

ИНФОРМАЦИОННО- УПРАВЛЯЮЩИЕ СИСТЕМЫ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

3(28)/2007

3(28)/2007

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

РЕЦЕНЗИРУЕМОЕ ИЗДАНИЕ

Учредитель

ОАО «Издательство «Политехника»»

Главный редактор

М. Б. Сергеев,
доктор технических наук, профессор

Зам. главного редактора

Г. Ф. Мощенко

Редакционный совет:

Председатель А. А. Оводенко,
доктор технических наук, профессор
В. Н. Васильев,
доктор технических наук, профессор
В. Н. Козлов,
доктор технических наук, профессор
Ю. Ф. Подоплекин,
доктор технических наук, профессор
Д. В. Пузанков,
доктор технических наук, профессор
В. В. Симаков,
доктор технических наук, профессор
А. Л. Фрадков,
доктор технических наук, профессор
Л. И. Чубраева,
доктор технических наук, профессор, чл.-корр. РАН
Р. М. Юсупов,
доктор технических наук, профессор, чл.-корр. РАН

Редакционная коллегия:

В. Г. Анисимов,
доктор технических наук, профессор
Е. А. Крук,
доктор технических наук, профессор
В. Ф. Мелехин,
доктор технических наук, профессор
А. В. Смирнов,
доктор технических наук, профессор
В. И. Хименко,
доктор технических наук, профессор
А. А. Шальто,
доктор технических наук, профессор
А. П. Шепета,
доктор технических наук, профессор
З. М. Юлдашев,
доктор технических наук, профессор

Редактор: А. Г. Ларионова

Корректор: Т. В. Звертановская

Дизайн: М. Л. Черненко, А. Н. Колешко

Компьютерная верстка: Т. М. Каргапольцева

Ответственный секретарь: О. В. Муравцова

Адрес редакции: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Тел.: (812) 494-70-36
Факс: (812) 494-70-18
E-mail: 80x@mail.ru; ius@aanet.ru
Сайт: www.i-us.ru

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций. Свидетельство о регистрации ПИ № 77-12412 от 19 апреля 2002 г.

Журнал распространяется по подписке. Подписку можно оформить через редакцию, а также в любом отделении связи по каталогам: «Пресса России» – № 42476; «Роспечать» («Газеты и журналы») – № 15385

© Коллектив авторов, 2007

ОБРАБОТКА ИНФОРМАЦИИ И УПРАВЛЕНИЕ

Тихонов Э. П. Аналитико-имитационное исследование и оптимизация алгоритмов аналого-цифрового преобразования в условиях воздействия помех (Часть 2) 2

МОДЕЛИРОВАНИЕ СИСТЕМ И ПРОЦЕССОВ

Агиевич С. Н., Беспалов В. Л. Использование функций сплайн–Вилленкина–Крестенсона для построения аналитических моделей радиосигналов 15

ПРОГРАММНЫЕ И АППАРАТНЫЕ СРЕДСТВА

Лебедев И. С. Способ формализации связей в конструкциях текста при создании естественно-языковых интерфейсов 23

Вельдер С. Э., Шальто А. А. О верификации простых автоматных программ на основе метода Model Checking 27

ЗАЩИТА ИНФОРМАЦИИ

Молдованин Т. В. Решение задачи выбора оптимального варианта комплексной защиты информации с помощью метода экспертного оценивания 39

КОДИРОВАНИЕ И ПЕРЕДАЧА ИНФОРМАЦИИ

Кацов И. В. Пространственное мультиплексирование с субсимвольным временным сдвигом между передающими антеннами 45

ИНФОРМАЦИОННЫЕ КАНАЛЫ И СРЕДЫ

Зикратов И. А., Зикратова Т. В. К вопросу об оптимизации зоны покрытия систем сотовой связи на загородных участках местности 52

КРАТКИЕ СООБЩЕНИЯ

Рыжиков Ю. И. Расчет систем со случайным выбором на обслуживание 56

СВЕДЕНИЯ ОБ АВТОРАХ

60

АННОТАЦИИ

62

ЛР № 010292 от 18.08.98.

Сдано в набор 05.05.07. Подписано в печать 21.06.07. Формат 60×84/8. Бумага офсетная. Гарнитура SchoolBookC. Печать офсетная. Усл. печ. л. 8,0. Уч.-изд. л. 9,0. Тираж 1000 экз. Заказ 326.

Оригинал-макет изготовлен в редакционно-издательском центре ГУАП. 190000, Санкт-Петербург, Б. Морская ул., 67.

Отпечатано с готовых диапозитивов в редакционно-издательском центре ГУАП. 190000, Санкт-Петербург, Б. Морская ул., 67.

УДК 681.314+681.51.011

АНАЛИТИКО-ИМИТАЦИОННОЕ ИССЛЕДОВАНИЕ И ОПТИМИЗАЦИЯ АЛГОРИТМОВ АНАЛОГО-ЦИФРОВОГО ПРЕОБРАЗОВАНИЯ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ПОМЕХ (Часть 2)

Э. П. Тихонов,

канд. техн. наук, доцент

Санкт-Петербургский государственный электротехнический университет

На основании предложенных автором информационных алгоритмов проведен аналитико-имитационный анализ потенциальных возможностей адекватных алгоритмов аналого-цифрового преобразования поразрядного уравнивания, в том числе, при воздействии аддитивной помехи. На основе критерия помехоустойчивости разработаны рекомендации по оптимальному выбору параметров адекватных алгоритмов аналого-цифрового преобразования в зависимости от уровня аддитивной помехи.

On the basis of the information algorithms proposed by the author, certain methods of analog-digital transformation are investigated in the presence of noise. The results of research allow us to receive recommendations as to an optimum choice of parameters of adequate algorithms of analog-digital transformation depending on noise.

(Продолжение. Начало см. в № 2, 2007)

Проанализируем влияние на погрешность аналого-цифрового преобразования посредством исследуемых алгоритмов аддитивной помехи ξ , неизбежно присутствующей в любой электронной схеме. Источниками аддитивной помехи являются электронные компоненты и схемы, из которых состоит АЦП. Поэтому в дальнейшем эту помеху по аналогии с инструментальной погрешностью будем называть, в отличие от погрешности усечения (ее свойство позволяет рассматривать эту погрешность как помеху усечения), инструментальной помехой. Анализ реально-информационных алгоритмов существенно облегчает решение задачи исследования влияния инструментальной помехи на погрешности преобразования. Действительно, как следует из отображений (10), (11), их вид не меняется при отличии от нуля инструментальной помехи. Инструментальная помеха и ее суперпозиция вида $\eta_n = \gamma + \xi_n$ обладают следующими свойствами, влияющими на отображения (10) и (11):

- закон распределения вероятностей инструментальной помехи отличен от равномерного закона распределения;

- для любого разряда выполняется следующее очевидное условие для дисперсии суммарной помехи и помехи усечения: $\sigma_\eta^2 > \sigma_\gamma^2$ или $\sigma_\eta^2 > 0,083$;

- инструментальные помехи могут возникать как «внутри» схемы АЦП и таким образом воздействовать на входной сигнал, так и по различным причинам «наводиться» на его входных электрических цепях;

- адекватной плотностью распределения вероятности инструментальной помехи, как правило, является гауссова плотность с нулевым математическим ожиданием.

Указанные свойства, прежде всего, приводят к тому, что для функции распределения вероятности суммарной помехи, даже для случая, когда дисперсия инструментальной помехи σ_ξ^2 значительно меньше дисперсии погрешности усечения, т. е. когда выполняется условие $\sigma_\gamma^2 \gg \sigma_\xi^2$, неравенства в формуле (16) строго не выполняются. Следовательно, изменяются условия для установления тождества между уравнивающей величиной и входным сигналом, т. е. между состояниями АЦП и структурой входного сигнала, поэтому меняются и условия сходимости уравнивающей величины к значению входного сигнала. Для того чтобы выяснить степень нарушения сходимости

соответствующего алгоритма, перейдем от индикаторного идеально-информационного алгоритма, заданного в виде (13), к его реальному представлению при $\Delta t = 1$ и $\xi < \Delta q$:

$$a_n = \begin{cases} 1, & \text{если } \sum_{i=1}^{n-1} (a_{xi} - a_i) 2^{N-i} + \\ & + \sum_{i=n}^N a_{xi} 2^{N-i} - 2^{N-n} + \gamma + \xi_H \geq 0, \\ 0, & \text{если } \sum_{i=1}^{n-1} (a_{xi} - a_i) 2^{N-i} + \\ & + \sum_{i=n}^N a_{xi} 2^{N-i} - 2^{N-n} + \gamma + \xi_H < 0, \end{cases} \quad (18)$$

или к его модификации

$$a_n = \begin{cases} 1, & \text{если } \left[\begin{array}{l} \sum_{i=1}^{n-1} (a_{xi} - a_i) 2^{n-i} + \\ + \sum_{i=n}^N a_{xi} 2^{n-i} - 1 + (\gamma + \xi_H) 2^{-N+n} \end{array} \right] \geq 0, \\ 0, & \text{если } \left[\begin{array}{l} \sum_{i=1}^{n-1} (a_{xi} - a_i) 2^{n-i} + \\ + \sum_{i=n}^N a_{xi} 2^{n-i} - 1 + (\gamma + \xi_H) 2^{-N+n} \end{array} \right] < 0. \end{cases}$$

Проанализируем первый вариант (18) представления индикаторного алгоритма при условии, что $\xi < \Delta q$ и $\eta_H = \gamma + \xi_H$. Для этого положим вначале $n = 1$, тогда

$$a_1 = \begin{cases} 1, & \text{если } \sum_{i=1}^N a_{xi} 2^{N-i} - 2^{N-1} + \eta_H \geq 0, \\ 0, & \text{если } \sum_{i=1}^N a_{xi} 2^{N-i} - 2^{N-1} + \eta_H < 0. \end{cases}$$

Рассмотрим трансформацию плотности распределения вероятности суммарной помехи $\eta_H = \gamma_H + \xi_H$. Поскольку первое слагаемое распределено по равномерному закону с математическим ожиданием $\Delta q/2$, а второе слагаемое — по гауссовому закону с нулевым математическим ожиданием, то их композиция с учетом аналитических выводов [1] по составлению композиции равномерной и гауссовой плотностей вероятностей имеет довольно сложный вид:

$$w(\eta) = \frac{1}{\Delta q} \left[\Phi\left(\frac{\eta}{\sigma}\right) - \Phi\left(\frac{\eta - \Delta q}{\sigma}\right) \right],$$

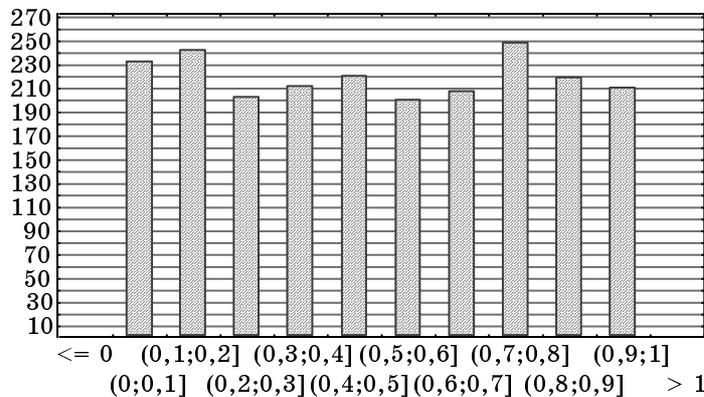
$$\text{где } \Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-\frac{t^2}{2}} dt,$$

где σ — среднеквадратическая ошибка (СКО) инструментальной составляющей помехи.

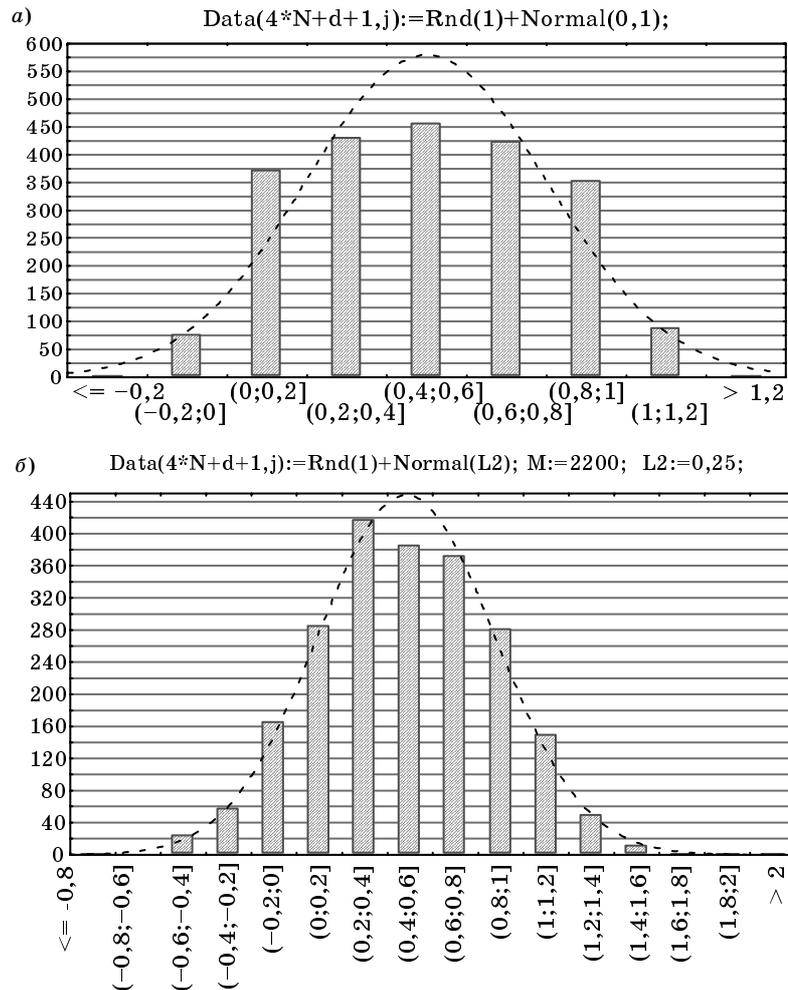
Гистограммы (рис. 7, 8) иллюстрируют трансформацию композиционной плотности распределения вероятностей при различных значениях СКО инструментальной помехи по сравнению с гауссовой плотностью распределения вероятностей для объема выборки $M = 2200$. Из рис. 8, а, в частности, следует, что уже для $\sigma = 0,1\Delta q$ суммарная помеха η может принимать отрицательные значения с вероятностью

$$P(\eta < 0) = \int_{-\Delta q}^0 w(\eta) d\eta = \frac{1}{\Delta q} \int_{-\Delta q}^0 \left[\Phi\left(\frac{\eta}{\sigma}\right) - \Phi\left(\frac{\eta - \Delta q}{\sigma}\right) \right] d\eta,$$

```
Data(i+2,j):=Data(i+1,j)+(2^(N-i))*0.5*(1+Sign(((Data(1,j)-
-Data(i+1,j)) *(2^(i-N))))-1)); N:=10; M:=2200; L1:=1023;Data(1,j):=Rnd(L1);
Data(N+2+d,j):=Data(1,j)-Data(N+2,j);
```



■ Рис. 7. Гистограмма погрешности усечения аналого-цифрового преобразования в соответствии с индикаторным 10-разрядным алгоритмом без помех, построенная для сигнала, принимающего значение на интервале (1023, 1024)



■ Рис. 8. Гистограмма суперпозиции плотности распределения вероятностей нормированной гауссовой помехи с СКЮ, равной 0,1 (а) и 0,25 (б), и нулевым математическим ожиданием, с равномерной плотностью распределения вероятностей, равной 1

и поэтому условия сходимости реально-информационного и идеально-информационного алгоритмов существенно отличаются.

Для того чтобы выяснить характер и степень нарушения сходимости реально-информационного алгоритма по сравнению с идеально-информационным алгоритмом, перейдем от отображения (15) к следующему его представлению:

$$V^*(n) = V^*(n-1) - F_{\eta(n)}[V^*(n-1)]. \quad (19)$$

В отличие от (15) в усредненном по суммарной помехе $\eta_n(n) = \gamma(n) + \xi_n(n)$, нормированной к текущему кванту $\Delta q 2^{N-n}$, эквивалентном представлении алгоритма (19) соответствующая функция распределения $F_{\eta(n)}[V^*(n-1)]$, даже при равномерно распределенном входном сигнале, отлична от равномерного закона. При крайних значениях аргумента $V^*(n-1)$, равного нулю или единице, функция распределения $F_{\eta(n)}[V^*(n-1)]$ уже отличается соответственно от нуля или единицы (см. рис. 6). Поэтому, с учетом того, что помеха $\xi_n(n) < 1$, имеем

$$a_n = \begin{cases} 1 \text{ с вероятностью } F_{\eta(n)}(1), \\ \text{если } \sum_{i=1}^{n-1} (a_{xi} - a_i) 2^{n-i} + \sum_{i=n}^N a_{xi} 2^{n-i} = 1; \\ 1 \text{ с вероятностью } 1, \\ \text{если } \sum_{i=1}^{n-1} (a_{xi} - a_i) 2^{n-i} + \sum_{i=n}^N a_{xi} 2^{n-i} > 1; \\ 0 \text{ с вероятностью } F_{\eta(n)}(0), \\ \text{если } \sum_{i=1}^{n-1} (a_{xi} - a_i) 2^{n-i} + \sum_{i=n}^N a_{xi} 2^{n-i} = 0; \\ 0 \text{ с вероятностью } 1, \\ \text{если } \sum_{i=1}^{n-1} (a_{xi} - a_i) 2^{n-i} + \sum_{i=n}^N a_{xi} 2^{n-i} < 0. \end{cases} \quad (20)$$

Из формулы (20) [ср. с (17)] можно определить динамику изменения искомого коэффициента a_n в зависимости от изменения номера шага итерации

$n = 1, 2, \dots, N$. В частности, для $n = 1$ получаем четыре возможных варианта для определения значения коэффициента a_1 в зависимости от разности между значением входного сигнала и уравнивающей величиной. Если разность между входным сигналом и уравнивающей величиной соизмерима с квантом, то с указанными в формуле (20) вероятностями возможен сбой.

При рассмотрении случая, когда $n = 2$, при условии, что на первом шаге итерации отсутствовал сбой, получаем четыре возможных варианта для определения значения коэффициента a_2 в зависимости от разности между значением входного сигнала и уравнивающей величиной, так как придется анализировать уже 4 комбинации: 11, 10, 01, 00, и т. д. Из проведенного анализа следует, что под воздействием инструментальной помехи при определении текущего значения в каждом анализируемом разряде возникают так называемые ошибки первого и второго рода, а именно:

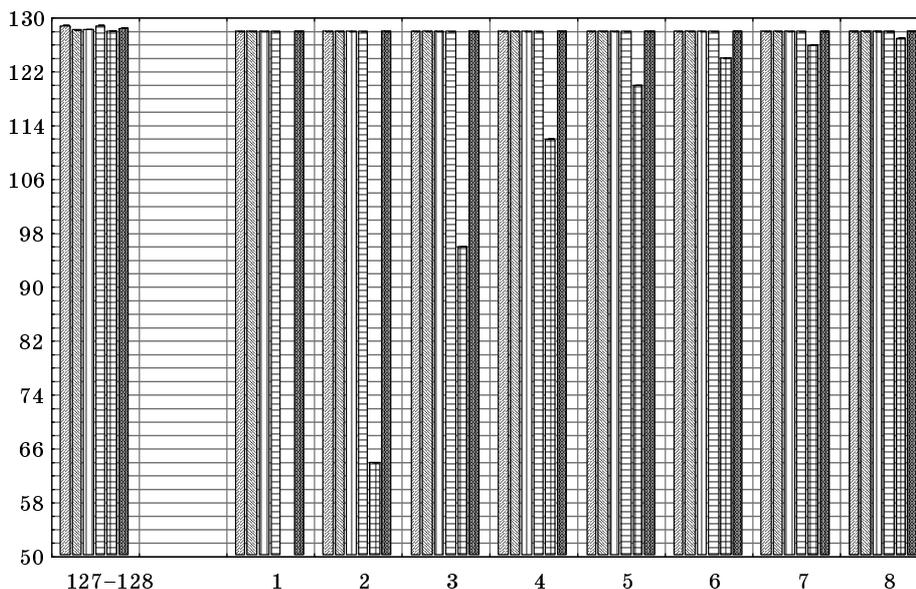
1) у входного нормированного к кванту сигнала анализируемый разряд равен нулю, тем не менее, с вероятностью, отличной от нуля, для уравнивающей физической величины устанавливается для соответствующего разряда значение, равное единице;

2) у входного нормированного к кванту сигнала анализируемый разряд равен единице, однако с вероятностью, отличной от нуля, для уравнивающей физической величины устанавливается для соответствующего разряда значение, равное нулю.

Таким образом, для реально-информационного алгоритма нарушаются условия достижения равновесия, присущие для идеально-информационного алгоритма, даже при одинаковом структурировании АЦП и входного сигнала. Степень или вероятность этого нарушения определяется уровнем инструментальной помехи, в результате чего и образуется инструментальная составляющая погрешности преобразования. При этом указанные вероятности ошибок первого и второго родов для принятого уровня аддитивной помехи ξ менее кванта не равны между собой и отличны от нуля только при условии выпадения для входного сигнала минимального и максимального значений наборов $\langle a_{x2}, \dots, a_{xN} \rangle$, т. е. с довольно малой вероятностью (см. рис. 8). Действительно, достаточно одного младшего разряда, отличного от нуля, в минимальном наборе $\langle a_{x2}, \dots, a_{xN} \rangle$ или одного младшего разряда, отличного от единицы, в соответствующем максимальном наборе, чтобы вероятности ошибок были фактически равными нулю. А это значит, что возникновение ошибок первого и второго родов возможно для первого такта преобразования из всего множества квантованных значений входного сигнала только для двух значений $\langle 1, 0, \dots, 0 \rangle$ и $\langle 0, 1, 1, \dots, 1 \rangle$, вероятность осуществления которых для равномерного закона распределения входного сигнала равна $2^{-(N-1)}$.

Проанализированный случай иллюстрируется рис. 9, где процесс уравнивания постоянного сигнала, изменяющегося случайно с равномерной плотностью распределения вероятностей в преде-

$N:=8; M:=2200; L1:=1; L2:=0.05*(N-8+1); L:=0.0001+(2^{(N-1)});$
 $Data(i+2,j):=Data(i+1,j)+(2^{(N-i)})*0.5*(1+Sign(((Data(1,j)-$
 $-Data(i+1,j))*(2^{(i-N))}-1)+((Normal(L2))*(2^{(i-N)))))); Data(1,j):=L+Rnd(L1);$



■ Рис. 9. Иллюстрация процесса уравнивания постоянного сигнала при воздействии помехи

лах 127–128 посредством 8-разрядного индикаторного алгоритма в присутствии инструментальной помехи с СКО, равной 0,05 от величины кванта, представлен в виде столбчатой диаграммы. Выборка, состоящая из 6 преобразований, включает преобразование, в котором произошел сбой из-за воздействия помехи с указанной величиной СКО. Этот сбой, как это было логически показано, компенсируется на последующих тактах уравнивания. На графике хорошо различима случайная вариация входного сигнала в пределах 127–128, тогда как результат преобразования остается неизменным, кроме случая, когда произошел сбой. Для лучшей различимости случайной вариации входного сигнала в пределах кванта на рисунке диаграмма начинается не с нуля, а со значения, равного 50. Для всех остальных значений входного сигнала указанные ошибки будут отсутствовать. Однако на втором такте итерации, если входной сигнал отличен более чем на один квант от $E_0/2$, подобные ошибки могут возникнуть уже для четырех случаев, т. е. для кодов $\langle 1, 1, 0, \dots, 0 \rangle$, $\langle 1, 0, 1, \dots, 1 \rangle$, $\langle 0, 1, 0, \dots, 0 \rangle$, $\langle 0, 0, 1, \dots, 1 \rangle$, вероятность осуществления которых для случая равномерного закона распределения входного сигнала равна $2^{-(N-2)}$, и т. д. На последнем такте преобразования ошибки в младшем разряде с соответствующей вероятностью могут возникнуть для любого кода, принадлежащего множеству кодов 2^N .

В соответствии с формальной логикой анализа напрашивается вывод о возможности возникновения соответствующих ошибок в течение одного цикла преобразования на каждом такте преобразования. Однако реально из-за указанного выше ограничения на величину аддитивной помехи этого не происходит. Действительно, если произошел сбой, например, в старшем разряде, а этот сбой может произойти только для двух указанных выше значений кодов, то на последующих тактах, вплоть до $(N - 1)$ -го такта преобразования, кроме младшего разряда, подобные сбои, как это подтверждается анализом выражения (20) и рис. 9, исключаются. Это свя-

зано с коррекцией на последующих тактах преобразования ошибки, возникшей на предыдущем такте преобразования. При этом разность между уравнивающей величиной и входным сигналом на этих тактах преобразования превышает величину кванта Δq и тем самым анализируемую величину суммарной помехи η . Аналогичный процесс происходит на втором и последующих тактах преобразования.

Пусть $n = k$. Предположим, что на предыдущих $k - 1$ тактах преобразования установлено, что $a_1 = a_{x1}, \dots, a_{k-1} = a_{xk-1}$, тогда для $a_{xk} = 1$ минимальное, нормированное к кванту Δq значение входного сигнала равно 2^{N-k} , а при $a_{xk} = 0$ максимальное, нормированное к кванту Δq значение входного сигнала равно

$$\sum_{i=k+1}^N 2^{N-i} = (2^{N-k} - 1). \text{ Поэтому для } k = 1, 2, \dots, N - 1 \text{ получаем}$$

$$a_k = \begin{cases} 1 \text{ с вероятностью } P_{\eta > 0}, \\ \text{если } a_{xk} = 1 \text{ при любом наборе } \langle a_{xk+1}, \dots, a_{xN} \rangle, \\ \text{так как } P(\eta_{\text{н}} \geq 0) = P_{\eta > 0}; \\ 0 \text{ с вероятностью } P_{\eta < 1}, \\ \text{если } a_{xk} = 0 \text{ при любом наборе } \langle a_{xk+1}, \dots, a_{xN} \rangle, \\ \text{так как } P(\eta_{\text{н}} < 1) = P_{\eta < 1}; \\ 1 \text{ с вероятностью } P_{\eta > 0}, \\ \text{если } a_{xk} = 0 \text{ при максимальном наборе } \langle a_{xk+1}, \dots, a_{xN} \rangle, \\ \text{так как } P(\eta_{\text{н}} \geq 1) = P_{\eta > 1}; \\ 0 \text{ с вероятностью } P_{\eta < 0}, \\ \text{если } a_{xk} = 1 \text{ при минимальном наборе } \langle a_{xk+1}, \dots, a_{xN} \rangle, \\ \text{так как } P(\eta_{\text{н}} < 0) = P_{\eta < 0}. \end{cases} \quad (21)$$

Следовательно, в течение одного цикла преобразования при условии, что аддитивная помеха не превышает величины одного кванта Δq , т. е. выполняется неравенство $\xi_{\text{н}} < 1$, возможны следующие события, связанные с погрешностью преобразования:

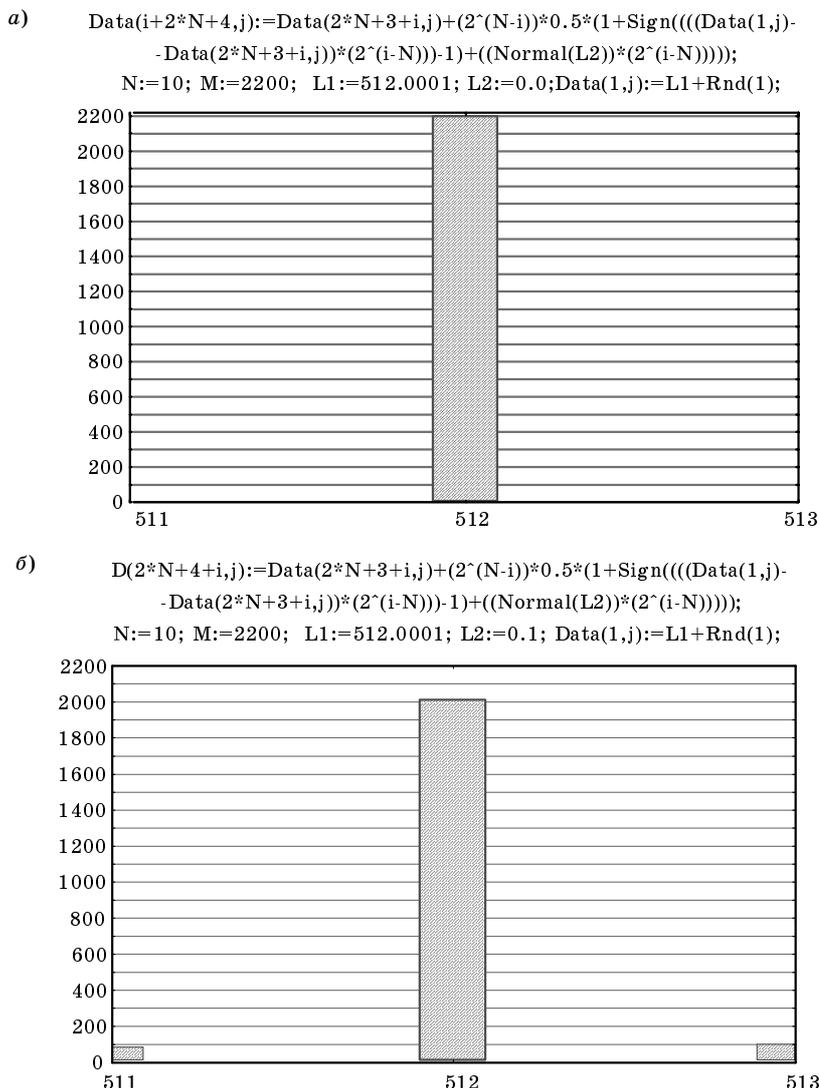
- сбой отсутствует с вероятностью, приближающейся к нулю, по мере уменьшения СКО погрешности (см. рис. 9);
- сбой в младшем разряде в большую или меньшую сторону соответственно с вероятностями (подтверждается рис. 10, 11)

$$P(\eta_{\text{н}} \leq 0) = \int_{-\Delta q}^0 w(\eta_{\text{н}}) d\eta_{\text{н}} \text{ или } P(\eta_{\text{н}} \geq 1) = \int_1^{\Delta q} w(\eta_{\text{н}}) d\eta_{\text{н}}; \quad (22)$$

- возможен сбой в двух младших разрядах с незначительно увеличивающейся вероятностью с ростом в пределах кванта СКО помехи (подтверждается рис. 12 и 13).

Формулы (21) и (22) с учетом сделанных выше пояснений дают возможность оценить вероятность того, что в течение времени преобразования произойдет сбой, в соответствии с формулой

$$P_{\text{сб.п}} = [P(\eta \geq 0) + P(\eta \leq 1)] [1 + 2^{-1} + 2^{-2} + \dots + 2^{-(N-1)}] = 2 [P(\eta \geq 0) + P(\eta \leq 1)] (1 - 2^{-N}).$$



■ **Рис. 10.** Гистограмма результатов преобразования входного сигнала с равномерным законом распределения вероятностей в пределах $512 \leq x \leq 513$ индикаторным 10-разрядным алгоритмом: а — при отсутствии инструментальных помех; б — при воздействии приведенной к кванту инструментальной гауссовой помехи с СКО, равной 0,1, и нулевым математическим ожиданием

Тогда вероятность правильной работы алгоритма

$$P_{\text{пр.п}} = 1 - 2 \left[P(\eta \geq 0) + P(\eta \leq 1) \right] (1 - 2^{-N}).$$

Из этих формул следует, что при указанной величине инструментальной помехи вероятность сбоя в течение всего времени преобразования совсем мало отличается от вероятности сбоя, который может произойти на любом такте преобразования. Проведенным аналитическим анализом целесообразно воспользоваться для планирования и интерпретации результатов имитационного моделирования, в том числе при оценке математического ожидания и СКО погрешности аналого-цифрового преобразования в условиях воздействия аддитивной помехи.

Рассмотрим предварительно случай отсутствия инструментальной помехи для индикаторного идеально-информационно-

го алгоритма при преобразовании постоянного входного сигнала, принимающего значение с равномерным законом распределения вероятностей в пределах $512 \leq x \leq 513$. На рис. 10, а приведена гистограмма результатов преобразования данного сигнала. Как и ожидалось, следует вывод о равенстве нулю погрешности преобразования.

Гистограмме результатов преобразования без помех (см. рис. 10, а) соответствует гистограмма погрешности усечения (см. рис. 7). Рассмотрим теперь случай, когда инструментальная погрешность преобразования отличается от нуля, причем приведенная к кванту СКО помехи равна 0,1, т. е. составляет всего 10 % от приведенного интервала квантования, равного единице. В этом случае гистограмма результатов преобразования без помех, представленная на рис. 10, а, отличается от соответствующей гистограммы рис. 10, б тем, что в последнем случае появляются дополнительные значения кодов, отличные в большую или меньшую сторону на единицу от основного значения. При этом, как и предсказывалось по результатам аналитического анализа, помеха соответствует закону распределения вероятностей, отличному от равномерного, и частоты появления дополнительных кодов отличаются друг от друга и в сумме составляют менее 10 % от общего объема выборки. Гистограммы погрешностей преобразования, представленные на рис. 8, когда присутствует инструментальная помеха, отвечают законам распределения вероятностей, отличным от равномерного, причем, как это следует из рис. 8, б, с ростом СКО инструментальной помехи гистограмма погрешности преобразования приближается к гауссовому закону распределения вероятностей.

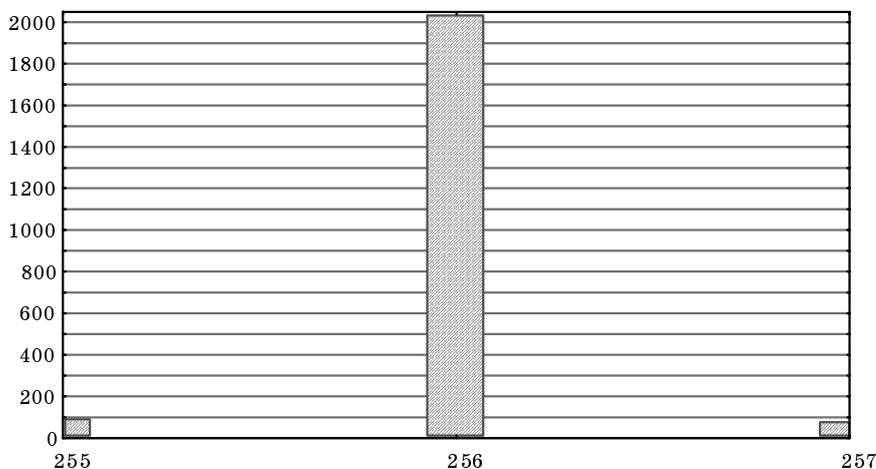
Поскольку инструментальная помеха зависит от элементов схемы АЦП и условий его включения, то не зависит от параметров алгоритма, а ее СКО определяется многими конструктивными, технологическими и другими факторами. Тогда как погрешность усечения зависит от параметров установленного алгоритма аналого-цифрового преобра-

зования, в частности от выбранного числа разрядов. Поэтому уменьшить суммарную помеху, возникающую при аналого-цифровом преобразовании, можно за счет уменьшения погрешности усечения, т. е. за счет увеличения числа разрядов N . Подтверждение этого вывода, наряду с наглядным представлением конкретных количественных примеров по оценке погрешности АЦП, а также других полезных сведений о поведении исследуемых алгоритмов в условиях воздействия помех, целесообразно получить посредством имитационного моделирования, что значительно проще, чем проведение соответствующих аналитических расчетов и, тем более, экспериментов. Результаты моделирования наряду с аналитическими выводами составят достаточно полную картину по динамике основных составляющих погрешности, помехоустойчивости и другим особенностям поведения алгоритмов АЦП в условиях воздействия помех.

