ISSN 1684–8853

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

2(33)/2008

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

2(33)/2008

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

РЕЦЕНЗИРУЕМОЕ ИЗДАНИЕ

Учредитель
ОАО «Издательство “Политехника”»

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

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

Журнал 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:
«Пресса России» — № 42476; «Роспечать» («Газеты и журналы») — № 15385.

ЛР № 010292 от 18.08.98.
Сдано в набор 01.03.08. Подписано в печать 15.04.08. Формат 60×84 1/8.
Бумага офсетная. Гарнитура SchoolBookC. Печать офсетная.
Усл. печ. л. 7,5. Уч.-изд. л. 9,0. Тираж 1000 экз. Заказ 179.

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 629.78

АЛГОРИТМ РАСПОЗНАВАНИЯ КОНФИГУРАЦИЙ ЗВЕЗД

С. Н. Воробьев,
канд. техн. наук, доцент
И. В. Лазарев,
студент
Санкт-Петербургский государственный университет аэрокосмического приборостроения

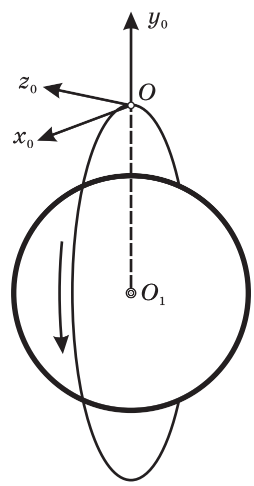
Предлагается процедура распознавания звезд, основанная на сравнении наблюдаемой конфигурации звезд с множеством эталонных конфигураций, задаваемых по каталогу. Показано, что при произвольной ориентации искусственного спутника Земли алгоритм вычисления угловых расстояний между звездами конфигурации и ускоренного перебора эталонов реализуется в режиме реального времени и не требует больших объемов памяти.

Введение

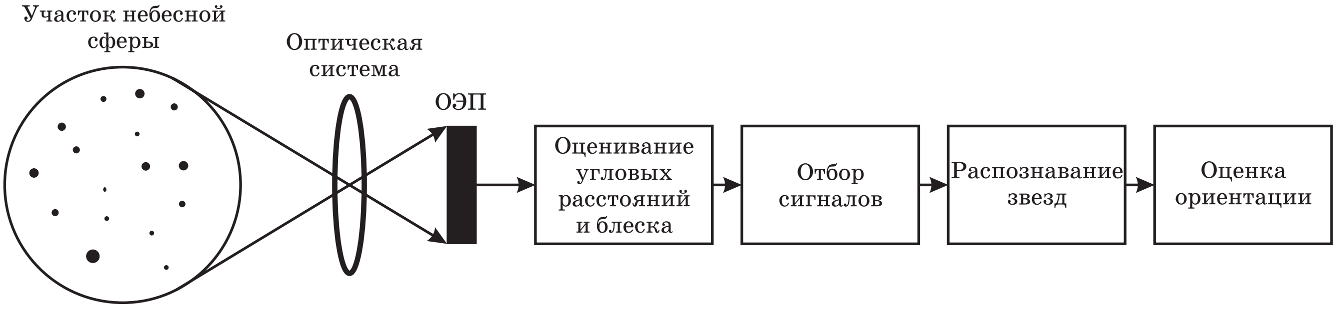
Управление угловым положением искусственного спутника Земли (ИСЗ) — его ориентация [1] — может базироваться на измерении угловых положений наблюдаемых звезд. Информационный подход к ориентации ИСЗ [2] предполагает выработку направляющих косинусов для определения матрицы перехода связанной (с ИСЗ) системы координат к базовой, имеющей общее начало со связанной системой. Кинематические параметры могут быть измерены при одновременной фиксации как минимум двух неколлинеарных векторов, ориентация которых относительно базовой системы координат известна [2, 3]. Фиксация линий визирования на две и более звезды позволяет рассчитать углы рыскания, тангажа и крена, характеризующие взаимное положение связанной и базовой систем координат. В качестве базовой, как правило, используется орбитальная система координат $Ox_0y_0z_0$ (рис. 1).

Оптические изображения наблюдаемых звезд, например ПЗС-матрицей (рис. 2), преобразуются в последовательности импульсных электрических сигналов, из которых отбираются подходящие для распознавания звезд.

Распознавание наблюдаемых звезд (их идентификация с указанными в каталогах [4]) позволя-



■ ***Рис. 1.*** *Орбитальная система координат*



■ ***Рис. 2.*** *Система ориентации ИСЗ* ет оценить текущую ориентацию ИСЗ и выработать управляющие сигналы для придания нужной. Стандартные оптико-электронные преобразователи *ОЭП* обеспечивают достаточные значения отношения сигнал/шум при наблюдении звезд $5–6^m$, общее количество которых велико (тысячи) [5, 6]. Распознавание нескольких наблюдаемых звезд на этом фоне при отсутствии априорных сведений возможно при использовании некоторой процедуры с приемлемыми вычислительной сложностью и требованиями к объему памяти.

Процесс ориентации может начинаться в произвольной точке орбиты при неизвестном угловом положении ИСЗ, т. е. ось оптической системы может быть направлена в любую точку сферы, а изображение участка звездного неба Θ может быть повернуто на любой угол относительно соответствующего стандартного изображения $\Theta_{кат}$ из звездного каталога. Одним из условий быстрого распознавания звезд является его инвариантность: нормализация Θ (преобразование Θ к $\Theta_{кат}$) должна быть исключена. В работе предлагается инвариантный к Θ алгоритм распознавания звезд в системе ориентации с погрешностями порядка угловых минут и оцениваются требования к памяти.

Алгоритм распознавания звезд

Наиболее достоверным методом распознавания групп звезд считается сравнение оценок угловых расстояний с их эталонами [6, 7]. Процедура распознавания базируется на инвариантности взаимных угловых расстояний α_{ij} между звездами с номерами i и j относительно углового положения идеальной оптической системы, в которой значения α_{ij} одинаковы в центре и на краях изображения. Звезды из каталога [4] ярче 5^m (всего 1620 звезд) нумеруются, образуя рабочий каталог. Угловые расстояния хранятся в градусах, а не в косинусах углов, как в работе [6]. Угол, измеряемый с погрешностью порядка угловых минут (картографирование, посадка и стыковка ИСЗ [2]), в любом из этих форматов записывается в двух байтах, и экономии памяти при переходе от углов к косинусам нет. Собственные движения звезд не учитываются: данные о положении звезд соответствуют эпохе каталога HIPPARCOS [4] $T_0 = J1991{,}25$.

Эталонными являются значения α_{ij} для всех пар звезд. При распознавании оцениваются угловые расстояния между парами наиболее ярких звезд, и оценки $\hat{\alpha}_{ij}$ сравниваются с эталонными значениями α_{ij} [в блоке оценивания (см. рис. 2), вырабатываются $\hat{\alpha}_{ij} \in (\alpha_{ij} \pm \Delta/2)$].

Инвариантность к изображению Θ достигается введением конфигураций **ST** звезд — совокупности нескольких пар с одной общей (центральной) звездой. Эталонной конфигурацией $\mathbf{ST}_0$ является множество номеров звезд из рабочего каталога и соответствующих им взаимных угловых расстояний α_{ij}. Условие уникальности угловых расстояний [6], приводящее к необходимости их измерений с погрешностями в угловые секунды, снимается: в пределах $\pm\Delta/2$ угловые расстояния могут повторяться.

Пример эталонной конфигурации, включающей три яркие звезды из созвездия Ориона и попавшую в поле зрения звезду Альдебаран из созвездия Тельца, показан на рис. 3 (шесть угловых расстояний $\alpha_{01}, ..., \alpha_{23}$). Видимые звездные величины для β Ori $m = 0{,}18^m$, для α Ori $m = 0{,}45^m$, для α Tau $m = 0{,}87^m$, для γ Ori $m = 1{,}54^m$. На рис. 3 указаны индексы звезд, включенных в $\mathbf{ST}_0$, и их номера из рабочего каталога. Например, метка (0: 322) для звезды Ригель означает: индекс 0 — центральная в конфигурации, 322 — ее номер в рабочем каталоге; метка (2: 273) для Альдебарана: 2 — номер в конфигурации, 273 — номер в рабочем каталоге.

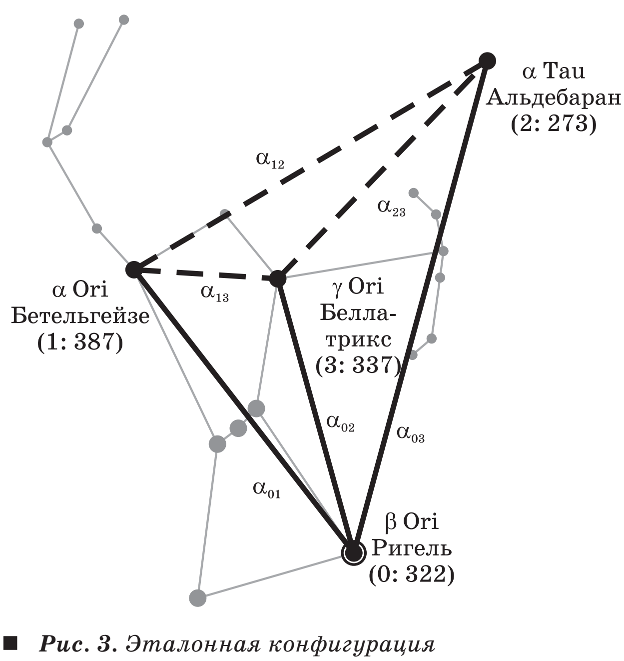
Эталонные конфигурации не хранятся в памяти — они формируются на заключительных этапах распознавания.

Множество **C** возможных конфигураций можно сформировать из множества **A** оценок угловых расстояний $\hat{\alpha}_{ij}$. Оценки **A** позволяют также по рабочему каталогу получить множество допустимых $\mathbf{ST}_k$ эталонных конфигураций. Теперь распознавание заключается в сравнении **C** с $\mathbf{ST}_k$ для выделения $\mathbf{ST}_0 \approx \mathbf{C}$. Если это равенство выполняется для одной конфигурации, распознавание однозначно. Процедура упрощается, если в **C** оставить одну конфигурацию: можно организовать эффективный просмотр рабочего каталога и формирование эталонных конфигураций.

Алгоритм распознавания включает следующие этапы:

1) формирование исходной конфигурации наблюдаемых звезд;

2) выделение базы исходной конфигурации;



■ ***Рис. 3.*** *Эталонная конфигурация*

3) формирование баз-кандидатов;

4) формирование эталонных конфигураций-кандидатов;

5) сопоставление исходной конфигурации с эталонными (распознавание).

Исходная конфигурация **C** формируется выбором центральной (наиболее яркой) звезды, которой присваивается индекс $i = 0$, и n базовых звезд (с индексами $i = 1, \ldots, n$). Базовые звезды выбираются в окрестности центральной звезды по признаку убывания блеска. Например, для созвездия Ориона при измерении угловых расстояний с ошибкой $\Delta\alpha \in \mathrm{N}(0, \sigma)$, $\sigma = \alpha_{01}/20$ ($\Delta \approx 6\sigma$), исходная конфигурация $\mathbf{C} = \left\{\hat{\alpha}_{01}, \hat{\alpha}_{02}, \hat{\alpha}_{03}, \hat{\alpha}_{12}, \hat{\alpha}_{13}, \hat{\alpha}_{23}\right\} =$ $= \{18{,}606;\ 26{,}494;\ 14{,}789;\ 21{,}389;\ 7{,}530;\ 15{,}754°\}$ ($n = 3$) может соответствовать наблюдениям и измерениям, показанным на рис. 4.

Поскольку блеск первых четырех звезд β Ori, α Ori, α Tau, γ Ori различается не более чем на $1{,}5^m$, их сигналы должны отбираться после оценки блеска с соответствующей точностью. Яркие планеты и объекты исключаются из конфигураций по признакам слишком большого блеска.

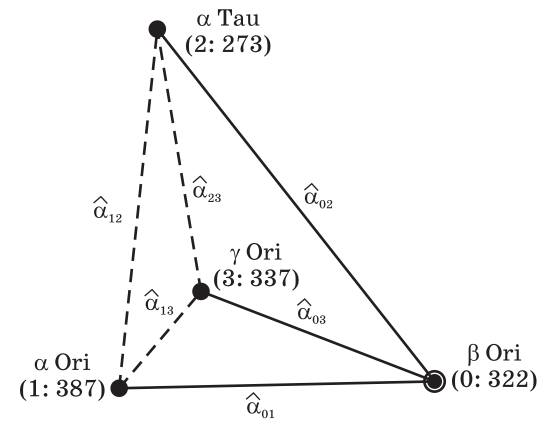
База исходной конфигурации $\mathbf{B}_C$ состоит из угловых расстояний между центральной звездой и базовыми: на рис. 4 база $\mathbf{B}_C = \left\{\hat{\alpha}_{01}, \hat{\alpha}_{02}, \hat{\alpha}_{03}\right\}$.

База-кандидат $\mathbf{B}_k$ — множество звезд из рабочего каталога с угловыми расстояниями, близкими к $\mathbf{B}_C$. Базы-кандидаты графически могут отличаться от $\mathbf{B}_C$ и формироваться вокруг разных центральных звезд (рис. 5): кроме центральной звезды Ригель в каталоге нашлись звезды 22 Ori и HIP87936, образующие $\mathbf{B}_k^1 = \{18{,}587;\ 26{,}513;\ 14{,}774°\}$ и $\mathbf{B}_k^2 = \{18{,}583;\ 26{,}483;\ 14{,}797°\}$.

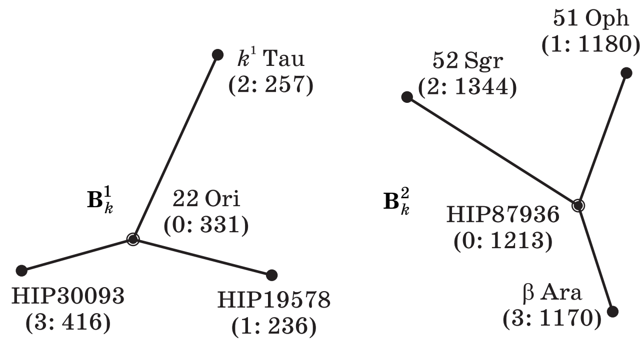
Ниже множество номеров центральных звезд обозначено R_0, набор множеств номеров базовых звезд, соответствующих каждой центральной звезде, — $R_1(r_0), R_2(r_0), \ldots, R_n(r_0)$, $r_0 \in R_0$.

Для всех пар звезд $\{0, i\}$, $i = 1, 2, \ldots, n$, из базы конфигурации (исходных пар) формируются множества соответствующих им эталонных пар из рабочего каталога. Так как угловые расстояния в исходных парах измерены с погрешностью, каждой исходной паре могут соответствовать несколько эталонных $S_{0i} = \{\{k_1, l_1\}_{0i}, \{k_2, l_2\}_{0i}, \ldots, \{k_m, l_m\}_{0i}\}$. Следовательно, эталонной парой $\{k, l\}$ для исходной пары $\{0, i\}$ является любая пара с угловым расстоянием $\alpha_{kl} \in (\hat{\alpha}_{0i} \pm \Delta/2)$. Для формирования множеств S_{0i} удобно использовать дополнительные таблицы: таблицу пар, в которой хранятся эталонные номера звезд k и l и соответствующие им угловые расстояния α_{kl}, а также хеш-таблицу для быстрого доступа к таблице пар. Таблица пар упорядочивается по возрастанию α_{kl}, следовательно, в качестве результата достаточно для каждой пары $\{0, i\}$ выделить номера начальных строк и числа строк, которые необходимо будет выбрать из таблицы пар. Общее количество пар для $N_{зв}$ звезд есть число сочетаний $N_{пар} = \binom{N_{зв}}{2}$.

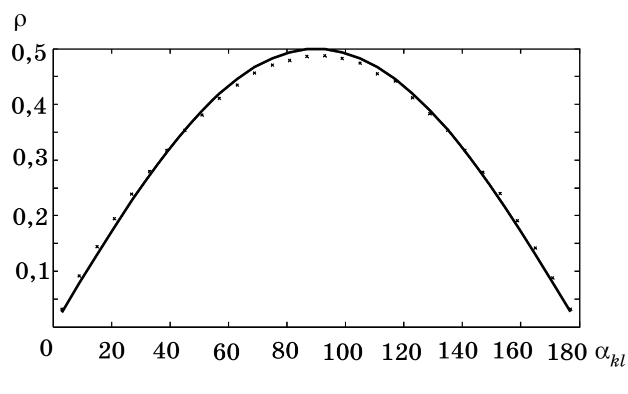
Оценка плотности распределения количества пар $\rho(\alpha_{kl})$, полученная по рабочему каталогу, показана точками на рис. 6. Она может аппроксимироваться синусоидальной зависимостью (см. рис. 6, сплошная линия)



■ ***Рис. 4.*** *Возможная исходная конфигурация*



■ ***Рис. 5.*** *Примеры баз-кандидатов*



■ ***Рис. 6.*** *Плотность распределения количества пар звезд*

$$\rho(\alpha_{kl}) = \frac{1}{2}\sin\alpha_{kl}.$$

Тогда количество пар, заключенных в интервале $[\alpha_{\min}, \alpha_{\max}]$:

$$N_{\text{пар}}(\alpha_{\min}, \alpha_{\max}) \approx N_{\text{пар}} \int\limits_{\alpha_{\min}}^{\alpha_{\max}} \rho(\alpha_{kl})\,\mathrm{d}\alpha_{kl} =$$

$$= \frac{N_{\text{пар}}}{2}(\cos\alpha_{\min} - \cos\alpha_{\max}).$$

Объем памяти, необходимый для хранения таблицы пар:

$$V_{\text{т.п}} = N_{\text{пар}}(\alpha_{\min}, \alpha_{\max})(V_k + V_l + V_\alpha), \qquad (1)$$

где $V_k = V_l$ — размеры ячеек для эталонных номеров k и l; V_α — размер ячейки, отводимой под хранение взаимного углового расстояния α_{kl} данной пары. Например, при отведении по 2 байт на хранение эталонных номеров и 2 байт на хранение α_{kl} и ограничении размера таблицы пар интервалом $[0, 60°]$ $V_{\text{т.п}} \approx 1921$ кбайт.

Хеширование (использование хеш-функции и хеш-таблицы) предназначено для ускорения поиска эталонных номеров пар звезд. В обычном режиме (без хеширования) поиск велся бы, начиная с пары с наименьшим взаимным угловым расстоянием. Если в среднем выбиралась бы исходная пара звезд с угловым расстоянием, близким к половине угла зрения оптической системы, то перебирались бы $N_{\text{пар}}(\alpha_{\min}, \alpha_{\max}/2) \approx 88\,000$ пар звезд. Так как все пары в таблице пар упорядочены по возрастанию взаимного углового расстояния α_{kl}, то поиск интересующей пары можно начинать не с начала таблицы, а с некоторой пары, у которой угловое расстояние α_{kl} близко к $\hat{\alpha}_{0i}$ исходной пары $\{0, i\}$, $i = 1, 2, \ldots, n$. Номера строк для таких пар записываются в хеш-таблицу. Для этого весь возможный диапазон угловых расстояний делится на равные промежутки (с шагом Δ_h) и каждому такому промежутку ставится в соответствие строка из хеш-таблицы. Затем в каждую строку хеш-таблицы записываются номера строк таблицы пар, в которых взаимное угловое расстояние α_{kl} наиболее близко сверху к началу каждого промежутка $\alpha_{kl} \approx \approx \Delta_h j$, j — номер строки хеш-таблицы. Таким образом, если требуется найти пару с некоторым заданным α_{kl}, то хеш-функцией

$$f_{hash}(\alpha_{kl}) = \operatorname{floor}\left(\frac{\alpha_{kl}}{\Delta_h}\right)$$

(округление до меньшего целого) находится номер строки хеш-таблицы, в котором хранится адрес пары (номер строки таблицы пар) с близким к α_{kl} угловым расстоянием. Далее необходимо перебрать некоторое количество пар, чтобы найти искомую. В примере, рассмотренном на рис. 7, интервал $\Delta_h = 0{,}05°$, а номера строк хеш-таблицы 0, 1, 2 и 261 соответствуют интервалам $[0; 0{,}05°)$, $[0{,}05; 0{,}1°)$, $[0{,}1; 0{,}15°)$ и $[13{,}05; 13{,}1°)$.

Хеш-таблица

	Адрес
0:	0
1:	5
2:	10
...	...
261:	19875
...	...

Таблица пар

	k	l	α_{kl}
0:	1077	1078	0,004
...	...	...	...
4:	1182	1184	0,017
5:	1273	1274	0,058
6:	801	802	0,075
...	...	...	...
9:	1141	1142	0,096
10:	1393	1395	0,106
11:	724	725	0,106
...	...	...	...
19874:	392	468	13,049
19875:	1298	1400	13,050
19876:	450	477	13,051
...	...	...	...

■ ***Рис. 7.*** *Пример взаимосвязи хеш-таблицы и таблицы пар*

Объем памяти, отводимый для хранения хеш-таблицы:

$$V_{\text{хт}} = V_n \times \operatorname{ceil}\left(\frac{\alpha_{\max} - \alpha_{\min}}{\Delta_h}\right) \qquad (2)$$

(округление до большего целого), где V_n — размер поля адреса (номера строки таблицы пар). Шаг Δ_h удобно выбирать кратным погрешности Δ. Для $V_n = 4$ байт и $\Delta_h = \Delta = 0{,}05°$ требуется $V_{\text{хт}} \approx 4{,}8$ кбайт.

Список (множество) эталонных пар S_{0i} (т. е. начальный номер и число строк таблицы пар) для исходной пары $\{0, i\}$ находится с помощью вычисления двух хеш-функций: для $\hat{\alpha}_{0i} - \Delta/2$ и $\hat{\alpha}_{0i} + \Delta/2$. Полученный список S_{0i} содержит все пары, у которых $\alpha_{kl} \in (\hat{\alpha}_{0i} \pm \Delta/2)$, а также еще некоторое количество пар, выходящих за рамки заданного интервала (вследствие округлений при разбиении пар на интервалы). Лишние пары следует исключить из результирующего списка путем их перебора. При этом для рассматриваемого случая в среднем придется перебирать около $N_{\text{пар}}\left(\frac{\alpha_{\max} - \Delta_h}{2}, \frac{\alpha_{\max} + \Delta_h}{2}\right) \approx 300$ пар — использование хеширования уменьшает количество вычислений на два порядка.

По полученным множествам пар S_{0i} строится таблица баз-кандидатов $\mathbf{B}_k$ (рис. 8). В этой таблице основной столбец соответствует R_0 — множеству всех возможных эталонных номеров центральной звезды (от 0 до $N_{\text{зв}}-1$). Каждой строке основного столбца (элементу $r_0 \in R_0$) соответствует подтаблица, содержащая n множеств $R_i(r_0) = \{r_i(0), r_i(1), \ldots, r_i(m_{ir_0})\}$ эталонных номеров базовых звезд.

