ISSN 1684–8853

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

1(38)/2009

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

1(38)/2009

РЕЦЕНЗИРУЕМОЕ ИЗДАНИЕ

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

Адрес редакции: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Тел.: (812) 494-70-44
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 входит в «Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук».

Журнал распространяется по подписке. Подписку можно оформить через редакцию, а также в любом отделении связи по каталогам: «Роспечать»: № 48060, № 15385; «Пресса России»: № 42476.

ЛР № 010292 от 18.08.98.
Сдано в набор 29.12.08. Подписано в печать 20.02.09. Формат 60×84 1/8.
Бумага офсетная. Гарнитура SchoolBookC. Печать офсетная.
Усл. печ. л. 9,8. Уч.-изд. л. 11,8. Тираж 1000 экз. Заказ 88.

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

МОДИФИЦИРОВАННЫЕ АЛГОРИТМЫ И КЛАССИФИКАЦИЯ АНАЛОГО-ЦИФРОВЫХ ПРЕОБРАЗОВАТЕЛЕЙ
Часть 1: Параллельно-последовательные алгоритмы

Э. П. Тихонов,
канд. техн. наук, доцент
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

Предложено аналитическое описание различных модификаций алгоритмов аналого-цифровых преобразователей, включая мажоритарный и нейронноподобный принцип обработки информации, на базе которых выполнен сравнительный анализ их свойств, доведенных до численных результатов, и разработана классификационная схема аналого-цифровых преобразователей.

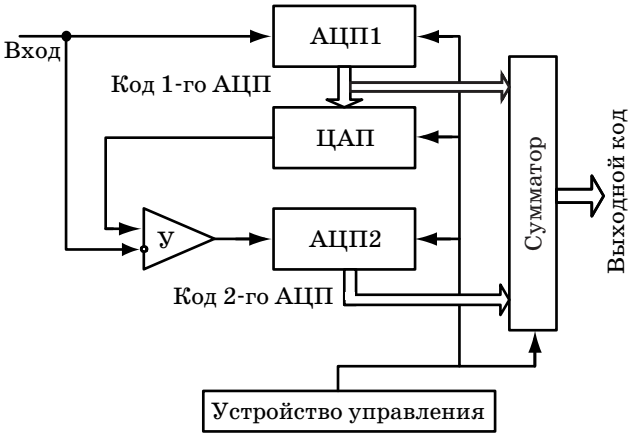
Ключевые слова *— преобразователь аналог-код, параллельно-последовательный алгоритм, древовидный фрактал, конвейерный преобразователь, параллельный преобразователь.*

Эволюция алгоритмов аналого-цифрового преобразования неразрывно связана с процессом совершенствования структур аналого-цифровых преобразователей (АЦП), причем развитие этих процессов взаимодополняющее. Стремление максимально приспособить алгоритм аналого-цифрового преобразования к современным требованиям информационных технологий, а также к процессу совершенствования электронных компонентов, из которых состоит схема АЦП, для улучшения в целом технических средств обработки информации приводит к поиску новых принципов построения АЦП. Типичным примером является возникновение параллельно-последовательных структур АЦП на основе известных алгоритмов поразрядного уравновешивания или в комбинации с чисто параллельными АЦП [1–3], а также алгоритмов сигма-дельта АЦП [4, 5]. Поиск способов преодоления недостатков, ограничивающих возможности по быстродействию алгоритмов последовательного типа, с одной стороны, и связанных с ограничениями по точности и сложности реализации алгоритмов параллельного типа, с другой стороны, привел к созданию новых параллельно-последовательных структур АЦП. Алгоритмы, лежащие в основе новых АЦП, в литературе называются многокаскадными или с циклическим уточнением. Встречаются также иные названия этих алгоритмов: многотактные (многоступенчатые), поддиапазонные алгоритмы, а также, с учетом их некоторой модификации, конвейерные алгоритмы и, соответственно, конвейерные АЦП. Причем, если в структуре АЦП используются только два диапазона, то такой АЦП называется двухтактным, если используются три диапазона, то — трехтактными и т. д. Вариации в терминологии, в частности многотактных алгоритмов, алгоритмов конвейерного типа, вводятся для привязки этого названия к определенным модификациям технического решения фактически одного и того же алгоритма, главным отличительным признаком которого являются параллельно-последовательные действия в процессе аналого-цифрового преобразования. Преимуществом подобных алгоритмов является существенное повышение быстродействия при сохранении высокой точности аналого-цифрового преобразования в том случае, когда при преобразовании в каждом или хотя бы в одном цикле преобразования используется алгоритм и, следовательно, АЦП параллельного типа. Параллельно-последовательные алгоритмы позволяют решить проблему значительного увеличения быстродействия без существенного усложнения схемы, свойственного АЦП параллельного типа, в котором при увеличении числа разрядов нелинейно по степенному закону возрастает сложность реализации схемы и, следовательно, стоимость АЦП. В этом случае переход к двухтактному АЦП позволяет применить два однотипных параллельных АЦП либо комбинированно использовать один параллельный АЦП, а второй —

АЦП поразрядного уравновешивания, что, несомненно, приводит к существенному сокращению времени преобразования.

В предлагаемой работе, в развитие работ [1–4, 6], представлены в математической форме и исследованы методами имитационного моделирования алгоритмы многотактных АЦП, а также алгоритмы с дополнительной обработкой функции сравнения. Формальная или математическая запись алгоритмов аналого-цифрового преобразования в виде отображений существенно расширяет возможности по синтезу новых алгоритмов, так как позволяет в комбинации математических методов и методов имитационного моделирования без существенных затрат создавать и исследовать новые, более совершенные алгоритмы, приспосабливая для их технической реализации современные электронные технологии. Алгоритмы, представленные ниже в математической форме, предполагают использование в многотактных АЦП алгоритмов поразрядного уравновешивания. Однако их легко можно модифицировать для применения в каждом цикле различных по виду алгоритмов преобразования.

Один из возможных простейших вариантов известной структурной схемы двухтактного АЦП показан на рис. 1. В соответствии с приведенной схемой входной сигнал одновременно подается на вход первого N-разрядного *АЦП*1 и вычитающий вход усилителя *У* с коэффициентом усиления, равным 2^N. Выходной код *АЦП*1 параллельно поступает на входы высокоточного *ЦАП* (цифроаналогового преобразователя) и N старших разрядов сумматора. Преобразованный в аналоговую форму *ЦАП* N-разрядный код *АЦП*1 по сигналу устройства управления поступает на вычитающий вход усилителя *У*. Усиленная в 2^N раз разность между входным сигналом и выходным напряжением *ЦАП* вновь преобразуется в цифровой код *АЦП*2 и записывается по сигналу устройства управления в N младших разрядов сумматора. Результат суммирования кода *АЦП*2, поделенного на делитель 2^N, с кодом *АЦП*1 по сигналу управления считывается на выходе сумматора и, таким образом, образует выходной $2N$-разрядный двоичный код. При этом входной сигнал может поступать на входы *АЦП*1 и усилителя *У* через устройство выборки и хранения (УВХ). Синхронизация и автоматическое управление всей схемой двухтактного АЦП осуществляется устройством управления, куда входит также и тактовый генератор.



■ ***Рис. 1.*** *Структурная схема параллельно-последовательного (двухступенчатого) АЦП*

Двухтактный алгоритм в аналитическом виде при использовании алгоритма поразрядного уравновешивания с индикаторной функцией сравнения [1] в каждом цикле преобразования имеет вид

$$E(n\Delta t) = E[(n-1)\Delta t] + a_n\, h\,[x - E[(n-1)\Delta t] - a_n],$$
$$n = 1, \ldots, N;$$

$$E(n\Delta t) = E[(n-1)\Delta t] + a_n h\{[x - E(N\Delta t)]2^N - E[(n-1)\Delta t] - a_n\},$$
$$n = N+1, \ldots, 2N, \qquad (1)$$

а при использовании алгоритма со знаковой функцией сравнения [1] получаем соответственно

$$E(n\Delta t) = E[(n-1)\Delta t] + a_n \mathrm{sign}[x - E[(n-1)\Delta t]],$$
$$n = 1, \ldots, N;$$

$$E(n\Delta t) = E[(n-1)\Delta t] + a_n \mathrm{sign}\{[x - E(N\Delta t)]2^N - E[(n-1)\Delta t]\},$$
$$n = N+1, \ldots, 2N. \qquad (2)$$

Окончательный результат выводится путем суммирования кодов:

$$K(2N\Delta t) = K(N\Delta t) + K(2N\Delta t)/2^N,$$

где $E[(n+1)\Delta t]$ и $E(n\Delta t)$ — уравновешивающая физическая величина, или просто уравновешивающая величина (напряжение, ток, сопротивление и т. п.), на $(n+1)$-м и n-м тактах преобразования (сравнения или уравновешивания) для каждого цикла преобразования; n — текущее значение (номер) временного такта уравновешивания, причем $n = 1, \ldots, N$; N — число двоичных разрядов; Δt — временной такт, через который осуществляется сравнение входного сигнала с уравновешивающей величиной на n-м такте сравнения (временной такт уравновешивания); a_n — заданная последовательность, определяющая закон изменения уравновешивающей ве-

личины в зависимости от изменения n, причем $a_n = E_0 2^{-n}$; E_0 — заданный диапазон изменения уравновешивающей величины; x — входной сигнал с ограничением $x \le E_0$ (обычно входной сигнал y, если пренебречь его изменением во времени на интервале преобразования, равен сумме собственно сигнала x и случайной аддитивной помехи ξ, т. е. $y = x + \xi$); $K(N\Delta t)$ и $K(2N\Delta t)$ — кодовые эквиваленты уравновешивающей величины на соответствующем такте уравновешивания, т. е. $\Delta qK(N\Delta t) = E(N\Delta t)$ и $\Delta qK(2N\Delta t) = E(2N\Delta t)$; Δq — величина кванта, определяющего число уровней квантования входного сигнала в пределах диапазона изменения E_0; $h[x - E(n\Delta t) - a_n]$ и $\mathrm{sign}[x - E(n\Delta t)]$ — функции сравнения входного сигнала y с уравновешивающей величиной $E(n\Delta t)$ для $n = 1, 2, \ldots$. Эти функции имеют следующий вид [1]:

$$h\{\ldots\} = \begin{cases} 1 \text{ при } x \ge E\left[(n-1)\Delta t\right] + a_n \\ 0 \text{ при } x \le E\left[(n-1)\Delta t\right] + a_n \end{cases};$$

$$\mathrm{sign} = \begin{cases} 1 \text{ при } x \ge E\left[(n-1)\Delta t\right] \\ -1 \text{ при } x \le E\left[(n-1)\Delta t\right] \end{cases}.$$

Напомним, что функция сравнения описывает работу реального сравнивающего устройства (СУ) [6]. Первую индикаторную функцию сравнения можно также выразить через вторую знаковую функцию сравнения в соответствии с формулой

$$h(x) = 0{,}5(1 + \mathrm{sign}(x)).$$

Как вытекает из полученных выражений (1) и (2), вид двухтактного алгоритма усложняется по сравнению с исходными алгоритмами поразрядного уравновешивания. Такое усложнение алгоритма приводит к естественному усложнению исходной структуры АЦП поразрядного уравновешивания. Структура АЦП, которая реализует рассмотренный выше двухтактный алгоритм, приобретает вид, указанный на рис. 1. В настоящее время известны серийные микросхемы АЦП, например **AD872A и AD876 фирмы ANA**LOG DEVICES с числом $k = 2$.

Если число тактов (поддиапазонов, циклов) в каждом цикле преобразования увеличить до $k > 2$ **значений, но в каждом такте преобразования** оставить одно и то же число разрядов N, то алгоритм усложняется и описывается системой

$$E(n_i\Delta t) = E[(n_i - 1)\Delta t] + \varphi\{x, E[(n_i - 1)\Delta t], 2^{(i-1)N}, a_n\}, \quad i = 1, 2, \ldots, k, \qquad (3)$$

где

$$\varphi\left\{x, E\left[(n_i - 1)\Delta t\right], 2^{(i-1)N}, a_n\right\} = \begin{cases} a_n h\left\{x, E\left[(n_i - 1)\Delta t\right], 2^{(i-1)N}, a_n\right\} \\ a_n \mathrm{sign}\left\{x, E\left[(n_i - 1)\Delta t\right], 2^{(i-1)N}\right\} \end{cases}$$

приобретает соответствующую форму для индикаторной или знаковой функции сравнения, причем для $n_1 = 1, \ldots, N$; $n_2 = N + 1, \ldots, 2N$; $\ldots$; $n_k = (k-1)N + 1, (k-1)N + 2, \ldots, kN$; здесь n_i — число тактов уравновешивания в i-м цикле преобразования k-го диапазона; $k = 1, \ldots, L$, здесь L — установленное число поддиапазонов (тактов) в полном цикле аналого-цифрового преобразования; $a_n = E_0 2^{-n}$, $n = 1, 2, \ldots, N$; $N = \mathrm{const}$. Результатом преобразования является значение кода

$$K(k\Delta tN) = \sum_{i=0}^{k-1} \frac{K\left[(i+1)\Delta tN\right]}{2^{iN}}.$$

В дальнейшем алгоритмы с индикаторной или знаковой функцией сравнения в зависимости от значения параметра k будем называть двухтактными, трехтактными и т. д. индикаторными или знаковыми алгоритмами аналого-цифрового преобразования соответственно.

Алгоритм многоступенчатого преобразования (3) может несколько измениться в зависимости от числа разрядов, устанавливаемых в каждом такте (ступени) преобразования, что приведет к несовпадению числа разрядов и соответствующих коэффициентов усиления результатов вычитания в каждом цикле преобразования. Действительно, если при k тактах преобразования на каждом такте преобразования число разрядов будет меняться и зависит от k, т. е. принимать значения N_k, то алгоритм усложняется и приобретает вид системы уравнений в конечных разностях

$$E(n_i\Delta t) = E\left[(n_i - 1)\Delta t\right] + \varphi\left\{\left[x, E\left[(n_i - 1)\Delta t\right]\right], 2^{\sum_{m=0}^{i-1} N_m}, a_{ni}\right\}, \quad i = 1, 2, \ldots, k, \qquad (4)$$

где $n_1 = N_0 + 1, \ldots, N_1$; $n_2 = N_1 + 1, \ldots, N_1 + N_2$; $\ldots$; $n_k = N_1 + \ldots + N_{k-1} + 1, \ldots, N_1 + \ldots + N_{k-1} + N_k$; $N_0 = 0$;

$$a_{ni} = E_0 2^{-ni}, \quad ni = 1, 2, \ldots, N_i.$$

Результатом преобразования является значение кода

$$K\left(\Delta t\sum_{i=1}^{k}N_i\right)=\sum_{i=0}^{k-1}\frac{K\left(\Delta t\sum\limits_{m=1}^{i+1}N_m\right)}{2^{\sum\limits_{m=0}^{i}N_m}}.$$

Для $k = 1$, т. е. для однотактного алгоритма, в данном случае алгоритма поразрядного уравновешивания, получаем

$$K[N_1\Delta t]=\sum_{i=0}^{0}\frac{K\left[\sum\limits_{m=1}^{i+1}\Delta tN_m\right]}{2^{\sum\limits_{m=0}^{i}N_i}}=$$

$$=\frac{K[\Delta tN_1]}{2^{N_0}}=K[\Delta tN_1],$$

так как $N_0 = 0$.

Для двухтактного алгоритма при $k = 2$ получаем

$$K[\Delta t(N_1+N_2)]=\sum_{i=0}^{1}\frac{K\left[\sum\limits_{m=1}^{i+1}\Delta tN_m\right]}{2^{\sum\limits_{m=0}^{i}N_i}}=$$

$$=K[\Delta tN_1]+\frac{K[\Delta t(N_1+N_2)]}{2^{N_1}}$$

и так далее.

Алгоритм (4) в явном виде, например для индикаторной функции сравнения при числе установленных тактов L в полном цикле поразрядного преобразования, раскрывается следующим образом:

$$E\left[\left(\sum_{i=1}^{k-1}N_i+n_k+1\right)\Delta t\right]=E\left[\left(\sum_{i=1}^{k-1}N_i+n_k\right)\Delta t\right]+$$

$$+\frac{E_0}{2^{n_k}}h\left[2^{\sum\limits_{i=1}^{k-1}N_i}x-\sum_{j=1}^{k-1}2^{\sum\limits_{i=j}^{k-1}N_i}E\left(\sum_{i=1}^{j}N_i\Delta t\right)-\right.$$

$$\left.-E\left[\left(\sum_{i=1}^{k-1}N_i+n_k\right)\Delta t\right]-\frac{E_0}{2^{n_k}}\right],\ k=1,2,...,L,$$

т. е. описывается системой итерационных алгоритмов L-го порядка и легко трансформируется в алгоритм вида (3) для $N_i = N = \text{const}$. При этом следует иметь в виду, что $\sum\limits_{i=1}^{0}\theta_i=0,\ 2^{\sum\limits_{i=1}^{0}N_i}=2^0.$

Параметр L определяет структурную схему АЦП и для $N_i = N = \text{const}$ и $L = 2$ соответствует структурной схеме, приведенной на рис. 1.

Промышленностью выпускаются также АЦП, построенные на основе алгоритмов многотактного преобразования, у которых допускается временное перекрытие кодов в каждом такте преобразования. Такие алгоритмы с определенной модификацией целесообразно использовать в АЦП конвейерного типа, которые имеют преимущество по быстродействию при преобразовании, в том числе для изменяющегося во времени входного сигнала [3]. Подобные модифицированные АЦП рассмотрены ниже. При числе разрядов p_i, на которое перекрываются коды в каждом i-м такте преобразования, алгоритм (3) представляется в виде

$$E(n_i\Delta t)=E[(n_i-1)\Delta t]+$$

$$+\varphi\left\{\left[x,E[(n_i-1)\Delta t]\right],\ 2^{\sum\limits_{m=0}^{i-1}N_m-p_m},\ a_{ni}\right\},$$

$$i=1,2,...,k, \qquad (5)$$

где $n_1 = N_0 + 1, ..., N_0 + N_1$; $n_2 = N_0 + N_1 + 1, ..., N_1 + N_2$; ...; $n_k = N_0 + N_1 + ... + N_{k-1} + 1, ..., N_0 + N_1 + ... + N_{k-1} + N_k$; $N_0 = 0$; $p_0 = 0$, $0 \le p_i < N_i$; $a_{ni} = E_0 2^{-ni}$, $i = 1, 2, ..., k$.

Результатом преобразования является значение кода

$$K\left(\Delta t\sum_{i=1}^{k}N_i\right)=\sum_{i=0}^{k-1}\frac{K\left(\Delta t\sum\limits_{m=1}^{i+1}N_m\right)}{2^{\sum\limits_{m=0}^{i}N_m-p_m}}.$$

Для двухтактного алгоритма при $k = 2$ получаем

$$E(n_1\Delta t)=E[(n_1-1)\Delta t]+$$

$$+\varphi\left\{\left[x,E[(n_1-1)\Delta t]\right],a_{n_1}\right\},$$

$$i=1;\ n_1=N_0+1,...,N_1;$$

$$E(n_2\Delta t)=E[(n_2-1)\Delta t]+$$

$$+\varphi\left\{\left[x,E[(n_2-1)\Delta t]\right],\ 2^{N_1-p_1},a_{n_2}\right\},$$

$$i=2;\ n_2=N_1+1,...,N_1+N_2;$$

$$K[\Delta t(N_1+N_2)]=\sum_{i=0}^{1}\frac{K\left[\sum\limits_{m=1}^{i+1}\Delta tN_m\right]}{2^{\sum\limits_{m=0}^{i}N_i-p_i}}=$$

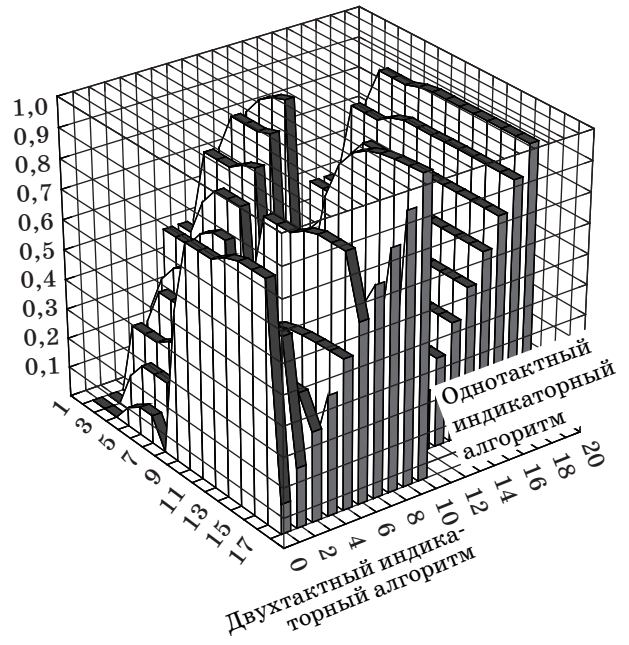
$$=K[\Delta tN_1]+\frac{K[\Delta t(N_1+N_2)]}{2^{N_1-p_1}}$$

и так далее.

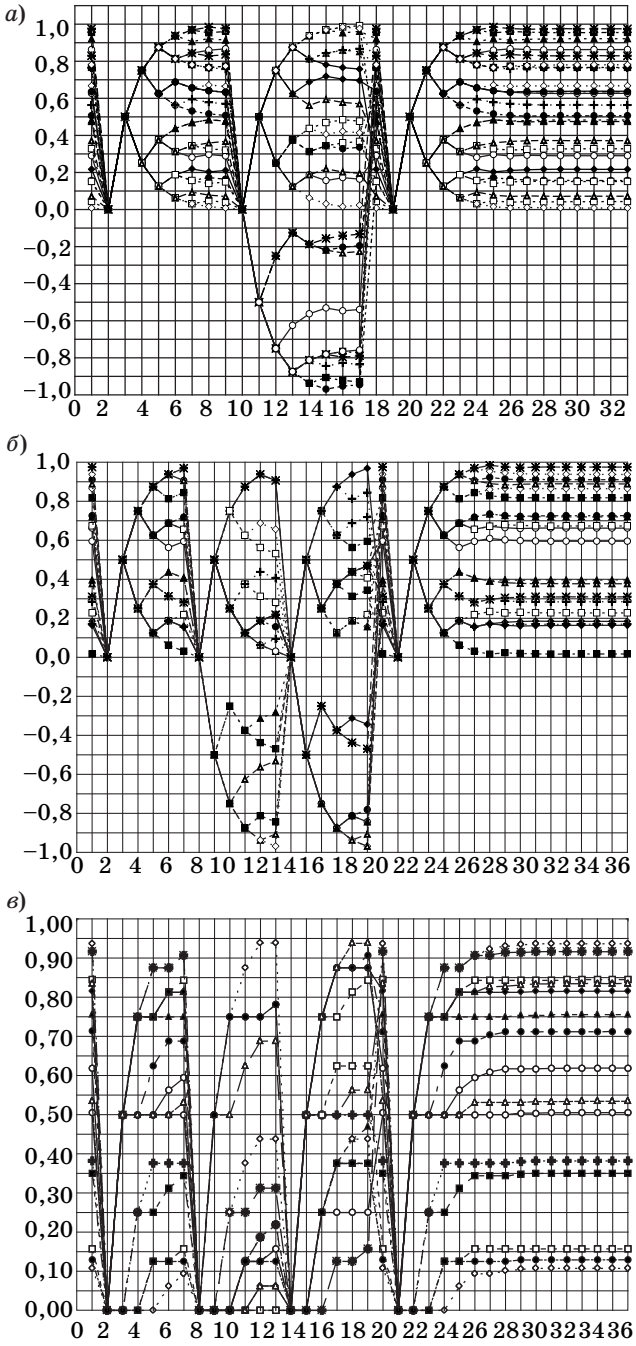
Исследуем представленные алгоритмы посредством моделирования. Для того чтобы выяснить, имеют ли многотактные алгоритмы допол-

нительные преимущества по сравнению с обычными алгоритмами поразрядного уравновешивания, проведем их сравнительный анализ при одном и том же числе разрядов преобразования. Рассмотрим динамику уравновешивающей величины для двухтактного индикаторного алгоритма аналого-цифрового преобразования и сравним ее с соответствующей динамикой обычного, фактически однотактного или индикаторного алгоритма [1].

На рис. 2 показаны 3-мерные графики, полученные в результате моделирования однотактного и двухтактного индикаторных алгоритмов преобразования при различных, одинаковых для обоих алгоритмов, значениях входного постоянного сигнала в отсутствие помех. На рис. 3, *а*—*в* представлены в виде древовидного фрактала графики процесса преобразования входного сигнала, изменяющегося случайно от преобразования к преобразованию и остающегося постоянным в процессе преобразования различными алгоритмами аналого-цифрового преобразования. Первая позиция графиков соответствует значениям входного сигнала, одинаковым для обоих рассматриваемых алгоритмов. Значения входного сигнала распределены в пределах диапазона преобразования от 0 до 1 по равномерному закону распределения вероятностей. Графики рис. 3, *а* и *б*



■ ***Рис. 2.*** *Сравнение результатов преобразования 15-разрядными (разряды отложены по оси x) индикаторными алгоритмами: поразрядного уравновешивания и двухтактным — разных значений входного сигнала, изменяющихся дискретно с шагом 0,15 от 0,15 до 1,5; позиция 17 по оси x соответствует операции суммирования для двухтактного индикаторного алгоритма*



■ ***Рис. 3.*** *Процесс преобразования входного, изменяющегося случайно от преобразования к преобразованию постоянного сигнала с равномерным законом распределения:*
а — 14-разрядными знаковыми алгоритмами аналого-цифрового преобразования: позиции 2–18 — двухтактный алгоритм; позиции 19–33 — однотактный алгоритм;
б — 15-разрядными знаковыми алгоритмами аналого-цифрового преобразования: позиции 2–20 — трехтактный алгоритм; позиции 21–36 — однотактный алгоритм;
в — 15-разрядными индикаторными алгоритмами аналого-цифрового преобразования: позиции 2–20 — трехтактный алгоритм; позиции 21–36 — однотактный алгоритм

получены по результатам преобразования для 20 случаев, рис. 3, *в* — для 15 случаев.

Моделирование показало, что среднеквадратические ошибки (СКО) погрешности остаются равными (в пределах статистической погрешности моделирования) для постоянного сигнала и при воздействии одинаковой аддитивной помехи. На рис. 4, *а, б* для сравнения представлены графики, характеризующие процесс преобразования синусоидального сигнала в код для различных типов алгоритмов. Как следует из сравнения алгоритмов, двухтактный алгоритм практически не имеет преимуществ по точности при одинаковом числе разрядов по сравнению с обычным алгоритмом поразрядного уравновешивания.

Если использовать в многотактном алгоритме АЦП алгоритм параллельного типа [3], то для исследования необходимо представить этот алгоритм также в аналитическом виде. Особенность алгоритма параллельного типа и реализующего его АЦП, представленного на рис. 5, состоит в том, что входной сигнал одновременно сравнивается в $2^N - 1$ СУ с аналогичным количеством уровней уравновешивающей величины, формируемой из источника опорного напряжения E_0 посредством делителя, собранного на сопротивлениях R. Результаты параллельного сравнения входного сигнала с уравновешивающими величинами за один такт преобразуются также параллельно в специальном электронном устройстве — приоритетном шифраторе — в двоичный выходной код.

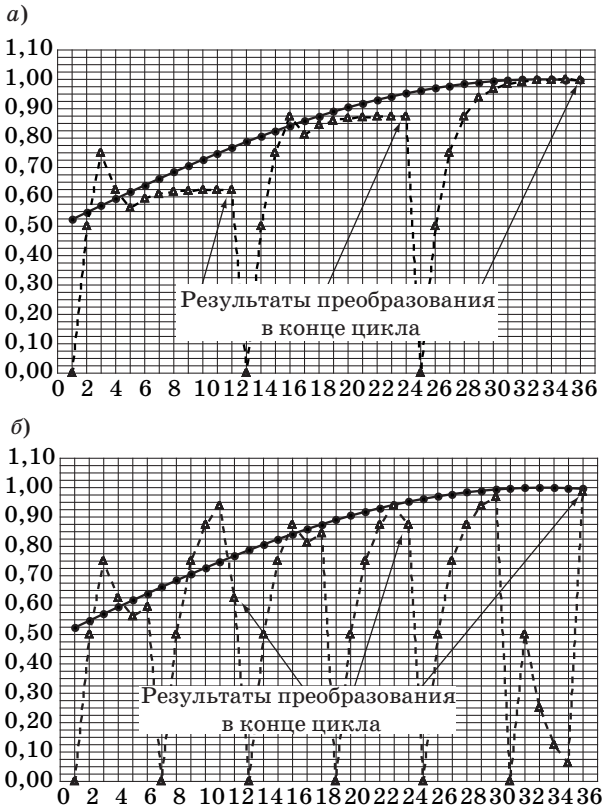
В математической форме операцию параллельного преобразования можно представить в виде

$$K(\Delta t) = H\left\{\overline{h}\left[x - E_0\sum_{i=1}^{N} a_i 2^{-i}\right]\right\}, \qquad (6)$$

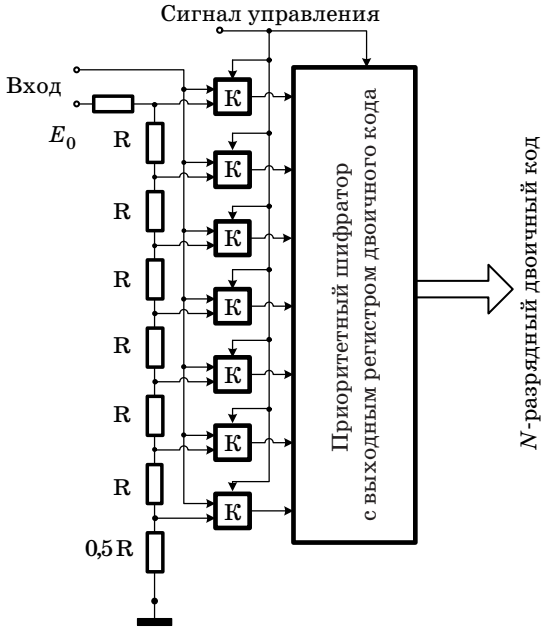
где a_i для индекса $i = 1, 2, ..., N$ принимает последовательно значения 1 или 0 по результатам сравнения в соответствии с нарастанием двоичного кода на 1 от 0 до 2^N, поэтому

$$\overline{h}\left[x - E_0\sum_{i=1}^{N} a_i 2^{-i}\right] = \begin{cases} 0 \\ h\left[x - E_0 2^{-N}\right] \\ h\left[x - E_0 2^{-N+1}\right] \\ \cdot \\ \cdot \\ \cdot \\ h\left[x - E_0\sum_{i=1}^{N} 2^{-i}\right] \end{cases},$$

$H\{...\}$ — оператор, описывающий функцию приоритетного шифратора результатов сравнения,



■ ***Рис. 4.*** *Процесс преобразования входного синусоидального сигнала: а — в двоичный 11-разрядный код посредством знакового алгоритма поразрядного уравновешивания; б — в двоичный 10-разрядный код посредством знакового двухтактного алгоритма: —●— — входной сигнал; – ▲ – — результат преобразования*

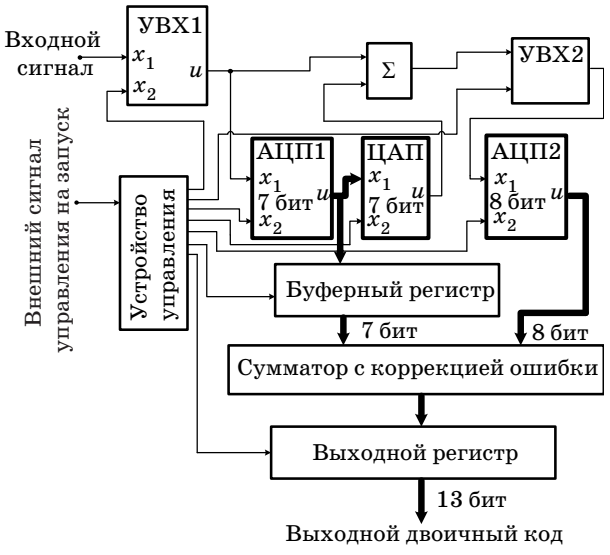


■ ***Рис. 5.*** *Структурная схема АЦП параллельного типа; К — компараторы, реализующие индикаторную функцию сравнения*

которая выполняется в течение временного такта Δt, формируемого сигналом управления.

Как следует из формулы (6), с увеличением числа разрядов двоичного кода на разряд количество СУ и, следовательно, сложность приоритетного шифратора удваивается. Это и является основной причиной, сдерживающей рост числа разрядов в АЦП параллельного типа и переход к схемам параллельно-последовательного типа, дальнейшим техническим совершенствованием которых являются параллельно-последовательные АЦП конвейерного типа.

Особенностью схемы рис. 6, в отличие от схемы, приведенной на рис. 1, является то [4], что в ней имеется два блока *УВХ*, назначение которых состоит в следующем. Поскольку общее время преобразования в течение одного цикла разбито на два временных подынтервала, в каждом из которых осуществляется одновременно процесс аналого-цифрового преобразования различными АЦП, то, естественно, можно организовать их параллельную работу по конвейерному принципу. Этот принцип заключается в том, что пока в *АЦП*2 осуществляется процесс преобразования, с *АЦП*1 считывается результат предыдущего преобразования в буферный регистр, происходит запоминание в блоке *УВХ*1 следующего значения входного сигнала и выполнение нового преобразования. Процесс нового преобразования в *АЦП*1 несколько сдвинут на короткое время относительно начала процесса преобразования *АЦП*2 для выполнения на фиксированном интервале Δt следующих операций: считывания результата предыдущего преобразования с *АЦП*1 в буферный регистр и в регистр *ЦАП*; подготовки к следующему преобразованию *АЦП*1 («сброс» в исходное состояние); операций на аналоговом сумматоре-усилителе; запуска *УВХ*1 и *УВХ*2 и, наконец, запуска на преобразование *АЦП*1 и *АЦП*2. Однако по величине суммарный сдвиг Δt от перечисленных вспомогательных операций значительно меньше, чем общее время преобразования в каждом АЦП, участвующем в полном цикле аналого-цифрового преобразования. Для компенсации этого временного сдвига и уравнивания времени преобразования в каждом АЦП *АЦП*2 имеет большее число разрядов по сравнению с *АЦП*1. Эта разница в разрядности позволяет также на цифровом сумматоре с коррекцией выполнять суммирование кодов с усреднением и тем самым улучшать не только динамические свойства АЦП, а и дополнительно его помехоустойчивость. Подключение *УВХ*2 к входному сигналу можно осуществить различными способами (см. рис. 6).



■ ***Рис. 6.*** *Структурная схема параллельно-последовательного АЦП конвейерного типа*

Аналого-цифровые преобразователи конвейерного типа имеют определенное преимущество по быстродействию при преобразовании, в том числе при преобразовании изменяющегося во времени входного сигнала, даже при использовании в АЦП1 и АЦП2 алгоритмов последовательного действия типа поразрядного уравновешивания. При числе разрядов p_i, на которое перекрываются коды в каждом i-м цикле преобразования, алгоритм для конвейерного АЦП представляется в виде

$$E(n_i\Delta t) = E\left[(n_i - 1)\Delta t\right] + \\ + \varphi\left\{\left[x, E\left[(n_i - 1)\Delta t\right]\right], \ 2^{\sum_{m=0}^{i-1} N_m - p_m}, \ a_{ni}\right\}, \\ i = 1, 2, ..., k, \qquad (7)$$

где $n_1 = N_0 - r_0 + 1$, ..., $N_0 - r_0 + N_1$; $n_2 = N_1 - r_0 + 1$, ..., $N_1 - r_1 + N_2$; ...; $n_k = N_2 - r_0 + ... + N_{k-1} + 1$, ..., $N_1 + ... + N_{k-1} + N_k$; $N_0 = 0$; $p_0 = 0$, $0 \le p_i < N_i$; $k = 1, ..., L$ — число установленных тактов преобразования; $a_{ni} = E_0 2^{ni}$, $ni = 1, 2, ..., N_i$; $n_1 = N_0 - r_0 + 1$, ..., $N_0 - r_0 + N_1$; $n_2 = N_1 - r_1 + 1$, ..., $N_1 - r_1 + N_2$; ... ; $n_k = N_1 - r_1 + 1$, ..., $N_{k-1} - r_{k-1} + N_k$ — число тактов сравнения в соответствующем поддиапазоне; r_i — число перекрывающихся временных тактов уравновешивания в i-м поддиапазоне преобразования; $N_0 = 0$; $p_0 = 0$, $r_0 = 0$; $k = 1, ..., L$. Результатом преобразования является значение кода

$$K\left(\Delta t \sum_{i=1}^{k} N_i - r_{i-1}\right) = \sum_{i=0}^{k-1} \frac{K\left(\Delta t \sum_{m=1}^{i+1} N_m - r_{m-1}\right)}{2^{\sum_{m=0}^{i} N_m - p_m}}.$$

Для двухтактного алгоритма при $k = 2$ получаем

$$E(n_1\Delta t) = E\left[(n_1 - 1)\Delta t\right] + \\ + \varphi\left\{\left[x, E\left[(n_1 - 1)\Delta t\right]\right], a_n\right\},$$

$$i = 1;\ n_1 = N_0 + 1, \ldots, N_1;$$

$$E(n_2\Delta t) = E\left[(n_2 - 1)\Delta t\right] + \\ + \varphi\left\{\left[x, E\left[(n_2 - 1)\Delta t\right]\right], 2^{N_1 - p_1}, a_n\right\},$$

$$i = 2;\ n_2 = N_1 + 1, \ldots, N_1 + N_2;$$

$$K\left[\Delta t(N_1 + N_2 - r_1)\right] = \sum_{i=0}^{1} \frac{K\left[\sum\limits_{m=1}^{i+1} \Delta t(N_m - r_{m-1})\right]}{2^{\sum\limits_{m=0}^{i} N_m - p_m}} = \\ = K\left[\Delta t N_1\right] + \frac{K\left[\Delta t(N_2 - r_1)\right]}{2^{N_1 - p_1}}$$

и так далее.

Алгоритм, представленный формулой (7), при соответствующем выборе параметров L, p и r трансформируется в алгоритмы (1)–(5) и последовательный алгоритм поразрядного уравновешивания и, таким образом, иллюстрирует динамику творческой мысли инженеров в исторический период развития цифровой электроники, охватывающий вторую половину прошлого века.

Литература

1. **Тихонов Э. П.** Аналитико-имитационное исследование и оптимизация алгоритмов аналого-цифрового преобразования в условиях воздействия помех // Информационно-управляющие системы. 2007. № 2 (27). Ч. 1. С. 12–21; № 3 (28). Ч. 2. С. 2–14.
2. **Романов О.** Обзор новых АЦП компании ANALOG DEVICES // Электронные компоненты. 2004. № 2. С. 33–35.
3. **Аналого-цифровые преобразователи:** http://www.gaw.ru/html.cgi/txt/doc/adc/adc_4_2.htm
4. **Сигма-дельта** АЦП фирмы Analog Devices // Электронные компоненты и системы. Киев: VD MAIS. Май 1996. С. 20–25.
5. **Тихонов Э. П.** Алгоритмическое описание и сравнительный анализ свойств сигма-дельта АЦП // Информационно-управляющие системы. 2007. № 4 (29). Ч. 1. С. 2–12; № 5 (30). Ч. 2. С. 2–13.
6. **Юдич М. З.** Аналоговые сравнивающие устройства. М.: Машиностроение, 1984. 96 с.

УДК 681.3.07

СИНТЕЗ ТРЕБОВАНИЙ К БОРТОВОМУ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНОМУ И МОДЕЛИРУЮЩЕМУ КОМПЛЕКСУ

Д. П. Тетерин,
канд. техн. наук, гл. конструктор
ОАО «КБ Электроприбор»

Изложены основные понятия и определения теории номенклатурного нормирования и вариант синтеза технических требований по назначению бортового информационно-измерительного и моделирующего комплекса.

Ключевые слова *— технические требования, техническое задание на проектирование, математическое моделирование.*

Введение

При проектировании сложных технических систем наиболее распространенными являются ошибки, связанные с формированием и обоснованием требований. Стоимость их устранения, как правило, самая высокая, что приводит к дополнительным затратам, составляющим 25–40 % бюджета проекта разработки в целом. Так, только в США ежегодно тратится более 250 млрд дол. на разработку приложений информационных технологий в рамках примерно 175 тыс. проектов. 31 % этих проектов прекращается до завершения. Затраты на 52,7 % проектов составляют 189 % от первоначальной оценки. Причинами провалов третьей части проектов, по данным статистики, являются проблемы, непосредственно связанные «со сбором и документированием требований, а также с управлением ими» [1].

Бурное развитие в последние десятилетия вычислительной техники предопределило повсеместное использование систем автоматизированного проектирования (САПР). Сроки проектирования сложных технических систем сократились на 20–40 %, но проблемы обоснования требований остались. В современных САПР средства поддержки начальных этапов проектирования систем, связанных с формированием технического задания и обоснованием требований, наименее развиты. Формирование требований является исключительной прерогативой высококвалифицированных специалистов, не застрахованных от принятия ошибочных решений. Теоретические исследования в обозначенной проблемной области охватывают в основном процессы обоснования количественных частей требований и не позволяют формализовать (автоматизировать) весь процесс формирования технического задания на разработку (модернизацию) сложных технических систем.

Постановка и решение задачи

Используя понятия теории принятия решений, теории систем, системного и нормативного анализа, стандартизации и нормативного обеспечения, математической логики, теории четких и нечетких множеств, теории вероятностей, комбинаторики, теории эффективности и качества, рассмотрим вариант синтеза технических требований по назначению на примере формирования технического задания на разработку бортового информационно-измерительного и моделирующего комплекса (БИИМК) летательного аппарата.

Проблема обоснования требований к БИИМК решается на взаимосвязанных стадиях номенклатурного, структурного и количественного нормирования, которые при необходимости повторяются на различных уровнях абстрагирования.

Прежде чем обосновывать какое-либо требование количественно, целесообразно установить необходимость непосредственного включения его в техническое задание или последующего преобразования в нормируемые функции, задачи или характеристики комплексов, т. е. вначале следу-

ет определиться со словесными частями требований [2, 3].

Словесные части требований по назначению БИИМК могут быть получены методами синтеза из элементарных и производных составляющих требований. *Элементарной составляющей* (элементом требования — ЭТ) называется неделимая на исследуемом уровне часть требования. Элементы требования представляют собой часто встречающиеся во многих требованиях компоненты. Из элементов образуются *производные составляющие*, т. е. подцели, работы, задачи комплекса, словесные части требований и конкретные требования по назначению.

К элементам исходных требований относятся:

— цели комплекса;

— объекты, обслуживаемые комплексом;

— наименования требований;

— исходные состояния и условия применения комплекса;

— задачи, функции, операции и работы подсистем комплекса;

— количественные части требований.

Например, целями разработки БИИМК могут быть: управление, контроль состояния, ремонт и т. п. В процессе преобразований цели будем обозначать кодами: Ц = {$Ц_0$, $Ц_1$, ... }, где Ц — подмножество целей создания комплекса; $Ц_i$ — *i*-я цель разработки комплекса (i = 0, 1, 2, ...).

Цель — это то, чего добивается, к чему стремится или для достижения чего создается комплекс.

Объекты, обслуживаемые БИИМК (газотурбинный двигатель — ГТД, регулятор, датчики, исполнительные механизмы): А = {$А_1$, $А_2$, ...}.

Возможные *исходные состояния* комплекса (степени готовности): Г = {$Г_1$, $Г_2$, ...}.

У*словия* (географические, климатические, противодействия, специфические), в которых должны достигаться цели разработки комплекса: У = {$У_э$, $У_п$, $У_с$}, где $У_э$ — подмножество условий эксплуатации; $У_п$ — подмножество условий противодействия; $У_с$ — подмножество специфических условий.

В процессе достижения своих целей БИИМК, его подсистемы и элементы выполняют определенные задачи, функции, операции и работы:

— *функции* разрабатываемого комплекса (например, по отношению к цели «моделирование ГТД» функциями могут быть: численное моделирование, аналитическое моделирование, аналоговое моделирование): Ф = {$Ф_1$, $Ф_2$, ...};

— *операции,* выполняемые комплексом (по отношению к функции «аналитическое моделирование» операциями могут быть: построение обратного преобразования Лапласа, решение обыкновенного дифференциального уравнения).

Наименования требований (по эффективности, безопасности, надежности, конструктивные требования и т. д.): Н = {$Н_1$, $Н_2$, ...}.

Кодирование ЭТ и самих требований. ЭТ не удобны для математических преобразований, так как представляют собой положения, относящиеся к физически разнородным явлениям, процессам и объектам, измеряемым по различным шкалам. Поэтому исходные и промежуточные данные, необходимые для обоснования требований, приводятся к виду, позволяющему быстро перейти от физической сущности задачи к ее формальному описанию на этапах решения и наоборот — от формального описания результатов к их физической сущности на этапах анализа результатов. При этом каждой составляющей присваивается свой код, который применяется вместо нее в процессе математических преобразований (табл. 1). В качестве кодов могут использоваться слова, обозначения, числа, буквы и комбинации символов.

Комбинациями ЭТ будем называть производные составляющие требований (подцели, работы, ситуации, задачи, конкретные требования) и комбинаторные соединения из ЭТ (перестановки, сочетания, размещения, объединения, пересечения и выборки), когда нужно применить общее для них название или нет необходимости уточнять их классификационные особенности.

Комбинации ЭТ в процессе преобразований представляются соответствующими комбинациями кодов, т. е. кодировками. Коды ЭТ в кодировках разделяются точками.

Например, подмножество кодов $Ц_1 \times А_1 \times Г_5$ из табл. 1 означает: аналитическое моделирование

■ ***Таблица 1****. Выборка ЭТ к БИИМК*

Коды ЭТ		Формулировка элементов требования
Ц	$Ц_1$	Аналитическое моделирование
	$Ц_2$	Приближенное численное моделирование
	$Ц_3$	Аналоговое моделирование
Г	$Г_1$	Дифференциальные уравнения *n*-го порядка в форме Коши
	$Г_5$	Дифференциальные уравнения *n*-го порядка с переменными коэффициентами и функцией Дирака (Хевисайда) в правой части
	$Г_7$	Типовые динамические звенья
	$Г_{10}$	Дробно-рациональные комплексные функции
А	$А_1$	Линейные элементы ГТД
	$А_2$	Нелинейные элементы ГТД
Н	$Н_2$	С достоверностью β_i математическое ожидание времени выполнения задачи E_i не должно превышать значения M_i

линейных элементов ГТД, описанных дифференциальными уравнениями n-го порядка с переменными коэффициентами и функцией Дирака (Хевисайда) в правой части.