Заметим, что если входной сигнал распределен, например, по гауссовому закону, то вероятность сбоя на первом такте уравнивания будет больше, чем для равномерного закона распределения входного сигнала на этом же такте. При этом вероятность сбоя для первого такта будет больше, чем суммарная вероятность сбоя на втором такте, в 1,173 раза, тогда как для равномерного распределения входного сигнала, наоборот, вероятность сбоя во втором такте увеличивается по сравнению с первым тактом в два раза. Тем не менее, вероятность сбоя в течение всего цикла аналого-цифрового преобразования практически не зависит от закона распределения вероятности входного сигнала.

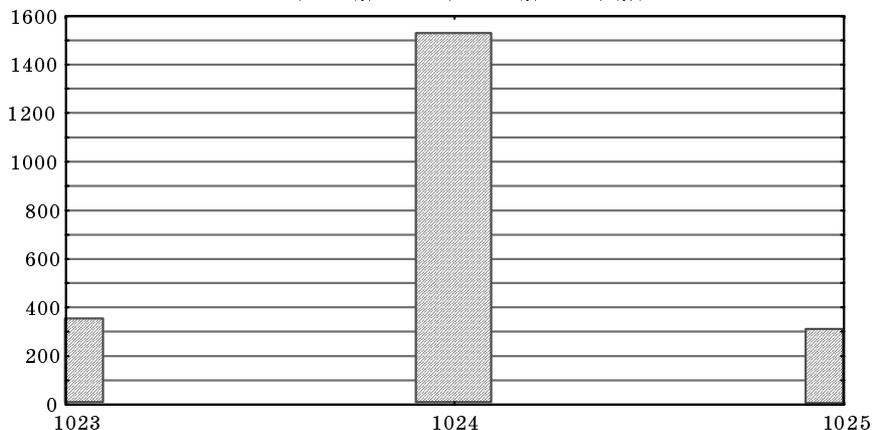
Особый интерес связан с оценкой помехоустойчивости алгоритмов АЦП и с разработкой рекомендаций по рациональному выбору числа разрядов АЦП при условии заданной величины СКО аддитивной помехи. Для этого сначала проанализируем динамику изменения случайной составляющей погрешности результатов преобразования при фиксированных значениях СКО помехи и входного сигнала, равного половине приведенного к кванту диапазона преобразования, в зависимости от изменения числа разрядов в индикаторном реально-информационном алгоритме. Отметим, что особенностью реально-информационного алгоритма является то, что при фиксированных значениях входного сигнала и СКО помехи с ростом числа разрядов увеличивается число квантов, укладываемых в установленном уровне входного сигнала и СКО помехи. В связи с этим сохраняется постоянство приведенной погрешности усечения, равной единице, с одной стороны, и увеличиваются в соответствующее число раз приведенные значения входного сигнала и СКО помехи, с другой стороны. С учетом этого на рис. 11–14 отложенные на оси абсцисс увеличивающиеся значения приведенного к кванту входного сигнала фактически соответствуют постоянному исходному значению входного сигнала, равного половине диапазона преобразования. То же можно сказать и о приведенном значении СКО инструментальной помехи, отложенном на оси абсцисс (рис. 15). Как следует из гистограмм значений результатов преобразования (см. рис. 12–14), рост числа разрядов при фиксированных значениях СКО помехи и входном сигнале приводит к увеличению вероят-

```
N:=9; M:=2200; L1:=1; L2:=0.1; L:=256.001; Data(1,j):=L+Rnd(L1);
Data(i+N+4,j):=Data(N+3+i,j)+(2^(N-i))*0.5*(1+Sign((((Data(1,j)-
-Data(N+3+i,j))*(2^(i-N))))-1)+((Normal(L2))*(2^(i-N)))));
Data(35+d,j):=Data(2*N+4,j)-Data(1,j);
```



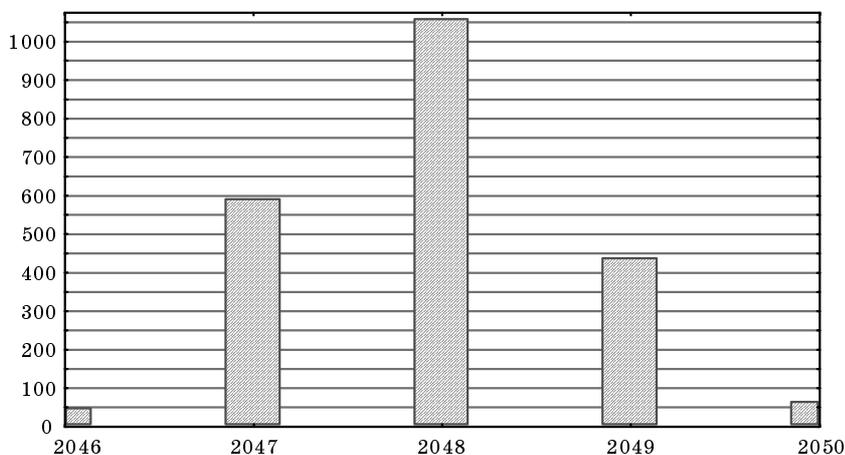
■ **Рис. 11.** Гистограмма результатов преобразования входного сигнала с равномерным законом распределения вероятностей в пределах $255 \leq x \leq 257$ индикаторным 9-разрядным алгоритмом, при воздействии приведенной к кванту инструментальной гауссовой помехи с СКО, равной 0,1, и нулевым математическим ожиданием

$N:=11; M:=2200; L1:=1; L2:=0.4; L:=1024.001; \text{Data}(1,j):=L+\text{Rnd}(L1);$
 $\text{Data}(i+N+4,j):=\text{Data}(N+3+i,j)+(2^{(N-i)}*0.5*(1+\text{Sign}(((\text{Data}(1,j)-$
 $-\text{Data}(N+3+i,j))*(2^{(i-N)}))-1)+((\text{Normal}(L2))*(2^{(i-N)})))));$
 $\text{Data}(35+d,j):=\text{Data}(2*N+4,j)-\text{Data}(1,j);$



■ *Рис. 12. Гистограмма результатов преобразования входного сигнала с равномерным законом распределения вероятностей в пределах $1023 \leq x \leq 1025$ индикаторным 11-разрядным алгоритмом, при воздействии приведенной к кванту инструментальной гауссовой помехи с СКО, равной 0,4, и нулевым математическим ожиданием*

$N:=12; M:=2200; L1:=1; L2:=0.8; L:=2048.001; \text{Data}(1,j):=L+\text{Rnd}(L1);$
 $\text{Data}(i+N+4,j):=\text{Data}(N+3+i,j)+(2^{(N-i)}*0.5*(1+\text{Sign}(((\text{Data}(1,j)-$
 $-\text{Data}(N+3+i,j))*(2^{(i-N)}))-1)+((\text{Normal}(L2))*(2^{(i-N)})))));$
 $\text{Data}(35+d,j):=\text{Data}(2*N+4,j)-\text{Data}(1,j);$



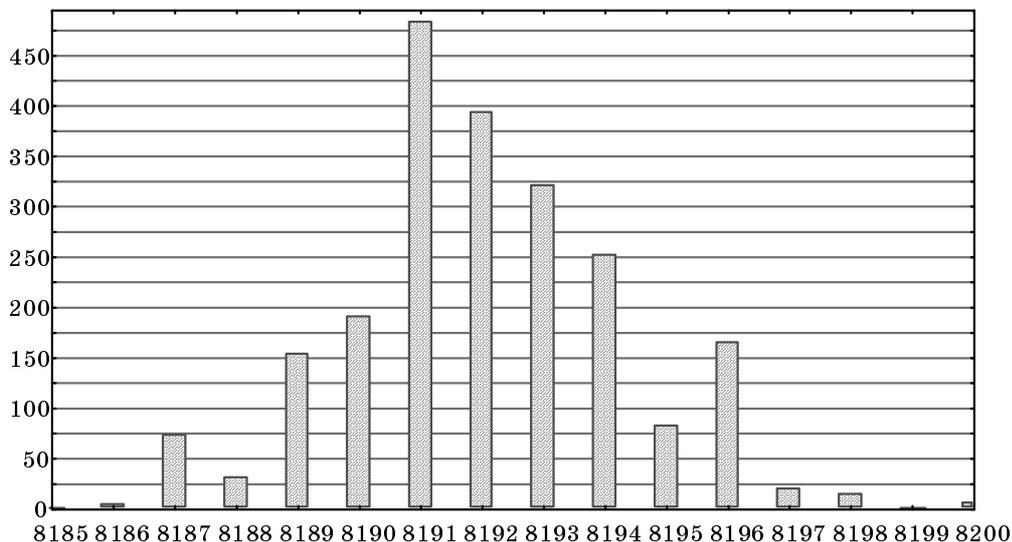
■ *Рис. 13. Гистограмма результатов преобразования входного сигнала с равномерным законом распределения вероятностей в пределах $2046 \leq x \leq 2050$ индикаторным 12-разрядным алгоритмом, при воздействии приведенной к кванту инструментальной гауссовой помехи с СКО, равной 0,8, и нулевым математическим ожиданием*

ностей ошибок первого и второго рода. Поэтому возникает вопрос, будет ли при этом увеличиваться СКО погрешности преобразования, и если да, то в каком соотношении это увеличение будет с динамикой изменения числа разрядов и соответственно с оценкой помехоустойчивости исследуемого алгоритма в целом? На этот вопрос можно найти ответ в результате анализа графика изменения приведенного значения СКО погрешности пре-

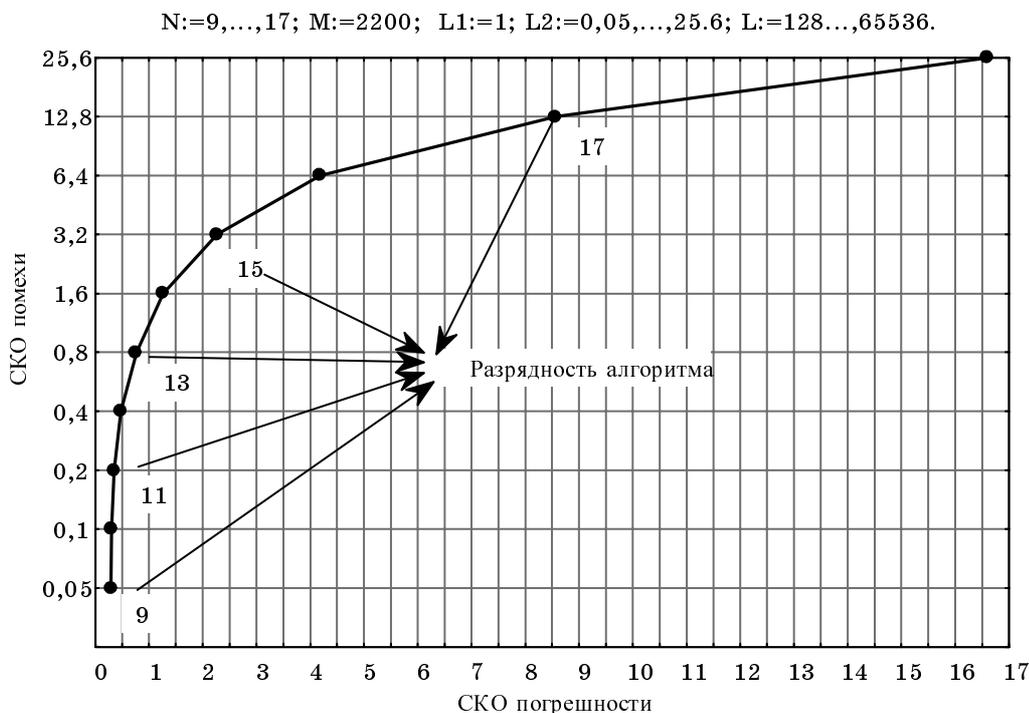
образования в зависимости от изменения числа разрядов алгоритма при фиксированном значении СКО инструментальной помехи (см. рис. 15). Напомним, что инструментальная помеха воздействует на результаты сравнения входного сигнала с уравнивающей величиной независимо на каждом такте уравнивания.

Анализ динамики графика на рис. 15 показывает, что при существенном превышении СКО по-

$N:=14; M:=2200; L1:=1; L2:=3.2; L:=8192.001; \text{Data}(1,j):=L+\text{Rnd}(L1);$
 $\text{Data}(i+N+4,j):=\text{Data}(N+3+i,j)+(2^{(N-i)}*0.5*(1+\text{Sign}(((\text{Data}(1,j)-$
 $-\text{Data}(N+3+i,j))*(2^{(i-N)}))-1)+(\text{Normal}(L2))*(2^{(i-N)})))));$
 $\text{Data}(35+d,j):=\text{Data}(2*N+4,j)-\text{Data}(1,j);$



■ *Рис. 14. Гистограмма результатов преобразования входного сигнала с равномерным законом распределения вероятностей в пределах $8192 \leq x \leq 8193$ индикаторным 14-разрядным алгоритмом, при воздействии приведенной к кванту инструментальной гауссовой помехи с СКО, равной 3,2, и нулевым математическим ожиданием*



■ *Рис. 15. График, характеризующий динамику приведенных к кванту СКО погрешности преобразования и взаимосвязанную с ней СКО инструментальной помехи в зависимости от изменения числа разрядов индикаторного реально-информационного алгоритма*

грешности усечения СКО инструментальной помехи, рост числа разрядов и, следовательно, величины, приведенной к кванту инструментальной помехи, приводит к незначительному росту погрешности преобразования. Однако динамика роста СКО погрешности преобразования изменяется нелинейно, причем темпы роста погрешности преобразования по сравнению с темпом роста приведенной СКО $\sigma_{и.п}$ инструментальной помехи увеличиваются по мере увеличения числа разрядов. Это особенно наглядно показано на рис. 16, где представлены графики изменения СКО погрешности преобразования и СКО помехи в зависимости от изменения числа разрядов. Точка пересечения графиков определяет число разрядов, ниже которого при заданном уровне инструментальных помех нерационально устанавливать количество рабочих разрядов в используемом или проектируемом АЦП.

Для количественной характеристики и наглядного представления темпа роста погрешности преобразования в зависимости от увеличения приведенной к кванту СКО инструментальной помехи целесообразно ввести коэффициент помехоустойчивости вида

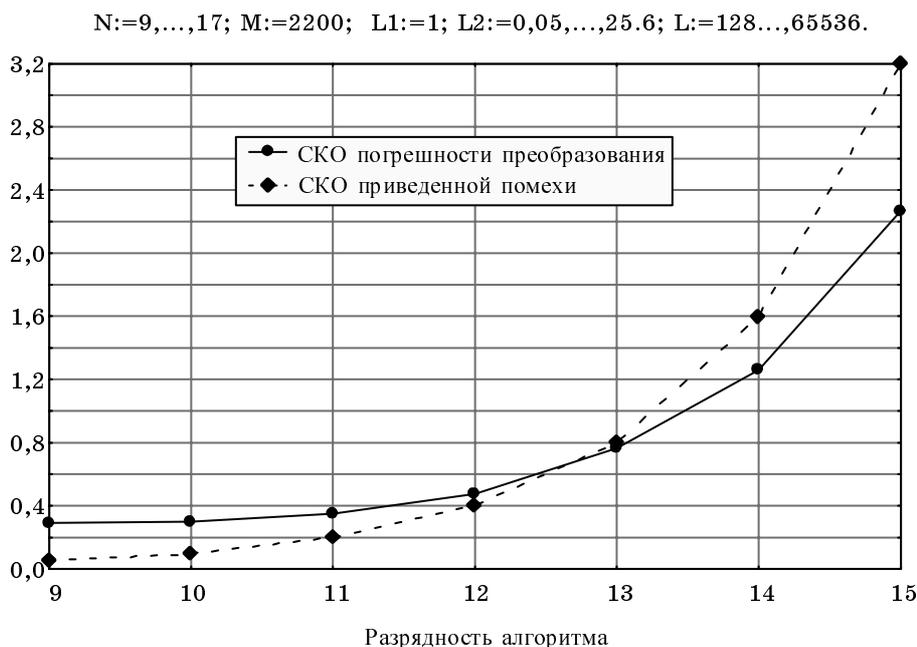
$$K(N) = \frac{\sigma_{и.п}(N)}{\sigma_{п.п}(N)},$$

где $\sigma_{и.п}(N)$ — приведенная величина СКО инструментальной помехи; $\sigma_{п.п}(N)$ — приведенная величина СКО погрешности преобразования. Все указанные в формуле переменные зависят от установленного числа разрядов N .

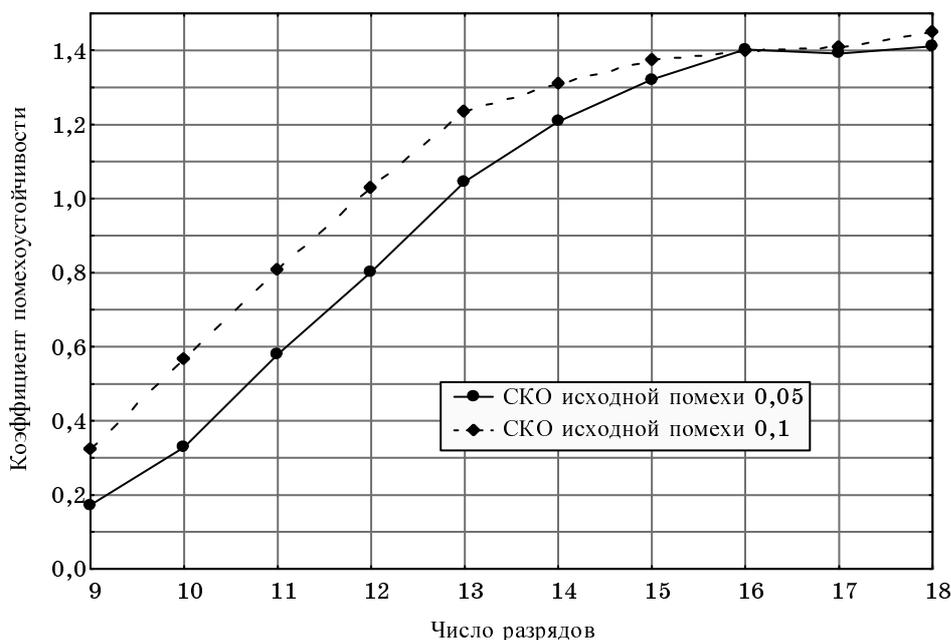
На рис. 17 показаны графики изменения коэффициента помехоустойчивости в зависимости от роста числа разрядов для двух значений СКО помехи, отличающихся в два раза. По мере увеличения числа разрядов коэффициент помехоустойчивости меняется по нелинейному закону, и при 16 разрядах наступает эффект «насыщения», т. е. увеличение числа разрядов не приводит к росту коэффициента помехоустойчивости. Причем, равенство $K(N) = 1$ имеет место для случая, когда для соответствующих СКО выполняется равенство $\sigma_{п.п} = \sigma_{и.п}$, т. е. в точках перегиба графиков рис. 17, где производная по кривым графиков равна единице — касательная к графику образует с осью абсцисс 45° .

Точка перегиба является нижней границей интервала на оси абсцисс, выше которой при заданном значении приведенной СКО помехи для коэффициента помехоустойчивости выполняется неравенство $K(N) > 1$. Верхняя точка интервала определяется числом разрядов, при котором еще наблюдается рост коэффициента помехоустойчивости. Согласно графику рис. 17, это число разрядов равно 15. Изменение СКО приведенной погрешности приводит фактически к сдвигу соответствующего графика, что позволяет легко предсказать значения коэффициента помехоустойчивости для других значений СКО помехи.

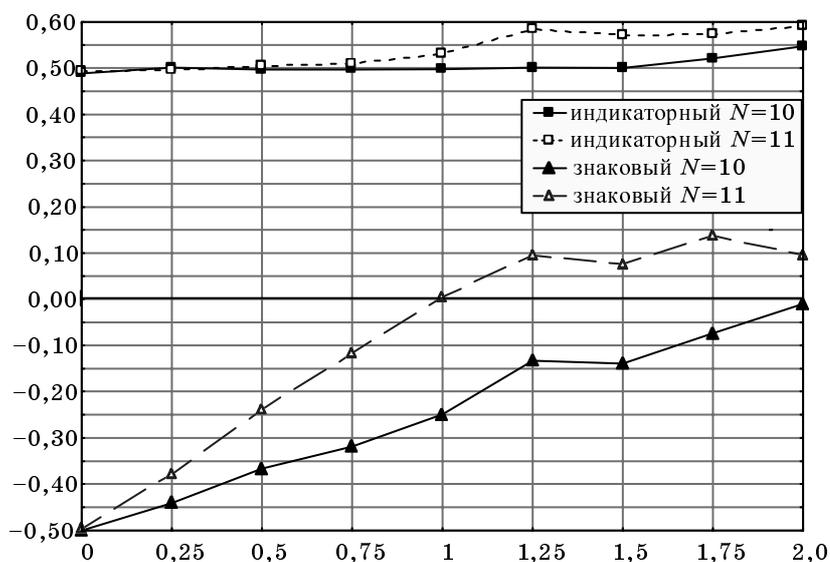
На рис. 18 приведен график погрешности смещения индикаторного и знакового алгоритмов в зависимости от изменения СКО аддитивной помехи. Как и было доказано в работе [2], для знакового алгоритма с увеличением СКО инструментальной



■ **Рис. 16.** Изменение СКО погрешности преобразования индикаторным алгоритмом в условиях воздействия помехи одного и того же значения сигнала, приведенного к кванту, в зависимости от изменения числа разрядов



■ Рис. 17. Изменение коэффициента помехоустойчивости в зависимости от увеличения числа разрядов реально-информационного индикаторного алгоритма для СКО помехи



■ Рис. 18. Математическое ожидание погрешности (погрешность смещения) для индикаторного и знакового реально-информационных алгоритмов в зависимости от изменения уровня инструментальной помехи для $N = 10$ и 11

ной помехи погрешность смещения стремится к нулю, тогда как для индикаторного алгоритма всегда присутствует погрешность смещения, близкая к половине кванта. Для уменьшения погрешности смещения для индикаторного алгоритма можно ввести дополнительный такт преобразования, на котором из результата преобразования на $(N + 1)$ -м такте вычитается половина кванта. В этом случае алгоритм (1) можно представить в виде

$$E(n\Delta t) = \begin{cases} E(n-1) + E_n h[x + \xi(n) - E(n-1) - E_n] \\ \text{для } n \leq N; \\ E(n) = E(n-1) - E_0 2^{-(N+1)} \text{ для } n = N+1. \end{cases}$$

Таким образом, как показал анализ реально-информационного алгоритма, инструментальная помеха, несмотря на определенный эффект ее фильтрации, приводит, естественно, к ухудшению

работы АЦП, т. е. к увеличению его случайной составляющей погрешности. Для более эффективной борьбы с этой помехой, а также для ослабления воздействия других видов помех предложены и широко применяются алгоритмы аналого-цифрового преобразования [3], отличные от рассмотренных алгоритмов поразрядного уравнивания. Однако, даже не меняя принцип поразрядного уравнивания в рассмотренных алгоритмах, можно существенно повысить их помехоустойчивость к инструментальной помехе путем введения мажоритарной функции сравнения входного сигнала с уравнивающей величиной.

В заключение отметим, что рассматриваемый в настоящей работе подход к алгоритмическому описанию информационных процессов в АЦП, с одной стороны, близок к развитой в работах Я. З. Цыпкина (см., например, [4]) информационной теории идентификации. С другой стороны, разработанная в статье теория алгоритмов аналого-цифрового преобразования имеет существенные отличия от известной теории идентификации. Близость к теоретической постановке и решениям задач идентификации следует воспринимать в том смысле, что в настоящей работе также решается задача минимизации заданной функции меры, в том числе в условиях воздействия помех и, тем самым, в рамках работ [4, 5] может интерпретироваться как оптимальное оценивание входного сигнала при заданных ограничениях. Существует еще более общее понятие «наблюдаемость» [5], которое в теории автоматического управления часто также отождествляют с измерением. Некоторые авторы [6] прямое измерение относят к методам идентификации. Очевидно, общее, что отождествляет эти понятия, — цель, заключающаяся в получении информации в результате проведения того или иного действия над входным сигналом.

Отличие этих представлений содержится в объекте исследования, способе оценки достоверности, в виде представления и объеме получаемой информации. Наиболее значительные отличия состоят в следующем:

- при идентификации по входному тестовому и выходному, не обязательно измеренному, а просто оцениваемому тем или иным способом сигналу, получают информацию в том или ином виде об объекте исследования;
- при измерениях, наоборот, по известной структуре средства измерения и выходному сигналу получают информацию о входном сигнале с нормируемой погрешностью;
- различны способы оценки достоверности получаемой числовой информации техническими средствами, заключающейся в нормировке погрешности [7, 8] и, особенно для измерения, возможности передачи единицы измерения на конечный результат.

Если нормирование погрешности и контролируемая передача единицы измерения невозмож-

ны, то в этом случае можно получить только общие количественные данные и, тем самым, общее представление об исследуемом явлении или процессе в виде результатов наблюдения, в том числе и при решении задачи идентификации. Простой пример: о наличии или отсутствии ветра и, приближенно, о его силе можно судить по результатам наблюдения за поведением волн на водной поверхности или листьев деревьев. Но если количественно связать посредством градуировочной характеристики величину амплитуды колебания листьев деревьев или волн с силой или скоростью ветра и при этом нормировать погрешность с соответствующей передачей единицы измерения от эталона (который еще для данного примера нужно создать), то это будет уже измерение силы или скорости ветра.

Таким образом, отличие рассмотренного в настоящей работе подхода заключается не только в конечной цели применения этих алгоритмов и в постановке исходной задачи, а и в решении основной измерительной задачи — в получении числового значения некоторой физической величины с нормируемой погрешностью путем ее сравнения с единицей измерения, представленной в опорной (образцовой) величине. Поэтому целью алгоритмов аналого-цифрового преобразования, в отличие от итерационных алгоритмов идентификации, рассмотренных в работах [4, 5], является не оптимальная оценка структуры или параметров исследуемого объекта, а измерение, которое отождествляется с преобразованием в цифровой код соответствующих значений аналогового входного сигнала с нормируемой погрешностью. Эта цель достигается за счет введения уравнивающей величины, которая определяет опорную (образцовую) физическую величину в соответствии с алгоритмом, реализуемым схемой АЦП (см. рис. 2), по результатам ее сравнения с входным сигналом.

Отметим, что прямая задача идентификации возникает при проверке АЦП, так как структура АЦП априори известна, и в момент его проверки (или для определения не метрологических, а точностных характеристик — тестирования) она отождествляется в пространстве состояний с соответствующей структурой входного тестируемого сигнала. Следовательно, в АЦП входной образцовый (или тестовый) сигнал поступает непосредственно на вход сравнивающего устройства, в котором выполняется операция сравнения с сигналом выхода (в терминах теории идентификации) настраиваемой модели, реализуемой в АЦП. Технически выходом настраиваемой модели, реализуемой в АЦП, является аналоговый сигнал $E(n\Delta t)$, по которому и осуществляется так называемая параметрическая идентификация или диагностика [9] состояния АЦП в целом. Если и имеется технический объект между входным сигналом и непосредственным входом АЦП, то он имеет единичную передаточную функцию, поэтому ис-

ключается из рассмотрения и может тестироваться отдельно (например, усилитель-повторитель, который может применяться при необходимости согласования импеданса входа АЦП с выходным импедансом источника аналогового сигнала, или устройство выборки или хранения). Заметим, что поверка или тестирование АЦП может проводиться и по испытательному входному сигналу, который одновременно подается на поверяемый и образцовый АЦП, а диагностика осуществляется по сравнению их выходных сигналов.

Для учета всех возможных источников погрешности, возникающих при технической реализации алгоритма, в том числе мультипликативной

составляющей, необходимо ввести в исходные алгоритмы дополнительные влияющие факторы, существенно усложняющие и изменяющие общий вид этих алгоритмов. Однако основной вес в полную погрешность преобразования вносит аддитивная составляющая помехи. Исследованию данной помехи, в определенной степени, была посвящена работа [2], тем не менее, в предлагаемой работе не только проведен наиболее полный аналитико-имитационный анализ влияния аддитивной помехи на метрологические характеристики АЦП, а и разработаны рекомендации по оптимизации параметров АЦП в условиях воздействия помех с учетом его конкретных количественных данных.

Литература

1. Справочник по вероятностным расчетам / Г. Г. Абезгауз, А. П. Тронь, Ю. Н. Копенкин и др. 2-е изд., доп. и испр. М.: Воен. изд-во МО СССР, 1970. 536 с.
2. **Иванов В. Н., Тихонов Э. П.** Исследование алгоритмов аналого-цифрового преобразования при воздействии аддитивной помехи // Информационно-управляющие системы. 2006. № 4(23). С. 17–28.
3. **Иванов В. Н., Тихонов Э. П.** Стохастический алгоритм аналого-цифрового преобразования // Вестник МА СЗО. 2006. Вып. 17. С. 12–35.
4. **Цыпкин Я. З.** Информационная теория идентификации. М.: Наука. Физматлит, 1995. 336 с.
5. Справочник по теории автоматического управления / Под ред. А. А. Красовского. М.: Наука, 1987. 712 с.
6. **Шульце К.-П., Реберг К.-Ю.** Инженерный анализ адаптивных систем: Пер. с нем. М.: Мир, 1992. 280 с.
7. **Цветков Э. И.** Основы математической метрологии. СПб.: Политехника, 2005. 510 с.
8. **Селиванов М. Н., Фридман А. Э., Кудряшова Ж. Ф.** Качество измерений: Метрологическая справочная книга. Л.: Лениздат, 1987. 295 с.
9. Обобщенный спектрально-аналитический метод обработки информационных массивов. Задачи анализа изображений и распознавания образов / Ф. Ф. Дедус, С. А. Махортых, М. Н. Устинин, А. Ф. Дедус; Под общ. ред. Ф. Ф. Дедуса. М.: Машиностроение, 1999. 357 с.

УДК 621.391

ИСПОЛЬЗОВАНИЕ ФУНКЦИЙ СПЛАЙН—ВИЛЕНКИНА—КРЕСТЕНСОНА ДЛЯ ПОСТРОЕНИЯ АНАЛИТИЧЕСКИХ МОДЕЛЕЙ РАДИОСИГНАЛОВ

С. Н. Агиевич,

канд. техн. наук, старший научный сотрудник

В. Л. Беспалов,

адъюнкт

Военная академия связи им. С. М. Буденного

Рассматриваются возможности использования базисов функций сплайн—Виленкина—Крестенсона для построения аналитических моделей радиосигналов с целью повышения скорости их цифровой обработки. Излагаются основы современной теории сплайн-гармонического анализа. Определяются понятия свертки и корреляции для функций сплайн—Виленкина—Крестенсона. Производится оценка скорости цифровой обработки радиосигналов, полученных на основе представленных моделей.

We study the use of spline-Vilenkin-Chrestenson functions for the construction of analytical models of radiosignals in order to increase the speed of their digital processing. Fundamentals of the modern theory of spline-harmonic analysis are given. For the spline-Vilenkin-Chrestenson functions the notions of convolution and correlation are defined. Finally, we give some estimates for the speed of digital processing of the radiosignals based on the proposed model.

В настоящее время вопрос использования негармонических функций для передачи радиосигналов в системах связи большей частью был вне поля зрения специалистов. Для этой цели широко используются экспоненциальные функции [1]. Они обладают важными достоинствами: во-первых, являются гладкими (бесконечно дифференцируемыми), а во-вторых, при приеме таких радиосигналов с использованием средств цифровой обработки сигналов (ЦОС) для нахождения спектральных коэффициентов, осуществления фильтрации, нахождения корреляционных функций в базисе дискретных экспоненциальных функций (ДЭФ) [2] используются быстрые алгоритмы, например быстрое преобразование Фурье (БПФ). Между тем ДЭФ, лежащие в основе БПФ, являются частным случаем функций Виленкина—Крестенсона (ВКФ). Скорость быстрых преобразований на основе этих функций может быть существенно выше за счет меньшего модуля представления чисел. Однако гладкие (несколько раз дифференцируемые) аналоги для ВКФ до недавнего времени отсутствовали. Ситуация изменилась с появлением множества систем новых базисов [3] на основе сплайн—Виленкина—Крестенсона функций

(СВКФ). СВКФ являются гладкими (положительное свойство экспоненциальных функций), для них имеются быстрые алгоритмы, причем эти алгоритмы для разложения сигналов по СВКФ в общем случае выполняются значительно быстрее, чем вычисляется БПФ (положительное свойство быстрых алгоритмов в базисе ВКФ). Это позволяет разрабатывать практически новые средства связи на базе существующих с меньшими вычислительными затратами на формирование сигналов и обработку в процессе их приема методами ЦОС.

Кратко поясним суть теории сплайн-гармонического анализа (СГА). В ее основе лежат теоремы и следствия, представленные в работах [3–5]. Для сигналов ${}_{\text{Pal}}S^p(t)$ из пространства ${}_{\text{Pal}}G_n^p$ периодических сплайнов с упорядочением по Пэли [2] (здесь Pal – значок упорядочения по Пэли, p – порядок сплайна дефекта 1, n – номер базисной функции) справедливо:

Теорема 1. Обобщенный ряд Фурье-сигнала из ${}_{\text{Pal}}G_f^p$ представляется:

$${}_{\text{Pal}}S^p(t) = \sum_{n=-\infty}^{\infty} {}_{\text{Pal}}c_n {}_{\text{Pal}}U_n^p(t) = \sum_{n=-\infty}^{\infty} {}_{\text{Pal}}c_n \frac{{}_{\text{Pal}}m_n^p(t)}{{}_{\text{Pal}}u_n^p},$$

где

$$\text{Pal } c_n = \text{Pal } F_n(z);$$

$$\text{Pal } U_n^p(t) = \frac{\text{Pal } m_n^p(t)}{\text{Pal } u_n^p};$$

$\text{Pal } m_n^p(t) = \frac{1}{N} \sum_k \overline{\text{Pal}}(n, k) M^p \left(t \Theta t_k \right)$, μ — модуль представления чисел, Θ — сдвиг по модулю μ , $t_k = \left(\frac{p}{2} + k \right) / N$, N — количество и длина базисных функций;

$$\text{Pal } u_n^p = \text{Pal } F_n(M^p) = 1/N \sum_k \overline{\text{Pal}}(n, k) M^p(t_k);$$

$\text{Pal } F_n(z) = \frac{1}{N} \sum_k \text{Pal}(n, k) z_k$, $\text{Pal}(n, k) = w^{\sum_{i=1}^l n_{i+1} - i k_i}$, $w = \exp(j2\pi/\mu)$, l — число разрядов представления числа по модулю μ , $\overline{\text{Pal}}(n, k)$ — комплексно-сопряженное $\text{Pal}(n, k)$.

Примечание. $\text{Pal } U_n^p(t)$, $\text{Pal } m_n^p(t)$ — базисные СВКФ. Они получены с использованием сплайнов дефекта 1 и обладают их свойствами.