Для заполнения таблицы баз-кандидатов перебираются все пары из множеств S_{0i}, и для каж-

■ *Рис. 8. Таблица баз-кандидатов*

дой пары $\{k, l\} \in S_{0i}$ выполняются следующие операции:

— пусть k — номер центральной звезды: $k = r_0(j)$, тогда в множество $R_i(k)$ добавляется l-й номер $R_i(k) := R_i(k) \cup l$;

— пусть l — номер центральной звезды: $l = r_0(j)$, тогда в множество $R_i(l)$ добавляется k-й номер $R_i(l) := R_i(l) \cup k$.

Объем памяти, отводимый для хранения таблицы баз-кандидатов:

$$V_{т.бк} = V_n \times c_n \times n \times N_{зв}, \tag{3}$$

где V_n — размер ячеек для эталонных номеров; c_n — количество ячеек, отводимых для хранения множества R_i. Количество ячеек c_n следует выбирать так, чтобы не возникло переполнения множества R_i, иначе может произойти потеря некоторых эталонных конфигураций. При $V_n = 2$ байт, $c_n = 15$ значение $V_{т.бк} \approx 142$ кбайт.

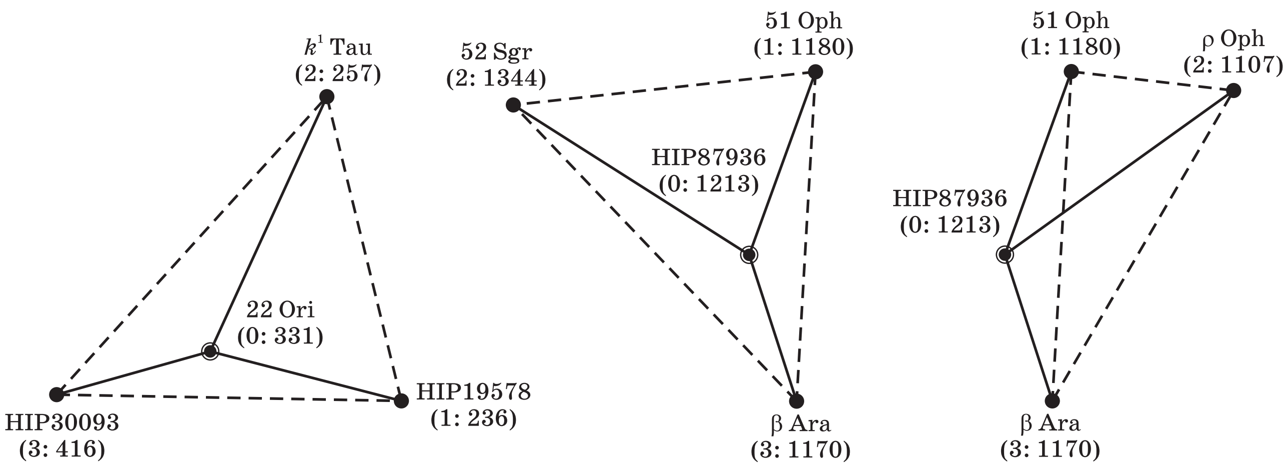
Эталонные конфигурации-кандидаты $\mathbf{ST}_k$ формируются дополнением баз-кандидатов $\mathbf{B}_k$ угловыми расстояниями между базовыми звездами (рис. 9). В табл. 1 приведены номера звезд, в табл. 2 — уг-

■ ***Таблица 1***

№	$i = 0$	$i = 1$	$i = 2$	$i = 3$
1	187	78	167	296
2	283	349	259	237
3	283	397	259	237
4	301	351	254	330
5	322	387	273	337
6	322	387	363	337
7	331	236	257	416
	...	...	...	...
21	1213	1180	1344	1170
22	1213	1180	1167	1170
23	1213	1180	1091	1170
24	1213	1180	1107	1170
	...	...	...	...

■ ***Таблица 2***

№	α_{01}	α_{02}	α_{03}	α_{12}	α_{13}	α_{23}
1	18,623	26,475	14,767	27,644	30,982	23,177
2	18,605	26,486	14,784	43,758	33,349	13,870
3	18,611	26,486	14,784	34,542	29,175	13,870
4	18,623	26,483	14,797	19,221	30,931	41,263
5	18,606	26,494	14,789	21,389	7,530	15,754
6	18,606	26,511	14,789	41,644	7,530	40,569
7	18,587	26,514	14,774	29,319	32,143	37,687
...	...	...	...	...	...	...
21	18,583	26,483	14,797	28,472	31,587	38,902
22	18,583	26,499	14,797	43,832	31,587	12,247
23	18,583	26,501	14,797	41,661	31,587	11,953
24	18,583	26,503	14,797	15,069	31,587	33,927
...	...	...	...	...	...	...



■ *Рис. 9. Конфигурации-кандидаты*

ловые расстояния конфигураций-кандидатов; для каждой центральной звезды составляется множество возможных комбинаций угловых расстояний (см. рис. 8).

Выделенные в табл. 1 строки соответствуют конфигурациям, показанным на рис. 9, строка в рамке — исходной конфигурации **C** (см. рис. 4).

Для исходной конфигурации **C** множество $\mathbf{ST}_k$ при погрешности измерений $\Delta = 0{,}05°$ состоит из 28 конфигураций.

Распознавание — сравнение **C** с $\mathbf{ST}_k$ с целью выделения единственного эталона $\mathbf{ST}_0 \approx \mathbf{C}$. Случаи $\mathbf{ST}_0 = \varnothing$ и $|\mathbf{ST}_0| > 1$ считаются ошибками распознавания. В рассматриваемом примере распознавание однозначно. Если в исходную конфигурацию попадает далекая планета или ИСЗ (не входящие в каталоги), велика вероятность $\mathbf{ST}_0 = \varnothing$.

Для вычисления расстояния α_{kl} эталонной пары $\{k, l\}$ используется дополнительная таблица — матрица **AL** угловых расстояний между эталонными парами. **AL** — симметричная матрица с нулевыми диагональными элементами, поэтому в памяти хранится только верхняя треугольная матрица. Объем памяти для хранения матрицы расстояний

$$V_{\mathbf{AL}} = V_{\alpha} \frac{N_{\text{зв}}^2 - N_{\text{зв}}}{2}. \quad (4)$$

Для рассмотренного случая ($N_{\text{зв}} = 1620$) $V_{\mathbf{AL}} \approx$ ≈ 2564 кбайт.

Тестирование алгоритма

Память, используемая алгоритмом, делится на статическую (не изменяющуюся в процессе работы алгоритма) и динамическую (изменяющуюся). К статической памяти относятся: таблица пар, хеш-таблица и матрица расстояний; к динамической — таблица баз-кандидатов. Объем статической памяти $V_{\text{стат}}$ оценивается по формулам (1), (2), (4), динамической $V_{\text{дин}}$ — по (3). В рассматриваемом примере $V_{\text{стат}} \approx 4{,}5$ Мбайт, $V_{\text{дин}} = V_{\text{т.бк}} =$ $= 142$ кбайт.

Результаты тестирования алгоритма представлены в табл. 3. Погрешности Δ задавались в соответствии с вышеупомянутыми задачами картографирования, ориентации для посадки и стыковки [2]. В каждом случае тестирование проводилось для 10 тыс. случайных положений оптической системы. Использовались два критерия выбора звезд: наиболее яркие звезды и случайно расположенные звезды. Тестирование проводилось на персональном компьютере с процессором класса Intel Pentium IV 3,0 GHz. Время работы алгоритма не превышало 16 мкс.

Заключение

Распознавание выбранного множества звезд реализуется на базе инвариантной к ориентации ИСЗ конфигурации звезд — набором взаимных угловых расстояний между ними. Нормализация исходной конфигурации — необходимые поворот и сдвиг изображения к стандартной форме, соответствующей данным звездного каталога, позволит рассчитать ориентацию (углы рыскания, тангажа и крена).

Рассмотренный алгоритм распознавания конфигурации, состоящей из четырех звезд, достаточно надежен и реализуем в современных вычислительных средах в режиме реального времени.

В работе рассматривался пример с наиболее яркими звездами созвездия Ориона и Tau Альдеба-

■ *Таблица 3*

Количество опорных звезд	Угол зрения, град	Погрешность Δ, мин	Количество успешных распознаваний		Среднее количество конфигураций-кандидатов	
			наиболее ярких звезд	случайно расположенных звезд	наиболее ярких звезд	случайно расположенных звезд
3	60	2	10000	9997	24	21
3	60	5	10000	9991	329	310
3	60	10	9909	9867	2670	2433
3	50	2	10000	9997	16	15
3	50	5	10000	9993	217	211
3	50	10	9953	9873	1730	1675
3	40	2	10000	9994	10	10
3	40	5	9998	9992	124	132
3	40	10	9944	9889	969	1038
3	30	2	10000	9994	5	6
3	30	5	10000	9985	68	72
3	30	10	9898	9887	528	553
2	60	2	9155	9179	88	84
2	60	5	3285	3907	541	518
2	60	10	54	49	2157	2079
2	30	2	9316	9420	28	29
2	30	5	5589	5312	170	182
2	30	10	365	214	674	712

рана. Привязка к созвездиям и наиболее ярким отдельным звездам не обязательна — надежно распознаются любые выбранные четыре звезды с достаточным блеском. Использование в исходной конфигурации произвольных звезд упрощает требования к оцениванию их блеска.

Литература

1. **Раушенбах Б. В., Токарь Е. Н.** Управление ориентацией космических аппаратов. М.: Наука, 1974. 600 с.
2. **Бесекерский В. А., Иванов В. А., Самотокин Б. Б.** Орбитальное гирокомпасирование / Под ред. Б. Б. Самотокина. СПб.: Политехника, 1993. 256 с.
3. Справочник по космонавтике / Под ред. Н. Я. Кондратьева, В. А. Одинцова. М.: Воениздат, 1966. 328 с.
4. The HIPPARCOS and TYCHO catalogues. ESA, 1997. Vol. 1–16.
5. **Николаев А. Г. и др.** Основы проектирования космических секстантов. М.: Машиностроение, 1978. 216 с.
6. **Малинин В. В.** Моделирование и оптимизация оптико-электронных приборов с фотоприемными матрицами. Новосибирск: Наука. 2005.
7. **Осипик В. А., Федосеев В. И.** Математическое моделирование алгоритмов опознавания группы звезд // Оптический журнал. 1996. № 7. С. 10–14.

Институт проблем управления имени В. А. Трапезникова РАН
Российский Национальный Комитет по автоматическому управлению
Отделение энергетики, машиностроения, механики и процессов управления РАН

VIII МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ «ИДЕНТИФИКАЦИЯ СИСТЕМ И ЗАДАЧИ УПРАВЛЕНИЯ — SICPRO'09» с 26 по 30 января 2009 г.

Место проведения: институт проблем управления имени В. А. Трапезникова РАН
Адрес: 117997, ГСП-7, Россия, Москва, улица Профсоюзная, 65

Направления работы

Развитие теории и методологии идентификации, моделирования и управления

Математические задачи теории управления

Параметрическая идентификация

Непараметрическая идентификация

Структурная идентификация и экспертный анализ

Задачи выбора и анализ данных

Системы управления с идентификатором

Задачи идентификации в интеллектуальных системах

Прикладные задачи идентификации

Имитационное моделирование

Методическое и программное обеспечение идентификации и моделирования

Когнитивные аспекты идентификации

Верификация и проблемы качества программного обеспечения сложных систем

Глобальные сетевые ресурсы поддержки процессов идентификации, управления и моделирования

Участие в конференции

Авторам, желающим принять участие в Конференции, необходимо не позднее 31 марта 2008 г. отправить по электронному адресу Оргкомитета тезисы доклада, оформленные в соответствии с Правилами. Тезисы, не соответствующие Правилам, не регистрируются и не рассматриваются.

На основе тезисов проводится отбор докладов для включения их в Программу Конференции. Тезисы не публикуются. О включении докладов в программу Конференции сообщается не позднее 31 мая 2008 г. на Интернет-странице Конференции.

Принятые доклады должны быть отправлены по электронному адресу Оргкомитета в электронном виде (doc- или tex-файлы) не позднее 31 июля 2008 г. Правила оформления доклада и создания его электронной версии будут приведены на Интернет-странице Конференции.

Издание трудов конференции

Труды Конференции (с полными текстами всех докладов (объем докладов не ограничивается), отвечающих требованиям к оформлению) будут изданы на компакт-диске. Данный компакт-диск будет официально зарегистрирован (с присвоением ISBN-кода) как сборник трудов Конференции.

Дополнительная информация и справки

Оргкомитет:

117997, ГСП-7, Россия, Москва, улица Профсоюзная, 65

Кирилл Романович Чернышев, Елена Филипповна Жарко;

тел./факс: +7 (495) 334-89-90

эл. почта: sicpro@ipu.rssi.ru;

сайт: http://www.sicpro.org/sicpro09/code/r09_01.htm

УДК 629.075

НЕЛИНЕЙНАЯ ДИНАМИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ ЗАПАС-ПОПОЛНЕНИЕ

А. Ю. Переварюха,
аспирант
Санкт-Петербургский институт информатики и автоматизации РАН

Исследуется динамическая система, основанная на модели запас-пополнение Рикера. Делается вывод об ограниченности применения известных дискретных моделей пополнения популяций. Предлагается модифицированная непрерывно-дискретная модель воспроизводства, качественно отличающаяся от модели Рикера.

Введение

Контринтуитивные процессы, протекающие в сложных саморегулируемых биологических системах, не имеют простых объяснений, а «серебряная пуля» в арсенале математической теории динамики популяции либо просто не существует, либо является хорошо охраняемой тайной. В сложных ситуациях автору приходится использовать нетрадиционные для математической биологии подходы, например непрерывно-дискретные динамические системы. Необходимость в разработке описываемой в этой статье модели обусловлена целью анализа имеющихся данных наблюдений, а не является попыткой дать умозрительную популяционную интерпретацию некоему математическому аппарату.

Проблема стабильности биологических сообществ и отдельных популяций — одна из наиболее актуальных и обсуждаемых в теоретической экологии [1]. Природные системы могут иметь более одного устойчивого режима существования; если значения некоторых показателей находятся в пределах некоторого диапазона, незначительные возмущения поглощаются. Количественные показатели будут колебаться, но качественное поведение динамических процессов останется постоянным, пока внешнее воздействие не выведет систему за границы области устойчивого равновесия и переведет в иное качественное состояние. Если возможны два таких состояния и одно из них нежелательно, то задача управления состоит в поддержании параметров природной системы в диапазоне значений, удаленных от критических. Выведенная из равновесия экосистема может стабилизироваться в новом и непригодном для хозяйственного использования состоянии.

Для анализа устойчивости были предложены различные методы, в частности, использование в качестве меры устойчивости аналога информационной энтропии. МакАртур (MacArthur) в 1955 г. предложил характеризовать стабильность сообщества величиной

$$S' = -\sum_{i=1}^{n} p(s_i) \ln p(s_i),$$

где $p(s_i)$ — вероятность переноса энергии по определенному пути. Чем больше S', тем устойчивее считается сообщество. Но при использовании такого подхода возникают противоречия. Достижение максимума S' возможно, когда равновероятен выбор любого пути переноса энергии, т. е. такое сообщество не будет обладать какой-либо иерархичностью и структурой, что не подтверждается наблюдениями над реальными сообществами. Энтропийная мера применима на ранних стадиях сукцессии, когда конкурентные отношения еще не столь жесткие и сообщество может быть рассмотрено как система со слабыми взаимодействиями [2].

Другой подход, развивающийся в последнее десятилетие, заключается в применении идей нелинейной динамики в экологических процессах и изучении качественного поведения динамических моделей [3]. В настоящей статье речь пойдет о нелинейных динамических системах, имеющих интерпретацию в теории запас-пополнение популяций рыб.

Продолжительное и экономически эффективное управление популяцией возможно только тогда, когда воспроизводство обеспечивает восстановление промыслового запаса. Амплитуда и частота колебаний численности обуславливаются изменчивостью процессов формирования пополнения и темпом обновления нерестового стада за счет новых возрастных классов. Концепции о линейной зависимости между запасом и пополнением Ф. Баранова и К. Бэра [4] не нашли подтверждения в последующих исследованиях.

Определение зависимости между запасом и пополнением показывает, при каких значениях запаса воспроизводство становится восполняющим запас, и может служить важнейшим критерием при прогнозировании уловов. Результат действия различных факторов смертности молоди выражается в итоговой численности поколения, полученного от нерестового запаса данной численности через определенный «интервал уязвимости» $[0, T]$.

Уравнение для численности пополнения (recruits) R предложено известным канадским исследователем У. Е. Рикером (W. E. Ricker) в 1953 г. [5] (до Рикера вопрос о возможности уменьшения пополнения при возрастании нерестового стада никем не рассматривался):

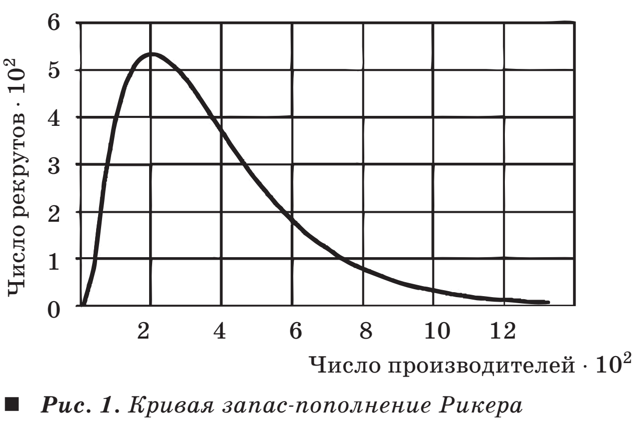
$$R = aS\exp(-bS), \qquad (1)$$

где S (stock) — величина нерестового запаса; b — коэффициент, отражающий величину, обратную количеству выметанной икры, при котором число выжившей молоди максимально, соответственно, имеет смысл только $b << 1$; a — параметр. График зависимости представляет собой куполообразную кривую с единственным нетривиальным пересечением с биссектрисой координатного угла $R = S$. Количество икры определяется, исходя из средней плодовитости особей: $E = \lambda S$. График зависимости числа рекрутов от численности производителей называется кривой пополнения (рис. 1).

Очевидно, что применение модели (1) вызывает ряд сложностей, наиболее значимая из которых состоит в том, что при увеличении количества отложенной икры выживаемость молоди будет стремиться к нулю, что не согласуется с наблюдениями биологов. Для ограничения возможности возникновения такого явления модель Рикера при имитационном моделировании популяций корректно использовать только до некоторого критического количества икры $E_к$, как делал А. Б. Казанский [6], при превышении $E_к$ количество молоди зависит от соотношения постоянных коэффициентов модели или определяется константой. Фактически в таком подходе при имитационном моделировании формирования пополнения используется только восходящая ветвь кривой запас-пополнение:

$$R = \begin{cases} aE\exp(-bE), \text{если } E \le 1/b \\ \dfrac{a}{b\ell}, \text{если } E > 1/b \end{cases}$$

$$\text{или } R = \begin{cases} aE\exp(-bE), \text{если } E \le E_к \\ E_к, \text{если } E > E_к \end{cases}.$$



■ *Рис. 1. Кривая запас-пополнение Рикера*

Не столь очевидные, но существенные проблемы для моделирования воспроизводства возникают при значительном уменьшении нерестового запаса. При крайне низких численностях производителей уравнение Рикера предсказывает увеличение эффективности воспроизводства популяции. Когда количество отложенной икры стремится к нулю, выживаемость пополнения N стремится к предельному значению:

$$\frac{dN}{dE} = a\exp(-bE)(1-bE), \ \lim_{E\to 0} a\exp(-bE)(1-bE) = a.$$

Подобное предположение не соответствует фундаментальным представлениям экологии о существовании нижней критической численности популяций животных, известным как принцип Олли, согласно которому при низкой численности репродуктивной части популяции эффективность воспроизводства должна снижаться, так как уменьшается вероятность встречи особей разного пола на нерестилищах. Также не согласуются с биологическими представлениями, в частности, с теорией этапности развития организмов, предположения о постоянстве коэффициентов мгновенной смертности и о факторах, лимитирующих численность рыб в критические периоды развития. Сам Рикер считал более приемлемой свою модель для ситуаций, когда каннибализм является важным регуляторным механизмом и когда реакция хищников на численность молоди определяется первоначальной численностью поколения.

Запас-пополнение Рикера как нелинейная динамическая система

Описания свойств моделей запас-пополнение как математических функций оказывается явно недостаточно. Один из пионеров отечественного гидробиологического моделирования В. В. Суханов писал следующее: «Оказалось, что собственно кривой Рикера результаты расчетов не дали. На плоскости $S \times R$ получилось сгущение точек, мало чем напоминающее вышеуказанную кривую. При тех параметрах, при которых популяция испытывала наиболее регулярные колебания, точки на графике образовывали нечто вроде неотчетливого эллипса. Применение метода наименьших квадратов для определения значений параметров a и b привело к абсурдным результатам: коэффициент a оказался меньшим, чем единица, что невозможно для популяции с ненулевой численностью. Полученные результаты говорят о том, что кривая Рикера не является хорошим приближением к эмпирическим данным» [7]. Для понимания того, что аспекты, отмечаемые многими критиками теории зависимостей запас-пополнение, на самом деле не содержат противоречий, необходимо провести дальнейшие исследования.

Представим процесс изменения состояния популяции, определяемый зависимостью запас-пополнение, в виде динамической системы — математического объекта, для которого можно указать набор динамических переменных, характеризующих состояние системы. Значения таких переменных в последующий момент времени рассчитываются из текущих значений по определенному правилу (называемому оператором эволюции). Динамическая система — это тройка (M, T, ψ), состоящая из фазового пространства M, времени T, оператора эволюции ψ. Причем для всех $x \in M$ и t, $s \in T$ выполняется условие

$$\psi(\psi(x, t), s) = \psi(x, s+t).$$

Множество $\{\psi^{(t)}(x)\}_{t \in T}$ называют фазовой траекторией точки x. Графически эволюция динамической системы во времени представляется движением точек в фазовом пространстве. Важным понятием теории диссипативных динамических систем является аттрактор. Словарное значение слова «attractor» — то, что привлекает или притягивает. Под аттрактором мы будем понимать подмножество фазового пространства $A \subseteq M$, инвариантное относительно эволюции в системе: $\psi^{(t)}(A) = A$ для всех $t \in T$, и такое, что существует окрестность U множества A, в которой для всех $y \in U$ выполняется условие

$$\lim_{t\to\infty} \psi^{(t)}(y) = A.$$

Простые аттракторы — устойчивое состояние равновесия с неподвижной точкой x^*:

$$\lim_{t\to\infty} \psi^{(t)}(y) = x^*,$$

и устойчивый цикл, отвечающий режиму периодических автоколебаний: $\psi^{(t)}(x^*) = \psi^{(t+p)}(x^*), p \in T$. Множество точек, приводящих к некоторому аттрактору, называется его областью или бассейном притяжения (basin of attraction). Рассмотрим динамическую систему как полугруппу итераций $\{\psi^{(j)}\}_{j \ge 0}$, и пусть $R_0, R_1, R_2, \ldots$ — последовательность точек, описывающих эволюцию системы, определенных условием $R_{j+1} = \psi(R_j)$ при всех $j \ge 0$. Оператор эволюции в непрерывно-дискретной динамической системе запишем в следующей форме:

$$\frac{\mathrm{d}N_{i+1}}{\mathrm{d}t} = -(\alpha N_{i+1}(0) + \beta) N_{i+1}(t); \quad \left.\frac{\mathrm{d}N_{i+1}}{\mathrm{d}t}\right|_{t=0} = \lambda \left.\frac{\mathrm{d}N_i}{\mathrm{d}t}\right|_{t=\tau}.$$

Константы α, β, τ соотносятся с константами a, b формулы Рикера: $a = \lambda\exp(-\beta\tau)$, $b = \alpha\tau$. Качественное поведение системы зависит от параметра a, он является управляющим. Исследование динамической системы на основе (1) показало интересное и подчас весьма странное ее поведение. До определенного значения a, не превышающего бифуркационное, система стремится к точечному аттрактору $R^* = \ln(a)/b$, даже если искусственно выводить ее из равновесия (рис. 2).