Словесно описанные ЭТ, требования и выборки требований при большом их числе становятся не обозримыми для анализа. Поэтому уже в процессе сбора исходных данных осуществляется их упорядочение в целях последующей формализации, т. е. дискретизации, редактирования, систематизации и кодирования. Благодаря формализации обеспечиваются возможности формирования словесных частей требований по математическим законам и появляются следующие преимущества:

— существенно сокращается подлежащий анализу текст;

— отпадает необходимость в чтении и осмысливании содержания требований в процессе преобразований;

— упрощается процесс выполнения логических и математических операций;

— появляется возможность математического исчисления содержательной части требований;

— создаются условия для применения ЭВМ в процессе нормирования.

Упорядочение ЭТ и самих требований заключается в распределении их по уровням абстрагирования, в разбиении по признакам и аспектам нормирования на классы, группы, подгруппы, в ранжировании по предпочтениям в составе групп. Распределение по уровням осуществляется в целях выдвижения требований на уровнях комплекса, подсистем или элементов разрабатываемого БИИМК.

Классификация ЭТ производится по признакам принадлежности к элементарным и производным составляющим.

Ранжирование по предпочтениям предполагает упорядочение по важности, по установленному порядку следования, по отношениям больше — меньше и т. д.

Множество возможных сочетаний условий эксплуатации и параметров будущего комплекса является бесконечным. Число ЭТ в подмножествах состояний и объектов обслуживания также может быть избыточным. Для уменьшения числа конкретных требований применяются *приемы дискретизации*:

— диапазон возможных значений непрерывной составляющей (например, температура от −40 до +85 °С) разбивается на интервалы. Длина интервала выбирается такой, чтобы проверка способности выполнения функций комплекса в любой его точке обеспечивала достаточную способность к выполнению функций во всем интервале. Выполнение требований в интервале должно гарантировать достаточную эффективность комплекса во всем диапазоне;

— экстремальный прием дискретизации, ориентированный на критический случай, т. е. на самое неблагоприятное сочетание условий и параметров БИИМК, основывается на подборе таких сочетаний условий и параметров, в которых эксплуатация комплекса гарантирует возможность его применения во всех других вероятных условиях;

— прием дискретизации, ориентированный на наиболее вероятные условия, предполагает задание требований, включающих наиболее вероятные комбинации условий.

Среди исходных могут быть требования, принадлежащие любому подразделу технического задания. Но, прежде всего, в их числе должны быть требования по назначению разрабатываемого комплекса. В работе [2] предлагаются методы синтеза, декомпозиции, отбора и оптимизации требований по назначению сложной технической системы.

Перед применением методов синтеза составляющие требований подвергаются упорядочению, дискретизации и кодированию. Формализованные исходные данные сводятся в таблицы или заносятся в память ЭВМ.

Исходные данные анализируются в целях выявления и описания связей между ними. При этом устанавливаются совместимые (сочетающиеся) и несовместимые составляющие, виды связи, наиболее вероятные и экстремальные сочетания составляющих и комбинации составляющих требований, которые можно отбросить. Например, цель $Ц_1$ совместима с объектом $А_1$, с исходными состояниями $Г_1$, $Г_5$, $Г_{10}$. Цель $Ц_1$ несовместима с обслуживаемым объектом $А_2$ и с состоянием $Г_7$ (типовые динамические звенья описывают линейные элементы только 1-го и 2-го порядков).

Путем комбинирования и объединения совместимых составляющих требований в порядке, зависящем от конкретного метода синтеза, формируются производные требования и их кодовые описания.

К производным требованиям относятся подцели, производные функции, ситуации, работы, задачи комплекса, словесные части требований и конкретные требования.

Подцели — это более конкретные цели разработки системы. Различают следующие подцели:

— подцель, как элементарная функция или цель подсистемы (характерна для декомпозиции цели);

— подцель, как более конкретная цель, например производная функция из (Ц × Г) или бинарное отношение из (Ц × А) (характерна для синтеза подцелей по закону композиции).

Заметим, что подцели образуют нечеткое подмножество П, так как включают элементарные и производные функции [2]:

$$П = \{П_1, П_2, ...\} \subset (Ц \times Г, Ц \times А, Ф),$$

где (Ц × Г, Ц × А) — прямые (декартовые) произведения ЭТ из подмножеств Ц, А и Г.

Например: $П_1 = Ц_1 \times Г_1$ — аналитическое моделирование дифференциальных уравнений *n*-го порядка в форме Коши; $П_2 = Ц_1 \times Г_{10}$ — аналитическое моделирование дробно-рациональных комплексных функций. Тогда $\{П_1, П_2\} \subset (Ц \times Г)$.

Комбинируя и объединяя совместимые элементы подмножеств Ц, Г и А из табл. 1, получим кодовые описания работ БИИМК.

Подмножество работ, для выполнения которых создается комплекс: $Р = \{Р_1, Р_2, ...\} \subset (Ц \times \times А \times Г)$.

Например: $Р_5 = Ц_2 \cup А_1 \cup Г_5 = Ц_2 \times А_1 \times Г_5$ — приближенное численное моделирование линейных элементов ГТД, описанных дифференциальными уравнениями *n*-го порядка с переменными коэффициентами и функцией Дирака (Хевисайда) в правой части, где ∪ — обозначение операции объединения ЭТ; $Р_6 = Ц_2 \times А_1 \times Г_{10}$ — приближенное численное моделирование линейных элементов ГТД, описанных дробно-рациональными комплексными функциями; $Р_8 = Ц_3 \times А_1 \times Г_{10}$ — аналоговое моделирование линейных элементов ГТД, описанных дробно-рациональными комплексными функциями.

Ситуации представляют собой комбинации из условий, в которых должны достигаться подцели и выполняться работы комплекса: $С = \{С_1, С_2, ...\} \subset (У_э \times У_п \times У_с)$.

Ситуациями описываются возможные варианты обстановки, в которых планируется эксплуатация будущего БИИМК. Методами синтеза кодировки ситуаций образуются путем комбинирования и объединения условий из подмножеств $У_э$, $У_п$, $У_с$.

Коды применяемых ситуаций и сведения о неблагоприятных условиях, принадлежащих этим ситуациям, приведены в табл. 2. ЭТ, входящие в конъюнктивную часть ситуации, подлежат обязательному учету в расчетах и при испытаниях. Благоприятные и типовые ситуации используются в требованиях, реализующих рекламные возможности разрабатываемого БИИМК.

■ ***Таблица 2.*** *Нормируемые ситуации и условия применения комплекса*

Коды ЭТ и ситуаций		Формулировка элементов требования
$У_э$	$Э_1$	В условиях проектирования
	$Э_2$	В условиях производства
	$Э_3$	В условиях эксплуатации
$У_п$	$Л_1$	Ионизирующее излучение

Задачи, для решения (выполнения) которых разрабатывается комплекс: $E = \{E_1, E_2, ...\} \subset (П \times \times С, Р \times С)$.

Задачи БИИМК определяют цели, которые должны достигаться из возможных исходных состояний комплекса в конкретных ситуациях. Иначе, задачи — это работы, выполняемые в определенных условиях. В простейшем случае кодировки задач получаются путем комбинирования и объединения совместимых подцелей или работ с ситуациями. Подцели (работы) и ситуации в составе задачи комплекса связаны конъюнктивно.

Например: $E_1 = Р_7 \cup С_1 = Ц_3 \times А_1 \times Г_1 \times С_1 \Rightarrow$ $\Rightarrow Ц_3 \wedge А_1 \wedge Г_1 \wedge С_1$ — аналоговое моделирование линейных элементов ГТД, описанных дифференциальными уравнениями *n*-го порядка в форме Коши при ионизирующем излучении в условиях эксплуатации; $E_2 = Ц_3 \times А_1 \times Г_{10} \times С_1$ — аналоговое моделирование линейных элементов ГТД, описанных дробно-рациональными комплексными функциями при ионизирующем излучении в условиях эксплуатации.

В общем случае одной кодировке задачи может соответствовать подмножество, содержащее пустое множество, или одну, или более одной задачи. Поэтому кодировки подлежат нормативному анализу в целях раскрытия логических и комбинаторных связей и последующего отбора нормируемых задач.

Словесные части требований представляют собой короткие, четкие формулировки требований, исключающие двойное толкование и подлежащие количественному нормированию: $Т_н = \{m_1, m_2, ...\} \subset (Н \times E)$.

Кодировки словесных частей требований получаются путем комбинирования и объединения задач комплекса с совместимыми наименованиями требований из подмножества Н (см. табл. 1). В сочетании с количественными частями эти требования устанавливают необходимую способность разрабатываемого БИИМК к выполнению соответствующих задач. Для примера приведем формулировки двух требований с конъюнктивной связью между элементарными составляющими.

Количественным требованием называется охарактеризованная числом словесная часть требования. Решению задач количественного нормирования и оптимизации количественных частей требований посвящены работы [4–7].

Пример.

Дано: выборки элементов исходных требований (см. табл. 1) и нормируемых ситуаций и условий применения БИИМК (см. табл. 2).

Необходимо: по данным табл. 1 и 2 сформировать технические требования по назначению

к подсистеме моделирования линейных элементов ГТД из состава БИИМК.

Решение. Подмножества работ, для выполнения которых создается подсистема моделирования линейных элементов ГТД, и ситуаций применения подсистемы определяются табличным методом:

	$Ц_1$	$Ц_2$	$Ц_3$
$А_1$	1	1	1
$А_2$	0	1	1

	$Э_1$	$Э_2$	$Э_3$
$Л_1$	0	0	1

	$Ц_1 \times А_1$	$Ц_2 \times А_1$	$Ц_2 \times А_2$	$Ц_3 \times А_1$	$Ц_3 \times А_2$
$Г_1$	1	1	0	1	0
$Г_5$	1	1	0	0	0
$Г_7$	0	0	0	0	0
$Г_{10}$	1	1	0	1	0

	$Р_1$	$Р_2$	$Р_3$	$Р_4$	$Р_5$	$Р_6$	$Р_7$	$Р_8$
$С_1$	0	0	0	0	0	0	1	1

Откуда $Р = \{Р_1, Р_2, Р_3, Р_4, Р_5, Р_6, Р_7, Р_8\} \subset \subset (Р_1 = Ц_1 \times А_1 \times Г_1, Р_2 = Ц_1 \times А_1 \times Г_5, Р_3 = Ц_1 \times А_1 \times Г_{10}, Р_4 = Ц_2 \times А_1 \times Г_1, Р_5 = Ц_2 \times А_1 \times Г_5, Р_6 = Ц_2 \times А_1 \times Г_{10}, Р_7 = Ц_3 \times А_1 \times Г_1, Р_8 = Ц_3 \times А_1 \times Г_{10})$; $С = \{С_1\} \subset (Л_1 \times Э_3)$.

В результате применения методов нормативного анализа определяются словесные части требований:

$m_1 = Н_2 \times E_1$ — с достоверностью β_1 вероятность выполнения задачи аналогового моделирования линейных элементов ГТД, описанных дифференциальными уравнениями n-го порядка в форме Коши, при ионизирующем излучении в условиях эксплуатации должна быть не менее W_1;

$m_2 = Н_2 \times E_2$ — с достоверностью β_2 вероятность выполнения задачи аналогового моделирования линейных элементов ГТД, описанных дробно-рациональными комплексными функциями, при ионизирующем излучении в условиях эксплуатации должна быть не менее W_2.

В результате количественного нормирования требования по назначению к подсистеме моделирования линейных элементов ГТД имеют вид

$$Т_н = \{Т_1, Т_2\} = \{Т_1 = Н_2 \times E_1\ (t \le 2\ мс) \ge 0{,}85,\ Т_2 = Н_2 \times E_2\ (t \le 2\ мс) \ge 0{,}85\},$$

где $Т_1$, $Т_2$ — с достоверностью 0,85 вероятность выполнения задачи аналогового моделирования линейных элементов ГТД, описанных дифференциальными уравнениями n-го порядка в форме Коши и дробно-рациональными комплексными функциями соответственно, при ионизирующем излучении в условиях эксплуатации должна быть не менее 2 мс.

Заключение

В статье изложены основной понятийный аппарат теории номенклатурного нормирования и вариант синтеза технических требований по назначению бортового информационно-измерительного и моделирующего комплекса летательного аппарата. В совокупности с методами обоснования целей создания технических систем, количественного нормирования, декомпозиции и отбора требований возможно построение в рамках САПР подсистемы формирования технического задания на разработку (модернизацию) сложных технических систем.

Литература

1. **Леффингуэлл Д., Уидриг Д.** Принципы работы с требованиями к программному обеспечению. Унифицированный подход: Пер. с англ. М.: Вильямс, 2002.
2. **Тетерин П. Г.** Основные этапы обоснования словесных частей и состава требований заказчика // Стандартизация военной техники. 1994. № 2–3.
3. **Тетерин П. Г.** Основные аксиомы и операции обоснования технических требований // Стандартизация военной техники. 1995. № 1–2.
4. **Фендриков Н. М., Яковлев В. И.** Методы расчетов боевой эффективности вооружения. М.: Воениздат, 1971.
5. **Извеков Е. В., Каплунов Б. А.** Оптимизация средств обеспечения стрельбы артиллерии. М.: Воениздат, 1979.
6. **Методика** выбора номенклатуры нормируемых показателей надежности технических устройств. М.: Изд-во стандартов, 1970.
7. **Лобыцин В. В.** Системный подход к формированию требований // Стандарты и качество. 1976. № 1.

УДК 681.5.013

ИССЛЕДОВАНИЕ АНОРМАЛЬНЫХ РЕЖИМОВ РАБОТЫ АВТОНОМНОЙ ЭЛЕКТРОЭНЕРГЕТИЧЕСКОЙ УСТАНОВКИ

В. Ф. Шишлаков,
доктор техн. наук, профессор
Д. В. Шишлаков,
аспирант
С. А. Цветков,
ассистент
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Приводятся результаты исследований анормальных режимов работы автономной электроэнергетической установки с синтезированными обобщенным методом Галеркина параметрами при внешних возмущающих воздействиях на входах приводного двигателя и синхронного генератора.

Ключевые слова *— автономная электроэнергетическая установка, режимы работы, внешние воздействия.*

Авторами было подробно рассмотрено решение задачи синтеза многосвязной системы автоматического управления автономной электроэнергетической установки (ЭЭУ) [1], структурная схема математической модели которой показана на рис. 1, где приняты следующие обозначения:

$\Delta u_{\text{г}}(t) = u_{\text{г}0}(t) - u_{\text{г}}(t)$ — относительное изменение напряжения, здесь $u_{\text{г}0}(t)$ — заданное значение напряжения на выходе ЭЭУ; $u_{\text{г}}(t)$ — напряжение на выходе ЭЭУ;

$\Delta\nu(t) = \nu_0(t) - \nu(t)$ — относительное изменение скорости вращения приводного двигателя, здесь $\nu_0(t)$ — заданное значение скорости (частоты напряжения на выходе установки), $\nu(t)$ — скорость вращения приводного двигателя (частота напряжения на выходе ЭЭУ);

$g_{\nu}(t)$ — внешнее возмущающее воздействие в канале изменения частоты, действующее на приводной двигатель;

$g_u(t)$ — внешнее возмущающее воздействие в канале регулирования напряжения, действующее на синхронный генератор;

$u_{\text{в}}(t)$ — напряжение на зажимах возбудителя;

$u_{\text{в.в}}(t)$ — напряжение на обмотке возбуждения возбудителя;

$T_{\text{м}} = 1$ с — постоянная времени приводного двигателя;

$T_{\text{в}} = 0{,}01$ с — постоянная времени возбудителя;

$T_{\text{в}1} = 0{,}5$ с; $T_{\text{в}2} = 0{,}01$ с — постоянные времени синхронного генератора, обусловленные индуктивностью цепи возбуждения и реакцией якоря;

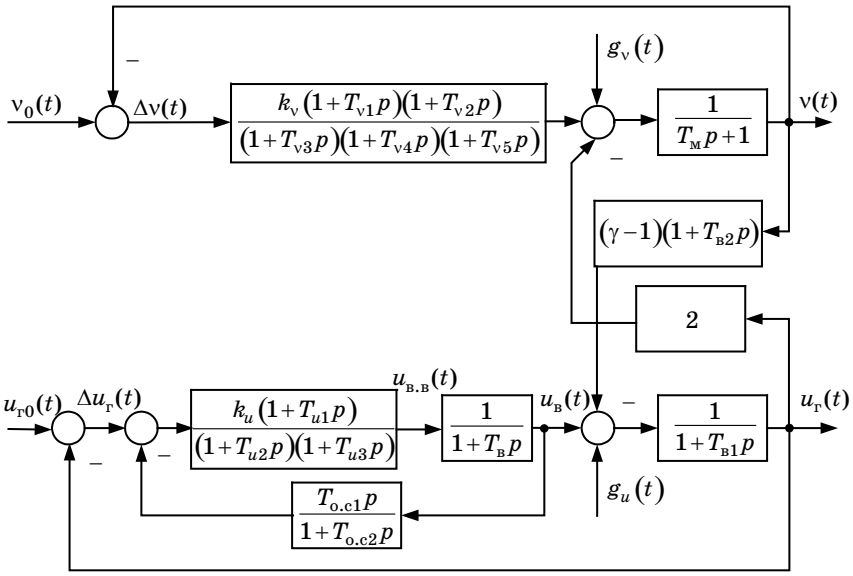
$(1 - \gamma) = 0{,}8$ — коэффициент, характеризующий режим работы синхронного генератора;

$T_{\nu 1}, ..., T_{\nu 5}, k_{\nu}$ — постоянные времени и коэффициент передачи регулятора скорости вращения приводного двигателя; T_{u1}, T_{u2}, T_{u3}, k_u — постоянные времени и коэффициент передачи регулятора напряжения ЭЭУ; $T_{\text{о.с}1}$, $T_{\text{о.с}2}$ — постоянные времени звена коррекции в цепи гибкой обратной связи (ГОС).

В результате решения данной задачи обобщенным методом Галеркина [2–5] были определены значения 12 параметров регуляторов в каналах регулирования напряжения и частоты (табл. 1).

Вычислительная модель (рис. 2) получена путем эквивалентных преобразований структурной схемы математической модели ЭЭУ с учетом особенностей применяемого для моделирования программного обеспечения Matlab Simulink.

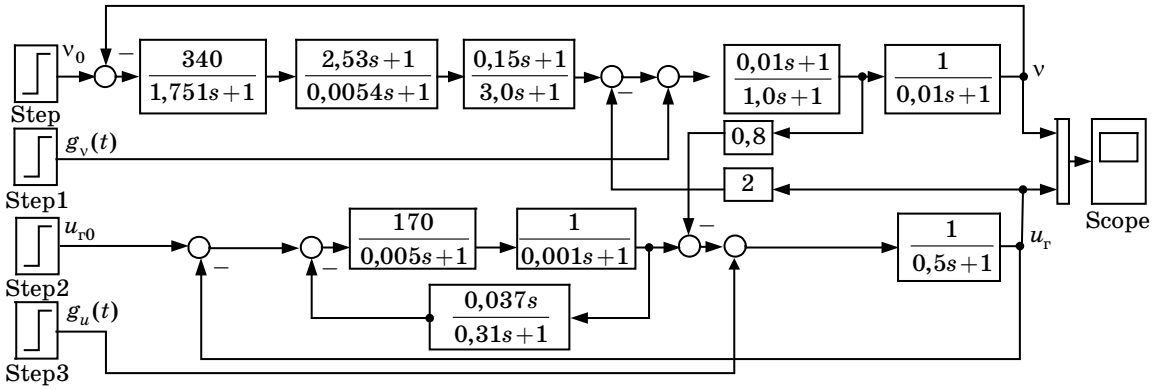
Определение амплитуд возмущающих воздействий для моделирования анормальных режимов работы ЭЭУ. Для моделирования анормальных режимов работы требуется подавать внешние возмущающие воздействия определенной амплитуды на входы приводного двигателя, что соответствует изменению напряжения управления исполнительного двигателя, и синхронного генератора, что соответствует изменению напряжения возбудителя. Для оценки требуемых величин внешних возмущающих воздействий был проведен анализ процессов изменения сигналов на входах приводного двигателя и генератора



■ ***Рис. 1.*** *Структурная схема математической модели ЭЭУ*

■ ***Таблица 1.*** *Значения варьируемых параметров ЭЭУ*

Регулятор частоты						Регулятор напряжения				ГОС	
k_ν	$T_{\nu1}$, с	$T_{\nu2}$, с	$T_{\nu3}$, с	$T_{\nu4}$, с	$T_{\nu5}$, с	k_u	T_{u1}	T_{u2}	T_{u3}	$T_{о.с1}$	$T_{о.с2}$
340	2,53	0,15	1,751	0,0054	3,0	170	0,01	0,001	0,005	0,037	0,31

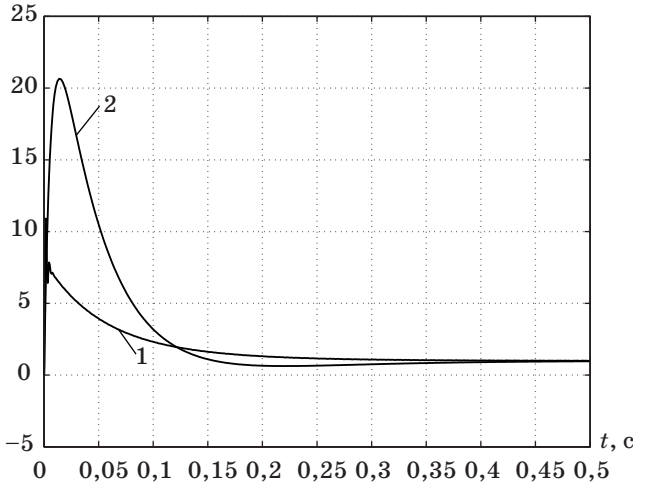


■ ***Рис. 2.*** *Структурная схема вычислительной модели ЭЭУ в Matlab Simulink*

при нормальном режиме работы (рис. 3), из которого следует, что максимальное отклонение сигнала на входе приводного двигателя составляет 21 относительную единицу (о. е.), а на входе генератора — 11 о. е.

Поэтому при моделировании анормальных режимов работы ЭЭУ амплитуда внешних возмущающих воздействий по частоте и напряжению должна изменяться в диапазоне 0,1÷10 о. е. (значение амплитуды возмущающего воздействия 0,1 о. е. соответствует 5 %-му отклонению частоты и 10 %-му отклонению напряжения от заданных значений). Такой, достаточно широкий, диапазон изменения амплитуды возмущающих воздействий целесообразно применять для исследования анормальных режимов работы, поскольку параметры регуляторов ЭЭУ в ходе решения задачи синтеза определялись из условия приближенного обеспечения заданных показателей качества работы многоканальной системы автоматического управления (МСАУ) в переходном режиме при нормальной работе, т. е. при отсутствии возмущений в каналах регулирования.

Моделирование анормальных режимов работы ЭЭУ с синтезированными параметрами. Поскольку возмущающие воздействия могут дей-



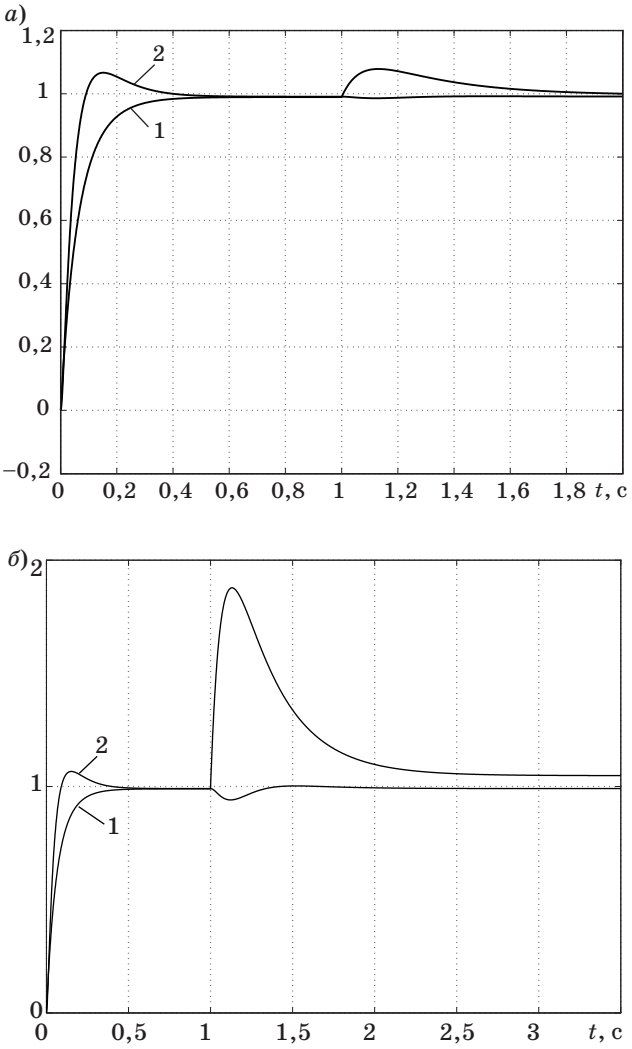
■ ***Рис. 3.*** *Изменение сигналов на входах генератора (1) и приводного двигателя (2) ЭЭУ*

ствовать как по отдельности, так и одновременно, то это обстоятельство учитывалось при исследованиях динамических свойств ЭЭУ в анормальных режимах. Внешние возмущающие воздействия подавались на входы генератора и приводного двигателя через 0,5 с после окончания переходных процессов по управляемым координатам системы регулирования частоты и напряжения (через 1 с после подачи на входы МСАУ управляющих воздействий). Время переходных процессов по напряжению и частоте определялось, как интервал времени, в течение которого сигналы $u_г(t)$ и $\nu(t)$ отклонялись от установившихся значений более чем на 5 и 2 % соответственно.

Анализ динамических свойств ЭЭУ при внешнем возмущающем воздействии на входе синхронного генератора. Динамические свойства МСАУ исследовались при подаче на вход синхронного генератора возмущающего воздействия $g_u(t) = H_u 1(t)$ (соответствует увеличению напряжения с выхода возбудителя) амплитудой $H_u = 1$ (рис. 4, *а*), 2, 5, 10 (рис. 4, *б*) о. е.

Показатели качества работы ЭЭУ при возмущающем воздействии $g_u(t)$ представлены в табл. 2. Анализ динамических свойств МСАУ в данном анормальном режиме работы показывает, что увеличение амплитуды H_u приводит к росту статической ошибки сигнала $u_г(t)$, которая, однако, не превышает 0,05 от установившегося значения даже при $H_u = 10$.

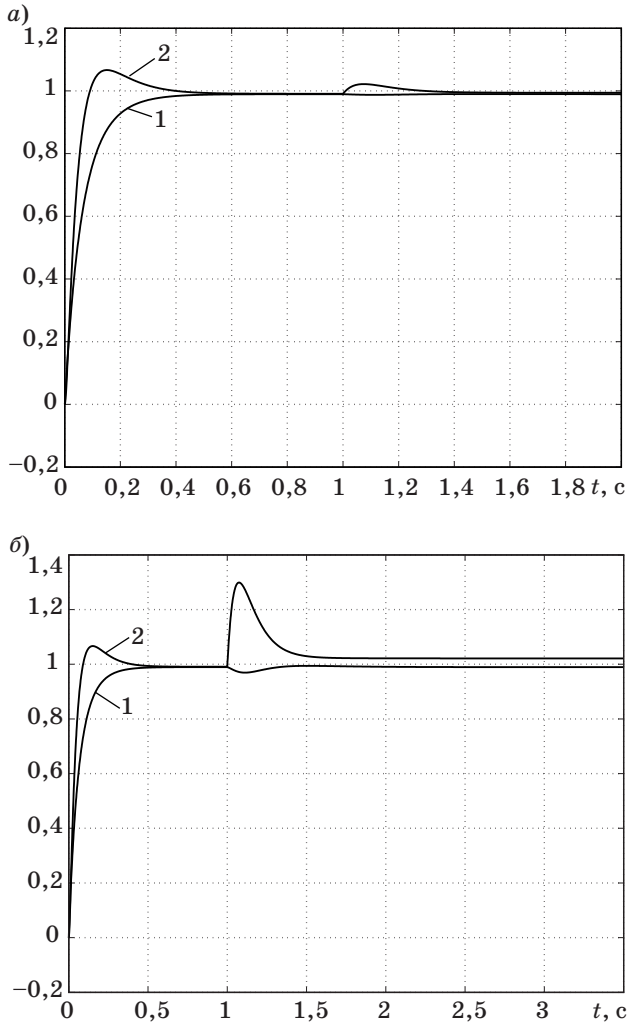
Анализ динамических свойств ЭЭУ при внешнем возмущающем воздействии на входе приводного двигателя. Динамические свойства МСАУ исследовались при подаче возмущающего воздействия $g_\nu(t) = H_\nu 1(t)$ (соответствует увеличению напряжения с выхода регулятора скорости вращения) амплитудой $H_\nu = 1$ (рис. 5, *а*), 2, 5, 10 (рис. 5, *б*) о. е. на приводной двигатель.



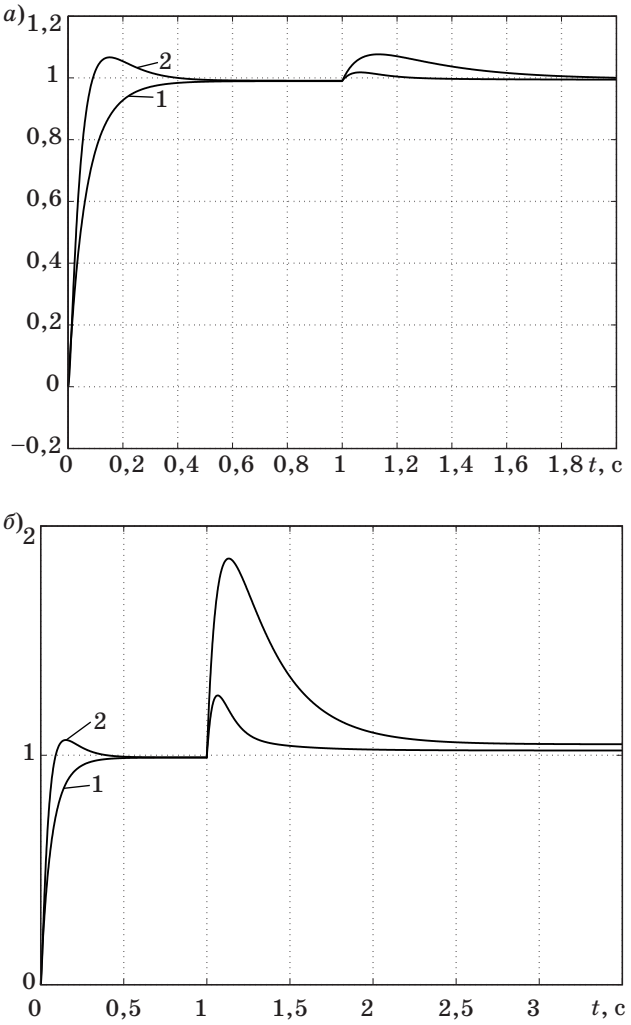
■ ***Рис. 4.*** *Процессы на выходах МСАУ: а — при $H_u = 1$; б — при $H_u = 10$: 1 — генератор; 2 — приводной двигатель*

■ ***Таблица 2.*** *Показатели качества работы ЭЭУ при возмущающем воздействии $g_u(t)$*

Амплитуда H_u возмущающего воздействия $g_u(t)$	Показатель качества					
	Максимальное отклонение от установившегося значения		Время переходного процесса, с		Статическая ошибка	
	$\nu(t)$	$u_г(t)$	$\nu(t)$	$u_г(t)$	$\nu(t)$	$u_г(t)$
1	0,02	0,08	–	0,32	–	–
2	0,02	0,165	–	0,55	–	0,02
5	0,035	0,43	0,2	1,2	–	0,02
10	0,055	0,90	0,25	2,5	–	0,05



■ ***Рис. 5.*** *Процессы на выходах МСАУ: а — при $H_\nu = 1$; б — при $H_\nu = 10$: 1 — генератор; 2 — приводной двигатель*



■ ***Рис. 6.*** *Процессы на выходах МСАУ: а — при $H_\nu = H_u = 1$; б — при $H_\nu = H_u = 10$: 1 — генератор; 2 — приводной двигатель*

■ ***Таблица 3.*** *Показатели качества работы ЭЭУ при возмущающем воздействии $g_\nu(t)$*

Амплитуда H_ν возмущающего воздействия $g_\nu(t)$	Показатель качества					
	Максимальное отклонение от установившегося значения		Время переходного процесса, с		Статическая ошибка	
	$\nu(t)$	$u_г(t)$	$\nu(t)$	$u_г(t)$	$\nu(t)$	$u_г(t)$
1	0,021	0,015	0,05	–	–	–
2	0,052	0,015	0,2	–	–	–
5	0,15	0,022	0,38	–	–	–
10	0,3	0,031	0,7	–	0,021	–

■ ***Таблица 4.*** *Показатели качества работы ЭЭУ при возмущающих воздействиях $g_\nu(t)$, $g_u(t)$*

Амплитуды возмущающих воздействий g_ν, g_u	Показатель качества					
	Максимальное отклонение от установившегося значения		Время переходного процесса, с		Статическая ошибка	
	$\nu(t)$	$u_г(t)$	$\nu(t)$	$u_г(t)$	$\nu(t)$	$u_г(t)$
$H_\nu = H_u = 1$	0,018	0,07	–	0,25	–	–
$H_\nu = H_u = 2$	0,045	0,17	–	0,55	–	–
$H_\nu = H_u = 5$	0,13	0,43	0,25	1,0	0,0006	0,019
$H_\nu = H_u = 10$	0,27	0,88	0,4	1,4	0,0201	0,047

Показатели качества работы ЭЭУ при возмущающем воздействии $g_\nu(t)$ представлены в табл. 3. Анализ динамических свойств МСАУ в данном анормальном режиме работы показывает, что увеличение амплитуды H_ν приводит к возникновению незначительной статической ошибки по частоте (0,021 от заданного значения при $H_\nu = 10$). Вместе с тем статическая ошибка в сигнале $u_г(t)$ отсутствует, т. е. регуляторы обеспечивают стабильность частоты и напряжения при возмущающем воздействии на входе приводного двигателя. Поскольку отклонение сигнала $u_г(t)$ от установившегося значения при регулировании не превышает 5 %, то полагаем, что время переходного процесса равно нулю.

Анализ динамических свойств ЭЭУ при одновременном действии возмущений на входах синхронного генератора и приводного двигателя. Наиболее сложным случаем для работы регуляторов ЭЭУ является одновременное действие возмущений по входам приводного двигателя и генератора, т. е. $g_\nu(t) = H_\nu 1(t)$, $g_u(t) = H_u 1(t)$. Исследования проводились при нескольких значениях амплитуд внешних возмущающих воздействий $H_u = H_\nu = 1$ (рис. 6, *а*), 2, 5, 10 (рис. 6, *б*) о. е.

Показатели качества работы ЭЭУ при одновременных возмущающих воздействиях $g_\nu(t)$, $g_u(t)$ представлены в табл. 4. Анализ динамических свойств МСАУ в данном анормальном режиме работы показывает, что увеличение амплитуды возмущений приводит к возникновению статической ошибки по частоте и напряжению (0,02 и 0,047 от заданного значения соответственно) при $H_\nu = H_u = 10$. При меньших величинах возмущений статические ошибки в каналах регулирования отсутствуют, т. е. регуляторы обеспечивают стабильность частоты и напряжения при одновременных возмущающих воздействиях на входах приводного двигателя и генератора. Длительность переходных процессов определялась, как интервал времени, в течение которого отклонение сигнала $u_г(t)$ в процессе регулирования превышало 5 %, а сигнала $\nu(t)$ — 2 % от установившегося значения.

Заключение

Проведены исследования математической модели ЭЭУ в анормальных режимах работы, при наличии внешних возмущающих воздействий различной амплитуды в каналах регулирования частоты и напряжения, которые показали высокую степень устойчивости МСАУ с синтезированными параметрами к внешним возмущающим воздействиям. При этом показатели качества регулирования по напряжению и частоте соответствуют ГОСТ 28173 (МЭК 60034-1).

Результаты, представленные в данной статье, получены при выполнении проекта «Исследование установившихся и переходных режимов автономной электроэнергетической установки со сверхпроводниковым оборудованием и системой криогенного обеспечения», выполняемого по заданию Рособразования по аналитической ведомственной целевой программе «Развитие научного потенциала высшей школы (2006–2008 годы)» (код ГРНТИ РНП.2.1.2.9319).

Литература

1. **Шишлаков В. Ф., Шишлаков Д. В., Цветков С. А.** Синтез и моделирование автономной электроэнергетической установки // Информационно-управляющие системы. 2008. № 4. С. 14–17.
2. **Никитин А. В., Шишлаков В. Ф.** Параметрический синтез нелинейных систем автоматического управления: Монография / Под ред. В. Ф. Шишлакова; ГУАП. СПб., 2003. 358 с.
3. **Шишлаков В. Ф., Цветков С. А., Шишлаков Д. В.** Синтез параметров непрерывных и импульсных многосвязных систем автоматического управления: Монография / Под ред. **В. Ф. Шишлакова**. СПб.: ГУАП, 2009. 180 с.
4. **Шишлаков В. Ф., Шишлаков Д. В.** Параметрический синтез многосвязных систем автоматического управления обобщенным методом Галеркина // Информационно-управляющие системы. 2006. № 3. С. 51–62.
5. **Шишлаков В. Ф., Шишлаков Д. В.** Параметрический синтез многосвязных систем автоматического управления во временной области // Известия вузов. Сер. Проблемы энергетики. 2006. № 12. С. 49–54.

УДК 519.95

МЕТОД ДИНАМИЧЕСКОЙ ДЕКОМПОЗИЦИИ В МОДЕЛИРОВАНИИ СИСТЕМ УПРАВЛЕНИЯ СО СТРУКТУРНЫМИ ИЗМЕНЕНИЯМИ

А. Н. Кириллов,
канд. физ.-мат. наук, доцент
Санкт-Петербургский государственный технологический университет растительных полимеров

Предлагается метод построения математических моделей сложных систем с изменяющейся в процессе функционирования структурой. Вводится динамическая система, состоящая из переменного количества подсистем. На ее основе моделируется процесс инвестирования динамической экономической системы, описывающей крупный промышленный комплекс.

Ключевые слова *— динамическая система управления, декомпозиция, структура, переменная размерность, экономическая система, моделирование динамики.*

Введение

Математическое моделирование сложных динамических систем, например крупных производственных комплексов, биоценозов, многостадийных технологических процессов, связано с труднопреодолимым противоречием. С одной стороны, для использования модели в целях прогнозирования поведения реальной системы следует получать более полное ее описание, что приводит к невозможности аналитического или качественного исследования. С другой стороны, упрощение модели лишает ее практической ценности. Необходим компромисс между точностью описания и сложностью исследования. Наиболее удачные математические модели сочетают в себе эти качества. В данной работе предлагается подход, в некоторой степени разрешающий указанное выше противоречие. Вводится процедура разбиения жизненного цикла системы на временные промежутки так, чтобы исходная сложная система на каждом промежутке представлялась относительно простой моделью. Этот подход был реализован в работе [1], где рассмотрена двухвидовая система «хищник–жертва» с миграцией популяции хищника, которая зависит от его трофической связи с популяцией жертв. При этом процесс функционирования сообщества представляется последовательностью сменяющих друг друга стадий. Сменяемость стадий характерна также для процесса управления системой химических реакторов [2], моделей динамики метапопуляций, экономических систем с переменной структурой. При моделировании этих процессов используются динамические системы, размерность которых, в зависимости от состояния, может изменяться с течением времени, т. е. происходит динамическая декомпозиция сложной системы [3]. Возможность использования систем с переменной размерностью при моделировании динамики биологических сообществ указывалась еще в работе Ю. М. Свирежева [4]. При построении теории реализации Р. Калман предложил [5] обобщить понятие динамической системы таким образом, чтобы размерность ее пространства состояний могла меняться во времени. Систему оптимального управления со сменой фазового пространства рассматривал В. Г. Болтянский [6]. Вопросы моделирования многосвязных систем с изменяющейся структурой исследовались в работах [7–9]. В настоящей работе продолжается исследование систем с переменной размерностью, начатое автором [1, 3]. Вводится понятие линейной системы с переменной размерностью, которая применяется для построения модели инвестирования производственного объединения.

Структура системы

Предположим, что система S состоит из подсистем S_i $i = 1, \ldots, n$. Взаимосвязи между подсистемами характеризуют внутреннюю структуру

системы. Исследование влияния их интенсивности на устойчивость положений равновесия проводилось [7, 8]. Здесь же рассмотрим внешнюю структуру системы, которую введем следующим образом. В процессе функционирования влияние некоторых из подсистем S_i на динамику S может или ослабевать, или усиливаться. Возможно также полное отключение каких-либо подсистем на некоторое время. Если влиянием подсистемы S_i на динамику S можно пренебречь, то будем говорить, что S_i находится в пассивном режиме, иначе — в активном. В связи с этим введем вектор $\boldsymbol{\gamma}\in R^n$ с компонентами γ_i, $i = 1, ..., n$, при этом $\gamma_i = 1$, если подсистема S_i находится в активном режиме, и $\gamma_i = 0$, если S_i — в пассивном режиме. Вектор $\boldsymbol{\gamma}$ назовем вектором внешней структуры системы S, или, короче, структурой S. Из определения следует, что $\boldsymbol{\gamma}$ принимает значения на множестве вершин единичного n-мерного куба. Под внутренней структурой системы S будем понимать структуру взаимосвязей между подсистемами, но здесь этот вопрос не освещается. Для описания процесса изменения структуры системы введем вектор $\mathbf{y}\in R^n$ с компонентами y_i, $i = 1, ..., n$, динамика которого задается некоторой системой дифференциальных уравнений. Пусть Δ — множество значений $\mathbf{y}$, $\Delta\subset R^n$. Разобьем Δ на непересекающиеся подмножества Δ_i^0, Δ_i^1, $\Delta = \Delta_i^0\cup\Delta_i^1$, $\Delta_i^0\cap\Delta_i^1 = \varnothing$. Будем полагать, что $\gamma_i = 0$, если $y_i\in\Delta_i^0$; $\gamma_i = 1$, если $y_i\in\Delta_i^1$. Таким образом, при изменении $\mathbf{y}$ структура системы эволюционирует. В связи с этим вектор $\mathbf{y}$ можно считать многомерным временем эволюции системы, в отличие от текущего времени t, изменение которого влияет на состояние системы.

Линейная система с переменной размерностью

Введем в рассмотрение следующую многостадийную линейную систему. Пусть $\mathbf{x}$ — вектор состояний системы S, x_i — его компоненты. Размерность $\mathbf{x}$ может изменяться во времени при изменении структуры системы. Пусть подсистемы с номерами s_k, $k = 1, ..., m$, активны, а с номерами s_j, $j = m + 1, ..., n$, — пассивны. Введем уравнения, задающие динамику компонентов x_{s_k}, входящих в состав $\mathbf{x}$, в зависимости от условий, которым удовлетворяют компоненты y_{s_i} вектора времени эволюции $\mathbf{y}$. Пусть при

$$y_{s_k} > d_{s_k},\ \ k = 1, \ldots, m,\ \ m\in\{1, \ldots, n\}; \qquad (1)$$

$$y_{s_j} < d_{s_j},\ \ j = m+1, \ldots, n \qquad (2)$$

система S задается уравнениями

$$\dot{x}_{s_k} = a_{s_k, s_k} x_{s_k} + \ldots + a_{s_k, s_m} x_{s_m}; \qquad (3)$$

$$\dot{y}_{s_k} = b_{s_k, s_k} x_{s_k} + \ldots + b_{s_k, s_m} x_{s_m}; \qquad (4)$$

$$\dot{y}_{s_j} = \tilde{b}_{s_j, s_1} x_{s_1} + \ldots + \tilde{b}_{s_j, s_m} x_{s_m}, \qquad (5)$$

где d_{s_k}, a_{s_k, s_k}, b_{s_k, s_k}, $\tilde{b}_{s_j, s_k}$ — заданные постоянные. При этом будем говорить, что многостадийная система S находится в стадии $S(s_1, ..., s_m)$. Здесь индексы в скобках — номера переменных x_{s_k}, входящих в данную стадию. Уравнения (3) задают динамику вектора состояний системы в стадии $S(s_1, ..., s_m)$, уравнения (4), (5) — динамику времени эволюции активных и пассивных подсистем соответственно.

Уменьшение размерности системы. Пусть при попадании траектории системы (3)–(5) в некоторый момент времени t^- из области (1), (2) на плоскость $y_{s_l} = d_{s_l}$ при некотором $l\in\{1, ..., m\}$ происходит переход от стадии $S(s_1, ..., s_m)$ к стадии $S(s_1, \ldots, \hat{s}_l, \ldots, s_m)$, где символом $\hat{s}_l$ обозначен отсутствующий компонент в наборе индексов. Таким образом, стадия $S(s_1, \ldots, \hat{s}_l, \ldots, s_m)$ будет описываться системой (3)–(5), в которую не входит уравнение, задающее динамику переменной x_{s_l}, а уравнение, задающее динамику y_{s_l}, принимает вид

$$\dot{y}_{s_l} = \tilde{b}_{s_1, s_1} x_{s_1} + \ldots + \tilde{b}_{s_1, s_m} x_{s_m},$$

причем в его правой части, а также в правых частях других уравнений (3)–(5) отсутствуют слагаемые, содержащие переменную x_{s_l}. Для формального описания процесса уменьшения размерности введем следующие обозначения.