Следствие 1. При $\mu = N$ справедливо:

$$\text{Pal } S^p(t) = \text{ДЭФ } S^p(t) = \sum_{n=-\infty}^{\infty} c_n U_n^p(t).$$

Следствие 2. При $\mu = N$ и $p \rightarrow \infty$ имеем ряд

Фурье: $\lim_{\substack{p \rightarrow \infty \\ \mu = N}} \text{Pal } S^p(t) = \sum_{n=-\infty}^{\infty} c_n e^{2\pi j n t}$.

Следствие 3. При $\mu = N$ и $p = 1$ справедливо:

$$S^1(t) = \sum_{n=-\infty}^{\infty} c_n U_n^1(t), \text{ где } \text{Pal } U_n^1(t) \text{ — ДЭФ.}$$

Пример системы базисных функций $\text{Pal } U_n^p(t)$ с модулем $\mu = 4$, порядком сплайна дефекта 1 $p = 3$ показан на рис. 1, а, система ВКФ, из которой функции $\text{Pal } U_n^p(t)$ получены, продемонстрирована на рис. 1, б.

Теорема 2. Обобщенный ряд Котельникова для сигналов $\text{Pal } S^p(t)$ из пространства непериодических сплайнов $\text{Pal } G_f^p$ может быть представлен с помощью выражения

$$\text{Pal } S^p(t) = \sum_{k=-\infty}^{\infty} z_k \text{Pal } L^p \left(t \Theta t_k \right),$$

где

$$\text{Pal } L^p \left(t \Theta t_k \right) = \frac{1}{F_{\max} - F_{\max}/2} \int_{-F_{\max}/2}^{F_{\max}/2} \text{Pal} \left(f, \frac{k}{F_{\max}} \right) U_f^p(t) df,$$

f и F_{\max} — текущая и максимальная частоты в базисах,

$$\text{Pal } U_f^p(t) = \frac{\text{Pal } m_f^p(t)}{\text{Pal } u_f^p},$$

$$\text{Pal } m_f^p(t) = \frac{1}{N} \sum_{k=-\infty}^{\infty} \overline{\text{Pal}} \left(f, \frac{k}{F_{\max}} \right) M^p \left(t \Theta t_k \right),$$

$$\text{Pal } u_f^p = \frac{1}{N} \sum_{k=-\infty}^{\infty} \overline{\text{Pal}} \left(f, \frac{k}{F_{\max}} \right) M^p(t_k).$$

Следствие 1. При $\mu = N$ $S^p(t)$ представляется кар-

динальными сплайнами: $S^p(t) = \sum_{k=-\infty}^{\infty} z_k L^p(t - t_k)$,

$$L^p(t - t_k) = \frac{1}{F_{\max} - F_{\max}/2} \int_{-F_{\max}/2}^{F_{\max}/2} e^{-2\pi j f k / F_{\max}} U_f^p(t) df.$$

Следствие 2. При $\mu = N$ и $p \rightarrow \infty$ получаем классический ряд Котельникова: $\text{Pal } S^p(t) \stackrel{\substack{\mu=N \\ p \rightarrow \infty}}{=} \sum_{k=-\infty}^{\infty} z_k \frac{\sin \pi(t - t_k) F_{\max}}{\pi(t - t_k) F_{\max}}$.

Замечание. В обозначениях работы [6] ядро

$\text{Pal } L^{p-1} \left(t \Theta t_k \right)$ можно записать следующим обра-

зом: $\text{Pal } L^{p-1} \left(t \Theta t_k \right) = \sum_{k \in Z} \text{Pal} \left(b_N^{p-1} \right)^{-1} M^{p-1} \left(t \Theta t_k \right)$.

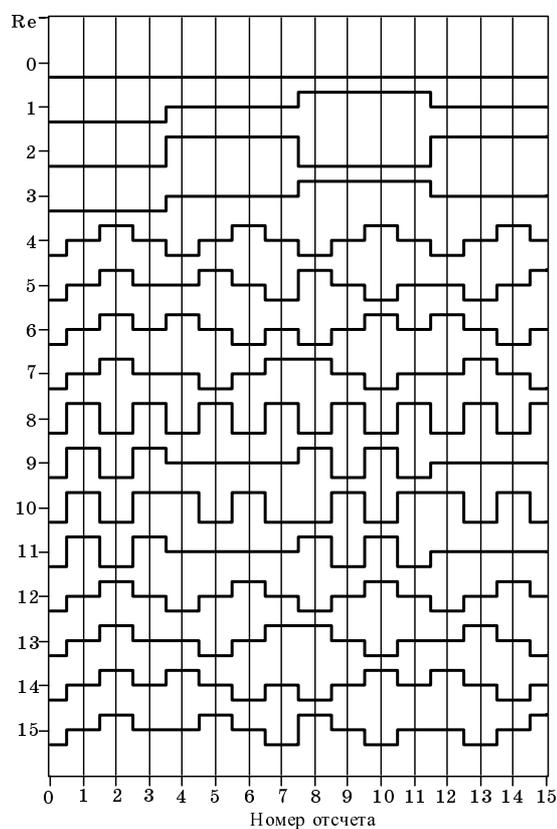
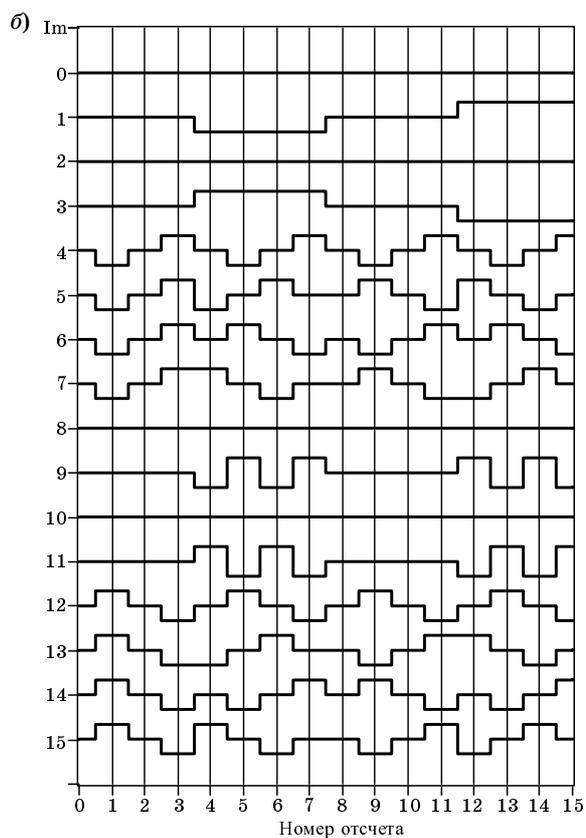
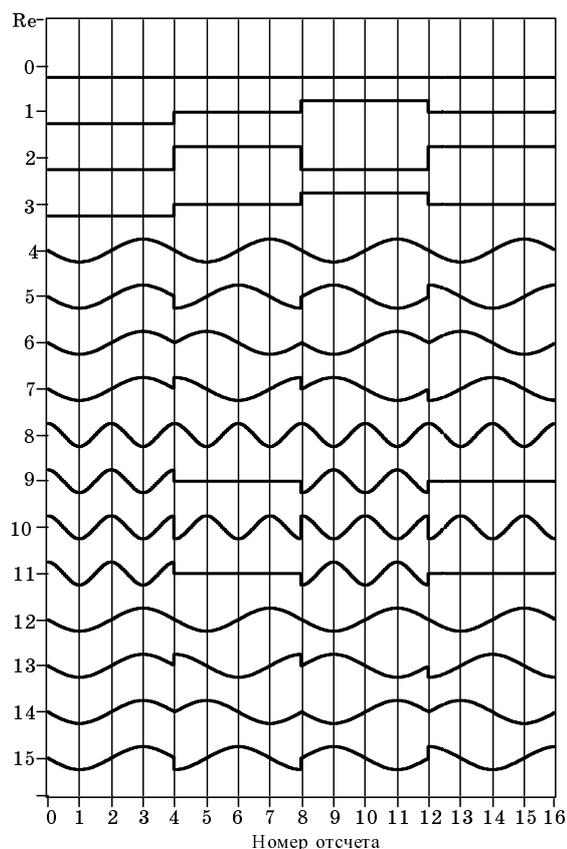
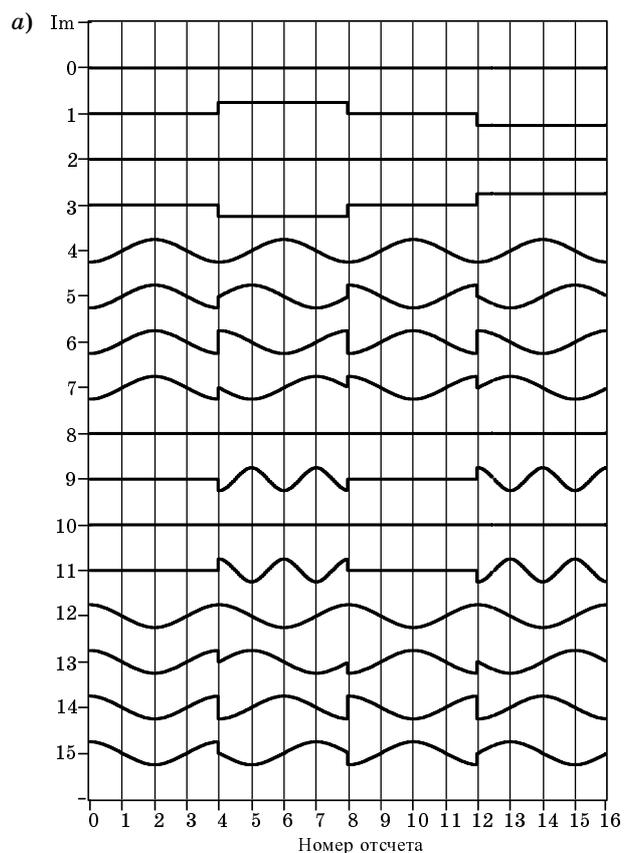
Проанализируем приведенные выше формулировки теорем и следствий к ним с точки зрения возможности построения на их основе аналитических моделей сигналов.

Теорема 1 и следствия к ней позволяют констатировать следующее.

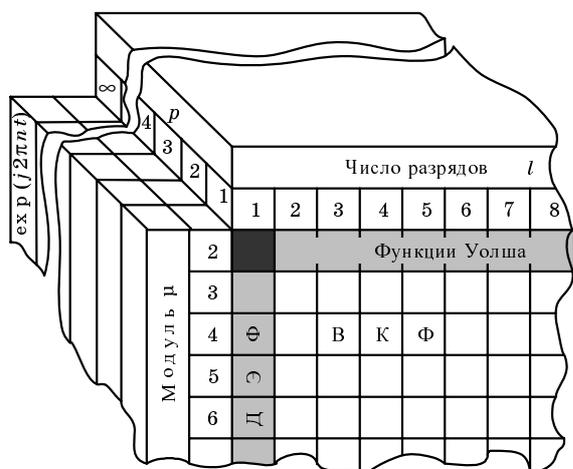
Во-первых, СВКФ в отличие от ВКФ, приобрели свойство гладкости, определяемое параметром p , которым их наделили сплайны. Следовательно, на их основе возможна реализация радиосигналов (т. е. сигналы, сформированные на основе СВКФ, могут передаваться по радиоканалу).

Во-вторых, существует бесконечный набор систем базисных СВКФ, полученных путем свертки ВКФ и базисных сплайнов (рис. 2). Следовательно, если СВКФ пригодны для формирования радиосигналов, то сменой базисов (которых бесконечное количество) в процессе передачи информации может быть решена задача адаптации сигнала под конкретные условия функционирования системы связи.

В-третьих, частными случаями функций СВКФ являются классические непрерывные экспоненциальные функции. Из этого следует, что на основе СВКФ возможно получение обобщенных аналитических моделей сигналов, частными случаями которых являются известные классические модели на основе $\sin(t)$, $\cos(t)$. Средства связи, в основе построения которых будут лежать обобщенные аналитические модели, получают возможность функционирования как в рамках СВКФ, так и



■ Рис. 1. Функции (модуль 4, длина функции $N = 16$): а — СВКФ; б — ВКФ



■ Рис. 2. Базисные функции $PalU_n^p(t)$

классического экспоненциального базиса. Тем самым может быть заложено важное свойство сопрягаемости существующих и предлагаемых к разработке средств и систем связи.

В-четвертых, основой формирования СВКФ являются дискретные Виленкина—Крестенсона функции (ДВКФ). ДЭФ — частный случай ДВКФ. Для ДВКФ существуют быстрые алгоритмы, подобные алгоритму БПФ. Следовательно, возможно создание универсального модуля формирования сигналов на основе СВКФ. При этом смена базиса может осуществляться чисто программными изменениями или сменой коэффициентов. А скорость цифровой обработки радиосигналов, сформированных на основе СВКФ, может быть существенно увеличена по сравнению со скоростью ЦОС, построенных на основе экспоненциальных функций. Это связано с модулем представления функций μ [2].

В-пятых, СВКФ — в общем случае несинусоидальные функции. Следовательно, возникает возможность борьбы с гармоническими помехами.

Теперь перейдем к теореме 2 и следствиям к ней.

Из указанных утверждений следует, что раз существует бесконечный набор систем базисных СВКФ, то существует и бесконечный набор соответствующих ядер, полученных путем свертки соответствующих дискретных и непрерывных СВКФ. Частными случаями этих ядер являются фундаментальные сплайны (ядра Котельникова для сплайнов) и классическое ядро Котельникова. Бесконечный набор ядер — бесконечный набор импульсных характеристик фильтров. Следовательно, если СВКФ пригодны для формирования радиосигналов, то в процессе передачи и приема таких излучений всегда возникает необходимость фильтрации. Выбор импульсной характеристики, соответствующей выбранному базису, может способствовать адаптации системы связи под конкретные условия функционирования.

Приведенный выше анализ теоретических результатов теории СГА показал, что на ее основе

возможно создание аналитических моделей сигналов, реализация которых позволила бы повысить качественные показатели мобильных систем персонального радиосервиса. Поэтому ниже остановимся на получении этих моделей и проанализируем возможность повышения скорости цифровой обработки радиосигналов при осуществлении их регистрации.

Как известно, в качестве модулируемого колебания в классических системах связи обычно используются функции $\sin(t)$ или $\cos(t)$. Другими словами, это мнимая и реальная части экспоненциальной функции. Будем придерживаться такого подхода и при использовании функций СВКФ. Тогда аналитическое выражение для частотно-манипулированного (ЧМ) сигнала может быть записано в следующем виде:

$$S_{Pal}^{\mu(\tau)} S_n^p(t) = A_{Pal}^{\mu(\tau)} U_n^p(t, \varphi), \quad n = 1 \dots R, \quad 0 \leq t \leq T,$$

$$\mu = 2 \dots r, \quad T \leq \tau \leq T_\mu, \quad (1)$$

где A — амплитуда сигнала; φ — фаза — произвольная константа; n — номер базисной функции (физический смысл — частота в базисе СВКФ); R — размерность сигнала (количество функций, используемых для формирования сигнала); T — длительность символа сигнала; T_μ — длительность передачи информации в пределах фиксированного базиса.

При этом, естественно, если модуль представления числа μ равен длине базисной функции N ($\mu = N$) и гладкость функции (порядок сплайна дефекта 1) $p-1 \rightarrow \infty$, то приходим к классическому аналитическому выражению радиосигнала [1] в терминах экспоненциальных функций:

$$\lim_{\substack{p \rightarrow \infty \\ \mu = N}} S_{Pal}^p S_n^p(t) = \lim_{\substack{p \rightarrow \infty \\ \mu = N}} A \operatorname{Re}[S_{Pal} U_n^p(t, \varphi)] \rightarrow$$

$$\rightarrow A \cos(\omega_n t + \varphi), \quad n = 1 \dots R, \quad 0 \leq t \leq T. \quad (2)$$

Аналогично можно представить выражение для фазоманипулированного (ФМ) сигнала:

$$S_{Pal}^{\mu(\tau)} S_i^p(t) = A_{Pal}^{\mu(\tau)} U_n^p(t, \varphi_i), \quad i = 1 \dots R, \quad 0 \leq t \leq T,$$

$$\mu = 2 \dots r, \quad T \leq \tau \leq T_\mu, \quad (3)$$

где $\varphi_i = 2\pi i/R$ — фаза сигнала. Естественно, что при $\mu = N$ и $p \rightarrow \infty$ приходим к классической аналитической модели для фазоманипулированного сигнала [1]:

$$\lim_{\substack{p \rightarrow \infty \\ \mu = N}} S_{Pal}^p S_i^p(t) = \lim_{\substack{p \rightarrow \infty \\ \mu = N}} A \operatorname{Re}[S_{Pal} U_n^p(t, \varphi_i)] \rightarrow$$

$$\rightarrow A \cos(\omega_n t + \varphi), \quad i = 1 \dots R, \quad 0 \leq t \leq T. \quad (4)$$

Выражения (1) и (3) — это аналитические модели сигналов, на основе которых возможно формирование радиосигналов для передачи и приема информации. Проанализируем эти выражения с точки зрения скорости ЦОС этих радиосигналов.

При осуществлении радиоприема методами ЦОС часто возникает необходимость фильтрации, определения спектральных характеристик, нахождения корреляционных функций. При радиосигналах, построенных с использованием классических моделей, для достижения этих целей может использоваться алгоритм БПФ. Поэтому целесообразно произвести оценку скорости ЦОС радиосигналов, сформированных на основе (1), (3), сравнительно с БПФ. Однако, прежде всего, необходимо определить, каким образом свертка, корреляция определяются в терминах СГА при обработке дискретных отсчетов. В этом нам помогут следующие теоремы.

Теорема о спектре свертки двух сигналов.

Пусть

$$\text{Pal } S^p(t) = \frac{1}{N} \sum_{k=0}^{N-1} q_k M^p \left(t \Theta t_k \right) = \frac{1}{N} \sum_{k=0}^{N-1} z_k L^p \left(t \Theta t_k \right) \in \sigma^p; \quad (5)$$

$$\text{Pal } S^b(t) = \frac{1}{N} \sum_{k=0}^{N-1} a_k M^b \left(t \Theta t_k \right) = \frac{1}{N} \sum_{k=0}^{N-1} y_k L^b \left(t \Theta t_k \right) \in \sigma^b; \quad (6)$$

$$\text{Pal } F_n(a) = \frac{1}{N} \sum_{k=0}^{N-1} a_k \text{Pal}(n, k), \quad a = \{a_k\}_0^{N-1}, \quad (7)$$

тогда:

1) $\text{Pal } S^p(t_k) \underset{\mu}{*} \text{Pal } S^b(t) \in \sigma^{p+b}$ — свертка сплайнов порядка p и b есть сплайн порядка $p + b$ (здесь $*$ — знак свертки);

2) $\frac{1}{N} \overline{\text{Pal } S^p(t_k) \underset{\mu}{*} \text{Pal } S^b(t_k)} = \sum_{n=0}^{N-1} \text{Pal } F_n(y) \text{Pal } F_n(z) \times \text{Pal}(n, k) = \sum_{n=0}^{N-1} \text{Pal } F_n(a) \text{Pal } F_n(q) \text{Pal } m_n^{p+b}(n, k)$ — спектр комплексно-сопряженной свертки двух сигналов (сплайнов) есть произведение спектров этих сигналов (здесь $\overline{\quad}$ — знак комплексного сопряжения).

Доказательство 1:

$$\begin{aligned} \text{Pal } S^p(t_k) \underset{\mu}{*} \text{Pal } S^b(t) &= \sum_{t_k=0}^{N-1} \text{Pal } S^p(t_k) \text{Pal } S^b \left(t \Theta t_k \right) = \\ &= \sum_{t_k=0}^{N-1} q_k M^p(t_k) a_k M^b \left(t \Theta t_k \right) = \\ &= \sum_{t_k=0}^{N-1} q_k a_k M^{p+b} \left(t \Theta t_k \right) \in \sigma^{p+b}. \end{aligned}$$

Доказательство 2:

$$\text{Pal } S^p(t_k) \underset{\mu}{*} \text{Pal } S^b(t_k) = \sum_{t_i=0}^{N-1} \text{Pal } S^p(t_i) \text{Pal } S^b \left(t_k \Theta t_i \right).$$

Пусть $t_k = k, t_i = i$, тогда:

$$\begin{aligned} &\sum_{i=0}^{N-1} \text{Pal } S^p(i) \text{Pal } S^b \left(k \Theta i \right) = \\ &= \sum_{i=0}^{N-1} \text{Pal } S^p(i) \sum_{n=0}^{N-1} \overline{\text{Pal } F_n(a)} \overline{\text{Pal } m_n^b \left(k \Theta i \right)} = \\ &= \sum_{i=0}^{N-1} \text{Pal } S^p(i) \sum_{n=0}^{N-1} \overline{\text{Pal } F_n(a)} \overline{\text{Pal } m_n^b(k) \text{Pal}(n, i)} = \\ &= \sum_{i=0}^{N-1} \text{Pal } S^p(i) \sum_{n=0}^{N-1} \overline{\text{Pal } F_n(a)} \overline{\text{Pal } u_n^b \text{Pal}(n, k) \text{Pal}(n, i)} = \\ &= \sum_{n=0}^{N-1} \overline{\text{Pal } F_n(a)} \overline{\text{Pal } u_n^b} \sum_{i=0}^{N-1} q_k M^p(i) \text{Pal}(n, i) \overline{\text{Pal}(n, k)} = \\ &= N \sum_{n=0}^{N-1} \overline{\text{Pal } F_n(a)} \overline{\text{Pal } u_n^b} \overline{\text{Pal } F_n(q)} \overline{\text{Pal } u_n^p \text{Pal}(n, k)} = \\ &= N \sum_{n=0}^{N-1} \overline{\text{Pal } F_n(a)} \overline{\text{Pal } F_n(q)} \overline{\text{Pal } m_n^{p+b}(n, k)}. \end{aligned}$$

Перейдем в исходном и конечном выражениях к комплексно-сопряженным функциям:

$$\begin{aligned} \frac{1}{N} \overline{\text{Pal } S^p(t_k) \underset{\mu}{*} \text{Pal } S^b(t_k)} &= \sum_{n=0}^{N-1} \text{Pal } F_n(y) \text{Pal } F_n(z) \text{Pal}(n, k) = \\ &= \sum_{n=0}^{N-1} \text{Pal } F_n(a) \text{Pal } F_n(q) \text{Pal } m_n^{p+b}(n, k). \end{aligned}$$

Таким образом, спектр комплексно-сопряженной свертки двух сигналов, описываемых сплайнами, есть произведение спектров этих сплайнов.

Из теоремы следует, что при свертке двух сигналов (сплайнов) результирующий сигнал есть сплайн, у которого порядок равен сумме порядков сплайнов $p + b$. Вместе с тем, если, например, сигнал и импульсная характеристика фильтра описываются сплайнами порядка p и b соответственно, то на выходе фильтра будет последовательность, описываемая сплайном порядка $p + b$, но для ее получения в спектральной области достаточно перемножить спектры сигналов в базисе ВКФ.

Теорема 3. Спектр взаимокорреляционной функции $B_{S^p S^b}(i)$ сигналов $\text{Pal } S^p(t)$ в соответствии с (5) и $\text{Pal } S^b(t)$ в соответствии с (6) определяется следующим образом:

$$\begin{aligned} B_{S^p, S^b}(i) &= N \sum_{n=0}^{N-1} \text{Pal } F_n(y) \overline{\text{Pal } F_n(z)} \text{Pal}(n, i) = \\ &= N \sum_{n=0}^{N-1} \text{Pal } F_n(a) \text{Pal } F_n(q) \text{Pal } m_n^{p+b}(n, i). \end{aligned}$$

Доказательство:

$$\begin{aligned}
 B_{S^p, S^b}(i) &= \sum_{k=0}^{N-1} \text{Pal} S^p(k) \text{Pal} \overline{S^b} \left(k \Theta i \right) = \\
 &= \sum_{k=0}^{N-1} \text{Pal} S^p(k) \sum_{n=0}^{N-1} \text{Pal} F_n(a) \text{Pal} m_n^b \left(k \Theta i \right) = \\
 &= \sum_{k=0}^{N-1} \text{Pal} S^p(k) \sum_{n=0}^{N-1} \text{Pal} F_n(a) \text{Pal} m_n^b(k) \text{Pal}(n, i) = \\
 &= \sum_{k=0}^{N-1} \text{Pal} S^p(k) \sum_{n=0}^{N-1} \text{Pal} F_n(a) \text{Pal} u_n^b \text{Pal}(n, k) \text{Pal}(n, i) = \\
 &= N \sum_{n=0}^{N-1} \text{Pal} F_n(a) \text{Pal} u_n^b \text{Pal}(n, i) \frac{1}{N} \sum_{k=0}^{N-1} \text{Pal} S^p(k) \text{Pal}(n, k) = \\
 &= N \sum_{n=0}^{N-1} \text{Pal} F_n(a) u_n^b \overline{\text{Pal} F_n(q) \text{Pal} u_n^p} \text{Pal}(n, i) = \\
 &= N \sum_{n=0}^{N-1} \text{Pal} F_n(y) \overline{\text{Pal} F_n(z)} \text{Pal}(n, i) = \\
 &= N \sum_{n=0}^{N-1} \text{Pal} F_n(a) \text{Pal} F_n(q) \text{Pal} m_n^{p+b}(n, i).
 \end{aligned}$$

Следствие 1. Спектр автокорреляционной функции сигнала $\text{Pal} S^p(t)$ определяется следующим образом:

$$\begin{aligned}
 B(i) &= N \sum_{n=0}^{N-1} \text{Pal} F_n(z) \overline{\text{Pal} F_n(z)} \text{Pal}(n, i) = \\
 &= N \sum_{n=0}^{N-1} \text{Pal} F_n(q) \text{Pal} F_n(q) \text{Pal} m_n^{2p}(n, i).
 \end{aligned}$$

Это выражение можно трактовать как теорему Винера—Хинчина применительно к СВКФ.

Следствие 2. Спектр взаимокорреляционной функции сигналов $\text{Pal} m_n^p(t)$ и $\text{Pal} S^b(t)$ в соответствии с (6) определяется следующим образом:

$$\begin{aligned}
 B_{m_n^p, S^b}(i) &= N \sum_{n=0}^{N-1} \text{Pal} F_n(y) \text{Pal}(n, i) = \\
 &= N \sum_{n=0}^{N-1} \text{Pal} F_n(a) \text{Pal} m_n^{p+b}(n, i).
 \end{aligned}$$

Следствие 3. Спектр автокорреляционной функции сигнала $\text{Pal} m_n^p(t)$ определяется следующим образом:

$$\begin{aligned}
 B(i) &= \text{Pal} m_n^p(k) *_{\mu} \text{Pal} m_n^p(k) = \\
 &= N \sum_{n=0}^{N-1} \text{Pal} m_n^{p+p}(n, i) = N \sum_{n=0}^{N-1} (\text{Pal} u_n^p)^2 \text{Pal}(n, i).
 \end{aligned}$$

Теорема об инвариантности энергетического спектра относительно μ -сдвига.

Энергетический спектр сигнала $\text{Pal} S^p(t)$ в базисе СВКФ не изменяется при его μ -сдвиге, т. е.

$$\begin{aligned}
 \sum_{k=0}^{N-1} \text{Pal} S^p \left(k \Theta i \right) \text{Pal} S^p \left(k \Theta i \right) &= N \sum_{n=0}^{N-1} \overline{\text{Pal} F_n(z)} \text{Pal} F_n(z) = \\
 &= N \sum_{n=0}^{N-1} \overline{\text{Pal} F_n(q) \text{Pal} F_n(q) \text{Pal} u_n^p(k) \text{Pal} u_n^p(k)}.
 \end{aligned}$$

Доказательство:

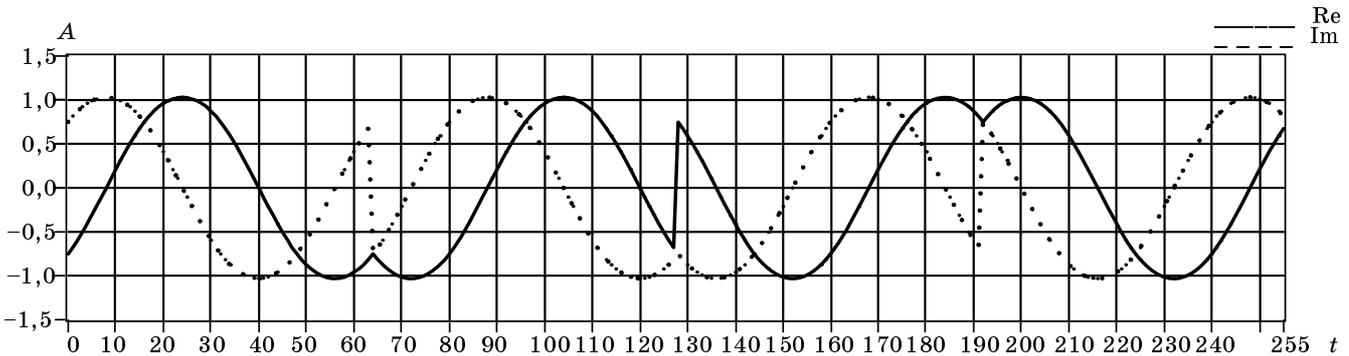
$$\begin{aligned}
 \sum_{k=0}^{N-1} \text{Pal} S^p \left(k \Theta i \right) \text{Pal} S^p \left(k \Theta i \right) &= \\
 &= \sum_{k=0}^{N-1} \text{Pal} S^p \left(k \Theta i \right) \sum_{n=0}^{N-1} \text{Pal} F_n(q) \text{Pal} m_n^p \left(k \Theta i \right) = \\
 &= \sum_{k=0}^{N-1} \text{Pal} S^p \left(k \Theta i \right) \sum_{n=0}^{N-1} \text{Pal} F_n(q) \text{Pal} m_n^p(k) \text{Pal}(n, i) = \\
 &= \sum_{n=0}^{N-1} \sum_{k=0}^{N-1} \overline{\text{Pal} F_n(q) \text{Pal} m_n^p(k) \text{Pal}(n, i)} F_n(q) \text{Pal} m_n^p(k) \text{Pal}(n, i) = \\
 &= \sum_{n=0}^{N-1} \overline{\text{Pal} F_n(q) \text{Pal} F_n(q) \text{Pal}(n, i) \text{Pal}(n, i)} \sum_{k=0}^{N-1} \overline{\text{Pal} m_n^p(k) \text{Pal} m_n^p(k)} = \\
 &= N \sum_{n=0}^{N-1} \overline{\text{Pal} F_n(q) \text{Pal} F_n(q) \text{Pal}(n, i) \text{Pal}(n, i)} \text{Pal} u_n^p(k) \text{Pal} u_n^p(k) = \\
 &= N \sum_{n=0}^{N-1} \overline{\text{Pal} F_n(z) \text{Pal} F_n(z)} = N \sum_{n=0}^{N-1} \overline{\text{Pal} F_n(q) \text{Pal} F_n(q) \text{Pal} u_n^p(k) \text{Pal} u_n^p(k)},
 \end{aligned}$$

что и требовалось доказать.

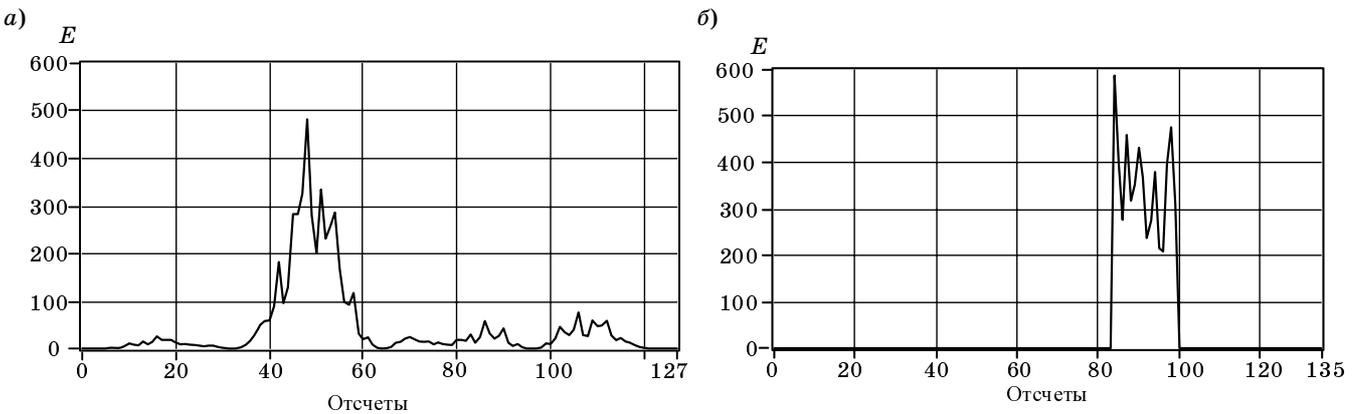
Таким образом, во-первых, результатами операций свертки, корреляции сигналов, описываемых сплайнами, являются сплайны, порядок которых есть сумма порядков исходных сигналов; во-вторых, при обработке таких сигналов методами ЦОС возможно использование алгоритма ДПФ, а следовательно, и БПФ в базисах ВКФ. Для перехода в базис СВКФ достаточно осуществить N умножений в спектральной области. Теперь имеется все для проведения оценки скорости ЦОС радиосигналов, сформированных на основе (1), (3), сравнительно с БПФ.

В качестве примера рассмотрим сигнал ФМ-4, сформированный в базисе СВКФ с параметрами: $\mu = 4, l = 2, p = 4, n = 7$ (рис. 3). Его спектр в базисе Фурье представлен на рис. 4, а, спектр в базисе СВКФ — на рис. 4, б. Для сравнения на рис. 5 показан спектр Фурье классического сигнала ФМ-4. При этом скорости передачи информации, осуществляемой обоими сигналами, одинаковы.

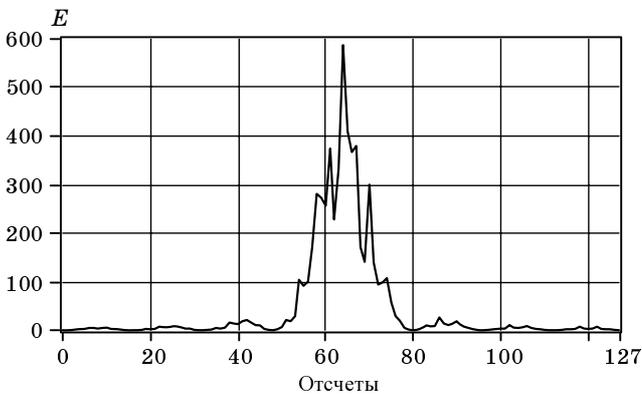
Нельзя не отметить, что при равной скорости передачи информации занимаемые полосы частот в базисе Фурье (см. рис. 4, а, 5) обоими сигналами сравнимы. А энергия сигнала ФМ-4 (см. рис. 3), рассматриваемая в собственном базисе, сосредоточена более компактно (см. рис. 4, б). Это обстоя-



■ Рис. 3. Сигнал ФМ-4 в базе СВКФ



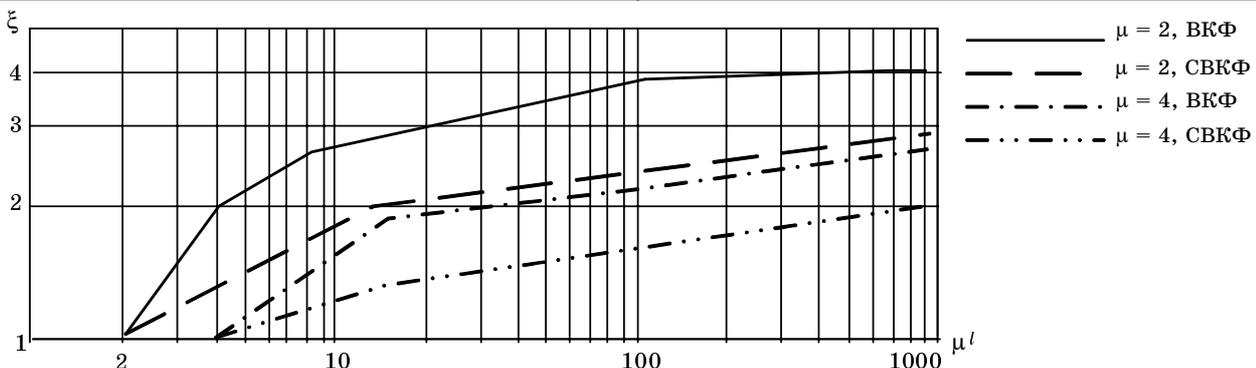
■ Рис. 4. Спектр сигнала ФМ-4: а — в базе Фурье; б — в базе СВКФ



■ Рис. 5. Спектр Фурье классического сигнала ФМ-4

тельство подтверждает положение о возможности передачи информации посредством использования предлагаемых аналитических моделей сигналов. Сравним вычислительные затраты, требуемые для получения спектров, представленных на рис. 4, б и 5.