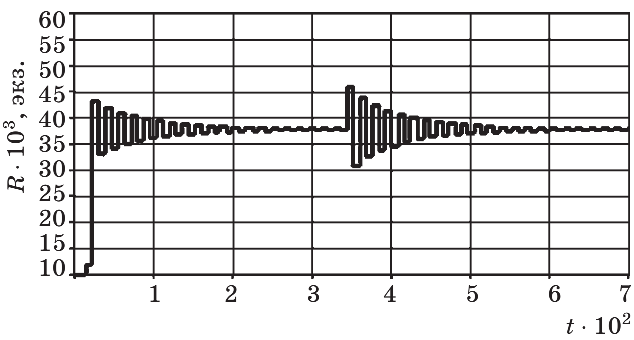
Первый метаморфоз поведения системы — отображенная на временной диаграмме бифуркация (рис. 3), происходит, когда производная в неподвижной точке перестает удовлетворять критерию устойчивости при выполнении условия $a > e^2$:

$$\psi'(R) = ae^{-bR} - bRae^{-bR};$$

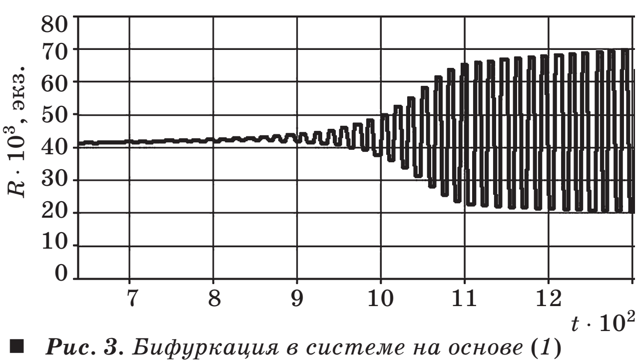
$$\psi'(R^*) = ae^{-b\frac{\ln a}{b}} - b\frac{\ln a}{b} ae^{-b\frac{\ln a}{b}} = \frac{a(1-\ln a)}{e^{\ln a}} = 1 - \ln a,$$

$$1 - \ln a = -1, \;\; a = e^2.$$

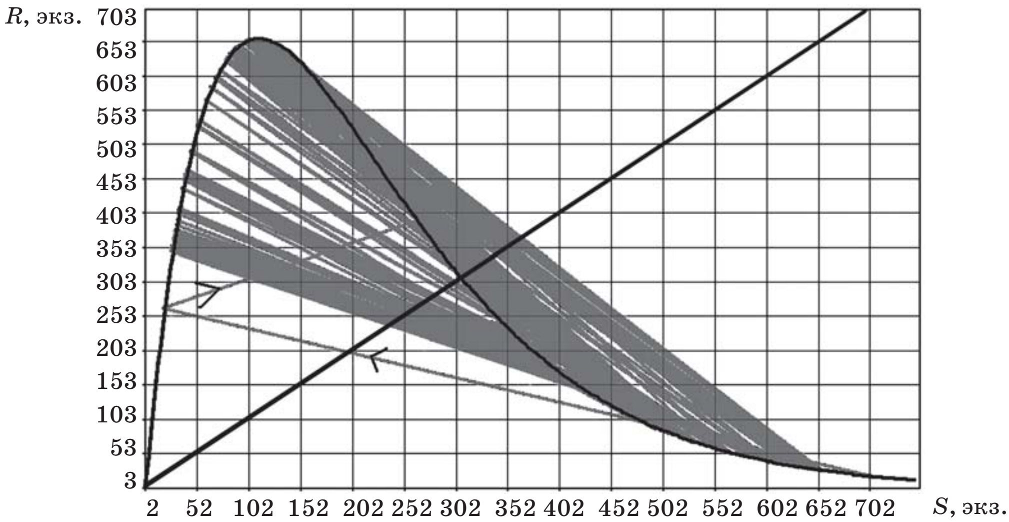
Теперь очевидно, что параметр b не влияет на топологические характеристики фазового портрета. Динамическая система стремится в устойчивое циклическое состояние с периодом 2 — глобальный аттрактор, состоящий из двух периодических точек — последовательности $(R_{T1}, R_{T2}, R_{T1}, R_{T2}, \ldots)$, областью притяжения которого является все фазовое пространство. Тот факт, что отображение Рикера имеет в этом диапазоне параметра цикл с периодом 2, говорит о том, что не стоит от построенного по эмпирическим данным графика ожи-



■ *Рис. 2. Притяжение к точечному аттрактору*



■ *Рис. 3. Бифуркация в системе на основе (1)*



■ ***Рис. 4.** Странный аттрактор в системе на основе (1)*

дать характерной куполообразной кривой, как на рис. 1. Если далее увеличивать параметр a, будет происходить увеличение амплитуды колебаний, и по достижении следующего порогового значения $a > 12{,}51$ произойдет бифуркация удвоения периода и установится цикл с периодом 4. При дальнейшем увеличении параметра a будет происходить каскад бифуркаций удвоения периода. При $a > 14{,}8$ невозможно выделить устойчивых точек или замкнутого цикла — происходит детерминированный хаос, напоминающий стохастический процесс, очень чувствительный к начальным условиям. При $i \to \infty$ фазовая диаграмма будет выглядеть так (рис. 4). Траектория притягивается к подмножеству фазового пространства — «странному аттрактору», не имеющему внутри себя ни одной устойчивой траектории.

Как показали дальнейшие исследования, описанным М. Фейгенбаумом сценарием перехода к хаосу (1) не ограничивается, для некоторых диапазонов $a > 14{,}8$ наблюдаются «окна периодичности» — появляются устойчивые циклы нечетных периодов, т. е. для (1) возможны касательные бифуркации. В диапазоне значений параметра $18{,}474 < a < 18{,}564$ появление ожидаемого странного аттрактора не наблюдается, возникает устойчивый цикл.

Дискретные отображения обладают свойствами, делающими их объектом исследования для теории динамического хаоса. Ли и Йорк в 1975 г. опубликовали статью «Period three implies chaos», в которой показали, что если одномерное отображение вида $R_{j+1} = \psi(R_j)$ при некотором значении одного из параметров имеет цикл периода три, то оно также имеет и бесконечное множество циклов других периодов. Даже самые простые дискретные модели, например: $x_{n+1} = \lambda \sin(\pi x_n)$, $x_{n+1} = \lambda x_n(1 - x_n)$ и т. п., могут приводить к хаотическим режимам динамического поведения. Появление хаоса в экологических моделях — отдельная проблема («Chaos Paradox», «Paradox of Enrichment»), различные исследования по анализу эмпирических данных, например работа [8], не смогли подтвердить наличие хаоса в реальных популяциях. В работе [9] МакАлистер показал, как «хаотическое» поведение сменяется стабилизацией при наличии для популяции ограничений со стороны внешней среды.

Для построения кривых запас-пополнение были предложены довольно сложные преобразования исходных данных наблюдений. Наверное, никогда исследователи не бывают так настойчивы, как в случае, когда пытаются отыскать то, чего нельзя обнаружить. Рикер предложил прологарифмировать формулу (1) и строить кривую с использованием регрессии $\ln(R/S)$ на S для арифметической средней. Возникает естественный вопрос: имеют ли смысл методы построения кривой, если эмпирические данные о воспроизводстве не находящихся в стадии деградации популяций, для которых справедлива зависимость Рикера, будут представлены в виде сгущений точек на графике, мало напоминающих ожидаемую кривую. Именно эллипсы (как верно заметил В. В. Суханов) образуют точки на фазовом портрете, стремящиеся по спирали к устойчивому состоянию (фокусу) в его области притяжения.

Модификация модели запас-пополнение

Необходимость модификации модели запас-пополнение возникла при выявлении нелинейной зависимости численности «скатывающейся» молоди от численности нерестового стада в задаче моделирования процессов, приведших к деградации популяции осетровых Каспия. Численность пропущенных на нерест производителей севрюги за период наблюдений изменялась очень существенно: от 230 тыс. экз. в 1979–81 гг. до 15 тыс. в 2000 г. [10].

П. Летт на основе анализа воспроизводства трески показал, что двухпараметрические модели не обеспечивают приемлемую интерпретацию данных наблюдений. Наличие ограниченных пищевых ресурсов в неявном виде учитывалось известными моделями, но общим недостатком существующих моделей является игнорирование декомпенсационного фактора смертности и изменения пищевых потребностей по мере развития молоди, которое совпадает во времени с началом сезонного уменьшения кормовой базы. Декомпенсационные факторы, увеличивающие смертность при уменьшении плотности (наблюдаются, например, у насекомых, для которых характерно групповое поведение), снижают эффективность нереста, уменьшая количество икры, реально вступившей в репродуктивный процесс при $S \to 0$. Введение такой зависимости становится очевидной необходимостью для популяций, подвергающихся «перелову». Целью модификации модели запас-пополнение стало создание гибкого математического аппарата для задачи согласования характера поведения имитационной модели динамики популяции со статистическими данными о популяциях, так как очевидно, что поведение модели зависит от математических особенностей выбранной функции воспроизводства. Куполообразная кривая подразумевает наличие диапазона оптимальной численности нерестового стада.

Рассмотрим увеличение пищевых потребностей молоди и будем исходить из того факта, что темп роста находится в обратной зависимости от численности поколения, но не в обратно пропорциональной. Это согласуется с данными наблюдений биологов (в частности, экспериментов Петерсена с ростом камбал при различной плотности), согласно которым при увеличении плотности возникает асимметричное распределение размерной структуры популяции в сторону преобладания особей с меньшими размерами. До достижения определенного веса w_k динамику численности поколения N будут отражать следующие объединенные в систему дифференциальные уравнения (α, β, ζ, c — константы):

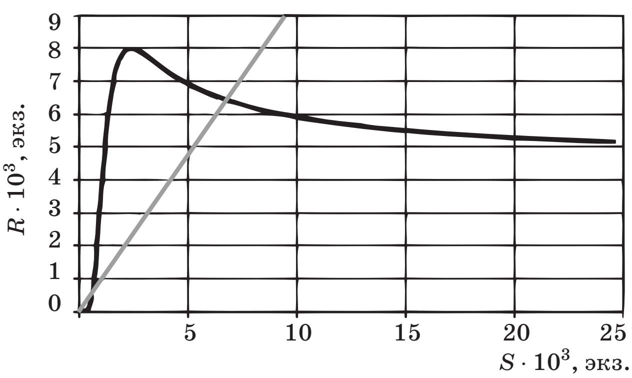
$$\begin{cases} \dfrac{\mathrm{d}N}{\mathrm{d}t} = -(\alpha w(t) N(t) + \theta(S)\beta) N(t), \quad N(0) = \lambda S \\ \dfrac{\mathrm{d}w}{\mathrm{d}t} = \dfrac{g N^n(t)}{N^k(t) + \zeta g}, \quad \theta(S) = \dfrac{1}{1 - \exp(-cS)}, \quad k > n \end{cases}, \quad (2)$$

где $w(t)$ отражает изменение пищевых потребностей в зависимости от массы особей; g — ограничивающий фактор, учитывающий количество доступных кормовых организмов; убывающая функция $\theta(S) \to 1$ при $S \to \infty$. Графиком предложенной автором и исследованной в инструментальной среде разработки имитационных моделей AnyLogic5 новой модели является куполообразная кривая. Среда AnyLogic предлагает достаточный выбор численных методов с изменяющимся шагом интегрирования для работы с системами обыкновенных дифференциальных уравнений в форме Коши и дифференциальных уравнений с отклоняющимся аргументом. При деградации нерестового стада кривая переходит в прямую линию с малым углом наклона. Кривая системы уравнений (2) имеет ниспадающую ветвь с уменьшающимся наклоном (рис. 5).

Полученная кривая адекватно воспроизводит динамику системы запас-пополнение и соответствует наблюдениям за воспроизводством популяций, для которых характерна значительная амплитуда колебаний численности производителей. В частности, для горбуши рек Аляски отмечено уменьшение относительного количества молоди как в периоды возрастания численности популяции, так и по мере ее уменьшения.

Поведение траектории динамической системы с использованием в качестве оператора эволюции модели автора качественно отличается от системы на основе формулы Рикера возможностью притяжения к двум аттракторам и, соответственно, наличием двух областей притяжения, границей между которыми служит репеллер — неустойчивая особая точка первого пересечения кривой с биссектрисой координатного угла. Один из аттракторов — точка с координатами (0, 0) на плоскости $R \times S$. Если начальная численность популяции соответствует области притяжения этого аттрактора, произойдет вымирание популяции. Другое отличие: в данной динамической системе нет бифуркационных значений коэффициентов, так как они представлены в виде функций времени.

Рассмотрение предложенной модели запас-пополнение приводит к выводам, что популяция, подвергшаяся воздействию неблагоприятных факторов, в том числе основного такого фактора — перелова, быстрее уменьшается и существенно медленнее восстанавливает численность в благоприятных условиях. Критическое воздействие приводит к дальнейшему уменьшению численности даже в случае последующего его прекращения. Подобная динамика наблюдалась ранее с популяциями реки Кура и с одним из когда-то промысловых видов осетра, промысел которого велся в реках Северной Европы, где сегодня он больше не встреча-



■ *Рис. 5. Кривая предложенной автором модели (2)* ется. Хорошо документирован коллапс без последующего восстановления промысловых запасов форели и сельди Великих Озер [11] в 1950-е гг., особенности графика деградации которых подтверждают предположения автора о наличии дополнительного максимума на кривой пополнения.

Литература

1. **Свирежев Ю. М., Логофет Д. О.** Устойчивость биологических сообществ. М.: Наука, 1978. 353 с.
2. **Свирежев Ю. М., Елизаров Е. Я.** Математическое моделирование биологических систем // Проблемы космической биологии. 1972. Т. 20. С. 133–139.
3. **Короновский А. А., Трубецков Д. И.** Нелинейная динамика в действии. Саратов: Изд-во ГосУНЦ «Колледж», 2002. 324 с.
4. **Шибаев С. В.** Промысловая ихтиология. СПб.: Проспект науки, 2007. 400 с.
5. **Ricker W.** Stock and recruitment // Journal Fisheries research board of Canada. 1954. N 11. P. 559–623.
6. **Казанский А. Б.** Имитационная модель популяции рыбы с учетом промыслового воздействия // Применение методов имитационного моделирования в рыбохозяйственных исследованиях на внутренних водоемах. Л.: Госниорх, 1989. С. 33–47.
7. **Суханов В. В.** Исследование модели популяции нерки Oncorhynchus nerka в условиях изменчивой кормовой базы// Вопросы ихтиологии. 1973. Т. 13. Вып. 4. С. 627–632.
8. **Ellner S., Turchin P.** Chaos in a noisy world: new methods and evidence from time-series analysis // Amer. Naturalist. 1995. N 145. P. 343–375.
9. **McAllister, C. D., R. J.** LeBrasseur Stability of enriched aquatic ecosystems // Science. 1971. N 175. P. 562–565.
10. **Довгопол Г. Ф., Вещев П. В.** Оценка численности поколений севрюги Acipenser stellatus и основных факторов, влияющих на структуру ее популяции// Вопросы ихтиологии. 1993. Т. 33. С. 93–99.
11. **Christie W. J.** Changes in the fish species composition of the Great Lakes//Journal Fisheries research board of Canada. 1954. N 5. P. 827–853.

УДК 004.412; 004.413.5

ИСПОЛЬЗОВАНИЕ АВТОМАТИЗИРОВАННОЙ КЛАССИФИКАЦИИ ИЗМЕНЕНИЙ ПРОГРАММНОГО КОДА В УПРАВЛЕНИИ ПРОЦЕССОМ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Е. Г. Князев,
старший разработчик программного обеспечения
ЗАО «Транзас Технологии»
Д. Г. Шопырин,
канд. техн. наук, доцент
Санкт-Петербургский государственный университет информационных технологий, механики и оптики

Описывается метод автоматизированной классификации изменений в контексте контроля развития программного кода, основанный на статистической кластеризации метрик изменений исходного кода. Показано применение автоматизированной классификации изменений для оптимизации процесса просмотра исходного кода и автоматизации контроля изменений на ответственных стадиях разработки. Приведен способ построения отчета по параметрам процесса разработки.

Введение

Наиболее важным активом проектов по разработке программного обеспечения является исходный код системы. Большинство современных проектов хранит всю историю изменений исходного кода в специальном хранилище, которое называется системой контроля версий. Однако эта информация доступна только тем участникам проекта, которые технически подготовлены для анализа исходного кода, т. е. в основном разработчикам, в то время как над проектом работают еще и тестировщики, менеджеры и другие специалисты, которым может быть полезна информация, полученная из исходного кода в виде списков реализованной в конкретной версии функциональности, различных отчетов и т. п. Более того, анализ истории изменений исходного кода затрудняется большим объемом входной информации. В частности, хранилище исходного кода содержит массу мелких и незначительных изменений, которые осложняют поиск важных, с точки зрения анализирующего, изменений.

Автоматизированная классификация изменений в качестве вспомогательного инструмента увеличивает производительность анализирующего при выполнении задач, связанных с анализом истории программных систем. В частности, использование автоматизированной классификации позволяет отфильтровать несущественные, по мнению анализирующего, изменения системы. Разработчик или технический лидер команды разработчиков может выделить изменения, которые привели, например, к реализации новой функциональности и сосредоточиться на них.

С помощью автоматизированной классификации изменений технический лидер может автоматизировать запрет некоторых типов изменений на определенных стадиях разработки. Например, настроить инструмент автоматизированной классификации изменений так, чтобы при внесении изменения по реализации новой функциональности на стадии тестирования формировалось автоматическое уведомление о недопустимом изменении для технического лидера и автора данного изменения.

В работе приводится несколько вариантов использования автоматизированной классификации изменений исходного кода участниками проекта, не связанными непосредственно с разработкой программного обеспечения. Автоматизированная классификация изменений дает возможность тестировщику получать информацию об изменениях, в которых реализуется новая функциональность, исправляются ошибки в виде исходного кода или текста комментария, ассоциированного с изменением. Менеджеру проекта метод классификации изменений позволит строить отчеты с распределением изменений по типам.

Таким образом, применение автоматизированной классификации изменений исходного кода способствует повышению скорости и качества просмотра изменений кода, а также предоставляет дополнительные механизмы контроля состояния процесса разработки.

Применяемый в работе метод классификации изменений базируется на кластеризации метрик изменений исходного кода алгоритмом *k*-средних Мак-Кина [1, 2]. Адекватность классификации подтверждается в ходе эксперимента, описанного в работе [3]. Получено значение коэффициента согласия Кохена [4], равное 0,79, которое лежит на границе значительной и превосходной степени согласованности экспертного и автоматизированного методов классификации [5].

Аспекты применения автоматизированной классификации

Автоматизированная классификация изменений может быть полезной всем членам команды разработки. Ниже подробно описаны возможные варианты использования инструмента, реализующего автоматизированную классификацию изменений программного кода всеми участниками проекта.

Применение метода разработчиком

Рядовой разработчик программного обеспечения часто сталкивается с необходимостью просмотра большого количества изменений. Например, при подключении к проекту, который уже имеет некоторую историю, или по возвращении из отпуска или командировки. В таких случаях ему приходится внимательно читать комментарий к каждому изменению, а если информации в комментарии недостаточно, то и просматривать содержимое изменения. Затраты времени на такой процесс могут быть существенными.

Автоматизированная классификация изменений избавит разработчика от необходимости погружаться в детали каждого изменения. Ему достаточно выбрать набор типов изменений, который его интересует, и просмотреть изменения, соответствующие данному типу. На рис. 1 изображена схема просмотра изменений с выбранным фильтром по типу изменения.

Автоматизированная классификация изменений пригодится разработчику для локализации ошибки, внесенной в код в определенный период времени. В этом случае разработчику будет достаточно выделить типы изменений, потенциально влияющие на выбранный модуль, и установить конкретное изменение, нарушившее работоспособность кода.

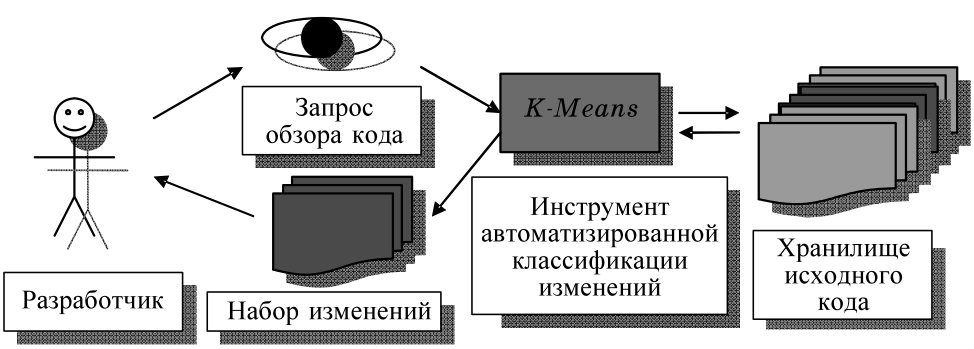
Применение метода техническим лидером

Задачами технического лидера команды разработчиков являются, во-первых, регулярный обзор исходного кода и, во-вторых, контроль изменений, вносимых на текущей стадии разработки. Обзор исходного кода — чрезвычайно полезная практика, состоящая в просмотре исходного кода на предмет поиска ошибок и проблем дизайна. Его выполнение позволяет выявить и разрешить большое количество проблем на ранней стадии разработки, пока исправление еще не требует больших затрат времени. Контроль изменений, вносимых на текущей стадии разработки, состоит в недопущении изменений, потенциально способных дестабилизировать систему на ответственной стадии процесса. По этим соображениям, например, недопустима реализация новой функциональности на финальных стадиях подготовки продукта к выпуску.

