УДК 621.396

Д. М. Ненадович, Б. И. Шахтарин

МЕТОДЫ ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ В ЗАДАЧАХ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ

Рассмотрены возможные подходы к решению задач обеспечения безопасности инфокоммуникационных сетей, разворачиваемых в интересах обеспечения государственного управления, основанные на методах теории эффективности и реализующие методы декомпозиции глобальной системы показателей качества.

В условиях интеграции информационной сферы России в мировое информационное пространство особую актуальность приобретают вопросы обеспечения безопасности информационных сетей специального назначения (ИС СН).

Решение задач обеспечения безопасности информации (БИ) ИС СН часто возлагается на системы обнаружения вторжений, позволяющие, как правило, выполнять следующие функции: выявлять информационные атаки; блокировать сетевой трафик, нарушающий установленную политику безопасности ИС; мониторинг трафика, циркулирующего в ИС на различных уровнях эталонной модели взаимодействия открытых систем; оповещать администратора безопасности об обнаруженных атаках или событиях, нарушающих политику безопасности ИС.

Все это способствует решению более обобщенной задачи обеспечения безопасности информационного обслуживания пользователей ИС при минимальных потерях производительности системы.

При решении частных и общих задач обеспечения БИ ИС перед специалистами неизбежно возникают вопросы: что наблюдать, как оценивать, на основании каких данных формировать оптимальное управляющее воздействие на ИС?

Один из подходов к решению таких задач основан на методах теории эффективности [1–3] и связан с формированием глобальной системы показателей качества (ГСПК) обеспечения БИ ИС. Далее на основе реализации методов декомпозиции [4–7] ГСПК разделяется на локальные системы показателей качества (ЛСПК) обеспечения БИ, характеризующие отдельные стороны этого процесса.

Необходимо отметить, что решение задач обеспечения БИ ИС, равно как и решение задач синтеза оптимальных ЛСПК БИ ИС, происходит в условиях различного уровня неопределенности. Классификация уровней неопределенности приведена на рис. 1.

Рис. 1. Классификация уровней (условий) неопределенности решения задач обеспечения ИС

Основным источником неопределенности при решении задач обеспечения БИ служит нестационарность режимов функционирования ИС в условиях воздействия дестабилизирующих факторов, возникающих вследствие природных явлений, осмысленной деятельности антагонистической системы. Кроме того, источниками неопределенности могут являться нечетко сформулированные цели управления и отсутствие в системе обеспечения информационной безопасности (СОБИ) некоторых статистических данных о параметрах самой ИС. Все это приводит к необходимости использования неопределенной, например нечеткой (лингвистической), формы описания задач управления.

С учетом неопределенности цели функционирования СОБИ и текущих задач управления, в качестве характеристики, получаемой в процессе эволюции, можно использовать [8, 9] функцию принадлежности μ. В этом случае процесс эволюции ЛСПК $\vec{Y}_{\text{осн. пр}}(x_m(k))$ и $\vec{Y}_{\text{др. пр}}(x_m(k))$ на третьем этапе декомпозиции можно записать в виде

$$\vec{Y}_{\text{осн. пр}}(x_m(k)) = \vec{Y}'_{\text{осн. пр}}(x_m(k)) = \vec{Y}_{\text{ф}}(x_m(k)); \tag{1}$$

$$\vec{Y}_{\text{др. пр}}(x_m(k)) = \vec{Y}'_{\text{др. пр}}(x_m(k)) = \vec{Y}_{\text{у}}(x_m(k)) \tag{2}$$

при условии, что $\mu[\vec{Y}'_{\text{осн.пр (др. пр)}}(x_m(k))] = \max$, где $\vec{Y}'_{\text{осн.пр (др.пр)}}(x_m(k))$ — допустимая эволюция исходной ЛСПК $\vec{Y}_{\text{осн.пр (др.пр)}}(x_m(k))$; μ: $\vec{Y}'_{\text{осн.пр (др.пр)}}(x_m(k)) \to [0, 1]$ — функция принадлежности, характеризующая $\vec{Y}'_{\text{осн.пр (др.пр)}}(x_m(k))$ и связанная с каждым i-м ее элементом (ПК). Например, если $\mu[\vec{Y}'_{\text{осн.пр (др.пр)}}(x_m(k))] = 1$, то $\vec{Y}'_{\text{осн.пр (др.пр)}}(x_m(k))$ точно принадлежит ЛСПК $\vec{Y}_{\text{осн.пр (др.пр)}}(x_m(k))$.