Для достижения этой цели будем пользоваться подходом, предложенным в работе [2]. Из результатов, приведенных в этом источнике, вытекает следующее. Если принять, что на операцию умножения и сложения тратится одинаковое время, то предельный выигрыш по скорости обработки в условиях использования функций Уолша (в алгоритме БПУ — быстрого преобразования Уолша) будет достигать $\xi = 5$ раз по сравнению с ис-



■ Рис. 6. Выигрыш в объеме вычислений БПФ при переходе от базиса ДЭФ к базисам ВКФ и СВКФ

пользованием функций ДЭФ (в алгоритме БПФ), а при использовании ВКФ по модулю 4 преимущество достигает величины $\xi = 3,25$.

В нашем случае для получения спектра в базе СВКФ использовался алгоритм сплайн-БПФ в базах СВКФ [3]. Согласно этому алгоритму, на N входных точек преобразования дополнительно к стандартному объему вычислений необходимо добавить N операций умножения. Что приводит к увеличению объема вычислений по сравнению с классическими алгоритмами БПУ и БПФ в базе ВКФ по модулю 4. Однако выигрыш в этих случаях по сравнению с использованием алгоритма БПФ все равно оказывается существенным. Используя данные об объеме вычислений при выполнении алгоритма БПФ [7] и результаты из статьи [2], покажем выигрыш в скорости ЦОС графически (рис. 6).

Таким образом, можно констатировать следующее. В работе представлены аналитические модели радиосигналов, на основе которых реально осуществление передачи и приема информации в радиоканалах систем мобильной связи. При этом излучаемые радиосигналы описываются гладкими функциями, поэтому возможно их непосредственное излучение в эфир обычным образом. Кроме того, при равной скорости передачи информации занимаемые полосы частот в базе Фурье для классического сигнала ФМ-4 и сформированного в базе СВКФ сравнимы. А объем вычислений в процессе ЦОС радиосигналов, сформированных и обработанных в базе СВКФ, может быть существенно сокращен по сравнению с объемом вычислений для сигналов, основанных на классических моделях.

Литература

1. Скляр Б. Цифровая связь: Пер. с англ. М.: Вильямс, 2003. 1099 с.
2. Трахтман А. М., Трахтман В. А. Основы теории дискретных сигналов на конечных интервалах. М.: Сов. радио, 1975. 208 с.
3. Агиевич С. Н. Сплайн—Виленкина—Крестенсона функции в представлении сигналов // Научное приборостроение. 2002. Т. 12. № 1. С. 79–89.
4. Желудев В. А. Периодические сплайны и быстрое преобразование Фурье // Журнал вычислительной

математики и математической физики. 1992. Т. 31. № 2. С. 179–198.

5. Zheludev V. A. Periodic splines, harmonic analysis and wavelets in Signal and image representation in combined spaces, wavelet // Anal. Appl., 7 / eds Y. Y. Zeevi and R. Coifman. Academic Press, San Diego, CA, 1998. P. 477–509.
6. Unser M. Splines // IEEE Signal Processing Magazine. 1999. Vol. 16. N 6. P. 22–38.
7. Рабинер Л., Голд Б. Теория и применение цифровой обработки сигналов: Пер. с англ. М.: Мир, 1978. 848 с.

УДК 681.3

СПОСОБ ФОРМАЛИЗАЦИИ СВЯЗЕЙ В КОНСТРУКЦИЯХ ТЕКСТА ПРИ СОЗДАНИИ ЕСТЕСТВЕННО-ЯЗЫКОВЫХ ИНТЕРФЕЙСОВ

И. С. Лебедев,

канд. техн. наук, преподаватель

Санкт-Петербургское высшее военное училище радиоэлектроники

Предложен способ, основанный на использовании структур, характеризующих лексические единицы текста, позволяющий вычислять ответы в тексте на вопросы, заданные в естественном виде. Рассмотрены вопросы разделения текста на семантически связанные единицы.

A method based on the usage of structures characterizing lexical units of a text is proposed which allows to calculate answers in the text to questions put in a natural form. Questions of text division into semantically connected units are considered.

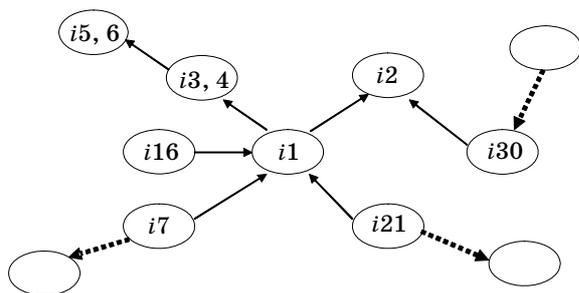
Автоматический анализ текстовой информации приобретает огромную актуальность в связи с развитием глобальных вычислительных сетей и формированием больших объемов распределенных данных.

Современные системы автоматической обработки текстов, доступные широкому кругу пользователей, например информационно-поисковые машины в глобальных вычислительных сетях, в основном сталкиваются с проблемой классификации документов по запросу. На сегодняшний день существуют довольно приемлемые решения, дающие хорошие результаты при анализе всего содержания документа в целом. Однако существует огромный класс программного обеспечения, где необходимо создание естественно-языкового (ЕЯ) интерфейса, позволяющего искать ответ по тексту на вопрос, заданный в удобном для пользователя виде. К таким системам относятся в первую очередь контролируемые, обучающие, вопросно-ответные, где необходимо приближать диалог к естественному для человека виду. Во многих случаях подобный интерфейс полезен информационно-справочным, поисковым системам помощи для анализа вопроса, заданного пользователем, и предоставления точного адекватного ответа в реальном режиме времени. Поэтому разбиение текста на смысловые составляющие, определение семантических связей между словами является актуальной задачей.

Большинство ее решений связано с использованием языков разметки, что требует либо предварительной обработки текста экспертом, либо наличия жесткой структуры. Альтернативные подходы заключаются в том, что текст представляется в виде информационного потока, и по нему стро-

ится граф отношений, содержащий объекты текста и связи между ними. Объекты текста, которые для простоты могут быть представлены словами, обозначаются соответствующими информационными элементами. В работе представлены результаты, на основе которых был создан реально работающий анализатор, позволяющий построить граф предложения. Его демонстрационная версия находится в сети Интернет по адресу www.semlp.com. В основу анализатора была положена «семантическая модель естественного языка» профессора Санкт-Петербургского государственного университета В. А. Тузова. При реализации были созданы морфологический, синтаксический словари и словарь, содержащий семантическую информацию о 100 000 исходных форм слов. Простейшие системы, использующие подобные подходы, могут не содержать никаких словарей или тезаурусов, что позволяет достичь скорости обработки за счет качества, но для более точного определения связей необходимо проводить морфологический, синтаксический и семантический анализ. На рис. 1 приведен пример графа текста со словами i_1, \dots, i_n .

В результате анализа графа, построенного по тексту, видно, что максимальное количество связей образуют несколько информационных элементов, которые являются основными для определения принадлежности тематики этого текста. Построение систем, дающих возможность обрабатывать запросы к тексту на естественном языке, требует как можно более точного определения связей между словами и семантического значения этих слов. Роль и значение слова в предложении определяет часть речи, поэтому необходима формали-



■ Рис. 1. Граф текста

зация существительных, прилагательных, глаголов, наречий, предлогов, частиц.

Наиболее сильно предложение характеризуют существительные. Они и представляют элементарные аргументы предложения и могут быть представлены в виде структуры, содержащей несколько полей, например:

$$S(k_1, \dots, k_n), \quad (1)$$

где S – объект на основе существительного, а аргументы k присоединяются с помощью связей *какой? сколько? чей? чего? кого? кем? чем?*

Применительно к тексту, на котором проводится поиск, объекты можно условно классифицировать по нескольким типам.

1. Существительное, стоящее в тексте: *знания, тестирование.*

2. Существительное, уточненное прилагательным:

мероприятия контрольные.

3. Существительные, уточняющие себя другими существительными в родительном или творительном падеже:

результаты тестирования.

4. Существительные с прилагательными, уточняющие себя другими существительными в родительном или творительном падеже:

тестирование путем проведения мероприятий контрольных.

Такое деление является относительным, но если в запросе пользователя, заданного в любой форме, выделяются подобные группы на основе какого-то объекта, то релевантный документ в своем тексте должен содержать слова уточняющей группы при нем.

На основе тех форм запросов, которые выдают пользователи, используя выражение (1) и подключив словарь синонимов, возможно задавать перефразировки. Например, для запроса «результаты тестирования», используя электронный словарь синонимов [1], находим описания:

<i>результат</i>	<i>следствие, последствие, след, итог, плод, сумма;</i>
<i>тестирование</i>	<i>проверка, испытание.</i>

Подставив их в выражение (1), получаем следующие перефразировки:

результаты тестирования, результаты проверки, результаты испытания, следствия тес-

тирования, следствия проверки, следствия испытания и т. д.

К подобным перефразировкам нужно относиться с осторожностью, так как в результате может исказиться смысл высказывания или возникнуть избыточность информации. Чтобы свести к минимуму возникновение подобных ситуаций, словари синонимов должны подключаться только в соответствии с той тематикой, стилем и жанром, которые являются основными для текста. Современный пользователь устроен таким образом, что желает увидеть в ответе те же словоформы, что и в запросе, поэтому приоритет необходимо отдавать исходным словам.

Базой конструкции предложения, к которой прикрепляются все основные члены, является глагол. Если глагола в предложении нет, то его можно заменить «пустым глаголом». Каждый глагол аналогично существительному может быть также рассмотрен в виде предиката

$$N(G(S_1(k_1, \dots, k_n) \dots S_m(k_1, \dots, k_n))), \quad (2)$$

где N — наречие, отвечающее на вопрос *как? когда? куда? где? откуда? как долго?*; G — глагольная функция; S — объект на основе существительного.

Аналогичным образом описываются и другие части речи. Более подробно это отражено в работе [2].

Основной материал для анализа текста представляют существительные или объекты на основе их [3, 4]. Если в тексте нет существительного или его синонима, которое встретилось в вопросе к тексту, то маловероятно, что в тексте будет содержаться конкретный ответ на вопрос.

Каждая стрелка в графе текста (см. рис. 1) определена совокупностью вопросов, которую можно задать от одного объекта к другому. Условно их можно разбить на две группы. Первая группа основывается на падежных вопросах (*кто? что? кого? чего? кому? чему? кем? чем? о ком? о чем?*). Она практически однозначно определяется предложно-падежной формой, и ее формализация зависит только от морфологической информации. Зная, в каком падеже стоит, например, существительное или прилагательное, всегда можно подобрать вопрос падежа и сформулировать вопрос к словоформе или словосочетанию.

Пришел (из чего?) из деревни.

Вторая группа – это смысловые вопросы, которые гораздо сложнее анализировать.

Пришел (откуда?) из деревни.

Пришел (почему?) из вежливости.

Для формализации смысловых вопросов, которые можно задать к тексту, необходимо вычленив элементарные структуры, внутри которых необходимо описать связи. В данном примере в качестве элементарной единицы рассматривается граф, изображенный на рис. 2.

Вершины этого графа составляют глагол G , прилагательное $Pril$, предлог $Predl$, существительное S , наречие Nar .

Создание формулы предложения состоит в том, чтобы определить каждый аргумент предложения и каждому слову приписать его семантико-грамматический тип. В случае построения такого предиката каждому аргументу можно задать вопрос от глагола, который будет определяться морфологической информацией, что позволит использовать падежный вопрос, а, с другой стороны — смысловой вопрос, стоящий в прямой зависимости от семантики слова.

Многие вопросы, заданные в естественном виде, будут содержать вопросительное слово либо падежей, либо смыслового вопроса. Например, на вопрос к тексту, состоящий из одного вопросительного аргумента *какой?*, могут отвечать не только прилагательные в именительном падеже единственного числа мужского рода, но и существительные в родительном с предлогами *от* и *из*, дательном с предлогами *по*, творительном с предлогом *с*.

Доклад (какой?) от 5-го числа.

Для описания смысловых вопросов необходимо приписать каждому существительному индекс некоторого класса. При описании этих классов с целью вычисления смысловых вопросов за основу было принято описание семантики предлогов русского языка [3]. Число классов может колебаться в зависимости от объема словаря, точности требуемого описания, но оно всегда недалеко от тридцати. Ниже приведены некоторые из них:

дата, направление, свойство, содержание, элемент, действие, материал, множество, мера, число, объект, отношение, чувство, время, емкость, расстояние, закон, часть, инф. источник.

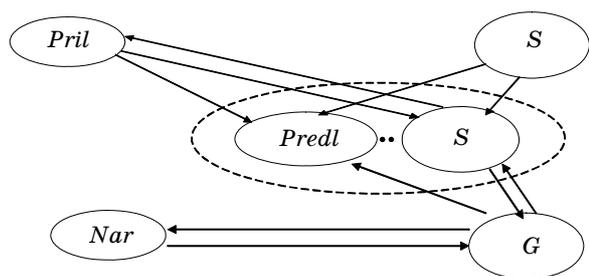
Каждый смысловой вопрос к существительному, независимо от какой части речи он задается, можно выразить по формуле

(ПРЕДЛОГ + ПАДЕЖНЫЙ ВОПРОС) ⊗ Семантика слова = СМЫСЛОВОЙ ВОПРОС,

где семантика слова определяется классом, к которому принадлежит обозначаемое им понятие.

Существительное с предлогом рассматривается как единое целое. На графе рис. 2 стрелками показаны основные связи, которые необходимо формализовать для вычисления ответа на ЕЯ-вопрос.

Однако несмотря на довольно строгое применение предлога для вычисления смыслового вопроса в предложении, человек, задающий вопрос к неизвестному предложению или даже тексту, может из-



■ Рис. 2. Связи между единицами графа текста

начально ставить его в неправильной форме, поэтому при разработке ЕЯ-интерфейсов необходимо расширять варианты поиска. Исходя из этого ниже приведен подход к формализации для некоторых смысловых вопросов. Необходимо отметить, что приводимая формализация находится в стадии внесения изменений и не является окончательной. Всего в русском языке существует около 25 вопросительных слов, в приведенном ниже примере (для вопроса *почему?*) показывается смысловой вопрос, предлог с падежным вопросом, формула согласно рис. 2, показывающая часть речи, от которой задается вопрос, и особенности существительных (падеж и класс), к которым вопрос ставится.

1. Вопрос *почему?*

1.1 почему? (от чего? от кого? с чего? из чего? из-за чего?)

1.1.1 с S образуется связь «элемент от S»: *серый (почему? от чего? с чего? из чего? из-за чего?) от (из-за) пыли*

$Pril + \{Predl = \text{от, с, из, из-за}\}$
 $S^{P.n} = \text{класс «объект»}$

1.1.2 образуется связь «чувство»

ушел (почему? от чего? с чего? из чего? из-за чего?) из вежливости

$G + \{Predl = \text{от, с, из, из-за}\}$
 $S^{P.n} = \text{класс «чувство»}$

1.2 почему? (по чему? по кому? как?)

1.2.1 образуется связь «по закону»: *трактовал (почему? по чему? как?) по закону*

$G + \{Predl = \text{по}\}$
 $S^{D.n} = \text{класс «закон»}$

1.3 почему? (на что? на кого?)

1.3.1 образуется связь «действие»: *закрыли (почему? на что? зачем?) на ремонт*

$G + \{Predl = \text{на}\}$
 $S^{B.n} = \text{класс «действие»}$

1.4 почему? (за чем?)

1.4.1 образуется связь «объект»: *шел (почему? за чем?) за неимением денег*

$G + \{Predl = \text{за}\}$
 $S^{T.n} = \text{класс «объект»}$

Таким образом, рассмотрим два выражения, где подчиненные существительные стоят в родительном падеже:

пришел из вежливости

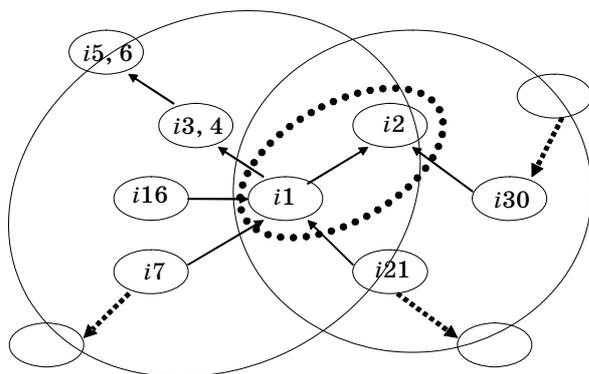
пришел из деревни

Анализатор выдает следующие конструкции:

@Глагол *Пришел* (@Почему из (@Род *вежливости*))

@Глагол *Пришел* (@Откуда из (@Род *деревни*))

Видно, что к первому словосочетанию можно поставить вопрос *Пришел почему? от чего?* и получить в качестве ответа *из вежливости, от безысходности, от горя* — существительные класса «чувства» в родительном падеже. Второе словосочетание отвечает на вопрос *откуда?* Его ответом будут существительные класса «объект» в родительном падеже: *из деревни, из дома, с поля.*



■ Рис. 3. Объекты и их окрестности

После того как построен граф текста, дуги, соединяющие объекты, могут принимать значения либо смысловых вопросов, либо вопросов падежей, в которых находятся объекты.

Цель создания ЕЯ-интерфейса состоит в том, чтобы на запрос пользователя вычислить информацию, адекватную запросу на семантическом уровне. Причем в зависимости от модели диалога, структур, алгоритмов обрабатываемая и выдаваемая информация может быть словом, синтаксической конструкцией, предложением и частью связанного текста. Рассматривая синтаксические конструкции вопроса, получаем некоторый портрет взаимосвязанных предложений, который во многих случаях является ответом. Зачастую здесь содержится основная информация об объекте текста, которую можно узнать, привлекая только формально морфологические признаки. На рис. 3 приведен пример, содержащий объекты и их окрестности.

Однако последнее время все чаще встречается мнение, что достичь качественного прорыва с применением одних только математических и лингвистических методов анализа текста не удастся, и все больше исследователей приходит к мнению о том, что необходимо подключать прагматику.

Например, предложения:

Он прочитал газету.

@Глагол прочитал (@Им Он, @Вин газету).

Он просмотрел газету.

@Глагол просмотрел (@Им Он, @Вин газету).

Он поддержал газету.

@Глагол поддержал (@Им Он, @Вин газету).

Литература

1. Информационный сервер г. Набережные Челны. Электронный словарь синонимов. <<http://www.chelni.ru/slovari/sinonim>>
2. Кондратьев А. В., Кривцов А. Н., Лебедев И. С. Анализаторы текстов формальной модели русского языка для компьютера // Процессы управления и устойчивость: Тр. XXIX науч. конф. студентов и аспирантов факультета ПМ-ПУ / НИИ химии СПбГУ. СПб., 1998. С. 142–154.

можно анализировать как ответы на вопросы:

Он прочитал газету?

@Глагол прочитал (@Им Он, @Вин газету)?

Он ознакомился с газетой?

@Глагол ознакомился (@Им Он, @СТв с газетой) ?

Он взял газету?

@Глагол взял (@Им Он, @Вин газету)?

В любом из перечисленных предложений необходимо сравнивать предикаты $G_1(Он, газета)$, $G_2(Он, газета)$. Если упростить анализ глагольных функций, то система будет выдавать все предложения из примера на любой из вопросов, в противном случае возрастает риск пропустить адекватную информацию. Для борьбы с подобными явлениями необходимо описывать модель реальной действительности, модель ситуаций, где должны содержаться правила сравнения.

В заключение хочется отметить следующее. В основе конструкции семантического языка находятся объекты, образующие между собой связи. Идентификация объектов и вычисление значения их связей основываются на модели представления естественного языка, на способе представления текстовой информации и являются зависящими друг от друга. Не вычислив связи, нельзя определить, является ли множество слов семантической конструкцией, и наоборот, не определив объект, сложно говорить о связях, которые он может образовывать с другими объектами. Формализация связей, способность их вычисления — основная проблема, от решения которой зависит построение адекватных правил работы с текстом.

Связь предложений в тексте в случае ее формализации дает возможность определить границы текста, где можно анализировать несколько предложений в качестве ответа на вопрос. Для анализа текста в вопросно-ответных системах необходимо получить как можно более полный и точный граф предложений.

При создании ЕЯ-интерфейсов огромная роль принадлежит формализации вопросов, задаваемых на естественном языке. Здесь необходимо учитывать и то, что пользователь может ставить семантически правильные вопросы в неправильной форме с точки зрения семантики синтаксиса.

Вычисление смыслового вопроса к предложно-падежной форме сводится к поиску конкретного атрибута присоединяющего слова.

3. Тузов В. А. Компьютерная семантика русского языка. СПб.: Изд-во СПбГУ, 2004. 400 с.

4. Комаров И. И., Кривцов А. Н., Лебедев И. С. Принципы построения семантической модели текста и ее применение в системах лингвистического обеспечения // Процессы управления и устойчивость: Тр. XXXIII науч. конф. студентов и аспирантов факультета ПМ-ПУ / НИИ химии СПбГУ. СПб., 2002. С. 373–382.

УДК 681.3.06

О ВЕРИФИКАЦИИ ПРОСТЫХ АВТОМАТНЫХ ПРОГРАММ НА ОСНОВЕ МЕТОДА *MODEL CHECKING*

С. Э. Вельдер,

магистрант

А. А. Шалыто,

доктор техн. наук, профессор

Санкт-Петербургский государственный университет информационных технологий, механики и оптики

Излагается применительно к простым автоматным программам (их поведение описывается одним конечным автоматом) техника верификации, которая базируется на темпоральных логиках и называется *Model Checking*. Для автоматных программ удается автоматизировать процесс построения модели программы, подлежащей верификации.

Verification of simple automata-based programs (whose behavior can be described with a single finite automaton) is considered. The applied verification technique is based on temporal logics and is known as Model Checking. For automata-based programs it is possible to automate the process of building program model subject to verification.

Введение

Model Checking — это автоматизированный подход, позволяющий для заданной модели поведения системы с конечным (возможно, очень большим) числом состояний и логического свойства (требования) проверить, выполняется ли это свойство в рассматриваемых состояниях данной модели.

Алгоритмы для *Model Checking* обычно базируются на полном переборе пространства состояний модели. При этом для каждого состояния проверяется, удовлетворяет ли оно сформулированным требованиям. Алгоритмы гарантированно завершаются, так как модель программы конечна. Принципиальная схема *Model Checking* приведена на рис. 1.

В проблематике верификации [1] сформировалось два направления: аксиоматическое и алгоритмическое. При использовании первого из них разрабатывается набор аксиом, с помощью которого может быть описана как сама система, так и ее свойства [2]. Основу второго направления составляет метод *Model Checking*.

Перечислим достоинства этого метода.

1. Эффективность. Программы для верификации моделей способны работать с большими пространствами состояний благодаря концепции упорядоченных двоичных разрешающих деревьев [3], которая также упоминается в данной работе.

2. Возможность генерации контрпримеров.

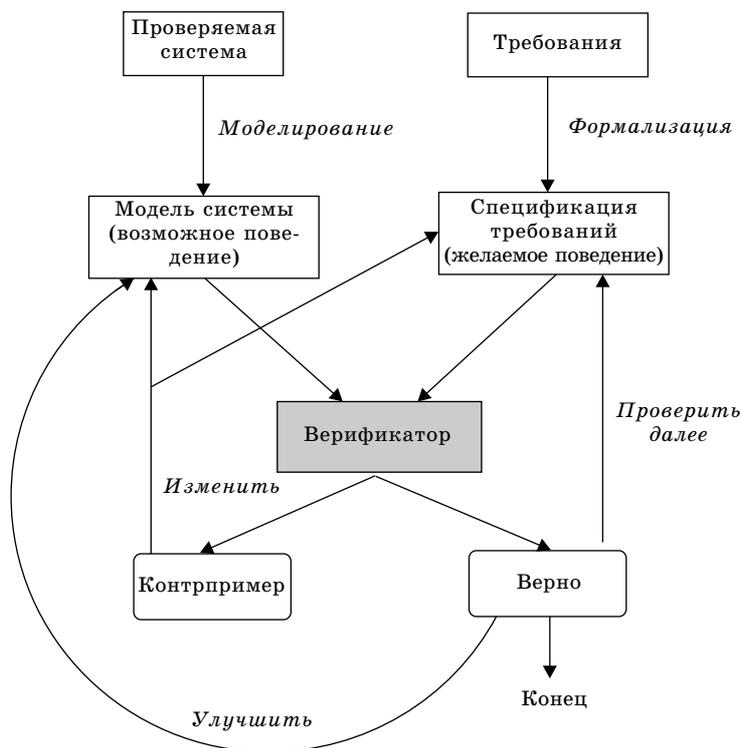
Перечислим ограничения рассматриваемого метода.

1. Поддержка только моделей с конечным числом состояний. Поэтому для большинства классов систем с бесконечным числом состояний необходимо выполнять формальную верификацию системы — математическое доказательство свойств самой программы, а не ее модели.

2. Ограниченность верификации. С использованием метода *Model Checking* проверяется модель системы вместо реальной системы. Таким образом, любое применение метода *Model Checking* настолько же качественно, как и сама модель системы. Кроме того, с помощью этого метода проверяются не любые свойства модели, а только темпоральные.

3. Для многопроцессорных систем размер пространства состояний в худшем случае пропорционален произведению размеров пространств состояний их индивидуальных компонент. Этот эффект называется проблемой показательного (экспоненциального) взрыва состояний (*state-space explosion problem*).

В рамках данной работы рассматривается автоматное программирование (программирование с явным выделением управляющих состояний) [4, 5], поэтому ограничения 1 и 3 в нашем случае не существенны.



■ Рис. 1. Model Checking

Отметим, что настоящая работа выполнялась «параллельно» с работой [6], которая появилась после знакомства ее авторов с автоматным подходом.

Технология верификации простых автоматных программ

Технология автоматного программирования использует такие модели [7], как автомат Мили [8], автомат Мура [9] и смешанный автомат, которые легко интерпретируются с помощью модели Крипке. Автоматную программу будем называть простой, если ее поведение описывается одним конечным автоматом.

Первым шагом в процессе верификации автоматной программы является преобразование графа переходов исходного автомата в модель Крипке, для которой удобно формулировать проверяемые свойства программ. В данной работе отдается предпочтение автомату Мили, который при необходимости всегда может быть преобразован в автомат Мура.

Исследования в данной области (моделирование автомата и конвертация его в модель Крипке) проводились в работах [10–13]. При этом конвертация была сопряжена со следующими проблемами:

- трудности с выполнением композиции автоматов;
- неоднозначность интерпретации формулы языка *Computational Tree Logic (CTL)* [14] в исходном автомате.

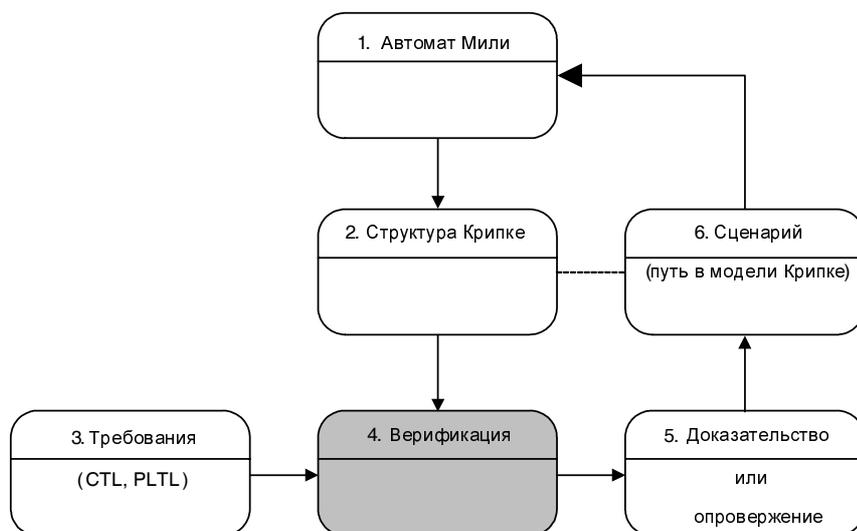
При решении первой проблемы, как правило, возникала вторая. Для ее решения применялась модификация языка *CTL*.

Методы моделирования, рассматриваемые в настоящей работе (в частности, «редуцированная» схема), проводят изменение семантики языка *CTL* для того, чтобы воспрепятствовать экспоненциальному росту числа состояний. При этом пути, построенные в качестве сценариев для *CTL*-формул, однозначно преобразуются из модели в автомат Мили. Это удобно, особенно если моделирование производится совместно с исполнением автомата, его визуализацией и отладкой [15, 16].

Кроме того, при использовании автоматного программирования число управляющих состояний относительно невелико. Это позволяет не применять в данной работе специальные техники для сжатия автоматов с большим числом состояний (упорядоченные двоичные разрешающие диаграммы), а использовать достаточно простые и наглядные алгоритмы, которые работают быстро при небольшом числе состояний, один из которых будет дополнен алгоритмом генерации сценариев.

Перечислим основные положения данной работы.

1. В автоматных программах [4, 5] поведение специфицируется с помощью конечных автоматов. В настоящей работе применяются спецификации, состоящие из одного автомата Мили. В общем случае модель может состоять из нескольких взаимодействующих автоматов. Для верификации таких



■ Рис. 2. Этапы верификации автоматных программ

систем применяется композиция исходных автоматов или моделей Крипке.

2. Использование подхода *Model Checking* для таких программ связано с преобразованием автомата Мулли в структуру Крипке (модель Крипке), так как она, в отличие от автомата, приспособлена для верификации.

3. Использование структуры Крипке предполагает применение темпоральной логики для записи требований, которые должны быть проверены. В настоящей работе при написании программ верификации требования описываются на языке *CTL*.

4. Собственно верификация модели (см. рис. 1) выполняется по структуре Крипке, построенной по автомату Мулли, и требованиям, записанным в виде формулы на языке темпоральной логики *CTL*.

Верификация осуществляется с использованием двух алгоритмов. Первый предназначен для определения набора состояний в структуре Крипке, в которых выполняется заданное формулой требование, а второй по заданному исходному состоянию и подформуле заданного требования с помощью построенного набора состояний формирует сценарий, который подтверждает или опровергает эту подформулу.

5. Сценарий для структуры Крипке преобразуется в сценарий для автомата Мулли.

6. Все этапы изложенной технологии верификации рассматриваемого класса автоматных программ (рис. 2) иллюстрируются на примере программы для «Универсального инфракрасного пульта для бытовой техники» [17].

Преобразование автомата Мулли в структуру Крипке и разработка требований

Построим несколько различных схем для генерации множества атомарных предложений авто-

матной программы, преобразования автомата Мулли в модель Крипке и записи требований к программе.

Выделим и опишем три основные схемы такого преобразования:

- 1) установка состояний на событиях и выходных воздействиях (переменных);
- 2) создание полного графа переходов;
- 3) редукция полного графа переходов с внесением тесных отрицаний (термин поясняется ниже) внутрь атомарной формулы.

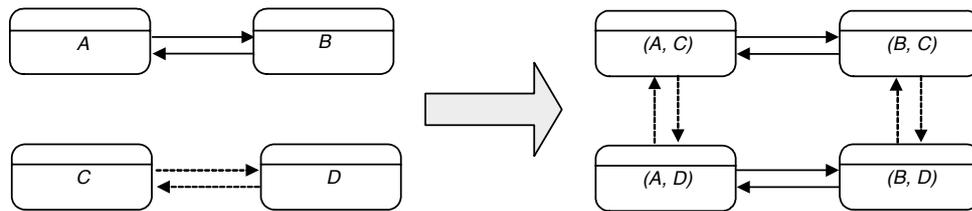
Учтем для любой схемы, что если конечная формула ее спецификации представима в виде конъюнкции нескольких подформул, то эту конъюнкцию целесообразно разбивать на операнды и рассматривать их по отдельности, так как при этом удобнее (и правильнее) исследовать, адекватны ли формальные требования к модели соображениям разработчика о них.

Автоматы, в которых состояния могут содержать внутри себя другие автоматы, можно исследовать тремя способами.

1. Для внешних и внутренних автоматов можно выполнять моделирование, спецификацию и верификацию независимо (конечно, этот способ влечет утрату определенных характеристик автомата при моделировании).

2. Можно «раскрыть» состояние *S* автомата *A*, внутри которого (состояния) находится другой автомат *B*, добавив для каждого перехода из состояния *S* в состояние *T* по одному эквивалентному переходу из каждого состояния автомата *B* в состояние *T*. Все переходы, которые ведут в состояние *S*, следует перенаправить в стартовое состояние автомата *B*. В результате, внутренний автомат *B* превращается в часть автомата *A*, и для него можно выполнять верификацию вместе с автоматом *A*.

3. Систему взаимодействующих автоматов можно привести к одному автомату с помощью



■ Рис. 3. Композиция структур Крипке

композиции (произведения) [10]. Также можно выполнять сначала моделирование каждого автомата, а после него — композицию моделей Крипке (рис. 3).

Выбор способа определяется соображениями эффективности и удобства. В примерах, описываемых далее, считается, что данный вопрос уже решен, и рассматриваются системы, описываемые одним автоматом без вложенных состояний.

Во всех трех схемах, которые будут построены, состояния исходного автомата изоморфно перейдут в состояния модели.

Для каждого перехода между состояниями S и T исходного автомата создадим не менее одного состояния в модели Крипке (назовем его *состоянием-событием*), атомарным предложением которого будет событие E , инициировавшее переход. При наличии выходных воздействий на переходе также создадим по одному состоянию на каждое воздействие Z , атомарным предложением которого (состояния) будет Z (такие состояния будем называть *состояниями-выходными воздействиями*). Добавим в модель переходы: между состоянием S и состоянием-событием E ; между состоянием-событием E и первым состоянием-выходным воздействием; далее последовательно (в порядке выполнения) между соседними состояниями для выходных воздействий и, наконец, между последним таким состоянием-выходным воздействием и состоянием T (далее будет приведен пример такой конвертации).

Если выходное воздействие Z размещалось в состоянии T и выполнялось при входе в него, то при конвертации добавляется еще одно состояние, соответствующее воздействию Z . В это состояние должен вести каждый переход, который первоначально вел в состояние T . Кроме этого, добавляется переход из состояния, соответствующего Z , в состояние T . Само же это воздействие после генерации состояний уничтожается.