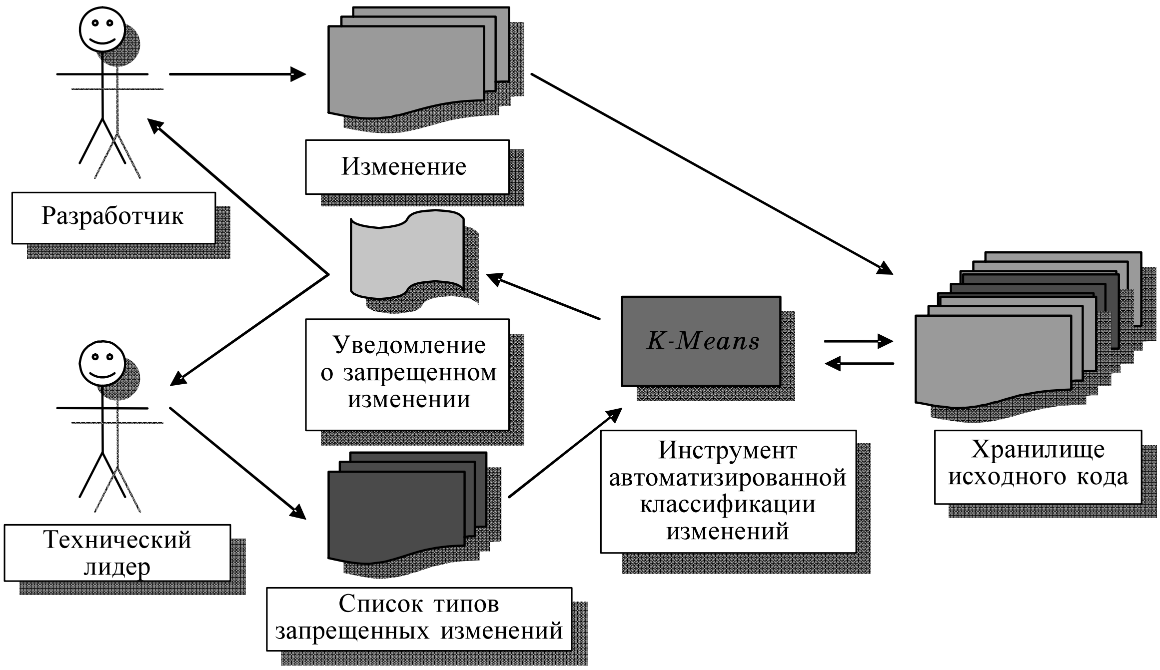
Рассмотрим задачу обзора исходного кода. Одной из основных мер поддержания качества кода на высоком уровне является постоянный просмотр

■ *Число изменений исходного кода по проектам за месяц*

Проект	Период	Число изменений
Tortoise SVN	22.09.2007–22.10.2007	215
Navi-Manager		72
KDE	17.09.2007–14.10.2007	11841 (!)



■ ***Рис. 1.*** *Просмотр изменений с фильтрацией по типу*



■ ***Рис. 2.*** *Автоматизация поиска изменений, нежелательных на текущей стадии разработки*

изменений, вносимых в код разработчиками. Команда программистов средних размеров генерирует большое количество изменений, что может приводить к физической неспособности технического лидера просмотреть все изменения.

В таблице приведены результаты подсчета количества изменений, внесенных в систему контроля версий, за период, приблизительно равный одному месяцу, для трех проектов: графического клиентского приложения для Subversion для Windows TortoiseSVN [6], клиент-серверной системы мониторинга флота Navi-Manager [7], разрабатываемой автором данной статьи в компании «Транзас Технологии», и графической оболочки для Linux и Unix KDE [8].

В некоторых проектах количество вносимых в исходный код изменений может быть очень большим. В этой ситуации технический лидер выбирает наиболее важные изменения, основываясь лишь на тексте комментариев к ним. Однако методика отбора изменений, не основанная на анализе кода, ведет к тому, что важным изменениям может быть не уделено должное внимание. Это, в свою очередь, приводит к потере контроля над качеством продукта.

Выходом из этой ситуации является использование автоматизированной классификации изменений. Просмотр кода с использованием дополнительной информации о типе каждого изменения дает возможность отсеивать неинтересные техническому лидеру изменения для более подробного изучения важных изменений.

Рассмотрим задачу контроля изменений, вносимых на текущей стадии разработки. В процессе реализации программный проект проходит несколько стадий. Например, при подготовке к выпуску версии объявляется состояние проекта `stop code`, при котором запрещается внесение любых изменений в коде, кроме исправлений найденных ошибок. Эта стадия предназначена для стабилизации версии перед выпуском.

Далее, когда все найденные ошибки исправлены, проект переводится в состояние `freeze code`, в котором разрешено внесение изменений только для исправления критичных ошибок. В качестве контроля обязателен просмотр каждого изменения еще одним членом команды перед внесением его в систему контроля версий. В этом состоянии версия исходного кода проекта находится в течение всего времени поддержки ее для заказчика.

Каждая стадия ограничивает процесс разработки определенным набором действий. В частности, в течение стадий `stop code` и `freeze code` от разработчиков ожидается деятельность по исправлению ошибок в коде, а не реализации новых функций.

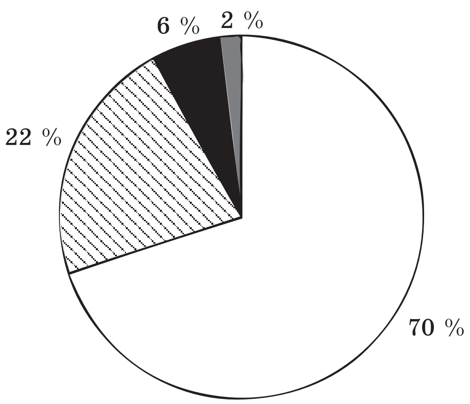
Автоматизированная классификация изменений позволяет автоматизировать процесс контроля внесения изменений на текущей стадии разработки. Достаточно предоставить информацию о допустимых на текущей стадии разработки изменениях. На рис. 2 показана возможность работы модуля по обнаружению нежелательных изменений.

Применение метода лидером по тестированию

В процессе работы над проектом специалистам по тестированию приходится взаимодействовать с разработчиками для уточнения состояния проекта. Тестировщикам часто не хватает информации относительно новой функциональности, реализованной в очередной версии программного обеспечения. Иногда единственный достоверный способ выяснить полный список новых функций в конкретной версии программного обеспечения состоит в полном просмотре изменений кода за интересующий период. В этой ситуации применение автоматизированной классификации уменьшает время на проведение операции за счет отсеивания изменений, классифицирующихся как нечто кроме реализации новой функциональности.

Применение метода менеджером проекта

Менеджер проекта заинтересован в высокоуровневых показателях процесса работы. Информация о том, какая часть изменений производится в рамках реализации новой функциональности, по сравнению с рефакторингом и исправлением ошибок, позволит оценить эффективность работы над проектом. На рис. 3 показано распределение изменений по типам для проекта Navi-Manager за один месяц стадии реализации новой функциональности. Можно сделать вывод, что проект Navi-Manager движется недостаточно быстро из-за того, что основные ресурсы команды разработчиков тратятся в основном на исправление ошибок, а не на реализацию основной функциональности.



■ ***Рис. 3.*** *Распределение изменений по типам:*
□ — правки ошибок + мелкие изменения;
▨ — небольшие функции + рефакторинг;
■ — крупные сложные функции;
■ — удаление кода

Классификация изменений исходного кода

В настоящей работе предлагается использовать метод классификации изменений программного кода, который автоматизирует процесс разделения семантически различных изменений на основе значений метрик исходного кода. В качестве примеров можно привести следующие семантические типы изменений (далее — типы изменений): реализация новой функциональности, рефакторинг [9], исправление ошибки, косметическое изменение. Существует несколько методов классификации изменений программного кода. Среди них можно выделить следующие группы [10]:

— неформальные методы: автоматизированная классификация изменений посредством анализа комментариев [11, 12], метод поиска и определения типа рефакторинга [13];

— методы анализа синтаксиса изменений: эвристическое сравнение синтаксических деревьев версий [14] и анализ разницы версий при помощи встраиваемых в исходный код тегов [15].

Метод автоматизированной классификации изменений [3], описываемый в настоящей работе, основан на кластеризации значений метрик изменений исходного кода при помощи метода МакКина [1, 2]. В результате его работы производится разбиение множества изменений на заданное число кластеров, каждый из которых соответствует определенному типу изменений.

Формализация задачи

Изменение кода программной системы δ трактуется в работе как отображение множества исходных данных S в другое множество модифицированных данных S^*:

$$\delta{:}S \xrightarrow{\delta} S^*.$$

В некоторых современных системах хранения исходного кода каждому состоянию исходного кода последовательно сопоставляется неотрицательное целое число r, которое называется ревизией или версией программного кода. Поэтому каждое изменение исходных данных можно описать следующим образом:

$$\delta_r{:}S_r \xrightarrow{\delta_r} S_{r+1}.$$

Каждое изменение δ_r может быть отнесено экспертом к некоторому множеству типов изменений t_i, где $t_i \in T$ — тип изменения δ_r. При этом T представляет собой множество типов изменений, специфичное для каждого конкретного проекта. Состав множества T определяется экспертом в зависимости от специфики проекта. Во множество T обычно входят такие типы изменений, как реализация новой функциональности, рефакторинг, исправление ошибки и т. д.

Задача отнесения изменения к тому или иному типу изменений трудоемка и требует высокой квалификации эксперта, так как нет четких критериев оценки типа изменения. Введем функцию интерпретации изменений I, отображающую множество изменений $\{\delta_r\}$ во множество их типов $\{t_i\}$:

$$I{:}\{\delta_r\} \xrightarrow{I} \{t_1,\ t_2,\ \ldots,\ t_n\}.$$

В данном методе предлагается автоматизировать процесс выделения типов изменений при помощи кластеризации метрик изменений. В процессе кластеризации строится множество кластеров изменений C такое, что каждое изменение δ_r относится к некоторому кластеру $c_j \in C$.

Введем функцию автоматизированной классификации изменений I_A, отображающую множество изменений $\{\delta_r\}$ во множество их типов $\{t_i\}$:

$$I_A:\{\delta_r\}\xrightarrow{I_A}\{t_1,\ t_2,\ \ldots,\ t_n\}.$$

Здесь функция автоматизированной классификации I_A есть композиция функций кластеризации I_C и интерпретации кластеров I_T:

$$I_A=I_C\circ I_T,\quad I_C:\{\delta_r\}\xrightarrow{I_C}\{c_1,\ c_2,\ \ldots,\ c_m\},$$

$$I_T:\{c_1,\ c_2,\ \ldots,\ c_m\}\xrightarrow{I_T}\{t_1,\ t_2,\ \ldots,\ t_n\}.$$

Функция кластеризации I_C отображает множество изменений в множество кластеров. Функция интерпретации кластеров I_T отображает множество кластеров C в множество типов изменений T.

Функция кластеризации I_C может быть построена с помощью метода кластеризации Мак-Кина. Кластеризацию изменений будем осуществлять на основе некоторых метрик изменений $M'\delta_r$. Определим понятие метрики изменения через понятие метрики программного обеспечения.

Метрика программного обеспечения (software metric) — это мера M, позволяющая получить численное значение некоторого свойства программного обеспечения S или его спецификаций [16], например, количество строк исходного файла, цикломатическая сложность [18], количество ошибок на строку кода, количество классов и интерфейсов, связность и другие.

Тогда метрику изменения программного обеспечения можно определить как разность значений метрики измененного кода MS_{r+1} и метрики исходного кода MS_r:

$$M'\delta_r=MS_{r+1}-MS_r.$$

Зададим набор метрик программного обеспечения $\mathbf{M}=<M_1, M_2, \ldots, M_k>$. Тогда для каждого изменения δ_r можно построить набор метрик изменения

$$\mathbf{M}'\delta_r=<M_1'\delta_r,\ M_2'\delta_r,\ \ldots,\ M_k'\delta_r>.$$

Тогда $\mathbf{M}'\delta_r$ — это точка в k-мерном пространстве кластеризации. Мерой расстояния между точками в этом пространстве выберем евклидово расстояние ρ:

$$\rho(<x_1,x_2,\ldots,x_k>,\ <y_1,y_2,\ldots,y_k>)=$$

$$=\sqrt{(x_1-y_1)^2+(x_2-y_2)^2+\ldots+(x_k-y_k)^2}.$$

Теперь разбиение на кластеры может быть задано следующим образом:

$$C=\{c_1, c_2, \ldots, c_m\},\ c_j=\{\delta_r, \delta_g\mid\rho\,(\mathbf{M}'\delta_r, \mathbf{M}'\delta_g)<\rho_{\min}\},$$

где $\rho_{\min}$ — величина, определяющая меру близости для включения объектов в один кластер.

Алгоритм кластеризации изменений

Пусть известно число кластеров m, выбран набор метрик $\mathbf{M}$ и мера расстояния ρ между точками пространства кластеризации принята евклидовой. В соответствии с методом кластеризации Мак-Кина алгоритм кластеризации изменений следующий.

1. Произвести начальное разбиение множества объектов $\{\delta_r\}$ случайным образом:

$$C^0=\{c_1, c_2, \ldots, c_n\},\ c_i=\{\delta_r\mid\delta_r\notin c_j,\ j\neq i\}.$$

2. Принять номер итерации $l=1$.

3. Определить центры кластеров cc_i по формуле

$$cc_i=\frac{\sum_r[\delta_r\in c_i]\overline{M'}\delta_r}{\sum_r[\delta_r\in c_i]}.$$

4. Обновить множества распределения объектов по кластерам $C^l=\{c_i\}$:

$$c_i=\{\delta_r\mid\rho(\mathbf{M}'\delta_r, cc_i)=\min\rho(\mathbf{M}'\delta_r, cc_j)\}.$$

5. Проверить условие $\sum_i\|c_i^l\Delta c_i^{l-1}\|=0$, где Δ — операция взятия симметрической разности множеств: $A\Delta B=(A\cup B)\setminus(A\cap B)$. Если условия выполнены, то завершить процесс, иначе перейти к шагу 3 с номером итерации $l=l+1$.

Приведенный алгоритм позволяет автоматизировать процесс разбиения множества изменений на кластеры. В каждый кластер группируются наиболее схожие друг с другом изменения.

Интерпретация результатов кластеризации

Подбор подходящего количества кластеров m и построение функции интерпретации кластеров I_T производится экспертом на основе выборочного анализа изменений, принадлежащих каждому кластеру. Эти задачи значительно менее трудоемки, чем исходная задача, так как на практике имеет смысл различать лишь небольшое число типов изменений.

В процессе построения функции интерпретации кластеров I_T экспертом анализируется изменение исходного кода и комментарий, сопровождающий изменение. В результате устанавливается, какому из типов t_j соответствует данный кластер c_i. При невозможности сопоставления кластера изменений экспертному типу следует повторно обратиться к выбору метрик для кластеризации.

Адекватность классификации

Для оценки согласованности автоматизированной и экспертной классификации в работе [3] используется коэффициент Кохена [4]. Коэффициент Кохена представляет собой меру согласия, с которой два эксперта конкурируют в своих сортировках N элементов по k взаимно исключающим категориям. Эксперта в данном контексте может представлять человек или множество людей, которые коллективно распределяют N элементов, или некоторый алгоритм, который распределяет элементы на основе некоторого критерия.

Выражение для расчета коэффициента согласия Кохена следующее:

$$\kappa = \frac{p_\alpha - p_e}{1 - p_e},$$

где p_α — относительное наблюдаемое согласие между экспертами; p_e — вероятность обусловленности этого согласия случайностью. Если эксперты находятся в абсолютном согласии между собой, тогда $\kappa = 1$. Если же согласие между экспертами отсутствует (но не по причине случайности), тогда $\kappa \le 1$.

По результатам эксперимента [3] получено значение $\kappa = 0{,}79$, которое лежит на границе значительной и превосходной степени согласованности двух методов классификации [5].

Практическое применение метода автоматизированной классификации

Описанный в работе метод может быть использован участниками практически любого проекта по разработке программного продукта. Инструмент, разработанный для применения метода на практике, в момент публикации поддерживает только один тип системы контроля версий — Subverison [19] и языки программирования C++, C#, для которых возможен расчет метрик [16, 17]: цикломатической сложности CC [18]; эффективного количества строк кода (без учета пустых строк и комментариев) $eLOC$; общего количества классов и структур CS.

Использование автоматизированной классификации изменений программного кода в процессе разработки проекта Navi-Manager позволило сократить время на просмотр исходного кода и повысить его качество, оперативно разрешать запросы на список новой функциональности в конкретных версиях без привлечения разработчиков, а также выявить существующую проблему эффективности разработки.

В результате применения автоматизированной классификации изменений исходного кода для анализа проекта Navi-Manager был достигнут значительный уровень согласованности экспертной и автоматизированной классификации.

При использовании метода проявляется проблема смешанных изменений, сочетающих в себе разнородные модификации кода. Настоящим методом не всегда возможна корректная классификация таких изменений. Нужно заметить, что наличие смешанных изменений на практике нежелательно и даже вредно. При их наличии усложняется процедура просмотра кода и другая работа с историей программного продукта. Выделение смешанных изменений в отдельный тип в процессе кластеризации и решение других проблем метода является целью дальнейших исследований.

Еще одно направление дальнейших исследований — анализ устойчивости метода кластеризации и учет эволюции характера изменений в программном коде при анализе длительных промежутков времени разработки проекта.

Преимущества описанного метода классификации изменений по сравнению с другими методами классификации изменений состоят в следующем:

— *объективность*: для анализа используется исходный код, а не, например, комментарий, сопровождающий изменение. Оценка по исходному коду адекватна в отличие от классификации комментариев к изменениям, ведь комментарии могут не в полной мере соответствовать характеру изменений [20];

— *настраиваемость*: множество метрик программного кода выбирается в зависимости от того, по каким аспектам изменений предполагается группировка;

— *адаптивность*: при кластеризации задается лишь результирующее количество групп. Следовательно, для каждого отдельно взятого проекта предложенный метод позволяет выделить специфичные множества изменений, которые затем интерпретируются как те или иные семантические группы изменений;

— *формальность*: классификация изменений производится с помощью формальных статистических методов.

Заключение

В данной работе было предложено использовать автоматизированную классификацию изменений программного кода в управлении процессом разработки программного продукта. Применение автоматизированной классификации позволяет повысить эффективность и качество процесса обзора исходного кода, а также дает возможность автоматизации контроля изменений, вносимых на ответственных этапах разработки. Предлагается применять автоматизированную классификацию изменений программного кода для предоставления списка новой функциональности в конкретной версии продукта для тестировщика, а также построения отчетов распределения изменений по типам для менеджера проекта.

Литература

1. **Барсегян А. А., Куприянов М. С., Степаненко В. В., Холод И. И.** Технологии анализа данных: Data Mining, Visual Mining, Text Mining, OLAP. СПб.: БХВ-Петербург, 2007.

2. **Мандель И. Д.** Кластерный анализ. М.: Финансы и статистика, 1988.

3. **Князев Е. Г., Шопырин Д. Г.** Автоматизированная классификация изменений программного кода методами многомерного статистического ана-

лиза // Информационные технологии. 2008. № 4. С. 10–15. В печати.

4. **Cohen J.** A Coefficient of Agreement for Nominal Scales // Educational and Psychological Measurement. 1960. P. 37–46.

5. **Emam E. K.** Benchmarking Kappa for Software Process Assessment Reliability Studies // Technical Report ISERN-98-0. International Software Engineering Research Network, 1998. http://citeseer.ist.psu.edu/elemam98benchmarking.html

6. **TortoiseSVN.** A Subversion client, implemented as a windows shell extension. http://tortoisesvn.tigris.org

7. **Navi-Manager Vessel Monitoring System.** http://www.transas.com/products/shorebased/manager/ http://www.transas.ru/products/shorebased/fleet/navi-manager/

8. **KDE.** A powerful Free Software graphical desktop environment for Linux and Unix workstations. http://www.kde.org

9. **Фаулер М.** Рефакторинг: улучшение существующего кода. СПб.: Символ-Плюс, 2003.

10. **Kagdi H., Collard M., Maletic J.** Towards a Taxonomy of Approaches for Mining of Source Code Repositories // ACM SIGSOFT Software Engineering Notes: Proc. of the 2005 Intern. Workshop on Mining Software Repositories MSR '05. St. Louis, Missouri, 2005. P. 1–5.

11. **Hassan A. E., Holt R. C.** Source Control Change Messages: How Are They Used And What Do They Mean? 2004. http://www.ece.uvic.ca/~ahmed/home/pubs/CVSSurvey.pdf

12. **Mockus A., Votta L. G.** Identifying reasons for software change using historic databases: Proc. of the Intern. Conf. on Software Maintenance (ICSM). San Jose, California, 2000. P. 120–130.

13. **Demeyer S., Ducasse S., Nierstrasz O.** Finding refactorings via change metrics: Proc. of the ACM Conf. on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA '00). 2000. P. 166–178.

14. **Raghavan S., Rohana R., Podgurski A., Augustine V.** Dex: A Semantic-Graph Differencing Tool for Studying Changes in Large Code Bases: Proc. of 20th IEEE Intern. Conf. on Software Maintenance (ICSM '04). Chicago, Illinois, 2004. P. 188–197.

15. **Maletic J. I., Collard M. L.** Supporting Source Code Difference Analysis: Proc. of IEEE Intern. Conf. on Software Maintenance (ICSM '04). Chicago, Illinois, 2004. P. 210–219.

16. **Орлов С. А.** Технологии разработки программного обеспечения: Учебник для вузов. СПб.: Питер, 2004.

17. **Липаев В. В.** Выбор и оценивание характеристик качества программных средств: Методы и стандарты. М.: Синтег, 2001.

18. **McCabe T. J.** A Complexity Measure // IEEE Trans SE-2. 1976. N 4.

19. **Collins-Sussman B., Fitzpatrick B. W., Pilato M.** Version Control with Subversion. O'Relly. 2004. http://svnbook.red-bean.com/

20. **Zimmermann T., Weigerber P., Diehl S., Zeller A.** Mining Version Histories to Guide Software Changes: Proc. of 26th Intern. Conf. on Software Engineering (ICSE '04). Edinburgh, Scotland, United Kingdom, 2004. P. 563–572.

УДК 681.3

ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ПОДПИСИ НА ОСНОВЕ СВЕРТКИ ИНДИВИДУАЛЬНЫХ ПАРАМЕТРОВ

М. Ю. Ананьев,
аспирант
Л. В. Гортинская,
научный сотрудник
Н. А. Молдовян,
доктор техн. наук, профессор
НФ ФГУП НИИ «Вектор» — специализированный центр программных систем «Спектр»

Предлагается новый протокол коллективной подписи, устраняющий недостаток ранее известных протоколов такого типа, заключающийся в участии в протоколе доверенной стороны, которой передаются личные секретные ключи пользователей, подписывающих электронный документ.