Рассмотрим вопросы формирования ГСПК и ЛСПК процессов обеспечения БИ ИС более подробно.

Заслуживает внимания подход к использованию нечетких множеств для синтеза систем ПК БИ ИС в рамках задач многокритериального выбора, предложенный в работе [10]. В рассматриваемом случае такой подход заключается в выражении общей цели обеспечения БИ ИС в виде иерархии подцелей, на нижнем уровне которой находятся q частных целей, связываемых с q элементарными критериями, которые, в свою очередь, позволяют оценить объекты из заданного множества. Эта цель выражается сложной лингвистической категорией, базовым множеством для которой будет декартово произведение $X_1 \times \ldots \times \times X_q$ (где X_i — область, в которой выбираются ПК БИ). В этом случае для синтеза систем ПК БИ ИС осуществляется операция свертки над нечеткими множествами, объединяющими частные цели. Выделяются четыре класса операции свертки, а именно классы операции пересечения, объединения, осреднения и симметричного суммирования. В результате свертывания может получиться даже нечеткое число. Это произойдет в том случае, когда среди выбранных ПК БИ ИС одни будут более вероятны (заслуживать большего доверия), чем другие. Тогда получим нечеткое множество ПК БИ ИС, которое при использовании принципа обобщения обеспечит синтез нечеткой системы ПК БИ ИС, подлежащих наблюдению, оцениванию и прогнозированию (НОП) в рамках решения задач обеспечения БИ.

Используя методы теории нечетких множеств, рассмотрим алгоритм синтеза СПК в интересах обеспечения БИ ИС, являющийся органичным продолжением этапов алгоритма декомпозиции представленного.

В целях дальнейшей декомпозиции и снижения размерности ЛСПК ИС необходимо ввести нечеткое отношение объединения (оценка сверху) или пересечения (оценка снизу) между частными ПК (ЧПК) БИ ИС. Известно [8–10], что операции пересечения и объединения не дают какого-нибудь систематического эффекта увеличения или понижения нечеткости. Для пессимистической оценки предлагается использовать пересечение нечетких подмножеств ЧПК БИ ИС, сформированных экспертами на этапе формирования матрицы функций принадлежности, характеризующей количественное сравнение степеней принадлежности.

Результатом опроса экспертов является матрица

$$B^{(l)}(k) = \|b_{ij}^{(l)}(k)\| \tag{3}$$

размерности $n \times n$, где n — число точек u_i, в которых сравниваются значения функции принадлежности, фактически равные количеству

экспертов, принимающих участие в опросе, а l — вариант оперативной обстановки.

Элемент $b_{ij}^{(l)}(k)$ матрицы $B^{(l)}(k)$ является субъективной оценкой отношения $\mu_{\tilde{A}}(u_i)/\mu_{\tilde{A}}(u_j)$ и показывает, во сколько раз, по мнению экспертов, $\mu_{\tilde{A}}(u_i)$ больше $\mu_{\tilde{A}}(u_j)$. Величина $b_{ij}^{(l)}(k)$ назначается в соответствии с балльной шкалой, значения которой интерпретируются в соответствии со шкалой интенсивности.

Количество вопросов к экспертам составляет не n^2, а $(n^2-n)/2$, так как по определению $b_{ij}^{(l)}(k)=1$ и в целях согласования оценок экспертов устанавливается, что $b_{ij}^{(l)}(k)=1/b_{ij}^{(l)}(k)$. Значения функции принадлежности $\mu_{\tilde{A}}(u_1),\ldots,\mu_{\tilde{A}}(u_n)$ в точках $u_1,\ldots,u_n$ определяются на основе решения задачи о нахождении собственного вектора матрицы $B^{(l)}(k)$:

$$B^{(l)}(k)W^{\mathrm{T}}=\zeta_{\max}W, \tag{4}$$

где $\zeta_{\max}$ — максимальное собственное число матрицы $B^{(l)}(k)$; $W=(\omega_1,\ldots,\omega_n)$ — соответствующий собственный вектор; "т" — символ транспонирования.