Матрицы:

$$\mathbf{A} = \{a_{ij}\},\ i, j = 1, \ldots, n;$$

$\mathbf{A}(s_1, ..., s_m|p_1, ..., p_r)$ — матрица, состоящая из элементов матрицы $\mathbf{A}$, стоящих на пересечении ее строк и столбцов с номерами $s_1, ..., s_m$ и $p_1, ..., p_r$ соответственно;

$\mathbf{A}(s_1, ..., s_m|s_1, ..., s_m) \equiv \mathbf{A}(s_1, ..., s_m)$ — квадратная матрица порядка m, составленная из элементов матрицы $\mathbf{A}$, стоящих на пересечении строк и столбцов с номерами $s_1, ..., s_m$;

$\mathbf{A}(s_1, \ldots, \hat{s}_l, \ldots, s_m)$ — квадратная матрица порядка $m - 1$, полученная из $\mathbf{A}(s_1, ..., s_m)$ удалением из нее строки и столбца с номером s_l;

$\mathbf{A}(s_1, ..., 0_{s_l}, ..., s_m)$ — квадратная матрица порядка m, полученная из $\mathbf{A}(s_1, ..., s_m)$ заменой ее строки и столбца с номером s_l нулевой строкой и столбцом;

$\mathbf{A}(s_1, ..., s_m|\cdot)$ — матрица, составленная из элементов матрицы $\mathbf{A}$, стоящих на пересечении ее строк с номерами $s_1, ..., s_m$ и столбцов со всеми номерами, не равными $s_1, ..., s_m$, т. е. с номерами множества $\{1, ..., n\}\backslash\{s_1, ..., s_m\}$; $\mathbf{A}(s_1, ..., s_m|\cdot)$ имеет размерность $m\times(n - m)$;

$\mathbf{B} = \{b_{ij}\}$, $\tilde{\mathbf{B}} = \{\tilde{b}_{ij}\}$, $\mathbf{C} = \{c_{ij}\}$ — заданные матрицы с постоянными элементами, $i, j = 1, ..., n$.

Векторы:

$\mathbf{x}(s_1, ..., s_m) = (x_{s_1}, ..., x_{s_m})^* \in R^m$; $\mathbf{x}(s_1, ..., s_m)(t) = (x_{s_1}(t), ..., x_{s_m}(t))^*$; * — символ операции транспонирования;

$\mathbf{x}(s_1, ..., \hat{s}_l, ..., s_m)$ — вектор, полученный из $\mathbf{x}(s_1, ..., s_m)$ удалением из него компонента с номером s_l, $\mathbf{x}(s_1, ..., \hat{s}_l, ..., s_m) \in R^{m-1}$;

$\mathbf{x}(s_1, ..., 0_{s_l}, ..., s_m)$ — вектор, полученный из $\mathbf{x}(s_1, ..., s_m)$ заменой его компонента с номером s_l нулем.

Тогда стадия $S(s_1, ..., s_m)$ задается уравнениями

$$\dot{\mathbf{x}}(s_1, ..., s_m) = \mathbf{A}(s_1, ..., s_m) \cdot \mathbf{x}(s_1, ..., s_m); \quad (6)$$

$$\dot{\mathbf{y}}(s_1, ..., s_m) = \mathbf{B}(s_1, ..., s_m) \cdot \mathbf{x}(s_1, ..., s_m); \quad (7)$$

$$\dot{\mathbf{y}}(s_{m+1}, ..., s_n) = \tilde{\mathbf{B}}(s_{m+1}, ..., s_n \,|\cdot) \cdot \mathbf{x}(s_1, ..., s_m). \quad (8)$$

Стадия $S(s_1, ..., \hat{s}_l, ..., s_m)$ задается уравнениями

$$\dot{\mathbf{x}}(s_1, ..., \hat{s}_l, ..., s_m) = \mathbf{A}(s_1, ..., \hat{s}_l, ..., s_m) \cdot \mathbf{x}(s_1, ..., \hat{s}_l, ..., s_m); \quad (9)$$

$$\dot{\mathbf{y}}(s_1, ..., \hat{s}_l, ..., s_m) = \mathbf{B}(s_1, ..., \hat{s}_l, ..., s_m) \cdot \mathbf{x}(s_1, ..., \hat{s}_l, ..., s_m); \quad (10)$$

$$\dot{\mathbf{y}}(s_l, s_{m+1}, ..., s_n) = \tilde{\mathbf{B}}(s_l, s_{m+1}, ..., s_n \,|\cdot) \cdot \mathbf{x}(s_1, ..., \hat{s}_l, ..., s_m). \quad (11)$$

Введем функции перехода $\varphi^-(s_1, ..., \hat{s}_l, ..., s_m)$ от $S(s_1, ..., s_m)$ к стадии $S(s_1, ..., \hat{s}_l, ..., s_m)$. Пусть $\mathbf{z}((s_1, ..., s_m)(s_l)) = (x_{s_1}, ..., x_{s_m}, y_{s_l})^*$. Тогда

$$\varphi^-(s_1, ..., \hat{s}_l, ..., s_m): \mathbf{z}((s_1, ..., s_m)(s_l)) \to \to (\tilde{\mathbf{x}}(s_1, ..., \hat{s}_l, ..., s_m), d_{s_l} - \varepsilon_{s_l})^*; \quad (12)$$

$$\tilde{\mathbf{x}}(s_1, ..., s_m) = \mathbf{C}(s_1, ..., 0_l, ..., s_m \,|\, s_1, ..., s_m) \times \times \mathbf{x}(s_1, ..., s_m), \quad (13)$$

где ε_{s_l} — заданные положительные постоянные. При этом

$$\mathbf{x}(s_1, ..., \hat{s}_l, ..., s_m)(t^- + 0) = = \tilde{\mathbf{x}}(s_1, ..., s_m)(t^-). \quad (14)$$

Увеличение размерности системы. Вернемся снова к области (1), (2) и к соответствующей ей системе (3)–(5). Пусть при попадании траектории этой системы в момент времени t^+ из области (1), (2) на плоскость $y_{s_p} = d_{s_p}$ при некотором $p \in \{m + 1, ..., n\}$ происходит переход от стадии $S(s_1, ..., s_m)$ к стадии $S(s_1, ..., s_m, s_p)$, которая будет описываться системой уравнений

$$\dot{x}_{s_k} = a_{s_k, s_1} x_{s_1} + ... + a_{s_k, s_m} x_{s_m} + a_{s_k, s_p} x_{s_p}; \quad (15)$$

$$\dot{y}_{s_k} = b_{s_k, s_1} x_{s_1} + ... + b_{s_k, s_m} x_{s_m} + b_{s_k, s_p} x_{s_p}; \quad (16)$$

$$\dot{y}_{s_j} = \tilde{b}_{s_j, s_1} x_{s_1} + ... + \tilde{b}_{s_j, s_m} x_{s_m} + \tilde{b}_{s_j, s_p} x_{s_p}, \quad (17)$$

где $k = 1, ..., m, p$; $j = m + 1, ..., n$, $j \neq p$, или

$$\dot{\mathbf{x}}(s_1, ..., s_m, s_p) = = \mathbf{A}(s_1, ..., s_m, s_p) \cdot \mathbf{x}(s_1, ..., s_m, s_p); \quad (18)$$

$$\dot{\mathbf{y}}(s_1, ..., s_m, s_p) = = \mathbf{B}(s_1, ..., s_m, s_p) \cdot \mathbf{x}(s_1, ..., s_m, s_p); \quad (19)$$

$$\dot{\mathbf{y}}(s_{m+1}, ..., \hat{s}_p, ..., s_n) = = \tilde{\mathbf{B}}(s_{m+1}, ..., \hat{s}_p, ..., s_n \,|\cdot) \cdot \mathbf{x}(s_1, ..., s_m, s_p). \quad (20)$$

Введем функции перехода $\varphi^+(s_1, ..., s_m, s_p)$ от $S(s_1, ..., s_m)$ к стадии $S(s_1, ..., s_m, s_p)$. Пусть $\mathbf{z}((s_1, ..., s_m)(s_l)) = (x_{s_1}, ..., x_{s_m}, y_{s_l})^*$. Тогда $\varphi^+(s_1, ..., s_m, s_p)$:

$$\mathbf{z}((s_1, ..., s_m)(s_l)) \to \to (\bar{x}_{s_1}, ..., \bar{x}_{s_m}, \bar{x}_{s_p}, d_{s_p} + \varepsilon_{s_p})^* \equiv \equiv (\bar{\mathbf{x}}(s_1, ..., s_m, s_p), d_{s_p} + \varepsilon_{s_p})^*, \quad (21)$$

где

$$\bar{\mathbf{x}}(s_1, ..., s_m, s_p) = = \mathbf{D}(s_1, ..., s_m, s_p \,|\, s_1, ..., s_m) \cdot \mathbf{x}(s_1, ..., s_m). \quad (22)$$

При этом

$$\mathbf{x}(s_1, ..., s_m, s_p)(t^+ + 0) = \bar{\mathbf{x}}(s_1, ..., s_m, s_p)(t^+). \quad (23)$$

Определение. Система (1)–(23) называется линейной системой с переменной размерностью (ЛСПР).

Частный случай ЛСПР был рассмотрен в работе [2], где стадия, соответствующая m подсистемам, имеет вид $S(1, ..., m)$. Такая система называется последовательной.

Замечание. Рассмотренную ЛСПР можно задать также следующим образом. Пусть

$$\mathbf{a} = (a_1, ..., a_n)^* \in R^n, \ \mathbf{b} = (b_1, ..., b_n)^*,$$
$$\mathbf{a(b)} = (a_1 b_1, ..., a_n b_n)^*, \ \dot{\mathbf{a}}(\mathbf{b}) = (\dot{a}_1 b_1, ..., \dot{a}_n b_n)^*.$$

Далее, если $\mathbf{A} = (\mathbf{A}_1^*, ..., \mathbf{A}_n^*)^*$ — матрица, где $\mathbf{A}_i^*$ — строка с номером i, то пусть

$$\mathbf{A(b)} = (b_1 \mathbf{A}_1^*, ..., b_n \mathbf{A}_n^*)^*.$$

Если γ_i — компоненты вектора структуры, то обозначим $\bar{\gamma}_i = 1 - \gamma_i$, $\bar{\boldsymbol{\gamma}} = (\bar{\gamma}_1, ..., \bar{\gamma}_n)^*$. Тогда динамика ЛСПР задается уравнениями

$$\dot{\mathbf{x}}(\boldsymbol{\gamma}) = \mathbf{A}(\boldsymbol{\gamma})\mathbf{x}(\boldsymbol{\gamma}); \quad \dot{\mathbf{y}}(\boldsymbol{\gamma}) = \mathbf{B}(\boldsymbol{\gamma})\mathbf{x}(\boldsymbol{\gamma}); \ \dot{\mathbf{y}}(\bar{\boldsymbol{\gamma}}) = \tilde{\mathbf{B}}(\bar{\boldsymbol{\gamma}})\mathbf{x}(\boldsymbol{\gamma}). \quad (24)$$

Определение. Векторы $\mathbf{y}(\boldsymbol{\gamma}) \in R^n$, $\mathbf{y}(\bar{\boldsymbol{\gamma}}) \in R^n$ назовем векторами активного и пассивного времени эволюции соответственно.

Введем управляемую ЛСПР

$$\dot{\mathbf{x}}(\gamma)=\mathbf{A}(\gamma)\mathbf{x}(\gamma)+\mathbf{C}(\gamma)\mathbf{u};\quad \dot{\mathbf{y}}(\gamma)=\mathbf{B}(\gamma)\mathbf{x}(\gamma)+\hat{\mathbf{C}}(\gamma)\mathbf{v};$$
$$\dot{\mathbf{y}}(\overline{\gamma})=\tilde{\mathbf{B}}(\overline{\gamma})\mathbf{x}(\gamma)+\tilde{\mathbf{C}}(\gamma)\mathbf{w},$$

где $\mathbf{u}\in R^r$, $\mathbf{v}\in R^s$, $\mathbf{w}\in R^p$ — управляющие воздействия; $\mathbf{C}, \hat{\mathbf{C}}, \tilde{\mathbf{C}}$ — матрицы соответствующих размерностей. В статье [2] решается задача управления структурой последовательной ЛСПР.

Модель производственного комплекса

Рассмотрим экономическую систему, состоящую из изменяющегося количества подсистем. Это изменение происходит согласно правилам, устанавливаемым некоторым центром управления (ЦУ). Примером такой системы могут быть государственная экономика, состоящая из отраслей производства, или крупная производственная корпорация, фирма, объединение, в состав которых входят предприятия, выпускающие некоторую продукцию. Для конкретизации предлагаемого подхода к построению соответствующей модели рассмотрим производственное объединение (ПО). ЦУ должен распределить инвестиции по предприятиям для их развития. Цель развития состоит в достижении предприятиями некоторых заданных уровней в течение заданного промежутка времени $[t_0, t_0 + T]$. При этом ЦУ может закрыть какое-либо предприятие или возобновить его работу в зависимости от эффективности его деятельности, а также может открыть новое предприятие при некоторых условиях.

Пусть количественная характеристика состояния i-го предприятия в момент времени t определяется функцией $x_i(t) \geq 0$, $x_i(t)\in R$. Скорость прироста инвестиций в предприятие i в момент t обозначим через $u_i(t, x_i(t))$, $u_i\in R$, $u_i(t, x_i(t)) \geq 0$. Далее, пусть $a_i(t)$ — скорость прироста уровня развития предприятия i на единицу капитала, вложенного в него, причем $a_i(t) \geq 0$, $a_i(t)$ — ограниченные, кусочно-непрерывные функции, $a_i(t)\in R$. Тогда дифференциальное уравнение, задающее динамику развития i-го предприятия, имеет вид

$$\dot{x}_i = a_i(t)u_i(t, x_i).$$

Заметим, что количество предприятий, функционирующих в составе ПО, не задано. В работе [10] рассматривалась модель с постоянным количеством предприятий. Будем считать, что инвестиции, направляемые ЦУ на развитие i-го предприятия, состоят из собственных средств и кредитов банка, которые получает ПО, а ЦУ распределяет по предприятиям. Таким образом:

$$u_i(t, x_i)=\mu_i(t)x_i(t)+w_i(t, x_i),$$

где $\mu_i = \mu_i(t)$ — коэффициент, характеризующий скорость прироста собственных средств предприятия на единицу объема его продукции; $w_i = w_i(t, x_i)$ — скорость прироста инвестиций за счет кредита банка. При этом $\mu_i(t) \geq 0$, $w_i(t, x_i) \geq 0$, $\mu_i(t)$, $w_i(t, x_i)$ — кусочно-непрерывны. Отсюда получаем уравнение динамики предприятия i

$$\dot{x}_i = \mu_i(t)x_i + w_i(t, x_i). \qquad (25)$$

Пусть t_0 — момент начала функционирования предприятия i. Введем переменную y_i:

$$y_i(t) = y_i^0 + \int_{t_0}^{t} (c_i(t, x_i(t)) - w_i(t, x_i(t))\mathrm{d}t, \qquad (26)$$

где $c_i(t, x_i(t))$, y_i^0 — заданные пороговые функции и постоянные соответственно. Продифференцировав равенство (26), получим

$$\dot{y}_i(t) = c_i(t, x_i) - w_i(t, x_i). \qquad (27)$$

Таким образом, предприятие i является подсистемой S_i в модели ЛСПР. Пусть наибольшее число предприятий, которые могут входить в состав ПО, равно n, $i\in\{1, ..., n\}$. Будем называть предприятие i, динамика которого задается системой уравнений (25), (27), активным. Вектор $\mathbf{y}$ с компонентами y_i представляет собой эволюционное время ПО. Выясним экономический смысл величины $\mathbf{y}$. Введем постоянные пороги d_i, $d_i < y_i^0$. Пусть найдется наименьший момент времени $t_i > t_0$ такой, что $y_i(t_i) = d_i$. Тогда в момент времени t_i происходит закрытие i-го предприятия. Экономический смысл этого процесса состоит в том, что эффективно работающее предприятие должно в большей степени развиваться не за счет кредитов, а за счет собственных средств. Поэтому превышение функцией $w_i(t, x_i)$ порогового значения $c_i(t, x_i)$ означает, что i-е предприятие использует слишком много кредитов, которые придется погашать с помощью собственных средств. Это является признаком неэффективной деятельности, что приводит к принятию органом управления решения о приостановке предприятия. Возникает вопрос: когда закрывать предприятие? Если его закрыть в момент выполнения условия $w_i(t, x_i) = c_i(t, x_i)$, то процесс закрытия станет слишком чувствительным и будет реагировать на мгновенные сбои в работе предприятия, приводящие к малозначительным снижениям его эффективности. Для органа управления желательно некоторое время наблюдать за деятельностью предприятия, прежде чем принимать решение. Поэтому наличие интеграла в условии закрытия $y_i(t_i) = d_i$ придает некоторую инерционность в принятии решения о закрытии предприятия, что дает последнему возможность отработать временные сбои. Напротив, если низкая эффективность его работы, что проявляется в выполнении условия $w_i(t, x_i) > c_i(t, x_i)$, наблюдается в течение достаточно длительного промежутка времени, то орган

управления закрывает i-е предприятие в момент t_i, введенный выше. После закрытия i-е предприятие переходит в пассивный режим, которому соответствует система уравнений:

$$\begin{cases} \dot{x}_i = -p_i w_i(t,\ x_i), \text{если } x_i > 0; \\ \dot{x}_i = 0, \text{если } x_i = 0; \\ \dot{y}_i = c_i(t, x_i^-), \end{cases} \qquad (28)$$

где постоянные p_i, x_i^- удовлетворяют условиям: $p_i > 0$, $x_i^- = x_i(t_i + 0) < x_i(t_i)$. Первое уравнение (28) задает динамику возврата кредитов, третье — динамику накопления ресурсов. Будем называть предприятие i, динамика которого задается уравнениями (28), законсервированным или пассивным.

Теперь рассмотрим процедуру возобновления работы предприятия i. Пусть на интервале $(t_i, \bar{t}_i)$ $y_i(t_i) < d_i$ и $y_i(\bar{t}_i) = d_i$. Тогда в момент времени $\bar{t}_i$ ЦУ переводит предприятие i из пассивного в активный режим, и его динамика задается уравнениями (25), (26). При этом $x_i(\bar{t}_i) = x_i(\bar{t}_i + 0) = \bar{x}_i$, $y_i(\bar{t}_i + 0) = d_i + \delta_i$, где $\bar{x}_i$, δ_i — заданные положительные постоянные. Наличие постоянной δ_i приводит к скачкообразному изменению $y_i(t)$ при достижении ею порогового значения d_i. Предприятие получает начальный кредит на развитие, иначе может оказаться, что сразу после открытия его придется закрывать. Таким образом, если на некотором промежутке $[t_0, t_0 + T]$ в состав ПО входят активные $i_1, \ldots, i_m$ и пассивные $j_1, \ldots, j_k$ предприятия, то его динамика задается системой уравнений

$$\dot{x}_{i_s} = \mu_{i_s}(t) x_{i_s} + w_{i_s}(t, x_{i_s});$$
$$\dot{y}_{i_s}(t) = c_{i_s}(t,\ x_{i_s}) - w_{i_s}(t, x_{i_s}),$$
$$s = 1, \ldots, m;$$

$$\begin{cases} \dot{x}_{j_r} = -p_{j_r} w_{j_r}(t,\ x_{j_r}), \text{если } x_{j_r} > 0; \\ \dot{x}_{j_r} = 0, \text{если } x_{j_r} = 0; \\ \dot{y}_{j_r} = c_{j_r}(t, x_{j_r}^-), r = 1, \ldots, k. \end{cases}$$

Можно рассмотреть процедуру открытия нового предприятия, а не ранее замороженного. Будем, например, считать, что ПО расширяется, открывая новое предприятие, в момент достижения всеми предприятиями, входящими в него, некоторых заданных уровней развития e_i. Пусть на промежутке $[t_0,\ \tilde{t}\,)$ ПО состояло из n предприятий (активных и пассивных), где $\tilde{t}$ — наименьший момент времени, для которого выполняются условия $y_i(\tilde{t}\,) \geq e_i$, $i = 1, \ldots, n$, причем при $t < \tilde{t}$ хотя бы одно из этих неравенств не выполняется. Тогда в момент времени $\tilde{t}$ орган управления ПО открывает новое $(n + 1)$-е предприятие, динамика которого задается уравнениями типа (25), (26), и при этом $x_{n+1}(\tilde{t}\,) = \tilde{x}_{n+1}$, $y_{n+1}(\tilde{t}\,) = \tilde{y}_{n+1}$, $\tilde{x}_{n+1}$, $\tilde{y}_{n+1}$ — заданные постоянные, удовлетворяющие условиям $d_{n+1} < \tilde{y}_{n+1} < e_{n+1}$. При этом $y_i(\tilde{t}\, + 0) = e_i + \tilde{\delta}_i$, $i = 1, \ldots, n$, где $\tilde{\delta}_i$ — заданные положительные постоянные.

Таким образом, на основе понятия ЛСПР построена модель динамики ПО с изменяющимся в процессе функционирования количеством предприятий.

Литература

1. **Кириллов А. Н.** Экологические системы с переменной размерностью // Обозрение прикладной и промышленной математики. 1999. Т. 6. Вып. 2. С. 318–336.
2. **Кириллов А. Н.** Управление многостадийными технологическими процессами // Вестник СПбГУ. Сер. 10. 2006. Вып. 4. С. 127–131.
3. **Кириллов А. Н.** Динамическая декомпозиция и устойчивость структур // Математический анализ и его приложения / Четинск. пед. ин-т им. Н. Г. Чернышевского. Чита, 1996. Вып. 2. С. 20–24.
4. **Свирежев Ю. М.** Нелинейные волны, диссипативные структуры и катастрофы в экологии. М.: Наука, 1987. 368 с.
5. **Калман Р., Фалб П., Арбиб М.** Очерки по математической теории систем. М.: Мир, 1971. 400 с.
6. **Болтянский В. Г.** Задачи оптимизации со сменой фазового пространства // Дифференциальные уравнения. 1983. Т. 19. № 3. С. 518–521.
7. **Шильяк Д.** Децентрализованное управление сложными системами. М.: Мир, 1994. 576 с.
8. **Груйич Л. Т., Мартынюк А. А., Риббенс-Павелла М.** Устойчивость крупномасштабных систем при структурных и сингулярных возмущениях. Киев: Наук. думка, 1984. 473 с.
9. **Охтилев М. Ю., Соколов Б. В., Юсупов Р. М.** Интеллектуальные технологии мониторинга и управления структурной динамикой сложных динамических объектов. М.: Наука, 2006. 410 с.
10. **Кириллов А. Н.** Одна математическая модель распределения капитальных вложений // Экономика и математические методы. 1982. № 5. С. 922–925.

УДК 004.434

ИСПОЛЬЗОВАНИЕ ЯЗЫКА ОПИСАНИЯ ДИАГРАММ

К. Б. Степанян*,*
начальник управления операционного обслуживания
ОАО «Управляющая компания «Арсагера»

Обсуждается практическое применение языка DiaDeL для описания графо-подобных диаграмм на примере диаграмм состояний. Приводится пример известной диаграммы состояний телефона, автоматически построенной по описанию на предложенном языке. Язык DiaDeL позволяет формально определить графический синтаксис (нотацию) диаграмм заданного типа и связать нотацию с семантикой, заданной в форме набора классов.

Ключевые слова *— графический язык, абстрактный синтаксис, метамодель, визуализация диаграмм, диаграмма состояний.*

Введение

Актуальность и эффективность практического применения двумерных графо-подобных диаграмм в настоящее время не ставятся под сомнение. Более того, большинство типов диаграмм имеет не только строго формализованную нотацию, но и семантику, что позволяет тем или иным образом интерпретировать их. Подобные диаграммы называются визуальными языками. Наиболее яркое применение они нашли в областях моделирования, проектирования и реализации программного обеспечения.

Ранее нами был предложен язык описания диаграмм DiaDeL (Diagram Definition Language) [1–3], основанный на предположении, что семантика каждой отдельной диаграммы задана в виде набора конкретных программных объектов определенных классов. Набор всех возможных классов объектов, которые могут появляться на диаграммах данного типа, называется семантической моделью, а набор объектов, соответствующих конкретной диаграмме, называется экземпляром ее семантической модели.

Настоящая статья демонстрирует применение языка DiaDeL на примере построения диаграмм состояний с помощью системы, описанной в работах [1, 2]. Существует множество различных диалектов диаграмм состояний. Из всех возможных выбраны диаграммы состояний языка UML [4], как наиболее показательные по ряду критериев:

- диаграммы состояний — очень важный и практически широко используемый тип диаграмм [5, 6];
- нотация позволяет продемонстрировать большинство возможностей языка DiaDeL;
- существует полная и непротиворечивая спецификация семантики [7];
- существует реализованная семантическая модель [8].

Следует оговориться сразу, что в статье не приводится синтаксис языка DiaDeL, он рассмотрен в других статьях [1, 2]. Основное назначение работы — продемонстрировать «выразительные» способности и возможности языка.

Анализ семантической модели диаграммы состояний

Первым шагом построения отображения диаграммы является анализ ее семантической модели. Цель анализа — определить, удовлетворяет ли модель требованиям, предъявляемым языком DiaDeL. Весь процесс можно разбить на следующие шаги.

1. Определение элементов, которые будут представлены на диаграмме, как фигуры или декорации. Для простоты будем называть их *элементы-вершины*.

2. Определение элементов, которые будут представлены на диаграмме, как линии (*элементы-связи*).

3. Определение «корневого» элемента, соответствующего самой диаграмме (*элемент-диаграмма*).

---

* Научный руководитель — канд. физ.-мат. наук, заведующий лабораторией астрономического программирования Института прикладной астрономии РАН *Ф. А. Новиков.*

4. Проверка, что эти элементы предоставляют необходимую информацию в соответствии с требованиями DiaDeL:

а) элемент-диаграмма и элементы-вершины, которые должны быть отображены, как контейнеры, предоставляют содержащиеся в них элементы-вершины в виде одного списка;

б) элементы-вершины, которые должны на диаграмме иметь инцидентные элементы-связи, предоставляют их в виде одного списка;

в) элементы-связи предоставляют элемент-вершину, инцидентную началу, и элемент-вершину, инцидентную концу.

5. Проверка, что всю остальную информацию, необходимую для отображения (если таковая имеется), модель предоставляет не в виде списков или массивов, поскольку DiaDeL не поддерживает циклы.

Семантическая модель диаграммы состояний отображена на рис. 1. Модель взята из официальной спецификации языка UML [7]. Для построения диаграмм состояний использовалась реализация модели EclipseUML v2.1 [8]. В ней все сущности модели представлены интерфейсами, а все свойства имеют традиционный для Java вид *getProperty()*, *setProperty()*.

Проанализируем представленную модель и пройдем по шагам описанного выше процесса.

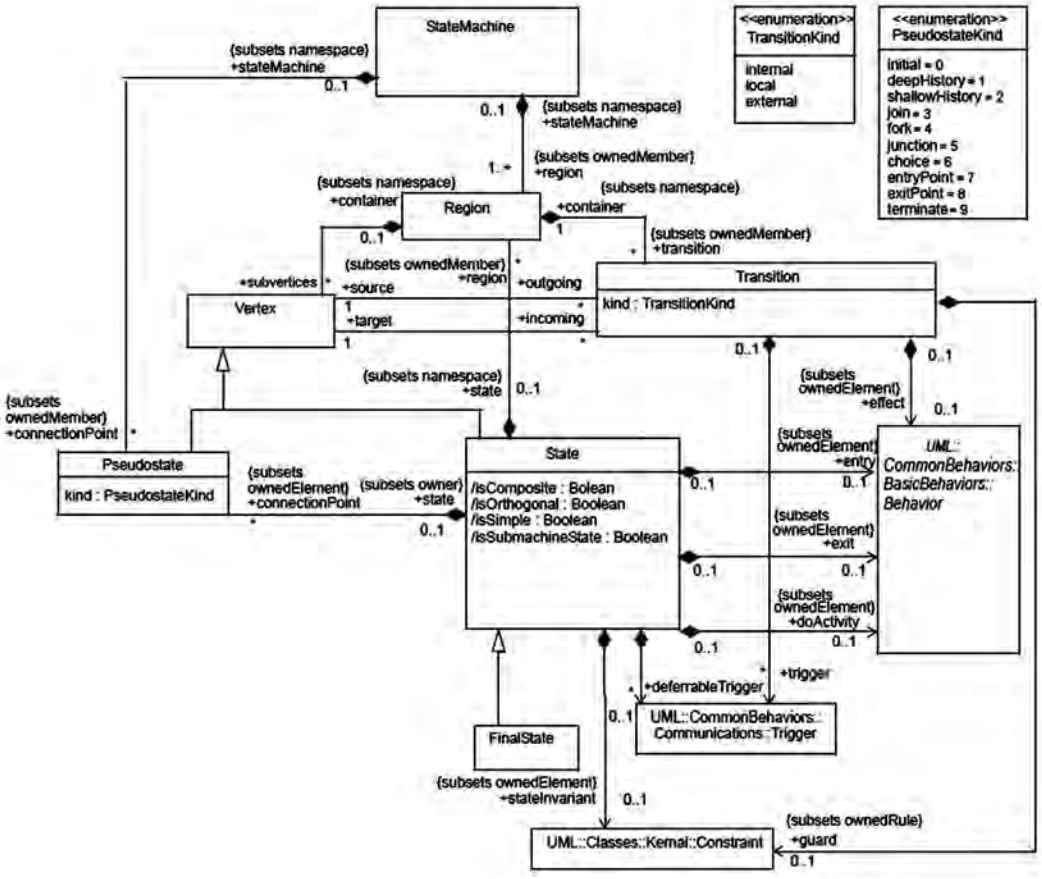
1. Элементы-вершины — это интерфейсы *State* (представляет состояние как простое, так и составное), *Pseudostate* (представляет специальные вершины) и *FinalState* (представляет конечное состояние).

2. Элемент-связь — это интерфейс *Transition* (представляет переход между состояниями).

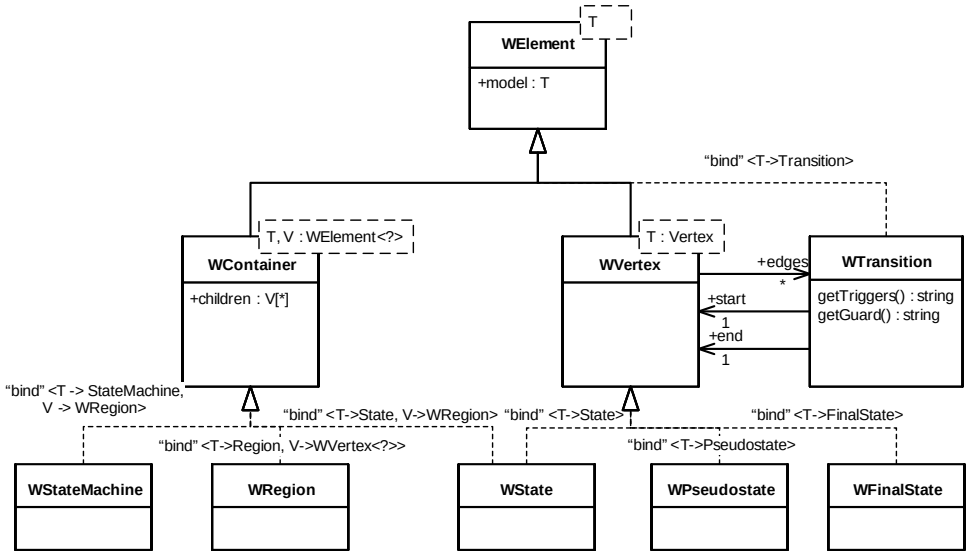
3. Элемент-диаграмма — это интерфейс *StateMachine* (представляет сам конечный автомат).

4. Проанализируем, предоставляет ли модель информацию в соответствии с требованиями DiaDeL. Заметим, что информация должна предоставляться с помощью вызова одного метода/свойства (или цепочки вызовов, которую можно записать через точки, например, *m.getParent().select("*", this)*).

а. Как видно из диаграммы, модель поддерживает регионы внутри состояний и конечного автомата. Конечный автомат (или состояние) содержит список регионов, каждый из которых содержит вложенные состояния. В силу сжатости изложения мы не будем ставить цель отобразить регионы и примем допущение, что конечный автомат и составные состояния имеют ровно один



■ ***Рис. 1.*** *Семантическая модель диаграммы состояний UML*



■ ***Рис. 2.*** *Структура классов-оболочек*

регион, содержащий вложенные состояния. Следовательно, получить коллекцию вложенных состояний можно следующим вызовом: *m.getRegions().get(0).getSubvertices()*, где *m* — это экземпляр, реализующий интерфейс *StateMachine* или *State*.

б. Интерфейс *Vertex* — базовый для всех элементов-вершин — предоставляет отдельные списки исходящих и входящих элементов-связей. Следовательно, этому требованию модель не удовлетворяет.

в. Интерфейс *Transition* позволяет определить начало и конец перехода, используя свойства *getSource()* и *getTarget()*.

5. **Мы не будем описывать анализ всех данных**, которые необходимо отобразить на диаграмме, ограничившись лишь тем, что не может быть обработано в секции **refresh()** для отображения согласно нотации. Заметим, что триггеры, которые инициируют переход, представлены списком *getTriggers()* (ассоциация между *Transition* и *Trigger*). Отобразить их необходимо в одну строку через запятую. Условие перехода *getGuard()* (ассоциация между *Transition* и *Constraint*) представляется набором объектов с корневым объектом класса *Constraint* (эта часть модели на рисунке не представлена). Для конструирования из них строки условия требуется циклический обход. В силу ограничений подобную обработку невозможно написать в секции **refresh()**.

Проведенный анализ показал, что экземпляры модели не могут быть использованы напрямую для отображения диаграммы состояний, и мы не можем изменить саму семантическую модель, поскольку она является внешним модулем для нашей системы. Решением в подобной ситуации может быть создание классов-оболочек, которые «обертывают» исходные объекты, предоставляют к ним доступ, а также предоставляют данные в удобном для обработки формате. Таким подходом является применение шаблона проектирования «Адаптер», описанного в книге [9]. Поскольку задача создания классов-оболочек является типовой и не представляет большого интереса, мы опустим описание ее построения, приведя лишь их структуру (рис. 2) и краткие комментарии.

Приведенная модель классов-оболочек построена на основании параметризованных классов. Базовый класс *WElement<T>* реализует доступ к объекту оборачиваемого класса (оборачиваемый класс представляется везде параметром *T*). Класс-оболочка для перехода *WTransition* позволяет получить триггеры и условие перехода сразу в виде строки. *WTransition* предоставляет доступ к инцидентным вершинам, как к объектам *WVertex<T : Vertex>*. Те, в свою очередь, предоставляют доступ ко всем инцидентным переходам через один список. Таким образом, решаются проблемы, обозначенные выше.

Описание графических конструкций

Описание графических конструкций начнем с описания представления конечного состояния, которое изображается значком ◉.

Конечное состояние должно иметь фиксированные размеры, поэтому в качестве основной конструкции необходимо использовать декорацию. Она же будет отображать внешнюю окружность. Для отображения внутреннего круга прикрепим к основной декорации вспомогательную.

Получится следующий программный код на языке DiaDeL:

```
decoration circle { // внутренний круг
    shape = ellipse;
    minsize = (30,30);
    brush.color = colors.black;
}
decoration finalstate { // основная конструкция
    shape = ellipse;
    minsize = (38, 38);
    brush.style = styles.no;
    attachments[50%, 50%] = (:circle)[50%, 50%];
}
```

По умолчанию все графические примитивы рисуются сплошным пером толщиной в 1 пиксель и закрашиваются белым цветом, поэтому здесь и далее значения по умолчанию в описании опускаются.

Для правильного отображения конструкции ее необходимо связать с сущностью семантической модели.

```
bridge <finalstate> {
    model := org.diadel.visualizer.wrapper.statemachine.WFinalState;
    edges := model.getEdges();
}
```

Вышеприведенный программный код связывает конструкцию *finalstate* с сущностью семантической модели *WFinalState* и декларирует, что элементы-связи, которые должны быть отображены как ребра, инцидентные конечному состоянию, доступны через метод *getEdges()*.

Специальные вершины, так же как и конечное состояние, должны отображаться на диаграмме в виде значков фиксированного размера. Следовательно, для их представления необходимо использовать декорацию. Сложность заключается в том, что в семантической модели все специальные вершины представлены одной сущностью — *Pseudostate*. В зависимости от типа (определяется свойством *kind*), которым обладает экземпляр *Pseudostate*, его необходимо отображать, используя различные графические конструкции. В рамках данной статьи мы ограничимся отображением только следующих специальных вершин:

●	начальная вершина	Ⓗ	вершина истории
◇	вершина выбора	⊗	вершина точки выхода

Поскольку отображаться они должны с помощью разных графических примитивов, то мы не можем взять за основу ни один из последних. Для решения этой проблемы используем следующий подход. Возьмем за основу декорацию без графического примитива и в центре прикрепим к ней декорации с различными графическими примитивами. В секции **refresh()** в зависимости от типа специальной вершины будем управлять видимостью прикрепленных декораций таким образом, чтобы на экране получались требуемые визуальные конструкции. Нам потребуется три вспомогательные декорации:

— декорация в виде креста:

```
decoration cross {
    shape = polyline((0%,0%), (100%,100%), (50%,50%), (100%,0%), (0%,100%));
    minsize = (21, 21);
}
```

— декорация в виде ромба:

```
decoration diamond {
    shape = polygon((0%,50%), (50%,0%), (100%,50%), (50%, 100%));
    minsize = (30,30);
}
```

— декорация в виде круга (или окружности) приведена уже выше при описании представления конечного состояния. Ее можно использовать еще раз, расширив описанием шрифта для отображения текста. Таким образом, в описание, приведенное выше, необходимо добавить следующие строки:

```
decoration circle {
    ...
    text.font.name = «Arial»;
    text.font.size = 10;
}
```

Основная декорация, к середине которой крепятся все перечисленные выше конструкции:

```
decoration pstate {
    minsize = (30,30);
    attachments[50%, 50%] = (c:circle)[50%, 50%];
    attachments[50%, 50%] = (d:diamond)[50%, 50%];
    attachments[50%, 50%] = (x:cross)[50%, 50%];
}
```

Связь декорации *pstate* с сущностью семантической модели:

```
bridge <pstate> {
    model := org.diadel.visualizer.wrapper.statemachine.WPseudostate;
    edges := model.getEdges();

    refresh() {
        // вершина выбора
        d.visible = 6 == model.getModel().getKind().getValue();
        c.visible = not d.visible;
        // начальная вершина
        if (0 == model.getModel().getKind().getValue()) {
            c.brush.color = colors.black;
        }
        // вершина истории
        if (2 == model.getModel().getKind().getValue()) {
            c.brush.style = styles.no;
            c.text.value = «H»;
        }
        // вершина точка выхода
        x.visible = 8 == model.getModel().getKind().getValue();
        if (x.visible) {
            c.brush.color = colors.white;
        }
    }
}
```

Данный программный код написан в расчете только на отображение заявленных четырех типов, но его несложно расширить и на остальные типы специальных вершин.

Самой сложной конструкцией у описываемой диаграммы является состояние. Состояние может быть простым (рис. 3, *а*) и составным (рис. 3, *б*) (содержащим вложенные состояния), но должно отображаться одной конструкцией, поскольку в семантической модели это одна сущность. Более того, нотация **UML-диаграмм состояний** допускает перечисление внутри состояния действий, связанных с состоянием.

Опишем сначала конструкцию, которая будет отображать на диаграмме состояние простым способом. А затем расширим ее так, чтобы она умела отображать состояние как в сложном, так и в простом варианте. Для представления состояния будем использовать фигуру, как конструкцию, позволяющую изменять свои размеры:

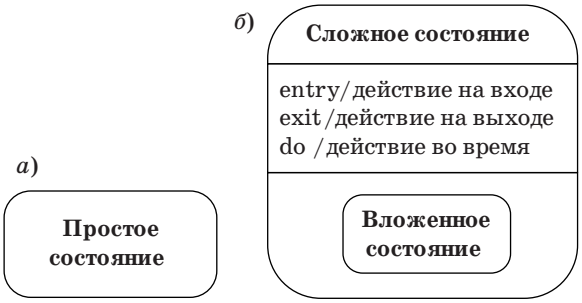
```
figure state {
    shape = roundedrectangle;
    minsize = (100, 50);
    text.font.name = «Arial»;
    text.font.size = 10;
}
```

Для правильного отображения свяжем конструкцию с сущностью *WState* из обертки семантической модели и инициализируем в секции *refresh()* текст внутри конструкции названием состояния:

```
bridge <state> {
    model := org.diadel.visualizer.wrapper.statemachine.WState;
    edges := model.getEdges();
    refresh() {
        text.value = model.getModel().getName();
    }
}
```

Этим небольшим программным кодом мы добились представления состояния в простом варианте. Проанализируем сложный вариант отображения (рис. 4).

Вся конструкция состоит из трех частей: первая отображает имя состояния, вторая — действия состояния, третья — вложенные состояния. Следовательно, основную конструкцию можно описать как фигуру, состоящую из трех других фигур (частей), расположенных вертикально. Первая часть будет отображать имя. Вторая часть, как и основная фигура, тоже состоит из трех конструкций, только они являются текстом. А третья часть является фигурой-контейнером, которая может содержать в себе любые конструкции-вершины диаграммы (потому что составное состояние может содержать в себе не только другие состояния, но и специальные вершины, и конечное состояние). Итак, нам потребуется описать пять конструкций: основную фигуру, три части и текст, из которого состоит вторая часть. Начнем с самого простого — текста и первой части:



■ ***Рис. 3.*** *Варианты представления состояния: а — простой; б — сложный*

■ ***Рис. 4.*** *Схематичное изображение сложного варианта представления состояния*

```
text label {
    font.size = 8;
    font.name = «Arial»;
    hor_align = align.left; // выравнивание по левому краю
}

figure name_section {
    shape = none;
    minsize = (70, 30);
    // используем стандартный шрифт
    text.font.size = 10;
    text.font.bold = true;
}
```

Вторая часть состоит из трех конструкций *label*, расположенных вертикально. Для того чтобы отделить ее от первой части, укажем горизонтальную линию, рисуемую в самом верху фигуры в качестве ее графического примитива:

```
figure behavior_section {
    shape = polyline((0%,0%), (100%,0%));
    minsize = (70, 13);
    layout = vertical;
    parts = {entry : label, exit : label, do : label};
}
```

Третья часть содержит в себе все допустимые конструкции-вершины диаграммы. Содержащи-

еся конструкции могут быть расположены свободно внутри фигуры:

```
figure substates_section {
    shape = polyline((0%,0%), (100%,0%));
    minsize = (70, 30);
    layout = free;
    contain = {state, pstate, finalstate};
}
```

Модифицируем описанную ранее фигуру для простого варианта отображения состояния так, чтобы она состояла из трех представленных выше частей:

```
figure state {
    shape = roundedrectangle;
    minsize = (100, 50);
    layout = vertical;
    parts = {ns : name_section, bs : behavior_section,
            ss : substates_section};
}
```

Определения для текста были убраны, поскольку мы больше не будем отображать внутри конструкции текст. Описание частей фигуры и их расположение добавлено.

Значительные изменения претерпит и семантический мост, связанный с состоянием. Однако перед описанием изменений поставим еще одну задачу. Для того чтобы построенные диаграммы были компактней, не будем отображать части состояния в том случае, если они пусты. Таким образом, если у состояния нет вложенных состояний (или других сущностей) и нет связанных с ним действий, оно должно выглядеть, как в случае простого варианта отображения:

```
bridge <state> {
    model := org.diadel.visualizer.wrapper.statemachine.WState;
    edges := model.getEdges();

    refresh() {
        // инициализируем текст внутри первой части
        ns.text.value = model.getModel().getName();
        // не отображать текст, если нет соответствующего действия
        bs.entry.visible = model.getModel().getEntry() != null;
        // если отображаем, то инициализируем типом и названием
        if (bs.entry.visible) {
            bs.entry.value = « entry / « +
                    model.getModel().getEntry().getName();
        }
        bs.exit.visible = model.getModel().getExit() != null;
        if (bs.exit.visible) {
            bs.exit.value = « exit / « +
                    model.getModel().getExit().getName();
        }
        bs.do.visible = model.getModel().getDoActivity() != null;
        if (bs.do.visible) {
            bs.do.value = « do / « +
                    model.getModel().getDoActivity().getName();
        }
        // если ни один текст не отображается, скрываем и вторую часть
        bs.visible = bs.entry.visible or bs.exit.visible or bs.do.visible;

        // отображаем третью часть, только если есть вложенные состояния
        ss.visible = model.getChildren().size() > 0;
        if (ss.visible) {
            // третья часть по вертикали занимает все оставшееся место
            ss.size.height = size.height - ns.size.height;
            if (bs.visible) {
                ss.size.height = ss.size.height - bs.size.height;
            }
        }
    }
}
```

Теперь, когда состояние отображается составной фигурой и все вложенные состояния должны отображаться в третьей части, необходимо также описать семантический мост для нее, чтобы указать, как извлекать информацию из семантической модели о вложенных сущностях:

```
bridge <substates_section> {
    model := parent.model;
    children := model.getChildren().get(0).getChildren();
}
```

Обратите внимание, что семантический мост не связывает часть с конкретной сущностью, а ссылается на сущность родительской фигуры. Подобным образом указывается, что этот семантический мост должен быть использован в том случае, если фигура является частью другой фигуры.

Пришло время описать графическое представление перехода. Переход должен отображаться следующим образом (рис. 5).

Конструкцию выше можно описать, как сплошную линию, к концу которой прикреплена открытая стрелка, а к середине — текст. Объявлять новую конструкцию для текста необходимости нет, так как можно использовать уже объявленную конструкцию *label*. Открытую стрелку опишем, как декорацию с графическим примитивом — полилинией:

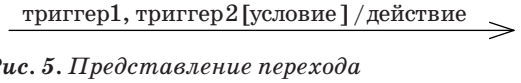
```
decoration open_arr {
    shape = polyline((0%,0%), (100%,50%), (0%,100%));
    minsize = (20,15);
}
```

Описание конструкции для перехода будет основываться на линии с двумя прикреплениями:

```
line transition {
    links = {(state,state), (state,pstate), (pstate,state),
        (pstate,pstate), (state,finalstate), (pstate,finalstate)};
    attachments[100%] = (:open_arr)[100%,50%];
    attachments[50%] = (lbl:label)[50%,110%];
}
```

Пара смежных вершин *state* и *pstate* входит в объявление дважды, поскольку графические связи в DiaDeL направленные.

Свяжем линию *transition* соответствующей оболочкой из нашей модели-обертки:



■ ***Рис. 5.*** *Представление перехода*

```
bridge <transition> {
    model := org.diadel.visualizer.wrapper.statemachine.WTransition;
    start := model.getStart();
    end   := model.getEnd();

    refresh() {
        lbl.value = «»;
        if («» != model.getTriggers()) {
            lbl.value = model.getTriggers();
        }
        if («» != model.getGuard()) {
            lbl.value = lbl.value + « [«;
            lbl.value = lbl.value + model.getGuard();
            lbl.value = lbl.value + «]»;
        }
        if (null != model.getModel().getEffect()) {
            lbl.value = lbl.value + « / «;
            lbl.value = lbl.value +
                    model.getModel().getEffect().getName();
        }
    }
}
```

Семантический мост для линии содержит объявления для определения инцидентных ее концам сущностей из модели и инициализацию метки на переходе. Для получения всех возможных триггеров, перечисленных через запятую, используется метод *getTriggers()* из обертки.