Для всех полученных состояний модели Крипке естественным образом устанавливаются атомарные предложения. Добавим также три «управляющих» атомарных предложения: *InState*, *InEvent*, *InAction* — для состояний модели, построенных соответственно из *состояний*, *событий*, *выходных воздействий* исходного автомата. Это сделано для того, чтобы при записи формулы в темпоральной логике можно было различать тип исполняемого состояния.

Таким образом, множество атомарных предложений во всех трех схемах содержит объединение множеств состояний, событий, выходных воздействий и трех описанных выше атомарных предложений. Далее будут рассмотрены индивидуальные особенности каждой из трех схем.

Схема «Состояния на событиях и выходных воздействиях» (ССВВ), как и две другие, наследует общую идеологию моделирования, описанную выше. От других схем ее отличает то, что кроме указанного общего принципа в ней больше ничего не содержится. Таким образом, применяя схему ССВВ для автоматной программы, можно полностью абстрагироваться от понятия входных переменных, оставляя только состояния (без них не обойдется ни одна базовая модель), события и выходные воздействия. Это самый простой подход.

Рассмотрим *пример*. Пусть исходное автоматное приложение эмулирует (в довольно упрощенной форме) универсальный инфракрасный пульт для бытовой техники [17]. Эмулятор представлен с помощью одного автомата *ARemote* (рис. 4). Граф переходов этого автомата приведен на рис. 5.

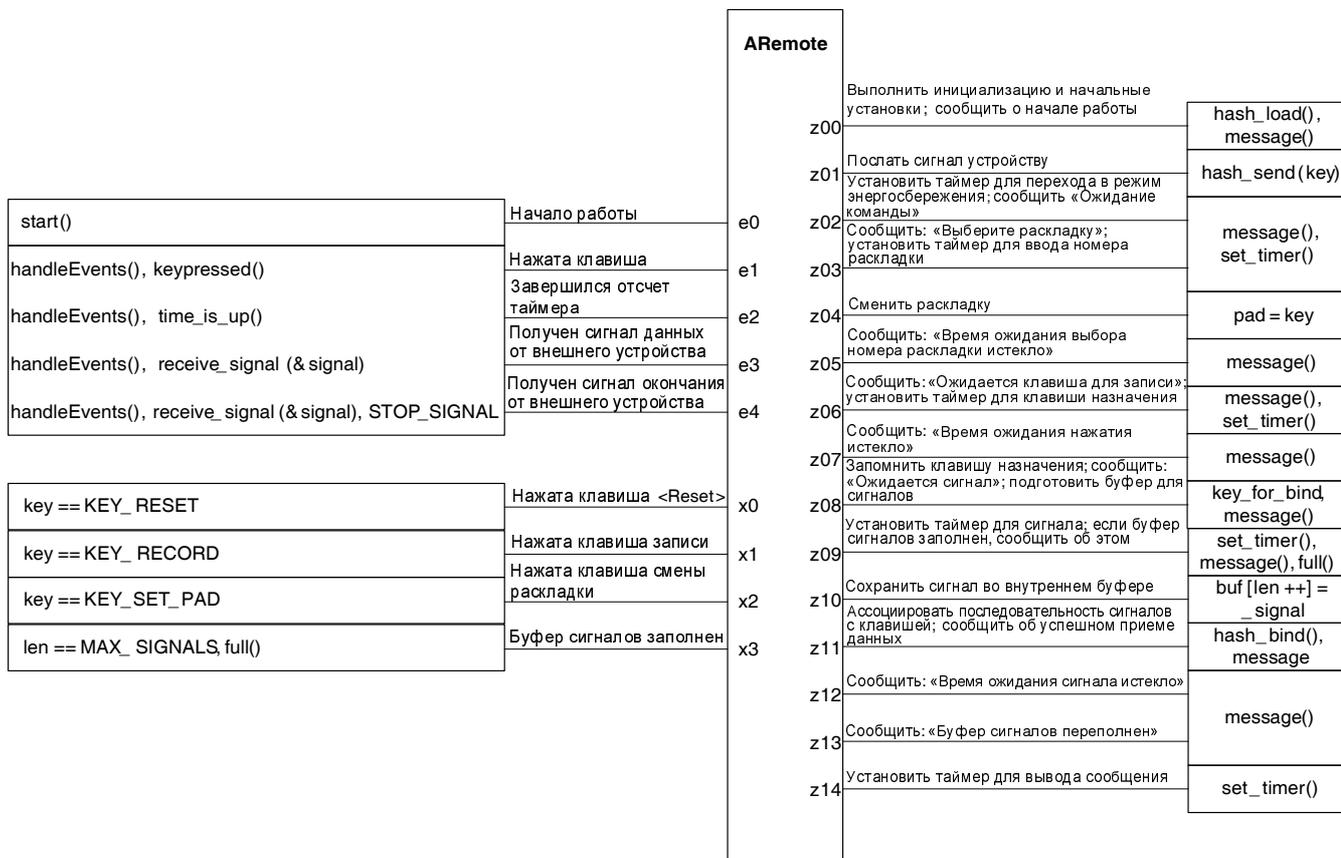
В рассматриваемом примере модель Крипке для автомата, построенная по схеме ССВВ, будет изоморфна графу на рис. 5.

В модели Крипке, изображенной на рис. 6, состояния-события и состояния-выходные воздействия указаны явно.

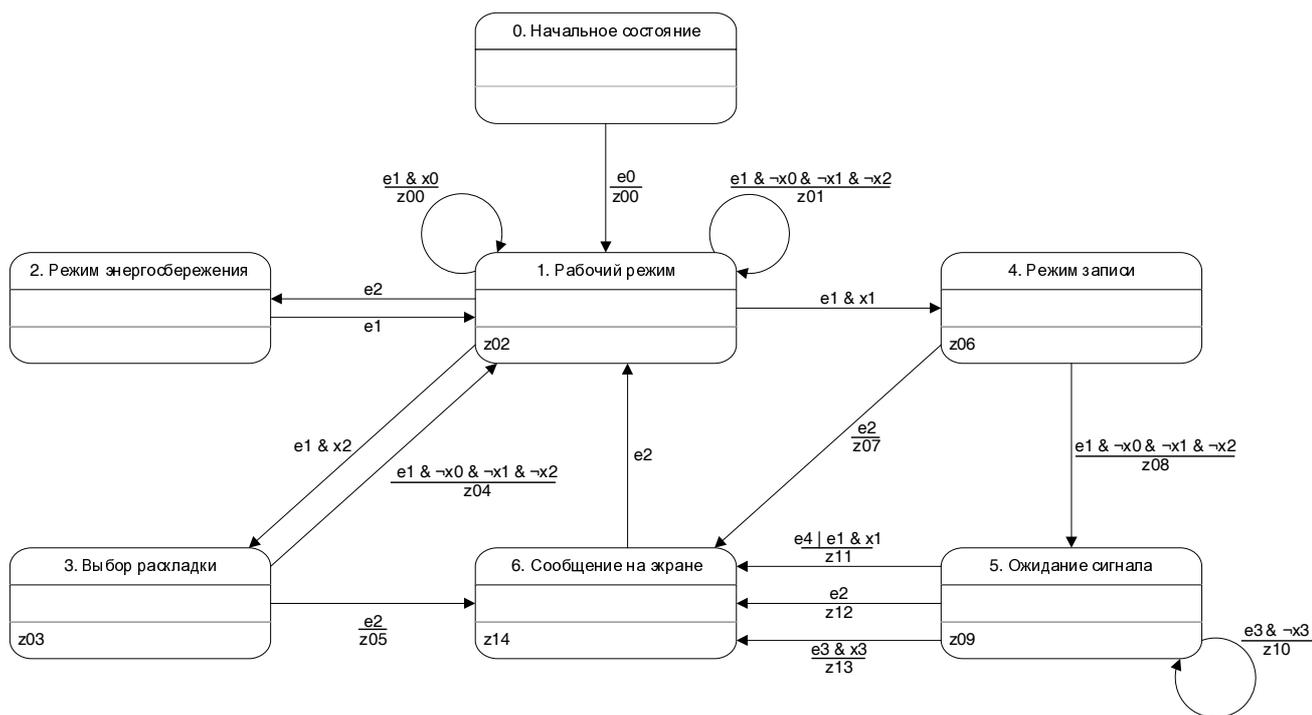
При интерактивном моделировании совместно с исполнением и визуализацией [14, 15] их целесообразно обозначать, как и в исходном автомате, в виде меток на дугах. Таким образом, модель построена.

Приведем теперь *пример* СТЛ-формулы, справедливость которой можно устанавливать верификацией: $\neg E[\neg(Y = 6)U(Y = 1)]$. Смысл этой формулы состоит в следующем: в состоянии 1 нельзя попасть, минуя состояние 6 (нельзя попасть в рабочий режим, минуя сообщение на экране). Эта формула справедлива для состояний 4, 5, 6 исходного автомата и только для них (для модели Крипке таких состояний больше).

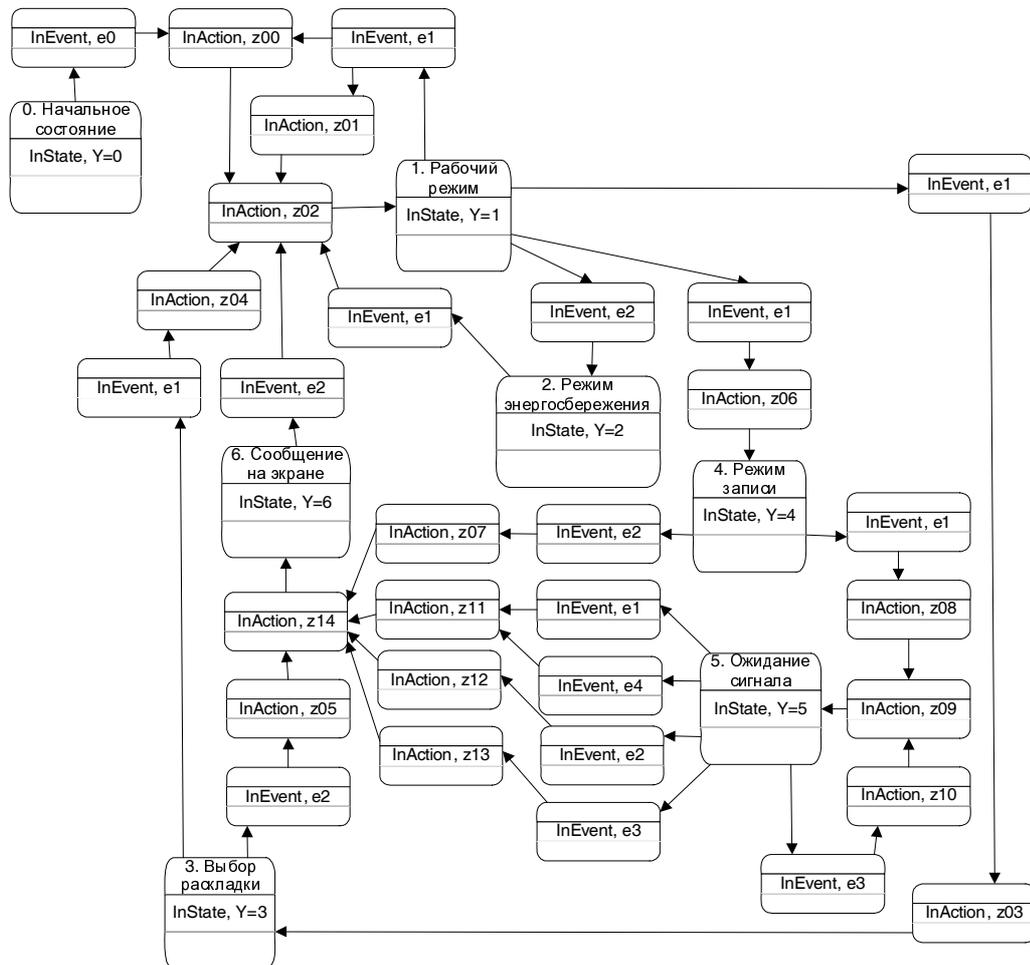
Схема «Полный автомат». Во второй схеме не будем абстрагироваться от входных переменных, а представим автомат моделью Крипке «со всей полнотой» относительно входных воздействий. В исходном автомате переходы могут быть заданы не полностью — могут существовать не указанные петли. Это означает, что для некоторого состояния (некоторых состояний) дизъюнкция формул,



■ Рис. 4. Схема связей автомата ARemote



■ Рис. 5. Граф переходов автомата ARemote



■ Рис. 6. Модель Крипке, построенная по схеме ССВВ

составленных из входных переменных, которые помечают переходы из него по одному и тому же событию E , не является тавтологией.

Снабдим это состояние (состояния) петлевыми переходами по событию E , соответствующими дополнению к рассматриваемой дизъюнкции. Это, конечно же, не изменит семантику автомата, а лишь полностью опишет его поведение. В конечном счете в автомате из каждого состояния по каждому событию должно исходить 2^n переходов, где n — общее число входных переменных автомата. При этом каждому переходу соответствует набор значений всех переменных. После получения полного автомата преобразуем его в модель Крипке по общей схеме с одной модификацией: для каждого состояния-события добавим во множество его атомарных предложений набор входных переменных, истинных на том переходе, на котором находится рассматриваемое состояние-событие. Таким образом, во множество атомарных предложений по отношению к обобщенной схеме добавились еще и входные переменные. Достоинство такой схемы (несмотря на ее расточительность, освобождение

от которой будет описано ниже) в том, что она и только она позволяет модели Крипке полностью отражать поведение исходного автомата.

«Редуцированная» схема. Основным недостатком предыдущей схемы было большое число генерируемых состояний для модели Крипке, а достоинством — ее полнота.

В «редуцированной» схеме семантика моделей будет изменена таким образом, чтобы число состояний в них можно было уменьшить, не потеряв при этом их выразительные возможности. Это можно сделать так, что размер модели изменится асимптотически *линейно* по отношению к размеру графа переходов исходного автомата и к числу переменных (*билинейно*), в отличие от предыдущей схемы, где размер модели увеличивался *экспоненциально* от числа входных переменных.

Множество атомарных предложений по отношению к предыдущей схеме также будет видоизменено.

Рассмотрим исходный автомат без дизъюнкций на переходах. Если такие переходы существуют, создадим эквивалентные переходы для каждого

дизъюнкта, а сами переходы с дизъюнкциями удалим. В качестве *примера* можно разбить переход “ $(e4 \mid e1 \& x1) / z11$ ” графа *ARemote* (см. рис. 5) на два перехода: “ $e4 / z11$ ” и “ $e1 \& x1 / z11$ ”.

Добавим в автомат состояния, соответствующие событиям, входным и выходным переменным, так, как это было сделано в первой схеме (ССВВ), но с одним отличием: во множества атомарных предложений на состояниях-событиях добавим входные переменные в том виде, в котором они присутствуют на переходах (вместе с отрицаниями, если они есть). Таким образом, в состав множества всех атомарных формул модели входят следующие элементы, и только они: состояния; события; выходные воздействия; все литералы, составленные из входных переменных (сами переменные и их отрицания). Кроме того, в атомарные предложения каждого полученного состояния-события добавим все литералы, составленные из несущественных входных переменных для данного перехода (несущественными будем называть те переменные исходного автомата, которые не обозначены на рассматриваемом переходе). Таким образом, будем добавлять на одно и то же состояние-событие и несущественные переменные, и их отрицания. С точки зрения синтаксиса и семантики темпоральной логики, это допустимо: процесс обработки модели Крипке не предполагает совместность множества атомарных предложений состояния, так как интерпретирует эти предложения просто как строки. Причина такого обращения с несущественными переменными ясна: требуется обеспечить, чтобы любая ссылка на несущественную в данном состоянии-событии переменную, упомянутая в *CTL*-формуле, давала истинный результат.

Не обязательно хранить все литералы, составленные из несущественных переменных в состоянии в явном виде. Важно лишь то, что во время обработки модели существенные и несущественные входные переменные интерпретируются отдельно: первые – в том виде, в каком они записаны на переходах исходного автомата, а вторые – «в двух экземплярах» (в прямом и инверсном виде).

Результат конвертации графа переходов автомата *ARemote*, выполненного с применением данной схемы, изображен на рис. 7.

Размер модели на рис. 7 совпадает с размером модели, созданной по схеме ССВВ. Первая схема может рассматриваться по аналогии с третьей или второй, в которой полностью исключены входные воздействия. Аналогично, третью схему можно рассматривать как видоизменение второй, при котором отождествляются наборы значений несущественных переменных.

Теперь рассмотрим построение и интерпретацию *CTL*-формул для «редуцированных» моделей.

CTL-семантика в данной схеме будет немного отличаться от общепринятой: все отрицания, стоящие непосредственно перед атомарными предложениями в *CTL*-формуле (их также называют *те-*

ными отрицаниями), следует внести внутрь атомарных предложений. При этом только результирующая формула в рассматриваемой схеме подлежит верификации методами, предназначенными для *CTL*-логики.

Рассмотрим *пример* для автомата *ARemote*. Пусть требуется проверить свойство: «существует способ провести инициализацию устройства, не нажимая кнопку *Reset*». В терминах языка *CTL* с исходной семантикой данное свойство может быть записано следующим образом: $E[(InEvent \rightarrow \neg x0) U z00]$.

Эта формула не выполняется в состоянии $Y = 0$ (см. рис. 7). На это, правда, и не стоило рассчитывать. Преобразуем формулу согласно третьей схеме: $E[(InEvent \rightarrow !x0) U z00]$. Вместо отрицания в языке *CTL* в формулу было внесено другое атомарное предложение, являющееся отрицанием исходного. Преобразованная формула уже верна для состояния $Y = 0$.

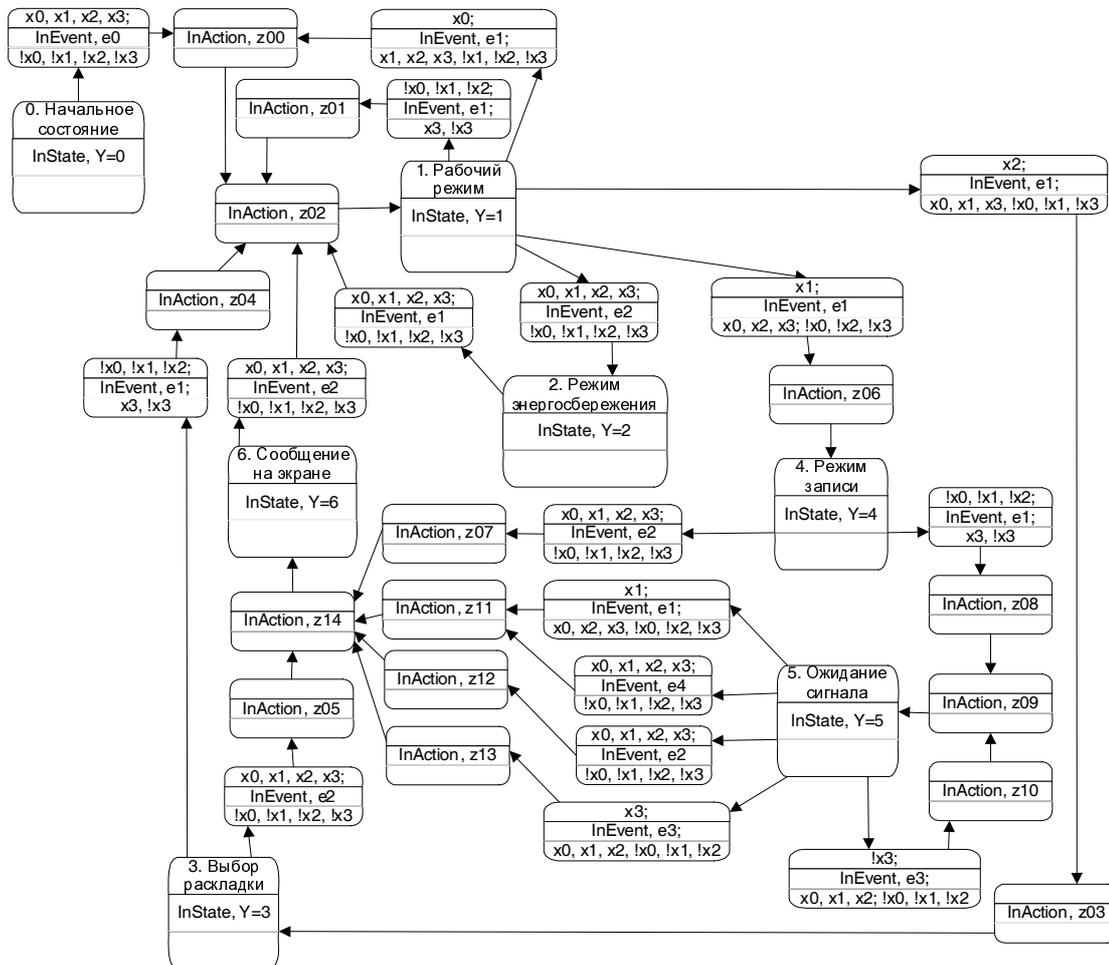
Подведем итог. Для уменьшения числа состояний и из соображений практичности была предложена схема моделирования автомата и изменена семантика языка *CTL*. Однако такое изменение семантики неудобно для верификации. В результате был предложен способ преобразования исходной формулы, соответствующей новой семантике, в новую формулу, для которой применима общепринятая семантика языка *CTL*.

Выполненные примеры показывают, что такой подход не существенно снижает выразительность модели по сравнению с предыдущим (схема «Полный автомат»). Опыт показывает, что для многих формул такая схема может быть использована.

Другие абстракции. Основным недостатком всех описанных выше схем моделирования автоматов является то, что при составлении требований к модели разработчику не всегда удобно различать, где состояния, которые перенесены из исходного графа, где состояния-события, а где состояния-выходные воздействия. Для различения состояний используются атомарные предложения *InState*, *InEvent* и *InAction*, но их применение может быть связано с дополнительными проверками. Для этого, а также для уменьшения числа состояний модели в принципе, можно при построении модели абстрагироваться от каких-либо других ее характеристик, помимо тех, которые были рассмотрены в описанных выше схемах.

Например, можно абстрагироваться не только от входных переменных, но и от событий, а также от выходных воздействий. Можно вообще преобразовать автомат в модель Крипке в один этап, например, с помощью исключения событий и выходных переменных на переходах. Для автомата *ARemote* результатом такого преобразования является модель на рис. 8.

Выбор альтернативного метода можно осуществлять, руководствуясь представлениями о производительности и результативности. Основное внимание необходимо уделять атомарности пере-



■ Рис. 7. Редуцированная модель Крипке для автомата ARemote

ходов. Если они слишком большие (по числу действий), то разработчик может пропустить ошибку, если же слишком маленькие — то размер модели может немотивированно увеличиться за счет появления несущественных свойств.

CTL-верификация автоматных программ

Опишем идею алгоритма CES (Clarke, Emerson, Sistla) [18], который основан на переформулировке синтаксиса языка CTL. Этот алгоритм дополнен таким образом, что позволяет строить подтверждающие сценарии для проверяемых формул. Применять этот алгоритм будем для изображенных явно моделей Крипке.

Под локальной задачей верификации обычно понимается вопрос: выяснить для данной модели и состояния в ней, выполняется ли в этом состоянии заданная формула.

При построении алгоритма формулируется глобальная задача верификации: для данной модели и проверяемой формулы построить множество всех состояний модели, в которых верна эта формула.

Когда число состояний невелико, как в случае автоматных программ, это множество можно строить в явном виде.

Запишем одну из форм определения синтаксиса и семантики языка CTL (в ней темпоральная часть будет целиком выражена через операции EX, EU, EG):

$$A(f U g) = \neg (E[(\neg g) U \neg (f \vee g)] \vee EG \neg g)$$

$$\phi ::= p \in AP \mid \neg \phi \mid \phi \vee \psi \mid EX \phi \mid E[\phi U \psi] \mid EG \phi,$$

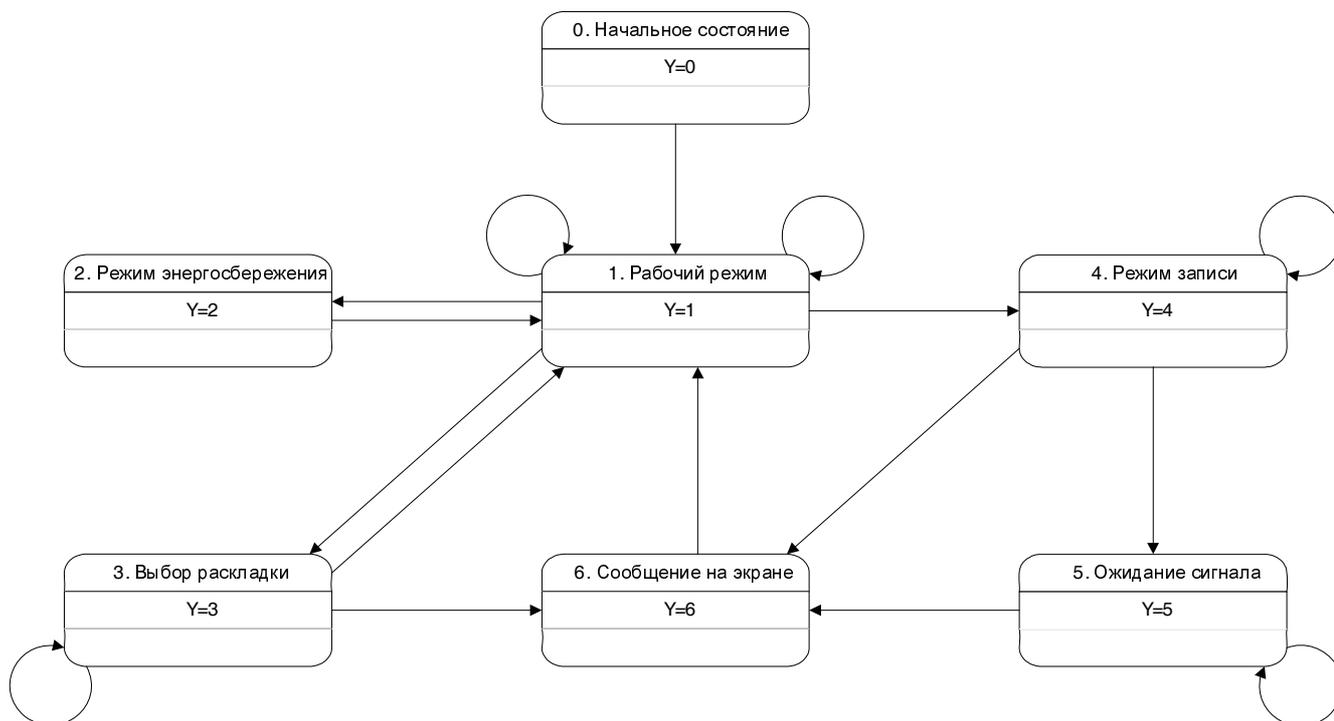
где AP — множество атомарных предложений.

CTL-моделью для множества состояний S называется тройка:

$$M = (S; R \subseteq S \times S; Label \subseteq S \times AP),$$

здесь R — тотальное отношение на множестве S (отношение переходов между состояниями), а Label — отношение, определяющее атомарные предложения, соответствующие каждому состоянию.

Множество выполняющих состояний алгоритм строит для каждой подформулы входной формулы (для каждого состояния создается список вы-



■ Рис. 8. Сокращенная модель ARemote (без событий и выходных переменных)

полненных в нем подформул). Идея алгоритма отражена в псевдокоде (рис. 9).

Как следует из рассмотрения текста этой программы, множество состояний, выполняющих формулу ϕ , строится индукцией по построению ϕ .

Будем считать для удобства, что из исходного графа Крипке построен симметричный ему граф, в котором все переходы заменены на противоположные. В алгоритме CES нетривиальными являются последние два шага, которые могут быть реализованы с помощью построения деревьев «обратных путей» и определением компонент сильной связности у графа модели.

Теперь осталось только дополнить этот алгоритм методами *предоставления подтверждений* истинности формул в моделях. Иными словами, требуется построить способ генерации сценариев.

Алгоритм генерации сценария для STL-формулы f в модели Крипке. Итак, требуется показать, что в данном состоянии s модели M выполняется (или не выполняется) формула f .

1. Если f — атомарное предложение, то предъявим описание состояния s в модели M — множество его атомарных предложений. В нем, в частности, содержится информация о выполняемости формулы f в данном состоянии s .

2. Доказательство $\neg f$ сводится к опровержению формулы f и наоборот.

3. Для доказательства формулы $f \vee g$ докажем одну из формул f или g , а для опровержения — опровергаем обе формулы f и g .

4. Для доказательства $EX f$ предъявим вершину в модели Крипке, в которую из вершины s имеется переход и которая выполняет f . Такая вершина обязательно существует, иначе на этапе верификации не обнаружилось бы, что формула $EX f$ верна. Опровержение $EX f$ (доказательство $AX \neg f$) подтверждается весьма просто, так как *любой* переход, который ведет из вершины s , будет вести только в вершину, выполняющую $\neg f$. Таким образом, любой переход из этой вершины можно предъявить пользователю в качестве опровержения.

5. Доказательство формул $E[f U g]$ и $EG f$ выполняется рекуррентным способом с использова-

```

function Sat( $\phi$ : Formula): set of State;
begin
if  $\phi = 1$       → return  $S$ 
 $\phi = 0$       → return  $\emptyset$ 
 $\phi \in AP$     → return  $\{s \mid Label(s, \phi)\}$ 
 $\phi = \neg \phi_1$  → return  $S \setminus Sat(\phi_1)$ 
 $\phi = \phi_1 \vee \phi_2$  → return  $Sat(\phi_1) \cup Sat(\phi_2)$ 
 $\phi = EX \phi_1$   → return  $\{s \in S \mid \exists (s, s') \in R \mid s' \in Sat(\phi_1)\}$ 
 $\phi = E[\phi_1 U \phi_2]$  → return  $Sat_{EU}(\phi_1, \phi_2)$ 
 $\phi = EG \phi_1$   → return  $Sat_{EG}(\phi_1)$ 
end if
end
    
```

■ Рис. 9. Индукция по построению формулы в алгоритме CES

нием пп. 1–4. Выполним рекуррентное разложение для этих формул:

$$E[f U g] = g \vee f \wedge EX E[f U g]$$

$$EG f = f \wedge EX EG f.$$

Тогда для доказательства формулы $E[f U g]$ достаточно построить путь в графе, применяя шаг за шагом пп. 1–4 к рекуррентному разложению этой формулы до тех пор, пока не попадем в вершину, выполняющую g .

Для доказательства формулы $EG f$ сделаем то же самое, пока не попадем в вершину, в которой уже были. Путь в этом случае, начиная с некоторого состояния, становится периодическим (рис. 10).

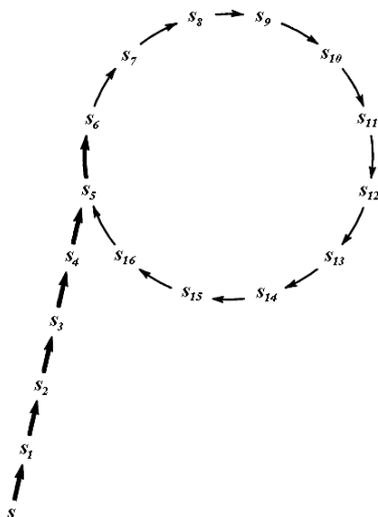
Опровержение формул $E[f U g]$ и $EG f$ выполняется аналогично опровержению формулы $EX f$. Любой (бесконечный) путь, который начинается в текущей вершине, можно предъявить пользователю для рассмотрения, так как путь не выполняет введенную формулу. Иначе говоря, вместо доказательства более выразительных CTL^* -формул $A-[f U g]$ и $A-EG f$ следует доказывать формулы $E-[f U g]$ и $E-EG f$. Проще всего предъявлять пути, замыкающиеся, начиная с некоторого состояния, в цикл, так как такие пути однозначно задаются конечным числом вершин.

На этом изложение алгоритма завершено.

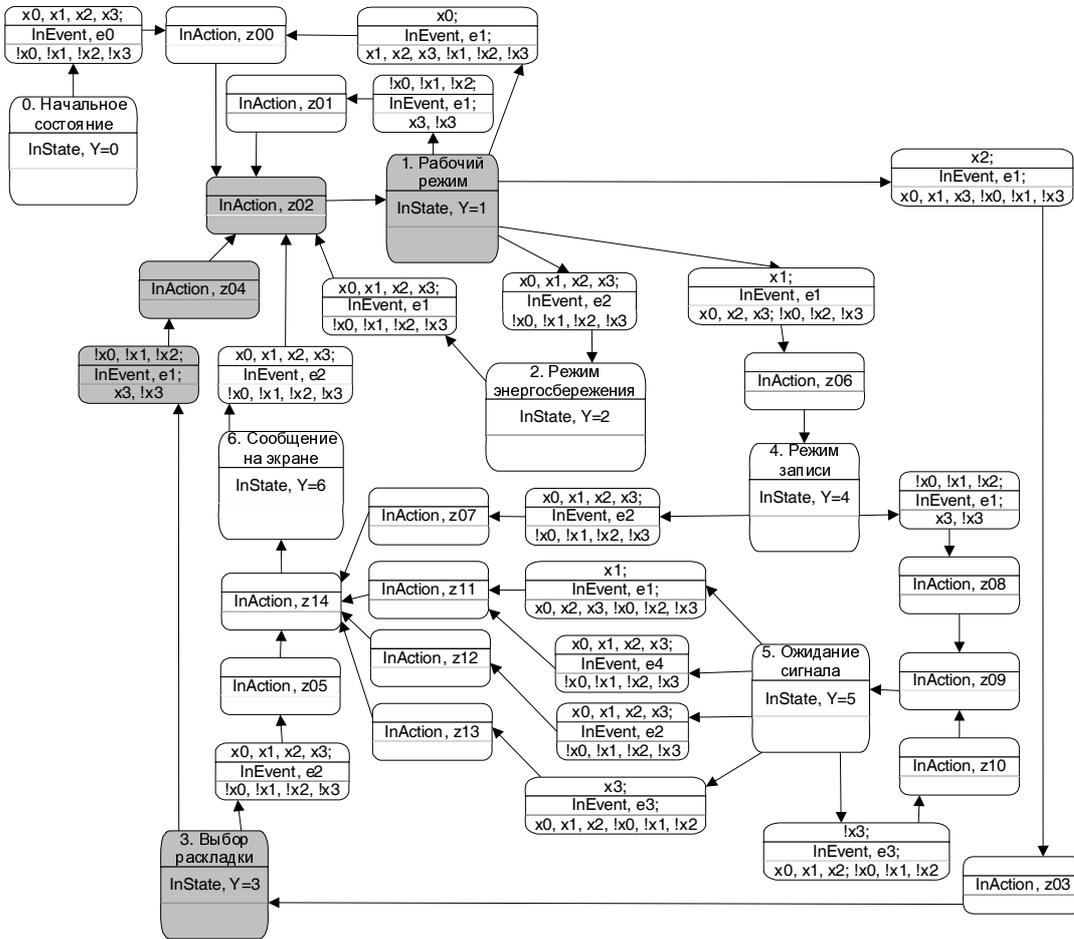
Анализ построенного алгоритма формирования сценариев, а также семантики языка CTL позволяет сформулировать следующее утверждение.

Утверждение. Если в модели Крипке существует бесконечный путь, выполняющий заданную CTL -формулу или являющийся контрпримером к ней, то существует и путь «в ρ -форме» (аналогично, выполняющий или опровергающий ее), представимый в виде объединения «предциклической» и «циклической» частей (см. рис. 10).