Поскольку матрица $B^{(l)}(k)$ положительна по построению, решение этой задачи всегда существует и является единственным. Можно показать, что в этом случае

$$\mu_{\tilde{A}}(u_i)=\omega_i\Big/\sum_{i=1}^{n}\omega_i. \tag{5}$$

При этом значения функции принадлежности $\mu_{\tilde{A}}(u_i)$ оказываются измеренными по шкале отношений.

Пусть $E_1(k)=\{y_1(k),y_2(k),\ldots,y_m(k)\}$ — подмножество ЧПК БИ ИС, сформированное первым экспертом, где каждому ПК соответствует функция принадлежности $\mu(y_i(k))$, $i=1,\ldots,m$, а $y_i(k)$ — элемент подмножества $E_1(k)$ (ЧПК БИ ИС). Тогда нечеткое отношение $\tilde{R}(k)$ принимает следующий вид:

$$E_1^l(k)\bigcap E_2^l(k)\bigcap\ldots E_i^l(k)\bigcap\ldots \\ \ldots\bigcap E_n^l(k):\mu_y^l(y_1(k),y_2(k),\ldots,y_m(k))\in M, \tag{6}$$

где $E_i^l(k)$ — подмножество ЧПК БИ ИС; $i=1,2,\ldots,n$; n — количество экспертов, принимавших участие в опросе; l — вариант оперативной обстановки; $y_j(k)$ — ЧПК БИ ИС; $j=1,2,\ldots,m$; m — количество ЧПК ИС в подмножестве $E_i^l(k)$; $M=[0,1]$ — множество принадлежностей пересечения $E(k)\bigcap E(k)$. Результатом данного пересечения будет являться нечеткое бинарное подмножество, которое можно представить в виде матрицы и нечеткого графа Бержа [10].

Следующий этап — это выявление свойств нечеткого отношения, а именно свойств транзитивности, рефлексивности и асимметричности, а также определение отношения подобия. Если $\tilde{R}(k) \subset E(k)$ — отношение нечеткою предпорядка и если существует обычное подмножество $E_1(k) \subset E(k)$, такое, что $\forall y(k),\ x(k) \in E_1(k) : \mu_{\tilde{R}(k)}(y(k),\ x(k)) = \mu_{\tilde{R}(k)}(x(k),\ y(k))$, то элементы множества $E_i(k)$ находятся между собой в отношении подобия, которое называется подотношением подобия в предпорядке $\tilde{R}(k)$. Подотношение подобия максимально, если в расматриваемом отношении не существует другого отношения подобия, той же природы.

Предположим теперь, что отношение предпорядка таково, что каждый из элементов (ЧПК БИ ИС) подмножества универсального множества ЧПК принадлежит максимальному подотношению подобия и не принадлежит никакому другому. С точки зрения нечеткой математики это значит, что все максимальные подотношения подобия не пересекаются. В этом случае подмножества, на которых определены такие непересекающиеся максимальные подотношения подобия, называют классами подобия предпорядка или в рассматриваемом случае ЛСПК БИ ИС. Нечеткий предпорядок, разложенный на классы подобия, называют приводимым нечетким предпорядком [8–10].

Если полученное нечеткое отношение является предпорядком, то предлагается использовать следующий алгоритм синтеза СПК БИ ИС.

Рассмотрим булеву матрицу отношения $\tilde{R}(k)$ такую, что

$$\mu_{R(k)}(y(k), x(k)) = 1, \quad \text{если} \quad \mu_{\tilde{R}(k)}(y(k), x(k)) \geq \alpha; \tag{7}$$

$$\mu_{R(k)}(y(k), x(k)) = 0, \quad \text{если} \quad \mu_{\tilde{R}(k)}(y(k), x(k)) < \alpha \tag{8}$$

или

$$\mu_{\tilde{R}(k)}(y(k), x(k)) = \mu_{\tilde{R}(k)}(x(k), y(k)) = 0,$$

где α — уровень нечеткости, задаваемый экспертом (минимальное значение функции принадлежности ЧПК данной ЛСПК БИ ИС).

Поочередно в каждой строке матрицы выделим нули. Рассматривая элементы матрицы как булевы переменные, свяжем булевым знаком суммирования “+” индекс строки и индексы столбцов, в которых находятся нулевые элементы этой строки, и полученные суммы объединим знаком булева произведения “о”, причем, если и строке нет нулей, считаем, что сумма равна 1.