Последним штрихом описания будет декларация самой диаграммы состояний и семантического моста для нее:

```
diagram state_machine_diagram {
    contain = {state, transition, pstate, finalstate};
}
bridge <state_machine_diagram> {
    model := org.diadel.visualizer.wrapper.statemachine.WStateMachine;
    children := model.getChildren().get(0).getChildren();
}
```

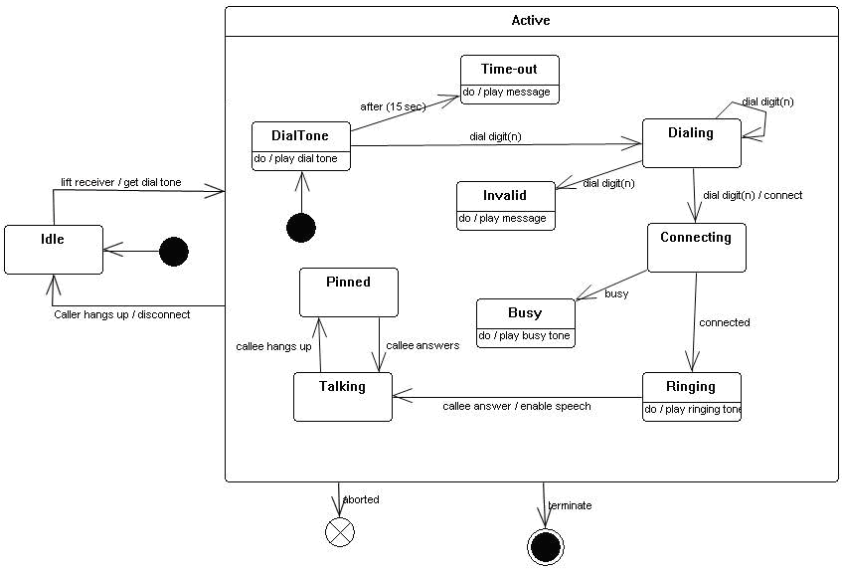
Получение коллекции сущностей, которые должны быть отображены на диаграмме, имеет несколько странный вид — *model.getChildren().get(0).getChildren()*. Это обусловлено тем, что состояния и прочие сущности-вершины содержатся в диаграмме опосредованно, через регионы. Ранее, в разделе «Анализ семантической модели», мы сделали предположение, что диаграмма и все составные состояния будут иметь ровно один регион, который и содержит все вложенные состояния и другие сущности-вершины.

Пример построенной диаграммы состояний

Используем приведенное выше DiaDeL-описание для построения экземпляра диаграммы состояний. Для этого нам понадобится экземпляр семантической модели, показанной на рис. 1, который будет отображен согласно описанию. В качестве экземпляра семантической модели возьмем машину состояний, моделирующую работу телефона [7]. Передав описание и экземпляр модели на вход системе автоматического представления диаграмм, мы получим результат, представленный на рис. 6.

Построенная диаграмма соответствует графической нотации диаграмм состояний UML. Мы добились компактного представления состояний, т. е. отображаются только те секции состояния, которые содержат информацию для отображения. Диаграмма не лишена недостатков, но все они носят графический характер и являются недостатками системы визуализации.

Следует также отметить, что вопрос укладывания построенных диаграмм лежит вне рамок языка **DiaDeL, т. е. расположение вершин и линий**, которое читатель видит на диаграмме, было выполнено вручную.



■ ***Рис. 6.*** *Диаграмма состояний, отображающая модель работы телефона, построенная по DiaDeL-описанию*

Заключение

В статье представлено практическое использование языка описания диаграмм DiaDeL на примере построения диаграммы состояний UML. Проанализирована входная семантическая модель, описаны на языке DiaDeL графические конструкции и их связь с элементами семантической модели. Приведена построенная диаграмма состояний.

Пример использования языка DiaDeL показывает, что поставленные перед языком цели успешно достигнуты. Язык позволяет гибко определять различные графические конструкции и свойства их отображения, связывать конструкции с внешними сущностями и определять их конечное представление в зависимости от состояния представляемых сущностей.

Платой за гибкость являются достаточно жесткие требования, предъявляемые к семантической модели. Однако их можно удовлетворить, разработав обертку для семантической модели, что в большинстве случаев не является сложной задачей для опытного программиста.

Язык DiaDeL дает возможность определять конечное отображение конструкции в зависимости от состояния представляемого объекта. Это позволяет, с одной стороны, решить базовые задачи, такие как отображение имени или других данных, с другой стороны, создавать более сложные конструкции и подстраивать их представление под отображаемый объект, что вносит еще одну «степень свободы» в проектирование конструкций и связей между ними и сущностями семантической модели.

Текущая версия реализации языка DiaDeL еще не может претендовать на промышленный уровень. Однако положенные в основу языка идеи обеспечивают его дальнейшее развитие. Концепция внешней семантической модели соответствует современному компонентному построению систем. Текстовая форма языка дает возможность расширять его в дальнейшем новыми конструкциями в целях повышения удобства использования и предоставления новых возможностей. Эти и другие факты позволяют считать разработку языка DiaDeL востребованной и перспективной.

Литература

1. **Степанян К. Б.** Язык описания диаграмм // Научно-технические ведомости СПбГПУ. 2006. № 6-1. С. 36–41.
2. **Новиков Ф. А., Степанян К. Б.** Язык описания диаграмм // Информационно-управляющие системы. 2007. № 4. С. 28–36.
3. **Новиков Ф. А., Степанян К. Б.** Использование порождающего программирования при реализации языка описания диаграмм // Информационно-управляющие системы. 2008. № 6. С. 33–36.
4. **Буч Г., Якобсон А., Рамбо Д.** UML. 2-е изд. СПб.: Питер, 2006.
5. **Канжелев С., Шалыто А.** Автоматическая генерация кода программ с явным выделением состояний / Software Engineering Conference (Russia) «Paths to Competitive Advantage» (SECR 2006). М., 2006. С. 60–63.
6. **Канжелев С., Шалыто А.** Преобразование графов переходов, представленных в формате MS Visio, в исходные коды программ для различных языков программирования (инструментальное средство MetaAuto). 102 с. http://is.ifmo.ru/projects/metaauto
7. **OMG Unified Modeling Language** (OMG UML), Superstructure, v2.1.2. http://www.omg.org/spec/UML/2.1.2/Superstructure/PDF
8. **EclipseUML.** http://www.eclipseplugincentral.com/displayarticle572.html
9. **Гамма Э., Хелм Р., Джонсон Р., Влиссидес Дж.** Приемы объектно-ориентированного проектирования. Паттерны проектирования. СПб.: Питер, 2004. 366 с.

УДК 681.3

КОНЕЧНЫЕ РАСШИРЕННЫЕ ПОЛЯ ДЛЯ АЛГОРИТМОВ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Н. А. Молдовян,
доктор техн. наук, профессор, гл. научный сотрудник
НФ ФГУП НИИ «Вектор» — специализированный центр программных систем «Спектр»
С. Е. Доронин,
аспирант
В. Е. Синев,
аспирант
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

Описываются новые частные варианты реализации конечных расширенных полей, предназначенных для построения производительных алгоритмов электронной цифровой подписи. Показано, что новая форма представления конечных расширенных полей путем задания специальной операции умножения в конечном m-мерном векторном пространстве обеспечивает возможность эффективного распараллеливания вычислений, благодаря чему обеспечивается повышение производительности алгоритмов электронной цифровой подписи, основанных на конечных группах матриц и эллиптических кривых при их задании над конечными расширенными полями, представленными в новой форме.

Ключевые слова *— эллиптические кривые, цифровая подпись, векторные конечные поля, конечные группы матриц.*

Введение

Из известных алгебраических структур, применяемых для построения алгоритмов электронной цифровой подписи (ЭЦП), наибольшую производительность процедур формирования и проверки подлинности ЭЦП при заданном уровне стойкости обеспечивают конечные группы точек эллиптической кривой (ЭК) благодаря тому, что в качестве координат ЭК достаточно использовать элементы конечного поля, порядок которого имеет сравнительно малый размер (160–256 бит). Групповой операцией на ЭК является композиция (сложение) точек, для выполнения которой осуществляется одна операция инверсии и несколько операций умножения координат [1–3]. Операция инверсии вносит основной вклад в ограничение производительности алгоритмов аутентификации информации, построенных с использованием ЭК. Актуальной для практики задачей является дальнейшее повышение производительности алгоритмов ЭЦП. В случае использования ЭК уменьшение сложности операции композиции точек достигается при представлении ЭК в проективных координатах [3], когда устраняется операция инверсии в конечном поле, над которым задана ЭК, однако увеличивается число умножений в этом поле. Предложение использовать конечные группы невырожденных матриц (КГНМ), заданные над конечным полем, для построения алгоритмов ЭЦП [4] дает возможность дальнейшего повышения производительности алгоритмов ЭЦП, однако при этом в два раза увеличивается размер открытого ключа.

В случае использования ЭК и КГНМ для построения алгоритмов ЭЦП определяющим фактором, влияющим на производительности, является сложность операции умножения в конечном поле, над которым задаются эти алгебраические структуры, и невозможность распараллеливания этой операции при использовании известных форм задания конечных полей. В известных реализациях ЭК и КГНМ используется простое поле, представленное кольцом Z_p, где p — простое число, или расширенное конечное поле многочленов. В первом случае умножение элементов поля реализуется как умножение чисел по модулю p, а во втором случае — как умножение многочленов по модулю неприводимого многочлена. Оба типа операции модульного умножения реализуются

с использованием операции обычного умножения и деления результата на простое число или неприводимый многочлен соответственно. Это не позволяет распараллелить операцию умножения в конечном поле с целью повысить производительности алгоритмов ЭЦП.

В настоящей работе для задания ЭК и КГНМ предлагается использовать конечные расширенные поля, формируемые в конечных m-мерных векторных пространствах, в которых операция умножения является распараллеливаемой по определению, а именно, координаты вектора-результата вычисляются независимо друг от друга. Это позволяет при аппаратной реализации существенно повысить производительность алгоритмов ЭЦП, использующих вычисления на ЭК или в КГНМ. Общая схема синтеза алгоритмов ЭЦП на основе ЭК и КГНМ остается прежней. Изменяется только форма представления конечного поля, над которым задаются эти структуры. Ввиду известного факта о изоморфизме всех конечных полей заданного порядка ожидается, что такая замена формы представления конечного поля не приведет к изменению структурных свойств ЭК и КГНМ и сложности задачи дискретного логарифмирования на ЭК или в КГНМ, которая определяет безопасность алгоритмов ЭЦП, построенных с использованием ЭК и КГНМ. В связи с этим в статье акцент делается на способ задания конечных расширенных полей в новой форме и условиях их формирования.

Конечные расширенные поля векторов над полем $GF(p)$

Рассмотрим конечное множество m-мерных векторов

$$a\mathbf{e} + b\mathbf{i} + ... + c\mathbf{j},$$

где **e**, **i**, ... **j** — базисные векторы, которые будем представлять также и в виде набора координат $(a, b, ..., c)$, являющихся элементами конечного поля $GF(p)$, где p — простое число. В дальнейшем нас будут интересовать условия, при которых рассматриваемое множество векторов будет обладать свойствами расширенного поля, поэтому определим на этом множестве две операции — сложение и умножение векторов. Операцию сложения векторов определим по следующему естественному правилу:

$$(a, b, ..., c) + (x, y, ..., z) = (a + x, b + y, ..., c + z).$$

Операцию умножения векторов определим по правилу умножения многочленов с учетом того, что умножение базисных векторов выполняется по некоторым табличным правилам, ставящим в соответствие каждой паре умножаемых базисных векторов третий базисный вектор (возможно, совпадающий с одним из перемножаемых базисных векторов) или третий базисный вектор, умноженный на некоторый коэффициент ε, являющийся элементом поля $GF(p)$. Таким образом, имеем

$$(a\mathbf{e} + b\mathbf{i} + ... + c\mathbf{j})(x\mathbf{e} + y\mathbf{i} + ... + z\mathbf{j}) = \\ = ax\cdot\mathbf{ee} + ay\cdot\mathbf{ei} + ... + az\cdot\mathbf{ej} + bx\cdot\mathbf{ie} + by\cdot\mathbf{ii} + ... + \\ + bz\cdot\mathbf{ij} + ... + cx\cdot\mathbf{je} + cy\cdot\mathbf{ji} + ... + cz\cdot\mathbf{jj},$$

где каждое из произведений **ee**, **ei**, ..., **ej**, **ie**, **ii**, ..., **ij**, **je**, **ji**, ..., **jj** следует заменить на задаваемое таблицей умножения базисных векторов значение ε**v**, где **v** — вектор, принадлежащий множеству базисных векторов. Синтез таблицы является определяющим моментом в задании конкретного варианта операции умножения, которая определяет тип алгебраической структуры, формируемой в конечном пространстве m-мерных векторов при заданном поле $GF(p)$. Таблица умножения базисных векторов определяет над их множеством некоторую операцию. Нас интересует случай образования конечных групп в пространстве m-мерных векторов, поэтому указанная таблица должна быть составлена с учетом обеспечения свойства ассоциативности умножения базисных векторов. В общем случае порядок умножаемых базисных векторов имеет значение, однако мы ограничимся рассмотрением наиболее интересного для нас случая задания коммутативной операции умножения базисных векторов. Легко показать, что свойство коммутативности и ассоциативности умножения базисных векторов естественным способом переходит в свойство коммутативности и ассоциативности умножения m-мерных векторов. При выполнении этого условия в конечном векторном пространстве формируются структуры со свойствами коммутативной группы. Конкретные варианты таблиц, задающих правила умножения базисных векторов, рассмотрены далее.

Ниже будет показано, что при определенных соотношениях между размерностью векторов m и порядком поля p в частных случаях задания операции умножения векторов формируются конечные расширенные поля $GF(p^m)$. Сравним сложность операции умножения в поле такого типа со сложностью умножения в простом поле $\boldsymbol{Z}_{p'}$, где $|p'| = m|p|$ и $|p|$ обозначает битовую длину числа p (т. е. в случае полей с одинаковым размером порядка). Операция умножения элементов поля $GF(p^m)$ включает m^2 операций умножения в поле $GF(p)$, причем сложность операции умножения в поле $GF(p)$ пропорциональна $|p|^2$, поэто-

му при прямолинейном выполнении операции умножения в поле $GF(p^m)$, представленном в векторной форме, ее сложность примерно равна сложности умножения в поле Z_p, (операции арифметического сложения мы не учитываем, поскольку их вклад достаточно мал).

Однако имеется возможность снизить сложность умножения элементов поля $GF(p^m)$ следующим образом. Осуществляются обычные арифметические операции умножения соответствующих пар координат векторов-сомножителей, результаты суммируются, а затем выполняется операция арифметического деления полученного результата на значение p. При этом число арифметических умножений остается равным m^2, а число делений уменьшается в m раз, становясь равным m. При этом сложность операции деления возрастает за счет увеличения делимого несущественно, так как размер последнего увеличивается всего лишь в m раз, т. е. его длина возрастает на несколько битов. Это не вносит существенного увеличения сложности операции деления в случае практически значимых размеров значений координат, которые определяются размерами модуля от $|p| = 16$ до $|p| = 200$ бит для значений размерности от $m = 13$ до $m = 3$ соответственно. Поскольку сложность операции деления значительно превосходит сложность операции умножения, то сложность операции умножения элементов поля $GF(p^m)$ снижается примерно пропорционально значению m. Наличие дополнительных операций умножения на коэффициенты растяжения, используемые для создания условия формирования полей в конечных векторных пространствах, не вносит существенного вклада в общую сложность всех операций арифметического умножения, поскольку в качестве таких коэффициентов можно подобрать числа размером в 2–3 бит.

Рассмотрим сложность умножения в поле $GF(p^m)$, заданном в виде конечного кольца многочленов степени $m - 1$. Операция умножения двух многочленов включает m^2 операций арифметического умножения $|p|$-битовых чисел и m операций деления $2|p|$-битовых чисел на модуль p (операциями сложения пренебрегаем ввиду их низкой сложности). В результате получаем многочлен степени $2m - 2$, который далее делится на неприводимый многочлен. Наличие этой операции не допускает эффективного распараллеливания операции умножения в поле многочленов. Наиболее эффективная реализация деления на неприводимый многочлен требует выполнения примерно m^2 операций арифметического умножения $|p|$-битовых чисел и m операций деления $2|p|$-битовых чисел на модуль p. Видим, что в целом операция умножения в поле многочленов, по крайней мере, в два раза сложнее операции умножения в поле $GF(p^m)$, заданном в векторном пространстве.

Таким образом, переход к новой форме задания расширенных конечных полей дает выигрыш в вычислительной эффективности *даже в случае использования однопроцессорного вычислительного устройства*. При этом операция умножения в поле $GF(p^m)$, заданном в конечном векторном пространстве, обладает возможностью эффективного распараллеливания на m процессов, поэтому при увеличении сложности аппаратной реализации имеется возможность сократить время выполнения умножения в поле $GF(p^m)$ примерно до m^2 раз в сравнении с простым полем и до $2m$ раз в сравнении с конечным полем многочленов. (Процедуры, входящие в операцию умножения в поле многочленов и выполняемые до деления на неприводимый многочлен, могут быть выполнены параллельно, но это увеличивает аппаратные затраты, приводя к уменьшению времени выполнения умножения в поле многочленов всего лишь в $2m(m + 1)^{-1}$ раз. В сравнении с этим вариантом реализации операции умножения многочленов распараллеливание операции умножения в векторном поле дает сокращение времени в m раз.)

Конечные группы и поля в пространстве трехмерных векторов

При $m = 3$ общие правила умножения базисных векторов, обеспечивающие свойства коммутативности и ассоциативности операции умножения векторов, представлены в табл. 1, где ε и μ — коэффициенты растяжения, $\varepsilon, \mu \in GF(p)$. В зависимости от конкретной пары значений ε и μ множество трехмерных векторов является конечным полем или конечной группой. Поскольку определенные нами операции сложения и умножения векторов являются коммутативными и ассоциативными, а операция умножения дистрибутивна по отношению к операции сложения, то конечное пространство трехмерных векторов будет образовывать расширенное поле $GF(p^3)$, если для каждого отличного от (0, 0, 0) трехмерного вектора существует вектор, являющийся обратным к нему. В противном случае будем иметь группу, порядок которой определяется числом векторов, для которых существуют соответствующие обратные элементы. Решение этого вопроса связано с анализом характеристического уравнения третьей степени, возникающего из условия существования вектора $(x\mathbf{e} + y\mathbf{i} + z\mathbf{j})$, являющегося обратным значением к векторам вида $a\mathbf{e} + b\mathbf{i} + c\mathbf{j}$, где хотя бы одна из координат a, b, c отлична от нуля. Исходя из условия существования обрат-

ных значений запишем в соответствии с табл. 1 и общим определением операции умножения векторов следующее соотношение:

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j})(x\mathbf{e} + y\mathbf{i} + z\mathbf{j}) = (ax + \varepsilon\mu cy + \mu\varepsilon bz)\mathbf{e} + (bx + ay + \mu cz)\mathbf{i} + (az + \varepsilon by + az)\mathbf{j},$$

из которого видно, что вопрос существования обратных значений сводится к вопросу существования решений системы уравнений вида

$$\begin{cases} ax + \varepsilon\mu cy + \varepsilon\mu bz = 1 \\ bx + ay + \mu cz = 0 \\ cx + \varepsilon by + az = 0 \end{cases}.$$

Равенство нулю главного определителя этой системы для некоторых троек значений (a, b, c) задает векторы $a\mathbf{e} + b\mathbf{i} + c\mathbf{j}$, для которых не существует обратных элементов. Таким образом, получаем следующее характеристическое уравнение:

$$a^3 - 3\varepsilon\mu bca + \varepsilon^2\mu b^3 + \varepsilon\mu^2 c^3 \equiv 0 \bmod p.$$

Используя формулу Кардано [5] и обозначение $B = (\varepsilon^2\mu b^3 + \varepsilon\mu^2 c^3)/2$, решение последнего уравнения относительно неизвестного a можно записать в виде

$$a_0 = A' + A'',$$

где

$$A' = \sqrt[3]{B + \sqrt{B^2 - (\varepsilon\mu bc)^3}} = \sqrt[3]{-\varepsilon\mu^2 c^3} \pmod p \text{ и}$$

$$A'' = \sqrt[3]{B - \sqrt{B^2 - (\varepsilon\mu bc)^3}} = \sqrt[3]{-\varepsilon^2\mu b^3} \pmod p.$$

Из исследования характеристического уравнения вытекают следующие типовые варианты структур рассматриваемого множества трехмерных векторов.

Случай 1. Число 3 не делит $p - 1$. Существует единственное значение кубичного корня для всех значений подкоренного выражения. В этом случае число корней характеристического уравнения определяется значением его дискриминанта [5]

$$D = -27\left(\varepsilon^2\mu b^3 - \varepsilon\mu^2 c^3\right)^2 \pmod p.$$

Если $c \equiv b\sqrt[3]{\varepsilon} \bmod p$, то $D = 0$ и существует два разных корня a'_0 и a''_0, поэтому для $2(p - 1)$ векторов вида $\left(a'_0, b, b\sqrt[3]{\varepsilon} \bmod p\right)$ и $\left(a''_0, b, b\sqrt[3]{\varepsilon} \bmod p\right)$, где $b \in \{1, 2, ..., p - 1\}$, не существует обратных значений. Если $c \neq b\sqrt[3]{\varepsilon} \bmod p$, то $D \neq 0$ и существует только один корень a_0, поэтому для $p(p - 1)$ векторов вида (a_0, b, c), где $b, c \in \{1, 2, ..., p - 1\}$, не существует обратных значений. Учитывая также, что не существует обратного значения для вектора (0, 0, 0), и вычитая из полного числа трехмерных векторов число векторов, для которых не существует обратных значений, получаем формулу для порядка группы трехмерных векторов

$$\Omega = p^3 - 2(p - 1) - p(p - 1) - 1 = (p - 1)^2(p + 1).$$

Экспериментально установлено, что в рассматриваемом случае группа векторов является нециклической и содержит циклические подгруппы порядка, равного $\Omega' \le (p - 1)(p + 1)$. Случай таких групп при $p = Nk^2 + 1$ или $p = Nk^2 - 1$, где k — большое простое число и N – нечетное число, представляет значительный интерес для разработки алгоритмов ЭЦП, основанных на сложности вычисления корней большой простой степени, аналогичных алгоритмам, предложенным в работе [6].

Случай 2. Число 3 делит $p - 1$, и каждое из произведений $\varepsilon^2\mu$ и $\varepsilon\mu^2$ является кубичным вычетом в поле $GF(p)$. Анализ дискриминанта характеристического уравнения показывает, что для $h = 6(p - 1) - 3(p^2 + 9(p - 1) + 2$ векторов не существует обратных значений. Вычитая из полного числа векторов значение h, получаем порядок группы

$$\Omega = p^3 - h = (p - 1)^3.$$

Эксперимент показал, что в рассматриваемом случае группа векторов является нециклической и содержит циклические подгруппы порядка, равного $\Omega' \le (p - 1)$. Случай таких групп также представляет интерес для разработки алгоритмов ЭЦП (основанных на сложности вычисления корней большой простой степени).

Случай 3. Число 3 делит $p - 1$, и каждое из произведений $\varepsilon^2\mu$ и $\varepsilon\mu^2$ является кубичным невычетом в поле $GF(p)$. Это может иметь место, например, в случае, когда ε — кубичный вычет, а μ — кубичный невычет, или наоборот. Тогда существует единственная пара значений b и c, а именно

■ ***Таблица 1.*** *Таблица умножения базисных векторов трехмерного пространства*

×	**e**	**i**	**j**
e	**e**	**i**	**j**
i	**i**	ε**j**	$\varepsilon\mu$**e**
j	**j**	$\varepsilon\mu$**e**	μ**i**

$b = c = 0$, для которой имеется решение $a_0 = 0$ характеристического уравнения. Это означает, что в этом случае каждому ненулевому вектору можно сопоставить обратный вектор. Следовательно, в рассматриваемом случае совокупность всех трехмерных векторов образует поле $GF(p^3)$, мультипликативная группа которого является циклической и имеет порядок

$$\Omega = p^3 - 1 = (p - 1)(p^2 + p + 1).$$

Эксперимент показывает, что и в этом случае легко найти такое значение p, при котором значение $\Omega' = (p^2 + p + 1)/3$ является простым. Циклические подгруппы такого порядка представляют интерес для построения алгоритмов ЭЦП, основанных на сложности задачи дискретного логарифмирования в поле трехмерных векторов.

Случай 4. При $\varepsilon = 0$, либо $\mu = 0$, либо $\varepsilon = 0$ и $\mu = 0$ имеем «вырожденный случай», когда характеристическое уравнение имеет вид $a^3 \equiv 0 \bmod p$ и единственное решение $a_0 = 0$ для всех пар значений b и c. Для этого случая получаем следующее значение порядка группы:

$$\Omega = p^3 - p^2 = p^2(p - 1).$$

Эксперимент показал, что такая группа векторов является нециклической и содержит циклические подгруппы порядка, равного $\Omega' \le p(p - 1)$.

Пример 1. *Векторное поле* $GF(p^3)$. Для простого $p = 604884627778815030120967$ и коэффициентов $\mu = 1$ и $\varepsilon = 3048145277787150301203$ (кубичный невычет) генератором мультипликативной группы поля $GF(p^3)$ является вектор $\mathbf{G}_\Omega = 2\mathbf{e} + 3\mathbf{i} + 5\mathbf{j}$, а генератором подгруппы простого порядка $q = 12196180430770520253333277444585228380992277120 19$ — вектор $\mathbf{G}_q = 2766732051010005739014 75\mathbf{e} + 3973984426601319676024 19\mathbf{i} + 5777541997290551329836 73\mathbf{j}$.

Поля многомерных векторов

Изучение вопроса существования полей векторов размерности $m \ge 4$ дало положительный ответ. Аналогично построению конечных полей трехмерных векторов, можно задать формирование полей многомерных векторов. Для того чтобы множество m-мерных векторов составляло поле $GF(p^m)$, следует выбирать поле $GF(p)$, для характеристики которого выполняется условие делимости $m \mid p - 1$. Кроме того, в соответствующую таблицу умножения базисных векторов надо ввести коэффициенты растяжения, значения которых являются невычетами степени m в поле $GF(p)$. В этом случае многомерные векторные пространства (для $m \ge 4$), над которыми заданы принятые выше операции сложения и умножения, могут составить конечное поле $GF(p^m)$. Рассмотрим некоторые частные варианты.

Случай $m = 4$. Определим операцию умножения четырехмерных векторов $a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ с помощью табл. 2, которая обеспечивает свойство коммутативности и ассоциативности. Задавая различные конкретные значения растягивающих коэффициентов, можно задавать различные варианты полей $GF(p^4)$. Существует еще несколько вариантов таблиц, с помощью которых можно задать формирование векторного поля в конечном пространстве четырехмерных векторов, которые отличаются распределением базисных векторов и коэффициентов растяжения, а также числом последних и их значениями. Для генерации следующего частного примера использована табл. 2.

Пример 2. *Векторное поле* $GF(p^4)$. Для простого $p = 670657405878917$ и коэффициентов $\mu = 1$ и $\varepsilon = 33322555333777$ (невычет 4-й степени) генератором мультипликативной группы поля $GF(p^4)$ является вектор $\mathbf{G}_\Omega = 2\mathbf{e} + 5\mathbf{i} + 7\mathbf{j} + 11\mathbf{k}$, а генератором подгруппы максимального простого порядка $q = 51058526584281452221$ является вектор $\mathbf{G}_q = 387227204127143\mathbf{e} + 285726718179315\mathbf{i} + 399932449346308\mathbf{j} + 297703341165198\mathbf{k}$.

Случай $m = 5$. Определим операцию умножения пятимерных векторов $a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} + g\mathbf{u}$ с помощью табл. 3, в которой присутствуют несколько различных независимых коэффициентов растяжения. При любой комбинации значений этих коэффициентов операция умножения

■ ***Таблица 2.*** *Таблица умножения базисных векторов для случая* $m = 4$

×	e	i	j	k
e	e	i	j	k
i	i	εμj	εk	εμe
j	j	εk	εe	i
k	k	εμe	i	μj

■ ***Таблица 3.*** *Таблица умножения базисных векторов для случая* $m = 5$

×	e	i	j	k	u
e	e	i	j	k	u
i	i	εj	εμk	εu	εμe
j	j	εμk	εμu	εμe	μi
k	k	εu	εμe	i	J
u	u	εμe	μi	j	μk

векторов является коммутативной и ассоциативной. При программной реализации операции умножения векторов в клетках таблицы, где присутствуют два или более растягивающих коэффициентов, значения последних следует перемножить, благодаря чему формируется таблица, в каждой клетке которой присутствует не более одного коэффициента. Табл. 3 использована для генерации следующего примера.

Пример 3. *Векторное поле* $GF(p^5)$. Для простого $p = 268675256028581$ и коэффициентов $\mu = 1$ и $\varepsilon = 3048145277787$ (невычет 5-й степени) генератором мультипликативной группы поля $GF(p^5)$ является вектор $\mathbf{G}_\Omega = 2\mathbf{e} + 5\mathbf{i} + 7\mathbf{j} + 11\mathbf{k} + 13\mathbf{u}$, а генератором подгруппы простого порядка $q = 10421\,75072703434265745203478134729214503105234181740193961$ — вектор $\mathbf{G}_q = 88815218764680\mathbf{e} + 238886012231841\mathbf{i} + 157317400153847\mathbf{j} + 21593513218048\mathbf{k} + 204824491909450\mathbf{u}$.

Формирование конечных полей для случая $m = 6$ можно обеспечить, используя табл. 4, а для случая $m = 7$ – табл. 5. Практическое значение для разработки алгоритмов ЭЦП, основанных на вычислениях в конечных группах ЭК и КГНМ, заданных над полями, представленными в предлагаемой форме, имеют также и случаи размерностей $m > 7$. Нами были построены таблицы умножения базисных векторов, обеспечивающие формирование полей, для произвольных значений размерности до $m = 23$. Для этих случаев эксперимент подтвердил существование полей при таких значениях размерности.

Найденные правила построения таблиц умножения базисных векторов, содержащих коэффициенты растяжения, позволяют обеспечить свойства коммутативности и ассоциативности умножения m-мерных векторов для произвольных значений размерности. Однако теоретическое доказательство факта возможности формирования полей по таким таблицам путем выбора соответствующих коэффициентов растяжения имеет принципиальные трудности и представляет самостоятельную задачу теории линейных алгебр. Объективная трудность такого доказательства определяется большой общностью этого факта. Для технических приложений представляется достаточным использование частных случаев значений размерности до $m = 23$, подтвержденных экспериментом. Если практика потребует использования конечных расширенных полей, заданных в векторном пространстве размерности $m > 23$, то экспериментальная проверка факта существования конечных полей и для таких случаев не составит существенных проблем.

■ ***Таблица 4.*** *Таблица умножения базисных векторов для случая* $m = 6$

×	**e**	**i**	**j**	**k**	**v**	**w**
e	**e**	**i**	**j**	**k**	**u**	**v**
i	**i**	ε**j**	$\varepsilon\mu$**k**	**u**	ε**v**	$\varepsilon\mu$**e**
j	**j**	$\varepsilon\mu$**k**	μ**u**	**v**	$\varepsilon\mu$**e**	μ**i**
k	**k**	**u**	**v**	**e**	**i**	**j**
u	**u**	ε**v**	$\varepsilon\mu$**e**	**i**	$\varepsilon\mu$**j**	$\varepsilon\mu$**k**
v	**v**	$\varepsilon\mu$**e**	μ**i**	**j**	$\varepsilon\mu$**k**	μ**u**

■ ***Таблица 5.*** *Таблица умножения базисных векторов для случая* $m = 7$

×	**e**	**i**	**j**	**k**	**u**	**v**	**w**
e	**e**	**i**	**j**	**k**	**u**	**v**	**w**
i	**i**	$\varepsilon\mu$**k**	$\varepsilon\nu$**v**	$\mu\tau$**u**	$\varepsilon\nu$**w**	$\varepsilon\mu\tau$**e**	$\mu\tau$**j**
j	**j**	$\varepsilon\nu$**v**	ε**u**	$\varepsilon\mu\tau$**e**	ε**i**	ε**w**	ε**k**
k	**k**	$\mu\tau$**u**	$\varepsilon\mu\tau$**e**	$\mu\tau$**w**	$\mu\tau$**j**	τ**i**	$\mu\tau$**v**
u	**u**	$\varepsilon\nu$**w**	ε**i**	$\mu\tau$**j**	$\varepsilon\nu$**v**	ε**k**	$\varepsilon\mu\tau$**e**
v	**v**	$\varepsilon\mu\tau$**e**	ε**w**	τ**i**	ε**k**	τ**j**	τ**u**
w	**w**	$\mu\tau$**j**	ε**k**	$\mu\tau$**v**	$\varepsilon\mu\tau$**e**	τ**u**	τ**v**

Алгоритмы ЭЦП с использованием конечных расширенных полей, заданных в новой форме

Рассмотренные выше конечные поля, представленные в векторной форме и допускающие эффективное распараллеливание операции умножения, представляют технический интерес для повышения быстродействия алгоритмов ЭЦП, построенных на основе использования ЭК и КГНМ, путем задания ЭК и КГНМ над такими полями. В случае ЭК вопрос стойкости алгоритмов ЭЦП связан с выбором ЭК соответствующего типа, определяемого значением характеристики поля (т. е. значением p), и выбором конкретного варианта ЭК, порядок которой делится на простое число большого размера. Методика генерации таких кривых хорошо апробирована [1, 2]. В случае КГНМ вопрос безопасности алгоритмов ЭЦП является весьма актуальным, поскольку это направление сравнительно мало освещено в литературе и вопрос стойкости алгоритмов на их основе исследован недостаточно. Касательно использования КГНМ в качестве примитивов алгоритмов ЭЦП, в настоящей работе преследуется цель только показать принципиальную возможность повышения производительности алгоритмов и в случае использования КГНМ. Этот факт представит значительный практический интерес, если дальнейшие специализированные исследования приведут к подтверждению высокой

сложности задачи дискретного логарифмирования в КГНМ, заданных над конечными полями размера 160–200 бит.

Следует отметить, что определенный интерес представляет также непосредственное применение конечных расширенных полей, представленных в новой форме. Рассмотрим возможный вариант обобщенной схемы ЭЦП, основанной на сложности дискретного логарифмирования в конечных расширенных полях, предполагая в нем использование циклической группы векторов Г. Подписывающий формирует свой открытый ключ Y в виде вектора $\mathbf{Y} = \mathbf{G}^x$, где $\mathbf{G}$ — вектор, являющийся генератором группы Г, имеющей достаточно большой порядок q ($|q| \geq 160$ бит).

Формирование подписи к сообщению M выполняется следующим образом.

1. Выбрать случайное число $k < q$ и вычислить вектор $\mathbf{R} = \mathbf{G}^k$.

2. Используя некоторую криптографически стойкую хэш-функцию F_h, вычислить хэш-код h от сообщения M с присоединенным к нему вектором $\mathbf{R}$: $h = F_h(M, \mathbf{R})$; значение h будет первым элементом ЭЦП.

3. Вычислить второй элемент ЭЦП: $s = xh + k \bmod q$.

Проверка подлинности подписи (h, s) состоит в следующем:

1) вычисляется вектор $\mathbf{R}' = \mathbf{Y}^{q-h}\mathbf{G}^s$;

2) вычисляется значение $h' = F_h(M, \mathbf{R}')$;

3) сравниваются значения h' и h; если $h' = h$, то ЭЦП признается подлинной.

Конкретный вариант алгоритмической реализации этой общей схемы ЭЦП задается выбором конкретной группы Г, характеризующейся размерностью векторов, заданным типом операции умножения векторов и полем $GF(p)$, над которым задается конечное векторное пространство. Многочисленные другие известные варианты схем ЭЦП [6–8], построенные с использованием простых конечных полей, могут быть заданы также и над полями, формируемыми в конечном векторном пространстве.

В целях реализации вычислительно эффективных алгоритмов ЭЦП, непосредственно базирующихся на полях в предлагаемой форме, требуется получить циклическую подгруппу векторов большого простого порядка q, размер которого удовлетворяет условиям $|q| \geq 160$ бит и $|q| \approx (m-1)|p|$. Последнее условие возможно только для простых значений m. Действительно, порядок мультипликативной группы конечного расширенного поля $GF(p^m)$ равен

$$\Omega = p^m - 1 = (p-1)(p^{m-1} + p^{m-2} + \ldots + p + 1).$$

Легко показать, что если размерность m не является простым числом, то вторая скобка разлагается на нетривиальные множители для любого простого числа p. При условии $m \mid p-1$ (которое имеет место в случае формирования векторных полей) сумма $p^{m-1} + p^{m-2} + \ldots + p + 1$ делится на m, поэтому простым может быть только порядок циклической подгруппы мультипликативной группы поля $GF(p^m)$, равный $q = m^{-1}(p^{m-1} + p^{m-2} + \ldots + p + 1)$. Эксперимент показывает, что легко найти такие значения простого p, для которых такое значение q также является простым. В этом случае имеем циклическую подгруппу векторов, размер порядка которой равен

$$|\Omega'| = |q| = (m-1)|p| - |m| \approx (m-1)|p|.$$

Для построения алгоритмов ЭЦП требуется использовать подгруппы простого порядка размером $|\Omega'| \geq$ **160 бит. Для этой цели следует формировать** поля m-мерных векторов, заданных над простым полем с размером характеристики $|p|$, удовлетворяющим условию

$$|p| \geq \frac{160 - |m|}{m-1} \approx \frac{160}{m-1} \text{ [бит]}.$$

Таким образом, важное требование наличия в мультипликативной группе поля подгруппы простого порядка достаточно большого размера реализуется при сравнительно малом размере $|p|$. Практическое значение для разработки алгоритмов ЭЦП, основанных на сложности задачи дискретного логарифмирования в новых полях, имеют случаи $m \in \{3, 5, 7, 11, 13, 17, 19, 23\}$.

В общем случае при построении векторных полей для непосредственного применения в алгоритмах ЭЦП, основанных на сложности задачи дискретного логарифмирования, таблицы умножения базисных векторов следует задавать с учетом компромисса между следующими моментами.

- В получаемой алгебраической структуре должны содержаться группы большого простого порядка, размер которого близок к значению $(m-1)|p|$.
- Количество умножений в поле $GF(p)$, необходимых для выполнения операции умножения двух векторов, следует минимизировать.
- Размер коэффициентов растяжения и число ячеек таблицы умножения базисных векторов, где они присутствуют, следует минимизировать.
- В получаемой циклической группе векторов сложность задачи дискретного логарифмирования (нахождение x в уравнении вида $\mathbf{Y} = \mathbf{G}^x$, где $\mathbf{G}$ — генератор группы) должна быть достаточно высокой.

Основной проблемой непосредственного использования конечных полей, заданных в предлагаемой форме, является то, что сложность задачи дискретного логарифмирования в них является новой. Поэтому повышение производительности путем снижения размера порядка поля

ниже 1024 бит, т. е. ниже безопасного значения, признанного в случае конечных полей многочленов, является преждевременным. Тем не менее, существенный выигрыш в производительности достигается благодаря снижению сложности операции умножения элементов поля и возможности эффективного распараллеливания в случае использования многопроцессорного вычислителя или за счет увеличения схемотехнических затрат в случае аппаратной реализации. С учетом этого можно предположить, что для некоторых приложений непосредственное применение полей, заданных в предлагаемой форме, также представит определенный интерес, поскольку достаточно высокая производительность алгоритмов ЭЦП, основанных на непосредственном использовании полей, заданных в конечном векторном пространстве, обеспечивается также и при больших размерах порядка такого поля.

Заключение

При обеспечении условия делимости числа $p - 1$ на m имеется возможность разработать таблицу умножения базисных векторов, определяющую формирование конечного расширенного поля в пространстве векторов, в котором операция умножения допускает эффективное распараллеливание. Кроме того, при заданном значении размера порядка поля в случае полей, заданных в новой форме, снижается сложность операции умножения элементов поля. Данное представление полей может быть использовано при построении алгоритмов ЭЦП, основанных на использовании ЭК и КГНМ, путем задания этих алгебраических структур над конечными полями предложенного вида. Также представляет интерес и непосредственное применение полей такого типа при построении алгоритмов ЭЦП, однако в последнем случае в настоящее время следует рекомендовать значения размера порядка поля, равные 1024 бит и более. Вопрос снижения этого значения в целях дальнейшего повышения производительности требует выполнения исследования сложности задачи дискретного логарифмирования в предлагаемом варианте расширенных полей, что составляет задачу самостоятельного исследования.

Работа поддержана грантом РФФИ № 08-07-00096-а.

Литература

1. **Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А.** Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. М.: КомКнига, 2006. 324 с.
2. **Болотов А. А., Гашков С. Б., Фролов А. Б.** Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006. 274 с.
3. **Koblitz N. A.** Course in Number Theory and Cryptography. Berlin: Springer-Verlag, 2003. 236 p.
4. **Гурьянов Д. Ю., Дернова Е. С., Молдовян Н. А.** Построение алгоритмов электронной цифровой подписи на основе групп матриц малой размерности // Информационная безопасность регионов России: Материалы V Санкт-Петербургской межрегион. конф. СПОИСУ. СПб., 2007. С. 79–80.
5. **Курош А. Г.** Курс высшей алгебры. М.: Наука, 1971. 431 с.
6. **Молдовян Н. А.** Вычисление корней по простому модулю как криптографический примитив // Вестник СПбГУ. Сер. 10. 2008. Вып. 1. С. 101–106.
7. **Молдовян Н. А.** Практикум по криптосистемам с открытым ключом. СПб.: БХВ-Петербург, 2007. 298 с.
8. **Menezes A. J., Van Oorschot P. C., Vanstone S. A.** Handbook of Applied Cryptography. CRC Press, Boca Raton, FL, 1997. 780 p.

УДК 519.688

ПРИМЕНЕНИЕ МОДИФИКАЦИИ КРИПТОСИСТЕМЫ НИДЕРРАЙТЕРА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ВИДЕОИЗОБРАЖЕНИЙ

М. А. Самохина*,
ассистент,
Московский физико-технический институт

Рассматривается построение модификации криптосистемы Нидеррайтера, основанной на матрице фробениусовского вида, а также применение данной криптосистемы для передачи и защиты меняющихся изображений. Сделано заключение о криптостойкости системы.

Ключевые слова *— криптосистемы с открытым ключом, линейные коды, ранговые коды, криптоанализ, теория информации, защита информации, помехоустойчивое кодирование.*

Введение. Классическая криптосистема Нидеррайтера

В теории криптосистем с открытым ключом известны два основных типа систем, основанных на линейных кодах: система Мак Элиса (McElice) [1] и система Нидеррайтера [2]. В данной работе остановимся на криптосистемах, построенных на основе последней.

В качестве секретных ключей выбираются:

- проверочная матрица $\mathbf{H} = \left[z_j x_j^i \right]$, где $j = 1, 2, ..., n$, $i = 0, 1, ..., r - 1$, некоторого обобщенного кода Рида—Соломона над полем $GF(q)$;
- случайно выбранная невырожденная скремблирующая матрица $\mathbf{S}$ порядка r над полем $GF(q)$. Эта матрица вводится для того, чтобы скрыть от криптоаналитика видимые закономерности, разрушая структуру проверочной матрицы.

Открытым ключом является скремблированная проверочная матрица $\mathbf{H}_{cr} = \mathbf{SH}$.

Сообщениями являются все n-векторы с координатами из поля $GF(q)$ с весом, не превосходящим $r/2$. Здесь сообщения не являются кодовыми словами выбранного кода Рида—Соломона, а представляют собой всевозможные ошибки, которые этот код в состоянии исправлять.

Шифротекст, соответствующий сообщению m, представляет собой r-вектор и вычисляется следующим образом:

$$c = m\mathbf{H}_{cr}^T = m\mathbf{H}^T\mathbf{S}^T.$$

Законный пользователь после приема шифротекста c умножает его справа на матрицу $(\mathbf{ST})^{-1}$, а затем применяет известный лишь ему алгоритм быстрого декодирования и получает переданное сообщение m.

После официального представления данной классической схемы были предприняты неоднократные попытки ее вскрыть, которые увенчались успехом. В 1992 г. российскими криптоаналитиками Сидельниковым и Шестаковым была опубликована работа [3], где авторы описывали успешную атаку и приводили ее подробный алгоритм. Основная идея атаки состояла в раскрытии структуры закрытого ключа по открытому и подборе матриц $\tilde{\mathbf{H}}$ и $\tilde{\mathbf{S}}$ таких, что $\mathbf{H}_{cr} = \tilde{\mathbf{S}}\tilde{\mathbf{H}}$.

Новая модификация криптосистемы Нидеррайтера

В настоящее время существует три основных подхода к модификации криптосистемы. Первый подход заключается в зашумлении проверочной матрицы кода введением скрывающей матрицы. Например, в работе [4] была предложена скрывающая матрица единичного ранга. В работе [5] использовались скрывающие матрицы ранга, значительно большего единицы. Второй

*Научный руководитель — доктор техн. наук, профессор, заведующий кафедрой радиотехники Московского физико-технического института *Э. М. Габидулин*.

подход заключается в использовании различных метрик, отличных от классической хэммингова метрики. Например, выбирается ранговая метрика (как в работе [6]) или вводится некая новая метрика. И третий вариант модифицирования классической криптосистемы Нидеррайтера — это построение кодов с набором специфических свойств. Рассмотрим вариант применения сразу трех способов модификаций.

