ЛСПК, заключается в следующем [9, 10].

Пусть ГСПК $Y_{\text{БИ ИС СН}}(k)$ на k-м шаге функционирования ИС СН представляет собой функционал

$$Y_{\text{БИ ИС СН}}(k) = F(Y_1(k); Y_2(k), \ldots, Y_N(k)), \tag{2}$$

где $Y_1(k); Y_2(k), \ldots, Y_N(k)$ — соответственно векторные локальные системы ПК процессов, определяющих БИ ИС СН. Тогда ГСПК БИ ИС СН, а также отношения ограничений и взаимосвязей между СПК можно записать в виде:

$$Y_{\text{БИ ИС СН}}(k) = [Y_1(x_m(k)); \ldots; Y_i(x_m(k)); \ldots; Y_I(x_m(k))]^{\text{т}}; \tag{3}$$

$$R_i(Y_i(k)) \geqslant 0; \tag{4}$$

$$Y_i(k) = T_{ij}(Y_j(k)), \tag{5}$$

где выражение (3) характеризует вид ГСПК БИ ИС СН, в котором $i = \overline{1,\ I}$ — число ЛСПК, входящих в множество $Y_{\text{ИБ ТКС СН}}(k)$ на k-м шаге функционирования сети, $m = \overline{1,\ M}$ — число переменных (ПК), входящих в ЛСПК; выражение (4) призвано характеризовать отношения ограничений, налагаемых на ЛСПК $Y_i(k)$ в условиях внешних и внутренних воздействий, влияющих на БИ ИС СН на k-м шаге ее функционирования; выражение (5) — отношения взаимосвязи между i-й и j-й ЛСПК в условиях различного рода воздействий на БИ ИС СН (отображение j-й ЛСПК в i-ю) на k-м шаге функционирования.

Анализ множества ПК БИ мультисервисной гетерогенной ИС СН показывает, что между векторными ПК, входящими в ее состав, может существовать сложная взаимосвязь, без учета которой невозможно осуществить декомпозицию в интересах обеспечения БИ сети. Помимо этого, отдельной задачей является определение эквивалентности получаемых в результате декомпозиции ЛСПК БИ ИС СН.

С целью преодолеть отмеченные сложности, воспользуемся методами декомпозиции. Примем за основу, что две ЛСПК являются эквивалентными в том случае, если имеют в своем составе тождественные ПК. Следует отметить, что хотя ЛСПК и могут содержать тождественные компоненты (ПК), данные компоненты могут определяться на основе отличных друг от друга аналитических выражений. В работах [3, 4] задача определения эквивалентности решается с помощью сокращенных (сжатых) множеств.

Опираясь на результаты работ [9, 10], можно отметить, что процесс декомпозиции ГСПК БИ ИС СН на иерархически связанную совокупность ЛСПК, процесс поиска адекватного условиям и ЗУ оператора состояния БИ ИС СН $\breve{R}_c(k)$ должны состоять из следующих этапов.

Этап 1. Применяется метод структурной декомпозиции, позволяющий получить пару взаимозависимых ЛСПК путем видоизменения цели функционирования ($W[Y(k)] \to w[Y_i(k)]$) и (или) множества ПК БИ ИС СН ($w[Y(k)] \to w[Y_i(k)]$). Использование данного метода обусловлено структурой (иерархией) процессов, характеризующих БИ ИС СН тем, что основное внешнее свойство БИ ИС СН характеризуется на уровне процесса обеспечения безопасного (в информационном смысле) обслуживания пользователей ИС СН в целом. Внутренние свойства характеризуются на уровне других процессов (управления БИ, подавления противоборствующей системы и т.д.), зависящих друг от друга. Формализованная запись первого этапа декомпозиции, опирающегося на метод структурной декомпозиции, имеет вид

$$Y_{\text{БИ ИС СН}}(k) \cup Y_{i\,\text{БИ ИС СН}}(k),\ Y_{i\text{БИ ИС СН}}(k)=\{Y_{\text{осн.пр}}(k);\ Y_{\text{др.пр}}(k)\}; \quad (6)$$
$$W[Y(k)] \to w[Y_i(k)];$$
$$w[Y(k)] \to w[Y_i(k)];$$
$$\forall(w,y) \in Y_i(k),$$

где $Y_{\text{осн.пр}}(k)$ и $\vec{Y}_{\text{др.пр}}(k)$ — соответственно ЛСПК основных процессов и других процессов, реализуемых СОБИ ИС СН.