Используя правила упрощения булевых выражений, упростим получившееся произведение, приведя его к максимальной форме. Для каждого слагаемого в этой форме возьмем его дополнение. Таким образом, получим максимальные подотношения (ЧПК) БИ ИС, устанавливающие покрытия, называемые классами подобия. С физической

точки зрения классы подобия эквивалентны ЛСПК БИ ИС. Если нас интересуют ЧПК БИ ИС, общие для попарно не содержащихся друг в друге отношений ЛСПК, то их можно получить непосредственно, подсчитав пересечения полученных подмножеств ЧПК БИ ИС.

Классы подобия образуют нечеткое отношение порядка в том случае, если для построения последнего используется понятие сильнейшего пути от одного класса к другому [8–10].

В общем случае процедура построения нечеткого отношения порядка между ЧПК БИ ИС состоит в следующем:

1. В приводимом нечетком предпорядке находим классы подобия $G_i(k)$. Для этого рассмотрим упорядоченные пары $(y(k), x(k))$, для которых

$$\mu_{\tilde{R}(k)}(y(k), x(k)) = \mu_{\tilde{R}(k)}(x(k), y(k)). \tag{9}$$

Для этих упорядоченных пар строим максимальные подотношения подобия, используя приведенный алгоритм. Если все они не пересекаются, то получим классы подобия ЛСПК БИ ИС (рис. 2).

2. Для каждой упорядоченный пары ЛСПК ИС $(G_i(k), G_j(k))$, $i \neq j$, рассмотрим нечеткое подотношение $\tilde{R}_{ij}(k)$ между $G_i(k)$ и $G_j(k)$ (строки $G_i(k)$ и столбцы $G_j(k)$). Определим глобальную проекцию подотношения $\tilde{R}_{ij}(k)$ на основе математического аппарата проекции нечетких отношений следующим образом:

$$h(\tilde{R}_{ij}(k)) = \bigvee_y \bigvee_x \mu_{\tilde{R}_{ij}(k)}(y(k), x(k)), \quad y(k) \in G_1(k), \quad x(k) \in G_2(k). \tag{10}$$

3. Присвоим значение $h(\tilde{R}_{ij}(k))$ функции принадлежности пары $(G_1(k), G_2(k))$. В том случае, если отношение $\tilde{R}(k)$ является отношением порядка, для него можно определить порядковую функцию.

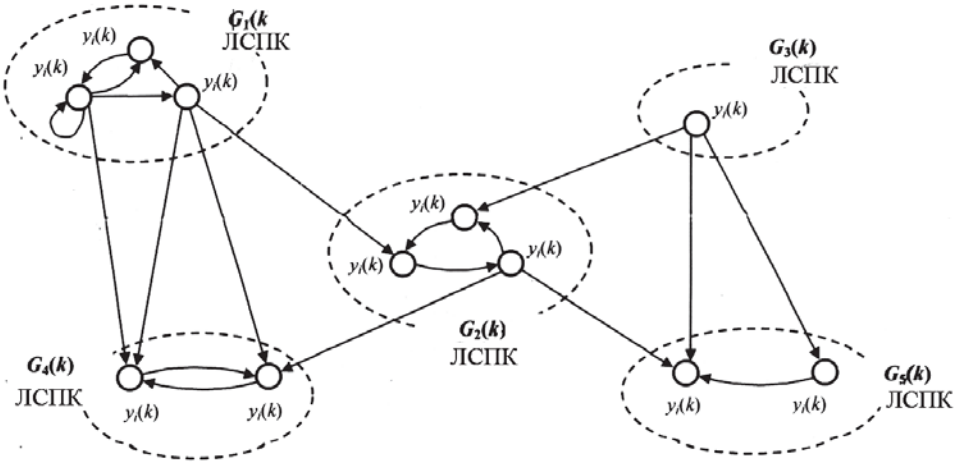

Рис. 2. Классы подобия ЛСПК БИ ИС на основе нечеткого отношения предпорядка

Функция $O(Y_i(k))$, определенная условием

$$Y_i(k) \in Q_r(k) \Rightarrow O(Y_i(k)) = r, \tag{11}$$

называется порядковой функцией графа без контуров.