Модификация на основе фробениусовской метрики. Новая нехэмминговая метрика данной модификации строится на немодифицированной матрице Фробениуса. Выбирается некоторая матрица **F** фробениусовского вида размером $N \times n$ с элементами из поля $GF(q^N)$:

$$\mathbf{F} = \begin{pmatrix} h_1 h_1^q \ldots\ldots\ldots h_1^{q^{n-1}} \\ h_2 h_2^q \ldots\ldots\ldots h_2^{q^{n-1}} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ h_N \ldots\ldots h_N^q h_N^{q^{n-1}} \end{pmatrix}.$$

Каждый элемент матрицы — элемент расширенного поля $GF(q^N)$. Элементы $h_1, h_2, \ldots, h_N$ выбираются таким образом, чтобы они были линейно независимыми над ***базовым*** полем. Необходимо, чтобы ранг матрицы **F** не превосходил n и $n < N$. Обозначим $\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_N$ строки матрицы **F**. Норма любого ненулевого вектора **x** из пространства $GF(q^N)^n$ определяется как минимальное число ненулевых коэффициентов a_i в разложении:

$$\mathbf{x} = \sum_{i=1}^{n} a_i \mathbf{h}_i.$$

Для построения кода используется конкатенация матрицы **F** и некоторой матрицы $\mathbf{G}_k$, имеющей такую же структуру, как и **F**:

$$\mathbf{Q} = \begin{pmatrix} h_1 & h_1^q & \ldots & h_1^{q^{n-1}} \\ h_2 & h_2^q & \ldots & h_2^{q^{n-1}} \\ \vdots & \vdots & \ldots & \vdots \\ h_{N_1} & h_{N_1}^q & \ldots & h_{N_1}^{q^{n-1}} \\ g_1 & g_1^q & \ldots & g_1^{q^{n-1}} \\ g_2 & g_2^q & \ldots & g_2^{q^{n-1}} \\ \vdots & \vdots & \ldots & \vdots \\ g_K & g_K^q & \ldots & g_K^{q^{n-1}} \end{pmatrix} = \begin{pmatrix} \mathbf{F} \\ \mathbf{G}_k \end{pmatrix},$$

где

$$\mathbf{F} = \begin{pmatrix} h_1 & h_1^q & \ldots & h_1^{q^{n-1}} \\ h_2 & h_2^q & \ldots & h_2^{q^{n-1}} \\ \vdots & \vdots & \ldots & \vdots \\ h_{N1} & h_{N1}^q & \ldots & h_{N1}^{q^{n-1}} \end{pmatrix};$$

$$\mathbf{G}_k = \begin{pmatrix} g_1 & g_1^q & \ldots & g_1^{q^{n-1}} \\ g_2 & g_2^q & \ldots & g_2^{q^{n-1}} \\ \vdots & \vdots & \ldots & \vdots \\ g_k & g_k^q & \ldots & g_k^{q^{n-1}} \end{pmatrix};$$

$N_1 + K = N$; h_i, g_i — элементы поля $GF(q^N)$, линейно независимые в совокупности над базовым полем $GF(q)$. Верхняя часть матрицы **Q** с элементами $h_j^{q^i}$ используется для определения метрики, а нижняя часть с элементами $g_j^{q^i}$ используется как порождающая матрица кода.

При шифровании открытого текста $\mathbf{a} = (a_1 \quad a_2 \quad \ldots \quad a_k)$ из k информационных символов кодовый вектор вычисляется следующим образом:

$$\mathbf{y} = \mathbf{a}\mathbf{G}_k.$$

Вектор **y** можно представить в виде

$$\mathbf{y} = \Big(a_1 g_1 + a_2 g_2 + \ldots + a_k g_k \quad \ldots \quad a_1 g_1^{q^{n-1}} + a_2 g_2^{q^{n-1}} + \ldots + a_k g_k^{q^{n-1}}\Big),$$

где число ненулевых коэффициентов a_i равно s. Пусть вектор **y** имеет в новой метрике норму, равную $N_F = m$. Тогда **y** можно представить в виде

$$\mathbf{y} = \Big(b_b h_1 + b_2 h_2 + \ldots + b_m h_m \quad \ldots \quad b_1 h_1^{q^{n-1}} + b_2 h_2^{q^{n-1}} + \ldots + b_m h_m^{q^{n-1}}\Big).$$

Из полученных представлений вектора **y** следует, что $s + m$ строк матрицы **Q** линейно зависимы. Учитывая, что s и m натуральные и $s + m > n$, то $s + m \geq n + 1$ или $N_F \geq n - s + 1$.

Минимальное расстояние линейного кода равно минимальному весу ненулевых кодовых слов, поэтому минимальное расстояние рассматриваемого кода не будет превосходить N_F. Так как $k > s$, то $d_F \geq n - k + 1$. Учитывая обобщенную границу Синглтона, можно записать равенство $d_F = n - k + 1$.

Для удобства рассмотрения алгоритма расшифрования шифротекст можно представить в виде суммы

$$\mathbf{c} = \mathbf{g} + \mathbf{e},$$

где $\mathbf{g} = (g_1 \quad g_2 \quad \ldots \quad g_{N1})$ — кодовый вектор, а $\mathbf{e} = (e_1 \quad e_2 \quad \ldots \quad e_{N1})$ — вектор ошибки.

Пусть норма строки ошибки в новой метрике равна t, тогда вектор **e** представляется в виде

$$\mathbf{e} = m_1 h_1 + m_2 h_2 + \ldots + m_{N_1} h_{N_1},$$

причем

$$d_H(\mathbf{m}) = t.$$

Очень важно, что для кодов, описанных выше, существуют быстрые алгоритмы декодирования. При расшифровании легальный пользователь умножает полученный шифротекст $(\mathbf{g} + \mathbf{e})\mathbf{S}$ на $\mathbf{S}^{-1}$. Затем применяет алгоритм быстрого декодирования в новой метрике. В результате пользователь получит векторы $\mathbf{g}$ и $\mathbf{e}$ по отдельности. После применения алгоритма быстрого декодирования ***родительского кода*** легальный пользователь получит вектор $\tilde{\mathbf{m}}$. Далее для получения открытого текста m остается умножить $\tilde{\mathbf{m}}$ на P^{-1}.

Криптоанализ новой модификации криптосистемы Нидеррайтера

После построения криптосистемы необходимо рассмотреть применимость к ней ранее известных атак. В случае, если атака применима, нужно вычислить ее трудоемкость и сравнить с трудоемкостью атак на криптосистемы, признанные мировым сообществом стойкими на данный момент. По результатам сравнения можно сделать вывод о стойкости самой криптосистемы.

Можно выделить два основных вида атак, применимых к рассматриваемой криптосистеме, — прямые и структурные. Под прямыми атаками понимаются перебор по искусственным ошибкам, перебор по сообщениям, декодирование опубликованного кода как случайного. Структурные атаки — это различные модификации атаки Гибсона, адаптированные к изменениям в криптосистеме, а также вариант атаки Сидельникова—Шестакова. При оценке трудоемкости каждой из атак необходимо учитывать размер открытого ключа.

Криптоанализ рассматриваемой криптосистемы можно свести к двум основным этапам:

1) нахождение вектора-ошибки, который необходим для исправления ошибки в новой метрике;

2) вычисление открытого текста по синдрому.

Что касается первого пункта, то для него необходимо выполнить ряд трудоемких операций. Второй этап менее ресурсоемкий и частично реализован на примере атаки Сидельникова—Шестакова, тем не менее, вторая часть атаки бессмысленна без прохождения первого этапа.

Декодирование случайного кода в ранговой метрике сводится к решению параметрической системы квадратных уравнений в базовом поле [7]. Подход к решению такой системы включает в себя перебор по некоторым переменным полученной системы.

Таким образом построена атака на модификацию криптосистемы Нидеррайтера, основанную на фробениусовской метрике [8]. Общая трудоемкость наиболее сложной части процесса декодирования составляет порядка $O((Nr)^3 q^{(r-1)(k+1)-2})$. Количество неизвестных в решаемой системе равно $(k + m + 1) + N(r - 1)$. Таким образом, чтобы система была разрешима, необходимо, чтобы $(k + m + 1) + N(r - 1) \le mN$. Например, для (24, 12)-кода над полем $GF(2^{12})$, который может исправлять ошибки ранга вплоть до 3, сложность декодирования составит 2^{52}.

Опираясь на результаты проведенного криптоанализа, можно выделить основные условия для параметров криптосистемы, основанной на матрице Фробениуса, так, чтобы она могла считаться стойкой. При выборе (48, 24)-кода над полем $GF(2^{16})$ размер открытого ключа будет составлять 1 Кбит, а вычислительная сложность приведенной атаки составит порядка 2^{140}. Из данного примера видно, что для ключа в 1 Кбит (сегодня такой размер ключа используется во многих стандартных асимметричных криптосистемах) количество операций рассматриваемой структурной атаки велико. Таким образом, структурные атаки, даже специально модифицированные под криптосистему, основанную на фробениусовской метрике, нельзя назвать успешными.

Применение новой криптосистемы в качестве системы совместного исправления ошибок и защиты от несанкционированного доступа

Рассмотрим применение предлагаемой модификации криптосистемы Нидеррайтера в качестве системы совместного исправления ошибок и защиты от несанкционированного доступа. За счет того, что в криптосистеме используются коды, которые успешно применяются в помехоустойчивом кодировании, система может быть использована и как система, исправляющая ошибки канала.

Предположим, что при передаче зашифрованного сообщения в криптосистеме возникают различного рода помехи, что приводит к искажению кодового слова. В случае, когда присутствует ошибка канала $\tilde{\mathbf{e}}$, совпадающая с одним из базисных векторов, она имеет в новой метрике норму, равную 1. Если искусственная ошибка $\mathbf{e}$ имеет норму $t = (d - 3)/2$, тогда система может исправлять также и ошибки канала.

Чтобы гарантировать коррекцию ошибок канала, необходимо наложить дополнительные ограничения на выбор матриц в модуле инициализации. Для исправления ошибок канала в любом случае мы должны иметь представление о характере ошибок. Необходимо собрать статистику и, предварительно проанализировав ее, сделать вывод о характере ошибок и модификации криптосистемы в целях их исправления. В базовом поле шифротекст представляет собой матрицу с элементами из $GF(q)$

$$\mathbf{C} = \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{N1} & \cdots & c_{Nn} \end{pmatrix}.$$

Элементы матрицы **C** имеют вид

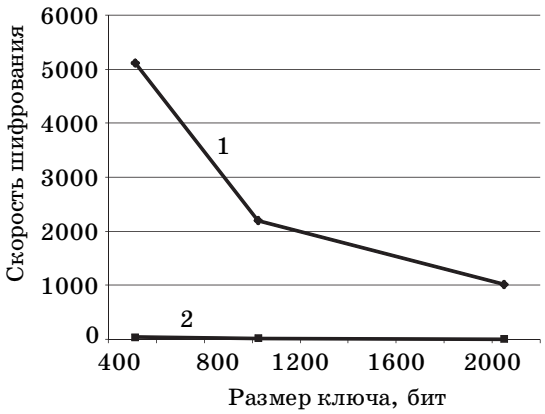
$$c_{ij} = \Big[s_{ij} \left(g_1 u_{1i} + \ldots + g_k u_{ki} + h_i \right) + \cdots + \\ + s_{jj} \left(g_1^{q^{j-1}} u_{1i} + \ldots + g_k^{q^{j-1}} u_{ki} + h_i^{q^{j-1}} \right) \Big] m_j.$$

Пусть приемник получил шифротекст, искаженный ошибкой, в виде $\mathbf{g} + \mathbf{e} + \tilde{\mathbf{e}}$. В таких случаях, для того чтобы гарантировать коррекцию ошибок канала, необходимо наложить дополнительные ограничения на выбор матрицы **Q**. В работе [9] подробно рассматриваются такие ограничения и их зависимость от вида ошибки канала. Дополнительные ограничения на выбор матрицы **Q** приводят к ухудшению криптосистемы с точки зрения ее криптостойкости, для увеличения стойкости системы в этом случае следует увеличивать размер ключа.

Применение криптосистемы для передачи и защиты меняющихся изображений

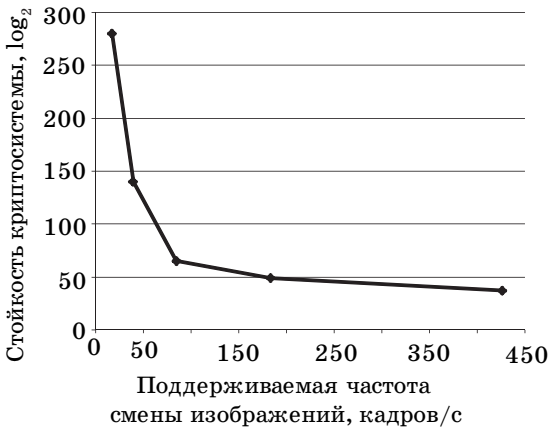
Новая модификация криптосистемы Нидеррайтера была предложена как часть новой системы с открытым ключом для передачи и защиты меняющихся изображений. При исследовании системы проводилось моделирование самой новой криптосистемы, системы сжатия видеоизображений и моделирование каналов с различного рода помехами. Автором данной статьи проводилось моделирование алгоритмов шифрования (и расшифрования) и согласование параметров системы в соответствии с существующими стандартами. Результаты исследования алгоритмов новой криптосистемы представлены на следующих графиках. На рис. 1 показана зависимость скорости шифрования от размера ключа криптосистемы для модифицированной системы Нидеррайтера, основанной на матрице Фробениуса, и криптосистемы RSA при размере ключа 512 бит в нешумящем канале. Из графика видно, что предлагаемая криптосистема оказывается быстрее, чем криптосистема RSA.

Значение поддерживаемой частоты для RSA в 2 раза ниже, чем аналогичное у предлагаемой новой криптосистемы. Такое сравнение не совсем корректно для шумящего канала, так как для использования RSA в шумящем канале необходимо производить кодирование с вероятностью ошибки в бите не более 10^{-8}. Это дополнительное ограничение на использование криптосистемы RSA, которое невозможно реализовать в случае канала с шумами, что приводит к дополнительным трудностям. Для их решения необходимы слишком ресурсоемкие затраты, такие как применение в дополнение к криптосистеме системы помехоустойчивого кодирования. В результате, кроме превосходства по скоростям, использование предлагаемой модификации криптосистемы Нидеррайтера не требует дополнительных затрат как для разработки программного комплекса, так и для увеличения вычислительных мощностей используемого аппаратного комплекса.

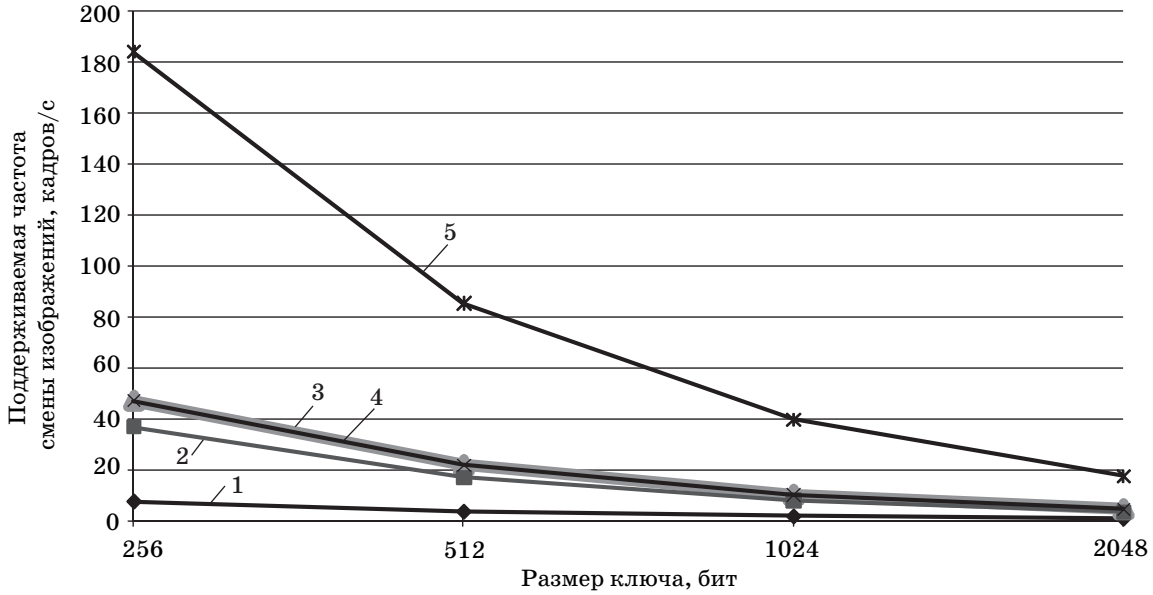


■ ***Рис. 1.*** *Зависимость скорости шифрования от размера ключа криптосистемы: 1 — модификация криптосистемы Нидеррайтера; 2 — RSA*

При различных параметрах криптосистемы ее стойкость будет варьироваться в зависимости от поддерживаемой частоты смены видеокадров. На рис. 2 представлен график такой зависимости в нешумящем канале при размере кадров, соответствующих возможностям сотового телефона SonyEricsson W900. Размер кадра при использовании современных методов сжатия составляет в среднем 12 Кбит (240 × 320 пикселей). Для ча-



■ ***Рис. 2.*** *Зависимость стойкости от поддерживаемой частоты смены кадров*



■ ***Рис. 3.*** *Зависимость частоты смены кадров от размера ключа: 1 — HDTV; 2 — видео стандартной четкости, SD; 3 — NTSC (National Television Standards Committee); 4 — сотовый телефон Nokia E66; 5 — сотовый телефон SonyEricsson W900*

стоты 25 кадров стойкость криптосистемы остается настолько высокой, что потери стойкости для исправления ошибок канала несущественны.

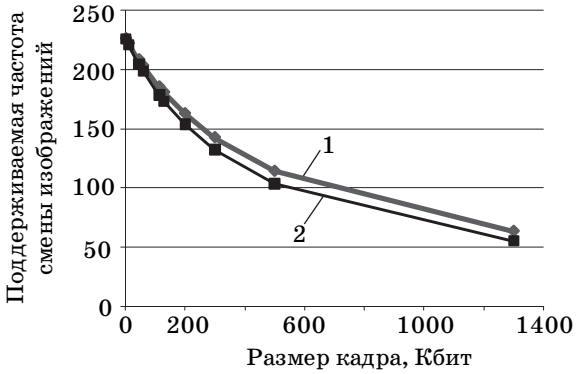
Далее рассмотрим результаты моделирования для размеров кадров, соответствующих различным стандартам. Графики зависимости поддерживаемой частоты смены кадров от размера ключа при различных размерах кадров при использовании модификации криптосистемы Нидеррайтера представлены на рис. 3.

Приведены средние значения размеров кадров для рассматриваемых стандартов и часто применяемых устройств, пиксель:

HDTV	1920 × 1080
Видео стандартной четкости, SD	720 × 576
NTSC	648 × 486
Сотовый телефон Nokia E66	640 × 480
Сотовый телефон SonyEricsson W990	240 × 320

В случае передачи видеоизображения повышенного качества HDTV частота смены изображений, поддерживаемой системой, заметно сокращается. Однако для видео стандартной четкости SD соответствующая этому стандарту частота в 25 кадров поддерживается и для канала с шумом.

Скорость шифрования в системе можно заметно увеличить, осуществляя шифрование изображения с помощью более производительных симметричных алгоритмов, а шифрование сеансового ключа осуществлять уже при помощи предлагаемой системы. Но такая модификация может быть применена только для случая канала без шума.



■ ***Рис. 4.*** *Зависимость частоты смены кадров от размера кадра: 1 — AES, теоретически возможный предел; 2 — AES*

Например, при использовании в качестве симметричного алгоритма AES или ГОСТ 28147–89 при выборе соответствующих параметров асимметричной криптосистемы можно уже гарантировать передачу изображения в формате стандарта HDTV.

Графики зависимости поддерживаемой частоты смены кадров от размера кадров при использовании симметричного алгоритма AES256 и новой модификации криптосистемы Нидеррайтера представлены на рис. 4. Размер сеансового ключа составляет 256 бит, размер открытого ключа системы — 512 бит.

Из графика видно, что даже при стандартной реализации AES без ускорений (линия *2*), поддерживаемая частота смены изображений возрастает в 10 раз.

Литература

1. **McElice R. J.** A Public Key Cryptosystem Based on Algebraic Coding Theory // DSN Progress Report 42-44. Pasadena, CA: Jet Propulsion Lab, 1978. P. 114–116.
2. **Niederreiter H.** Knapsack-Type Cryptosystem and Algebraic Coding Theory // Problem Control and Information Theory. 1986. Vol. 15. P. 19–34.
3. **Сидельников В. М., Шестаков С. О.** О системе шифрования, основанной на обобщенных кодах Рида—Соломона // Дискретная математика. 1992. Т. 3. Вып. 3.
4. **Gabidulin E., Ourivski A., Pavlouchkov V.** On the modified Niederreiter cryptosystem // Information Theory and Networking Workshop. Metsovo, Greece, 1999. P. 50.
5. **Габидулин Э. М., Обернихин В. А.** Коды в F-метрике Вандермонда и их применение. Долгопрудный: МФТИ, 2005.
6. **Габидулин Э. М.** Теория кодов с максимальным ранговым расстоянием // Проблемы передачи информации. Т. XXI. Вып. 1. 1985.
7. **Уривский А. В., Йоханссон Т.** Новые способы декодирования кодов в ранговой метрике и их криптографические приложения // Проблемы передачи информации. 2002. Т. 38. Вып. 3. С. 83–93.
8. **Самохина М. А.** Криптоанализ систем, основанных на линейных кодах // Проблемы информационной безопасности. Компьютерные системы. 2008. Вып. 2. С. 94–103.
9. **Самохина М. А.** Применение модификаций криптосистем Нидеррайтера в системах исправления ошибок и защиты от несанкционированного доступа // Моделирование и обработка информации: Сб. науч. тр. 2008. С. 127–136.

УВАЖАЕМЫЕ АВТОРЫ ЖУРНАЛА

При подготовке рукописей статей редакция просит Вас руководствоваться следующими рекомендациями.

Объем статьи (текст, таблицы, иллюстрации и библиография) не должен превышать эквивалента в 16 страниц, напечатанных на бумаге формата А4 на одной стороне через 1,5 интервала в Word шрифтом Times New Roman размером 13.

Обязательными элементами оформления статьи являются: индекс УДК, инициалы и фамилия автора (авторов), ученая степень, звание, полное название организации; заглавие, аннотация (5–7 строк) и ключевые слова на русском и английском языках.

Формулы набирайте в Word, при необходимости можно использовать формульный редактор; для набора одной формулы не используйте два редактора; при наборе формул в формульном редакторе знаки препинания, ограничивающие формулу, набирайте вместе с формулой; для установки размера шрифта никогда не пользуйтесь вкладкой Other..., используйте вкладку Define; в формулах не отделяйте пробелами знаки: + = –.

При наборе символов в тексте помните, что символы, обозначаемые латинскими буквами, набираются светлым курсивом, русскими и греческими — светлым прямым, векторы и матрицы — прямым полужирным шрифтом.

Иллюстрации в текст не заверстываются и предоставляются отдельными исходными файлами, поддающимися редактированию:

— рисунки, графики, диаграммы, блок-схемы изготавливаются в векторных программах: Visio 4, 5, 2002–2003 (*.vsd); Coreldraw (*.cdr); Excel; Word; AdobeIllustrator; AutoCad (*.dxf); Компас; Matlab (экспорт в формат *.ai);

— фото и растровые — в формате *.tif, *.png с максимальным разрешением (не менее 300 pixels/inch).

Наличие подрисуночных подписей обязательно (желательно не повторяющих дословно комментарии к рисункам в тексте статьи).

В редакцию предоставляются:

— сведения об авторе (фамилия, имя, отчество, место работы, должность, ученое звание, учебное заведение и год его окончания, ученая степень и год защиты диссертации, область научных интересов, количество научных публикаций, домашний и служебный адреса и телефоны, факс, e-mail), фото авторов: анфас, в темной одежде на белом фоне, должны быть видны плечи и грудь, высокая степень четкости изображения без теней и отблесков на лице, фото можно представить в электронном виде в формате *.tif, *.png с максимальным разрешением — не менее 300 pixels/inch при минимальном размере фото 40 × 55 мм;

— экспертное заключение.

Список литературы составляется по порядку ссылок в тексте и оформляется следующим образом:

— для книг и сборников — фамилия и инициалы авторов, полное название книги (сборника), город, издательство, год, общее количество страниц;

— для журнальных статей — фамилия и инициалы авторов, полное название статьи, название журнала, год издания, номер журнала, номера страниц;

— ссылки на иностранную литературу следует давать на языке оригинала без сокращений;

— при использовании web-материалов указывайте адрес сайта.

УДК 681.883.022: 681.883.65

ВЫБОР ТИПА ЗОНДИРУЮЩЕГО СИГНАЛА ДЛЯ АКТИВНОГО ГИДРОЛОКАТОРА С ПОМОЩЬЮ ТЕОРИИ ПЕРЕДАЧИ ДАННЫХ В КАНАЛАХ СВЯЗИ

Н. Н. Семенов,
соискатель
Б. П. Белов,
доктор техн. наук, профессор
Санкт-Петербургский государственный морской технический университет

В современной гидролокации не существует однозначного решения, какой тип сигнала посылки является для данной системы оптимальным. Это связано с тем, что водная среда насыщена специфическими шумами, является неоднородной, допускает многолучевое распространение и отражение от дна и поверхности. В статье рассматривается один из возможных алгоритмов выбора оптимального для определенной задачи типа сигнала посылки.

Ключевые слова *— гидролокатор, эхо-сигнал, сигнал посылки, обнаружение, локация, сравнение сигналов, модуляция, шумы, информативность.*

Введение

Существует большое количество работ по гидроакустике и радиолокации, где расписаны различные сигналы посылки, которые могут использоваться при построении гидролокатора [1–9]. Но среди этих книг и статей нет единого алгоритма выбора подходящего сигнала для конкретной задачи. Предлагается один из возможных алгоритмов, опирающийся на уравнения Шеннона и Котельникова для передачи информации в зашумленном канале, которым и является водная среда. Чем больше информации будет содержаться в сигнале посылки, тем больше информации об объекте локации можно будет выделить из эхо-сигнала.

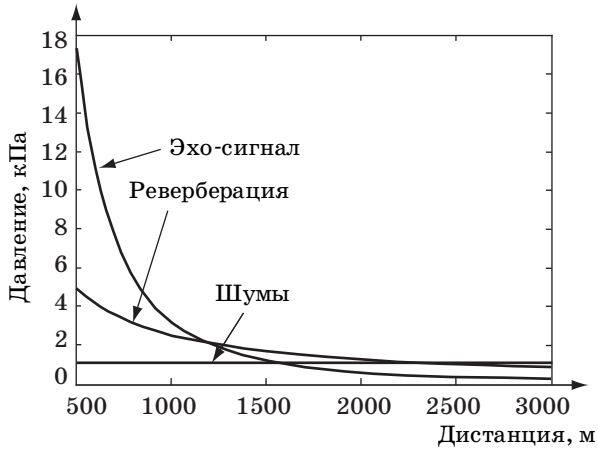
Модель сигнала и шума

Основной характеристикой гидролокаторов является дальность обнаружения, которая зависит от мощности излучаемого сигнала, уровня акустических помех и условий распространения звука в водной среде. Дальность обнаружения обычно определяют по величине порогового эхо-сигнала, т. е. эхо-сигнала минимальной интенсивности, различимого на фоне помех [1, 9].

Гидроакустическая антенна (ГА), погруженная на заданную глубину и имеющая определенный геометрический размер, может создавать акустическое давление не более некоторого критического значения, выше которого начинается кавитация [10]. Поэтому основное ограничение на излучаемый сигнал — максимальное акустическое давление. Вторым ограничением является ширина полосы частот, которые без искажений передаются и принимаются гидролокатором. Как известно, максимальную чувствительность ГА имеет вблизи частоты механического резонанса, и увеличить ширину области максимальной чувствительности можно только снижением добротности колебательного контура, т. е. снижая его чувствительность [10].

Если помеха и сигнал независимы, то пороговый сигнал определяется отношением полной энергии полезного сигнала к мощности помехи в данном частотном интервале. Таким образом, дальность обнаружения в условиях случайных помех для систем с различными видами модуляции будет одинаковой, если одинакова их полная энергия излучаемых сигналов [8].

Если основная помеха — хаотическое отражение сигнала от неоднородностей среды (так называемая реверберационная помеха), то относительный пороговый сигнал обнаружителя не зависит от мощности излучаемого сигнала, а определяется исключительно шириной полосы его частот.



■ ***Рис. 1.*** *Соотношение мощностей эхо-сигнала и шумов*

Мощности сигнала и реверберационной помехи связаны между собой, и в этом случае более эффективны системы с частотной или фазовой модуляцией сигнала и с шумовой посылкой [10].

График зависимости соотношения мощностей полезного эхо-сигнала и различных шумов показан на рис. 1. Здесь хорошо видны три зоны: ближняя (когда мощность эхо-сигнала выше любой помехи), средняя (когда мощность эхо-сигнала оказывается меньше реверберационной помехи) и дальняя (мощность эхо-сигнала меньше и реверберационной помехи, и естественных шумов моря) [10].

Но наряду с самим фактом обнаружения сигнала в гидролокации появляется дополнительный набор требований по точности определения дистанции, различению эхо-сигналов от рядом стоящих объектов и определению параметров движения этих объектов (наличия доплеровского смещения частоты эхо-сигнала).

Простые и сложные сигналы

Для описания «сложности» сигнала существует понятие «база сигнала» [6]

$$B = W_e T_e, \qquad (1)$$

где W_e — ширина полосы частот, используемых сигналом; T_e — длительность посылки.

Эффективная полоса сигнала W_e определяется следующим способом [1]:

$$W_e = \frac{\left[\int\limits_{-\infty}^{\infty} (U(\omega))^2 \mathrm{d}\omega\right]^2}{4\pi \int\limits_{-\infty}^{\infty} (U(\omega))^4 \mathrm{d}\omega}, \qquad (2)$$

где $U(\omega)$ — спектральное представление сигнала посылки.

Это позволяет представить постоянную разрешения по запаздыванию (а следовательно, и по дальности) в виде [1]

$$\delta t = 1/(2W_e). \qquad (3)$$

Таким образом, если желательно иметь одну величину, наилучшим образом характеризующую способность сигнала по дальности, то такой величиной будет эффективная полоса сигнала. [Заметим, что длительность сигнала не входит в явной форме в выражение (3) для разрешающей способности по дальности].

А разрешающую способность по доплеровской частоте можно записать как [1]

$$\delta f = 1/(2T_e), \qquad (4)$$

где T_e — эффективная длительность, определяемая как

$$T_e = \frac{\left[\int\limits_{-\infty}^{\infty} |u(t)|^2 \mathrm{d}t\right]^2}{\int\limits_{-\infty}^{\infty} |u(t)|^4 \mathrm{d}t}, \qquad (5)$$

где $u(t)$ — сигнал посылки.

То есть разрешающая способность по доплеровской частоте зависит только от длительности сигнала и в общем случае никак не зависит от эффективной полосы частот сигнала, что видно из (4).

Если в выражение (1) подставить выражения длительности и ширины полосы сигнала посылки через точность определения дистанции и смещения частоты, получится выражение [11]

$$B = T_e W_e = \frac{1}{2\delta f}\frac{1}{2\delta t} = \frac{1}{4\delta f \delta t}. \qquad (6)$$

Из (6) видно, что чем больше база сигнала, тем выше точность определения дистанции и смещения частоты эхо-сигнала.

Простые сигналы — отрезок синусоиды (длительностью T и шириной полосы $1/T$) и короткий импульс, имитирующий математическую дельта-функцию (бесконечно малой длительности и широкой полосы) [12]. База таких сигналов близка или равна 1. Простые сигналы позволяют с высокой точностью определять либо дистанцию, либо частоту, но не оба параметра одновременно.

Следовательно, для получения максимального количества информации об объекте локации по одному эхо-сигналу необходимо использовать сложные сигналы, т. е. сигналы, база которых много больше 1. Согласно [10], при использовании сигналов с базой больше 100 по причине многолучевого распространения, неоднородности водной среды и подвижности объекта локации возможны проблемы с когерентным приемом, необходимым для получения максимального соотношения сиг-

нал/шум на выходе согласованного фильтра. Использование ГЧМ-сигнала (с гиперболической частотной модуляцией) позволяет применять теоретически сигнал любой сложности, но только за счет инвариантности к сдвигу частоты. Поэтому такой сигнал для гидролокатора в данной статье не рассматривался. Частично-когерентный прием тоже теоретически позволяет использовать сигнал любой сложности, но для малогабаритного гидролокатора с ограничением на эффективную полосу сигнала увеличение сложности может привести к увеличению длительности посылки, что увеличит размер «мертвой зоны» вокруг гидролокатора и при этом практически не даст выигрыша по точности определения частоты.

Следовательно, необходимо остановиться на когерентном приеме сложного сигнала и принять сложность сигнала равной 100.

Анализ помехоустойчивости и спектрально-энергетической эффективности гидролокатора

Рассмотрим один из подходов к решению задачи выбора вида манипуляции, заимствованный из теории передачи информации. Результатом данного подхода может быть установление компромиссного варианта, т. е. типа сигнала, соединяющего в себе физическую реализуемость, энергетическую эффективность излучения и высокую точность определения обоих параметров локации (дистанции и частоты). Воспользуемся диаграммами, изображенными на рис. 2 и 3 [8].

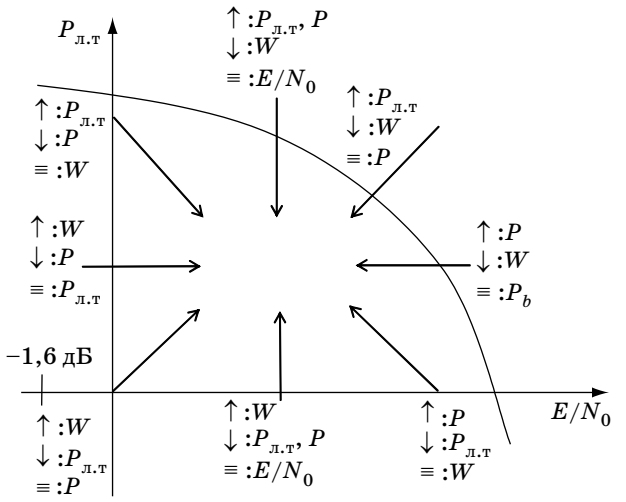
Рис. 2 представляет собой семейство кривых помехоустойчивости, т. е. зависимостей вероятности ошибки ложного обнаружения (или ложной тревоги) $P_{л.т}$ от отношения энергии E, затрачиваемой на передачу, к спектральной плотности шума N_0 (отношение сигнал/помеха — ОСП); рис. 3 — диаграмму спектрально-энергетической эффективности, т. е. семейство зависимостей удельной скорости передаваемой информации R_b/W от E/N_0 (ОСП).

Направления стрелок и соответствующие метки указывают общий эффект от перемещения рабочей точки по направлению, указанному стрелкой, при соответствующем выборе вида модуляции. Взаимному размену подлежат параметры $P_{л.т}$, R_b/W (удельная скорость передачи информации в полосе W), P (мощность сигнала).

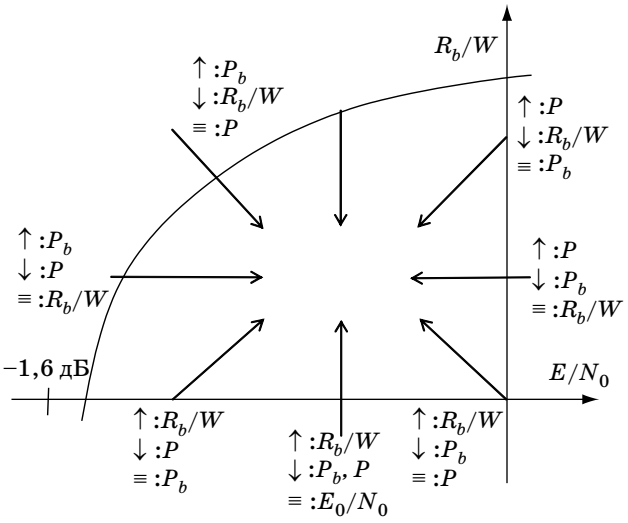
С точки зрения гидролокации, R_b является параметром разрешения эхо-сигналов по дистанции, т. е.

$$R_b = 1/T_b = c/\Delta r,$$

где T_b — время передачи одной дискреты модуляции, если модуляция дискретная, или $T_b = 1/W_e$, если модуляция непрерывная; c — скорость звука в воде; Δr — разрешение по дистанции.



■ ***Рис. 2.*** *Помехоустойчивость сигнала (зависимость вероятности ошибки ложного срабатывания $P_{л.т}$ от ОСП): ↑ — улучшение; ↓ — ухудшение; ≡ — неизменность*



■ ***Рис. 3.*** *Спектрально-энергетическая эффективность сигнала (зависимость разрешающей способности от ОСП): ↑ — улучшение; ↓ — ухудшение; ≡ — неизменность*

На диаграммах указано минимальное значение удельных энергетических затрат, равное −1,6 дБ и определяемое из формулы Шеннона для пропускной способности абстрактного канала связи с ограниченной полосой W, средней мощностью посылки P и помехой в виде аддитивного белого гауссова шума.

На диаграмме спектрально-энергетической эффективности (см. рис. 3) построена предельная кривая, определяемая выражением

$$\frac{E}{N_0} = \frac{2^{R_b/W} - 1}{R_b / W}. \qquad (7)$$

Это выражение следует из формулы Шеннона при подстановке $C = R_b$. Тогда для идеального вида модуляции рост энергетических затрат при увеличении спектральной эффективности происходит по экспоненциальному закону. Минимально возможное значение удельных энергетических затрат определяется путем вычисления предела:

$$\left(\frac{E}{N_0}\right)_{\min} = \lim_{R_b/W \to 0} \frac{2^{R_b/W} - 1}{R_b / W} = \ln 2 = -1{,}6 \text{ дБ}. \qquad (8)$$

Двигаясь к пределу Шеннона на рис. 2, можно обеспечить снижение вероятности ошибки $P_{\text{л.т}}$ или удельных энергетических затрат за счет расширения полосы. Напротив, двигаясь к пределу Шеннона на рис. 3, можно повысить спектральную эффективность за счет увеличения удельных энергетических затрат или вероятности ошибки ложного обнаружения $P_{\text{л.т}}$. Поскольку обычно бывает заданным значение $P_{\text{л.т}}$, то наибольший интерес представляют собой стрелки, отмеченные как (≡: $P_{\text{л.т}}$) — по две на рис. 2 и 3. Эти рисунки, иллюстрирующие возможность взаимного размена различных показателей вида модуляции, лишь качественно демонстрируют основные закономерности, проявляющиеся при подобном размене. Для получения более точных данных необходим детальный анализ.

Результаты моделирования

Для сравнения различных видов модуляции примем следующие ограничения, характерные для реально существующей ГА:

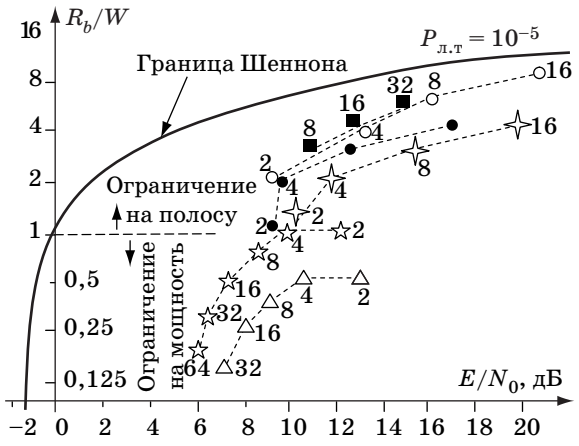
1) частота несущей 20 кГц;

2) ширина полосы частот не более 10 % (2 кГц);

3) максимально допустимое акустическое давление излучателя (максимальная амплитуда сигнала) 10^5 Па, ограничивающее энергию сигнала посылки.

Построенные с учетом ограничений сигналы смешивались с равномерным шумом, ограниченным полосой работы гидролокатора (для имитации работы приемного тракта гидролокатора), и затем подавались на согласованный фильтр.

Результаты подобного сравнения представлены на рис. 4. Здесь предполагается заданным значение вероятности ложного обнаружения $P_{\text{л.т}} = 10^{-5}$. Вероятность ложного обнаружения использовалась при выставлении порога обнаружения сигнала на выходе согласованного фильтра. ОСП вычислялось через энергию одной дискреты модулированного сигнала. Цифры 2, 4, 8, 16 и 32



■ ***Рис. 4.*** *Сравнение различных видов модуляции*: ○ — *АМ-ОБП*; ● — *ФМ* (*когерентная*); ■ — *АМ-ФМ*; ✧ — *ОФМ*; ☆ — *МЧМ*; △ — *ЧМ* (*некогерентная*)

на графиках показывают количество возможных позиций кода в каждой дискрете посылки. Для каждой точки графика было проведено не менее 32 испытаний, позволяющих определить ОСП, при котором сигнал с заданным R_b/W принимается с вероятностью $P_{\text{л.т}}$. Цифра 32 была получена эмпирически, так как при меньших значениях результат имеет большой разброс значений, а при больших значениях результат меняется не более чем на 2–3 %.

Шумоподобные полосовые сигналы имеют низкую энергетическую эффективность (при ограничении на максимальное давление излучателя) в сравнении с модулированными гармоническими сигналами, и поэтому их использование в качестве зондирующего сигнала для малогабаритного гидролокатора не рассматривается.

Из приведенных на рис. 4 данных следует, что АМ (амплитудная модуляция), ФМ (фазовая манипуляция) и ОФМ (относительная фазовая манипуляция) являются спектрально-эффективными видами модуляции, поскольку соответствующие точки располагаются выше разграничительной линии $R_b/W = 1$. Часть диаграммы, расположенная выше этой линии, соответствует ситуации, когда основное ограничение приходится на имеющуюся полосу частот. Поэтому увеличение спектральной эффективности может быть достигнуто за счет увеличения числа позиций модуляции M. При заданной $P_{\text{л.т}}$ побочным эффектом является увеличение удельных энергетических затрат.

С другой стороны, при ЧМ (частотной модуляции) неэффективно используется имеющаяся полоса, поскольку соответствующие ей точки располагаются ниже разграничительной линии $R_b/W = 1$. Для данного вида модуляции характер-

ны повышенные значения показателя энергетической эффективности.

Многопозиционная частотная модуляция (МЧМ) эффективнее ЧМ, как видно из рис. 4, но ее имеет смысл использовать только в системах с основным ограничением на максимальную мощность.

Следует отметить различный характер размена показателей спектральной и энергетической эффективности в областях, лежащих выше и ниже разграничительной линии. В соответствии с формой предельной кривой Шеннона в области, лежащей выше разграничительной линии, этот размен носит плавный характер. Поэтому за увеличение спектральной эффективности (точности определения дистанции) приходится расплачиваться существенным снижением энергетической эффективности. Напротив, в области, лежащей ниже разграничительной линии, небольшие потери энергетической эффективности приводят к заметному увеличению спектральной эффективности.

Из приведенных данных следует, что АМ-ОБП (амплитудная модуляция с одной боковой полосой) является асимптотически оптимальным видом модуляции для области диаграммы, характеризующейся ограничением на частотный ресурс системы. Ортогональная модуляция в сочетании с когерентной демодуляцией является асимптотически оптимальным видом модуляции для области диаграммы, характеризующейся ограничением на энергетический ресурс системы.

Выводы

В заключение необходимо сделать ряд замечаний практического характера, которые подтверждаются данными моделирования, приведенными на диаграмме спектрально-энергетической эффективности. Если прием и излучение сигнала ограничены по полосе частот, определяемой ГА, то в таких системах целесообразно использовать многопозиционные сигналы с АМ (амплитудной модуляцией), ФМ (фазовой манипуляцией) или АМ-ФМ (амплитудно-фазовой модуляцией) в сочетании с когерентной демодуляцией. Примечательна точка, характеризующая 8-позиционную АМ-ФМ, поскольку этот вид модуляции имеет заметные преимущества перед 8-позиционной ФМ. Что касается 8-позиционной ФМ и многопозиционной АМ-ОБП, то они обладают примерно одинаковыми характеристиками размена показателей спектральной и энергетической эффективности. Однако наибольший эффект использования полосы в случае АМ-ОБП достигается за счет увеличения удельных энергетических затрат. АМ-ОБП при $M = 2$ и ФМ при $M = 4$ имеют одинаковые и достаточно высокие показатели (поскольку сигналы имеют одинаковую форму).

Таким образом, наилучшие показатели соотношения информативности и энергетической эффективности для малогабаритного гидролокатора имеют ФМ-сигналы с небольшим (не больше четырех) числом состояний (ФМ-2, ФМ-4).

Литература

1. **Берковиц Р.** Современная радиолокация. М.: Сов. радио, 1969. 570 с.
2. **Витерби Э. Д.** Принципы когерентной связи. М.: Сов. радио, 1970. 392 с.
3. **Котельников В. А.** Теория потенциальной помехоустойчивости / ГЭИ. М., 1956. 151 с.
4. **Фалькович С. Е.** Оценка параметров сигнала. М.: Сов. радио, 1970. 336 с.
5. **Куликов Е. И., Трифонов А. П.** Оценка параметров сигналов на фоне помех. М.: Сов. радио, 1978. 242 с.
6. **Вайнштейн Л. А., Зубаков В. Д.** Выделение сигналов на фоне случайных помех. М.: Сов. радио, 1960. 448 с.
7. **Быховский М. А.** Потенциальная помехоустойчивость разделения двух сигналов с ЧМ. М.: Электросвязь, 1979. 277 с.
8. **Амиантов И. Н.** Избранные вопросы статистической теории связи. М.: Сов. радио, 1971. 416 с.
9. **Бакут П. А. и др.** Вопросы статистической теории радиолокации: В 2 т. / Под ред. Г. П. Тартаковского. М.: Сов. радио, 1963–1964.
10. **Евтютов А. П., Митько В. Б.** Инженерные расчеты в гидроакустике. Л.: Судостроение, 1988. 520 с.
11. **Амиантов И. Н.** Применение теории решений к задачам обнаружения сигналов и выделения сигналов из шумов / ВВИА им. Жуковского. М., 1958. 578 с.
12. **Тихонов В. И.** Оптимальный прием сигналов. М.: Радио и связь, 1972. 320 с.

УДК 303.732:[338+658.01](075.8)

МЕТОД МНОГОКРИТЕРИАЛЬНОГО ПРЕДПОЧТЕНИЯ СЛОЖНЫХ СИСТЕМ

Ю. В. Ведерников,
канд. техн. наук, доцент
Михайловская военная артиллерийская академия

Рассматривается задача определения отношений предпочтения на множестве сложных технических систем для случая, когда критерии оптимальности разнородны и могут быть заданы в частично формализованном, интервальном виде. Задача сводится к построению упорядоченного множества эффективных вариантов (кортежа предпочтений Парето) сложных систем. Предлагается метод решения, основанный на комплексном применении аксиоматических методов теории принятия решений, нечетких множеств и интервального анализа. Приведен численный пример.