Этап 2. Применяется метод параметрической декомпозиции, позволяющий декомпозировать ЛСПК $Y_{\text{осн.пр}}(k)$ и $Y_{\text{др.пр}}(k)$ на отдельные пары локальных систем ПК обеспечивающих процессов. В общем виде

$$Y_{\text{осн.пр}}(k) = Y_{\text{осн.пр}}[Y_1^*(k), Y_2(k)] \ \cup\ Y_{\text{осн.пр}}[Y_1(k), Y_2^*\{Y_1(k)\}]; \quad (7)$$
$$\text{при условии } \forall\{(Y_1^{(}k), Y_2(k)) \in \vec{Y}_{\text{осн.пр}}(k)\};$$
$$\exists(Y_2(k) : Y_2(k) \in \vec{Y}_{\text{осн.пр}}(k); Y_2(k)\, R\, Y_1(k)).$$

Для системы СПК других процессов $\vec{Y}_{\text{др.пр}}(k)$ задача решается аналогично:

$$Y_{\text{др.пр}}(k) = Y_{\text{др.пр}}[Y_1^*(k), Y_2(k)] \cup Y_{\text{др.пр}}[Y_1(k), Y_2^*\{Y_1(k)\}]; \quad (8)$$
$$\text{при условии } \forall\{(Y_1^{(}k), Y_2(k)) \in Y_{\text{др.пр}}(k)\};$$
$$\exists(Y_2(k) : Y_2(k) \in Y_{\text{др.пр}}(k); Y_2(k)\, R\, Y_1(k)).$$

Рассмотрим содержание процесса параметрической декомпозиции. Параметрическая декомпозиция ГСПК позволяет декомпозировать ее на пару взаимозависимых ЛСПК посредством временного установления (фиксации) значений некоторых ПК процессов по отношению друг к другу ($Y_1^*\{Y_2(k)\}$) и ($Y_2^*\{Y_1(k)\}$). Эти параметры обеспечивают взаимосвязь между ЛСПК. В одной ЛСПК параметр $Y_1^*(k)$ считается фиксированным, в то время как в другой он может изменяться, а второй параметр фиксируется в своем оптимальном значении.

На основе обобщенной записи процесса параметрической декомпозиции (7) и (8), используя рассмотренный в работе [9] частный случай применения градиентных методов, получаем алгоритм параметрической декомпозиции ГСПК БИ, представленный на рис. 2.