Введение

В основе процедур аутентификации электронной информации лежат алгоритмы электронной цифровой подписи (ЭЦП), при разработке которых обычно используются три вычислительно сложные задачи:

1) факторизация составных чисел вида $n = qr$, где q и r — два больших простых числа, удовлетворяющих специальным требованиям [1];

2) нахождение дискретного логарифма по простому модулю p [2];

3) нахождение дискретного логарифма на эллиптической кривой (ЭК) специального вида [3].

Предложенная недавно [4] в качестве нового криптографического примитива трудная вычислительная задача извлечения корней большой простой степени по большому простому модулю специального вида дала возможность построить алгоритмы ЭЦП, позволяющие осуществить свертку индивидуальных параметров, генерируемых при вычислении подписи, в некоторые коллективные значения, по которым формируется коллективная ЭЦП (КЭЦП) малого размера. В отличие от известных протоколов аналогичного типа [5, 6] протокол на основе свертки индивидуальных параметров устраняет необходимость передачи индивидуальных секретных ключей некоторой доверенной стороне, что делает его весьма перспективным для практического применения.

В настоящей работе рассматривается механизм формирования КЭЦП на основе процедур свертки индивидуальных параметров, показывается возможность его переноса на схемы ЭЦП, основанные на трудности дискретного логарифмирования, предлагаются протоколы КЭЦП, использующие алгоритмы генерации ЭЦП, специфицируемые ГОСТ Р 34.10–94 и ГОСТ Р 34.10–2001, и формально доказывается стойкость предложенных протоколов КЭЦП.

Коллективная подпись для двух пользователей

Рассмотрим схему КЭЦП, использующую трудность извлечения корней большой простой степени k по простому модулю вида $p = Nk^s + 1$, где N — четное число, $s \geq 2$ и k — простое число достаточно большого размера. Открытый ключ y вычисляется по формуле $y = x^k \bmod p$. Подписью является пара чисел S и R. Формирование подписи к сообщению M выполняется следующим образом.

1. Выбрать случайное значение $t < p - 1$ и вычислить $R = t^k \bmod p$.

2. Используя некоторую специфицированную хэш-функцию F_H, вычислить $H = F_H(M)$ и значение некоторой сжимающей функции $f(R, M)$, в качестве которой можно использовать $f(R, M) = RH \bmod \delta$, где δ — большое простое число, например δ, имеющее длину 160 бит.

3. Вычислить второй элемент ЭЦП: $S = x^{f(R, M)} \times t \bmod p$.

Соотношением проверки подписи является уравнение $S^k = y^{f(R, M)} R \bmod p$.

Реализация единой подписи, принадлежащей одновременно двум пользователям A и B, обладающим открытыми ключами $y_A = x_A{}^k \bmod p$ и $y_B = x_B{}^k \bmod p$ соответственно, выполняется следующим образом.

1. Пользователь A генерирует $R_A = r_A^k \bmod p$, где r_A — случайное число.

2. Пользователь B генерирует $R_B = r_B^k \bmod p$, где r_B — случайное число.

3. Вычисляют $R = R_A R_B \bmod p$.

4. A вычисляет $S_A = x_A^{f(R)} r_A^H \bmod p$.

5. B вычисляет $S_B = x_B^{f(R)} r_B^H \bmod p$.

6. Вычисляют общую подпись (R, S):

$$S = S_A S_B \bmod p.$$

Проверка такой коллективной подписи осуществляется по уравнению $S^k = (y_A y_B)^{f(R)} R^H \bmod p$, в котором произведение $y_A y_B$ может быть заменено сверткой индивидуальных открытых ключей пользователей: $y_{AB} = y_A y_B \bmod p$. Из приведенной процедуры генерации КЭЦП, принадлежащей двум пользователям, вытекают следующие свойства подписи:

1) общая подпись имеет размер обычной подписи;

2) подписи (R_A, S_A) и (R_B, S_B) недействительны к H;

3) можно сформировать коллективную подпись для произвольного числа пользователей m ($m = 2, 3, 4$...).

Обобщенная схема формирования КЭЦП для *m* пользователей

При реализации протокола КЭЦП на основе свертки индивидуальных параметров, генерируемых подписывающими сторонами в процессе формирования подписи, обеспечиваются следующие важные для практики свойства.

• Целостность — из КЭЦП, принадлежащей заданному подмножеству пользователей, нельзя вычислить правильную подпись, соответствующую другому подмножеству пользователей.

• Независимость от пользователей — КЭЦП может сформировать любая группа пользователей, независимо от их числа и состава.

• Одновременность генерации КЭЦП — все значения, возникающие на промежуточных этапах процедуры генерации КЭЦП, не являются правильными подписями к каким-либо сообщениям, и из них не могут быть вычислены индивидуальные секретные ключи или значения.

• Возможность обнаружить нарушителя — умышленные или неумышленные отклонения от процедур, специфицируемых протоколом, обнаруживаются по проверочному уравнению, причем анализ индивидуальных параметров позволяет установить, кто из пользователей осуществил неправильные действия.

• Использование стандартной инфраструктуры открытых ключей — никакие дополнительные изменения в используемые на практике процедуры распределения открытых ключей не требуются.

В качестве базовой для протокола коллективной подписи была принята идея использования коллективного открытого ключа, являющегося функцией открытых ключей подписывающих. Коллективный открытый ключ некоторой произвольно задаваемой совокупности m пользователей, каждый из которых является владельцем соответствующего открытого ключа из множества Y_1, Y_2, ..., Y_m, представляет собой некоторое значение $Y = f(Y_1, Y_2, ..., Y_m)$. Общая схема формирования коллективной подписи представлена на рис. 1, а процедура проверки подлинности КЭЦП — на рис. 2.

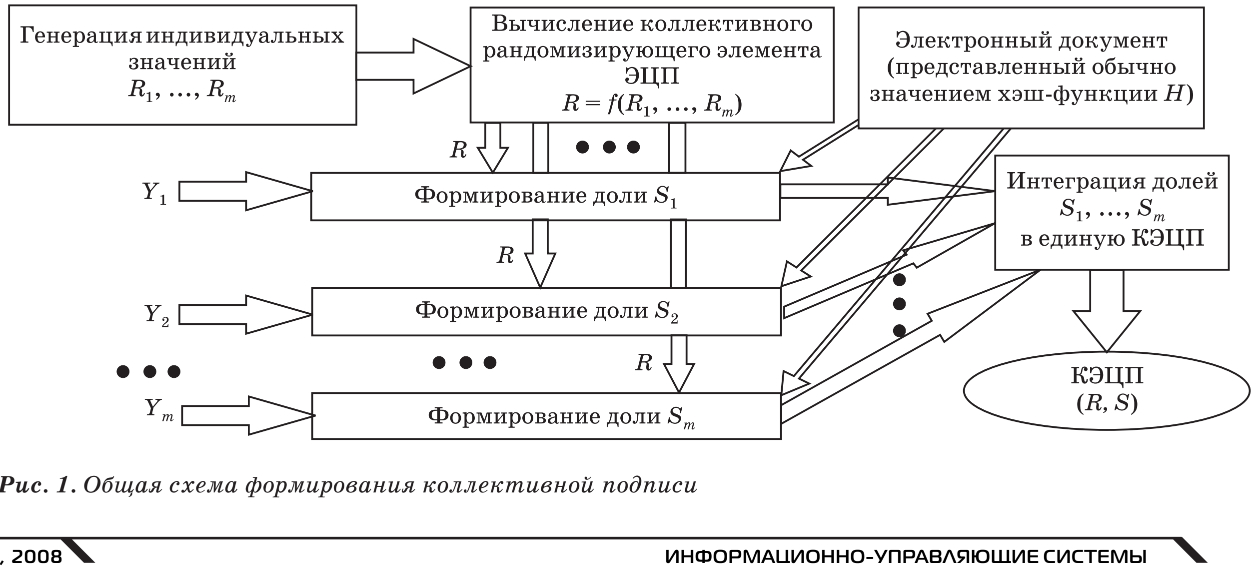
Представленная выше общая схема формирования КЭЦП была реализована в виде конкретных алгоритмов и протоколов, удовлетворяющих перечисленным требованиям. Использовались следующие трудные вычислительные задачи:

• извлечение корней большой простой степени по большому простому модулю;

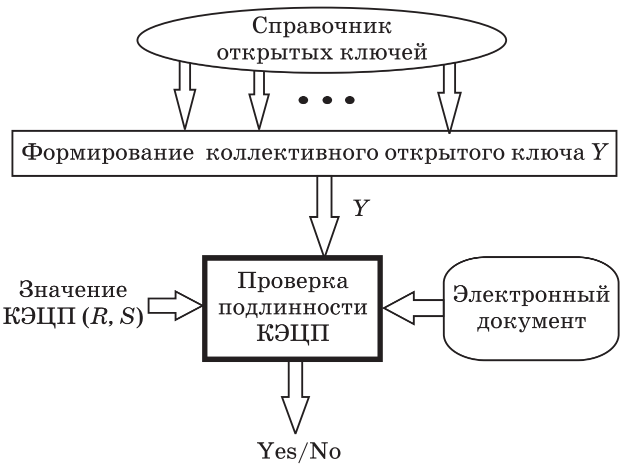
• дискретное логарифмирование в мультипликативной группе большого простого порядка;

• дискретное логарифмирование в группе точек эллиптической кривой специального вида.

Наибольший интерес представляют алгоритмы, основанные на последней задаче, поскольку в этом случае обеспечивается наибольшая производитель-



■ ***Рис. 1.*** *Общая схема формирования коллективной подписи*



■ *Рис. 2. Процедура проверки подлинности КЭЦП*

ность процедур генерации и проверки подписи. Достоинство предложенной идеологии КЭЦП состоит в использовании стандартной инфраструктуры открытых ключей и возможности реализации с применением процедур генерации и проверки, регламентируемых российскими стандартами ЭЦП.

Рассмотрим реализацию описанной идеологии построения протоколов КЭЦП на основе трудности задачи дискретного логарифмирования в конечной мультипликативной группе (на примере использования ЭЦП Шнорра и ГОСТ Р 34.10–94 в качестве базовой схемы) и трудности логарифмирования на ЭК (на примере использования ГОСТ Р 34.10–2001).

Реализация на основе алгоритма Шнорра

Как указано выше, схема Шнорра основывается на сложности задачи дискретного логарифмирования. Общими параметрами являются: p и q — большие простые числа такие, что q делит $p-1$; α — число, относящееся к показателю q по модулю p, т. е. $\alpha^q \bmod p = 1$. Секретный ключ представляет собой случайно генерируемое число k, $1 < k < q$. Формирование открытого ключа осуществляется путем возведения числа α в степень k по модулю p: $y = \alpha^k \bmod p$.

Вычисление подписи к сообщению M включает следующие шаги.

1. Генерируется случайное число t, $1 < t < q$, играющее роль разового секретного ключа.
2. Вычисляется значение $R = \alpha^t \bmod p$.
3. К сообщению M присоединяется число R, и вычисляется хэш-функция H от значения $M\|R$: $E = F_H(M\|R)$. Значение E является первой частью подписи.
4. Вычисляется вторая часть подписи: $S = t + kE \bmod q$, где k — секретный ключ.

Процедура проверки подлинности ЭЦП.

1. Вычисляется значение R': $R' = \alpha^S y^{-E} \bmod p$.
2. К сообщению M присоединяется число R', и вычисляется хэш-функция H от значения $M\|R'$: $E' = F_H(M\|R')$.
3. Сравниваются значения E и E'. Если $E = E'$, то подпись признается верной.

Протокол коллективной подписи на основе схемы Шнорра реализуется следующим образом. Каждый i-й пользователь формирует открытый ключ вида $y_i = \alpha_i^k \bmod p$, k_i — личный (секретный) ключ, $i = 1, 2, \ldots, m$.

1. Каждый подписывающий генерирует разовый случайный секретный ключ — число t_i, затем вычисляет $R_i = \alpha_i^t \bmod p$ и предоставляет это значение для коллективного использования.
2. Вычисляется произведение

$$R = R_1 R_2 R_3 \ldots R_m \bmod p.$$

3. Вычисляется $E = F_H(M\|R)$.
4. Каждый i-й пользователь вычисляет свою долю второй части подписи: $S_i = t_i + k_i E \bmod q$.

Коллективной подписью является пара чисел (R, S), где S вычисляется по формуле

$$S = S_1 + S_2 + S_3 + \ldots + S_m \bmod q.$$

Проверка подписи осуществляется по алгоритму, описанному выше. Покажем корректность алгоритма:

$$R = y^{-E}\alpha^S \bmod p = y^{-E}\alpha^{\sum_{i=1}^{m} S_i} \bmod p =$$
$$= y^{-E}\alpha^{\sum_{i=1}^{m}(t_i + k_i E)} \bmod p =$$
$$= y^{-E}\alpha^{\sum_{i=1}^{m} t_i}\alpha^{E\sum_{i=1}^{m} k_i} \bmod p = y^{-E}\alpha^{\sum_{i=1}^{m} t_i} y^E \bmod p =$$
$$= \alpha^{\sum_{i=1}^{m} t_i} \bmod p = \prod_{i=1}^{m} R_i \bmod p.$$

Реализация на основе ГОСТ Р 34.10–94

Стандарт ЭЦП ГОСТ Р 34.10–94 регламентирует использование простого числа p такого, что $510 \le |p| \le 512$ бит либо $1022 \le |p| \le 1024$ бит, где $|p|$ — разрядность p в двоичном представлении, причем число $p-1$ содержит большой простой делитель $2^{255} \le q \le 2^{256}$ либо $2^{511} \le q \le 2^{512}$ соответственно. Специфицируемые алгоритмы генерации и проверки ЭЦП используют число $\alpha \ne 1$ такое, что $\alpha^q \bmod p = 1$. Вычисление ЭЦП осуществляется следующим образом.

1. Генерируется случайное число t, $1 < t < q$.
2. Вычисляется значение $R = (\alpha^t \bmod p) \bmod q$, являющееся первой частью подписи.
3. По ГОСТ Р 34.11–94 вычисляется хэш-функция H от подписываемого сообщения.
4. Вычисляется вторая часть подписи: $S = tH + kR \bmod q$.

Если $S = 0$, процедура генерации подписи повторяется.

Процедура проверки подлинности ЭЦП.

1. Проверяется выполнение условий $R < q$ и $S < q$. Если они не выполняются, то подпись недействительна.

2. Вычисляется значение

$$R' = (\alpha^{S/H} y^{-R/H} \bmod p) \bmod q.$$

3. Сравниваются значения R и R'. Если $R = R'$, то подпись признается действительной.

Рассмотрим реализацию КЭЦП на основе этого стандарта. Каждый i-й пользователь формирует открытый ключ вида $y_i = \alpha_i^k \bmod p$, где α — генератор подгруппы достаточно большого простого порядка q (т. е. $\alpha^q \bmod p = 1$). Коллективным открытым ключом является произведение

$$y = y_1 y_2 y_3 ... y_m \bmod p.$$

Коллективная подпись формируется следующим путем. Каждый подписывающий выбирает разовый случайный секретный ключ — число t_i, затем вычисляет $R_i = (\alpha_i^t \bmod p) \bmod q$ и предоставляет это значение для коллективного использования. Далее вычисляется произведение

$$R = R_1 R_2 R_3 ... R_m \bmod q.$$

Затем каждый пользователь по своему значению R_i и величине H вычисляет свою долю подписи $S_i = t_i H + k_i R \bmod q$.

Коллективной подписью является пара чисел (R, S), где S вычисляется по формуле

$$S = S_1 + S_2 + S_3 + ... + S_m \bmod q.$$

Проверка коллективной подписи осуществляется по проверочной формуле

$$R' = (\alpha^{S/H} y^{-R/H} \bmod p) \bmod q.$$

Если $R = R'$, то КЭЦП совокупности пользователей $1, 2, ..., m$ является подлинной, так как она могла быть сформирована только при участии каждого пользователя из этой группы, поскольку для ее формирования требуется использование секретного ключа каждого из них. Отметим, что аутентификация значений R_i осуществляется автоматически при проверке подлинности коллективной ЭЦП. Если нарушитель попытается подменить какое-либо из этих значений или заменить ранее использованными значениями, то факт вмешательства в протокол будет сразу же выявлен при проверке подлинности ЭЦП, т. е. будет получено $R' \neq R$. Легко видеть, что размер КЭЦП не зависит от m.

Покажем корректность предложенного алгоритма КЭЦП. Подставив подпись (R, S) в проверочное уравнение

$$R = (\alpha^{S/H} y^{-R/H} \bmod p) \bmod q,$$

где

$$S = \sum_{i=1}^{m} S_i \bmod q \quad \text{и} \quad R = \prod_{i=1}^{m} R_i \bmod q,$$

убеждаемся, что оно выполняется:

$$R = \left(\alpha^{\sum_{i=1}^{m} S_i / H} \left(\prod_{i=1}^{m} y_i \right)^{-R/H} \bmod p \right) \bmod q =$$

$$= \left(\prod_{i=1}^{m} \alpha^{S_i/H} \prod_{i=1}^{m} y_i^{-R/H} \bmod p \right) \bmod q =$$

$$= \left(\prod_{i=1}^{m} \left(\alpha^{S_i/H} \alpha^{-k_i R/H} \bmod p \right) \right) \bmod q =$$

$$= \left(\prod_{i=1}^{m} \left(\alpha^{(t_i H + k_i R)/H} \alpha^{-k_i R/H} \bmod p \right) \right) \bmod q =$$

$$= \left(\prod_{i=1}^{m} \alpha^{t_i} \bmod p \right) \bmod q =$$

$$= \left(\prod_{i=1}^{m} \left(\alpha^{t_i} \bmod p \right) \bmod q \right) \bmod q = \left(\prod_{i=1}^{m} R_i \right) \bmod q.$$

Реализация на основе ГОСТ Р 34.10–2001

Стандарт ЭЦП ГОСТ Р 34.10–2001 регламентирует использование простого числа p — модуля ЭК, которая задается в декартовой системе координат уравнением $y^2 = x^2 + ax + b \bmod p$ с коэффициентами a и b: $a, b \in GF_p$; простого числа q — порядка циклической подгруппы точек ЭК; точки G с координатами (x_G, y_G), такой, что $G \neq O$, $qG = O$. Секретным ключом является достаточно большое целое число k, а открытым ключом — точка $Q = kG$. Формирование подписи (R, S) осуществляется в соответствии со следующим алгоритмом.

1. Генерируется случайное целое число t, $0 < t < q$.

2. Вычисляется точка ЭК $C = tG$ и определяется значение $R = x_C \bmod q$, где x_C — координата точки C.

3. Вычисляется значение $S = (Rk + te) \bmod q$, где $e = H \bmod q$, H — значение хэш-функции от подписываемого сообщения.

Подписью является пара чисел R и S.

Проверка подписи заключается в вычислении координат точки ЭК:

$$C = ((Se^{-1}) \bmod q)G + ((q - R)e^{-1} \bmod q)Q, \quad (1)$$

определении значения $R' = x_C \bmod q$ и проверке выполнения равенства $R' = R$.

Протокол КЭЦП реализуется следующим образом. Каждый i-й пользователь формирует открытый ключ вида $Q_i = Gk_i$. Коллективным открытым ключом является сумма

$$Q = Q_1 + Q_2 + Q_3 + ... + Q_m.$$

Коллективная подпись формируется следующим путем. Каждый подписывающий выбирает разовый случайный секретный ключ — число t_i, затем вычисляет $C_i = t_i G$ и предоставляет это значение для коллективного использования. Далее вычисляется сумма всех точек C_i

$$C = C_1 + C_2 + C_3 + \ldots + C_m,$$

по которой вычисляется значение $R = x_C \bmod q$. После этого каждый i-й пользователь по своему секретному ключу, значению t_i и величине e вычисляет свою долю подписи $S_i = (Rk_i + t_i e) \bmod q$.

Коллективной подписью является пара чисел R и S, где S вычисляется по формуле

$$S = S_1 + S_2 + S_3 + \ldots + S_m \bmod q.$$

Проверка коллективной подписи осуществляется по проверочной формуле. Если

$$R' = x_{C'} \bmod q = R,$$

где точка C' вычисляется по проверочному соотношению (1), то КЭЦП совокупности пользователей 1, 2, ..., m является подлинной, так как она могла быть сформирована только при участии каждого пользователя из этой группы, поскольку для ее формирования требуется использование секретного ключа каждого из них.

Сведение стойкости протокола КЭЦП к стойкости базового алгоритма ЭЦП

При разработке криптографических протоколов важным вопросом является доказательство их стойкости. В предлагаемых протоколах КЭЦП это может быть сделано путем формального доказательства того факта, что если протокол КЭЦП не является стойким, то тогда может быть взломан базовый алгоритм ЭЦП. Из этого доказательства вытекает безопасность протокола при использовании стойкой базовой схемы ЭЦП. Если в протоколе использовать стойкие апробированные алгоритмы ЭЦП, например стандарты ЭЦП, то и сам протокол будет стойким.

Рассмотрим формальное доказательство стойкости протокола КЭЦП при использовании проверочного уравнение $R = (\alpha^{S/H}\alpha^{-R/H} \bmod p) \bmod q$, регламентируемого стандартом ЭЦП ГОСТ Р 34.10–94. При доказательстве следует рассмотреть две возможности: подделки КЭЦП и вычисления секретного ключа одного из пользователей, являющегося совладельцем коллективной подписи, объединенными усилиями остальных совладельцев КЭЦП. Рассмотрим первый вариант.

Очевидно, что для посторонних нарушителей, не являющихся абонентами рассматриваемой системы ЭЦП, подделка КЭЦП так же сложна, как и подделка индивидуальной подписи некоторого отдельного пользователя. Новые возможности возникают у пользователей, объединяющих свои усилия, чтобы сформировать КЭЦП, относящуюся к коллективу, в который кроме них входит еще один или несколько других пользователей, которые об этом не оповещаются (доказательство для обоих случаев аналогично). Пусть $m - 1$ пользователей хотят сформировать КЭЦП, проверяемую по коллективному открытому ключу $y = y'y_m \bmod p$, где $y' = \prod_{i=1}^{m} y_i \bmod p$, т. е. $m - 1$ пользователей объединяют свои усилия, чтобы сформировать пару чисел (R, S) такую, что $R = (\alpha^{S/H}(y'y_m)^{-R/H} \bmod p) \bmod q$. Это означает, что они могут подделать подпись «под» открытый ключ $y^* = y'y_m \bmod p$, т. е. вычислить значения R и S, которые удовлетворяют уравнению $R = (\alpha^{S/H}(y^*)^{-R/H} \bmod p) \bmod q$. Из интуитивных соображений ясно, что последнее означает возможность подделать цифровую подпись в базовой схеме ЭЦП, поскольку открытый ключ y^* имеет случайное значение, так же как и открытый ключ, принадлежащий какому-то отдельному пользователю. Рассмотрим формальное доказательство этого факта. Используя предполагаемую возможность, коллективный нарушитель формирует КЭЦП (R^*, S^*), соответствующую коллективному открытому ключу $y = y'y'_m \bmod p$, где в качестве y'_m взято значение $y'_m = y_m/y' \bmod p$. Коллективная подпись удовлетворяет соотношению

$$R^* = (\alpha^{S^*/H} y^{-R^*/H} \bmod p) \bmod q =$$
$$= \left(\alpha^{S^*/H} (y'y'_m)^{-R^*/H} \bmod p\right) \bmod q \Rightarrow$$
$$\Rightarrow R^* = \left(\alpha^{S^*/H} y_m^{-R^*/H} \bmod p\right) \bmod q.$$

Последнее выражение показывает, что (R^*, S^*) является подлинной индивидуальной ЭЦП m-го пользователя. Таким образом, мы формально показали, как возможность подделать коллективную подпись может быть легко использована для подделки подписи в базовой схеме ЭЦП.