Ключевые слова *— техническая система, отношение предпочтения, интервальный анализ, векторная оптимизация.*

Введение

В настоящий момент осложненные условия эксплуатации современных технических систем (СТС) различного назначения приводят в процессе оценки качества их функционирования к необходимости учета различных видов неопределенности. При этом достаточно часто большинство показателей рассматриваемых СТС оказываются заданными в виде диапазона их изменения. Для нахождения решений в задачах подобного класса используют интервальные [1–7] и нечеткие [2, 8–10] методы.

Приоритет в исследованиях, посвященных интервальному анализу, принадлежит академику Л. В. Канторовичу [11], идеи которого применительно к задачам оптимизации развил А. А. Ватолин. Он сформулировал для них определение множества решений. Математическим и вычислительным аспектам анализа статических систем в условиях интервальной неопределенности посвящена работа С. П. Шарыя [5]. Разработка методов оптимизации СТС для случая, когда критерии оптимальности заданы в интервальном виде, оказалась возможной благодаря результатам, полученным в теории интервального анализа такими учеными как Е. Каухер, Ю. Херцберг, Ю. И. Шокин и многими другими [1, 4, 6, 12, 17]. Вместе с тем эта проблема полностью еще не решена. Известные методы [4, 6] предполагают, что для двух интервалов A и B, определенных в соответствующих границах $A = [\underline{a}; a]$ и $B = [\underline{b}; b]$, считается, что $A > B$ (или $A < B$), если $\underline{a} > \underline{b}$, $a > b$ (или $\underline{a} < \underline{b}$, $a < b$). При условии $\underline{a} < \underline{b}$, $a > b$ (или $\underline{a} > \underline{b}$, $a < b$) два интервала A и B будут считаться несравнимыми. В частности, это относится и к важному для практики случаю, когда СТС характеризуется векторным разнородным критерием оптимальности. Кроме того, для нестандартных операций вычитания «–» и деления «:», определенных для элементов A, B, существует правило [4], что из равенства $A - C = B - C$ не следует, что $A = B$, например: $[\underline{9}; 13] - [\underline{1}; 4] = [\underline{10}; 12] - [\underline{1}; 4]$, или из равенства $A : C = B : C$ не следует, что $A = B$, например: $[\underline{2}; 6]:[\underline{1}; 2] = [\underline{3}; 4]:[\underline{1}; 2]$. Однако именно вышеперечисленные случаи достаточно часто встречаются при решении практических задач.

В статье предлагается метод, позволяющий определять предпочтения между вариантами систем, характеризующихся множеством интервальных характеристик. Он основан на сочетании отличительных свойств аксиоматических методов теории принятия решений, нечетких множеств и интервального анализа.

Постановка задачи

В основу предлагаемого метода положена идея сравнения неоднородных интервальных критериальных значений на основе построения интервального отношения предпочтения (ИОП). Рассмотрим его сущность и для этого введем необходимые в дальнейшем обозначения [13–15]:

$S = \{S_\alpha, \alpha = \overline{1,n}\}$ — множество возможных альтернативных вариантов структурного построения СТС;

$K_i(S_\alpha) = [\underline{K_i(S_\alpha)};\ \overline{K_i(S_\alpha)}]$ — частные критерии оптимальности, заданные в интервальном виде, характеризующие каждый отдельный вариант системы S_α, где $\underline{K_i(S_\alpha)}$ — нижняя граница интервала критериальной оценки, а $\overline{K_i(S_\alpha)}$ — верхняя граница интервала, $i = \overline{1,r}$; $\alpha = \overline{1,n}$;

$K(S_\alpha) = \{K_1(S_\alpha), K_2(S_\alpha), ..., K_r(S_\alpha)\} = \{[\underline{K_1(S_\alpha)};\ \overline{K_1(S_\alpha)}], [\underline{K_2(S_\alpha)};\ \overline{K_2(S_\alpha)}], ..., [\underline{K_r(S_\alpha)};\ \overline{K_r(S_\alpha)}]\}$ — векторный критерий, характеризующий каждый вариант системы;

$S^P \subset S$ — множество эффективных (парето-оптимальных) вариантов системы S_α с числом элементов n^P;

$P = (S^0_{k_1}, S^0_{k_2}, ..., S^0_{k_{n^P}})$ – упорядоченное множество эффективных вариантов (кортеж Парето), для элементов $S^0_{k_j} \in S^P$ которого справедливо

$$S^0_{k_1} \succ S^0_{k_2} \succ ... \succ S^0_{k_{n^P}}, \tag{1}$$

где «$\succ$» — знак отношения доминирования, $k_j \in \{\overline{1, n^P}\}$. Длина кортежа равна n^P.

С учетом введенных обозначений сформулируем задачу.

Требуется найти упорядоченное множество эффективных вариантов структурного построения сложной системы (кортеж Парето) (1), для элементов $S^0_{k_j}$ которого в зависимости от смысла задачи выполняются условия

$$K_i(S^0_{k_j}) = \min_{i=1,r;\ \alpha=1,n} [K_i(S_\alpha)],\ S^0_{k_j} \in S^P, \tag{2}$$

или

$$K_i(S^0_{k_j}) = \max_{i=1,r;\ \alpha=1,n} [K_i(S_\alpha)],\ S^0_{k_j} \in S^P \tag{3}$$

для случая, когда скалярные критерии оптимальности $K_i(S_\alpha) = [\underline{K_i(S_\alpha)};\ \overline{K_i(S_\alpha)}]$ представлены в интервальном виде. Обычный (не интервальный) скалярный критерий $K_i(S_\alpha)$ целесообразно рассматривать как частный случай интервального критерия, который представлен в виде *вырожденного интервала* [2], т. е. интервала с совпадающими концами $K_i(S_\alpha) = \underline{K_i(S_\alpha)} = \overline{K_i(S_\alpha)}$.

Метод построения интервальных отношений предпочтения на множестве сложных систем, характеризующихся скалярными разнородными критериями оптимальности

При построении реальных СТС различного назначения встречаются ситуации (являющиеся, скорее, правилом, чем исключением), когда у лица, принимающего решение, нет четкого представления о предпочтениях между всеми или некоторыми из альтернативных вариантов [10]. Кроме того, только при наличии условия, *обеспечивающего сравнимость частных критериев*, возможно в дальнейшем построение принципа оптимальности и вытекающих из него алгоритмов решения многокритериальных задач. Несравнимость частных критериев является основной особенностью и главным препятствием к решению задач многокритериальной оптимизации [8]. Представленные обстоятельства существенно усиливаются в условиях, когда частные критерии не только неаддитивные, но еще и представлены в интервальном виде, с различными диапазонами отклонения качества от лучшего до худшего значения.

Исходя из перечисленного выше предлагается на основе анализа множества упорядоченных пар S_k и S_l ($S_k \in S$ и $S_l \in S$, где $k = \overline{1,n}; l = \overline{1,n}; k \neq l$) вариантов сложной системы $S = \{S_\alpha, \alpha = \overline{1,n}\}$ по аналогии с нечетким отношением предпочтения [10, п. 1.2.1] ввести ***интервальное отношение предпочтения*** $R^u K_i(S_k,\ S_l)$ по i-му частному интервальному критерию оптимальности $K_i(S_\alpha) = [\underline{K_i(S_\alpha)};\ \overline{K_i(S_\alpha)}]$, $i = \overline{1,r}; \alpha = \overline{1,n}$ и для пары систем (S_k, S_l) определить интервальной функцией принадлежности $\mu^u K_i(S_k,\ S_l)$. Результаты анализа предлагается заносить в специальную оценочную матрицу $\|\mu^u K_i(S_k,\ S_l)\|$. При сравнении систем S_k и S_l k-системы располагать в строках, а l-системы — в столбцах.

Элементы $\mu^u K_i(S_k,\ S_l)$ оценочной матрицы, исходя из подходов, изложенных в работах [4, 8, 10, 14], определяются по выражению

$$\mu^u K_i(S_k, S_l) = \frac{K_i(S_k) - K_i(S_l)}{m_i} = \frac{[\underline{K_i(S_k)};\ \overline{K_i(S_k)}] - [\underline{K_i(S_l)}; \overline{K_i(S_l)}]}{m_i} =$$

$$= \frac{[\min\{\underline{K_i(S_k)} - \underline{K_i(S_l)}; \overline{K_i(S_k)} - \overline{K_i(S_l)}\};\ \max\{\underline{K_i(S_k)} - \underline{K_i(S_l)}; \overline{K_i(S_k)} - \overline{K_i(S_l)}\}]}{m_i}, \tag{4}$$

где $K_i(S_k)$ и $K_i(S_l)$ — значения i-го скалярного критерия для систем S_k и S_l; m_i — ширина интервала оценок по i-му частному критерию оптимальности [2]. Средством числового представления критериев высту-

пают интервальные значения, которые показывают допустимое отклонение качества варианта системы от худшего до лучшего (т. е. от минимального до максимального) в определенном диапазоне.

Важным моментом в данном случае является назначение величины m_i. При необходимости можно использовать в качестве m_i: предельно допустимые значения критериев оптимальности эталонной системы; предельно допустимые значения критериев оптимальности, которые хотелось бы достигнуть в ходе решения задачи оптимизации; в задачах контроля — предельно допустимые значения контролируемых параметров и т. д.

В результате функция принадлежности $\mu^u K_i(S_k, S_l)$ для пары систем (S_k, S_l), характеризующая степень согласия с тем, что система S_k доминирует над системой S_l по i-му частному интервальному критерию, будет также представлена в интервальном виде:

$$\mu^u K_i(S_k, S_l) = [\underline{\mu^u K_i(S_k, S_l)}; \overline{\mu^u K_i(S_k, S_l)}].$$

Отличительной особенностью рассматриваемого подхода от методов теории нечетких множеств [8–10] является определение интервальной функции принадлежности в интервале [–1; 1].

Определение. *Интервальным отношением предпочтения* R^u на множестве S_α называется множество декартова произведения $(S_k \times S_l$, где $k = \overline{1,n}; l = \overline{1,n}; k \neq l)$, характеризующееся интервальной функцией принадлежности $\mu^u K_i(S_k, S_l) : S_k \times S_l \to [-1; 1]$. Значение этой функции $\mu^u K_i(S_k, S_l) = [\underline{\mu^u K_i(S_k, S_l)}; \overline{\mu^u K_i(S_k, S_l)}]$ понимается как объективная мера степени выполнения отношения $S_k R^u S_l$ по скалярному критерию оптимальности $\underline{K_i}(S_\alpha) = [\underline{K_i}(S_\alpha); \overline{K_i}(S_\alpha)]$, $(i = \overline{1,r}; \alpha = \overline{1,n})$, заданному в интервальном виде, характеризующему каждый отдельный вариант системы S_α, где:

$\underline{\mu^u K_i(S_k, S_l)} \in [-1; 0]$ — значение, характеризующее максимальную степень потерь при признании системы S_k, доминирующей систему S_l по скалярному интервальному критерию оптимальности K_i;

$\overline{\mu^u K_i(S_k, S_l)} \in [0; 1]$ — значение, характеризующее максимальную степень выигрыша при признании системы S_k, доминирующей систему S_l по рассматриваемому K_i;

$\overline{\mu^u K_i(S_k, S_l)} \in [-1; 0]$ — означает абсолютное отсутствие доминирования системы S_k над системой S_l по скалярному интервальному критерию K_i;

$\underline{\mu^u K_i(S_k, S_l)} \in [0; 1]$ — означает абсолютное доминирование системы S_k над системой S_l по скалярному интервальному критерию K_i;

$[\underline{\mu^u K_i(S_k, S_l)}; \overline{\mu^u K_i(S_k, S_l)}] \in [-1; 1]$ — интервальное значение (комплексная характеристика), характеризующее степень выигрыша и степень потерь при признании системы S_k, доминирующей систему S_l по рассматриваемому K_i.

Введем отношение *строгого интервального предпочтения* системы S_k над системой S_l и определим его функцией принадлежности $\mu^u_D K_i(S_k, S_l)$, характеризующей интенсивность доминирования системы S_k над системой S_l по i-му частному интервальному критерию оптимальности, в виде

$$\begin{aligned}
\mu^u_D K_i(S_k, S_l) &= \mu^u K_i(S_k, S_l) - \mu^u K_i(S_l, S_k) = \\
&= [\underline{\mu^u K_i(S_k, S_l)};\ \overline{\mu^u K_i(S_k, S_l)}] - \\
&- [\underline{\mu^u K_i(S_l, S_k)};\ \overline{\mu^u K_i(S_l, S_k)}] = \\
&= [\min\{\underline{\mu^u K_i(S_k, S_l)} - \underline{\mu^u K_i(S_l, S_k)}; \\
&\quad \overline{\mu^u K_i(S_k, S_l)} - \overline{\mu^u K_i(S_l, S_k)}\}; \\
&\quad \max\{\underline{\mu^u K_i(S_k, S_l)} - \underline{\mu^u K_i(S_l, S_k)}; \\
&\quad \overline{\mu^u K_i(S_k, S_l)} - \overline{\mu^u K_i(S_l, S_k)}\}].
\end{aligned} \tag{5}$$

Результаты сравнения $\mu^u K_i(S_k, S_l)$ и $\mu^u K_i(S_l, S_k)$, $(\forall S_k$ и $S_l)$ будем заносить в специальную оценочную матрицу $\|\mu^u_D K_i(S_k, S_l)\|$.

Введем отношение интервального недоминирования системы S_k над системой S_l и определим его функцией принадлежности $\mu_{ND} K_i(S_k, S_l)$ как дополнение к $\mu^u_D K_i(S_k, S_l)$ в виде

$$\mu_{ND} K_i(S_k, S_l) = \begin{cases} 1, \text{если } \mu^u_D K_i(S_k, S_l) < 0 \\ 1 - \mu^u_D K_i(S_k, S_l), \text{если } \mu^u_D K_i(S_k, S_l) \geq 0 \end{cases}. \tag{6}$$

Результаты выполнения условия (6) будем заносить в оценочную матрицу $\|\mu_{ND} K_i(S_k, S_l)\|$.

Степень «недоминируемости» системы S_k ни одной другой системой по i-му скалярному интервальному критерию оптимальности характеризуется [10] функцией принадлежности множеству недоминируемых систем $\mu^*_D K_i(S_k)$ в виде

$$\mu^*_D K_i(S_k) = \min \mu_{ND} K_i(S_k, S_l). \tag{7}$$

Значение функции принадлежности $\mu^*_D K_i(S_k)$ показывает степень близости варианта системы S_k к эффективному (парето-оптимальному) варианту по рассматриваемому скалярному интервальному i-му критерию оптимальности.

Если в процессе решения, в зависимости от смысла задачи, необходимо выполнить условие (2), то выбор значения $\mu^*_D K_i(S_k)$ необходимо осу-

■ ***Таблица 1.*** *Таблица исходных данных*

Критерии $K_i(S_\alpha)$	Системы (S_α)			
	S_1	S_2	S_3	m_i
1. $K_1(S_\alpha)$ — ориентировочная стоимость образца (тыс. у. е.)	[40; 90]	[50; 70]	[60; 65]	100
2. $K_2(S_\alpha)$ — ожидаемый эффект от эксплуатации образца (баллы)	[5; 6]	[3; 9]	[4; 7]	10
3. $K_3(S_\alpha)$ — ожидаемая скорость выполнения операций (опер./с)	[80; 100]	[100; 120]	[110; 115]	150

ществлять из k-й строки оценочной матрицы $\|\mu_{ND}K_i(S_k, S_l)\|$. Если в процессе решения необходимо выполнить условие (3), то выбор значения $\mu^*_D K_i(S_k)$ необходимо осуществлять из l-го столбца оценочной матрицы $\|\mu_{ND}K_i(S_k, S_l)\|$.

Величину $\mu^*_D K_i(S_k)$ будем рассматривать как *меру предпочтения*, обеспечивающую объективный и адекватный реальности способ сравнения сложных систем, характеризующихся разнородными интервальными критериальными значениями, и устанавливающую значение приоритета системы при выборе.

Рассмотрим иллюстративный пример.

Пример. Необходимо отдать предпочтение одной из трех систем $\{S_1, S_2, S_3\}$, характеризующихся тремя критериями $K_1(S_\alpha)$, $K_2(S_\alpha)$ и $K_3(S_\alpha)$, значения которых заданы в интервальном виде, остальные системы расположить в порядке убывания предпочтения.

Варианты систем, значения критериев оптимальности и ширина интервала оценок по i-му частному критерию представлены в табл. 1. При этом должны выполняться условия

$$K_1(S^*_\alpha) = \min_{\alpha=1,3}[K_1(S_\alpha)]; \quad (8)$$

$$K_2(S^*_\alpha) = \max_{\alpha=1,3}[K_2(S_\alpha)]; \quad (9)$$

$$K_3(S^*_\alpha) = \max_{\alpha=1,3}[K_3(S_\alpha)]. \quad (10)$$

Как видно из табл. 1, критерии $K_1(S_\alpha)$, $K_2(S_\alpha)$ и $K_3(S_\alpha)$ являются разнородными, измеряемыми в различных шкалах, с различными диапазонами отклонения качества. Кроме того, условия (8) и (9), (10) являются диаметрально противоположными.

Решение задачи:

1. С использованием выражения (4) определяем $\mu^u K_1(S_1, S_2)$:

$$\mu^u K_1(S_1, S_2) = \frac{[40; 90] - [50; 70]}{100} =$$

$$= \frac{[\min\{40-50; 90-70\}; \max\{40-50; 90-70\}]}{100} =$$

$$= \frac{[-10; 20]}{100} = [-0{,}1; 0{,}2].$$

Аналогично представленным вычислениям рассчитываем $\mu^u K_1(S_k, S_l)$, $\mu^u K_2(S_k, S_l)$ и $\mu^u K_3 \times (S_k, S_l)$ ($\forall S_k$ и S_l). Полученные данные сводим в табл. 2.

2. С использованием выражения (5) определяем $\mu^u_D K_1(S_1, S_2)$:

$$\mu^u_D K_1(S_1, S_2) = [-0{,}1; 0{,}2] - [-0{,}2; 0{,}1] =$$

$$= [\min\{-0{,}1-(-0{,}2); 0{,}2-0{,}1\};$$

$$\max\{-0{,}1-(-0{,}2); 0{,}2-0{,}1\}] = 0{,}1.$$

Аналогично представленным вычислениям рассчитываем $\mu^u_D K_1(S_k, S_l)$, $\mu^u_D K_2(S_k, S_l)$ и $\mu^u_D K_3(S_k, S_l)$ ($\forall S_k$ и S_l). Полученные данные сводим в табл. 3.

3. С использованием выражения (6) находим значения $\mu_{ND}K_1(S_k, S_l)$, $\mu_{ND}K_2(S_k, S_l)$ и $\mu_{ND}K_3(S_k, S_l)$. Полученные данные представим в табл. 4 и 5.

4. Значения $\mu^*_D K_i(S_k)$ для всех критериев сведем в табл. 6.

Согласно работе [16], значения $\mu^*_D K_i(S_k)$ определяются в диапазоне $\to$ [0; 1], где $\mu^*_D K_i(S_k) = 1$ оз-

■ ***Таблица 2.*** *Оценочная матрица* $\|\mu^u K_i(S_k, S_l)\|$

Системы (S_k)	Системы (S_l)		
	S_1	S_2	S_3
$\|\mu^u K_1(S_k, S_l)\|$			
S_1	–	[–0,1; 0,2]	[–0,2; 0,25]
S_2	[–0,2; 0,1]	–	[–0,1; 0,05]
S_3	[–0,25; 0,2]	[–0,05; 0,1]	–
$\|\mu^u K_2(S_k, S_l)\|$			
S_1	–	[–0,3; 0,2]	[–0,1; 0,1]
S_2	[–0,2; 0,3]	–	[–0,1; 0,2]
S_3	[–0,1; 0,1]	[–0,2; 0,1]	–
$\|\mu^u K_3(S_k, S_l)\|$			
S_1	–	[–0,13]	[–0,2; –0,1]
S_2	[0,13]	–	[–0,06; 0,03]
S_3	[0,1; 0,2]	[–0,03; 0,06]	–

■ ***Таблица 3.*** *Оценочная матрица* $\mu^{u}_{D}K_i(S_k, S_l)$

Системы (S_k)	Системы (S_l)		
	S_1	S_2	S_3
$\mu^{u}_{D}K_1(S_k, S_l)$			
S_1	–	0,1	0,05
S_2	–0,1	–	–0,05
S_3	–0,05	0,05	–
$\mu^{u}_{D}K_2(S_k, S_l)$			
S_1	–	0,1	0
S_2	–0,1	–	0,1
S_3	0	–0,1	–
$\mu^{u}_{D}K_3(S_k, S_l)$			
S_1	–	–0,26	–0,3
S_2	0,26	–	–0,03
S_3	0,3	0, 03	–

■ ***Таблица 4.*** *Оценочная матрица* $\mu_{ND}K_1(S_k, S_l)$

Системы (S_k)	Системы (S_l)			
	S_1	S_2	S_3	$\mu^{*}_{D}K_1(S_k)$
S_1	–	0,9	0,95	0,9
S_2	1	–	1	1
S_3	1	0,95	–	0,95

■ ***Таблица 5.*** *Значения* $\mu_{ND}K_i(S_k, S_l)$

Системы (S_k)	Системы (S_l)		
	S_1	S_2	S_3
$\mu_{ND}K_2(S_k, S_l)$			
S_1	–	0,9	1
S_2	1	–1	0,9
S_3	1	1	–
$\mu^{*}_{D}K_2(S_k)$	1	0,9	0,9
$\mu_{ND}K_3(S_k, S_l)$			
S_1	–	1	1
S_2	0,74	–	1
S_3	0,7	0,97	–
$\mu^{*}_{D}K_3(S_k)$	0,7	0,97	1

■ ***Таблица 6.*** *Значения* $\mu^{*}_{D}K_i(S_k)$

Системы (S_k)	$\mu^{*}_{D}K_i(S_k)$		
	$\mu^{*}_{D}K_1(S_k)$	$\mu^{*}_{D}K_2(S_k)$	$\mu^{*}_{D}K_3(S_k)$
S_1	0,9	1	0,7
S_2	1	0,9	0,97
S_3	0,95	0,9	1

начает, что система S_k является лучшей по i-му скалярному критерию в рассматриваемом множестве систем, 0 — худшей, а значение из диапазона [0; 1] показывает величину приоритета системы при выборе. Чем она выше, тем предпочтительней является рассматриваемая система S_k по i-му скалярному критерию оптимальности.

В результате решения задачи все интервальные критериальные оценки приведены к общему виду, удобному для сравнения при решении задач многокритериальной оптимизации.

Предложенный метод позволил сформулировать задачу построения отношения предпочтения на множестве СТС, характеризующихся векторным неоднородным критерием оптимальности, в следующем виде.

Требуется найти множество эффективных упорядоченных систем (кортеж предпочтений Парето) P^{μ}

$$S^{\mu}_{k_1} \succ S^{\mu}_{k_2} \succ \ldots \succ S^{\mu}_{k_{n^P}}, \qquad (11)$$

— для элементов $S^{\mu}_{k_j}$ которого справедливо

$$\mu^{*}_{D}K(S^{\mu}_{k_j}) = \max_{i=\overline{1,r};\ \alpha=\overline{1,n}} \{\mu^{*}_{D}K_i(S_\alpha)\},\ S^{\mu}_{k_j} \in S^{P}. \qquad (12)$$

Рассмотрим метод решения задачи (11) при условии (12).

Метод построения отношения предпочтения на множестве сложных систем, характеризующихся векторным неоднородным критерием оптимальности

При несомненных достоинствах методов решения задач многокритериальной (векторной) оптимизации [3, 15, 17] их общим недостатком, как, впрочем, и всех аксиоматических методов теории принятия решений, является то, что идет определение предпочтительности одного скалярного критерия над другим (т. е. определение того, что одна система лучше (хуже) другой по рассматриваемому критерию), далее каким бы то ни было *субъективным*, как правило, эвристическим или экспертным методом вводятся коэффициенты важности скалярных критериев оптимальности и уже с ними в дальнейшем производятся различные вычисления. Однако в реальных ситуациях достаточно часто оказывается, что относительную важность критериев (или признаков, по которым оцениваются альтернативы) невозможно достоверно описать соответствующими коэффициентами, кроме того, субъективизм назначения коэффициентов важности понижает достоверность принимаемого решения.

Предлагаемый метод построения отношения предпочтения на множестве СТС, характеризую-

щихся векторным неоднородным критерием оптимальности (*метод многокритериального предпочтения*), в отличие от известных (семейства методов *ЭЛЕКТРА* Б. Руа, метода «жесткого» ранжирования [13], методов, изложенных в работах [3, 5], и т. д.) позволяет вместо коэффициентов важности критериев использовать функции принадлежности $\mu_D^* K_i(S_\alpha)$, определяемые по описанной выше процедуре и показывающие степень близости систем S_α к эффективной (парето-оптимальной) системе по $K_i(S_\alpha)$ — частному критерию оптимальности. Сущность рассматриваемого метода многокритериального предпочтения [16] при решении задачи (11) и выполнении условия (12) заключается в следующем.

1. На основе анализа $\mu_D^* K_i(S_k)$ и $\mu_D^* K_i(S_l)$, $i = \overline{1,r}$ проведем попарное сравнение систем S_k и S_l и определим элементы C_{kl}^{μ} оценочной матрицы $\|C_{kl}^{\mu}\|$, $k = \overline{1,n}; l = \overline{1,n}; k \neq l$, в следующей последовательности.

Обозначим $I_{kl}^{+}, I_{kl}^{-}, I_{kl}^{=}$ соответственно подмножества лучших, худших и равных значений $\mu_D^* K_i(S_k)$ и $\mu_D^* K_i(S_l)$ для каждой пары систем S_k и S_l, $k = \overline{1,n}; l = \overline{1,n}; k \neq l$. Осуществим попарное сравнение систем S_k и S_l на основе анализа $\mu_D^* K_i(S_k)$ и $\mu_D^* K_i(S_l)$, $i = \overline{1,r}$. Для возможных значений подмножеств $I_{kl}^{+}, I_{kl}^{-}, I_{kl}^{=}$ введем следующие значения элементов оценочной матрицы $\|C_{kl}^{\mu}\|$:

$$\text{если } I_{kl}^{+} = \varnothing, I_{kl}^{-} = \varnothing, I_{kl}^{=} = \{\overline{1,r}\},$$
$$\text{то } C_{kl}^{\mu} = 1, C_{lk}^{\mu} = 1; \qquad (13)$$

$$\text{если } I_{kl}^{+} = \{\overline{1,r}\}, I_{kl}^{-} = \varnothing, I_{kl}^{=} = \varnothing,$$
$$\text{то } C_{kl}^{\mu} = N_2, C_{lk}^{\mu} = 0, N_2 >> 1; \qquad (14)$$

$$\text{если } I_{kl}^{+} = \varnothing, I_{kl}^{-} = \{\overline{1,r}\}, I_{kl}^{=} = \varnothing,$$
$$\text{то } C_{kl}^{\mu} = 0, C_{lk}^{\mu} = N_2; \qquad (15)$$

$$\text{если } I_{kl}^{+} \neq \varnothing, I_{kl}^{-} = \varnothing, I_{kl}^{=} \neq 0,$$
$$\text{то } C_{kl}^{\mu} = N_3, C_{lk}^{\mu} = 0; 1 << N_3 < N_2; \qquad (16)$$

$$\text{если } I_{kl}^{+} = \varnothing, I_{kl}^{-} \neq \varnothing, I_{kl}^{=} \neq 0,$$
$$\text{то } C_{kl}^{\mu} = 0, C_{lk}^{\mu} = N_3; \qquad (17)$$

$$\text{если } I_{kl}^{+} \neq \varnothing, I_{kl}^{-} \neq \varnothing, \left|I_{kl}^{=}\right| \geq 0, \qquad (18)$$

то C_{kl}^{μ}, в отличие от [15], определим в виде

$$C_{kl}^{\mu} = \left(\sum_{i=1}^{r} \mu_D^* K_i(S_k)\right)\left(\sum_{i=1}^{r} \mu_D^* K_i(S_l)\right)^{-1},$$
$$C_{kl}^{\mu} = C_{lk}^{\mu\,-1}. \qquad (19)$$

В случае, когда при формировании исходных данных для решения задачи заданы коэффициенты важности рассматриваемых скалярных критериев оптимальности, то C_{kl}^{μ} для условия (18) определим в виде

$$C_{kl}^{\mu} = \left(\sum_{i=1}^{r} \mu_D^* K_i(S_k) a_i\right)\left(\sum_{i=1}^{r} \mu_D^* K_i(S_l) a_i\right)^{-1},$$
$$C_{kl}^{\mu} = C_{lk}^{\mu\,-1}, \qquad (20)$$

где a_i — коэффициент важности i-го критерия, причем $\sum_{i=1}^{r} a_i = 1$.

Согласно теореме 1 [16], если в l-м ($l \in \{\overline{1,n}\}$) столбце оценочной матрицы одно из чисел C_{kl}^{μ} равно значению N_2 или N_3, то l-й вариант системы не принадлежит множеству эффективных вариантов.

2. Для формулировки решающих правил, по аналогии с методом «жесткого» ранжирования [15], введем систему показателей: H_l^{μ} — количество элементов в l-м столбце оценочной матрицы $\|C_{kl}^{\mu}\|$, значения которых больше единицы; M_l^{μ} — количество элементов в l-м столбце той же матрицы, значения которых меньше единицы, но больше нуля; $C_{kl\,\max}^{\mu}$ — максимальное значение элемента в l-м столбце матрицы. *Физический смысл показателей*: H_l^{μ} показывает, сколько вариантов из рассматриваемого множества превышает l-й; M_l^{μ} — в скольких вариантах доминирует l-я система; $C_{kl\,\max}^{\mu}$ определяет максимальную степень доминирования k-й системы над l-й, $k = \overline{1,n}$; $l = \overline{1,n}$; $k \neq l$.

3. Для определения порядка предпочтений на множестве систем перейдем от одношагового процесса поиска приоритетного расположения альтернатив к многошаговому процессу [3, 15]. На каждом шаге t, $t = 1, 2, ..., n^P - 1$, где n^P — число эффективных вариантов, выбираем j-ю альтернативу, лучшую с точки зрения предлагаемых ниже решающих правил (**RP**). **Затем ее номер включаем** в кортеж Парето P и в последующем рассмотрении j-я альтернатива больше не участвует (в матрице $\|C_{kl}^{\mu}\|$ вычеркиваем j-ю строку и j-й столбец). Это позволяет исключить влияние варианта S_j на выбор лучшей альтернативы, проводимой на следующем шаге. Далее вновь используем, но теперь на каждом шаге $t + 1$, показатели $H_l^{\mu(t)}$, $M_l^{\mu(t)}$, $C_{kl\,\max}^{\mu(t)}$, которые имеют оговоренный выше физический смысл.

Решающие правила многокритериального предпочтения (*RP МП*).

1. Поиск приоритетного расположения СТС необходимо проводить только среди эффективных вариантов по шагам t, $t = 1, 2, ..., n^P - 1$.

2. Положить $t = 1$.

3. Найти показатели $H_l^{\mu(t)}$, $M_l^{\mu(t)}$, $C_{kl\,\max}^{\mu(t)}$ и определить лучшую альтернативу S_j с минимальным значением $H_l^{\mu(t)}$.

4. Номер j занести в множество P.

5. Исключить из оценочной матрицы j-ю строку и j-й столбец.

6. Если альтернативы с номерами $l_j \in L_{k(t)} = \{l_1, l_2, ..., l_j, ..., l_{k(t)}\}$ имеют одинаковые минимальные значения $H_{l_j}^{\mu(t)}$, то лучшей является альтернатива S_{l_j} с максимальным значением $M_{l_j}^{\mu(t)} = \max_{l_j \in L_{k(t)}} M_{l_j}^{\mu(t)}$.

7. Если варианты с номерами $l_j \in L_{k(t)} = \{l_1, l_2, ..., l_j, ..., l_{k(t)}\}$ имеют соответственно одинаковые значения $H_{l_j}^{\mu(t)}$, $M_{l_j}^{\mu(t)}$, то лучшей является альтернатива S_{l_j} с минимальным значением $C_{kl\max_j}^{\mu(t)}$.

8. Если лучшие системы имеют соответственно равные значения $H_{l_j}^{\mu(t)}$, $M_{l_j}^{\mu(t)}$, $C_{kl\max_j}^{\mu(t)}$, то такие системы считают эквивалентными.

9. Положить $t = t + 1$.

10. Если $t < (n^P - 1)$, перейти к шагу 3, иначе — к шагу 11.

11. Конец решения.

Пример (продолжение). Для определения отношения предпочтения на рассматриваемом множестве СТС $\{S_1, S_2, S_3\}$, характеризующихся векторным неоднородным критерием оптимальности $K(S_\alpha) = \{K_1(S_\alpha), K_2(S_\alpha), K_3(S_\alpha)\}$, $\alpha = \{1, 2, 3\}$, будем использовать $\mu_D^* K_i(S_k)$, определенные на предыдущем этапе решения (табл. 8), и RP МП.

1. Построим матрицу предпочтений $\|C_{kl}^{\mu}\|$ (табл. 7).

Порядок расчета чисел C_{kl}^{μ}:

$$C_{12}^{\mu} = \frac{\mu_D^* K_1(S_1) + \mu_D^* K_2(S_1) + \mu_D^* K_3(S_1)}{\mu_D^* K_1(S_2) + \mu_D^* K_2(S_2) + \mu_D^* K_3(S_2)} = \frac{0{,}9 + 1 + 0{,}7}{1 + 0{,}9 + 0{,}97} = \frac{2{,}6}{2{,}87} = 0{,}9.$$

2. Анализ оценочной матрицы $\|C_{kl}^{\mu}\|$ позволяет получить на 1-м шаге ($t = 1$) решения показатели $H_{l_j}^{\mu(1)}$, $M_{l_j}^{\mu(1)}$, $C_{kl\max_j}^{\mu(1)}$, которые приведены в табл. 8.

3. Анализ табл. 8 показывает, что в соответствии с принятыми RP МП предпочтение на 1-м шаге решения ($t = 1$) необходимо отдать системе S_2. Включаем ее в кортеж Парето P. В табл. 7 удаляем вторую (S_2) строку и второй (S_2) столбец.

4. На 2-м шаге ($t = t + 1 = 2$) получаем вторую матрицу предпочтений (табл. 9) и матрицу показателей (табл. 10).

5. Предпочтение на 2-м шаге в соответствии с RP МП отдаем системе S_3. Так как $t = 2 = n^P - 1$,

■ ***Таблица 7.*** *Матрица предпочтений* $\|C_{kl}^{\mu}\|$

Системы (S_k)	Системы (S_l)		
	S_1	S_2	S_3
S_1	–	0,9	0,91
S_2	1,1	–	1,01
S_3	1,09	0,99	–

■ ***Таблица 8.*** *Матрица показателей*

Показатели	Системы (S_l)		
	S_1	S_2	S_3
$H_{l_j}^{\mu(1)}$	2	0	1
$M_{l_j}^{\mu(1)}$	0	2	1
$C_{kl_j\max}^{\mu(1)}$	1,1	0,99	1,01

■ ***Таблица 9.*** *Матрица предпочтений (шаг 2)*

Системы (S_k)	Системы (S_l)	
	S_1	S_3
S_1	–	0,91
S_3	1,09	–

■ ***Таблица 10.*** *Матрица показателей (шаг 2)*

Показатели	Системы (S_l)	
	S_1	S_3
$H_{l_j}^{\mu(2)}$	1	0
$M_{l_j}^{\mu(2)}$	0	1
$C_{kl_j\max}^{\mu(2)}$	1,09	0,91

где $n^P = 3$, решение заканчиваем и строим кортеж предпочтений Парето: $P = \{S_2, S_3, S_1\}$.

В результате решения задачи получили, что предпочтение по векторному неоднородному критерию оптимальности $K(S_\alpha) = \{K_1(S_\alpha), K_2(S_\alpha), K_3(S_\alpha)\}$ следует отдать *второй* системе (S_2), *третья* (S_3) и *первая* (S_1) системы занимают соответственно второе и третье места в кортеже.

Заключение

Таким образом, поставлена и решена важная в прикладном плане задача определения отношений предпочтения на множестве СТС для случая, когда критерии оптимальности разнородны и могут быть заданы в частично формализованном,

интервальном виде. Задача сводится к построению упорядоченного множества эффективных вариантов (кортежа предпочтений Парето) СТС по векторному разнородному критерию оптимальности.

На наш взгляд, метод может найти широкое применение при решении прикладных задач принятия решений в экономике, социальной сфере, оценке вариантов СТС различного назначения и т. д.

Литература

1. **Аленфельд Г., Херцбергер Ю.** Введение в интервальные вычисления. М.: Мир, 1987. 360 с.
2. **Алтунин А. Е., Семухин М. В.** Модели и алгоритмы принятия решений в нечетких условиях: Монография. Тюмень: Изд-во Тюменского гос. ун-та, 2000. 352 с.
3. **Белкин А. Р., Левин М. Ш.** Принятие решений: комбинаторные модели аппроксимации. М.: Наука, 1990. 160 с.
4. **Калмыков С. А., Шокин Ю. И., Юлдашев З. Х.** Методы интервального анализа. Новосибирск: Наука, 1986. 222 с.
5. **Шарый С. П.** Новый подход к анализу статических систем с интервальной неопределенностью в данных // Вычислительные технологии. 1997. № 1. С. 84–101.
6. **Шокин И. Ю.** Интервальный анализ. Новосибирск: Наука, 1981. 112 с.
7. **Левин В. И.** Задачи непрерывной оптимизации в условиях интервальной неопределенности // Информационные технологии. 1999. № 7. С. 31– 37.
8. **Жуковин В. Е.** Нечеткие многокритериальные модели принятия решений. Тбилиси: Мецниереба, 1988. 71 с.
9. **Заде Л. А.** Понятие лингвистической переменной и его применение к принятию приближенных решений. М.: Мир, 1976. 165 с.
10. **Орловский С. А.** Проблемы принятия решений при нечеткой исходной информации: Монография. М.: Наука, 1981. 203 с.
11. **Канторович Л. В.** Математические методы организации и планирования производства. Л.: Изд-во ЛГУ, 1939.
12. **Kaucher E.** Algebraische Erweiterungen der Intervallrechnung unter Erhaltung Ordnungs und Verbandsstrukturen // Computing Suppl. 1977. № 1. P. 65–79.
13. **Сафронов В. В., Ведерников Ю. В. и др.** Методика оптимизации структуры сложных технических систем в условиях риска // Информационно-управляющие системы. 2007. № 1. С. 40–46.
14. **Сафронов В. В., Ведерников Ю. В.** Метод многокритериального ранжирования сложных систем при различных видах неопределенности исходных данных // Информационно-управляющие системы. 2008. № 3. С. 32–39.
15. **Сафронов В. В., Ведерников Ю. В.** Научно-методический аппарат векторной оптимизации систем контроля и управления сложными динамическими объектами при разнородных исходных данных // Информационные технологии. (Приложение). 2007. № 11. 32 с.
16. **Ведерников Ю. В.** Теоретико-множественное обоснование выбора сложных систем при разнородной исходной информации: Монография. СПб.: МО РФ, 2008.
17. **Дубов Ю. А., Травкин С. И., Якимец В. Н.** Многокритериальные модели формирования и выбора вариантов систем. М.: Наука, 1986. 296 с.

УДК 004.588

ТЕХНОЛОГИЯ СТРУКТУРИРОВАНИЯ И ВИЗУАЛИЗАЦИИ УЧЕБНОЙ ИНФОРМАЦИИ В РЕПЕТИТОРСКИХ СИСТЕМАХ

А. Д. Тазетдинов,
канд. техн. наук, директор центра информационных технологий
АНО ВПО «Международный банковский институт»

Предлагаются: метод построения графов понятий учебного материала, реализующий механизм укрупнения информации за счет свертки нескольких понятий в одно; алгоритм автоматического разбиения графа понятий на подграфы с учетом требований когнитивной психологии на ограничение по количеству единиц информации, а также метод визуализации этих подграфов.

Ключевые слова *— репетиторские системы, визуализация и структурирование учебной информации, автоматизированные диалоги.*

Введение

Смысловое содержание учебного материала (УМ) представляет собой целостное единство теоретической и фактической информации, а понимание отдельных слов непосредственно связано с правильным пониманием смысла УМ. Результаты многочисленных исследований говорят о том, что *понимание* учебного материала является важнейшим фактором, влияющим как на скорость запоминания, так и на длительность хранения информации в памяти [1, 2]. В свою очередь, понимание зависит от *языка* (понятийного множества, используемого при изложении УМ) и *структуры* (топологии связей — графа понятий) этого УМ.

Если уровень знаний в основном зависит от личных усилий и способностей, а также от психофизиологических особенностей личности обучаемых, то структура знаний отражает особенности организации учебного процесса, так как на формирование структуры знаний обучаемых в большей степени влияет умение преподавателя правильно построить программу подготовки и эффективно ее изложить [3]. Чем лучше структурирована информация, предъявляемая на учебном занятии, тем проще она запоминается и дольше сохраняется в памяти. Поэтому одним из ключевых моментов в создании механизма понятийно-смысловой адаптации в репетиторской системе является анализ содержания учебной дисциплины и ее структурирование.

Графы понятий

Понятия в предметной области существуют не отдельно, сами по себе, а логически связаны между собой в структуры (орграфы, в дальнейшем — просто графы понятий). Структуры необходимы для выражения более сложных понятий предметной области.

Каждая вершина такого графа содержит одно понятие (семантическую единицу информации), которое, в свою очередь, может быть также представлено в виде графа, имеющего свои собственные исходные вершины (свои семантические единицы информации, изученные на предыдущих этапах обучения). Каждая дуга графа есть не что иное, как символ отношения (связи) между понятиями, которые она соединяет. Связи между понятиями могут быть не только прямыми, но и транзитивными (иерархическими, косвенными), когда путь между двумя вершинами (понятиями) содержит больше одной дуги. В дальнейшем, поскольку речь идет о понятиях УМ и их связях, а графовая модель является лишь математическим аппаратом и средством визуализации этих связей, для обозначения дуг и путей на графе понятий будут использоваться термины «связь» и «длина связи» (минимальная длина соответствует одной дуге графа).

Идея представления понятий (концептов) УМ и их связей в виде графа не нова, ей посвящены работы А. И. Уемова [4], В. М. Мизинцева, А. В. Кочергина [5], Л. П. Леонтьева, О. Г. Гохмана [6], В. Б. Швыркова [7], И. О. Александрова

[8], Н. М. Леоновой [1] и многих других ученых. Основная задача, решаемая в их работах, — определение оптимального объема УМ, выдаваемого за один раз. Чем больше семантического материала содержится в порции УМ, тем труднее он усваивается. Следовательно, важным параметром для графа УМ является его семантический вес, влияющий на трудность усвоения материала.

В репетиторской системе решение вышеозначенной задачи влияет как на стратегию изложения УМ (как и в какой последовательности должна проявляться структура УМ в сознании обучаемого), так и на тактику формирования комментариев в режиме обучающего диалога. Кроме того, прочность запоминания зависит от правильности выбора ключевых элементов УМ для повторения, связана со стратегией формирования графа понятий и, следовательно, зависит от стратегии изложения УМ.

В педагогической литературе известны две методики расчета семантического веса УМ — В. М. Мизинцева [5] и Л. П. Леонтьева [6]. В основе обеих методик лежат сформулированные в предметной области теории систем идеи А. И. Уемова, в соответствии с которыми информационная мера сложности графовой модели определяется длиной (количеством) дуг графа. Последняя рассматривается как отношения между его элементами (вершинами) и конфигурацией графовой модели, определяемой показателем относительной энтропии как мерой неопределенности системы. Каждая вершина такого графа содержит одну семантическую единицу информации, представляющую собой сложное или простое понятие, а также конкретные формулы, теоремы, определения, аксиомы, леммы, следствия, законы, правила, события и факты, рассматриваемые в контексте УМ [6].

Такой прямой теоретико-множественный подход к связям (отношениям) между понятиями не всегда объективно отражает реальную структуру отношений между понятиями внутри УМ. Поэтому задача определения оптимального объема в порции УМ решалась не только в области педагогики, но и в области когнитивной психологии.

Сторонники коннекционистской теории полагают, что связи могут измеряться не только количественно, но и качественно [2, 9]. То есть вес (сила и важность) одной связи зачастую не совпадает с весом другой связи (отношения). Кроме того, экспериментальные данные когнитивной психологии говорят о том, что мозг организован вокруг изначально различных систем хранения информации [2, 10]. Проходя через разные системы хранения, информация подвергается анализу и обработке, прежде чем попадает в долговременную память (ДВП). Эксперименты, проводимые на протяжении века, показали, что кратковременная память (КВП) удерживает 7 ± 2 единицы информации независимо от вида содержащихся в них данных (буква, цифра, слово или понятие). Несмотря на то что объем КВП ограничен, ее фактический объем может значительно расширяться за счет «укрупнения» или разбиения на крупные блоки, т. е. кодирования отдельных единиц в более крупных единицах. Но такое укрупнение не может произойти, пока не будет активизирована некоторая информация из ДВП. Как только произошло сопоставление входящих элементов и их репрезентаций в ДВП, наши знания помогают систематизировать кажущийся несвязным материал. Следовательно, важными характеристиками понятий в когнитивном подходе являются структура хранения, топология, вес связей и механизм свертки нескольких понятий в одно.

Сравнивая эти два подхода, можно сказать следующее.

В когнитивном подходе существует ограничение на количество новых понятий, но также имеется возможность укрупнения объема УМ за счет свертки нескольких связанных понятий в одно, что является существенным отличием когнитивного подхода от педагогического. Технология свертки позволяет не только представить несколько понятий в виде одного, но и дать объяснение, почему количество связей влияет на семантический вес графа понятий. Рассматривая граф не как целостную (неделимую) структуру, а с позиции теоретико-множественного представления, можно каждый маршрут графа свернуть и представить в качестве единицы информации. Тогда максимальное, теоретическое количество вновь образованных единиц информации при m вершинах вычисляется как сумма от одного до n размещений:

$$k = \sum_{n=1}^{m} A_m^n,$$

т. е. на четырех вершинах (понятиях) мы получаем 40 вновь образованных единиц информации. Безусловно, четыре понятия за один раз запомнить несложно, а 40 практически невозможно. Однако такая связанность может отражать реальную систему взаимоотношений понятий предметной области. Следовательно, во избежание снижения качества запоминания УМ требуется специальная технология предъявления такого графа обучаемому.

В применении к репетиторской системе предлагается объединить оба подхода, создав синтетический подход, в котором будут использовать-

ся и теоретико-множественные представления, и механизм свертки.

В этом случае, с точки зрения системного подхода и целостного представления об учебном материале, граф понятий УМ должен иметь следующие характеристики.