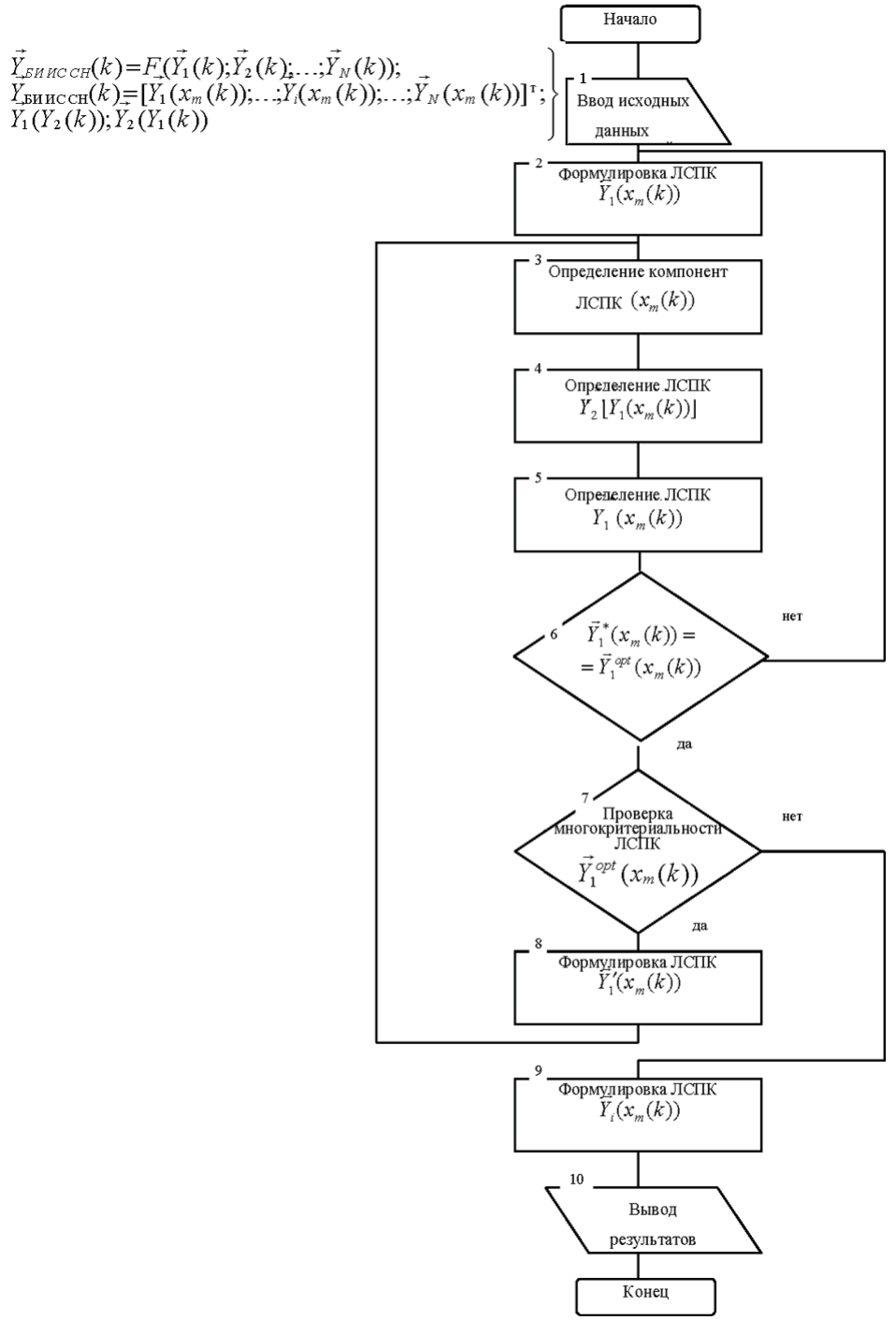

Рис. 2. Алгоритм параметрической декомпозиции ГСПК БИ ИС СН на ЛСПК

На первом шаге реализации процесса декомпозиции (блок *2* алгоритма) формулируется предполагаемое значение ЛСПК $Y_1(x_m(k))$, наиболее полно характеризующее ОЗФ СОБИ ИС СН.

В блоке *3* алгоритма определяются значения компонентов ПК — $x_m(k)$, входящих в выбранную ЛСПК $Y_1(x_m(k))$. В блоке *4* определяется $Y_2^*[Y_1(x_m(k))]$, т. е., используя полученное в блоке *3* решение для ПК $Y_1(x_m(k))$, проводят анализ ЛСПК $Y_2(x_m(k))$ в целях формулировки ее оптимального значения. Блок *5* алгоритма декомпозиции формирует оптимальный набор компонентов вектора ПК $Y_1^*(x_m(k))$. Блок *6* алгоритма предназначен для проверки, имеет ли ЛСПК $Y_1^*(x_m(k))$ оптимальное значение $Y_1^{opt}(x_m(k))$ на данном шаге. Если не формулируется новое значение $Y_1(x_m(k))$, которое является лучшим, — $Y_1^*(x_m(k))$, происходит возврат к блоку *2*.