Рассмотрим атаку, осуществляемую объединенными усилиями подмножества совладельцев коллективной подписи и направленную на вычисление секретного ключа другого совладельца КЭЦП. Рассмотрим случай, связанный с наибольшими возможностями у атакующих. Покажем, что если $m - 1$ совладельцев КЭЦП могут вычислить секретный ключ m-го совладельца, против которого направлена атака, то тогда они могут вычислить секретный ключ по индивидуальной ЭЦП, сформированной по базовому алгоритму ЭЦП. Пусть (R^*, S^*) — это ЭЦП, сформированная m-м пользователем к документу, соответствующему хэш-функции H. Тогда выполняется

$$R^* = (\alpha^{S/H}(y_m)^{-R^*/H} \bmod p) \bmod q. \qquad (2)$$

Атакующие генерируют случайные значения t_i и вычисляют $R_i = (\alpha_i^{t} \bmod p) \bmod q$ для $i = 1, 2, \ldots, m - 1$. После этого они вычисляют параметры $R = \left(R^* \prod_{i=1}^{m-1} y_i \bmod p\right) \bmod q$ и S_i, удовлетворяющие уравнениям

$$R_i = \left(\alpha^{S_i/H} y_i^{-R/H} \bmod p\right) \bmod q, \qquad (3)$$

где $i = 1, 2, \ldots, m-1$. Вводя обозначение

$$y^* = y^{R^*/R} \bmod p, \qquad (4)$$

из (3) и (4) получаем

$$R = (\alpha^{S/H}(Y)^{-R/H} \bmod p) \bmod q,$$

где $S = \left(S^* + \sum_{i=1}^{m-1} S_i\right) \bmod q$ и $Y = \left(y^* \prod_{i=1}^{m-1} y_i\right) \bmod p$. Это означает, что атакующие получили правильное значение коллективной подписи (R, S), в которой участвуют они и еще один пользователь, обладающий открытым ключом $y^* = \alpha^{k^*} \bmod p$. Согласно допущению, из полученной коллективной подписи атакующие могут вычислить секретный ключ k^*. Из (4) легко получить

$$k = Rk^*/R^* \bmod q.$$

Таким образом, атакующие вычислили секретный ключ m-го пользователя по его индивидуальной ЭЦП, сформированной в рамках базового алгоритма ЭЦП. То есть было формально доказано, что если протокол КЭЦП допускает вычисление секретного ключа одного из пользователей, то по индивидуальной ЭЦП, сформированной по базовому алгоритму ЭЦП, также можно вычислить секретный ключ. Это означает, что предложенный протокол КЭЦП не снижает стойкости базового алгоритма ЭЦП. (С интуитивной точки зрения, доказанное утверждение изначально очевидно. Однако ценность данного доказательства состоит в том, что оно является формальным.)

Заключение

В данной работе показана возможность применения подхода к построению протокола КЭЦП на основе процедур свертки индивидуальных параметров отдельных пользователей в коллективные значения с использованием алгоритмов на основе сложности задачи дискретного логарифмирования в конечной мультипликативной группе и в группе точек ЭК, включая использование стандартов ЭЦП, действующих в России. Показана сводимость безопасности предложенных протоколов КЭЦП к безопасности алгоритмов ЭЦП, на основе которых строятся данные протоколы.

Работа выполнена при поддержке гранта РФФИ 08-07-00096-а.

Литература

1. **Молдовян Н. А.** Практикум по криптосистемам с открытым ключом. СПб.: БХВ-Петербург, 2007. 298 с.
2. **Pieprzyk J., Hardjono Th., Seberry J.** Fundamentals of Computer Security. Berlin: Springer-Verlag, 2003. 677 p.
3. **Венбо Мао.** Современная криптография. Теория и практика. М.; СПб.; Киев: Издательский дом «Вильямс», 2005. 763 с.
4. **Koblitz N.** A Course in Number Theory and Cryptography. Berlin: Heidelberg; N. Y.: Springer, 1994. 235 p.
5. **Молдовян Н. А., Молдовяну П. А.** Новые протоколы слепой подписи // Безопасность информационных технологий. 2007. № 3.
6. **Boldyreva A.** Efficient Threshold Signature, Multisignature and Blind Signature Shemes Based on the Gap-Diffi-Hellman-Group Signature Sheme // LNCS. 2003. Vol. 2139. P. 31–46.

УДК 004.728.3.057.4

ИСПОЛЬЗОВАНИЕ ИДЕНТИФИКАТОРОВ АБОНЕНТОВ ДЛЯ РЕЗЕРВИРОВАНИЯ КАНАЛА МНОЖЕСТВЕННОГО ДОСТУПА

С. Г. Марковский,
канд. техн. наук, доцент
А. М. Тюрликов,
канд. техн. наук, доцент
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Рассмотрены режимы передачи запросов, используемые в стандарте IEEE 802.16, для резервирования канала множественного доступа. Вводится способ передачи запросов с использованием идентификаторов абонентов. Показано, что предложенный способ позволяет уменьшить среднюю задержку передачи запроса и может быть реализован в рамках режима multicast polling стандарта IEEE 802.16.

Введение

Последние годы характеризуются бурным развитием беспроводных систем передачи информации. При этом ведущая роль отводится беспроводным городским сетям связи, построенным на базе стандарта IEEE 802.16 [1]. Для таких систем характерно наличие базовой станции (БС), большого числа абонентов и двух каналов связи: канала множественного доступа (вход канала доступен всем абонентам) — от абонентов к БС, называемого *восходящим каналом*, и широковещательного канала от БС к абонентам (выход канала доступен всем абонентам), называемого *нисходящим каналом*.

Абоненты используют часть ресурсов восходящего канала для передачи служебной информации, называемой в дальнейшем *запросами*, для резервирования времени последующей передачи данных. Базовая станция по нисходящему каналу сообщает абонентам о выделяемых ресурсах восходящего канала для передачи данных. При одновременной передаче запросов от нескольких абонентов в восходящем канале возникает конфликт, и БС не может правильно принять информацию. Для разрешения конфликта стандарт IEEE 802.16 предлагает использовать алгоритм, в котором абонент повторяет передачу запроса через случайные интервалы времени до момента его успешного приема БС.

В настоящей статье для разрешения конфликтов предлагается использовать идентификаторы (адреса) абонентов. Применение этого подхода позволяет повысить оперативность доставки запросов по сравнению с подходами, которые используются при разрешении конфликтов в современных стандартах.

Организация передачи запросов в стандарте IEEE 802.16

В стандарте IEEE 802.16 абонент, желающий обмениваться данными, некоторым образом взаимодействуя с БС, регистрируется в системе. По завершении регистрации БС присваивает данному абоненту *уникальный идентификатор*. Каждому зарегистрированному абоненту БС по определенному правилу предоставляет относительно небольшую долю ресурса восходящего канала для передачи запроса. Абонент передает запрос к БС после появления каждой новой порции данных. В запросе абонент указывает ресурс, необходимый ему для передачи этой порции данных в восходящем канале. Базовая станция, используя определенную дисциплину планирования, принимает решение о выделении (или не выделении) запрашиваемого ресурса и передает эту информацию абонентам.

В стандарте IEEE 802.16 предусмотрено три основных режима передачи запроса абонента. Обозначены эти режимы в стандарте терминами unicast polling, multicast polling, broadcast polling. При этом может быть использовано частотное, временное, кодовое разделение ресурса канала и их комбинация. Вне зависимости от вида разделения ресурса канала будем полагать, что для передачи запросов выделяется некоторая фиксированная доля ресурса канала. Эту долю далее будем называть *окном для передачи запроса*.

В режиме unicast polling БС выделяет каждому абоненту свое окно для передачи запроса.

В режиме broadcast polling БС назначает всем абонентам одну и ту же группу окон для передачи запросов. При одновременной передаче запроса от разных абонентов в одном *окне* возникает конфликт, который разрешается в соответствии с определенным алгоритмом.

Режим multicast polling можно рассматривать как обобщение режимов unicast polling и broadcast polling. В этом режиме все множество абонентов разбивается на подмножества. Всем абонентам из одного подмножества назначается одна и та же группа окон для передачи.

В дополнение к трем основным режимам передачи запроса стандарт 802.16 позволяет передавать запрос, присоединяя его к передаче данных. Такой режим получил название piggybacking.

В настоящей работе ограничимся рассмотрением только случая, когда входной поток данных характеризуется тем, что порции данных появляются через случайные интервалы времени с достаточно низкой интенсивностью. Кроме того, не предъявляется конкретных требований к времени обработки этих данных. Примером такого потока является HTTP-трафик. Подобные входные потоки данных чаще всего относят к классам nrtPS (Non-Real-Time Polling Service) и BE (Best Effort Service) [1]. Стандарт рекомендует для этих классов использовать режимы передачи запросов broadcast polling и multicast polling.

Модель системы

Время работы системы разбивается на кадры одинаковой длительности. Кадры пронумерованы целыми неотрицательными числами. Далее в работе для краткости изложения кадр с номером t будем называть кадром t. Будем полагать, что в системе имеется M абонентов. Каждому абоненту, успешно прошедшему регистрацию в системе, ставится в соответствие уникальный двоичный l-разрядный идентификатор из множества $\{0, 1, 2, ..., M-1\}$, $M = 2^l$. Относительно процессов появления запросов у абонентов и организации передачи этих запросов сделаем ряд допущений.

Допущение 1. В каждом кадре для передачи запроса выделяется **одно окно**.

Допущение 2. В каждом окне может возникнуть одна **из трех ситуаций**:

- в окне передает запрос один абонент (ситуация «успех» (У));
- в окне не передает запрос ни один абонент (ситуация «пусто» (П));
- в окне передают запросы два или более абонентов, при этом ни один из запросов не может быть успешно принят БС (ситуация «конфликт» (К)).

Допущение 3. Будем полагать, что **шумы в восходящем канале отсутствуют**. При этом БС, анализируя ситуацию в окне, достоверно определяет, какое из трех возможных событий произошло в окне. Если в окне один абонент передает запрос (ситуация «успех»), то БС безошибочно принимает информацию, передаваемую в запросе.

Допущение 4. Базовая станция в нисходящем канале кадра t передает абонентам свое решение о распределении ресурсов восходящего канала в кадре t по результатам наблюдения окна для запроса в кадре $t-1$. Считается, что абоненты узнают это решение к началу кадра t.

Допущение 5. Будем полагать, что **шумы в нисходящем канале отсутствуют**. При этом абоненты безошибочно принимают решение БС о распределении ресурсов восходящего канала.

Допущение 6. У каждого абонента имеется **буфер для хранения $b+1$ запросов**, где $b > 0$. Ячейки буфера пронумерованы числами от 0 до b. В канал может передаваться только тот запрос, который хранится в ячейке с номером 0. Абонент по определенному правилу удаляет успешно переданный запрос из нулевой ячейки буфера. В начале работы системы эта ячейка пуста. В каждом кадре в свободные ячейки буфера с номерами от 1 до b записываются те запросы, которые возникли в течение этого кадра. Запись происходит в порядке поступления. Те запросы, которые не поместились в буфер, теряются.

Допущение 7. Если к началу кадра t абонент узнает, что нулевая ячейка буфера пуста, то запрос, который хранился в ячейке с номером 1, переписывается в ячейку с номером 0 и т. д. Считается, что все эти действия происходят мгновенно.

Допущение 8. Обозначим через $X_i(t)$ случайную величину, равную числу запросов, возникших в окне t у абонента с номером i. Для всех $t >= 0$ и $i = 0, ..., M-1$ случайные величины $X_i(t)$ **статистически независимы и одинаково распределены**. Будем полагать, что в одном кадре у каждого абонента может появиться **не более одного запроса**. Вероятность появления запроса обозначим через y. Тогда $E[X_i(t)] = y$ для всех $t >= 0$ и $i = 0, ...,$

$M-1$, а $E\left[\sum_{i=0}^{M-1} X_i(t)\right] = My$. В дальнейшем будем называть входной поток запросов, удовлетворяющий данному допущению, *бернуллиевским входным потоком*.

С учетом сделанных допущений модель полностью задается следующими тремя параметрами: M — число абонентов; b — число ячеек в буфере для хранения поступающих запросов; λ — интенсивность входного потока, т. е. среднее число запросов, возникающих у всех абонентов в одном кадре. При этом $\lambda = My$.

В режиме unicast polling в каждом кадре может передавать свой запрос только один абонент. Будем полагать, что в кадре t может передавать абонент, номер которого равен $(t+1) \bmod M$. Таким образом, каждый абонент может передавать свой запрос только один раз за M кадров.

В режиме broadcast polling в каждом кадре может передавать запрос любой абонент. Кадры, в которых абонент будет передавать запрос, выбираются с помощью определенного алгоритма, правила работы которого приведены ниже. Числа $W_{\min}$ и $W_{\max}$ являются параметрами алгоритма. При работе алгоритма также используется целочисленная переменная W.

Правило 1. Если в начале некоторого кадра t в соответствии с допущением 7 запрос помещается в нулевую ячейку буфера, то переменной W присваивается значение $W_{\min}$.

Правило 2. Если у абонента возник запрос в кадре $t-1$ и буфер для хранения запросов пуст, то абонент помещает этот запрос в нулевую ячейку буфера в начале кадра t и передает этот запрос в кадре t.

Во всех других случаях, если запрос был помещен в нулевую ячейку буфера в начале кадра t, абонент действует следующим образом:

• случайным образом выбирает число I из множества $\{0, 1, ..., W-1\}$;

• первый раз передает запрос в кадре $t+I$.

Правило 3. Если в некотором кадре $t-1$ возникает конфликт, то значение W удваивается и абонент, который передавал этот запрос, действует следующим образом:

• случайным образом выбирает число I из множества $\{0, 1, ..., W-1\}$;

• передает запрос в кадре $t+I$.

Если снова возникает конфликт, вышеописанные действия повторяются. Значение W удваивается до тех пор, пока не станет равным $W_{\max}$.

Передача запросов с использованием идентификаторов абонентов

На примере стандарта IEEE 802.16 покажем, как можно организовать передачу запросов с использованием идентификаторов без существенных видоизменений стандарта. Применительно к описанной модели сначала сформулируем основную идею, а затем дадим строгое описание предложенного подхода в форме алгоритмов, которыми должны руководствоваться абоненты и БС при передаче запросов.

Основная идея состоит в том, что используется передача запросов в режиме multicast polling. В стандарте IEEE 802.16 разбиение на подмножества не регламентируется. Предлагаемый подход заключается в динамическом разбиении в каждом кадре множества абонентов на подмножества. Динамическое разбиение имеет следующие особенности.

1. Если в некотором кадре t в окне для запроса БС наблюдает событие «конфликт», то она считает этот кадр первым кадром так называемого *сеанса разрешения конфликта*. Абонентов, которые передавали запрос в кадре t, будем называть *участниками конфликта*. Общее число участников конфликта образует *кратность конфликта* или *кратность сеанса*. В ходе сеанса разрешения конфликта БС будет указывать участникам конфликта кадры, в которых следует повторно передавать запрос.

Остальным абонентам запрещено передавать запросы до конца сеанса. Сеанс разрешения конфликта заканчивается после того, когда БС определит, что все участники конфликта успешно передали запрос.

2. Базовая станция сообщает, что в первом кадре сеанса окно для передачи запроса разрешено использовать всем абонентам. Если в этом окне БС наблюдает событие «успех» или «пусто», то сеанс завершается и в следующем кадре начинается новый сеанс.

Алгоритмы передачи запросов с использованием идентификаторов абонентов

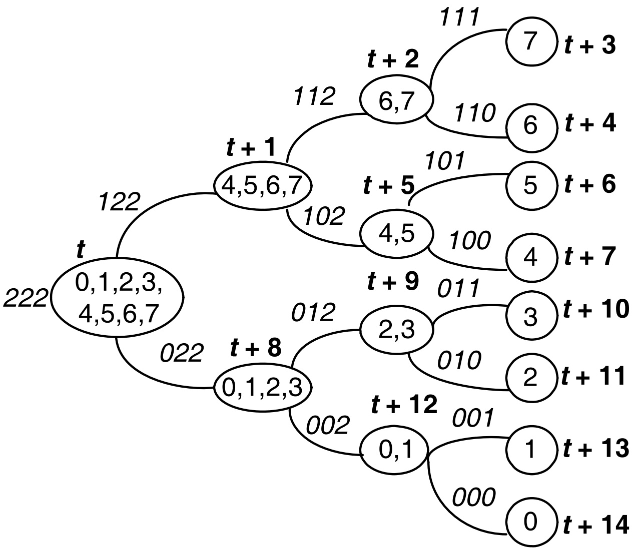
Для определения кадров, в которых абоненты могут передавать запросы в восходящий канал, БС передает некоторую служебную информацию, называемую *маской*. Маска представляет собой слово размерности $\log_2 M$, записанное в троичной системе счисления, которое формируется БС по ситуации в восходящем канале связи и передается в нисходящий канал связи для организации доступа абонентов к восходящему каналу. Маска может состоять из символов 0, 1, 2.

Маску, состоящую только из символов «2», будем называть *старт/стоповой маской*. Интервал времени между двумя соседними старт/стоповыми масками образует сеанс. Сеанс можно представить в виде дерева разрешения конфликта (ДРК), которое в дальнейшем будем именовать *деревом сеанса*. Вершины дерева сеанса соответствуют кадрам сеанса. Корень дерева образует первый кадр сеанса, соответствующий первоначальному конфликту, а концевые вершины дерева соответствуют кадрам с ситуациями «пусто» или «успех».

Дерево сеанса между M абонентами называется *деревом сеанса максимальной кратности*.

Каждой вершине дерева сеанса максимальной кратности можно однозначно поставить в соответствие маску. Маска определяет возможность передачи абонентом запроса в восходящий канал в случае полного поразрядного совпадения маски и идентификатора абонента. Наличие символа «2» в одном из разрядов маски означает, что идентификатор в этом разряде может принимать безразличное значение («0» или «1»), и сравнение по этому разряду можно не проводить. Например, если $M = 8$, то значение маски, равное 022, означает, что в данном кадре разрешена передача абонентам с двоичными адресами 000, 001, 010 и 011. На рис. 1 представлено дерево сеанса максимальной кратности для $M = 8$.

В каждой вершине дерева указаны: номер кадра и маска, соответствующие вершине, а также идентификаторы абонентов в десятичной системе



■ ***Рис. 1.*** *Дерево сеанса максимальной кратности для $M = 8$*

счисления, которым разрешена передача в данном кадре.

Количество разрядов маски, совпадающих с символом «2», определяет номер уровня (яруса) дерева сеанса, к которому относится вершина с данной маской. Обозначим это количество $N2$.

Рассмотрим метод управления доступом, который использует маску БС для передачи запросов в восходящий канал. Данный метод можно рассматривать как комбинацию алгоритмов работы БС и работы абонента.

Алгоритм работы базовой станции заключается в формировании маски, согласно ситуации в восходящем канале, в соответствии с деревом сеанса. Можно показать, что любое дерево сеанса является поддеревом дерева сеанса максимальной кратности.

Введем следующие обозначения:

$m(t)$ — маска, сформированная БС в начале кадра t и передаваемая в канал в кадре t:

$$m(t) = (m_{l-1}, m_{l-2}, \ldots, m_1, m_0) = \sum_{i=0}^{l-1} m_i 3^i,\ \ m_i = \{0, 1, 2\}.$$

$i(t)$ — номер яруса в дереве сеанса максимальной кратности, используемый при формировании $m(t)$:

$$i(t) = \{l, l-1, \ldots, 1, 0\};$$

номер яруса определяется как $\log_2 G$, где G — число абонентов, передающих в кадре дерева сеанса максимальной кратности; концевые вершины дерева принадлежат нулевому ярусу, вершины с двумя абонентами — первому и т. д.

$\eta(t) = \{П, У, К\}$ — ситуация в восходящем канале связи в кадре t.

$N2(m(t))$ — число символов «2» в маске $m(t)$.

В момент времени $t = 0$ устанавливаются следующие начальные условия функционирования системы: $m(t) = (222 \ldots 22) = 3^l - 1$, $i(t) = l$.

Ниже приведены инструкции алгоритма (все вычисления выполняются в троичной системе счисления).

1. Если $\eta(t)$ = К, то $m(t+1) = m(t) - 3^{i(t)-1}$ и $i(t+1) = i(t) - 1$.

2. Если $\eta(t)$ = П или $\eta(t)$ = У, то $m(t+1) = m(t) - 3^{i(t)}$; если $m(t+1) < 0$, то $m(t+1) = 3^l - 1$. $i(t+1) = N2(m(t+1))$.

В дальнейшем на рассмотренный алгоритм работы БС будем ссылаться как на *основной* алгоритм.

Алгоритм работы абонента заключается в сравнении маски БС $m(t)$ с собственным идентификатором. В случае совпадения абонент передает запрос в восходящий канал связи.

Альтернативный алгоритм работы базовой станции (с чередованием бит маски)

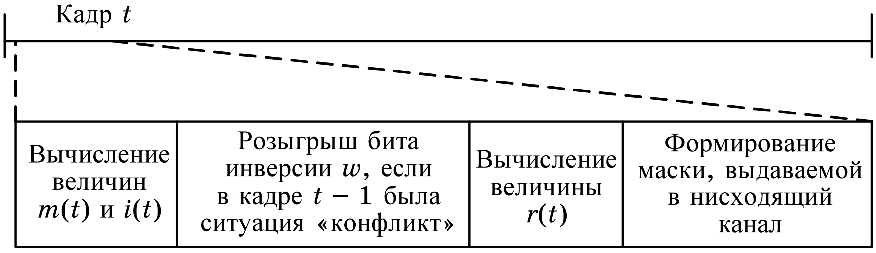
Алгоритм с чередованием бит маски является модификацией основного алгоритма. Его главное отличие заключается в том, что при ситуации «конфликт» очередной разряд маски формируется БС случайным образом.

В алгоритме с чередованием бит в добавление к переменным, используемым в основном алгоритме, вводится дополнительная переменная $r(t)$, которая формируется БС в кадре с номером t и называется *вектором инверсии*: $r(t) = (r_{l-1}, \ldots, r_1, r_0)$, где $r_i = \{0,1\}$. Вектор инверсии содержит единичные биты на тех позициях, на которых надо поменять разряды маски $m(t)$ на противоположные перед выдачей ее в канал. Операция инвертирования может быть легко реализована как сложение по модулю 2 битов маски l-го разряда с l-м битом вектора инверсии. При этом разряд маски, содержащий символ «2», не инвертируется, так как значение соответствующего бита вектора инверсии при этом равно нулю. Следует отметить, что если каждой вершине дерева сеанса соответствует своя маска, то вектор инверсии является одинаковым для двух вершин дерева, исходящих из общей вершины и принадлежащих одному ярусу. Корневой вершине дерева всегда соответствует вектор инверсии, состоящий из всех нулей.