Обычные подмножества $Q_r(k)$, $r = 0, 1, 2, \ldots, n$, образуют разбиение универсального множества и полностью строго упорядочены отношением

$$Q_r(k) \prec Q_{r'}(k) \Leftrightarrow r < r'. \tag{12}$$

Таким образом, можно разложить множество вершин графа (вершинами графа являются ЧПК БИ ИС без контуров) на обычные подмножества, т. е. ЛСПК, непересекающиеся и упорядоченные так, что если один из ЧПК БИ ИС принадлежит ЛСПК БИ ИС, имеющей номер r, то все ЧПК. следующие за данным IIK БИ ИС, должны располагаться в ЛСПК БИ ИС с номером, бóльшим, чем r. Обычные подмножества ЛСПК БИ ИС такого разложения называются уровнями (классами).

Алгоритм определения уровней нечеткого графа, т. е. определения подмножеств ПК БИ ИС, заключается в следующем. На первом шаге строится матрица Λ вида

$$[\Lambda(k)] = \begin{array}{c|cccccc} & y_1(k) & y_2(k) & \ldots & y_i(k) & \ldots & y_m(k) \\ \ldots\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \Lambda_0(k) & \lambda_{01}(k) & \lambda_{02}(k) & \ldots & \lambda_{0i}(k) & \ldots & \lambda_{0m}(k) \\ \Lambda_1(k) & \lambda_{11}(k) & \lambda_{12}(k) & \ldots & \lambda_{1i}(k) & \ldots & \lambda_{1m}(k) \\ \vdots & \ldots & \ldots & \ldots & \ldots & \ldots & \vdots \\ \Lambda_j(k) & \lambda_{j1}(k) & \lambda_{j2}(k) & \ldots & \lambda_{ji}(k) & \ldots & \lambda_{jm}(k) \\ \vdots & \ldots & \ldots & \ldots & \ldots & \ldots & \vdots \\ \Lambda_n(k) & \lambda_{n1}(k) & \lambda_{n2}(k) & \ldots & \lambda_{ni}(k) & \ldots & \lambda_{nm}(k) \end{array}. \tag{13}$$

В строке $\Lambda_0(k)$ подсчитываются суммы строк булевой матрицы, построенной в соответствии с условиями (8), (9), т.е. сумма элементов в соответствующих столбцах. Нули в строке $\Lambda_0(k)$ определяют ЧПК, которым не предшествует ни один другой ЧПК. Такие ЧПК БИ ИС, у которых $\lambda_{0i}(k) = 0$, составляют уровень $Q_0(k)$ или ЛСПК № 1. Исключив из сумм строки $\Lambda_0(k)$ значения, записанные в строках с нулевыми значениями, получим строку $\Lambda_1(k)$, в которой нули из $\Lambda_0(k)$ заменены знаком $\times$ (крестом). Появившиеся в строке $\Lambda_1(k)$ нули определяют ЧПК, которые не предшествует ни один другой ЧПК, кроме удаленных в $\Lambda_0(k)$. Эти ЧПК БИ ИС образуют уровень $Q_1(k)$ или ЛСПК № 2. Теперь из строки $\Lambda_1(k)$ вычтем суммы нулевых строк после замены всех ранее появившихся нулей крестами; новые нули, появившиеся в строке $\Lambda_2(k)$, определяют ЧПК БИ ИС, для которых не существует

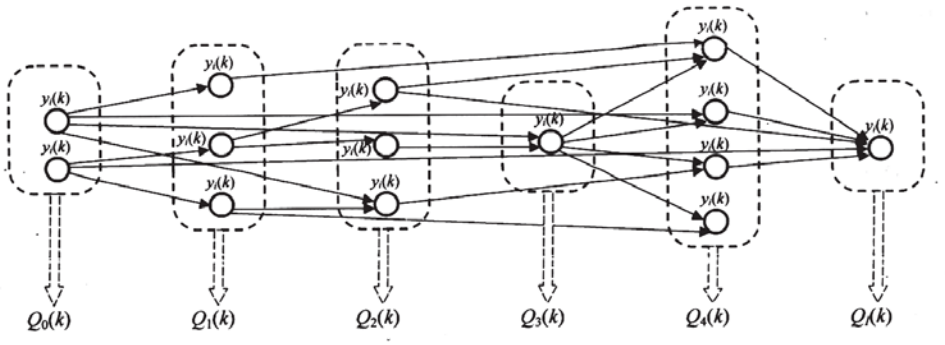

Рис. 3. Граф уровней, определяющий нечеткие подмножества ПК БИ ИС

других предшествующих ЧПК, кроме удаленных на предыдущих шагах, ЧПК БИ ИС с нулевыми значениями в строке $\Lambda_2(k)$ составляют уровень $Q_2(k)$ или ЛСПК № 3. Данный процесс продолжается до тех пор, пока не будет закончен перебор всех точек. После этого остается только построить обычный граф, в котором ЧПК БИ ИС расположены на соответствующих им уровнях (рис. 3).