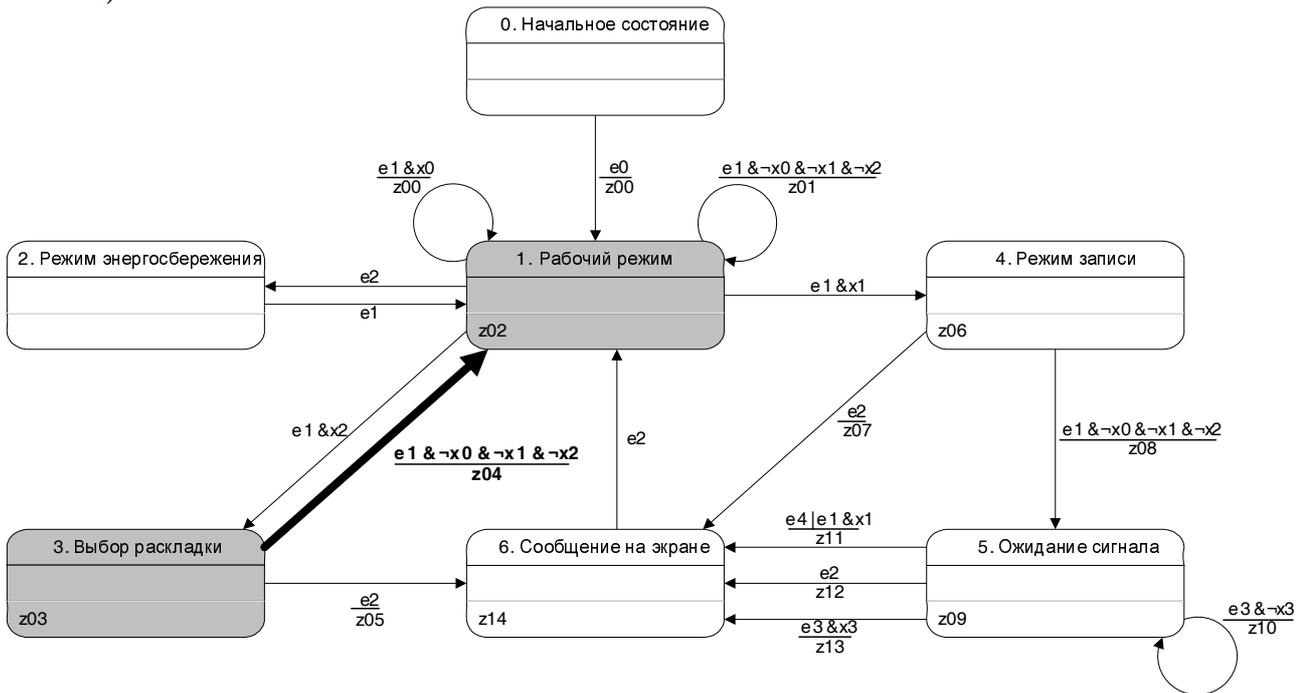
Доказательство этого утверждения является конструктивным и целиком опирается на приме-



a)



b)



■ Рис. 11. Контрпример: а — путь в модели Крипке; б — путь в автомате Мулли

в состоянии Z не выполняется. Верификатор сгенерировал (кратчайший и единственный в данном случае) контрпример, который на рис. 11, *a* выделен серым цветом. Это конечный путь, любое продолжение которого удовлетворяет формуле $\neg E[\neg(Y = 6)U(Y = 1)]$.

Этот же путь, но представленный в исходном автомате, приведен на рис. 11, *б*.

В случае, когда при моделировании выполнялась композиция автоматов/моделей Крипке, независимая нумерация их состояний позволит для каждого перехода в пути, представленном в окончатальной модели, однозначно решить вопрос, в какой именно индивидуальной компоненте системы взаимодействующих автоматов произошел переход. Это, опять же, дает возможность отобразить путь на модели в путь на исходном автомате.

Заключение

В работе были предложены методы для моделирования автомата Мили структурами Крипке. Был разработан алгоритм для построения сценариев и их интерпретации в исходном автомате. В связи с созданием этого алгоритма было сформулировано утверждение, позволяющее привести все сценарии к общему виду.

Составление сценариев (в том числе, контрпримеров) с помощью верифицирующих инструментов

позволяет проводить исследования в области автоматической или интерактивной коррекции модели или автомата с целью удовлетворить предъявляемым условиям. Например, если программа-верификатор предъявила путь, опровергающий некоторое желательное свойство для системы, она может предложить разработчику исказить/ликвидировать этот путь, например, за счет удаления какого-либо перехода. При этом, разумеется, не гарантируется, что в модели тогда не возникнет других противоречий со спецификацией, хотя не исключается возможность и более интеллектуальной коррекции.

Исходя из изложенного можно кратко сформулировать основные достоинства автоматных программ в части их верификации [19].

1. Класс автоматных программ является наиболее удобным для верификации методом *Model Checking*, так как в этом случае модель программы может быть автоматически построена по спецификации ее поведения, задаваемой в общем случае системой взаимодействующих конечных автоматов, в то время как для программ других классов модель приходится строить вручную.

2. Структура автоматных программ, в которых функции входных и выходных воздействий почти полностью отделены от логики программ, делает практичным верификацию этих функций на основе формальных доказательств с использованием пред- и постусловий [20, 21].

Литература

1. Джексон Д. Программы проверяют программы // В мире науки. 2006. № 10. С. 52–57.
2. Вудкок Дж. Первые шаги к решению проблемы верификации программ // Открытые системы. 2006. № 8. С. 36–57.
3. Katoen J.-P. Concepts, Algorithms, and Tools for Model Checking. Lehrstuhl für Informatik VII, Friedrich-Alexander Universität Erlangen-Nürnberg. Lecture Notes of the Course (Mechanised Validation of Parallel Systems) (course number 10359). Semester 1998/1999.
4. Шалыто А. А. SWITCH-технология. Алгоритмизация и программирование задач логического управления. СПб.: Наука, 1998. <http://is.ifmo.ru/books/switch/1>
5. Шалыто А. А. Логическое управление. Методы аппаратной и программной реализации. СПб.: Наука, 2000. http://is.ifmo.ru/books/log_upr/1
6. Кузьмин Е. В., Соколов В. А. Верификация автоматных программ с использованием LTL // Моделирование и анализ информационных систем / ЯрГУ. Ярославль. 2007. № 1. С. 3–14. <http://is.ifmo.ru>, раздел «Верификация».
7. Finite state machine. http://en.wikipedia.org/wiki/Finite_state_machine
8. Mealy machine. http://en.wikipedia.org/wiki/Mealy_machine
9. Moore machine. http://en.wikipedia.org/wiki/Moore_machine
10. Sebastiani R. Introduction to Formal Methods, 2005–2006. http://dit.unitn.it/~rseba/DIDATTICA/fm2005/02_transition_systems.pdf
11. Margaria T. Model Structures. Service Engineering – SS06. <https://www.cs.uni-potsdam.de/sse/teaching/ss06/sveg/ps/2-ServEng-Model-Structures.pdf>
12. Roux C., Encrenaz E. CTL May Be Ambiguous when Model Checking Moore Machines. UPMC LIP6 ASIM. CHARME, 2003. <http://sed.free.fr/cr/charme2003-presentation.pdf>
13. Hull R. Web Services Composition: A Story of Models, Automata and Logics. Bell Labs, Lucent Technologies, 2004. <http://edbtss04.dia.uniroma3.it/Hull.pdf>
14. Миронов А. М. Математическая теория программных систем. <http://intsys.msu.ru/study/mironov/mthprogsys.pdf>
15. Сайт проекта UniMod. <http://unimod.sf.net>
16. Сайт eVeloopers Corporation. <http://www.evelopers.com>
17. Вельдер С. Э., Бедный Ю. Д. Универсальный инфракрасный пульт для бытовой техники: Курсовая работа / СПбГУ ИТМО, 2005. <http://is.ifmo.ru/projects/irrc/>
18. Clarke E. M., Emerson E. A., Sistla A. P. Automatic Verification of Finite-State Concurrent Using Temporal Logic Specifications // ACM Transactions on Programming Languages and Systems (TOPLAS). 1986. Vol. 8. N 2. P. 244–263.
19. Switch-technology. <http://en.wikipedia.org/wiki/Switch-technology>
20. Дейкстра Э. Заметки по структурному программированию // Дал У., Дейкстра Э., Хоор К. Структурное программирование. М.: Мир, 1975.
21. Мейер В. Объектно-ориентированное конструирование программных систем. М.: Русская редакция, 2005.

УДК 681.324:681.326

РЕШЕНИЕ ЗАДАЧИ ВЫБОРА ОПТИМАЛЬНОГО ВАРИАНТА КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ С ПОМОЩЬЮ МЕТОДА ЭКСПЕРТНОГО ОЦЕНИВАНИЯ

Т. В. Молдованин,
аспирант
Российский университет дружбы народов

Рассмотрен один из подходов к выбору оптимального варианта комплексной защиты информации на примере информационно-управляющей системы предприятия, основанный на экспертной оценке. Рассмотрены задачи оценки степени согласованности экспертных суждений и способы улучшения этой согласованности.

The problem of information complex security optimal variant selection by the example of information-controlling system of enterprise is given in this work. The group expertise is used for reliability support of evaluation results. Problems of dimension of agreement evaluation of expert evaluations and improvement of this agreement are also given in this work.

Введение

Основной характеристикой информационно-управляющей системы (ИУС) предприятия является ежедневное обеспечение сотрудников необходимым и достаточным для выполнения служебных обязанностей информационным сервисом. Число ежедневно обрабатываемой информации, гибкость технологии и скорость ее аналитической обработки требуют активного взаимодействия и высочайшего уровня надежности, а также квалифицированно построенной системы защиты. Задача усложняется сложностью структуры, которая является территориально-распределенной за счет наличия отдаленных площадок.

Описание ИУС предприятия

Рассматривается задача выбора оптимального варианта комплексной защиты информации информационно-управляющей системы конкретного предприятия. ИУС предприятия представляет собой сложный взаимоувязанный комплекс средств, призванный решать задачи оперативного управления технологическими процессами и процессами учета (рисунок). Среда передачи данных (Ethernet и Internet) является одним из ключевых звеньев при анализе степени защищенности ИУС. Использование технологий передачи данных просто невозможно без обеспечения надежной сетевой защиты каждого компьютера в отдельности.

При этом трудно достигнуть гарантий безопасности только путем шифрования отдельных ви-

дов трафика или использования только межсетевых экранов и систем обнаружения атак, устанавливаемых на границах сетей. Единственным способом, позволяющим обеспечить высокий уровень безопасности работы компьютеров в сети в этих условиях, является реализация максимального уровня контроля над всем трафиком, поступающим в компьютер извне, и его шифрование при соединениях с другими компьютерами.

Анализ степени защищенности ИУС предприятия

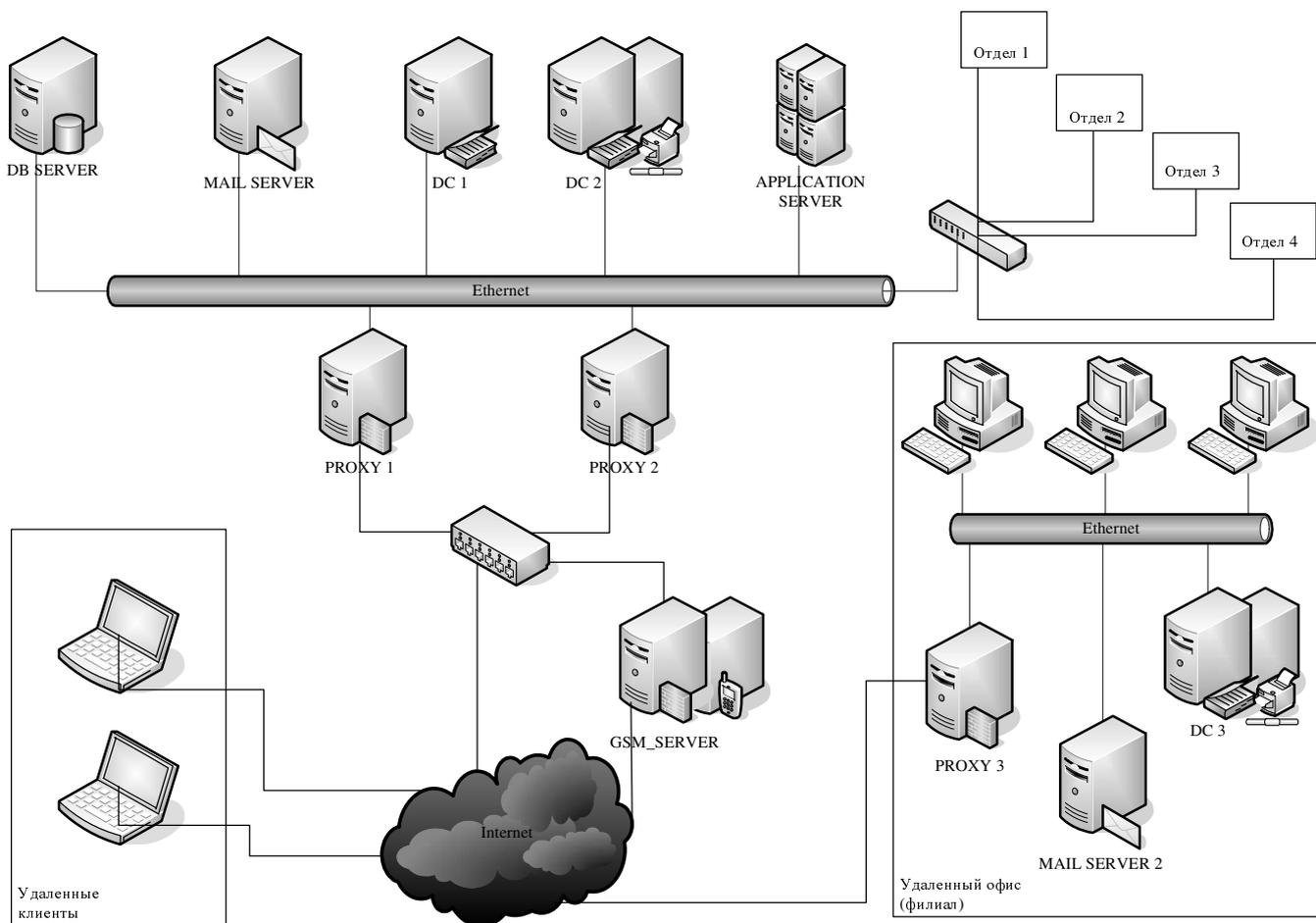
Анализ степени защищенности ИУС предприятия осуществлялся сотрудниками информационного отдела, выступающими в качестве экспертов, которым предложили оценить методом ранжирования следующие угрозы информационной безопасности.

1. Неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных, и т. п.).

2. Неправомерное отключение оборудования или изменение режимов работы устройств и программ.

3. Неумышленная порча носителей информации.

4. Запуск технологических программ, способных при некомпетентном использовании вызвать



■ *Схема ИУС предприятия*

потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения (форматирование или реструктуризацию носителей информации, удаление данных и т. п.).

5. Нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходом ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях).

6. Заражение компьютера вирусами.

7. Неосторожные действия, приводящие к разглашению конфиденциальной информации или делающие ее общедоступной.

8. Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т. д.).

9. Проектирование архитектуры системы, технологии обработки данных, разработка приклад-

ных программ с возможностями, представляющими опасность для работоспособности системы и безопасности информации.

10. Игнорирование организационных ограничений (установленных правил) при работе в системе.

11. Вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т. п.).

12. Некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности.

13. Пересылка данных по ошибочному адресу абонента (устройства).

14. Ввод ошибочных данных.

15. Неумышленное повреждение каналов связи.

16. Физическое разрушение системы (путем взрыва, поджога и др.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т. п.).

17. Отключение или вывод из строя подсистем обеспечения функционирования вычислительных

систем (электропитания, охлаждения и вентиляции, линий связи и т. д.).

18. Действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т. п.).

19. Внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность).

20. Вербовка (путем подкупа, шантажа и т. п.) персонала или отдельных пользователей, имеющих определенные полномочия.

21. Применение подслушивающих устройств, дистанционная фото- и видеосъемка и т. д.

22. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и др.).

23. перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему.

24. Хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ).

25. Несанкционированное копирование носителей информации.

26. Хищение производственных отходов (распечаток, записей, списанных носителей информации и т. п.).

27. Чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств.

28. Чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме, воспользовавшись недостатками мультизадачных операционных систем и систем программирования.

29. Незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т. д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»).

30. Несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т. п.

31. Вскрытие шифров криптозащиты информации.

32. Внедрение аппаратных спецвложений, программных «закладок» и «вирусов» («тройных коней» и «жучков»), т. е. таких участков программ, которые не нужны для осуществления за-

явленных функций, но позволяют преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы.

Для определения наибольшей угрозы вычислялось среднее значение \tilde{x}_i места i -угрозы, σ_i^2 — среднеквадратичное отклонение i -угрозы от ее среднего значения \tilde{x}_i по формулам¹:

$$\tilde{x}_i = \frac{1}{m} \sum_{j=1}^m c_{ij},$$

$$\sigma_i^2 = \frac{1}{(m-1)} \sum_{j=1}^m (c_{ij} - \tilde{x}_i)^2.$$

По всем i -угрозам выставлены предварительные ранги r . Все данные сведены в табл. 1.

Для повторного ранжирования вычислялись коэффициенты компетентности экспертов

$$\alpha_j = \frac{1}{D_j} \sum_{j=1}^m \frac{1}{D_j}$$

на основе ранговой корреляции по формуле Спирмена

$$\rho_j = 1 - \frac{6}{n(n^2 - 1)} D_j,$$

где $D_j = \sum_{i=1}^n d_{ij}^2$, $d_{ij} = r_i - c_{ij}$.

С помощью коэффициентов ранговой корреляции повторно вычислялись среднее значение \tilde{x}_i^* места i -угрозы и σ_i^{*2} — среднеквадратичное отклонение i -угрозы от ее среднего значения \tilde{x}_i^* :

$$\tilde{x}_i^* = \sum_{j=1}^m \alpha_j c_{ij},$$

$$(\sigma_i^*)^2 = \sum_{j=1}^m \alpha_j (c_{ij} - \tilde{x}_i^*)^2.$$

Формирование окончательных рангов (с учетом компетентности экспертов) проводилось по формуле

$$\gamma_i = \frac{1}{r_i^*} \sum_{i=1}^n \frac{1}{r_i^*}.$$

Были получены весовые коэффициенты каждой угрозы (табл. 2).

¹ Конеев И. Р. Информационная безопасность предприятия. СПб.: БХВ Петербург, 2003. 733 с.

■ *Таблица 1. Первичное ранжирование*

Угроза	Эксперт					\bar{x}_i	σ_i^2	r
	1	2	3	4	5			
1	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
2	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
3	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
4	7	8	7	7	7	7,20	0,20	8
5	7	8	7	7	7	7,20	0,20	8
6	27	27	27	27	27	27,00	0,00	27
7	11	11	11	11	11	11,00	0,00	11
8	7	4	7	7	7	6,40	1,80	4,5
9	2	2	2	2	2	2,00	0,00	2
10	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
11	7	5	7	7	7	6,60	0,80	4,5
12	7	8	7	7	7	7,20	0,20	8
13	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
14	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
15	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
16	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
17	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
18	16,5	16,5	16,5	16,5	16,5	16,50	0,00	16,5
19	27	27	27	27	27	27,00	0,00	27
20	27	27	27	27	27	27,00	0,00	27
21	27	27	27	27	27	27,00	0,00	27
22	27	27	27	27	27	27,00	0,00	27
23	3	3	3	3	3	3,00	0,00	3
24	27	27	27	27	27	27,00	0,00	27
25	27	27	27	27	27	27,00	0,00	27
26	27	27	27	27	27	27,00	0,00	27
27	27	27	27	27	27	27,00	0,00	27
28	27	27	27	27	27	27,00	0,00	27
29	7	8	7	7	7	7,20	0,20	8
30	7	8	7	7	7	7,20	0,20	8
31	1	1	1	1	1	1,00	0,00	1
32	27	27	27	27	27	27,00	0,00	27

■ Таблица 2. Повторное ранжирование

Угроза	\tilde{x}_i^*	$\tilde{x}_i^* + \tilde{\sigma}_i^2$	r	α
1	16,50	17,16	16,5	0,02
2	16,50	17,16	16,5	0,02
3	16,50	17,16	16,5	0,02
4	7,74	8,41	8	0,03
5	7,74	8,41	8	0,03
6	27,00	27,66	27	0,01
7	11,00	11,66	11	0,02
8	4,77	5,43	4	0,06
9	2,00	2,66	2	0,12
10	16,50	17,16	16,5	0,02
11	5,51	6,17	5	0,05
12	7,74	8,41	8	0,03
13	16,50	17,16	16,5	0,02
14	16,50	17,16	16,5	0,02
15	16,50	17,16	16,5	0,02
16	16,50	17,16	16,5	0,02
17	16,50	17,16	16,5	0,02
18	16,50	17,16	16,5	0,02
19	27,00	27,66	27	0,01
20	27,00	27,66	27	0,01
21	27,00	27,66	27	0,01
22	27,00	27,66	27	0,01
23	3,00	3,66	3	0,8
24	27,00	27,66	27	0,01
25	27,00	27,66	27	0,01
26	27,00	27,66	27	0,01
27	27,00	27,66	27	0,01
28	27,00	27,66	27	0,01
29	7,74	8,41	8	0,03
30	7,74	8,41	8	0,03
31	1,00	1,66	1	0,25
32	27,00	27,66	27	0,01

Алгоритм расчета индекса согласованности в задачах группового выбора и принятия решений и улучшение согласованности суждений в нечетком экспертном оценивании

Одной из важнейших задач принятия решений является выбор множества наилучших объектов (критериев) из заданной совокупности с помощью экспертов. Для обеспечения надежности результатов оценивания обычно используется групповая экспертиза. В этом случае возникают задачи оценки степени согласованности экспертных суждений и улучшения этой согласованности.

В работе предлагается новый конструктивный алгоритм вычисления индекса согласованности, основным отличием которого от известных подходов является простота математической формулировки и использование при вычислениях стандартных линейно-алгебраических операций. Разложение матрицы ранговых экспертных оценок A размером $n \times m$ ($n \leq m$) по сингулярным числам определяется соотношениями

$$A = U \sum V^T, U^{-1} = U^T, V^{-1} = V^T. \quad (1)$$

Уравнение $A = U \sum V^T$ можно переписать в виде

$$A = \sigma_1 P_1 + \sigma_2 P_2 + \dots + \sigma_n P_n, \quad (2)$$

где $P_i = u_i v_i^T$ — матрица ранга 1 — есть внешнее произведение столбца матрицы U и соответствующего столбца матрицы V .

Предлагается в качестве индекса согласованности экспертных суждений использовать соотношение

$$IC = \|\sigma_1 P_1\|_2 / \|A\|_2 = \sigma_1^2 / \sum \sigma_i^2, \quad (3)$$

причем если A — согласованная матрица ранговых экспертных оценок, то при этом ранг матрицы A равен 1, $A = u_1 \sigma_1 v_1^T$ и $IC = 1$, а для несогласованных матриц $IC < 1$.

Ввиду большой трудоемкости нахождения индекса согласованности по соотношению (1) с использованием разложения матрицы A по сингулярным числам разработан эффективный итерационный алгоритм, позволяющий на порядок уменьшить вычислительные затраты. Особенности данного алгоритма:

- находятся наибольшие сингулярные числа и соответствующие им правые и левые сингулярные векторы (сингулярные тройки) с использованием модификации степенного метода для собственных значений симметричной матрицы;

- поочередно, начиная с первого, находятся слагаемые соотношения (2), при этом производится последовательное уменьшение ранга матрицы, получаемой как разность между A и суммой найденных членов ряда для A ;

- на каждом шаге выполняется ортогонализация рассчитанных сингулярных векторов к ранее найденным сингулярным подпространствам;

- используются 2 критерия окончания вычислительного процесса (нахождение первых k сингулярных троек и/или достижение заданной степени аппроксимации исходной матрицы).

Предлагаемый алгоритм является конструктивным в том смысле, что в результате вычислений, кроме индекса согласованности, находятся и векторы ранжирования альтернатив и критериев, в качестве которых используются нормализованные сингулярные векторы v_1 и u_1 соответственно.

Для улучшения согласованности суждений в нечетком экспертном оценивании предлагается итерационный алгоритм, включающий следующие шаги (этапы):

- 1) нахождение по соотношениям (1) и (2) наилучшей аппроксимации матрицы A матрицей ранга 1 в смысле метода наименьших квадратов, являющейся согласованной матрицей экспертных суждений (МЭС);

- 2) расчет среднего отклонения элементов исходной матрицы A от найденной ближайшей согласованной МЭС;

- 3) отнесение к достоверным суждения исходной МЭС, величина которых превышает величину сред-

него отклонения, и замену недостоверных суждений в матрице A оценками равной важности;

- 4) повторное выполнение этапов 1–3 до достижения заданной величины индекса согласованности МЭС.

Заключение

В результате экспертизы анализа степени защищенности ИУС предприятия выделены следующие угрозы, которые имеют весовой коэффициент $\alpha \geq 0,7$:

- вскрытие шифров криптозащиты информации;

- проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему.

Из данных анализа угроз, проведенного экспертами предприятия, следует, что первостепенной задачей эффективного построения системы защиты информации является выбор метода шифрования.

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (80x@mail.ru).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию. Рукописи не возвращаются.

Редакция журнала напоминает, что ответственность за достоверность и точность рекламных материалов несут рекламодатели.

УДК 621.396.24

ПРОСТРАНСТВЕННОЕ МУЛЬТИПЛЕКСИРОВАНИЕ С СУБСИМВОЛЬНЫМ ВРЕМЕННЫМ СДВИГОМ МЕЖДУ ПЕРЕДАЮЩИМИ АНТЕННАМИ

И. В. Кацов,
разработчик

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Предлагается метод пространственного мультиплексирования с субсимвольным временным сдвигом, который позволяет реализовать высокоскоростную передачу в беспроводных системах с малым количеством антенн. Высокая скорость предложенных пространственно-временных кодов позволяет использовать помехоустойчивое кодирование без расширения полосы частот или увеличения значности модуляции. Рассмотрены вычислительно простые алгоритмы декодирования предложенных кодов.

Spatial multiplexing with transmit antennas subsymbol time delay is a novel technique for high-throughput wireless MIMO systems with small receive antenna arrays. The high rate of proposed space-time codes provides error-correction coding usage without spectral band expansion or signal constellation expansion. Effective equalization algorithms with low computational complexity are also proposed for new codes.

Введение

На протяжении последних лет в области многоантенной связи (MIMO — multiple in multiple out) было получено большое число результатов как в теории, так и в построении конкретных методов и алгоритмов передачи данных [1, 2]. Использование дополнительных антенн на передающей и приемной стороне позволяет либо уменьшить вероятность ошибки за счет пространственного разнесения передаваемых символов, либо увеличить скорость передачи за счет использования пространственного мультиплексирования передаваемых потоков данных с последующим их разделением на приемной стороне.

Методы разнесения на стороне передатчика описаны в работах по пространственно-временному кодированию [3–5]. Поскольку пространственно-временные коды имеют высокую избыточность, то их использование, как правило, ограничивается низкоскоростными режимами систем связи. Если же необходимо использовать и внешнее кодирование, то возникает дополнительная задача согласования скоростей внутреннего и внешнего кодов. При этом часто пространственно-временные коды оказываются слишком низкоскоростными, что не позволяет при фиксированной общей скорости эффективно использовать избыточность внешнего кода для повышения помехоустойчивости связи [6].

Методы декодирования пространственно мультиплексированных потоков данных были развиты в работах по алгоритмам BLAST [7, 8]. Высокая эффективность использования полосы частот этими методами обусловила высокую скорость передачи данных. Как следствие, были развиты методы введения избыточности в передаваемые данные средствами помехоустойчивого кодирования [9] и методы использования этой избыточности для эквализации принятых сигналов [10]. К сожалению, обычные алгоритмы BLAST неприменимы, если число приемных антенн меньше числа передающих антенн, что не всегда приемлемо на практике.

В работах [4, 11] был рассмотрен метод DD (delay diversity), использующий элементы сверточного кодирования. В статье [12] были предложены коды CGDD (circular generalized delay diversity), являющиеся развитием метода DD и понижающие сложность декодирования за счет своей регулярной структуры. Метод DD оказался эффективен и в условиях частотно-селективных замираний [12, 13]. Другим направлением техники DD стало семейство методов CCD (cyclic delay diversity), разработанных для использования в OFDM-системах и показавших высокую эффективность [14].

В данной работе предлагается методика пространственного мультиплексирования, основанная на субсимвольном сдвиге интервалов амплитудофазовой модуляции (АМ-ФМ) между передающими

ми антеннами (модуляция с субсимвольным сдвигом). Данный метод использует пространственно-временные матрицы с алгебраической структурой, близкой к CGDD и к кодам OSTBC (orthogonal space-time block code) [15], что позволяет принимать сигнал на малое количество антенн и производить его эффективную эквализацию. Близость предложенного метода к стандартным техникам пространственного мультиплексирования обеспечивает высокую скорость передачи в узкой полосе частот и возможность применения алгоритмов декодирования семейства BLAST и родственных им.

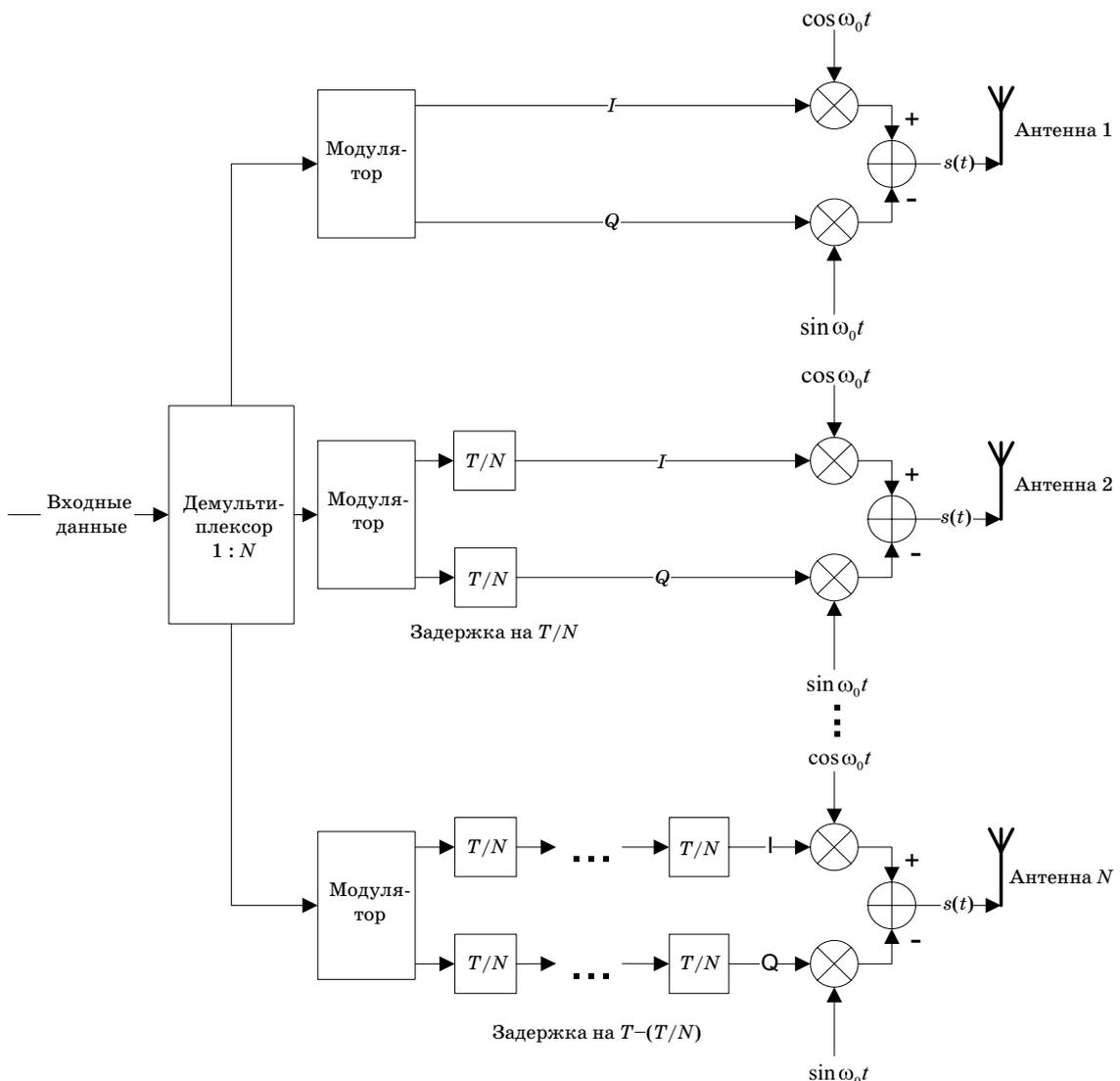
Коды с субсимвольным сдвигом

В большинстве алгоритмов MIMO используется АРК-модуляция. При этом каждый модуляционный символ представляет собой отрезок синусоиды, заданный своей фазой и амплитудой (частота ω_0 и длительность T символа предполагаются равными для всех символов). Переключение с одного символа на другой происходит одновременно для всех N передающих антенн. При этом каждая из приемных антенн не может получить более одной линейной комбинации переданных символов за период T .

При внесении сдвига между передающими антеннами на время T/N полоса сигнала не увеличивается, поскольку не меняется спектр

излучения каждой из передающих антенн. Общая схема такого передатчика представлена на рис. 1. При увеличении временного разрешения приемника до $1/(TN)$ субсимволов в секунду каждая из приемных антенн сможет получить N линейных комбинаций переданных субсимволов за период T . Под субсимволами будем понимать фрагменты символа, имеющие одинаковые фазу (или известную приемнику разность фаз, которая компенсируется перед декодированием) и амплитуду, а также в N раз меньшую длительность.

Передаваемые сигналы могут быть записаны в виде пространственно-временной матрицы, элементами которой являются субсимволы:



■ Рис. 1. Общая схема передатчика для модуляции с субсимвольным сдвигом

$$\mathbf{G} = \begin{pmatrix} \overline{g_{11}} & 0 & 0 & \dots & 0 \\ g_{11} & \overline{g_{12}} & 0 & \dots & 0 \\ g_{11} & g_{12} & \overline{g_{13}} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{11} & g_{12} & g_{13} & \dots & 0 \\ \overline{g_{11}} & \overline{g_{12}} & \overline{g_{13}} & \dots & \overline{g_{1N}} \\ g_{21} & \overline{g_{22}} & g_{23} & \dots & g_{2N} \\ g_{21} & g_{22} & \overline{g_{23}} & \dots & g_{2N} \\ g_{21} & g_{22} & g_{23} & \dots & g_{2N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \overline{g_{21}} & \overline{g_{22}} & \overline{g_{23}} & \dots & \overline{g_{2N}} \\ g_{31} & \overline{g_{32}} & g_{33} & \dots & g_{3N} \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}. \quad (1)$$

Каждый АМ-ФМ-символ $s_{ij} \in \mathbb{C}$ (i -й символ, поступивший на антенну номер j) представлен N субсимволами $g_{ij} \in \mathbb{C}$. Энергия каждого из субсимволов в N раз меньше энергии символа, т. е. $g_{ij} = s_{ij} / \sqrt{N}$. Код, заданный выражением (1), далее будем называть кодом с субсимвольным сдвигом (КСС).