Возврат к блоку *2* алгоритма происходит в целях формулирования нового значения $Y_1(x_m(k))$, когда ЛСПК $Y_1(k)$ и $Y_2(k)$ содержат более одного элемента (параметра), т.е. могут быть декомпозированы неоднозначно.

Блоки *7–9* алгоритма декомпозиции отвечают за реализацию третьего этапа декомпозиции.

Этап 3. Формулируется иерархия ЛСПК, поскольку получаемые в блоке *6* системы ПК взаимозависимы. Для формулировки иерархии СПК БИ ИС СН необходимо двухстороннюю зависимость между отдельными ЛСПК преобразовать в одностороннюю. Для этого система $Y_1(x_m(k))$ должна содержать информацию, совместимую с $Y_2(x_m(k))$, и формулироваться независимо от $Y_2(x_m(k))$, но с учетом ограничений $Y_1(x_m(k)) = Y_1^*(x_m(k))$.

Отсюда следует, что $Y_1(k)$ имеет приоритет перед $Y_2(k)$ и множество ЛСПК составляет иерархию. Иными словами, для получения иерархии СПК БИ ИС СН необходимо, чтобы данные системы не были тождественными. Эту задачу предлагается решить путем раздельных эволюций исходной ЛСПК БИ ИС СН.

Обоснованность данного подхода обусловлена взаимоподчиненным и взаимозависимым характером процессов реализуемых СОБИ ИС СН. Поэтому в результате эволюции $Y_{\text{осн.пр}}(k)$ и $Y_{\text{др.пр}}(k)$ можно сформулировать СПК безопасности обслуживания пользователей, управления, выявления и прогнозирования внутренних и внешних угроз БИ ИС СН.

В общем виде последовательность этапов декомпозиции ГСПК в интересах обеспечения БИ ИС СН представлена на рис. 3.

Таким образом, на основе предложенного алгоритма поэтапной декомпозиции может быть разработана оптимальная структура СПК БИ