• Граф всегда имеет начальную (корневую) вершину, содержащую понятие самого изучаемого раздела или дисциплины (если граф строится для целой дисциплины).

• Из начальной вершины достижима любая другая вершина графа. Эта характеристика необходима для работы механизма свертки. То есть все понятия УМ могут быть свернуты к его определению (входят в основное понятие УМ).

• Граф может иметь контуры и циклы.

• Для каждой вершины и дуги графа может быть определен вес, указывающий степень ее значимости (наличие весов существенно упрощает обработку графа и поэтому весьма желательно).

• Учитывая иерархичность построения графа, веса вершинам и дугам могут быть определены автоматически по принципу: чем дальше от корня, тем меньше вес. При необходимости эти веса могут быть переопределены вручную.

Очевидно, что для предъявления обучаемому такой граф должен быть разделен на части. Возникает вопрос о топологии этих частей. Определив в качестве критерия оценки топологии степень связанности графа, можно построить шкалу, где с одной стороны располагается несвязный граф (фактически тезаурус), а с другой — сильно связный граф. Среднее значение шкалы занимает топология типа дерево. Дерево, реализуя естественную иерархию связей понятий предметной области, позволяет обеспечить взаимодействие всех вершин графа понятий при минимальном количестве ребер, равном $n - 1$, при n вершин [11]. Независимо от алгоритма обхода дерева УМ, промежуточные вершины повторяются тем большее количество раз, чем ближе они расположены к корню. Таким образом, более общие понятия и структура УМ лучше понимаются и запоминаются.

Важность ограничения на количество единиц информации можно увидеть при анализе потери одного или нескольких понятий из дерева УМ. Потеря одной вершины не приводит к уменьшению количества цепочек понятий, но существенно сокращает количество связей. Количество оставшихся связей можно вычислить по формуле

$$L_{\text{УМ}} = \sum_{i=1}^{k} C_{n_i}^{m},$$

где k — количество образовавшихся деревьев; n_i — количество вершин в i-м дереве; $m = 2$.

Конечно, автоматизировать процесс структурирования информации (выделение понятий, определение их весов, иерархий и связей) о предметной области практически невозможно, и выполнение этой работы целиком ложится на плечи преподавателя. Тем не менее, формирование предъявляемой обучаемому информации в виде слоев графа может осуществляться как в ручном, так и в автоматическом и полуавтоматическом режимах с помощью метода и алгоритма, предложенного ниже.

Метод предъявления графа понятий обучаемому.

• Согласно коннекционистской концепции, забывание происходит по причине уменьшения силы (как бы истаивания) связей между простыми единицами сети, в результате чего доступ к отдельным частям информации, составляющим некоторое понятие, теряется. Поэтому предъявление графа понятий обучаемому должно происходить итерационно, как бы послойно, постепенно усиливая ключевые понятия и связи и формируя новые.

• Первые слои должны давать целостную, более общую картину об УМ, так как они закладывают фундамент понятийно-смысловой структуры УМ. Необходимость формирования целостной картины, пусть изначально и очень отдаленной, связана с тем, что если информация объединена с другими осмысленными воспоминаниями, то вероятность перевода информации в ДВП возрастает. Следовательно, даже самая символическая структура УМ, но усвоенная и присутствующая в сознании обучаемого, будет способствовать существенному повышению качества запоминания нового материала.

• На графе понятий выделяются подграфы таким образом, что с учетом ограничений на количество новых понятий и механизма свертки каждый подграф должен содержать не более 7 ± 2 единиц информации. Количество полученных подграфов определяется количеством вершин графа, так как каждая вершина должна входить в какой-нибудь подграф.

• Каждый подграф представляет собой некий срез или логический слой предметной области. Возможны частичные пересечения подграфов.

• Формирование подграфов (слоев) выполняется по следующему алгоритму.

Алгоритм. Формирование подграфов на графе понятий УМ.

Задача.

Объекты. Ориентированный граф понятий УМ G.

Операции. Для любой вершины p операция КРАТЧАЙШИЙ_МАРШРУТ(p) выдает количе-

ство дуг в минимальном пути от корневой вершины до вершины *p*. ВЫБРАТЬ_ВЕРШИНЫ(*fl*, G, <=*k*) — возвращает вершины графа G, сортируя их по весам по убыванию, когда *fl*=0 — выбираются все вершины, иначе только изученные; <=*k* — условие выбора (в данном случае — все вершины графа, длина кратчайшего пути которых меньше или равна *k*). ЗАПИСАТЬ_В_БАЗУ(*p*, M[*p*], Max_Вес — M[*p*]) — записывает в базу данных для вершины *p* длину кратчайшего пути и вес вершины. ЗАПИСАТЬ_В_БАЗУ_ПГРАФ(G, *i*, ПВЕРШ, ПДУГИ, *concept*) — записывает в базу данных для графа G подграф *i*, содержащий массив ПВЕРШ — вершин, массив ПДУГИ — дуг и *concept* — количество единиц информации. ВИ_ДУГИ(*p*, ИВЕРШ, ИДУГИ) — возвращает все входящие и исходящие дуги для вершины *p*, смежные вершинам из массива ИВЕРШ и не вошедшие в массив ИДУГИ. ДДУГИ(*p*, ИДУГИ) — возвращает все исходящие дуги, длина кратчайшего пути которых больше длины кратчайшего пути вершины *p*, и не вошедшие в массив ИДУГИ.

Дано. Граф G с не установленными весами вершин.

Требуется. Сформировать подграфы на графе G так, чтобы в каждый подграф входило не больше 7 ± 2 единиц информации.

Решение.

1. Выполнить функцию УСТАНОВИТЬ_ВЕСА (G) для графа G.

2. Скорректировать вручную веса вершин так, чтобы вершины с одинаковым значением длины кратчайшего пути имели разный вес. Чем больше вес, тем раньше они будут представлены обучаемому.

3. Выполнить функцию СФОРМИРОВАТЬ_ПГРАФЫ (G, *k*), где *k* — количество уровней для обхода графа G в ширину (для формирования первых слоев), задается преподавателем.

```
функ УСТАНОВИТЬ_ВЕСА (G) {
1.  M = массив(); // массив для хранения вершин и их длин кратчайших
                  // маршрутов до корневой вершины
2.  Max_Вес = 0;
3.  для всех p из множества вершин графа G цикл {
4.      M[p] = КРАТЧАЙШИЙ_МАРШРУТ(p);
5.      Если (M[p] > Max_Вес) Max_Вес = M[p];
6.  }
7.  для всех p из множества вершин графа G цикл {
8.      ЗАПИСАТЬ_В_БАЗУ(p, M[p], Max_Вес – M[p]);
9.  }
}

функ СПГРАФ (G, ИВЕРШ, ИДУГИ, ПВЕРШ, ПДУГИ, concept, i, p) {
1.  если (существует(ИВЕРШ[p])) выход;
2.  если (concept > 7) {
3.      ЗАПИСАТЬ_В_БАЗУ_ПГРАФ(G, i, ПВЕРШ, ПДУГИ, concept);
4.      concept = 0;
5.      ПДУГИ = массив(); // обнуление массива
6.      ПВЕРШ = массив(); // обнуление массива
7.      i = i + 1;
8.  }
9.  ПВЕРШ[] = p;
10. ИВЕРШ[] = p;
11. ДУГИ = ВИ_ДУГИ(p, ИВЕРШ, ИДУГИ);
12. для всех d из множества ДУГИ цикл {
13.     ПДУГИ[] = d;
14.     ИДУГИ[] = d;
15.     concept = concept + 1;
16. }
17. ДУГИ = ДДУГИ(p, ИДУГИ);
18. для всех d из множества ДУГИ цикл {
19.     СПГРАФ (G, ИВЕРШ, ИДУГИ, ПВЕРШ, ПДУГИ, concept, i);
20. }
}

функ СФОРМИРОВАТЬ_ПГРАФЫ (G, k) {
1.  i = 1;          // счетчик подграфов
2.  concept = 0; // количество понятий в формируемом подграфе
3.  ИВЕРШ = массив(); // массив выбранных из графа G вершин
4.  ИДУГИ = массив(); // массив выбранных из графа G дуг
5.  ПВЕРШ = массив(); // массив вершин подграфа i
6.  ПДУГИ = массив(); // массив дуг подграфа i
7.  ВЕРШИНЫ = ВЫБРАТЬ_ВЕРШИНЫ(0, G, <=k)
8.  для всех p из множества ВЕРШИНЫ цикл {
9.    если (concept > 7) {
10.     ЗАПИСАТЬ_В_БАЗУ_ПГРАФ(G, i, ПВЕРШ, ПДУГИ, concept);
11.     concept = 0;
12.     ПДУГИ = массив();
13.     ПВЕРШ = массив();
14.     i = i + 1;
15. }
16. ПВЕРШ[] = p;
17. ИВЕРШ[] = p;
18. ДУГИ = ВИ_ДУГИ(p, ИВЕРШ, ИДУГИ);
19. для всех d из множества ДУГИ цикл {
20.         ПДУГИ[] = d;
21.         ИДУГИ[] = d;
22.         concept = concept + 1;
23.     }
24. }
25. ВЕРШИНЫ = ВЫБРАТЬ_ВЕРШИНЫ(0, G, k+1)
26. для всех p из множества ВЕРШИНЫ цикл {
27.     СПГРАФ (G, ИВЕРШ, ИДУГИ, ПВЕРШ, ПДУГИ, concept, i);
28. }
}
```

Следующим важным механизмом повышения качества запоминания УМ является визуализация изучаемого и изученных подграфов (слоев), самого графа понятий с выделением текущего понятия и всей цепочки связи этого понятия с корневой вершиной. Визуализация позволяет дать целостный системный взгляд на изучаемую предметную область и решить целый ряд важных дидактических задач. В настоящее время визуализация графов не является проблемой и может быть выполнена с помощью бесплатно распространяемого программного средства Графвиз [12]. Модули расширений Графвиз существуют для многих скриптовых языков программирова-

ния, и создание **web-страницы с визуализированными** графами, построенными по вышеописанному алгоритму, не представляет большой сложности. Предлагается следующий метод визуализации изучаемых элементов:

Метод визуализации изучаемых элементов.

• Для реализации целостного взгляда на изучаемый УМ для каждого обучаемого должны визуализироваться следующие структуры:

— граф понятий;

— **все подграфы (слои) графа, отсортированные** в порядке предъявления (изложения) УМ;

— текущий подграф (слой).

• Изученные понятия отличаются цветом от неизученных.

• Каждое изученное понятие может быть окрашено в цвет, соответствующий уровню понимания этого понятия. Например: «хорошо» — синий; «удовлетворительно» — желтый; «плохо» — красный; «отлично» — серый. Глядя на граф, нужно в первую очередь видеть то, что требует дополнительной проработки, поэтому яркими цветами выделяются плохие оценки, а отличные не выделяются.

• Неизученные понятия окрашены в черный цвет (шрифт и обрамление).

• Текущая цепочка понятий выделяется жирным шрифтом и обрамлением, а текущее понятие — зеленым цветом.

• Преподаватель должен иметь возможность просмотреть результаты изучения УМ каждого из учеников. Результаты должны быть показаны, по желанию преподавателя, в сокращенном виде (только в виде графа) или в полном (со всем набором визуализированных подграфов). И в полном, и в сокращенном виде используются все соответствующие цветовые окраски, предоставляя преподавателю информацию об уровне знаний каждого из обучаемых.

• Визуализация может служить не только средством получения информации и обратной связи, но средством доступа (портального, в случае web-реализации) к обучающим диалогам. Графвиз обеспечивает технологию, когда при щелчке мышью на вершине (понятии) графа обучаемый может быть переадресован на страницу, содержащую ссылки на диалоги, связанные с этим понятием. Диалоги на странице могут быть сгруппированы по уровням сложности.

• При накоплении информации можно заметить, что одни и те же понятия используются разными УМ или дисциплинами. Происходит частичное пересечение графов. Не являясь средством организации междисциплинарных связей, предлагаемая технология тем не менее может служить средством визуализации этих связей.

Визуализация позволяет решить целый ряд дидактических задач. Наиболее важная из них — это целостное восприятие учебного материала [11]. Обучаемый воспринимает УМ не как множество понятий, а как объект, постоянно видя, на каком этапе процесса обучения он находится, как текущая изучаемая часть связана с другими частями УМ и что еще необходимо сделать. Точно так же преподаватель, подходя к анализу знаний обучаемого, видит целостную, объемную картину этих знаний, представленную визуализированным графом. В случае использования визуализации преподавателю нет необходимости проводить регулярные тестирования. Информация накапливается, и достаточно беглого взгляда на граф обучаемого для оценки ситуации. Кроме того, визуализация решает проблему портального доступа к web-контенту УМ.

Заключение

Одним из ключевых моментов повышения качества обучения является анализ содержания учебной дисциплины и ее структурирование. С точки зрения системного подхода к учебному материалу в репетиторской системе, граф понятий УМ должен иметь корневую вершину и реализовывать механизм свертки всех понятий в эту вершину. Такой подход отражает целостное представление об УМ, когда все частные понятия входят неотъемлемой частью в общее (или основное понятие). Необходимость в поэтапной, порционной подаче материала требует разделения графа на части. Такое разделение может быть выполнено в автоматическом режиме с помощью метода и алгоритма, предлагаемого в статье. Каждый полученный подграф будет иметь топологию дерево и содержать 7 ± 2 единицы информации, что, согласно концепциям когнитивной психологии, способствует повышению качества запоминания УМ.

Системный подход к структурированию информации в репетиторской системе позволяет использовать в учебном процессе технологию визуализации УМ. Визуализация позволяет решить одну из важных дидактических задач — задачу целостного восприятия учебного материала. Визуализируются сам граф понятий и его подграфы с выделением текущего изучаемого понятия и всей цепочки связи этого понятия с корневой вершиной. Не менее важным свойством визуализации является отображение информации по каждому обучаемому в виде расцвеченного графа, что оказывает преподавателю существенную помощь в оценивании знаний обучаемых.

Литература

1. **Леонова Н. М., Марковский М. В.** Имитационные математические модели процессов адаптивного управления образовательной деятельностью: Монография / Под ред. А. Д. Модяева. М.: МИФИ, 2006. 123 с. (Сер. Социальная кибернетика).
2. **Солсо Р.** Когнитивная психология. 6-е изд. СПб.: Питер, 2006. 589 с.
3. **Снигирева Т. А.** Основы квалитативной технологии диагностики структуры знаний обучаемых / Под ред. В. С. Черепанова; Исслед. центр проблем качества подготовки специалистов. «Экспертиза». М.; Ижевск, 2006. 128 с.
4. **Уемов А. И.** Системный подход и общая теория систем. М.: Мысль, 1978. 272 с.
5. **Мизинцев В. П., Кочергин А. В.** Проблема аналитической оценки качества и эффективности учебного процесса в школе / Куйб. гос. пед. ин-т. Куйбышев, 1986.
6. **Леонтьев А. П., Гохман О. Г.** Проблемы управления учебным процессом (математические модели). Рига: Зинанте, 1984.
7. **Швырков В. Б.** Введение в объективную психологию: Нейрональные основы психики: Избранные тр. / ИП РАН. М., 2006. 592 с.
8. **Александров И. О.** Формирование структуры индивидуального знания / ИП РАН. М., 2006. 560 с.
9. **Когнитивная психология памяти** / Под ред. У. Найссера, А. Хаймен. СПб.: Прайм-Еврознак, 2005. 640 с.
10. **Гейвин Х.** Когнитивная психология. СПб.: Питер, 2003. 272 с.
11. **Касьянов В. Н., Евстигнеев В. А.** Графы в программировании: обработка, визуализация и применение. СПб.: БХВ-Петербург, 2003. 1104 с.
12. **Официальный сайт Графвиз** // http://www.graphviz.org/Gallery.php

Министерство образования и науки Российской Федерации
Федеральное агентство по образованию
Комиссия Российской Федерации по делам ЮНЕСКО
Правительство Санкт-Петербурга
Совет ректоров вузов Санкт-Петербурга
Ассоциация государственных образовательных учреждений высшего профессионального образования
«Национальный объединенный аэрокосмический университет»
Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП)
Кафедра ЮНЕСКО «Дистанционное инженерное образование» (ГУАП)

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И ВЫСШЕЕ ОБРАЗОВАНИЕ — ПРИОРИТЕТЫ РАЗВИТИЯ СОВРЕМЕННОГО ОБЩЕСТВА
26–30 мая 2009 г.

Форум будет проходить на борту комфортабельного теплохода «Виссарион Белинский», который совершит круиз из Санкт-Петербурга по рекам Нева и Свирь, Ладожскому и Онежскому озерам — жемчужинам Северо-Западного региона России.

В рамках международного форума будут проведены
Конференция ЮНЕСКО по проблемам высшего образования в условиях глобализации информационных ресурсов
XII симпозиум по проблемам избыточности в информационных и управляющих системах
XII конференция по волновой электронике и ее применению в информационных и телекоммуникационных системах

Стоимость
Стоимость участия в форуме для российских участников — 23 000 рублей (в т. ч. НДС), для сопровождающего лица 17 000 (в т. ч. НДС). В стоимость входит регистрационный взнос, публикация тезисов докладов, проживание на теплоходе, трехразовое питание и экскурсионная и культурная программа во время круиза.

Контрольные сроки
Заявки на участие в форуме принимаются до 1 апреля 2009 г.

Дополнительная информация и справки
Оргкомитет международного форума:
Санкт-Петербургский государственный университет аэрокосмического приборостроения
190000, Санкт-Петербург,
Большая Морская ул., 67
Тел.+7(812) 312–09–37, факс:+7(812) 312–06–58
e-mail: int@aanet.ru

УДК 612.82

ИНФОРМАТИВНОСТЬ КОЛЕБАТЕЛЬНЫХ ПЕРЕХОДНЫХ ПРОЦЕССОВ В ЭЛЕКТРОЭНЦЕФАЛОГРАММЕ ЧЕЛОВЕКА

Н. Б. Суворов,
доктор биол. наук, профессор
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
С. В. Божокин,
канд. физ.-мат. наук, доцент
Санкт-Петербургский государственный политехнический университет

Проанализированы нестационарные записи ЭЭГ, спектры мощности Фурье, локальные распределения энергии сигнала по частотам, исследованы скелетоны интегрального вейвлет-преобразования, изучена динамика проинтегрированных по основным ритмам ЭЭГ локальных плотностей колебаний, а также найдены характерные времена усвоения и забывания ритмов, вызванных фотостимуляцией.

Ключевые слова *— вейвлет-анализ, электроэнцефалограмма, фотостимуляция.*

Введение

Нестационарность большинства биологических сигналов ограничивает возможности их математического анализа и использования для целей управления состоянием и его психофизиологической коррекции. Обусловлено это не только особенностями происхождения и генерации биоэлектрических сигналов, но и внутренними переходными процессами, происходящими на разных уровнях интеграции и проявляющимися для «наблюдателя» случайным образом. Одним из самых непредсказуемых биологических процессов является электрическая активность головного мозга, отражением которой является электроэнцефалограмма (ЭЭГ) [1, 2].

Анализ ЭЭГ во время функциональных проб (фотостимуляции — ФСТ, гипервентиляции, психоэмоциональных тестов) показывает, что ее нестационарность в этих режимах носит вызванный характер, поэтому наряду с традиционными методами анализа стационарных процессов (спектральный, когерентный и др.) необходимо развивать новые подходы [3–6].

Целью данной работы является разработка принципиально новых информационных параметров количественного анализа нестационарных сигналов. Для решения этой задачи мы используем вейвлет-преобразования для нахождения характеристик переходных процессов ЭЭГ человека в реакциях усвоения ритма ФСТ и воспроизведения кратных частот.

Методика

Электроэнцефалограмма регистрировалась компьютерным электроэнцефалографом «Мицар-ЭЭГ-202» разработки и производства ООО «Мицар» (Санкт-Петербург). Испытуемые находились в условиях, рекомендованных при проведении ЭЭГ-исследований. Регистрирующие электроды располагались по системе «10–20 %». Исследования проводились в одно и то же время суток. Возраст испытуемых (10 мужчин) составлял 30–40 лет. Обязательным условием отбора испытуемых было отсутствие в анамнезе черепно-мозговых травм и нейроинфекций. Анализ ЭЭГ производился с помощью пакета программного обеспечения для регистрации и обработки ЭЭГ WinEEG, версия 1.5 (автор В. А. Пономарев). Для определения источников активности ритмов ЭЭГ использовалась программа LORETA [7]. Осуществляемые программой расчеты позволяют оценить плотность распределения источников потенциалов мозга в условных единицах и проиллюстрировать их местоположение на трех ортогональных срезах мозга.

Записи ЭЭГ затылочных отведений (левого O1, центрального Oz и правого O2) длительностью до 10 с анализировались до включения, во время и после выключения ФСТ. Фотостимуляция длительностью до 5 с и ритмом 2–20 вспышек/с включалась в случайные моменты времени регистрации ЭЭГ.

Для изучения нестационарной ЭЭГ введено интегральное вейвлетное преобразование

$$V(\nu, t) = \nu \int_{-\infty}^{\infty} dt' z(t') \psi^* \left(\nu(t' - t)\right).$$

В этом выражении $\psi(x)$ — материнский вейвлет, который в общем случае может быть комплексным. Символ * означает комплексное сопряжение. Величина ν, имеющая размерность частоты, определяет масштаб сжатия или растяжения материнского вейвлета, аргумент t определяет положение центра локализации вейвлета на оси времени. Интегральное вейвлет-преобразование $V(\nu, t)$ отображает исходный одномерный сигнал энцефалограммы $z(t)$ на плоскость время-частота, характеризуя изменение его спектрального состава во время испытания. Основной вклад в интеграл $V(\nu, t)$ дают те составляющие сигнала $z(t')$, которые в наибольшей степени «похожи» на материнский вейвлет, центрированный в точке $t = t'$ и обладающий характерной частотой ν. Продвигаясь по оси времени и изменяя для каждого значения t масштабный параметр ν, мы рассматриваем фрагменты нашего сигнала под «микроскопом» с разной степенью увеличения, причем выбором материнского вейвлета $\psi(x)$ мы можем влиять на оптические свойства «микроскопа» [5–6].

Материнский вейвлет $\psi(x)$ должен быть хорошо локализован вблизи точки $x = 0$, иметь нулевое среднее значение, вычисленное по всему интервалу переменной $-\infty < x < \infty$, и обладать единичной нормой. Используя фурье-компонент $\psi(\Omega)$ материнского вейвлета $\psi(x)$, можно ввести константу

$$C_\psi = \int_{-\infty}^{\infty} \frac{d\Omega |\psi(\Omega)|^2}{|\Omega|},$$

конечность которой позволяет восстанавливать сигнал по его вейвлет-образу.

Всеми этими свойствами обладает материнский вейвлет Морле

$$\psi(x) = \frac{\exp\left(-\frac{x^2}{2}\right)\left(\exp(-i\Omega_0 x) - \exp\left(-\frac{\Omega_0^2}{2}\right)\right)}{\sqrt{\sqrt{\pi}\left(1 - 2\exp\left(-\frac{3\Omega_0^2}{4}\right) + \exp\left(-\Omega_0^2\right)\right)}}. \quad (1)$$

Среди многих функций $\psi(x)$ вейвлет Морле (1) характеризуется наилучшим спектральным разрешением. Если значение параметра $\Omega_0 = 2\pi$, то для гармонического сигнала $z(t) = \cos(2\pi f_1 t)$ частоты f_1 максимум величины $|V(\nu, t)|^2$ будет наблюдаться при $\nu = f_1$. Это делает материнский вейвлет Морле удобным для исследования нестационарных сигналов, свойства которых меняются со временем. Изменяющиеся во времени спектральные свойства сигнала ЭЭГ можно проанализировать, изучая зависимость мгновенных максимальных частот сигнала ν_{max}, если следить за положениями максимумов (хребтов) поверхности интегрального вейвлет-преобразования $|V(\nu, t)|^2$. Изображения таких хребтов называют скелетоном сигнала.

Для интегрального вейвлетного преобразования справедливо соотношение, аналогичное формуле Парсеваля в фурье-анализе:

$$\int_{-\infty}^{\infty} dt\, z^2(t) = \frac{2}{C_\psi} \int_{-\infty}^{\infty} dt \int_0^{\infty} d\nu \frac{|V(\nu, t)|^2}{\nu}.$$

Из этой формулы видно, что величина $\varepsilon(\nu, t)$, определяемая соотношением

$$\varepsilon(\nu, t) = \frac{2}{C_\psi} \frac{|V(\nu, t)|^2}{\nu},$$

характеризует мгновенное распределение энергии сигнала по частотам ν вейвлетного преобразования (локальная плотность спектра энергии сигнала).

Для исследования нестационарных сигналов введем в рассмотрение величину

$$P_i(t) = \int_{\nu_{i-1}}^{\nu_i} d\nu\, \varepsilon(\nu, t), \quad (2)$$

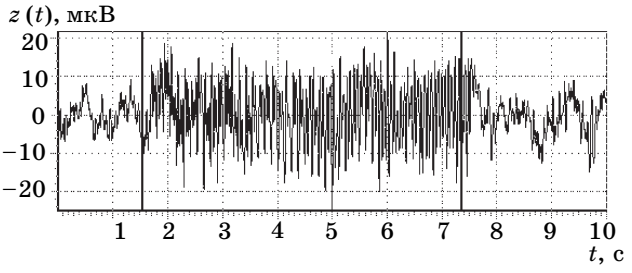
представляющую собой проинтегрированную по определенному интервалу частот локальную плотность спектра энергии сигнала, где величины ν_i, $i = 0, 1, 2, ..., k$ характеризуют границы соответствующего интервала. При анализе ЭЭГ весь диапазон частот обычно делят на 4 основных поддиапазона: δ — ритм с частотой 0,5–4 Гц, θ — ритм с частотой 4–7,5 Гц, α — ритм с частотой 7,5–14 Гц и β — ритм с частотой 14–30 Гц. В этом случае, полагая ν_0, ν_1, ..., ν_4 равными 0,5; 4; 7,5; 14; 30 Гц, получаем проинтегрированную локальную плотность в соответствующих диапазонах $P_\delta(t)$, $P_\theta(t)$, $P_\alpha(t)$, $P_\beta(t)$ в условных единицах. При изучении нестационарных ЭЭГ, формирующихся в результате включения и выключения ФСТ, нас также будет интересовать величина $P_{ФСТ}(t)$, которая будет представлять собой проинтегрированную локальную плотность в узком поддиапазоне

$[\nu_{ФСТ} - \Delta, \nu_{ФСТ} + \Delta]$ вблизи частоты ФСТ $\nu_{ФСТ}$, где $\Delta = 0{,}2$ Гц.

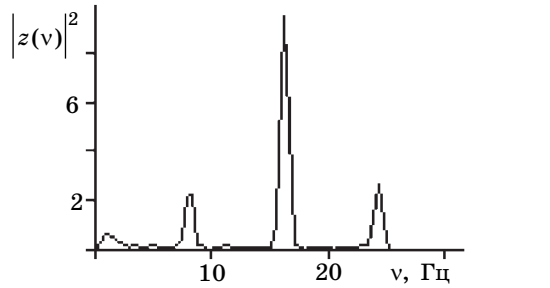
В данной статье мы рассмотрим различные сценарии поведения двумерных поверхностей интегрального вейвлет-преобразования $|V(\nu, t)|^2$ ЭЭГ в зависимости от частоты ν и времени t для ряда частот ФСТ. Изменение формы скелетона позволит проследить за динамикой возникновения и затухания максимальных частот ν_{max} при включении и выключении ФСТ. Кроме того, необходимо вычислять динамику проинтегрированных по определенному интервалу частот локальных плотностей колебаний $P_\delta(t)$, $P_\theta(t)$, $P_\alpha(t)$, $P_\beta(t)$, $P_{ФСТ}(t)$. Анализ этих кривых позволяет определить характерные времена усвоения ритма $t_1(i)$ при включении ФСТ, а также времена их «забывания» $t_2(i)$ после выключения ФСТ, где параметр i характеризует соответствующий спектральный диапазон $i = \alpha$, β, ФСТ, 2ФСТ, 3ФСТ. Время усвоения ритма $t_1(i)$ складывается из латентного периода (период «молчания» после включения ФСТ) и периода нарастания ритма. Время «забывания» ритма $t_2(i)$ складывается из периода сохранения соответствующего ритма в течение некоторого интервала времени после выключения ФСТ и периода его спадания.

Результаты и обсуждение

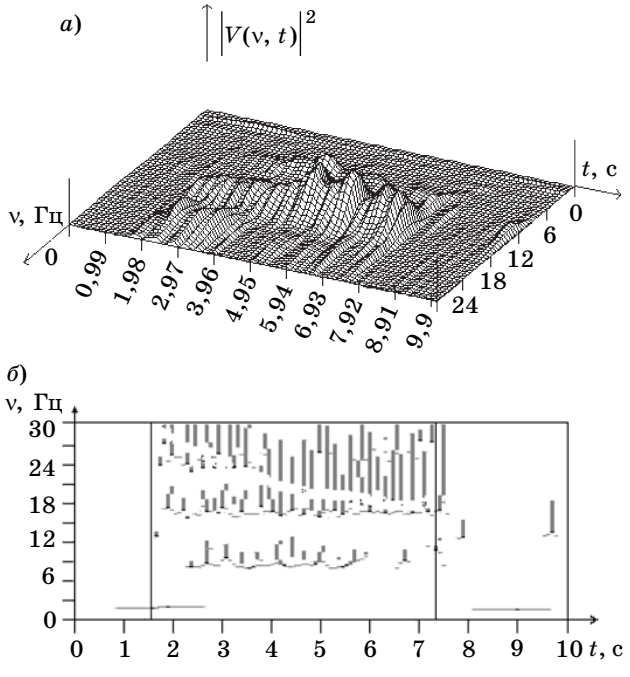
Цель работы состояла в изучении феномена усвоения ритма ФСТ при изменении частоты $\nu_{ФСТ}$ в указанных выше пределах и воспроизведения кратных частот. В качестве примера подробно разберем результаты анализа ЭЭГ левого затылочного отведения (О1) испытуемого при частоте $\nu_{ФСТ} = 8{,}12$ вспышек/с. На рис. 1 изображен фрагмент записи ЭЭГ, где вертикальными линиями обозначены моменты времени включения и выключения ФСТ. На рис. 2 показан спектр мощности для левого затылочного отведения с тремя пиками частот вблизи $\nu_{ФСТ} = 8{,}12$ Гц, $\nu_{2ФСТ} = 16{,}24$ Гц и $\nu_{3ФСТ} = 24{,}36$ Гц. На рис. 3, *а* построен квадрат модуля интегрального вейвлетного преобразования $|V(\nu, t)|^2$ в зависимости от частоты ν и времени t для фрагмента ЭЭГ (см. рис. 1). Трехмодальная структура $|V(\nu, t)|^2$ демонстрирует сложную динамику появления и затухания трех пиков частот $\nu_{ФСТ}$, $\nu_{2ФСТ}$, $\nu_{3ФСТ}$ и свидетельствует о сильной нестационарности сигнала ЭЭГ. На рис. 3, *б* построен скелетон, представляющий собой характерные «хребты» поверхности (см. рис. 3, *а*), отражающие перестройку структуры максимумов величины $|V(\nu, t)|^2$. ФСТ включается в момент времени $t = 1{,}55$ с от начала фрагмента, выключается при $t = 7{,}25$ с, причем после выключения ФСТ наступает десинхронизация ЭЭГ. На рис. 4, *а* представлена проинтегрированная по указанному выше диапазону α-ритма локальная плотность спектра его энергии $P_\alpha(t)$ (2) в зависимости от времени t.



■ ***Рис. 1.*** *Фрагмент ЭЭГ в левом затылочном отведении О1 при ФСТ с частотой* $\nu_{ФСТ} = 8{,}12$ *вспышек/с*



■ ***Рис. 2.*** *Спектр мощности* $|z(\nu)|^2$ *сигнала левого затылочного отведения О1 в зависимости от частоты*

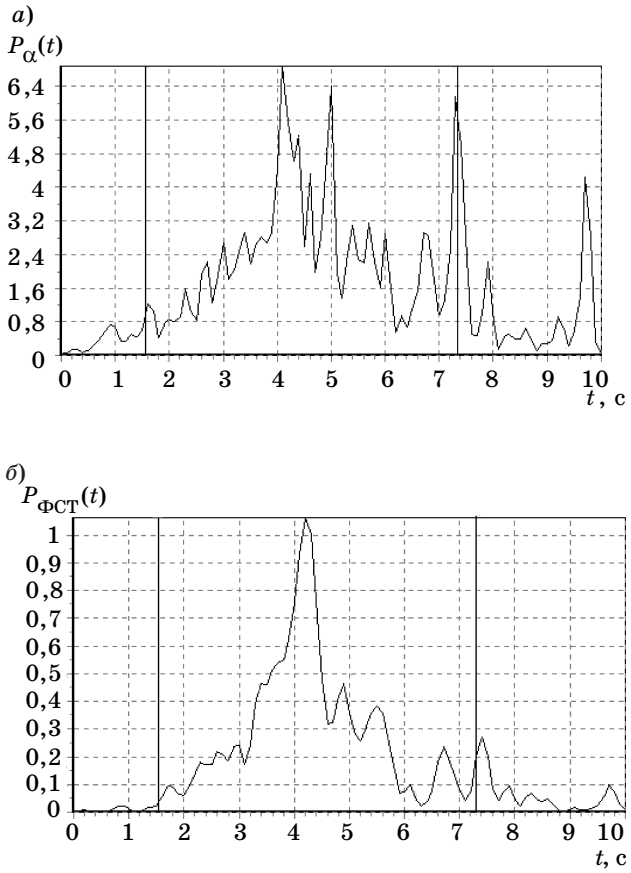


■ ***Рис. 3.*** *Квадрат модуля интегрального вейвлет-преобразования* $|V(\nu, t)|^2$ *в зависимости от частоты и времени* (*а*) *и его скелетон* (*б*)

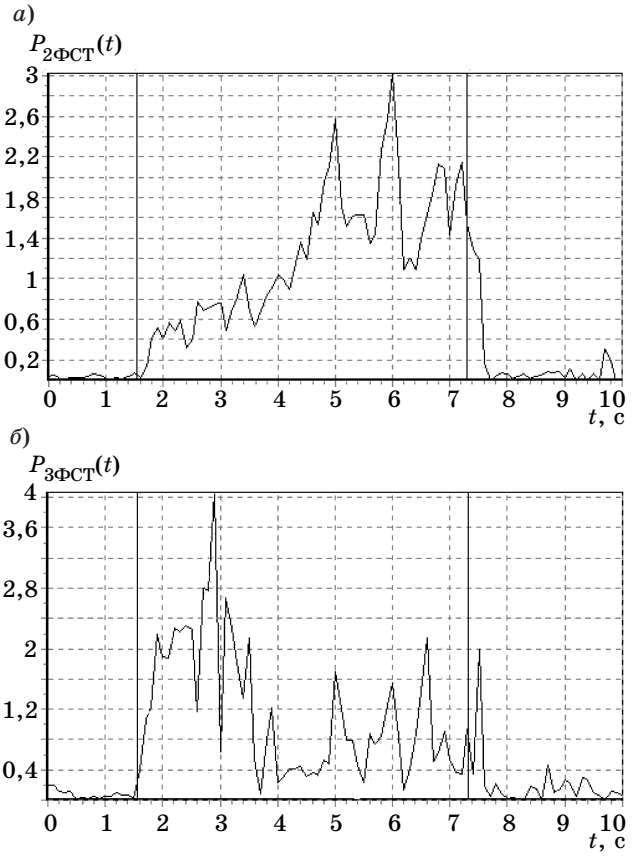
Локальная плотность спектра $P_{ФСТ}(t)$, проинтегрированная в узком поддиапазоне вблизи частоты фотостимуляции ($\nu_{ФСТ} \pm 0{,}2$) Гц, представлена на рис. 4, *б*. Переходной период усвоения ритма ФСТ складывается из латентного периода относительного «молчания», продолжающегося примерно 1,4 с, и периода нарастания ритма ФСТ, равного 1,3 с. После достижения максимума в момент времени $t \approx 4{,}3$ с интенсивность $P_{ФСТ}(t)$ быстро падает. Сравнение $P_{\alpha}(t)$ и $P_{ФСТ}(t)$ показывает, что внутри диапазона α-ритма помимо частоты ФСТ (совпадающие пики в момент времени $t \approx 4{,}2$ с) содержатся другие частоты. Эти различия видны при $t \approx 5$ с и особенно после отключения ФСТ.

Гармоника $P_{2ФСТ}(t)$ (2) с удвоенной частотой $\nu_{2ФСТ} = (16{,}24 \pm 0{,}2)$ Гц (рис. 5, *а*) достигает первого пика ($t \approx 5$ с) примерно через 3,5 с после момента включения ФСТ. Она имеет осциллирующий характер — периодичность ее усиленного воспроизведения составляет величину, примерно равную 1 с (пики в моменты $t \approx 5$; 6; 6,8 с). После выключения ФСТ вторая гармоника затухает за 0,3 с.

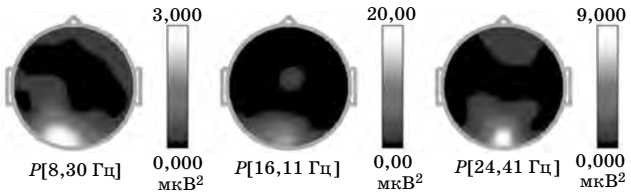
Минимальный период усвоения ритма ФСТ оказался при воспроизведении утроенной частоты $\nu_{3ФСТ} = (24{,}36 \pm 0{,}2)$ Гц. На рис. 5, б для $P_{3ФСТ}(t)$ видно, что после включения ФСТ ($t = 1{,}55$ с) быстрый период нарастания ритма $\nu_{3ФСТ}$ составляет величину 0,4 с ($t \approx 1{,}9$ с). После относительно стабильного периода усвоения наблюдается второй всплеск величины $P_{3ФСТ}(t)$ ($t \approx 2{,}9$ с) с характерным временем нарастания 0,4 с. После выключения ФСТ ($t = 7{,}25$ с) высокочастотная активность сохраняется примерно 0,2 с и затем еще через 0,2 с быстро спадает. Если построить сумму трех локальных плотностей частот $P_{ФСТ}(t) + P_{2ФСТ}(t) + P_{3ФСТ}(t)$, то этот график имеет профиль, близкий к трапециевидному. При этом латентный период усвоения «суммарного» ритма равен 0,4 с, а время «забывания» ритма — 0,3 с. Визуальный анализ ЭЭГ (см. рис. 1) также дает основание считать, что на временном отрезке 3,5–4,5 с наблюдается кратковременное снижение «средней» частоты ЭЭГ. Кривая характеризуется сильной нестационарностью, причем временную



■ ***Рис. 4.*** *Локальная плотность: а — альфа-ритма, проинтегрированная в интервале 7,5–14 Гц; б — спектра $P_{ФСТ}(t)$, проинтегрированная в узком интервале $[\nu_{ФСТ} - \Delta, \nu_{ФСТ} + \Delta]$ вблизи частоты $\nu_{ФСТ} = 8{,}12$ Гц*



■ ***Рис. 5.*** *Локальная плотность спектра: а — $P_{2ФСТ}(t)$, проинтегрированная в узком интервале $[\nu_{2ФСТ} - \Delta, \nu_{2ФСТ} + \Delta]$ вблизи удвоенной частоты ФСТ; б — $P_{3ФСТ}(t)$, проинтегрированная в узком интервале $[\nu_{3ФСТ} - \Delta, \nu_{3ФСТ} + \Delta]$ вблизи утроенной частоты ФСТ*



■ ***Рис. 6.*** *Пространственное распределение гармоник ФСТ, 2ФСТ, 3ФСТ по поверхности мозга*

и частотную динамику такого сигнала определить традиционными методами не представляется возможным.

Распределение трех упомянутых гармоник по поверхности мозга представлено на рис. 6. Очевидно, что реакция воспроизведения ритма ФСТ и кратных ритмов наблюдается в затылочных отведениях, причем ритм ФСТ — в основном слева (O1), 16 Гц — в трех отведениях (O1, O2 и Oz), 24 Гц — в основном в центре (Oz). В остальных отведениях интенсивность частот, связанных с ФСТ, чрезвычайно низка.

Применение программного пакета LORETA дало следующие результаты. Координаты источника частоты ФСТ (–3, –11, 64) — Medial Frontal Gyrus. Координаты источника удвоенной частоты (4, –67, 15) — Posterior Cingulate Limbic Lobe. Координаты источника утроенной частоты (–3, –53, 57) — Precuneus Parietal Lobe. Список источников, отмеченных у различных испытуемых на разных частотах ФСТ, достаточно ограничен, их перечисление и анализ выходит за рамки данной статьи.

Заключение

Проведенные исследования показали чрезвычайное разнообразие индивидуальных особенностей реагирования на ритмическую ФСТ. Мы опускаем наблюдения, в которых вообще не было реакции усвоения ритма, наблюдения, где имело место только усвоение ритма ФСТ без воспроизведения кратных частот — этот переходный режим достаточно хорошо идентифицируется стандартными программами, которыми располагает практически каждый компьютерный электроэнцефалограф. Временная динамика взаимодействия частоты ФСТ и кратных частот состоит из нескольких компонентов, количественно характеризующих сложный переходный процесс ЭЭГ.

Перечислим основные черты усвоения ФСТ и кратных ритмов на частотах $\nu_{ФСТ/2}$, $\nu_{ФСТ}$, $\nu_{2ФСТ}$, $\nu_{3ФСТ}$, $\nu_{4ФСТ}$, которые являются общими для наблюдавшихся испытуемых. Исследования многих испытуемых, выполненные для различных частот ФСТ, показывают, что характер усвоения и воспроизведения ритмов во многих случаях имеет ярко выраженную нестационарность. Асимметричные трапециевидные локальные плотности $P_i(t)$ (6), где $i = (\delta, \theta, \alpha, \beta, ФСТ/2, ФСТ, 2ФСТ, 3ФСТ$ и т. д.) могут изменяться на осциллирующие или смешанные. Каждый такой сценарий характеризуется определенным латентным периодом усвоения соответствующего ритма и периодом его нарастания после включения ФСТ. Для некоторых диапазонов $P_i(t)$ латентный период может отсутствовать. При выключении ФСТ часто наблюдается промежуток времени сохранения ритма, после которого наблюдается его затухание.

Таким образом, интегральное вейвлет-преобразование дает принципиально новую информацию, которая недоступна стандартным методам анализа ЭЭГ. Предлагаемый подход позволяет классифицировать и количественно оценивать переходные процессы, характеризующие лабильность центральной нервной системы человека, дает информацию о развитии амплитудно-частотных изменений в вызванной ЭЭГ, полезную для синтеза алгоритмов психофизиологической коррекции и управления состоянием организма или его функциональных систем.

Литература

1. **Федотчев А. И., Бондарь И. Г., Маевский А. А., Якулова Л. П.** Резонансные реакции при ритмической фотостимуляции и изменение функционального состояния // Журнал высшей нервной деятельности. 1996. Т. 46. № 3. С. 447–452.
2. **Суворов Н. Б., Гусева Н. Л., Зуева Н. Г.** Отражение индивидуально-типологических особенностей в структуре пространственного взаимодействия волн ЭЭГ различных частотных диапазонов // Физиология человека. 2000. Т. 26. № 3. С. 60–66.
3. **Чуи К.** Введение в вейвлеты. М.: Мир, 2001. С. 416.
4. **Малла С.** Вейвлеты в обработке сигналов. М.: Мир, 2005. С. 671.
5. **Божокин С. В., Лыков С. Н.** Дополнительные главы теоретической физики. Вейвлеты. СПб.: СПбГПУ, 2007. С. 252.
6. **Божокин С. В., Паршин Д. А.** Фракталы и мультифракталы. М. — Ижевск: Регулярная и хаотическая динамика, 2001. С. 128.
7. **LORETA** (Institute for Brain-Mind Research University Hospital of Psychiatry. Lenggstr. 31, CH-8029 Zurich, Switzerland). www.keyinst.unizh.ch/loreta.htm

УДК 621.317, 681.2

АППАРАТНАЯ РЕАЛИЗАЦИЯ ЭЛЕКТРИЧЕСКОГО ИМПЕДАНСНОГО ТОМОГРАФА

А. Г. Михайлова*,*
соискатель
Московский государственный университет приборостроения и информатики

Приводится описание разработанной системы сбора данных на основе платы PCI 6052E, являющейся лабораторным электрическим импедансным томографом и предназначенной для изучения резистивных и диэлектрических свойств среды. Предварительно кратко рассмотрены общие принципы построения импедансных томографов и существующие реализации.

Ключевые слова *— импедансный томограф, системы сбора данных.*

Метод импедансной томографии и требования к аппаратному обеспечению

В данной статье рассматривается импедансная томография как метод восстановления внутренней структуры биологических объектов путем построения распределений проводимости и диэлектрической проницаемости среды по измеренным напряжениям на поверхности объекта.

К настоящему времени разработано несколько лабораторных импедансных систем сбора данных. Одной из основных характеристик всех импедансных томографов является тип источника прикладываемого воздействия. Источник тока является более предпочтительным, так как обеспечивает независимый от величины нагрузки выходной ток (величина нагрузки в данном случае определяется внутренней структурой исследуемого биологического объекта и эффектами электрод—кожа). Некоторые разработанные системы используют один источник тока, так как такая реализация является проще (например, системы, разработанные в Университете Sheffield, Великобритания; Институте радиоэлектроники РАН, Россия), в то время как другие системы имеют несколько источников тока (Университет Oxford Brookes, Великобритания; Институт Rensselaer Polytechnic, США; Университет Dartmouth, США). Более сложная схемотехника с несколькими источниками тока позволяет получать изображения лучшего качества. Разработаны принципы, по которым определяются величины прикладываемых токов, в основе которых лежит идея максимизации различимости двух распределений проводимости (или диэлектрической проницаемости) [1].

Предъявляемые требования точности регистрации данных для импедансных томографов очень высоки, поэтому выходной импеданс систем с источниками прикладываемого тока должен быть очень высоким, чтобы избежать проблем с синфазными токами. Для этого часто разрабатываются специальные схемы компенсации [например, 2]. Альтернативой являются системы с источниками прикладываемого напряжения [например, 3]. Недостатком такого подхода является большая зависимость качества получаемого изображения от точности расположения электродов и невозможности оценить эффекты на границе электрод — кожа. Также необходимы одновременные точные измерения прикладываемых токов в каждом отведении, что усложняет схемотехнику систем.