В случае, когда матрица \mathbf{G} имеет высоту K символьных интервалов ($K \times N$ строк) и число приемных антенн равно M , принятые сигналы для модели псевдопостоянного ММО-канала без памяти с релеевскими замираниями можно представить следующим образом:

$$\mathbf{G} \times \mathbf{H} + \mathbf{N} = \mathbf{R}, \quad (2)$$

где $\mathbf{H} \in \mathbb{C}^{N \times M}$ и $\mathbf{R} \in \mathbb{C}^{KN \times M}$. Матрица \mathbf{N} представляет аддитивный белый гауссовый шум.

Структура кодов с субсимвольным сдвигом

Рассмотрим частный случай выражения (1) для двух передающих антенн:

$$\mathbf{G}_{2m-1} = \begin{pmatrix} g_1 & 0 \\ g_1 & g_2 \\ g_3 & g_2 \\ g_3 & g_4 \\ \vdots & \vdots \\ g_{2m-1} & g_{2m-2} \\ g_{2m-1} & 0 \end{pmatrix}. \quad (3)$$

Данный КСС имеет скорость $R = \frac{2m-1}{m}$, так как передает $2m-1$ символов за время mT . Поскольку декодирование блочных кодов для произвольного числа приемных антенн может быть сведено к разделному декодированию данных на каждой из антенн и их последующему объединению [2], то интерес представляет прием на одну антенну. В этом случае в выражении (2) матрица коэффициентов канала и матрица принятых значений представляют собой векторы-столбцы $\mathbf{H} = \mathbf{h} = (h_1 \ h_2)^T$, $\mathbf{R} = \mathbf{r} = (r_1 \dots r_{2m})^T$. Тогда уравнение (2) можно записать в виде выражения

$$\mathbf{\Omega} \mathbf{s} + \mathbf{N} = \mathbf{r}, \quad (4)$$

где $\mathbf{s} = (g_1 g_2 \dots g_{2m-2} g_{2m-1})^T$, а $\mathbf{\Omega} \in \mathbb{C}^{2m \times 2m-1}$ задается следующим образом:

$$\mathbf{\Omega} = \begin{pmatrix} h_1 & 0 & 0 & 0 & \dots & 0 & 0 \\ h_1 & h_2 & 0 & 0 & \dots & 0 & 0 \\ 0 & h_2 & h_1 & 0 & \dots & 0 & 0 \\ 0 & 0 & h_1 & h_2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & h_2 & 0 \\ 0 & 0 & 0 & 0 & \dots & h_2 & h_1 \\ 0 & 0 & 0 & 0 & \dots & 0 & h_1 \end{pmatrix}. \quad (5)$$

В работе [15] показано, что для OSTB-кодов аналогичная матрица является унитарной, т. е. ее произведение на свое эрмитово сопряжение является диагональной матрицей. Это свойство обеспечивает вычислительную простоту декодирования OSTB-кодов. Для матрицы, заданной равенством (5), $\mathbf{\Omega} \mathbf{\Omega}^H$ (H — эрмитово сопряжение) является тридиагональной матрицей (6).

$$\mathbf{\Omega} \mathbf{\Omega}^H = \begin{pmatrix} |h_1|^2 & |h_1|^2 & 0 & 0 & \dots & 0 & 0 \\ |h_1|^2 & |h_1|^2 + |h_2|^2 & |h_2|^2 & 0 & \dots & 0 & 0 \\ 0 & |h_2|^2 & |h_1|^2 + |h_2|^2 & |h_1|^2 & \dots & 0 & 0 \\ 0 & 0 & |h_1|^2 & |h_1|^2 + |h_2|^2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & |h_2|^2 & 0 \\ 0 & 0 & 0 & 0 & \dots & |h_1|^2 + |h_2|^2 & |h_1|^2 \\ 0 & 0 & 0 & 0 & \dots & |h_1|^2 & |h_1|^2 \end{pmatrix}. \quad (6)$$

Этот факт лежит в основе методов декодирования КСС, рассмотренных далее.

Алгоритмы декодирования

Очевидно, что одним из возможных методов декодирования является алгебраическое решение системы уравнений (4) относительно вектора \mathbf{s} :

$$\hat{\mathbf{s}} = \mathbf{\Omega}^+ \mathbf{r}. \quad (7)$$

Вследствие введения временного сдвига между антеннами матрица Ω не является квадратной, и при решении уравнения (2) должно быть найдено ее псевдообращение [16] $\Omega^+ \in \mathbb{C}^{2m-1 \times 2m}$. Для случая псевдообращения по критерию нулевых взаимных помех (НВП) данная матрица

$$\Omega^+ = \frac{\text{diag}(h_1^{-1}, h_2^{-1}, h_1^{-1}, \dots, h_2^{-1}, h_1^{-1})}{2m} \times \begin{pmatrix} 2m-1 & 1 & -1 & 1 & \dots & -1 & 1 \\ -(2m-2) & 2m-2 & 2 & -2 & \dots & 2 & -2 \\ 2m-3 & -(2m-3) & 2m-3 & 3 & \dots & -3 & 3 \\ -(2m-4) & 2m-4 & -(2m-4) & 2m-4 & \dots & 4 & -4 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 3 & -3 & 3 & -3 & \dots & -(2m-3) & 2m-3 \\ -2 & 2 & -2 & 2 & \dots & 2m-2 & -(2m-2) \\ 1 & -1 & 1 & -1 & \dots & 1 & 2m-1 \end{pmatrix}. \quad (8)$$

Подстановка Ω^+ в выражение (7) дает следующие формулы для оценки чипов:

$$\hat{g}_k = \frac{1}{2mh_{2-(k \bmod 2)}} \left(\sum_{j=1}^k (2m-k)(-1)^{j+k} r_j + \sum_{j=k+1}^{2m} k(-1)^{j-k-1} r_j \right). \quad (9)$$

При обращении согласно критерию минимума среднеквадратичной ошибки (МСКО) выражение, подобное (9), может быть получено из соотношения $\Omega^+ = \Omega^H (\mathbf{I}_{2m} / \gamma + \Omega \Omega^H)^{-1}$, где γ — отношение сигнал/шум на приемнике.

Используя технику, аналогичную представленной в работе [7], можно улучшить оценки, полученные согласно (9).

На первом шаге производится выбор канала с максимальным коэффициентом усиления и гашение интерференции субсимволов, переданных по этому каналу, на субсимволы, передаваемые по другим каналам. Применительно к случаю, задаваемому выражением (2), производится вычисление вектора $\mathbf{r}^{(1)} = \mathbf{r} - \tilde{\mathbf{s}}v$, где $\tilde{\mathbf{s}} \in \mathbb{C}^{2m \times 1}$ и скаляр v определяются следующим образом:

$$\begin{aligned} &\text{при } |h_1| > |h_2| \\ &\tilde{\mathbf{s}} = \left(Q(\hat{g}_1) \quad Q(\hat{g}_1) \quad Q(\hat{g}_3) \quad Q(\hat{g}_3) \quad \dots \quad Q(\hat{g}_{2m-1}) \right)^T, \\ &v = h_1; \\ &\text{при } |h_1| < |h_2| \\ &\tilde{\mathbf{s}} = \left(0 \quad 0 \quad Q(\hat{g}_2) \quad Q(\hat{g}_2) \quad \dots \quad Q(\hat{g}_{2m-2}) \quad 0 \quad 0 \right)^T, \\ &v = h_2. \end{aligned} \quad (10)$$

Оператор $Q(\bullet)$ обозначает квантование с точностью до элементов сигнального созвездия. На втором шаге из матрицы Ω путем обнуления всех нечетных (если $|h_1| > |h_2|$) или четных (если $|h_1| < |h_2|$) столбцов формируется матрица $\Omega^{(1)}$. Вычисление псевдообратной матрицы $(\Omega^{(1)})^+$ легко выполняется в символьном виде благодаря разреженности $\Omega^{(1)}$. Уточненные оценки для субсимволов могут

быть найдены по формуле (7) путем умножения $(\Omega^{(1)})^+$ на $\mathbf{r}^{(1)}$; при этом малое число ненулевых элементов в $(\Omega^{(1)})^+$ приводит к простым окончательным формулам для улучшенных оценок субсимволов \tilde{g}_k (для псевдообращения по критерию НВП):

$$\begin{aligned} &\text{при } |h_1| > |h_2| \\ &\tilde{g}_k = (r_k^{(1)} + r_{k+1}^{(1)}) (2h_2)^{-1}, \\ &k \in \{2, 4, \dots, 2m-2\}, \\ &\tilde{g}_k = \hat{g}_k, \quad k \in \{1, 3, \dots, 2m-1\}; \\ &\text{при } |h_1| < |h_2| \\ &\tilde{g}_k = (r_k^{(1)} + r_{k+1}^{(1)}) (2h_1)^{-1}, \\ &k \in \{1, 3, \dots, 2m-1\}, \\ &\tilde{g}_k = \hat{g}_k, \quad k \in \{2, 4, \dots, 2m-2\}. \end{aligned} \quad (11)$$

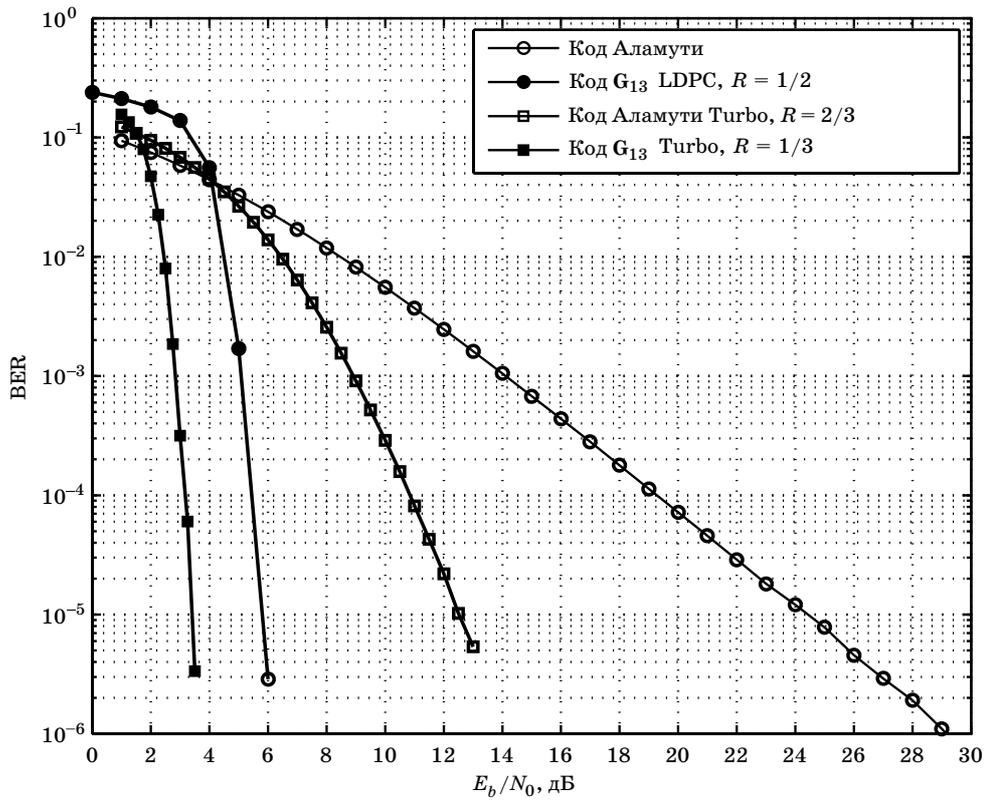
Результаты моделирования

Моделирование было произведено на основе псевдопостоянного ММО-канала без памяти с релейскими замираниями.

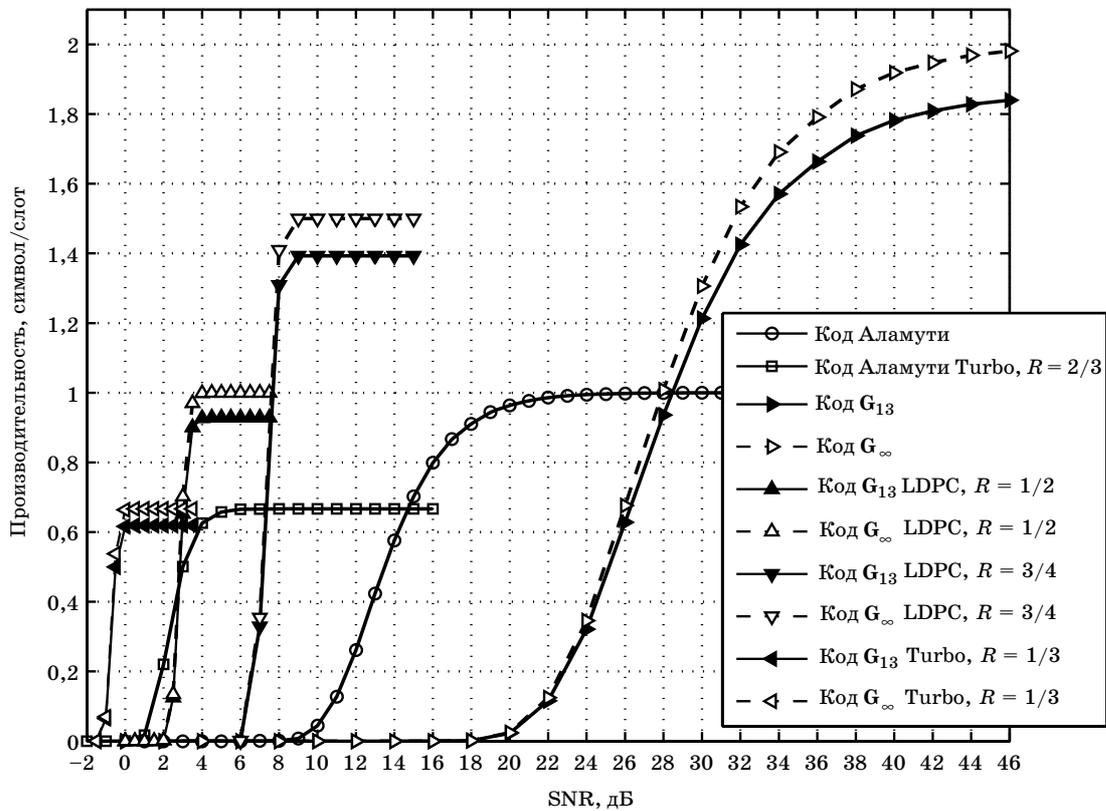
В качестве внешних помехоустойчивых кодов использовались LDPC-коды и турбокоды из стандартов 802.16e и 3GPP LTE; декодирование с мягким входом. При приеме на две антенны результаты декодирования объединялись по принципу MRC (maximum ratio combining).

Эффект от использования высокой скорости кода, определяемого выражением (3), для усиления помехоустойчивой защиты показан на рис. 2. По оси абсцисс отложено отношение энергии информационного бита (E_b) к спектральной плотности мощности аддитивного белого гауссового шума (N_0) в логарифмическом масштабе. Энергии на информационный бит и полосы сигналов для кода Аламути [17] и кода G_{13} при этом одинаковы; оба пространственно-временных кода декодировались переборным алгоритмом согласно критерию максимума правдоподобия (МП).

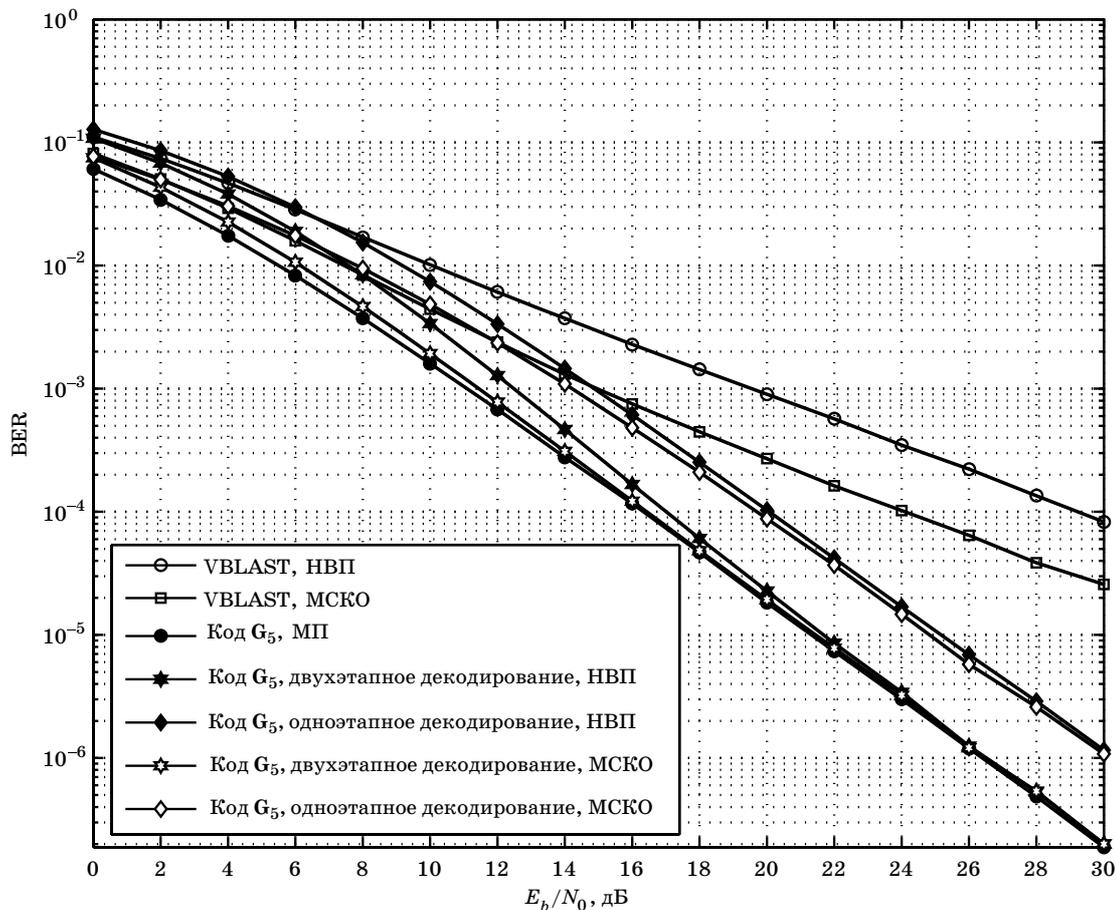
Поскольку речь идет о сравнении кодов с разной скоростью, то более наглядным является график результирующей скорости передачи



■ Рис. 2. Сравнение вероятности ошибки для кода Аламути и кода G_{13} ($N = 2, M = 1$, модуляция BPSK)



■ Рис. 3. Сравнение производительности кода Аламути и кода G_{13} ($N = 2, M = 1$, модуляция BPSK)



■ Рис. 4. Сравнение вероятности ошибки кода для алгоритма VBLAST и кода G_5 ($N = 2, M = 2$, модуляция BPSK)

данных (рис. 3). Обозначение G_∞ введено для асимптотической оценки производительности кода при длине блока, стремящейся к бесконечности, по оси абсцисс отложено отношение сигнал/шум (SNR — signal-to-noise ratio) в логарифмическом масштабе. Для КСС используется декодер на основе критерия МСКО с двухэтапным декодированием.

При наличии нескольких приемных антенн становится возможным использовать пространственное мультиплексирование. Алгебраические декодеры для КСС показывают более высокую эффективность в сравнении с алгоритмом VBLAST [7] и МП-декодированием (рис. 4).

Заключение

Рассмотрены пространственно-временные коды с субсимвольным сдвигом, которые позволяют реализовать пространственное мультиплексирование. Для предложенных кодов существуют непрерывные алгоритмы декодирования, по эффективности близкие к декодированию по максимуму правдоподобия. Моделирование показывает, что в сочетании с помехоустойчивым кодированием предложенные коды превосходят по эффективности ряд известных методов в широком диапазоне отношений сигнал/шум.

Литература

1. Kuhn V. Wireless communication over MIMO channels. New York: Wiley, 2006. 363 p.
2. Jafarkhani H. Space-Time Coding. Theory and Practice. Cambridge, U.K.: Cambridge Univ. Press, 2005. 302 p.
3. Tarokh V., Seshadri N., Calderbank A. R. Space-time codes for high data rate wireless communication:

- Performance criterion and code construction // IEEE Trans. Inf. Theory. Mar. 1998. Vol. 44. N 2. P. 744–765.
4. Wittneben A. A new bandwidth efficient transmit antenna modulation diversity scheme for linear digital modulation // Communications (ICC): Proc. Int. Conf. Geneva, Switzerland. May 1993. P. 1630–1634.
5. Jafarkhani H., Taherkhani F. Pseudo orthogonal designs as space-time block codes // IEEE Interna-

- tional Symposium on Advances in Wireless Communications (ISWC'02). Sept. 2002.
6. **Zheng L., Tse D.** Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels // IEEE Trans. Inform. Theory. May 2003. Vol. 49. N 5. P. 1073–1096.
 7. **Wolniansky P. W., Foschini G. J., Golden G. D., Valenzuela R. A.** VBLAST: an architecture for realizing very high data rates over the richscattering wireless channel, invited paper: Proc. ISSSE-98. Pisa, Italy. Sept. 29, 1998.
 8. **Choi W., Negi R., Cioffi J. M.** Combined ML and DFE decoding for the V-BLAST system: Communications IEEE International Conference. June 2000. Vol. 3. P. 1243–1248.
 9. **Minseok N., Kim N., Hyuncheol P., Hyuckjae L.** A variable rate LDPC coded V-BLAST system // Vehicular Technology Conference. Sept. 2004. Vol. 4. P. 2540–2543.
 10. **Sellathurai M., Haykin S.** TURBO-BLAST for wireless communications: theory and experiments // IEEE Transactions on Communications. Oct. 2002. Vol. 50. Issue: 10. P. 2538–2546.
 11. **Winters J. H.** A new bandwidth efficient transmit antenna modulation diversity scheme for linear digital modulation: Proc. IEEE'ICC. 1993. P. 1630–1634.
 12. **Gore D., Sandhu S., Paulraj A.** Delay diversity codes for frequency selective channels: Proc. IEEE Int. Conf. Communications (ICC). New York, May 2002. P. 1949–1953.
 13. **Hehn T., Schober R., Gerstacker W.** Optimized Delay Diversity for Frequency-Selective Fading Channels // IEEE Transactions on Wireless Communications. Sept. 2005. Vol. 4. P. 2289–2298.
 14. **Dammann A., Kaiser S.** Transmit/receive antenna diversity techniques for OFDM systems // European Transactions on Telecommunications. Sept. 2002. Vol. 13. N 5. P. 531–538.
 15. **Tarokh V., Jafarkhani H., Calderbank A. R.** Space-time Block Codes from Orthogonal Designs // IEEE Trans. Inform. Theory. 2000. Vol. 46. N 1. P. 314.
 16. **Watkins D.** Fundamentals of matrix computations. New York: Wiley, 2002. 618 p.
 17. **Alamouti S. M.** A simple transmitter diversity scheme for wireless communications // IEEE J. Select. Areas Commun. Oct. 1998. Vol. 16. P. 1451–1458.



Крук Е. А.

Комбинаторное декодирование линейных блочных кодов: монография / Е. А. Крук; ГУАП. — СПб., 2007. — 238 с.: ил. ISBN 978-5-8088-0247-6

В монографии рассмотрены вопросы комбинаторного декодирования линейных кодов в дискретных каналах. Дается введение в теорию общих методов декодирования, проводится асимптотический анализ сложности декодирования линейных блочных кодов. Основное внимание уделяется сложности декодирования «почти» по максимуму правдоподобия.

Рассматривается применение комбинаторных методов декодирования в задачах связи и защиты информации, в том числе нетрадиционное применение аппарата помехоустойчивого кодирования для сборки сообщений на транспортном уровне сети передачи данных с коммутацией пакетов.

Монография может быть использована студентами, обучающимися по специальности 090104, для самостоятельной работы и при выполнении заданий по НИР.

УДК 681.518

К ВОПРОСУ ОБ ОПТИМИЗАЦИИ ЗОНЫ ПОКРЫТИЯ СИСТЕМ СОТОВОЙ СВЯЗИ НА ЗАГОРОДНЫХ УЧАСТКАХ МЕСТНОСТИ

И. А. Зикратов,

доктор техн. наук, доцент

Т. В. Зикратова,

преподаватель

Санкт-Петербургское высшее военное училище радиоэлектроники

Обсуждаются вопросы рационального размещения ретрансляторов базовых станций сотовой связи на загородных участках местности с использованием цифровой картографической информации. Решение достигается путем представления целевой функции и ограничений задачи нелинейного программирования в виде эквивалентной задачи с булевыми переменными. Показано также, что задачу можно сформулировать как задачу стохастического программирования с вероятностными ограничениями.

The question of rational accommodation of basic cellular communication station retransmitters at the out-of-town surroundings using digital cartographical information are discussed. The decision is achieved by presentation of objective function and restriction of non-linear programming task in the kind of boolean values. It's shown also that the task can be formulated as stochastic programming one with restriction probabilities.

Интенсивное развитие операторов, предоставляющих услуги радиосвязи, приводит к необходимости рационального размещения на ограниченных площадях большого количества источников электромагнитных волн, как правило, различного частотного диапазона. Автоматизация расчета радиолиний с учетом влияния подстилающей поверхности стала возможной с появлением и широким внедрением в различных областях деятельности геоинформационных систем (ГИС), которые являются гибким и удобным инструментом для использования в ряде расчетных задач априорной цифровой картографической информации (ЦКИ) о земной поверхности.

В составе ЦКИ содержатся:

– метрическая информация о координатах точек, описывающих площадные, линейные и точечные объекты, представленная с определенной погрешностью;

– семантическая информация, которая содержит данные о характере местности и наличии на ней таких объектов как «река», «береговая линия», «дорога», «заболоченный участок леса» и т. д. в принятых форматах данных.

Использование ЦКИ в составе ГИС на базе вычислительных систем высокой производительности

дает возможность не только автоматизировать известные методы решения задач в какой-либо предметной области, но и позволяет разрабатывать и внедрять новые, более сложные, но эффективные алгоритмы информационно-расчетных задач различного назначения.

Основной процедурой при оптимизации позиций базовых станций является расчет зон устойчивого приема радиосигнала с учетом метрической и семантической информации о свойствах подстилающей земной поверхности, представленной в цифровых картах местности (ЦКМ). Для этого разработаны соответствующие модели земной поверхности и методы расчета напряженности электромагнитного поля в точке наблюдения [1, 2].

В результате решения информационно-расчетных задач, составляющих комплекс программ ГИС, определяется множество X координатных точек позиций, которые априорно удовлетворяют следующим основным условиям:

– диаграммы направленности антенн ретрансляторов должны охватывать предполагаемые места концентрации абонентов с учетом рельефа местности;

– обеспечивается электромагнитная совместимость источников электромагнитного излучения;

– обеспечивается возможность электроснабжения ретрансляторов и доступ к ним персонала и техники для удобства обслуживания базовых станций и т. д.

Из сформированного множества X координатных точек возможных позиций расположения базовых станций на некотором ограниченном участке местности площадью P необходимо выбрать минимальное количество N таких позиций, которые позволят расположенным на них базовым станциям обеспечить устойчивую связь в местах концентрации абонентов.

Решение задачи рационального расположения N базовых станций для городских условий сводится к отысканию такого множества точек установки, при котором будет обеспечена устойчивая связь в любой точке населенного пункта.

В пригородных участках местности службы связи стремятся обеспечить устойчивую связь, прежде всего, вблизи транспортных коммуникаций, пересекающих эти участки.

Положим, что на границах рассматриваемого участка зона покрытия достаточная. Тогда при выполнении условия

$$P \leq S', \quad (1)$$

где S' — площадь зоны покрытия, создаваемого одной базовой станцией, задача выбора ее места расположения тривиальна.

Если условие (1) не выполняется, задачу можно сформулировать следующим образом. Из множества X координатных точек возможного распо-

ложения базовых станций на заданном участке местности необходимо выбрать такое множество N ($N \subset X, N \rightarrow \min$), при котором любые точки всех трасс, пересекающих этот участок, будут находиться в зоне покрытия хотя бы одной базовой станции.

В рамках статьи подход к формализации и решению поставленной задачи нагляднее проиллюстрировать на элементарном примере.

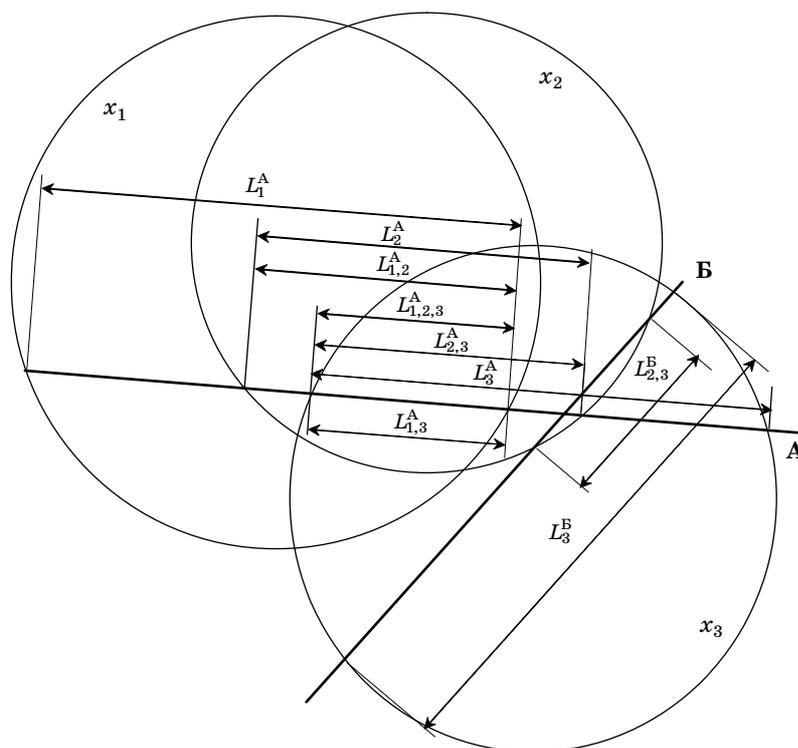
Пусть необходимо выбрать минимальное количество из трех возможных мест расположения на ограниченном участке местности базовых станций таким образом, чтобы обеспечить зону радиосвязи, охватывающую трассы А и Б. Суммарная протяженность трасс равна L_{Σ} . Обозначим возможные точки расположения на местности как x_1, x_2 и x_3 . Положим, что точки x_1, x_2, x_3 выбраны по результатам прогнозирования параметров зон покрытия на основе ЦКИ и удовлетворяют приведенным выше условиям. Зоны покрытия базовых станций x_1, x_2 и x_3 для наглядности аппроксимированы окружностями (рисунок).

Формализуем задачу.

Из постановки задачи следует, что x_1, x_2, x_3 могут принимать двоичные значения. Это означает, что физический смысл этих переменных следующий: если $x_j = 1$, то на i -й позиции ретранслятор установлен, если $x_j = 0$ — нет.

Тогда целевую функцию представим в виде

$$x_1 + x_2 + x_3 \rightarrow \min. \quad (2)$$



■ Зоны покрытия трасс А и Б диаграммами направленности базовых станций x_1, x_2, x_3

Пусть диаграмма направленности ретранслятора x_1 охватывает участок трассы А длиной L_1^A , ретранслятора x_2 — L_2^A и, соответственно, ретранслятора x_3 — L_3^A . По аналогии для трассы Б можно определить величины L_2^B и L_3^B . Кроме того, необходимо учесть, что часть трассы А пересекает места перекрытия диаграмм направленности ретрансляторов x_1 и x_2 , x_1 и x_3 , x_2 и x_3 . Длины этих участков соответственно обозначим как $L_{1,2}^A$, $L_{1,3}^A$ и $L_{2,3}^A$. Для трассы Б имеется один участок перекрытия диаграмм направленности ретрансляторов x_2 и x_3 , который обозначим $L_{2,3}^B$.

Следовательно, ограничение можно записать в виде полиномиальной функции

$$L_1^A x_1 + L_2^A x_2 + L_3^A x_3 + L_2^B x_2 + L_3^B x_3 - L_{1,2}^A x_1 x_2 - L_{1,2,3}^A x_1 x_2 x_3 - L_{1,3}^A x_1 x_3 - L_{2,3}^A x_2 x_3 - L_{2,3}^B x_2 x_3 \geq L_\Sigma. \quad (3)$$

Анализ полученного неравенства (3) показывает, что сформулированная задача сведена к задаче нелинейного программирования. В качестве ограничения отметим, что переменные x_1 , x_2 и x_3 могут принимать двоичные значения. В монографии [3] показано, что подобную задачу нелинейного программирования можно заменить эквивалентной линейной задачей с булевыми переменными.

Суть преобразований сводится к введению также булевых вспомогательных переменных, которыми замещают слагаемые исходного полинома. Так, вспомогательная переменная для k -го слагаемого полинома (3)

$$y_k = \prod_{j=1}^{n_k} x_j, \quad (4)$$

где n_k — количество сомножителей в k -м слагаемом. Для обеспечения условий $y_k = 1$ при всех $x_j = 1$ и $y_k = 0$ в противном случае на каждую переменную y_k накладываются очевидные ограничения

$$\sum_{j=1}^{n_k} x_j - (n_k - 1) \leq y_k; \quad (5)$$

$$\frac{1}{n_k} \sum_{j=1}^{n_k} x_j \geq y_k. \quad (6)$$

Используя формулу (4), введем переменные $y_1 = x_1 x_2$, $y_2 = x_1 x_2 x_3$, $y_3 = x_1 x_3$ и $y_4 = x_2 x_3$. После наложения дополнительных ограничений на эти переменные по формулам (5), (6) задачу можно записать в виде

$$x_1 + x_2 + x_3 \rightarrow \min \quad (7)$$

при следующих ограничениях:

$$L_1^A x_1 + L_2^A x_2 + L_3^A x_3 + L_2^B x_2 + L_3^B x_3 - L_{1,2}^A y_1 - L_{1,2,3}^A y_2 - L_{1,3}^A y_3 - y_4 (L_{2,3}^A + L_{2,3}^B) \geq L_\Sigma; \quad (8)$$

$$x_1 + x_2 - 1 \leq y_1; \quad (9)$$

$$x_1 + x_2 + x_3 - 2 \leq y_2; \quad (10)$$

$$x_1 + x_3 - 1 \leq y_3; \quad (11)$$

$$x_2 + x_3 - 1 \leq y_4; \quad (12)$$

$$\frac{1}{2}(x_1 + x_2) \geq y_1; \quad (13)$$

$$\frac{1}{3}(x_1 + x_2 + x_3) \geq y_2; \quad (14)$$

$$\frac{1}{2}(x_1 + x_3) \geq y_3; \quad (15)$$

$$\frac{1}{2}(x_2 + x_3) \geq y_4, \quad (16)$$

где $y_1, y_2, y_3, y_4, x_1, x_2, x_3$ — булевы переменные.

Алгоритмизация такой задачи для решения на ЭВМ существенно проще по сравнению с алгоритмизацией классических задач нелинейного программирования, решаемых, например, методом Лагранжа [4]. Это обусловлено отсутствием процедур дифференцирования, составления матриц и т. д.

Нетрудно рассчитать, что решением для нашего примера является вектор

$$\mathbf{X} = \{1, 0, 1\}, \quad (17)$$

где $x_1 = 1, x_2 = 0, x_3 = 1$, т. е. для обеспечения связи на трассах А и Б достаточно разместить базовые станции в точках x_1 и x_3 .

Отсюда можно записать постановку задачи в общем виде.