Чтобы получить порядковую функцию при обратном упорядочении уровней, когда выделяются наибольшие элементы (более предпочтительные ПК БИ ИС) данного порядка, можно применить ту же самую процедуру к транспонированной булевой матрице. Построение порядковой функции позволяет автоматически получать диаграмму Хассе [8–10], соответствующую отношению порядка, и определять уровни этой диаграммы.

Каждый класс подобия определяет состав ЛСПК БИ ИС, где степень принадлежности каждого ЧПК данной ЛСПК характеризуется значением функции принадлежности.

Таким образом, опираясь на мнения экспертов, формализующих неоднозначные (нечеткие) требования к ПК БИ ИС, подлежащим НОП, с учетом изменяющихся задач управления, алгоритм позволяет получить ряд ЛСПК, характеризующих состояние (качество) БИ ИС. На выходе алгоритма получается иерархическая (уровневая) СПК ИС $\tilde{\vec{Y}}_{\text{ИС}}(k)$, подлежащих НОП, в рамках обеспечения БИ ИС в конкретной управленческой ситуации.

СПИСОК ЛИТЕРАТУРЫ

1. Петухов Г. Б. Теоретические основы и методы исследования эффективности операционных целенаправленных процессов. – М.: МО СССР, 1979. – 176 с.
2. Терентьев В. М., Паращук И. Б. Теоретические основы управления сетями многоканальной радиосвязи. – С.-Пб.: ВАС, 1995. – 195 с.
3. Терентьев В. М., Санин Ю. В. Анализ эффективности функционирования автоматизированных сетей многоканальной радиосвязи. – С.-Пб.: ВАС, 1992. – 80 с.

4. Ц и ц и а ш в и л и Г. Ш. Декомпозиционные методы в задачах устойчивости и эффективности сложных систем. – ДВО АН СССР, 1989. – 116 с.
5. P e a r s o n J. D., T a k a h a r a Y. Optimization method for Large-scale System. “Int. J. Control”, 1975, vol. 26. № 4. P. 107–151.
6. L e f k o w i t z I., S c h o f f l e r J. D. Decomposition method for Large-scale System. “Сотр. & Elect. Eng.”, 1973, № 1. P. 55–71.
7. W i l s o n I. P. Foundations of hierarchical control. “Int. J. Control”. 1979. Vol. 29. № 6. P. 899–933.
8. Н е ч е т к и е множества и теория возможностей. Последние достижения: Пер. с англ. / Под ред. Р.Р. Ягера. – М.: Радио и связь. 1986. – 408 с.
9. П а р а щ у к И. Б., Б о б р и к И. П. Нечеткие множества в задачах анализа сетей связи. – С.-Пб.: ВАС, 2001. – 80 с.
10. Д ю б у а Д., П р а д А. Теория возможностей. Приложения к представлению знаний в информатике: Пер. с фр. – М.: Радио и связь, 1990. – 288 с.

Статья поступила в редакцию 23.11.2005

Борис Ильич Шахтарин родился в 1933 г., окончил в 1958 г. Ленинградскую Военно-воздушную инженерную академию им. А.Ф. Можайского и в 1968 г. ЛГУ. Д-р техн. наук, профессор МГТУ им. Н.Э. Баумана. Лауреат Государственной премии СССР, заслуженный деятель науки и техники РФ. Автор более 200 научных работ, в том числе 4 книг, в области анализа и синтеза систем обработки сигналов.

B.I. Shakhtarin (b. 1933) graduated from the Leningrad Air Force Engineering Academy n.a. A. F. Mozhaysky in 1958, and from Leningrad State University in 1968. D. Sc. (Eng.), professor of the Bauman Moscow State Technical University. USSR State Prize winner, RF Honoured Worker of science and technology. Author of more than 200 publications, among them 4 books, in the field of analysis and synthesis of signal processing systems.