Техническое задание на разработку измерительной импедансной системы

Разрабатываемая измерительная система предназначена для построения статического, дифференциального объекта с частото-зависимыми резистивными и диэлектрическими свойствами. Поэтому к основным требованиям относятся простота реализации и максимально достижимая

* Научный руководитель — доктор физ.-мат. наук, профессор Московского государственного университета приборостроения и информатики *А. С. Кравчук*.

точность получения экспериментальных данных. Требования к скорости получения данных не являются критическими. Также система должна обеспечивать возможность расширения функционала до получения динамических абсолютных изображений.

Принципы построения разработанной системы

Система состоит из двух больших частей: 1) программного и аппаратного обеспечения для проведения измерений и 2) программного обеспечения для получения реконструированных изображений. Измерительная часть реализована с помощью G-языка программирования LabVIEW 8.0 и платы PCI 6052E (National Instruments, США). Подробную спецификацию на плату PCI 6052E можно найти на сайте фирмы-производителя www.ni.com. Программное обеспечение для реконструкции реализовано с помощью функций MatLab 2007a. В данной статье описана измерительная часть разработанной системы.

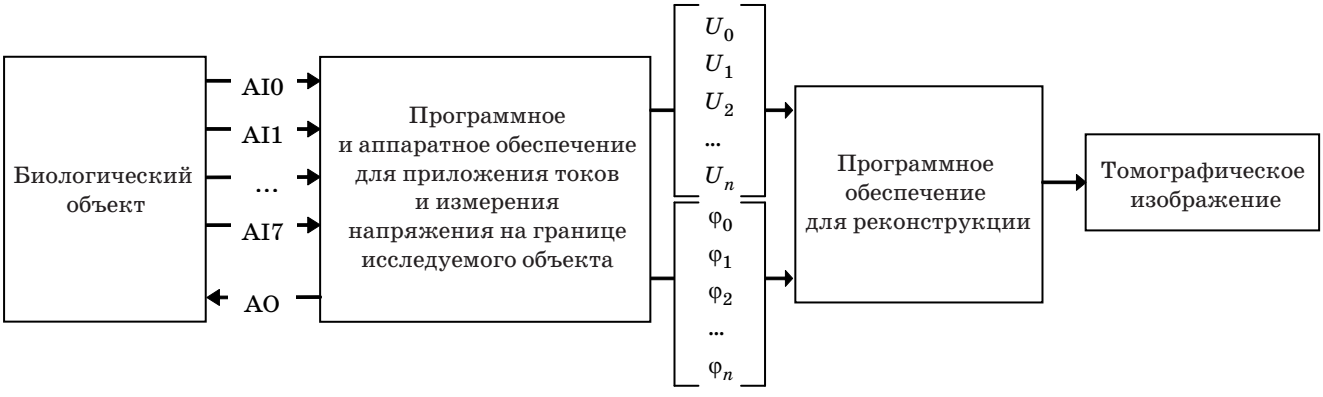
В настоящий момент разработанная измерительная система (рис. 1) используется для проведения измерений на лабораторном фантоме, но конструктивно позволяет проводить измерения и на реальном биологическом объекте.

Система имеет 8 отведений для одновременных измерений. Для экспериментов на фантоме и для получения статических изображений количество отведений может быть увеличено в несколько раз последовательным подключением отведений к следующим измерительным электродам.

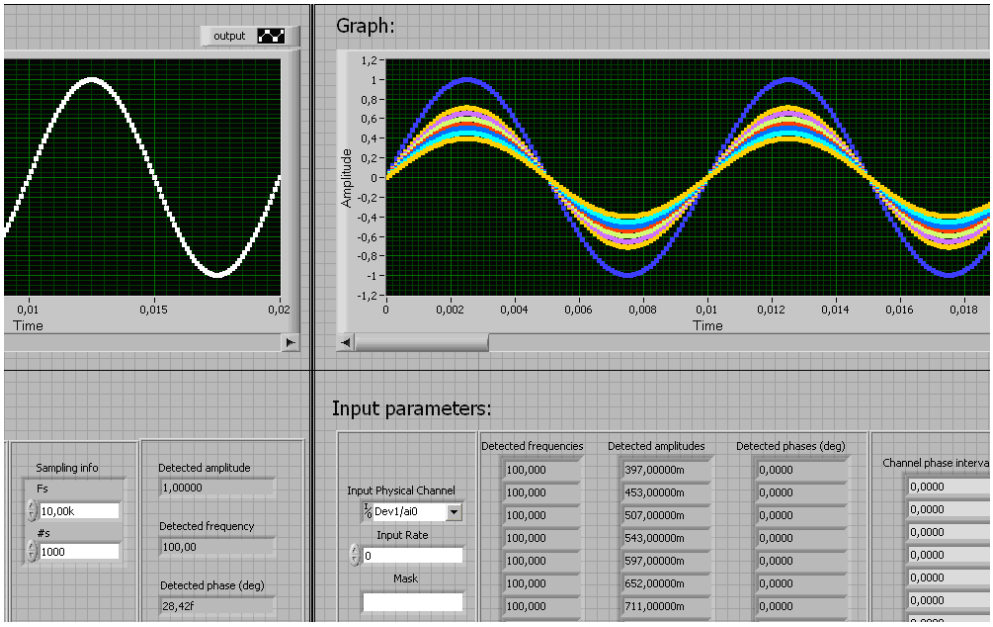
Для реконструкции биологического объекта необходимо измерять амплитуды напряжений на поверхности объекта (как характеристику резистивных свойств объекта) и сдвиг фаз (как характеристику диэлектрических свойств). Вследствие требований простоты реализации система имеет один канал для прикладываемого воздействия в виде сигнала синусоидального напряжения, генерируемого платой. Преимуществом такой схемотехники является возможность синхронизировать прикладываемое воздействие и регистрируемые сигналы с помощью функций LabVIEW. Недостатками же является необходимость измерения тока прикладываемого воздействия в каждой серии измерений (так как выходной ток источника напряжения зависит от нагрузки) и ограничение частот прикладываемого воздействия до 2–3 кГц (такая верхняя граница определяется техническими характеристиками самой платы — другие модели плат могут обеспечивать более высокие частоты прикладываемого воздействия). Однако независимо от максимально возможной частоты выходного сигнала, генерируемой платой, необходимо помнить, что исходно сигнал формируется в цифровом виде и только затем с помощью цифрового преобразователя (ЦАП) преобразуется в выходной аналоговый. Как следствие, принципиальной является частота дискретизации сигнала, определяемая характеристиками ЦАП платы (для PCI 6052E она составляет порядка 44 кГц), для формирования максимально гладкого выходного аналогового сигнала[1].

Часть пользовательского графического интерфейса представлена на рис. 2. Кривая слева показывает амплитуду приложенного сигнала, кривые справа — амплитуды регистрируемых сигналов. Для проведения тестовых измерений отведения подключены так, чтобы сформировался электрический делитель напряжения (из предположения, что тестовая среда обладает только резистивными свойствами), и каждое последующее отведение регистрировало сигнал меньшей амп-

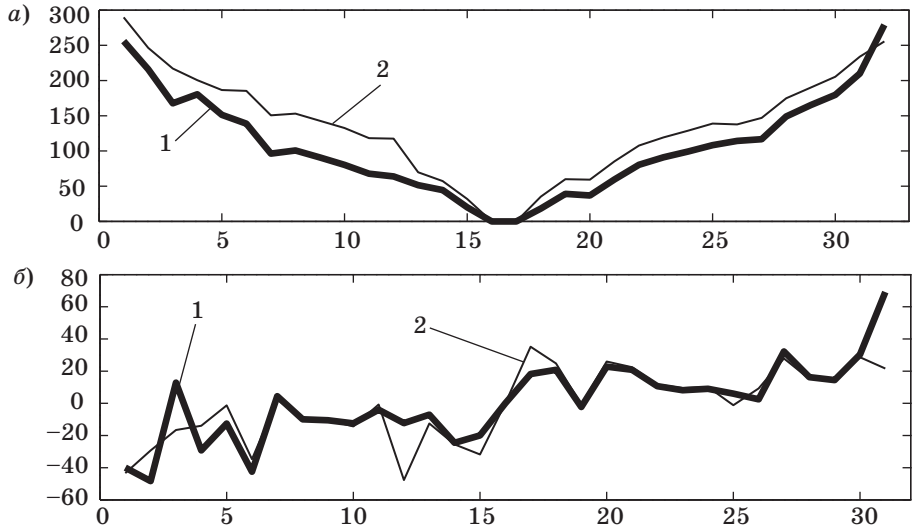
[1] В общем случае для формирования гладкого сигнала большей частоты возможно использовать сглаживающие схемы, в простейшем случае — одиночные конденсаторы.



■ ***Рис. 1.*** *Принципиальная схема системы*



■ ***Рис. 2.*** *Передняя панель пользовательского интерфейса с графическим изображением амплитуд регистрируемых сигналов*



■ ***Рис. 3.*** *Амплитуды измеренных сигналов в схеме с 32 измерительными электродами: а — абсолютные измеренные величины; б — разности между соседними отведениями: 1 — однородная среда; 2 — среда с неоднородностью*

литуды, чем предыдущее отведение. Графики измеренных сигналов по отведениям (32 измерения — абсолютные значения и 31 разностная величина) представлены на рис. 3.

Технические характеристики разработанной системы

Основное назначение разработанной системы — изучение свойств среды (резистивных и диэлектрических), поэтому определяющими параметрами являлись точность измерений и простота системы. Система предназначена для получения статических изображений (для построения динамических изображений необходимы большее количество измерительных каналов, более скоростной аналого-цифровой преобразователь (АЦП) и др.), поэтому требования к скорости АЦП — минимальные.

Любая измерительная система вносит систематические (которые возможно и необходимо калибровать) и случайные погрешности измере-

ния в получаемые данные. Необходимо различать абсолютную точность каждого канала и относительную точность между каналами. Второе более критично (т. е., например, зарегистрированные данные во всех каналах на 1 % выше их реальных значений вносят меньшую ошибку в реконструируемое изображение, нежели данные, на 1 % несогласованные между каналами).

Частота оцифровывания регистрируемого сигнала — максимальное значение для платы — 333 кГц, поэтому каждый канал (при одновременном измерении на восьми каналах) имеет максимальную частоту оцифровывания, равную 41,6 кГц.

Диапазон прикладываемого воздействия — конструктивно плата обеспечивает ±10 В, в эксперименте был выбран переменный сигнал напряжением 3 В.

Выходной импеданс системы равен 1,7–2,0 Ом и может считаться пренебрежимо малым. Таким образом, источник напряжения (реализованный через плату сбора данных) может рассматриваться как идеальный.

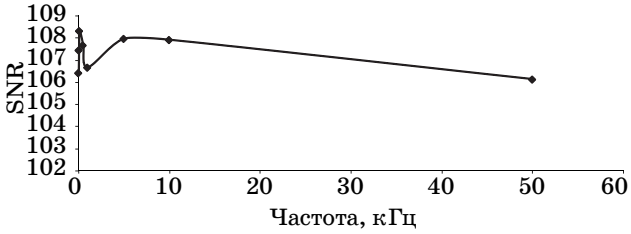
Входной импеданс равен около 150 МОм, что дает возможность достигать 16-разрядной точности.

Для оценки *соотношения сигнал/шум* была проведена серия из 50 измерений сигнала напряжением 3 В без нагрузки для нескольких частот. Значение сигнал/шум

$$\mathrm{SNR} = 10\log_{10}\left(\frac{\sum_{n=1}^{N} V_n^2}{\sum_{n=1}^{N}(V_n - \bar{V})^2}\right),$$

где V_n — величина сигнала n-го измерения; $\bar{V}$ — среднее значение измерений. Соотношение сигнал/шум как функция частоты показано на рис. 4.

Перекрестные помехи — конструктивно плата имеет один АЦП, который последовательно переключается между всеми измерительными каналами, поэтому в каждый момент времени электрическая цепь замкнута только для одного измерительного канала, что делает перекрестные помехи незначительными.



■ ***Рис. 4.*** *Соотношение сигнал/шум как функция частоты*

Реализация измерительной системы в G-коде

Разработанная система имеет переднюю панель пользовательского интерфейса и сам программный код.

Функционально и визуально передняя панель имеет две равные части.

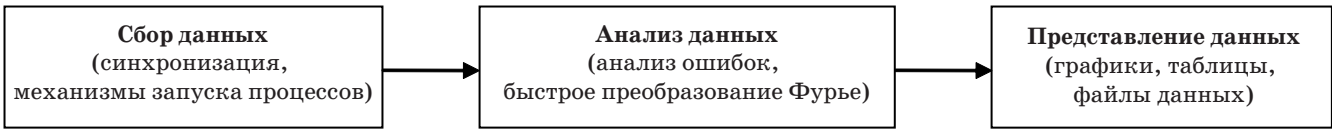
1. *Установка и отображение выходных параметров* (прикладываемое воздействие к биологическому объекту). Конструктивно плата 6052E может давать на выход только напряжение (т. е. реализована схема единственного источника напряжения), поэтому ток на выходе измеряется на отдельном резисторе (и варьируется в проведенных экспериментах в пределах 19–25 мА). Устанавливаемыми параметрами выходного сигнала платы являются частота выборки (*Fs*) (согласно теореме Котельникова) и общее количество сформированных точек (*#s*). Для визуального контроля над выходным сигналом реализовано его графическое отображение и независимое определение параметров.

2. *Установка и отображение входных параметров* (измеряемые величины). Измеренные напряжения после предварительной обработки используются в программном обеспечении для реконструкции (описание математических принципов реконструкции изображений выходит за рамки данной статьи). Одновременно плата дает возможность регистрировать данные с восьми входных каналов (система имеет 2 отведения для измерения тока и 6 отведений для измерения непосредственно напряжений на границе вследствие наличия внутренней неоднородной структуры биологического объекта).

Код на LabVIEW имеет 3 блока (рис. 5), позволяющих реализовать взаимодействие компьютера, платы сбора данных и физического сигнала от биологического объекта — сбор данных, анализ данных, представление данных.

В импедансной томографии при учете диэлектрических свойств биологического объекта необходима реализация временной синхронизации входного и выходного сигналов. Вследствие требований к высокой точности измерений разработанная система имеет аппаратную синхронизацию и механизмы пуска процессов.

Экспериментальные данные для реконструкции имеют величины амплитуд напряжений (резистивные свойства объекта) и сдвига фаз (диэлектрические свойства). Так как конструктивно плата имеет 8 входных отведений и 1 АЦП, по-



■ ***Рис. 5.*** *Блок-схема программной реализации*

следовательно переключаемый между этими каналами, временная задержка записи данных при максимально допустимой частоте оцифровывания и использовании всех каналов составляет порядка $3{,}1 \cdot 10^{-6}$ с, измеряется для каждой серии экспериментов и учитывается при последующей обработке полученных данных.

Выводы

Разработанная система позволяет получать статические дифференциальные изображения (изображение является разностью между однородной средой и средой с включением) для резистивных среды и неоднородностей (рис. 6, *а*, *б*, см. с. 3 обложки).

Разработанная система и проведенные тестовые эксперименты являются своего рода пилотными и подразумевают дальнейшую работу по улучшению качества получаемых изображений.

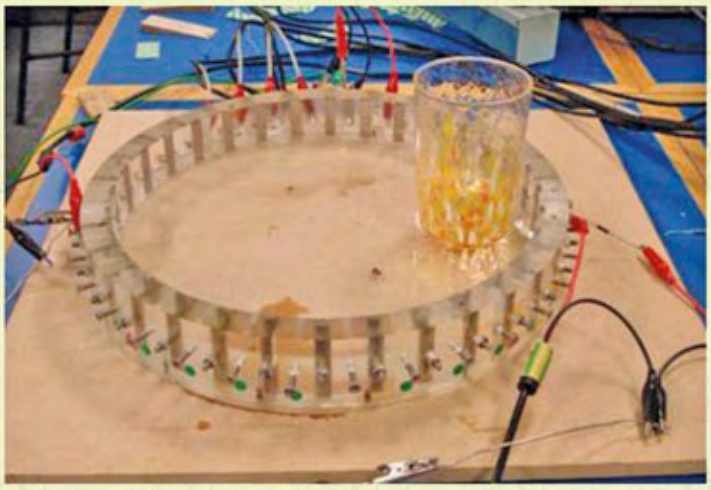
Автор благодарит профессора Криса МакЛауда (C. McLeod, Oxford Brookes University, Великобритания) за помощь в подготовке статьи.

Литература

1. **D. Isaacson.** Distinguishability of conductivities by electric current computed tomography // IEEE Trans. Med. Imaging. 1986. N MI-5. P. 92–95.
2. **A. S. Ross, G. J. Saulnier, J. C. Newell, D. Isaacson.** Current source design for electrical impedance tomography // Physiol. Meas. 2003. N 24. P. 509–516.
3. **G. J. Saulnier, A. S. Ross, N. Liu.** A high precision voltage source for EIT // Physiol. Meas. 2006. N 27. P. 221–236.

Иллюстрация к статье
А. Г. Михайловой.
«Аппаратная реализация электрического импедансного томографа», с. 75.

а)



б)

Рис. 6. Тестовая реконструкция:
а – проводящая среда (водный солевой раствор) с неоднородностью, проводимость которой равна нулю (пустой стакан); б – реконструированное изображение

ВЛАДИМИР БОРИСОВИЧ ЯКОВЛЕВ — УЧЕНЫЙ, ПЕДАГОГ И ОРГАНИЗАТОР. К 75-ЛЕТИЮ СО ДНЯ РОЖДЕНИЯ

В. Б. Яковлев родился в Москве 11 октября 1933 года. Первое знакомство Владимира Борисовича с кафедрой автоматики и телемеханики ЛЭТИ состоялось в октябре 1956 года — на четвертом курсе. С этого времени началась его научная работа, которая под руководством А. А. Вавилова продолжалась до октября 1983 года — до внезапной кончины Александра Александровича в день пятидесятилетия В. Б. Яковлева. Александр Александрович стал учителем и ближайшим другом В. Б. Яковлева. Своим примером он пробудил в молодом ученом жгучий интерес к теории автоматического управления, которую тот, так же как и А. А. Вавилов, полюбил и сделал делом своей жизни.

В 1965 году В. Б. Яковлев защищает кандидатскую диссертацию на тему «Многоканальные системы автоматического регулирования». Он стал создателем научной школы ЛЭТИ в области теории и практики многоканальных систем автоматического управления, которая впоследствии сформировала научные основы структурной и технической организации многоканальных систем управления технологическими процессами и сложными объектами на базе микропроцессоров. В 70-е годы А. А. Вавилов, В. Б. Яковлев и В. А. Терехов организовали при кафедре отраслевую лабораторию систем и средств контроля и управления Минприбора, где были разработаны принципы построения многоканальных регуляторов общепромышленного назначения в составе средств Государственной системы приборов, внедренных в серийное производство.

В 1971 году по инициативе А. А. Вавилова на кафедре автоматики и телемеханики появилась новая специальность 0646 — «Автоматизированные системы управления». В. Б. Яковлев был руководителем цикла по управлению, и поэтому ему поручили организацию подготовки по этой специальности. Кафедрой, в дальнейшем получившей название кафедра автоматики и процессов управления, Владимир Борисович и заведовал с 1983 года.

В 1978 году В. Б. Яковлев защитил докторскую диссертацию на тему «Разработка методов расчета нелинейных импульсных систем и многоканальных регуляторов». В диссертации была разработана теория систем многоканального управления, являющаяся научной основой структурной и технической реализации распределенных систем управления сложными объектами, в которых необходимо управлять большим числом переменных или параметров. В диссертации также получен ряд существенных результатов, связанных с развитием частотных и временных методов анализа и синтеза нелинейных дискретных систем.

Научная деятельность В. Б. Яковлева охватывает не только указанные выше вопросы, но и широкий круг фундаментальных и прикладных проблем теории и практики автоматического управления, автоматизированного управления технологическими процессами, автоматизации исследования и проектирования сложных динамических систем. Основными направлениями его научной деятельности являются теория и практика дискретных систем управления, методы автоматизированного исследования сложных динамических систем. Благодаря трудам А. В. Фатеева и А. А. Вавилова на кафедре сложилось направление частотных методов исследования линейных и нелинейных систем автоматического управления. В. Б. Яковлев получил ряд существенных результатов, связанных с развитием частотных методов анализа и синтеза в теории дискретных систем. В рамках этой теории им разработан метод расчета импульсных систем, основанный на замене малых постоянных времени эквивалентным запаздыванием. Разработаны частотные и аналитические методы исследования абсолютной устойчивости и периодических режимов в нелинейных дискретных системах.

В. Б. Яковлев проводил большую научно-организационную работу, являясь, в частности, в течение многих лет (с 1983 по 1998 год) председателем Ленинградской территориальной группы Национального комитета по автоматическому управлению.

В. Б. Яковлев является автором и соавтором более 250 печатных работ, среди которых четыре учебника по теории автоматического управления с грифом Минобразования. Под его руководством выполнено более 80 НИР и ОКР для различных предприятий народного хозяйства. Как научный руководитель В. Б. Яковлев подготовил 47 кандидатов технических наук и как консультант — семь докторов технических наук.

С 1967 года В. Б. Яковлев был ученым секретарем научно-методического совета по специальности 0606 «Автоматика и телемеханика», а с 1984 года — его председателем. В 1973 году по предложению В. Б. Яковлева и Г. К. Круга принимается решение о подготовке к открытию в рамках специальности 0606, кроме специализаций

«Элементы и устройства автоматики и телемеханики» и «Схемы и системы автоматики и телемеханики», двух новых специализаций — «Автоматизированные системы управления технологическими процессами» и «Автоматизированные системы научных исследований и испытаний», а в 1982 году по предложению В. Б. Яковлева и В. Д. Ефремова — специализация «Системы управления гибких автоматизированных производств». По предложению В. Б. Яковлева, в 1984 году было принято решение о новом наименовании специальности — «Автоматика и управление в технических системах».

В дальнейшем по инициативе В. Б. Яковлева была образована новая группа 21.00 «Автоматизация и управление» с девятью специальностями («Автоматика и управление в технических системах», «Автоматизация технологических процессов и производств», «Автоматические системы управления энергетическими установками», «Автоматика и телемеханика на железнодорожном транспорте», «Электропривод и автоматизация промышленного оборудования», «Робототехнические системы», «Системы автоматического управления летательными аппаратами», «Корабельные системы управления», «Автоматические навигационные приборы и устройства»), основой которых является автоматическое и автоматизированное управление.

В 1992 году в ряде вузов страны началась подготовка бакалавров и магистров техники и технологии. По направлению 550200 «Автоматизация и управление» в составе учебно-методического объединения по специальностям в области автоматики, электроники, микроэлектроники и радиотехники был сформирован координационный научно-методический совет, председателем которого стал В. Б. Яковлев, а ученым секретарем — доцент ЛЭТИ Н. Н. Кузьмин.

В 1993 году по распоряжению Госкомитета РФ по высшему образованию в учебно-методическом объединении по автоматике, электронике, микроэлектронике и радиотехнике под руководством В. Б. Яковлева началась разработка первого поколения государственных образовательных стандартов высшего профессионального образования подготовки бакалавров и магистров по направлению «Автоматизация и управление» и инженеров по специальности «Управление и информатика в технических системах». Эти стандарты по бакалаврам, инженерам и магистрам были утверждены в 1993, 1995 и 1996 годах соответственно. При этом учебный план подготовки магистров включал 20 различных программ.

С 1982 по 2002 год В. Б. Яковлев был председателем специализированного совета по защитам докторских диссертаций в области теории управления и автоматизированных систем обработки информации и управления, а с 1983 по 1997 год — членом экспертного совета ВАК по управлению, информатике и вычислительной технике. По поручению ВАК кафедра автоматики и процессов управления ЛЭТИ приняла участие в разработке паспортов и программ кандидатских экзаменов для специальностей научных работников «Управление в технических системах», «Автоматизированные системы управления технологическими процессами и производствами» и «Автоматизированные системы управления».

В 1986 году в связи со 100-летием ЛЭТИ за заслуги в области развития науки и образования В. Б. Яковлев был награжден орденом Дружбы народов.

В 1994 году в связи с 60-летием за успехи в области науки и образования В. Б. Яковлеву было присвоено почетное звание «Заслуженный деятель науки и техники Российской Федерации».

В 2003 году решением ученого совета ЛЭТИ В. Б. Яковлеву присвоено почетное звание «Заслуженный профессор ЛЭТИ». В 2005 году он написал и опубликовал книгу «Мои воспоминания» (http://is.ifmo.ru/books/_2007_09_26_jakovlev.pdf), которая по существу является изложением истории кафедры и развития специальности от автоматики и телемеханики к управлению и информатике.

Выпускник кафедры автоматики и телемеханики (1971 г.), заведующий кафедрой технологии программирования Санкт-Петербургского государственного университета информационных технологий, механики и оптики, доктор техн. наук, профессор А. А. Шалыто

СВЕДЕНИЯ ОБ АВТОРАХ

БЕЛОВ
Борис
Петрович

Профессор, заведующий кафедрой морских информационно-измерительных систем Санкт-Петербургского государственного морского технического университета.
В 1975 году окончил Ленинградский кораблестроительный институт.
В 1989 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором 110 научных публикаций.
Область научных интересов — гидролокация, пеленгование, шумы моря, антенные решетки и автономные необитаемые информационные системы.

ВЕДЕРНИКОВ
Юрий
Вадимович

Доцент, старший преподаватель кафедры систем управления ракет Михайловской военной артиллерийской академии.
В 1992 году окончил Саратовское высшее военное командно-инженерное училище ракетных войск им. А. И. Лизюкова.
В 2001 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 56 научных публикаций.
Область научных интересов — системный анализ, теория принятия решений, исследование операций, инновационные технологии управления, векторная оптимизация сложных технических систем, принятие решений в условиях неопределенности и риска, интервальный анализ.

КИРИЛЛОВ
Александр
Николаевич

Доцент кафедры высшей математики Санкт-Петербургского государственного технологического университета растительных полимеров. Почетный работник высшего профессионального образования РФ.
В 1976 году окончил Ленинградский государственный университет им. А. А. Жданова по специальности «Прикладная математика».
В 1983 году защитил диссертацию на соискание ученой степени кандидата физико-математических наук.
Является автором более 50 научных публикаций.
Область научных интересов — теория управления нелинейными динамическими системами, математическое моделирование экономических и экологических систем.

БОЖОКИН
Сергей
Валентинович

Доцент кафедры теоретической физики Санкт-Петербургского государственного политехнического университета.
В 1974 году окончил Ленинградский политехнический институт им. М. И. Калинина.
В 1978 году защитил диссертацию на соискание ученой степени кандидата физико-математических наук.
Является автором 58 научных публикаций, в том числе пяти книг.
Область научных интересов — мультифракталы, вейвлеты, нестационарные сигналы в биологии и медицине.

ДОРОНИН
Станислав
Евгеньевич

Аспирант кафедры автоматизированных систем обработки информации и управления Санкт-Петербургского государственного электротехнического университета «ЛЭТИ».
В 2008 году окончил Санкт-Петербургский государственный электротехнический университет «ЛЭТИ».
Является автором трех научных публикаций.
Область научных интересов — эллиптическая криптография.

МИХАЙЛОВА
Анна
Геннадьевна

Соискатель кафедры биомедицинской техники Московского государственного университета приборостроения и информатики.
В 2004 году окончила Московский государственный университет приборостроения и информатики.
Область научных интересов — томография, обратные некорректные задачи, цифровая обработка сигналов.

МОЛДОВЯН Николай Андреевич

Профессор, главный научный сотрудник научного филиала ФГУП НИИ «Вектор» — специализированного центра программных систем «Спектр». Заслуженный изобретатель РФ.
В 1975 году окончил Кишиневский политехнический институт по специальности «Полупроводниковые приборы».
В 2001 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 200 научных публикаций и 50 запатентованных изобретений.
Область научных интересов — информационная безопасность, криптография.

САМОХИНА Марина Андреевна

Ассистент кафедры радиотехники Московского физико-технического института.
В 2005 году окончила Московский физико-технический институт по специальности «Прикладные математика и физика».
Является автором 10 научных публикаций
Область научных интересов — помехоустойчивое кодирование, криптография, криптосистемы с открытым ключом, инфраструктура открытых ключей, опции безопасности баз данных.

СЕМЕНОВ Николай Николаевич

Инженер-разработчик НТЦ «Протей», по совместительству преподаватель кафедры морских информационно-измерительных систем Санкт-Петербургского государственного морского технического университета, соискатель ученой степени кандидата технических наук.
В 1998 году окончил Санкт-Петербургский государственный морской технический университет по специальности «Роботы и робототехнические системы».
Является автором 26 научных публикаций.
Область научных интересов — теория распознавания образов, оптимальный прием сигналов и их обнаружение, обработка, сжатие, распознавание и синтез речи, гидроакустика, цифровая обработка сигналов.

СИНЕВ Валерий Евгеньевич

Аспирант кафедры автоматизированных систем обработки информации и управления Санкт-Петербургского государственного электротехнического университета «ЛЭТИ».
В 2008 году окончил Санкт-Петербургский государственный электротехнический университет «ЛЭТИ».
Является автором двух научных публикаций.
Область научных интересов — алгоритмы цифровой подписи на основе матриц над конечными полями.

СТЕПАНЯН Карлен Багратович

Начальник отдела управления операционного обслуживания ОАО «Управляющая компания «Арсагера», аспирант кафедры прикладной математики Санкт-Петербургского государственного политехнического университета.
В 2003 году окончил Санкт-Петербургский государственный политехнический университет.
Является автором трех научных публикаций.
Область научных интересов — спецификация и построение диаграмм.

СУВОРОВ Николай Борисович

Профессор кафедры биомедицинской электроники и охраны среды Санкт-Петербургского государственного электротехнического университета «ЛЭТИ», заведующий лабораторией нейроэкологии НИИ экспериментальной медицины РАМН, действительный член Академии медико-технических наук, член Президиума Северо-Западного отделения Академии медико-технических наук.
В 1964 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина).
В 1993 году защитил диссертацию на соискание ученой степени доктора биологических наук.
Является автором более 250 научных публикаций.
Область научных интересов — управление в медико-биологических системах, синтез биотехнических систем, анализ сигналов.

ТЕТЕРИН Дмитрий Павлович

Главный конструктор ОАО «КБ Электроприбор» (г. Саратов).
В 1992 году окончил Саратовское высшее военное командно-инженерное училище Ракетных войск, в 1994 году — Поволжскую академию государственной службы, в 1997 году — Михайловскую артиллерийскую академию.
В 2004 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 70 научных публикаций, в том числе 12 патентов и свидетельств на изобретение (полезную модель), двух свидетельств об официальной регистрации топологии интегральной микросхемы, девяти свидетельств об официальной регистрации программы для ЭВМ и одной монографии.
Область научных интересов — математическое моделирование, компьютерная математика, теория обыкновенных дифференциальных уравнений.

ТИХОНОВ Эдуард Прокофьевич

Доцент кафедры биомедицинской электроники и охраны среды Санкт-Петербургского государственного электротехнического университета «ЛЭТИ», член-корреспондент Метрологической академии.
В 1963 году окончил Ленинградский институт авиационного приборостроения.
В 1968 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 190 научных публикаций, в том числе более 60 авторских свидетельств и патентов на изобретения.
Область научных интересов — кибернетика, информатика, моделирование, информационно-измерительные системы, биомедицинская инженерия.

ШИШЛАКОВ Владислав Федорович

Профессор кафедры информационных технологий в электромеханике и робототехнике Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1982 году окончил Ленинградский институт авиационного приборостроения.
В 2002 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 100 научных и учебно-методических публикаций, в том числе трех монографий.
Область научных интересов — синтез нелинейных систем автоматического управления с различными видами модуляции сигнала.

ТАЗЕТДИНОВ Андрей Дамирович

Директор центра информационных технологий Международного банковского института.
В 2002 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения по специальности «Автоматизированные системы обработки информации и управления».
В 2006 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 24 научных публикаций, двух монографий и одного авторского свидетельства.
Область научных интересов — автоматизированные обучающие системы, компьютерные сети, интеграция программного обеспечения с применением SOA.

ЦВЕТКОВ Сергей Александрович

Ассистент кафедры информационных технологий в электромеханике и робототехнике Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2004 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения.
Является автором 20 научных публикаций.
Область научных интересов — синтез нелинейных импульсных систем автоматического управления.

ШИШЛАКОВ Дмитрий Владиславович

Аспирант кафедры информационных технологий в электромеханике и робототехнике Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2006 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения.
Является автором 20 научных публикаций.
Область научных интересов — синтез нелинейных многосвязных систем автоматического управления.

УДК 681.314

Модифицированные алгоритмы и классификация аналого-цифровых преобразователей. Часть 1: Параллельно-последовательные алгоритмы

Тихонов Э. П. Информационно-управляющие системы, 2009. № 1. С. 2–9.

Предложено аналитическое описание различных модификаций алгоритмов аналого-цифровых преобразователей, включая мажоритарный и нейроноподобный принцип обработки информации, на базе которых выполнен сравнительный анализ их свойств, доведенных до численных результатов, и разработана классификационная схема аналого-цифровых преобразователей.

Ключевые слова — преобразователь аналог-код, параллельно-последовательный алгоритм, древовидный фрактал, конвейерный преобразователь, параллельный преобразователь.

Список лит.: 6 назв.

UDK 681.314

The modified algorithms and classification of analog-digital converters. Part 1: Parallel-serial algorithms

Tikhonov E. P. IUS, 2009. N 1. P. 2–9.

Various algorithms and block diagrams of analog-digital converters are presented, and their comparative analysis is performed. Numerical and graphic results of researches of the suggested algorithms are completed. A classification circuit of analog-digital converters is developed.

Keywords — analogue-code converter, parallel-serial algorithm, treelike fractal, conveyor converter, parallel converter.

Refs: 6 titles.

УДК 681.3.07

Синтез требований к бортовому информационно-измерительному и моделирующему комплексу

Тетерин Д. П. Информационно-управляющие системы, 2009. № 1. С. 10–14.

Изложены основные понятия и определения теории номенклатурного нормирования и вариант синтеза технических требований по назначению бортового информационно-измерительного и моделирующего комплекса.

Ключевые слова — технические требования, техническое задание на проектирование, математическое моделирование.

Список лит.: 7 назв.

UDK 681.3.07

Synthesis of requirements for the on-board information-measuring and modeling complex

Teterin D. P. IUS, 2009. N 1. P. 10–14.

The basic conceptual apparatus for the nomenclature normalization theory and the variant of requirements specifications synthesis for the information-measuring and modeling complex destination are set out in this article.

Keywords — engineering requirements, project requirements specification, mathematical modeling.

Refs: 7 titles.

УДК 681.5.013

Исследование анормальных режимов работы автономной электроэнергетической установки

Шишлаков В. Ф., Шишлаков Д. В., Цветков С. А. Информационно-управляющие системы, 2009. № 1. С. 15–19.

Приводятся результаты исследований анормальных режимов работы автономной электроэнергетической установки с синтезированными обобщенным методом Галеркина параметрами при внешних возмущающих воздействиях на входах приводного двигателя и синхронного генератора.

Ключевые слова — автономная электроэнергетическая установка, режимы работы, внешние воздействия.

UDK 681.5.013

A study of abnormal modes of operation of the autonomous electro power system

Shishlakov V. F., Shishlakov D. V., Tsvetkov S. A. IUS, 2009. N 1. P. 15–19.

The results of a research of abnormal modes of operation of the autonomous electro power system that synthesizes the parameters, calculated with external disturbing influence on the input of the driving engine and synchronous generator, employing the generalized Galerkin method, are presented in his paper.

Keywords — autonomous electro power system, modes of operation, external influence.

УДК 519.95

Метод динамической декомпозиции в моделировании систем управления со структурными изменениями

Кириллов А. Н. Информационно-управляющие системы, 2009. № 1. С. 20–24.

Предлагается метод построения математических моделей сложных систем с изменяющейся в процессе функционирования структурой. Вводится динамическая система, состоящая из переменного количества подсистем. На ее основе моделируется процесс инвестирования динамической экономической системы, описывающей крупный промышленный комплекс.

Ключевые слова — динамическая система управления, декомпозиция, структура, переменная размерность, экономическая система, моделирование динамики.

Список лит.: 10 назв.

UDK 519.95

The dynamic decomposition method in control systems modeling with structural variations

Kirillov A. N. IUS, 2009. N 1. P. 20–24.

A new approach to the mathematical modeling of complex systems with varying structure is proposed. A dynamic system that consists of variable number of subsystems is introduced. Employing this system, an investment process of dynamic economic system, describing a large industrial complex, is modeled.

Keywords — dynamic control system, decomposition, structure, variable dimension, economic system, dynamics modeling.

Refs: 10 titles.

УДК 004.434

Использование языка описания диаграмм

Степанян К. Б. Информационно-управляющие системы, 2009. № 1. С. 25–32.

Обсуждается практическое применение языка DiaDeL для описания графо-подобных диаграмм на примере диаграмм состояний. Приводится пример известной диаграммы состояний телефона, автоматически построенной по описанию на предложенном языке. Язык DiaDeL позволяет формально определить графический синтаксис (нотацию) диаграмм заданного типа и связать нотацию с семантикой, заданной в форме набора классов.

Ключевые слова — графический язык, абстрактный синтаксис, метамодель, визуализация диаграмм, диаграмма состояний.

Список лит.: 9 назв.

UDK 004.434

Diagram definition language application

Stepanyan K. B. IUS, 2009. N 1. P. 25–32.

The paper reviews a practical application of the Diagram Definition Language (DiaDeL) language using description of the statechart as a running example. A well known instance of the telephone statechart is provided as an example of automatically generated diagram by its specification. The DiaDeL language allows to specify a graphical notation for the graph like diagram and bind it to semantics. Semantics is defined as a set of classes.

Keywords — visual language, abstract syntax, metamodel, diagram visualization, statechart.

Refs: 9 titles.

УДК 681.3

Конечные расширенные поля для алгоритмов электронной цифровой подписи

Молдовян Н. А., Доронин С. Е., Синев В. Е. Информационно-управляющие системы, 2009. № 1. С. 33–40.

Описываются новые частные варианты реализации конечных расширенных полей, предназначенных для построения производительных алгоритмов электронной цифровой подписи. Показано, что новая форма представления конечных расширенных полей путем задания специальной операции умножения в конечном m-мерном векторном пространстве обеспечивает возможность эффективного распараллеливания вычислений, благодаря чему обеспечивается повышение производительности алгоритмов электронной цифровой подписи, основанных на конечных группах матриц и эллиптических кривых при их задании над конечными расширенными полями, представленными в новой форме.

Ключевые слова — эллиптические кривые, цифровая подпись, векторные конечные поля, конечные группы матриц.

Список лит.: 8 назв.

UDK 681.3

Finite extension fields for digital signature algorithms

Moldovyan N. A., Doronin S. E., Sinev V. E. IUS, 2009. N 1. P. 33–40.

Here we describe new particular variants for the implementation of the finite extension fields intended to construct computationally efficient digital signature (DS) algorithms. The new form of the finite extension fields is defined over the finite m-dimension vector space by special types of the multiplication operation which is suitable for efficient parallelization. Due to the last property, the performance the DS algorithms, based on elliptic curves (EC) and finite groups of matrices (FGM), can be significantly improved, while EC and FGM are defined over the finite fields represented in the new form.

Keywords — elliptic curves, digital signatures, vector finite fields, matrix finite groups.

Refs: 8 titles.

УДК 519.688

Применение модификации криптосистемы Ниддерайтера для защиты информации при передаче видеоизображений

Самохина М. А. Информационно-управляющие системы, 2009. № 1. С. 41–46.

Рассматривается построение модификации криптосистемы Нидеррайтера, основанной на матрице фробениусовского вида, а также применение данной криптосистемы для передачи и защиты меняющихся изображений. Сделано заключение о криптостойкости системы.

Ключевые слова — криптосистемы с открытым ключом, линейные коды, ранговые коды, криптоанализ, теория информации, защита информации, помехоустойчивое кодирование.

Список лит.: 9 назв.

UDK 519.688

Information security application of Niederreiter cryptosystem modification for video transmission

Samokhina M. A. IUS, 2009. N 1. P. 41–46.

Construction of Niederreiter cryptosystem modification based on a matrix of the Frobenius type is considered in this paper. This cryptosystem is applied for video transfer and security. A conclusion about cryptographic strength is made.

Keywords — public-key cryptography, error detection and correction, linear code, rank code, cryptanalysis, information theory, cryptography.

Refs: 9 titles.

УДК 681.883.022: 681.883.65

Выбор типа зондирующего сигнала для активного гидролокатора с помощью теории передачи данных в каналах связи

Семенов Н. Н., Белов Б. П. Информационно-управляющие системы, 2009. № 1. С. 47–51.

В современной гидролокации не существует однозначного решения, какой тип сигнала посылки является для данной системы оптимальным. Это связано с тем, что водная среда насыщена специфическими шумами, является неоднородной, допускает многолучевое распространение и отражение от дна и поверхности. В статье рассматривается один из возможных алгоритмов выбора оптимального для выбранной задачи типа сигнала посылки.

Ключевые слова — гидролокатор, эхо-сигнал, сигнал посылки, обнаружение, локация, сравнение сигналов, модуляция, шумы, информативность.

Список лит.: 12 назв.

UDK 681.883.022: 681.883.65

Choosing active sonar signal with data transmitting theory

Semenov N. N., Belov B. P. IUS, 2009. N 1. P. 47–51.

In modern sonar there is no unique solution as to what type of signal message is singularly accurate and optimum. This has to do with the fact that water is saturated with specific noise, it is heterogeneous, allows multiple-beam propagation, reflection from bottom and surfaces.

This article discusses one of the possible algorithms to choose an optimal sending signal for the particular task.

Keywords — sonar, echo signal, signal message, detection, location, signal comparison, modulation, noise, amount of information.

Refs: 12 titles.

УДК 303.732:[338+658.01](075.8)

Метод многокритериального предпочтения сложных систем

Ведерников Ю. В. Информационно-управляющие системы, 2009. № 1. С. 52–59.

Рассматривается задача определения отношений предпочтения на множестве сложных технических систем для случая, когда критерии оптимальности разнородны и могут быть заданы в частично формализованном, интервальном виде. Задача сводится к построению упорядоченного множества эффективных вариантов (кортежа предпочтений Парето) сложных систем. Предлагается метод решения, основанный на комплексном применении аксиоматических методов теории принятия решений, нечетких множеств и интервального анализа. Приведен численный пример.

Ключевые слова — техническая система, отношение предпочтения, интервальный анализ, векторная оптимизация.

Список лит.: 17 назв.

UDK 303.732:[338+658.01](075.8)

A method of multi-criterion prioritization of complex systems

Vedernikov Ju. V. IUS, 2009. N 1. P. 52–59.

A discussion of the task of defining the prioritizing ratio for the set of complex technical systems with the heterogeneous criterions of optimality, which could be preset as formalized within an interval, is set up. The task should be restricted to a composition of variety of effective alternatives (Pareto Cortege of Prioritizing) for complex systems. A method of solution based on the complex application of axiomatic methods of theory of decision-making, fuzzy sets analysis, and interval analysis is proposed. A numerical example is provided.

Keywords — vector optimization, technical system, interval analysis, prioritization ratio.

Refs: 17 titles.

УДК 004.588

Технология структурирования и визуализации учебной информации в репетиторских системах

Тазетдинов А. Д. Информационно-управляющие системы, 2009. № 1. С. 60–65.

Предлагаются: метод построения графов понятий учебного материала, реализующий механизм укрупнения информации за счет свертки нескольких понятий в одно; алгоритм автоматического разбиения графа понятий на подграфы с учетом требований когнитивной психологии на ограничение по количеству единиц информации, а также метод визуализации этих подграфов.

Ключевые слова — репетиторские системы, визуализация и структурирование учебной информации, автоматизированные диалоги.

Список лит.: 12 назв.

UDK 004.588

Technology of structuring and visualization of training information in tutorial systems

Tazetdinov A. D. IUS, 2009. N 1. P. 60–65.

The article suggests a method of constructing graphs of learning material concepts which provides the mechanism of information consolidation by convolving several concepts into one. An algorithm for automatic segmentation of the graph of concepts into subgraphs, taking into account the requirements of cognitive psychology for the limitation of units number of information and a method of visualization of these subgraphs, are proposed in the article.

Keywords — tutorial systems, visualization and structuring of training information, automated dialogues.

Refs: 12 titles.

УДК 612.82

Информативность колебательных переходных процессов в электроэнцефалограмме человека

Суворов Н. Б., Божокин С. В. Информационно-управляющие системы, 2009. № 1. С. 66–70.

Проанализированы нестационарные записи ЭЭГ, спектры мощности Фурье, локальные распределения энергии сигнала по частотам, исследованы скелетоны интегрального вейвлет-преобразования, изучена динамика проинтегрированных по основным ритмам ЭЭГ локальных плотностей колебаний, а также найдены характерные времена усвоения и забывания ритмов, вызванных фотостимуляцией.

Ключевые слова — вейвлет-анализ, электроэнцефалограмма, фотостимуляция.

Список лит.: 7 назв.

UDK 612.82

The information value of oscillating transients processes in human electroencephalogram

Suvorov N. B., Bozhokin S. V. IUS, 2009. N 1. P. 66–70.

This article analyses non-stationary EEG records, Fourier power spectrums, local distribution of the signal energy by frequencies; investigates the skeletons of integral transform wavelets; researches the dynamics of the EEG of local oscillation densities; and presents characteristic times of rhythm adoption and forgetting, caused by photostimulation.

Keywords — wavelet-analysis, electroencephalogram, photostimulation.

Refs: 7 titles.

УДК 621.317, 681.2

Аппаратная реализация электрического импедансного томографа

Михайлова А. Г. Информационно-управляющие системы, 2009. № 1. С. 71–75.

Приводится описание разработанной системы сбора данных на основе платы PCI 6052E, являющейся лабораторным электрическим импедансным томографом и предназначенной для изучения резистивных и диэлектрических свойств среды. Предварительно кратко рассмотрены общие принципы построения импедансных томографов и существующие реализации.

Ключевые слова — импедансный томограф, системы сбора данных.

Список лит.: 3 назв.

UDK 621.317, 681.2

Hardware implementation of an electrical impedance tomograph

Mikhailova A. G. IUS, 2009. N 1. P. 71–75.

This paper is devoted to the description of a laboratory developed electrical impedance tomograph, based on the PCI 6052E (NI, USA)board. The system is designed to investigate the resistive and dielectric media properties. At the beginning, the general principles and implementation of impedance tomographs are briefly reviewed.

Keywords — impedance tomograph, data acquisition systems.

Refs: 3 titles.

ISSN 1684-8853
9 771684 885009

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