Минимизировать

$$z = \sum_{j=1}^X x_j \quad (18)$$

при ограничении

$$\sum_{k=1, m=1}^{K, M} L_k^m x_j - \sum_{l=1, m=1}^{S, M} L_l^m y_l \geq L_\Sigma, \quad (19)$$

где K — количество участков трасс, охватываемых диаграммой направленности j -го ретранслятора; M — количество трасс, пересекающих участок местности; S — количество участков трасс, перекрываемых диаграммами направленности соседних ретрансляторов. Правила ввода переменных y_l и дополнительных ограничений, накладываемых на них, рассмотрены выше. Решением является \mathbf{X} -мерный вектор вида (17).

Можно показать, что, используя подобный подход, не составляет труда решить родственную задачу максимизации зоны покрытия коммуникаций на ограниченном участке местности заданным количеством S базовых станций.

При такой постановке задачи в качестве целевой функции следует полагать

$$\sum_{k=1, m=1}^{K, M} L_k^m x_j - \sum_{l=1, m=1}^{S, M} L_l^m y_l \rightarrow \max,$$

а в качестве ограничения записать $\sum_{j=1}^X x_j = C$.

Дальнейший порядок решения задачи аналогичен рассмотренному выше.

Однако следует учитывать, что сомножители $L_{k,l}^m$, входящие в состав функции ограничения, получены по результатам априорных расчетов характеристик направленности антенных систем ретрансляторов. На практике величина дальности радиосвязи зависит от множества влияющих факторов, большая часть из которых имеет стохастический характер. Кроме того, на точность расчета влияет точность исходного картографического материала, степень адекватности моделей подстилающей поверхности, методов расчета радиолинии, используемых в ГИС, и т. д. [5]. Отсюда следует, что $L_{k,l}^m$ необходимо рассматривать как случайные величины.

В этом случае задачу (7)–(16) следует рассматривать как одноэтапную задачу стохастического программирования с построчными вероятностными ограничениями. Решением такой задачи также является X -мерный детерминированный вектор. Учитывая, что на $L_{k,l}^m$ оказывает влияние большое число случайных независимых факторов, согласно центральной предельной теореме Ляпуно-

ва, эти величины можно полагать гауссовыми. Тогда задачу можно свести к задачам, рассмотренным в работах [3, 6].

Таким образом, основываясь на предварительных расчетах возможного расположения базовых станций операторов сотовой связи с использованием ЦКМ, можно реализовать относительно несложный алгоритм оптимального выбора их позиций без проведения предварительной топогеодезической обработки местности. При наличии в ГИС соответствующих расчетных модулей будет обеспечиваться минимизация затрат на приобретение и эксплуатацию ретрансляторов, требования к электромагнитной совместимости радиотехнических средств и т. д.

При разработке модуля ГИС выбора рационального размещения базовых станций целесообразно учитывать несколько замечаний.

1. ЦКМ изначально не ориентированы на решение задач в какой-либо предметной области, в частности электродинамики и распространения радиоволн, проектирования телекоммуникаций и т. д. Следовательно, разработчики ГИС должны предусмотреть возможность ввода дополнительной ЦКИ (метрической или семантической).

2. Учитывая, что ЦКМ обладает ошибками представления информации, природа возникновения которых различна, а также стохастический характер ряда факторов, влияющих на степень достоверности результатов расчетов, при разработке методов решения задач оптимизации в ГИС целесообразно использовать методы стохастического программирования.

Литература

1. Безлюдников О. Л. и др. Автоматизация анализа рельефа местности при расчете напряженности поля радиосигналов // Радиотехника. 2001. № 9. С. 86–88.
2. Зикратов И. А., Самотонин Д. Н. Геоинформационный анализ радиолокационных отражений. СПб.: Политехника, 2004. 144 с.
3. Таха Х. Введение в исследование операций: В 2 кн. Пер. с англ. М.: Мир, 1985. Кн. 1. 479 с.

4. Алексеев В. М., Тихомиров В. М., Фомин С. В. Оптимальное управление. М.: Наука, 1979. 432 с.
5. Зикратов И. А., Степаненко К. В. Обоснование требований к точности цифровой картографической информации в геоинформационных системах проектирования и анализа радиолиний // Информационно-управляющие системы. 2004. № 2. С. 21–25.
6. Юдин Д. Б. Математические методы управления в условиях неполной информации. М.: Сов. радио, 1974. 400 с.

УДК 519.872

РАСЧЕТ СИСТЕМ СО СЛУЧАЙНЫМ ВЫБОРОМ НА ОБСЛУЖИВАНИЕ

Ю. И. Рыжиков,

доктор техн. наук, профессор

Военно-космическая академия им. А. Ф. Можайского

Проверка на имитационной модели известных частных методов расчета систем с очередями при случайном выборе на обслуживание выявила заметные ошибки в высших моментах распределения времени ожидания. Предлагается решать задачу построением вложенной цепи Маркова, описывающей изменение числа заявок в очереди на моменты перед завершением обслуживания в многоканальной системе — до выбора меченой заявки. Конечный результат получен в виде преобразования Лапласа распределения времени ее ожидания. Алгоритм тестирован на модели с простейшим входящим потоком и обобщен на рекуррентный поток.

The verification of known special approaches to queuing systems with random choice by imitation has detected noticeable errors in the high order moments of waiting time distribution. It is proposed to construct embedded Markov chain which describe the changing of queue length in multi-channel system before service completing — until the marked demand is selected. The final result is the Laplace transform of waiting time distribution. An algorithm is tested for Poissonian input flow and generalized for recurrent flow.

Постановка задачи

подавляющее большинство работ по теории очередей посвящено системам с выборкой из очереди по принципу FCFS (первый пришел — первый обслужен). Однако значительный интерес вызывает и другой принцип — случайный выбор из очереди (RANDOM). Он особенно типичен для связанных приложений и ситуаций с разъездными бригадами обслуживания (ремонтными, аварийными, скорой помощи, групп быстрого реагирования и т. п.), где очередность обработки заявок не определяется моментами их поступления. Различные подходы к этой задаче предлагаются или воспроизводятся в работах [1–7]. В работах [2, 3, 6] обсуждаются чисто марковские системы $M/M/n$. В частности, в них выводятся формулы для коэффициентов увеличения высших моментов времени ожидания в сравнении с дисциплиной FCFS:

$$R_2 = (1 - \rho/2)^{-1};$$

$$R_3 = (4 + 2\rho)/(2 - \rho)^2.$$

В статье Кингмана [5] выполнен анализ системы $M/G/1$, к сожалению, не доведенный до расчетных зависимостей. Дисперсия времени ожидания для этой же системы приводится в справочнике Дж. Мартина [1]. В работе Розенлунда [7] для

модели $GI/M/n$ получены преобразования Лапласа—Стилтьеса (ПЛС) распределения времени ожидания и рекуррентный алгоритм вычисления моментов. Фрагмент его итоговой таблицы приведен в табл. 1.

Наконец, в статье Картера и Купера [4] рассматриваются системы $GI/M/n$ и $M/G/n$. Здесь подтверждены известные результаты для систем $M/M/n$ и $M/D/1$, рассчитана система $M/E_k/1$.

Все перечисленные результаты выводятся весьма громоздкими методами, к тому же различными для разных классов моделей, с трудно прослеживаемой аргументацией и с привлечением эвристических приемов. Это делает весьма желательной их проверку на простой и надежной имитационной модели. В табл. 2 приведены результаты имитационного моделирования системы $M/M/3$ с дисциплинами FCFS и RANDOM при 500 тыс. испытаний.

Средний интервал между заявками предполагался единичным, интенсивность обслуживания выбиралась через заданный коэффициент загрузки ρ . Аналитические результаты хорошо согласуются с имитационной моделью FCFS с учетом общеизвестного нарастания погрешностей при увеличении порядка моментов и коэффициента загрузки системы. Переделка модели под случайный выбор из очереди затронула лишь четыре операто-

■ Таблица 1. Поправки к FIFO-моментам

Порядок моментов	D/M/n			E ₄ /M/n			M/M/n		
	0.5	0.7	0.9	0.5	0.7	0.9	0.5	0.7	0.9
2	1.2550	1.5005	1.8125	1.2884	1.5164	1.8148	1.3333	1.5385	1.8182
3	1.9782	3.0602	4.7698	2.0776	3.1149	4.7793	2.2222	3.1953	4.7934
4	3.6889	7.6951	16.238	3.9570	7.8927	16.286	4.3704	8.1896	16.356

■ Таблица 2. Расчет и имитация марковской системы

ρ	Моменты	FCFS (расчет)	FCFS (имитация)	RANDOM (имитация)	Отношение RANDOM/FCFS
0.5	w ₁	0.2368	0.2346	0.2346	1.0000
	w ₂	0.4737	0.4628	0.5362	1.1585
	w ₃	1.4211	1.3572	2.2109	1.6290
0.7	w ₁	1.1488	1.1494	1.1494	1.0000
	w ₂	5.3611	5.2108	7.1150	1.3654
	w ₃	37.528	34.162	86.600	2.5350
0.9	w ₁	7.3535	7.6507	7.3628	0.9624
	w ₂	132.36	140.17	226.70	1.6173
	w ₃	3573.9	3687.5	14980	4.0624

ра программы, и в ней было невозможно ошибиться. Правильность RANDOM-модели подтверждается и практическим совпадением средних времен ожидания. Однако отношения высших моментов заметно отличаются от приведенных в табл. 1, что вынуждает поставить вопрос о новых методах расчета систем обслуживания с RANDOM-дисциплиной.

Вложенная цепь Маркова для простейшего входящего потока

Рассмотрим режим полной занятости системы GI/G/n/R и обозначим:

J = R - n — максимальную длину очереди;

B_n(t) — распределение интервалов между последовательными завершениями обслуживания;

B_n^{*}(t) — распределение интервала от прибытия «меченой» заявки до ближайшего завершения обслуживания;

λ — интенсивность входящего потока.

Вычислим вероятности прибытия ровно j заявок за время до ближайшего обслуживания:

$$q_j^*(t) = \int_0^{\infty} \frac{(\lambda t)^j}{j!} e^{-\lambda t} dB_n^*(t), \quad j = 0, 1, \dots$$

и с заменой B_n^{*}(t) на B_n(t) — аналогичный набор {q_j} вероятностей прибытия ровно j заявок за время между смежными обслуживаниями. Введем также вектор P = {p₀, p₁, ..., p_J} стационарного распределения вероятностей длины очереди в момент прибытия меченой заявки. Построим вложенную цепь Маркова изменения числа заявок в оче-

реди непосредственно перед очередным выбором на обслуживание. Элементы матрицы R* переходов за время ожидания первого обслуживания должны вычисляться согласно

$$r_{i,j}^* = q_{j-i-1}^*(j-1)/j, \quad i = \overline{0, J}, j = \overline{i+1, J}$$

(было i заявок, пришли меченая и еще j - i - 1 ≥ 0). Дробный множитель учитывает вероятность невыбора меченой и, следовательно, продолжения процесса. Процесс завершается выбором меченой заявки с вероятностью 1/j. Вектор-столбец T* определяет вероятности перехода в поглощающее состояние. Его компоненты

$$t_i^* = \sum_{j=0}^J \frac{q_j^*}{i+j+1}.$$

Продолжение процесса (переходы на интервалах между смежными обслуживаниями) возможно при начальных состояниях i = 2, J. Соответственно переход i → j получается после прибытия j - i + 1 заявок (одна заявка уходит сразу после начала отсчета интервала). Итак, элементы новой матрицы R

$$r_{i,j} = q_{j-i+1}(j-1)/j, \quad i, j = \overline{2, J},$$

а элементы нового вектора вероятностей поглощения

$$t_i = \sum_{j=0}^J \frac{q_j}{i+j-1}.$$

Введем ПЛС временных распределений:
 $\beta^*(s)$ — от прибытия меченой заявки до ближайшего обслуживания;
 $\beta(s)$ — между смежными завершениями обслуживания;
 $\omega_k(s)$ — ожидания меченой заявки, завершаемого через k шагов марковской цепи, $k = 1, 2, \dots$
 Нетрудно видеть, что

$$\begin{aligned} \omega_1(s) &= \beta^*(s) \mathbf{P} \mathbf{T}^*, \\ \omega_2(s) &= \beta^*(s) \mathbf{P} \mathbf{R}^* \beta(s) \mathbf{T}, \\ \omega_3(s) &= \beta^*(s) \mathbf{P} \mathbf{R}^* \beta(s) [\mathbf{R} \beta(s)] \mathbf{T}, \\ &\dots \dots \dots \\ \omega_k(s) &= \beta^*(s) \mathbf{P} \mathbf{R}^* \beta(s) [\mathbf{R} \beta(s)]^{k-2} \mathbf{T}. \end{aligned}$$

Суммируя эти выражения по всем k , находим

$$\begin{aligned} \omega(s) &= \beta^*(s) \mathbf{P} \left(\mathbf{T}^* + \mathbf{R}^* \beta(s) \sum_{k=2}^{\infty} [\mathbf{R} \beta(s)]^{k-2} \mathbf{T} \right) = \\ &= \beta^*(s) \mathbf{P} \left(\mathbf{T}^* + \mathbf{R}^* \beta(s) [\mathbf{I} - \mathbf{R} \beta(s)]^{-1} \mathbf{T} \right). \end{aligned}$$

Искомые моменты распределения могут быть получены численным дифференцированием $w(s)$ (точнее, построенного в окрестности $s = 0$ интерполяционного многочлена с последующей сменой знака у нечетных производных).

Тестирование базовой схемы на модели $M/M/n$

Описанную расчетную схему целесообразно тестировать применительно к простейшей ситуации — с показательными распределениями. При этом нет проблем с потоком заявок: все остаточные распределения остаются показательными с исходным параметром λ , а связанные с процессом обслуживания распределения суть $B_n(t) = B_n^*(t) = 1 - e^{-n\mu t}$ и соответственно $\beta(s) = \beta^*(s) = n\mu / (n\mu + s)$. При $\lambda = 1$, коэффициенте загрузки $\rho = 0,7$ и шаге $h = 10^{-3}\mu$ для построения таблицы $\omega(s)$ при интерполировании по Стирлингу были получены значения моментов времени ожидания $w_1 = 1,1479$, $w_2 = 7,3481$, $w_3 = 91,338$. Соотнесенные с аналогичными результатами при дисциплине FCFS, они дают коэффициенты роста $k_1 = 1,0000$, $k_2 = 1,3706$, $k_3 = 2,4339$. Хорошее их согласие с полученными на имитационной модели позволяет считать основной алгоритм правильным и применить его к более сложным случаям: с немарковским распределением обслуживания и произвольным рекуррентным потоком заявок.

Немарковское распределение длительности обслуживания

В данном случае получение распределения интервалов до очередного обслуживания становится самостоятельной проблемой. Дополнительная

функция распределения (ДФР) интервала от прибытия меченой заявки до ближайшего завершения обслуживания может быть подсчитана согласно

$$\overline{B}_n^*(t) = \left[\overline{B}^*(t) \right]^n. \tag{1}$$

Для работы с этой формулой вычислим моменты $B_n^*(t)$ через моменты $B^*(t)$, аппроксимируя ДФР последнего распределением Вейбулла:

$$\overline{B}^*(t) = \exp(-t^k / W) \tag{2}$$

с моментами $b_m^* = W^{m/k} \Gamma(1 + m/k)$, $m = 1, 2, \dots$ Подставляя (2) в формулу (1), убеждаемся, что интересующее нас распределение $B_n(t)$ вновь описывается формулой (2) с заменой W на W/n . Соответственно вычисляются и его моменты.

Вторым удобным вариантом аппроксимации ДФР является гиперэкспоненциальная H_2 . В этом случае параметры ДФР $\overline{B}(t) = \sum_{i=1}^2 y_i e^{-\mu_i t}$ определяются по трем моментам $\{b_i\}$ исходного распределения, а остаточного $\overline{B}^*(t) = \sum_{i=1}^2 z_i e^{-\gamma_i t}$ — по трем модифицированным $b_i^* = b_{i+1} / [(i+1)b_1]$. Соответственно:

$$\overline{B}_n^*(t) = \left(\sum_{i=1}^2 z_i e^{-\gamma_i t} \right)^n = \sum_{j=0}^n \binom{n}{j} z_1^j z_2^{n-j} e^{-[j\gamma_1 + (n-j)\gamma_2]t}.$$

Моменты этого распределения

$$b_{m,n}^* = \int_0^{\infty} t^{m-1} \overline{B}_n^*(t) dt = m! \sum_{j=0}^n \binom{n}{j} \frac{z_1^j z_2^{n-j}}{[j\gamma_1 + (n-j)\gamma_2]^m},$$

$$m = 1, 2, \dots$$

Для основного режима марковской цепи придется строить распределение интервалов между смежными завершениями обслуживания в n -канальной системе. Здесь (см. [3]) $\overline{B}_n(t) = \left[\overline{B}^*(t) \right]^{n-1} \overline{B}(t)$. В данной ситуации аппроксимация распределениями Вейбулла не имеет смысла, а гиперэкспоненциальная аппроксимация приводит к

$$\begin{aligned} \overline{B}_n(t) &= \left(\sum_{i=1}^2 z_i e^{-\gamma_i t} \right)^{n-1} \left(\sum_{i=1}^2 y_i e^{-\mu_i t} \right) = \\ &= \sum_{j=0}^{n-1} \binom{n-1}{j} z_1^j z_2^{n-1-j} e^{-[j\gamma_1 + (n-1-j)\gamma_2]t} \left(\sum_{i=1}^2 y_i e^{-\mu_i t} \right) = \\ &= \sum_{i=1}^2 y_i \sum_{j=0}^{n-1} \binom{n-1}{j} z_1^j z_2^{n-1-j} e^{-[j\gamma_1 + (n-1-j)\gamma_2 + \mu_i]t}. \end{aligned}$$

Ее моменты можно считать по формулам

$$b_{m,n} = m! \sum_{i=1}^2 y_i \sum_{j=0}^{n-1} \binom{n-1}{j} \frac{z_1^j z_2^{n-1-j}}{[j\gamma_1 + (n-1-j)\gamma_2 + \mu_i]^m},$$

$$m = 1, 2, \dots$$

Далее по найденным моментам подбирается аппроксимация, обеспечивающая удобное вычисление $\{q_j\}$. В частности, для гамма-плотности $b(t) = m(mt)^{\alpha-1} e^{-mt} / \Gamma(\alpha)$ параметры выражаются через среднее b_1 и дисперсию D согласно $\alpha = b_1^2 / D$, $m = \alpha / b_1$. Теперь

$$q_0 = \left(\frac{m}{\lambda + m} \right)^\alpha;$$

$$q_j = q_{j-1} \frac{\lambda}{\lambda + m} \frac{\alpha + j - 1}{j}, \quad j = 1, 2, \dots$$

Применение гамма-плотности с поправочным множителем, который строится на основе теории обобщенных многочленов Лагерра, позволяет выравнять произвольное число моментов. При этом сохраняется возможность рекуррентного вычисления $\{q_j\}$, но по более сложному алгоритму.

Рекуррентный поток

При рекуррентном входящем потоке общего вида приходится учитывать следующие дополнительные обстоятельства.

1. Для начального шага марковской цепи коэффициенты $\{q_j\}$ считаются как вероятности прибытия ровно j заявок рекуррентного потока за *модифицированный* интервал между смежными обслуживаниями (отсчет времени начинается с прибытия меченой заявки).

2. На последующих шагах расчет начинается с завершения очередного обслуживания, которое приходится на случайную точку интервала между смежными заявками. Соответственно, поток заявок представляется как рекуррентный с *запаздыванием*, а интервалы между обслуживаниями не модифицируются.

Рассмотрим способ расчета распределения числа событий рекуррентного потока на фиксированном интервале времени. Пусть $A_k(t)$ есть функция распределения суммы k независимых случайных величин, подчиняющихся распределению

$A_1(t) \equiv A(t)$. Очевидно, вероятность неприбытия заявок $q_0(t) = 1 - A(t) = \bar{A}(t)$, а вероятность появления ровно $k \geq 1$ требований потока $q_k(t) = A_k(t) - A_{k+1}(t)$.

Обозначим через $\alpha(s)$ ПЛС от плотности распределения $A(t)$. Тогда производящая функция ПЛС интересующих нас вероятностей

$$Q(s) = \frac{1}{s} \sum_{k=0}^{\infty} z^k [\alpha^k(s) - \alpha^{k+1}(s)] = a \frac{1 - \alpha(s)}{as} \sum_{k=0}^{\infty} z^k \alpha^k(s).$$

Здесь a есть средний интервал между смежными заявками, а дробь перед суммой — ПЛС от *остаточного* распределения интервалов между ними. Таким образом, для рекуррентного потока $q_k(t) = aL^{-1}[\alpha^*(s)\alpha^k(s)]$, $k = 0, 1, \dots$ (через L^{-1} обозначен оператор обратного ПЛС). Контрольное суммирование ПЛС дает $1/s$, откуда следует равенство суммы $\{q_k(t)\}$ единице. Произведение сверток в последней формуле имеет прозрачную вероятностную интерпретацию: чтобы за время t пришло ровно k заявок, в него должны уложиться k полных интервалов между заявками и один остаточный (последний). Напомним, что отсчет времени здесь начинается сразу после прибытия очередной заявки.

В случае рекуррентного потока с *запаздыванием* интервал времени до прибытия первой заявки является случайной модификацией типового. Это позволяет по аналогии с предыдущим вариантом сразу записать итоговые формулы в виде

$$q_0(t) = \bar{A}^*(t);$$

$$q_k(t) = aL^{-1}[(\alpha^*(s))^2 \alpha^{k-1}(s)], \quad k = 1, 2, \dots$$

Условие нормировки $\{q_j\}$ здесь проверяется (и выполняется) аналогично. Эти выражения должны интегрироваться с учетом вышеуказанных распределений длительности шагов марковской цепи.

Заключение

Результаты статьи позволяют с единых позиций подойти к расчету ПЛС распределения времени ожидания для многоканальных систем со случайным выбором заявок из очереди и произвольными распределениями длительности обслуживания и интервалов между заявками.

Литература

1. Мартин Дж. Системный анализ передачи данных: Пер. с англ. М.: Мир, 1975. Т. 2. 431 с.
2. Риордан Дж. Вероятностные системы обслуживания: Пер. с англ. М.: Связь, 1966. 164 с.
3. Саати Т. Л. Элементы теории массового обслуживания и ее приложения: Пер. с англ. М.: Сов. радио, 1965. 510 с.

4. Carter G. M., Cooper R. B. Queues with service in random order // Opns res. 1972. Vol. 20. N 2. P. 389–407.
5. Kingman J. F. C. On queues in which customers are served in random order // Proc. Camb. Phil. Soc. 1962. Vol. 58. N 1. P. 79–91.
6. Morse P. M. Queues, inventories, and maintenance. N.Y.: Wiley, 1958. 202 p.
7. Rosenlund S. I. The random order G/M/m queue // Naval Res. Logistics. 1980. Vol. 27. N 2. P. 207–215.

СВЕДЕНИЯ ОБ АВТОРАХ

АГИЕВИЧ
Сергей
Николаевич



Старший научный сотрудник, заместитель начальника научно-исследовательской группы Военной академии связи им. С. М. Буденного, заслуженный изобретатель Российской Федерации. В 1983 году окончил Череповецкое высшее военное инженерное училище радиозлектроники. В 1995 году защитил диссертацию на соискание ученой степени кандидата технических наук. Является автором более 50 научных публикаций и 60 изобретений. Область научных интересов — обработка сигналов в радиотехнических системах.

ВЕЛЬДЕР
Сергей
Эдуардович



Магистрант кафедры компьютерных технологий Санкт-Петербургского государственного университета информационных технологий, механики и оптики. Область научных интересов — верификация программ.

ЗИКРАТОВА
Татьяна
Викторовна



Преподаватель кафедры радиозлектроники Санкт-Петербургского высшего военного училища радиозлектроники. Окончила Томский политехнический институт в 1986 году. Является автором пяти научных публикаций. Область научных интересов — геоинформационные технологии.

БЕСПАЛОВ
Вячеслав
Леонидович



Адъюнкт Военной академии связи им. С. М. Буденного. В 1990 году окончил Череповецкое высшее военное инженерное училище радиозлектроники. В 2004 году окончил с отличием Военную академию связи им. С. М. Буденного. Является автором более 20 научных публикаций. Область научных интересов — обработка сигналов в радиотехнических системах.

ЗИКРАТОВ
Игорь
Алексеевич



Доцент, начальник кафедры военной кибернетики Санкт-Петербургского высшего военного училища радиозлектроники. В 1987 году окончил Киевское высшее инженерное радиотехническое училище ПВО им. маршала авиации А. И. Покрышкина. В 1999 году защитил диссертацию на соискание ученой степени кандидата технических наук. Является автором более 40 научных публикаций, в том числе соавтором двух монографий. Область научных интересов — геоинформационные технологии.

КАЦОВ
Илья
Владимирович



Сотрудник лаборатории кодовых приложений Intel. Студент кафедры безопасности информационных систем Санкт-Петербургского государственного университета аэрокосмического приборостроения. Область научных интересов — цифровая связь, пространственно-временное кодирование.

ЛЕБЕДЕВ
Илья
Сергеевич



Преподаватель кафедры военной кибернетики Санкт-Петербургского высшего военного училища радиоэлектроники. В 1998 году окончил Санкт-Петербургское высшее военное училище ПВО. В 2002 году защитил диссертацию на соискание ученой степени кандидата технических наук. Является автором более 30 научных публикаций. Область научных интересов — информационные технологии, компьютерная лингвистика.

МОЛДОВАНИН
Тимофей
Валерьевич



Аспирант кафедры технической кибернетики Российского университета дружбы народов. В 2004 году окончил Российский университет дружбы народов. Является автором семи научных публикаций. Область научных интересов — информационные технологии, защита информации.

РЫЖИКОВ
Юрий
Иванович



Профессор кафедры математического обеспечения ЭВМ Военно-космической академии им. А. Ф. Можайского, заслуженный деятель науки РФ. В 1958 году окончил Черноморское высшее военно-морское училище им. П. С. Нахимова. В 1969 году защитил диссертацию на соискание ученой степени доктора технических наук. Является автором более 200 научных публикаций, в том числе 40 учебных пособий и монографий. Область научных интересов — теория очередей, имитационное моделирование, вычислительные методы и прикладное программирование, управление запасами, науковедение и педагогика высшей школы.

ТИХОНОВ
Эдуард
Прокофьевич



Доцент кафедры биомедицинской электроники и охраны среды Санкт-Петербургского государственного электротехнического университета, член-корреспондент Метрологической академии. В 1962 году окончил Ленинградский институт авиационного приборостроения. Является автором более 190 научных публикаций, в том числе более 50 авторских свидетельств и патентов на изобретения. Область научных интересов — кибернетика, информатика, моделирование, информационно-измерительные системы, биомедицинская инженерия.

ШАЛЫТО
Анатолий
Абрамович



Заведующий кафедрой технологий программирования Санкт-Петербургского государственного университета информационных технологий, механики и оптики. Ученый секретарь НИО «Аврора». В 1971 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина) по специальности «Автоматика и телемеханика». В 1999 году защитил диссертацию на соискание ученой степени доктора технических наук. Является автором более 250 научных публикаций, трех монографий и 70 изобретений. Область научных интересов — системы логического управления, автоматное программирование.

УДК 681.314+681.51.011

Аналитико-имитационное исследование и оптимизация алгоритмов аналого-цифрового преобразования в условиях воздействия помех (Часть 2)

Тихонов Э. П. Информационно-управляющие системы, 2007. № 3. С. 2–14.

На основании предложенных автором информационных алгоритмов проведен аналитико-имитационный анализ потенциальных возможностей адекватных алгоритмов аналого-цифрового преобразования поразрядного уравнивания, в том числе, при воздействии аддитивной помехи. На основе критерия помехоустойчивости разработаны рекомендации по оптимальному выбору параметров адекватных алгоритмов аналого-цифрового преобразования в зависимости от уровня аддитивной помехи.

Список лит.: 9 назв.

УДК 621.391

Использование функций сплайн—Виленкина—Крестенсона для построения аналитических моделей радиосигналов

Агиевич С. Н., Беспалов В. Л. Информационно-управляющие системы, 2007. № 3. С. 15–22.

Рассматриваются возможности использования базисов функций сплайн—Виленкина—Крестенсона для построения аналитических моделей радиосигналов с целью повышения скорости их цифровой обработки. Излагаются основы современной теории сплайн-гармонического анализа. Определяются понятия свертки и корреляции для функций сплайн—Виленкина—Крестенсона. Производится оценка скорости цифровой обработки радиосигналов, полученных на основе представленных моделей.

Список лит.: 7 назв.

УДК 681.3

Способ формализации связей в конструкциях текста при создании естественно-языковых интерфейсов

Лебедев И. С. Информационно-управляющие системы, 2007. № 3. С. 23–26.

Предложен способ, основанный на использовании структур, характеризующих лексические единицы текста, позволяющий вычислять ответы в тексте на вопросы, заданные в естественном виде. Рассмотрены вопросы разделения текста на семантически связанные единицы.

Список лит.: 4 назв.

UDK 681.314+681.51.011

Analytical and imitating research and optimization of algorithms of analog-digital transformation in conditions of influence of noise (Part 1)

Tikhonov E. P. IUS, 2007. N 3. P. 2–14.

On the basis of the information algorithms proposed by the author, certain methods of analog-digital transformation are investigated in the presence of noise. The results of research allow us to receive recommendations as to an optimum choice of parameters of adequate algorithms of analog-digital transformation depending on noise.

Refs: 9 titles.

UDK 621.391

Using spline-Vilenkin-Chrestenson functions for the construction of analytical models of radiosignals
Agievich S. N., Bespalov V. L. IUS, 2007. N 3. P. 15–22.

We study the use of spline-Vilenkin-Chrestenson functions for the construction of analytical models of radiosignals in order to increase the speed of their digital processing. Fundamentals of the modern theory of spline-harmonic analysis are given. For the spline-Vilenkin-Chrestenson functions the notions of convolution and correlation are defined. Finally, we give some estimates for the speed of digital processing of the radiosignals based on the proposed model.

Refs: 7 titles.

UDK 681.3

Formalization of links in the text constructions for creation of natural language interfaces

Lebedev I. S. IUS, 2007. N 3. P. 23–26.

We propose a way based on the use of structures describing lexical units of a text and which allow us to calculate the answers to naturally given questions. The problems of division of the text to semantically connected units are considered.

Refs: 4 titles.

УДК 681.3.06

О верификации простых автоматных программ на основе метода Model Checking

Вельдер С. Э., Шалыто А. А. Информационно-управляющие системы, 2007. № 3. С. 27–38.

Излагается применительно к простым автоматным программам (их поведение описывается одним конечным автоматом) техника верификации, которая базируется на темпоральных логиках и называется Model Checking. Для автоматных программ удается автоматизировать процесс построения модели программы, подлежащей верификации.

Список лит.: 21 назв.

УДК 681.324:681.326

Решение задачи выбора оптимального варианта комплексной защиты информации с помощью метода экспертного оценивания

Молдованин Т. В. Информационно-управляющие системы, 2007. № 3. С. 39–44.

Рассмотрен один из подходов к выбору оптимального варианта комплексной защиты информации на примере информационно-управляющей системы предприятия, основанный на экспертной оценке. Рассмотрены задачи оценки степени согласованности экспертных суждений и способы улучшения этой согласованности.

УДК 681.324:681.326

УДК 621.396.24

Пространственное мультиплексирование с субсимвольным временным сдвигом между передающими антеннами

Кацов И. В. Информационно-управляющие системы, 2007. № 3. С. 45–51.

Предлагается метод пространственного мультиплексирования с субсимвольным временным сдвигом, который позволяет реализовать высокоскоростную передачу в беспроводных системах с малым количеством антенн. Высокая скорость предложенных пространственно-временных кодов позволяет использовать помехоустойчивое кодирование без расширения полосы частот или увеличения значности модуляции. Рассмотрены вычислительно простые алгоритмы декодирования предложенных кодов.

Список лит.: 17 назв.

UDK 681.3.06

Verification of simple automata-based programs using the model checking method

Velder S. E., Shalyto A. A. IUS, 2007. N 3. P. 27–38.

Verification of simple automata-based programs (whose behavior can be described with a single finite automaton) is considered. The applied verification technique is based on temporal logics and is known as Model Checking. For automata-based programs it is possible to automate the process of building program model subject to verification.

Refs: 21 titles.

Selecting the optimal variant of comprehensive information protection using the expert evaluation method

Moldovanin T. V. IUS, 2007. N 3. P. 39–44.

The problem of selecting the optimal variant of comprehensive information protection using the expert evaluation method is discussed on the example of information-controlling system of an enterprise. To enhance the reliability of evaluation we use group expert examination. Problems of agreement of expert evaluations and ways to improve this agreement are also considered.

UDK 621.396.24

Spatial multiplexing with subsymbol time delay between transmit antennas

Katsov I. V. IUS, 2007. N 3. P. 45–51.

Spatial multiplexing with transmit antennas subsymbol time delay is a novel technique for high-throughput wireless MIMO systems with small receive antenna arrays. The high rate of proposed space-time codes provides error-correction coding usage without spectral band expansion or signal constellation expansion. Effective equalization algorithms with low computational complexity are also proposed for new codes.

Refs: 17 titles.

УДК 681.518

К вопросу об оптимизации зоны покрытия систем сотовой связи на загородных участках местности

Зикратов И. А., Зикратова Т. В. Информационно-управляющие системы, 2007. № 3. С. 52–55.

Обсуждаются вопросы рационального размещения ретрансляторов базовых станций сотовой связи на загородных участках местности с использованием цифровой картографической информации. Решение достигается путем представления целевой функции и ограничений задачи нелинейного программирования в виде эквивалентной задачи с булевыми переменными. Показано также, что задачу можно сформулировать как задачу стохастического программирования с вероятностными ограничениями.

Список лит.: 6 назв.

УДК 519.872

Расчет систем со случайным выбором на обслуживание

Рыжиков Ю. И. Информационно-управляющие системы, 2007. № 3. С. 56–59.

Проверка на имитационной модели известных частных методов расчета систем с очередями при случайном выборе на обслуживание выявила заметные ошибки в высших моментах распределения времени ожидания. Предлагается решать задачу построением вложенной цепи Маркова, описывающей изменение числа заявок в очереди на моменты перед завершением обслуживания в многоканальной системе — до выбора меченой заявки. Конечный результат получен в виде преобразования Лапласа распределения времени ее ожидания. Алгоритм тестирован на модели с простейшим входящим потоком и обобщен на рекуррентный поток.

Список лит.: 7 назв.

UDK 681.518

Optimization of the coverage area for the cellular communication systems in out-of-town locations

Zikratov I. A., Zikratova T. V. IUS, 2007. N 3. P. 52–55.

The problems of rational allocation of basic cellular communication station retransmitters at the out-of-town surroundings using digital cartographical information are discussed. The decision is achieved by a presentation of the objective function and restriction of non-linear programming task in the form of Boolean values. We also show that the task can be reformulated as a stochastic programming problem with restriction probabilities.

Refs: 6 titles.

UDK 519.872

Design of systems with random choice from a queue

Ryzhikov Yu. I. IUS, 2007. N 3. P. 56–59.

The verification of known special approaches to queuing systems with random choice by imitation has detected noticeable errors in the high order moments of waiting time distribution. We propose to construct embedded Markov chain which describe the changing of queue length in multi-channel system before service completing — until the marked demand is selected. The final result is the Laplace transform of the waiting time distribution. An algorithm is tested for Poissonian input flow and is generalized for recurrent flow.

Refs: 7 titles.