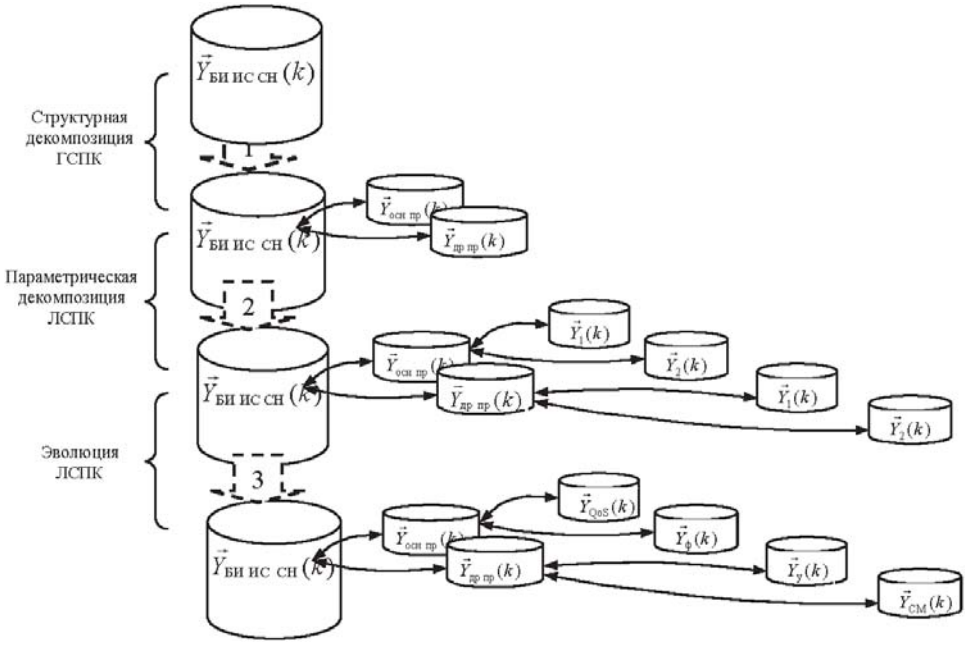

Рис. 3. Последовательность этапов декомпозиции ГСПК БИ ИС СН

ИС СН, включающая ГСПК безопасного обслуживания пользователей, ЛСПК функционирования, управления и сетевого мониторинга показателей БИ ИС СН.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом РФ 9 сентября 2000 г.
2. Цыгичко В. Н., Смолян Г. Л., Черешкин Д. С. Информационное оружие как геополитический фактор и инструмент силовой политики. – М.: ИСА АН РФ, 1997.
3. Wilson I. P. Foundations of hierarchical control // Int. J. Control, 1979. Vol. 29. – № 6. – P. 899–933.
4. Wilson I. P. Tree applications of decomposition method for designing hierarchical control system // Int. J. Control, 1979. Vol. 29. – № 6. – P. 935–947.
5. Жадан В. Г. Метод параметризации целевых функций в условиях многокритериальной оценки эффективности // ЖВМиМФ. – 1986. – Т. 26. – № 2. – С. 177–189.
6. Цицишвили Г. Ш. Декомпозиционные методы в задачах устойчивости и эффективности сложных систем. – ДВО АН СССР, 1989. – 116 с.
7. Pearson J. D. Takahara Y. Optimization method for large-scale system // Int. J. Control, 1975. Vol 26. – № 4. – P. 107–151.
8. Lefkowitz I., Schoffler J. D. Decomposition method for large-scale system // Comp. & Elect. Eng., 1973. – № 1. – P. 55–71.
9. Санин Ю. В. Использование математических методов теории декомпозиции при разработке системы показателей качества автоматизированных сетей спутниковой связи / Тез. докл. V ВНТК СПВВИУС. Ч. 1. – СПб.: СПВВИУС, 1993. – С. 19–22.

11. Терентьев В. М., Санин Ю. В. Использование методов декомпозиции при анализе эффективности сетей спутниковой связи / Сб. докл. ВНТК КВВИДКУС. – Киев: КВВИДКУС, 1991. – С. 25–26.

Статья поступила в редакцию 22.06.2007

Дмитрий Михайлович Ненадович родился в 1961 г., окончил Ленинградское высшее военное инженерное училище связи им. Ленсовета, Военную академию связи и Российскую академию государственной службы при Президенте РФ. Канд. техн. наук, ведущий специалист ОАО "МТС". Автор более 40 научных работ в области систем управления инфокоммуникационными сетями и экспертизы телекоммуникационных проектов.

D.M. Nenadovich (b. 1961) graduated from the Leningrad Higher Military Engineering School for Communication n. a. Lensovet, Military Academy for Communication and Russian Academy of Government Service at RF President. Ph. D. (Eng.), leading expert of joint-stock company "OAO "MTS". Author of more than 40 publications in the field of systems of management of data and communication networks and expertise of telecommunication projects.

В издательстве МГТУ им. Н.Э. Баумана
в 2008 г. вышла в свет книга

Меньшаков Ю.К.

Теоретические основы технических разведок: Учеб. пособие / Под ред. Ю.Н. Лаврухина. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 536 с.

Рассмотрены вопросы, связанные с различными направлениями и разновидностями технической разведки. Определены задачи, объекты и организация технической разведки. Приведены основные направления и классификация технической разведки по видам, источникам информации и используемой аппаратуре. Подробно рассмотрены все возможные направления и разновидности разведки.

Содержание учебного пособия соответствует курсу лекций, который читается в МГТУ им. Н.Э. Баумана. им. Н.Э. Баумана.

Для студентов высших учебных заведений и аспирантов, обучающихся по специальностям в области информационной безопасности.

По вопросам приобретения обращаться по тел. 263-60-45;
e-mail: press@bmstu.ru