Базовая станция в начале кадра t выполняет следующие действия (рис. 2):

- вычисляет маску $m(t)$ и номер яруса $i(t)$ аналогично основному алгоритму;
- в ситуации «конфликт», в кадре $t-1$, производит случайный розыгрыш бита инверсии w для вектора инверсии;
- вычисляет вектор инверсии $r(t)$;
- используя маску и вектор инверсии, формирует маску для передачи в нисходящий канал.

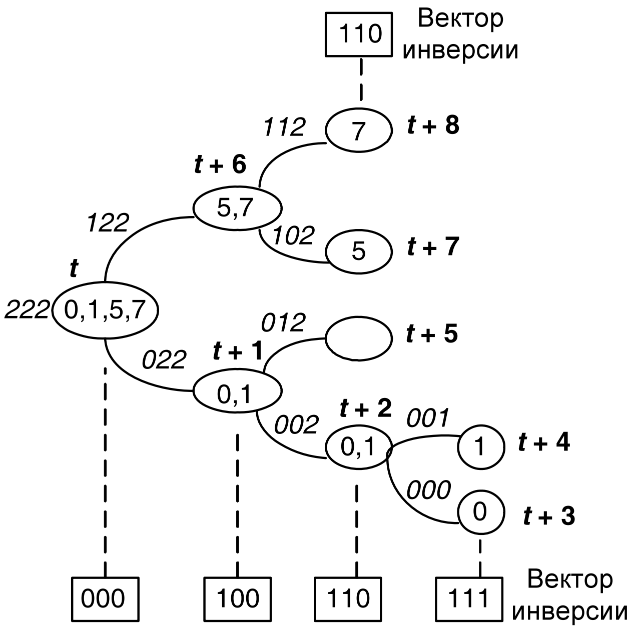
Основной алгоритм формирования маски БС можно считать частным случаем алгоритма с чере-



■ ***Рис. 2.*** *Действия, выполняемые БС в начале кадра*

■ ***Таблица 1.*** *Значения маски и вектора инверсии в алгоритме с чередованием бит*

Номер кадра	Маска, формируемая базовой станцией	Вектор инверсии	Маска, выдаваемая в канал
t	222	000	222
$t+1$	122	100	022
$t+2$	112	110	002
$t+3$	111	111	000
$t+4$	110	111	001
$t+5$	102	110	012
$t+6$	022	100	122
$t+7$	012	110	102
$t+8$	002	110	112



■ ***Рис. 3.*** *Дерево сеанса для разрешения конфликта*

■ ***Таблица 2.*** *Сравнение основного алгоритма и алгоритма с чередованием бит*

Номер абонента	Кадр, в котором абонент успешно передает запрос	
	Основной алгоритм	Алгоритм с чередованием бит
0	$t+8$	$t+3$
1	$t+7$	$t+4$
5	$t+3$	$t+7$
7	$t+2$	$t+8$

дованием бит, когда вектор инверсии постоянно равен нулю.

Правило вычисления величины $r(t)$.

1. В момент времени $t = 0$ устанавливается $r(t) = (000 \dots 00) = 0$.

2. Если $\eta(t) =$ К, то с вероятностью $^1/_2$ $w = 0$ и с вероятностью $^1/_2$ $w = 1$

$$r(t+1) = r(t) + w\,2^{i(t)-1}.$$

3. Если $\eta(t) =$ П или $\eta(t) =$ У и $i(t+1) = i(t)$, то $r(t+1) = r(t)$.

4. Если $\eta(t) =$ П или $\eta(t) =$ У и $i(t+1) \neq i(t)$, то $r(t+1) = r(t) - r_{i(t)}2^{i(t)}$.

Пример. В системе, состоящей из восьми абонентов, в кадре t возникает конфликт между абонентами с двоичными идентификаторами 000, 001, 101, 111. Рассмотрим использование алгоритма с чередованием бит для разрешения данного конфликта. В табл. 1 для каждого кадра сеанса приведены значения маски и вектора инверсии, формируемые БС, а также маска, выдаваемая в нисходящий канал. Будем считать, что при ситуациях «конфликт» в случае розыгрыша всегда выпадает $w = 1$.

На рис. 3 показано дерево сеанса для разрешения конфликта, а также нумерация вершин дерева, соответствующих отдельным кадрам сеанса; десятичные идентификаторы абонентов, передающие запросы в этих кадрах; маски и векторы инверсии, формируемые БС. Использование алгоритма с чередованием бит позволяет уменьшить задержки абонентов с номерами 0 и 1 по сравнению с основным вариантом. При этом задержки у абонентов с номерами 5 и 7, наоборот, увеличиваются. Результаты сравнения основного алгоритма и алгоритма с чередованием бит приведены в табл. 2.

Средняя задержка передачи запроса

Задержкой передачи запроса называется время от момента его поступления в систему до момента его успешной передачи. Занумеруем числовой последовательностью все поступающие в систему запросы и выделим из этой последовательности запрос с номером t. Этот запрос мы назовем *меченым* и найдем для него среднюю задержку.

Обозначим через δ_i случайную задержку передачи меченого запроса. Определим *среднюю задержку передачи запроса* равенством

$$D = \lim_{i\to\infty} E[\delta_i]. \quad (*)$$

Для того чтобы вычислить среднюю задержку передачи запроса, сопоставим предложенную систему допущений с системой допущений, введенной для базовой модели в работе [2] и уточненной в работе [3]. Из сопоставления этих систем допущений следует справедливость следующего утверждения.

Утверждение 1. Пусть число абонентов для рассматриваемой модели совпадает с числом абонентов для модели из работы [3] и средняя интенсивность поступления запросов от всех абонентов в расчете на один кадр для рассматриваемой модели совпадает со средней интенсивностью поступления пакетов от всех абонентов в расчете на одно окно для модели из работы [3]. Тогда средняя задержка передачи запроса, измеренная в числе кадров, основного алгоритма для рассматриваемой модели совпадает со средней задержкой передачи пакета, измеренной в числе окон, для блокированного немодифицированного стек-алгоритма из работы [3].

Непосредственно из утверждения 1 следует, что для расчета средней задержки передачи запроса основного алгоритма может быть без каких-либо изменений использована методика, приведенная в работе [3].

В основном алгоритме существующий порядок формирования масок БС приводит к неравномерным задержкам передачи запросов для разных абонентов. Так, абоненты, которые имеют большее число единиц в старших битах адреса, передают запросы с меньшей задержкой, чем абоненты, у которых в этих битах адреса содержатся нулевые значения. По аналогии со средней задержкой запроса в системе, введенной ранее в соответствии с формулой (*), введем *среднюю задержку запроса для абонента* с заданным номером. Занумеруем числовой последовательностью все поступающие запросы к абоненту с номером i и выделим из этой последовательности запрос с номером j. Этот запрос мы назовем *меченым*. Обозначим через δ_j^i случайную задержку передачи меченого запроса. Определим среднюю *задержку передачи запроса для абонента* с номером i равенством

$$D^i = \lim_{j\to\infty} E[\delta_j^i].$$

Анализируя работу основного алгоритма передачи запроса, можно доказать справедливость следующего утверждения.

Утверждение 2. Средняя задержка передачи запроса абонента уменьшается с увеличением номера абонента:

$$D^0 > D^1 > \ldots > D^{M-2} > D^{M-1},$$

а задержка передачи запроса в системе связана со средними задержками передачи запроса для абонентов следующим образом:

$$D = \sum_{i=0}^{M-1} D^i / M.$$

Для выравнивания задержек необходимо поменять порядок выдачи масок БС в нисходящий канал, что реализовано в алгоритме с чередованием бит маски. Как для основного алгоритма, так и для алгоритма с чередованием бит маски введем в рассмотрение среднюю задержку передачи запроса в системе и среднюю задержку передачи запроса для абонента с номером i. Для этих средних задержек будем использовать обозначения D_A и D_A^i соответственно.

Утверждение 3. Для алгоритма с чередованием бит средняя задержка передачи запроса для абонента не зависит от номера абонента и совпадает со средней задержкой передачи запроса в системе:

$$D_A^0 = D_A^1 = \ldots = D_A^{M-1} = D_A,$$

а средняя задержка передачи запроса в системе для алгоритма с чередованием бит равна средней задержке передачи запроса в системе для основного алгоритма:

$$D = D_A.$$

Справедливость утверждения 3 вытекает из способа формирования маски. Данный способ эквивалентен тому, что в системе с основным алгоритмом перед началом каждого сеанса выполняется случайная перестановка идентификаторов абонентов. Непосредственно из утверждения 3 следует, что для расчета средней задержки передачи запроса в системе с алгоритмом с чередованием бит может быть без каких-либо изменений использована методика численного расчета, приведенная в работе [3].

Утверждение 4. При бернуллиевском входном потоке средняя задержка модели с буфером на две ячейки, полученная численным расчетом [3], является нижней оценкой средней задержки алгоритма с чередованием бит маски при числе ячеек в буфере $b > 1$.

Справедливость утверждения следует из сравнения модели с буфером на две ячейки [3] и модели с буфером, состоящим из $b + 1$ ячеек (допущение 6).

Анализ эффективности алгоритма с чередованием бит маски

Сравним среднюю задержку доставки запроса предложенного подхода в режиме broadcast polling, используемом для передачи запросов HTTP-трафика. При сравнении, для того чтобы учесть специфику HTTP-трафика, кроме бернуллиевского входного потока, рассмотрим случай, когда входной поток характеризуется всплесками. В работе [4] такой поток называют прерывистым пуассоновским процессом (Interrupted Poisson Process). Используя аргументацию и обозначения рекомендаций рабочего комитета по стандарту 802.16 [4, 5], видоизменим допущение 8 из описания модели следующим образом.

Каждому кадру может соответствовать одно из двух состояний — *активное состояние* (ON) и *пассивное состояние* (OFF). В активном состоянии у каждого абонента с вероятностью y_{on} возникает новый запрос, в пассивном состоянии запросы не возникают. Если некоторому кадру t соответствует активное состояние, то с вероятностью C_1 кадру $t+1$ будет соответствовать пассивное состояние, а с вероятностью $1 - C_1$ кадру $t+1$ будет соответствовать активное состояние. Аналогично, если некоторому кадру t соответствует пассивное состояние, то с вероятностью C_2 кадру $t+1$ будет соответствовать активное состояние, а с вероятностью $1 - C_2$ кадру $t+1$ будет соответствовать пассивное состояние. Таким образом, процесс смены состояний описывается марковской цепью. Стационарная вероятность нахождения цепи в *активном состоянии* равна $C_2/(C_1 + C_2)$. Таким образом, интенсивность входного потока, т. е. среднее число запросов, возникающих у всех абонентов в одном кадре, вычисляется по следующей формуле:

$$\lambda = My_{on}C_2/(C_1 + C_2) = \lambda_{on}C_2/(C_1 + C_2),$$

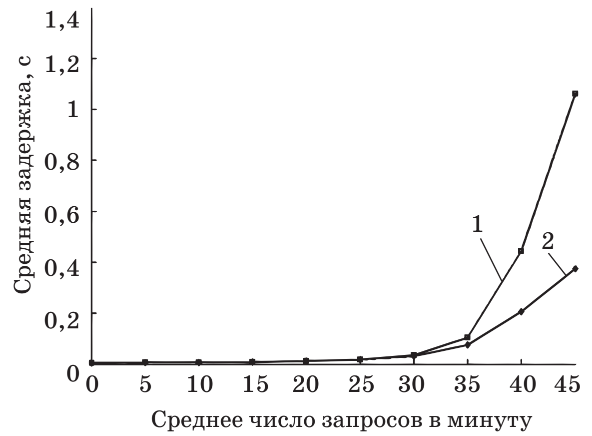
где λ_{on} — интенсивность входного потока в активном состоянии.

Далее описанный выше поток будем называть входным *потоком со всплесками*. При этом будем использовать рекомендованные [4] значения $C_1 = 0{,}01445$; $C_2 = 0{,}01085$.

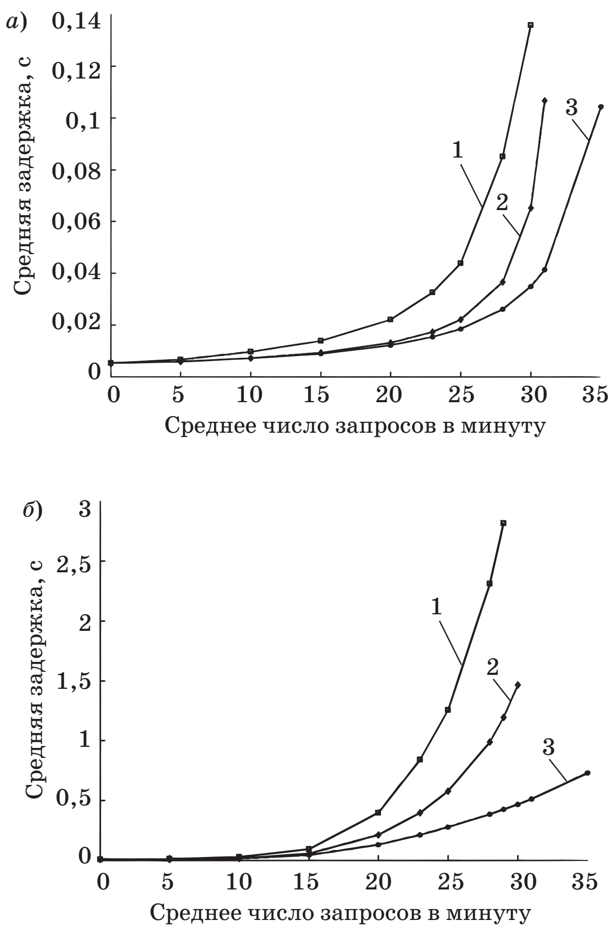
Средние задержки алгоритма с чередованием бит маски, алгоритма со случайными паспортами [2] и алгоритма, используемого в стандарте IEEE 802.16, при бернуллиевском потоке и потоке со всплесками для буфера с бесконечной очередью были получены путем имитационного моделирования. В качестве длительности кадра было выбрано значение 5 мс.

Графическая зависимость средней задержки от интенсивности входного потока при бернуллиевском входном потоке для буфера с бесконечным числом ячеек и буфера с двумя ячейками представлена на рис. 4. Из графика видно, что при среднем числе запросов в минуту, меньшем 35, оценка средней задержки из утверждения 4 является достаточно точной.

Проведем сравнение средних задержек для алгоритмов на основе идентификаторов абонентов, алгоритма со случайными паспортами и алгоритма, используемого в стандарте IEEE 802.16, для бернуллиевского входного потока (рис. 5, *а*) и для потока со всплесками (рис. 5, *б*). Видно, что предложенный алгоритм с идентификаторами абонентов, начиная с некоторого числа запросов, дает выигрыш по средней задержке доставки запроса. Например, для потока со всплесками при среднем числе запросов, близком к 30 в минуту, средняя



■ ***Рис. 4.*** *Зависимость средней задержки от интенсивности для алгоритма с использованием идентификаторов абонентов при бернуллиевском потоке: 1 — буфер с бесконечным числом ячеек; 2 — буфер с двумя ячейками*



■ ***Рис. 5.*** *Зависимость средней задержки от интенсивности: а — при бернуллиевском потоке; б — при потоке со всплесками: 1 — стандартный алгоритм IEEE 802.16; 2 — алгоритм со случайными паспортами; 3 — алгоритм с использованием идентификаторов* задержка алгоритма с использованием идентификаторов примерно на 3 с меньше средней задержки алгоритма, используемого в стандарте IEEE 802.16 (см. рис. 5, *б*).

Заключение

В данной работе представлен подход, использующий идентификаторы абонентов для резервирования канала множественного доступа. Подход базируется на предложенных в работе алгоритмах, использующих маску БС. Базовая станция посылает маску всем абонентам, которые, сравнивая ее со своим идентификатором, определяют момент передачи запроса. Предлагаемый вариант алгоритма с так называемым чередованием бит маски позволяет исключить зависимость задержки от идентификатора абонента.

Рассматриваемый подход может быть реализован в стандарте IEEE 802.16 в рамках режима multicast polling. Эффективность подхода продемонстрирована на примере потока со всплесками, имитирующего трафик протокола HTTP. Показано, что алгоритм с чередованием бит маски позволяет значительно уменьшить среднюю задержку передачи запроса по сравнению с алгоритмом, используемым в стандарте IEEE 802.16, как при бернуллиевском потоке, так и при потоке со всплесками. Причем, при потоке со всплесками выигрыш по средней задержке является более существенным.

Отметим, что, несмотря на отсутствие конкретных требований по задержке для HTTP-трафика, задержка передачи порядка нескольких секунд рассматривается пользователями как отказ в обслуживании. В работе показано, что предлагаемый подход позволяет снизить задержку до приемлемого уровня.

Представленные выше результаты получены в предположении, что как восходящий канал, так и нисходящий канал являются бесшумными каналами. На основе работы [6] данные результаты могут быть обобщены на случай, когда шум в восходящем канале может привести к ложным конфликтам. При этом незначительно усложняется алгоритм формирования маски, а алгоритм работы абонента не изменяется.

Литература

1. IEEE 802.16e-2005, IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands.
2. **Цыбаков Б. С., Михайлов В. А.** Свободный синхронный доступ пакетов в широковещательный канал с обратной связью // Проблемы передачи информации. 1978. Т. 14. № 4. С. 32–59.
3. **Тюрликов А. М., Марковский С. Г.** Использование адресов абонентов для организации доступа к высокоскоростному каналу связи // Информационно-управляющие системы. 2003. № 1. С. 32–38.
4. Traffic Model for 802.16 TG3 MAC/PHY Simulations. http://www.ieee802.org/16/tg3/contrib/802163c-01_30r1.pdf
5. **Schwartz R.** Proposal on traffic models. IEEE 802.16 Contribution 802.16.3p-01/27. http://www.wirelessman.org/tg3/contrib/802163p-01_27.pdf.
6. **Тюрликов А. М., Марковский С. Г.** Использование адресов абонентов для разрешения конфликтов в канале с шумом // Информационно-управляющие системы. 2006. № 2. С. 27–37.

УДК 551.46.08

МОДЕЛИРОВАНИЕ ЗАМКНУТОЙ СИСТЕМЫ УПРАВЛЕНИЯ «ПРИРОДА-ТЕХНОГЕНИКА»

Р. И. Сольницев,
доктор техн. наук, профессор
Г. И. Коршунов,
доктор техн. наук, профессор
А. А. Шабалов,
ассистент
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Рассмотрены вопросы создания замкнутой системы управления «Природа-техногеника», предназначенной для эффективного снижения загрязняющих веществ, выбрасываемых промышленными предприятиями в атмосферу. Представлена математическая модель замкнутой системы управления и модели составляющих ее звеньев. Приведены результаты анализа системы на основе моделирования.

Концепция «Природа-техногеника», предложенная и развитая в работах [1–6], предусматривает создание замкнутой системы управления «Природа-техногеника» (ЗСУПТ) для широкого класса объектов, где требуется минимизация концентрации загрязняющих веществ (ЗВ) техногенного характера.

Отличительные особенности концепции представлены тремя критериями:

— минимизация или полное исключение «человеческого фактора»;

— управление концентрациями ЗВ на основе определения их максимальных значений;

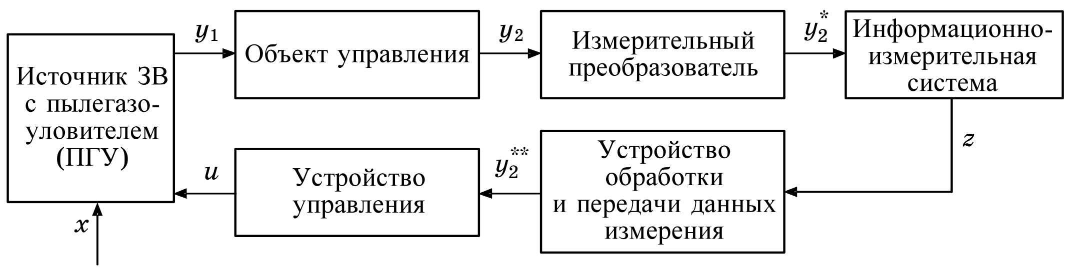
— сохранение технологии основного производства в условиях минимизации концентраций ЗВ.

В работе рассмотрена задача моделирования ЗСУПТ «Природа-техногеника», решение которой необходимо для создания таких систем в различных областях человеческой деятельности.

Объектом управления ЗСУПТ является масса (концентрация) ЗВ в газовоздушной смеси, перемещающаяся от устья «трубы» промышленного предприятия до точки, где расположен измерительный преобразователь. В работе рассматривается ЗСУПТ на примере только одной составляющей ЗВ — диоксида серы SO_2.

Ущерб, наносимый окружающей среде диоксидом серы, его характеристики и составляющие хорошо известны. Дополнительно можно отметить, что при производительности котла ТЭЦ 100 т пара/ч выброс SO_2 составит 2–3 т/сут, и выпадение серы будет иметь место в круге с радиусом до 100 км от i-го источника, что крайне отрицательно сказывается на здоровье людей, растениях, зданиях и других составляющих окружающей среды этой ТЭЦ.

Задачей математического моделирования является воспроизведение на ЭВМ динамики и процессов функционирования ЗСУПТ (рис. 1) и дальнейший



■ *Рис. 1. Схема замкнутой системы управления «Природа-техногеника»* анализ на основе моделирования. Для решения этой задачи необходимо составить математические модели всей системы и ее отдельных звеньев.

Для качественной оценки динамики ЗСУПТ рассмотрим уравнение материального баланса, выражающее неразрывность изменения массы или концентрации ЗВ:

$$\frac{\mathrm{d}y}{\mathrm{d}t} = K_1 x - K_2 y - K_3 y, \quad (1)$$

где x — среднее значение количества сжигаемого в ТЭЦ топлива при производстве основного продукта — пара; y — среднее значение количества массы ЗВ, выбрасываемого ТЭЦ в атмосферу; K_1 — коэффициент пропорциональности, определяющий содержание в топливе ЗВ (в частности, содержание серы в сланцах составляет $3{,}5\ \%$, мазуте — $2{,}5\ \%$, угле — от $0{,}5$ до $4\ \%$); K_2 — коэффициент, зависящий от синоптических, температурных, химических и других внешних параметров и определяющий поглощение SO_2 внешней средой; K_3 — коэффициент, выражающий величину позиционной обратной связи системы управления в ЗСУПТ. Уравнение (1) имеет аналитическое решение

$$y = \left(y_0 - \frac{K_1}{K_2 + K_3} x \right) e^{-(K_2+K_3)t} + \frac{K_1}{K_2 + K_3} x, \quad (2)$$

где y_0 — масса ЗВ в момент времени $t_0 = 0$.

Из этого следует очевидный результат: выбором регулируемого коэффициента K_3 можно принципиально снизить массу (концентрацию) ЗВ до предельно допустимой величины [5].

В случае заданных как функции времени $x(t)$ и $K_2(t)$ уравнение (1) примет вид

$$\frac{\mathrm{d}y}{\mathrm{d}t} + [K_2(t) + K_3] y = K_1 x(t). \quad (3)$$

Решение этого уравнения также находится аналитически двумя квадратурами:

$$y = y_0 e^{-\int_0^T [K_2(t)+K_3]\mathrm{d}t} + e^{-\int_0^T [K_2(t)+K_3]\mathrm{d}t} \int_0^T K_1 x(t) e^{\int_0^T [K_2(t)+K_3]\mathrm{d}t} \mathrm{d}t, \quad (4)$$

где T — время наблюдения.

Выражение (4) позволяет контролировать результаты моделирования и получать качественные оценки ЗСУПТ. Дальнейшее уточнение предложенной модели достигается содержательным представлением коэффициентов K_1 и K_2, которые определяются через связи выброса с расходом топлива (K_1) и с синоптическими, диффузионными, химическими и конвекционными процессами (K_2). Приближенное значение K_2 можно определить двумя аддитивными составляющими:

$$K_2 = K_{2\text{ф}} + K_{2\Sigma};$$

$$K_{2\text{ф}} = 0{,}6\ldots0{,}9;$$

$$K_{2\Sigma} = \frac{t_\text{в}}{\pi \sigma_y \sigma_z v} e^{-\frac{H^2}{2\sigma_z^2}},$$

где $K_{2\text{ф}}$ — составляющая от фильтрации ПГУ; $t_\text{в}$ — время выброса; H — высота выброса (высота трубы и высота факела выброса); v — скорость ветра; σ_y, σ_z — среднеквадратические отклонения факела от его оси.

Переменные $x(t)$ и $K_2(t)$ обычно известны по результатам мониторинга.

Для оценки характеристик ЗСУПТ по устойчивости, качеству, динамике процессов регулирования предлагается математическая модель ЗСУПТ на основе моделей отдельных звеньев, представляющих собой передаточные функции звеньев ЗСУПТ, показанной на рис. 1.

Структурная схема ЗСУПТ согласно рис. 1 изображена на рис. 2.

Приведем математические модели звеньев ЗСУПТ в виде передаточных функций отдельных звеньев.

Передаточная функция переноса ЗВ с выхода топливных газов до устья трубы (W_1) представлена выражением

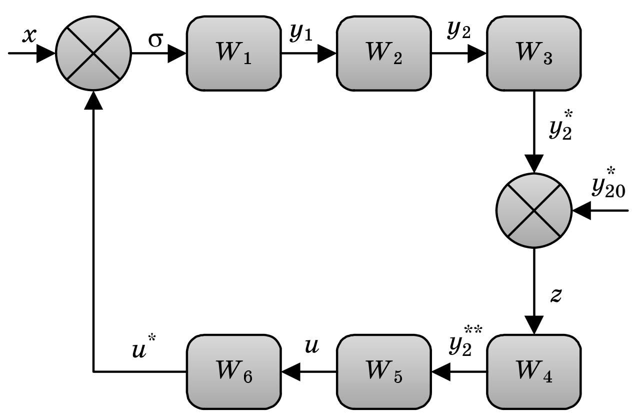
$$y_1(t) = W_1(p)\sigma(t), \ W_1 = \frac{K_1}{1 + T_1 p}, \quad (5)$$

где $p \equiv \frac{\mathrm{d}}{\mathrm{d}t}$ при нулевых начальных условиях;

$$\sigma(t) = x(t) - u^*(t), \quad (6)$$

где x — возмущающее воздействие; u^* — управляющее воздействие.

Передаточная функция преобразования массы ЗВ в составе факела при переносе от устья трубы до точки измерения (W_2) *в простейшем случае* может быть представлена выражением



■ **Рис. 2.** *Структурная схема ЗСУПТ*

$$y_2(t) = W_2(p) y_1(t),\ W_2 = \frac{K_4}{1+T_2 p} e^{-p\tau_1}, \tag{7}$$

где K_4 — коэффициент пропорциональности, зависящий от превращений параметров атмосферы, таких как давление, влажность, начальная концентрация ЗВ, температура окружающей среды, коэффициенты диффузии и поглощения ЗВ подстилающей поверхностью; T_2 — постоянная времени инерционных процессов переноса ЗВ; τ_1 — время чистого запаздывания при переносе количества вещества от устья трубы до точки измерения ЗВ датчиком. В общем случае величина τ_1 определяется в результате решения уравнения турбулентной диффузии при заданных краевых и начальных условиях. В простейшем случае при расчете τ_1 значениями горизонтальных коэффициентов диффузии можно пренебречь, а движение воздушных потоков считать однородными в рассматриваемой области пространства. В этом случае τ_1 рассчитывается по формуле

$$\tau_1 = S/v, \tag{8}$$

где S — расстояние от устья трубы до точки измерения максимума концентрации ЗВ датчиком; v — средняя скорость ветра на высоте факела (H).

Передаточная функция измерительного преобразования (W_3) представлена выражением

$$y_2^* = W_3(p) y_2,\ W_3 = \frac{K_5}{1+T_3 p} e^{-p\tau_2}, \tag{9}$$

где τ_2 — время измерительного преобразования, зависящее от принципа действия и конструкции используемого измерительного устройства. Для предполагаемых к использованию полупроводниковых сенсоров время реакции газочувствительной характеристики не превышает 5 с и время восстановления также не более 5 с. Измерительный преобразователь располагается в точке максимума концентрации ЗВ и выполняет полный цикл измерения за время, определяемое параметрами сенсора.

Передаточная функция процесса формирования, накопления, обработки, преобразования и передачи данных измерения (W_4) представлена выражением

$$y_2^{**}(t) = W_4(p) z(t),\ W_4 = \frac{K_6}{1+T_4 p} e^{-p\tau_3}, \tag{10}$$

где τ_3 — суммарное время, затрачиваемое на процессы формирования, накопления, обработки, преобразования и передачи данных измерения ЗВ; z — ошибка, вычисляемая по формуле

$$z = y_2^* - y_{20}^*, \tag{11}$$

где y_{20}^* — допустимая величина концентрации, в частности ЗВ, на расстоянии S от устья трубы при определенных погодных условиях и параметрах функционирования предприятия (ТЭЦ), которая всегда меньше ПДК.

Параметры передаточной функции W_4 определяются быстродействием аналого-цифрового преобразования и накопления в памяти информационно-вычислительного устройства, а также временным запаздыванием, зависящим от скорости передачи, времени обработки и накопления данных, которое может составлять единицы или десятки секунд. Выбор стандартных протоколов GSM и GPS обеспечивает стабильность передачи данных, однако возможно использование специальных протоколов.

Управляющее воздействие на агрегат очистки от загрязняющих веществ (W_5) представлено выражением

$$u = (K_7 + K_8 p + K_9/p) y_2^{**}. \tag{12}$$

Значения коэффициентов передачи по пропорциональной составляющей, по первой производной и изодромной составляющей выбираются из условий устойчивости и качества регулирования концентрации ЗВ. Синтез управлений в ЗСУПТ приведен в работах [3, 5]. Здесь использован ПИД-регулятор. Применение других управлений — инвариантных, импульсных, экстремальных — предусмотрено при дальнейшей разработке ЗСУПТ.

Передаточная функция очистного агрегата (W_6), *включающего усилительно-преобразующее устройство,* представлена выражением

$$u^*(t) = W_6(p) u(t),\ W_6(p) = \frac{K_{10}}{1+T_5 p}, \tag{13}$$

где K_{10}, T_5 зависят от типа и конструкции управляющих ПГУ.

Время реакции для различных типов ПГУ (рукавных, электрофильтров, импульсных, каталитических) составляет от единиц до десятков секунд.

На основе математических моделей (5)—(13) строится полная математическая модель (передаточная функция) ЗСУПТ, оценивается ее устойчивость, динамические и статические ошибки при вариации K_i, T_j, τ_s, $i = 1 \div 10$, $j = 1 \div 3$, $s = 1 \div 3$.

Передаточная функция ЗСУПТ по ошибке регулирования z/y_{20} имеет вид

$$\frac{z}{y_{20}} = \frac{p(1+T_1 p)(1+T_2 p)(1+T_3 p)(1+T_4 p)(1+T_5 p)}{p(1+T_1 p)(1+T_2 p)(1+T_3 p)(1+T_4 p)(1+T_5 p)+a}, \tag{14}$$

где $a = K_1 K_4 K_5 K_6 K_{10} (K_9 + K_7 p + K_8 p^2) e^{-p(\tau_1+\tau_2+\tau_3)}$.

Передаточная функция по отношению к возмущению x:

$$\frac{z}{x} = \frac{K_1 K_4 K_5 e^{-p(\tau_1+\tau_2)} p(1+T_4 p)(1+T_5 p)}{p(1+T_1 p)(1+T_2 p)(1+T_3 p)(1+T_4 p)(1+T_5 p)+a}. \tag{15}$$

Наименование	X	K_1	T_1	τ_1	K_4	T_2	τ_2	K_5	T_3	τ_3	K_6	T_4	y^*_{20}	K_7	K_8	K_9	K_{10}	T_5
Размерность	т	–	с	с	–	с	с	–	с	с	–	с	т	–	–	–	–	с
Значение	1000	0,01	1,6	60	1	10	6	1	1	0	1	1	1	2	0	0,35	1	10

Из (14) и (15) следует, что ЗСУПТ является астатической по отношению к ошибке регулирования y^*_{20} и по отношению к возмущению x.

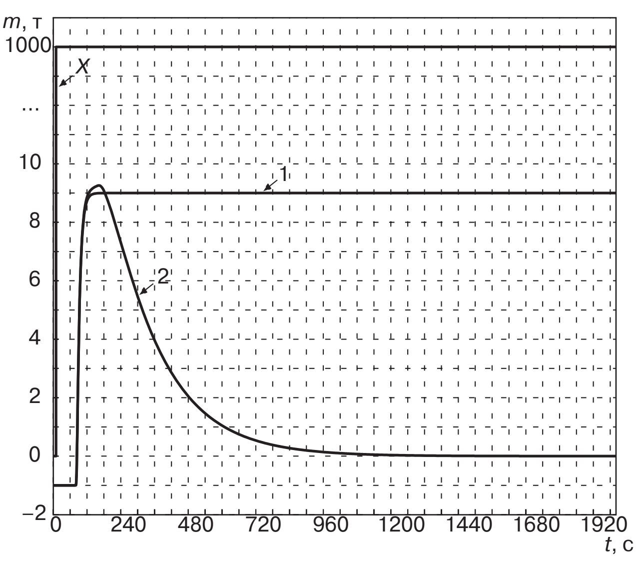
В таблице приведены номинальные значения параметров, полученные из различных источников [1–6]. На рис. 3 показано изменение ошибки z при ступенчатом входном воздействии функции X для разомкнутой (кривая *1*) и замкнутой (кривая *2*) систем.

На основе данных таблицы можно показать, что процессы измерения выполняются в режиме реального времени и параметры интегратора обеспечивают устойчивое регулирование при периодическом получении данных измерения по каналу связи. В дальнейшем осуществлялось моделирование поведения системы, заданной передаточной функцией, при изменении значений отдельных параметров. По результатам моделирования определены параметры управления, обеспечивающие устойчивость, требуемые величины затухания, динамической и статической ошибок.

Рисунки демонстрируют изменение процесса регулирования от изменения:

— величины чистого запаздывания при переносе количества вещества от устья трубы до точки измерения ЗВ датчиком (рис. 4, *а*);

— вида топлива (рис. 4, *б*);



■ ***Рис. 3.*** *Изменение ошибки z при ступенчатом изменении воздействия функции X, с замкнутой и разомкнутой обратной связью*

— параметров интегратора (рис. 4, *в*);

— выбранных комбинаций величины чистого запаздывания и параметров интегратора (рис. 4, *г*);

— коэффициента усиления регулятора (рис. 4, *д*).

Анализ зависимостей позволяет ввести допуски на значения параметров. Результаты моделирования показывают возможность создания эффективной системы управления, способной обеспечивать достаточное качество управления концентрацией ЗВ в газовоздушной смеси.

В дальнейшем учет диффузионных и конвекционных процессов в ЗСУПТ осуществляется на основе уравнения классической турбулентной диффузии:

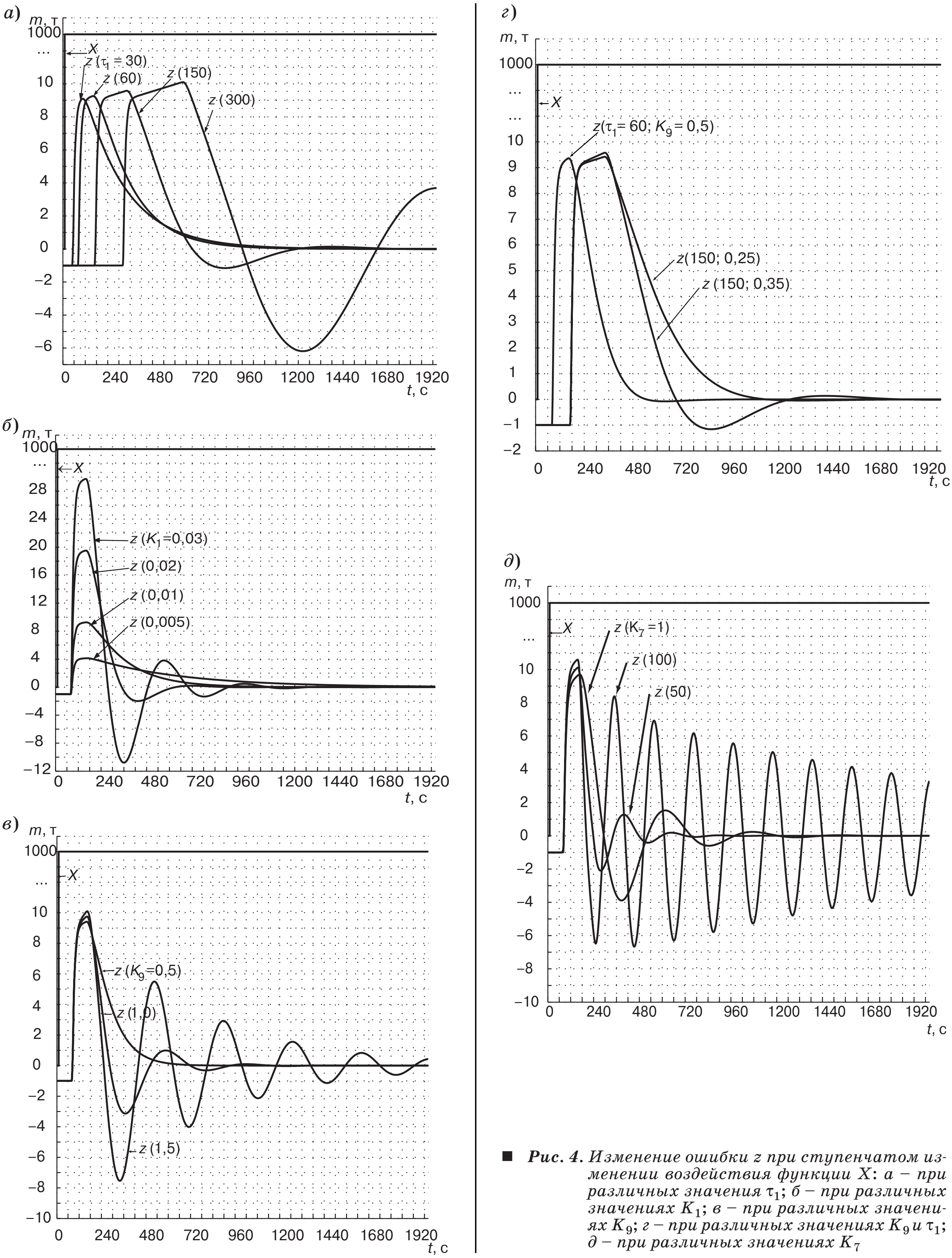
$$\frac{\partial y_\partial}{\partial t}+v_\zeta\frac{\partial y_\partial}{\partial \zeta}+v_\eta\frac{\partial y}{\partial \eta}+v_\xi\frac{\partial y_\partial}{\partial \xi}=$$
$$=\frac{\partial}{\partial \zeta}k_\zeta\frac{\partial y_\partial}{\partial \zeta}+\frac{\partial}{\partial \eta}k_\eta\frac{\partial y_\partial}{\partial \eta}+\frac{\partial}{\partial \xi}k_\xi\frac{\partial y_\partial}{\partial \xi}-ay, \qquad (16)$$

где y_∂ — концентрация ЗВ; k_ς, k_η, k_ξ — горизонтальные и вертикальная составляющие коэффициента турбулентного обмена; v_ς, v_η, v_ξ — горизонтальные и вертикальная составляющие скорости перемещения ЗВ; a — коэффициент, определяющий изменение концентрации за счет процессов химического превращения примеси, а также ее осаждения (пропорционален K_2). Дополняя это уравнение возмущающим воздействием x, получим

$$\frac{\partial y_\partial}{\partial t}+v_\zeta\frac{\partial y_\partial}{\partial \zeta}+v_\eta\frac{\partial y}{\partial \eta}+v_\xi\frac{\partial y_\partial}{\partial \xi}=$$
$$=\frac{\partial}{\partial \zeta}k_\zeta\frac{\partial y_\partial}{\partial \zeta}+\frac{\partial}{\partial \eta}k_\eta\frac{\partial y_\partial}{\partial \eta}+\frac{\partial}{\partial \xi}k_\xi\frac{\partial y_\partial}{\partial \xi}-K_1^*x-K_2^*y. \qquad (17)$$

Переход от модели (17) к модели вход-выход на основе функции Грина предложен в работе [3].

Предложенная в статье структура, математические модели и параметры ЗСУПТ и ее звеньев позволяют получить в результате моделирования качественные оценки устойчивости, регулирования, часть из которых приведена в работе. Также приведена оценка толерантности ЗСУПТ при изменении ее коэффициентов и параметров. Авторы использовали упрощенную модель преобразования массы ЗВ в составе факела в виде звена чистого запаздывания при принятых допущениях, один датчик, устанавливаемый в точке максимума концентрации ЗВ, и ПИД-регулятор. Это позволило по-



■ ***Рис. 4.** Изменение ошибки z при ступенчатом изменении воздействия функции X: а – при различных значения τ_1; б – при различных значениях K_1; в – при различных значениях K_9; г – при различных значениях K_9 и τ_1; д – при различных значениях K_7*

лучить качественные характеристики процесса регулирования и перейти к экспериментам, уточнению значений параметров, а при необходимости — функций звеньев. Для реализации конкретных проектов ЗСУПТ необходима дальнейшая детализация математических моделей и моделирование с целью выбора и обоснования технических решений, в том числе выбора значений допусков параметров, обеспечения расположения измерителя в точке максимума концентрации, уточнения типа и параметров канала связи. Полученные результаты подтверждают концепцию построения ЗСУПТ для минимизации ЗВ и дают основания для опытно-конструкторской разработки этой системы.

Литература

1. **Solnitsev R. I.** The instrumentation in ecology and human safety // IEHS'96. ISA — SPb. Russian sect. / SPb. SUAI, 1996. P. 16–18.
2. **Solnitsev R. I.** The simulation of "Nature-technogenic" system // IEHS'98. ISA — SPb. Russian sect. / SPb. SUAI, 1998. P. 8–10.
3. **Solnitsev R. I.** Creation of "Nature-technogenic" control systems on the base of information technologies // IEHS'02. ISA — SPb. Russian sect. / SPb. SUAI, 2002. P. 12–17.
4. **Solnitsev R. I.** Human factor minimization in the "Nature-technogenic" system // IEHS'04. ISA — SPb. Russian sect. / SPb. SUAI, 2004. P. 15–17.
5. **Сольницев Р. И.** Построение замкнутых систем «Природа-техногеника»: Тр. XXXIII МНТК IT+S&E'06, Украина, Крым, Ялта—Гурзуф, 20–30 мая 2006 г. // Открытое образование. С. 404–408.
6. **Solnitsev R. I., Korshunov G. I., Klotchkov I. B.** The "Nature-technogenic" closed system — innovational project // IEHS'07. ISA — SPb. Russian sect. / SPb. SUAI, 2007. P. 15–20.

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

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

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

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

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

УДК 004.435 + 004.4’423

СТРУКТУРА МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ МНОГОПРОФИЛЬНОГО СКРИНИНГА С УНИФИЦИРОВАННЫМ ФОРМАЛЬНЫМ ПРЕДСТАВЛЕНИЕМ МЕДИЦИНСКОГО ОБЕСПЕЧЕНИЯ

А. Б. Кубайчук,
начальник отдела
Федеральное государственное научное учреждение «Научно-исследовательский конструкторско-технологический институт биотехнических систем»

Рассматривается класс адаптивных информационных систем и методика их построения. Предлагается типовая архитектура, многоуровневая модель представления метаинформации и описывается процедура адаптации для подобных систем. В качестве примера системы, разработанной по указанной методике, приводится информационная система многопрофильного скрининга.

Среди широкого разнообразия современных информационных систем (ИС) в частности можно выделить класс адаптивных ИС, которые ориентированы на функционирование в различных областях применения при условии, что решаемая задача и структура используемых данных остаются неизменными.

Следует отметить, что, как правило, термин «адаптивный» применяется по отношению к объекту, обладающему способностью приспосабливаться к изменениям своего окружения. Если в качестве такого объекта рассматривать ИС, то справедливо полагать, что адаптивная ИС должна предоставлять пользователю возможность варьирования структуры данных и содержания вычислительного процесса их обработки при изменениях в соответствующей предметной области, другими словами, в такой ИС должна быть реализована возможность метауправления ее функциональностью [1]. Однако рассматриваемый класс ИС нельзя отнести к системам с метауправлением в «чистом» виде. При построении подобных ИС используется классический подход, который предполагает фиксацию структуры базы данных (БД) и алгоритмов обработки, составляющих функциональные приложения. Ключевые особенности таких систем проявляются в их архитектуре.

К адаптивной ИС можно отнести автоматизированный комплекс для диспансерного обследования (АКДО), который является разновидностью автоматизированных систем скринирующей диагностики (АССД), предназначенный для автоматизации деятельности специалистов, осуществляющих проведение диспансерных обследований [3]. Основой таких систем является медицинское обеспечение (МедО) [4], состав которого зависит от возрастной категории пациентов (дети, подростки, взрослые), а также области применения комплекса. Поэтому вместо разработки специализированных ИС для каждой возрастной группы при построении МедО АКДО целесообразно использовать метауправление следующего вида:

— состав опросников, профилей патологии и решающих правил для каждой группы описывается на языке представления метаинформации;

— разработанная универсальная ИС, состоящая из БД, системы управления базой данных (СУБД) и функциональных модулей, настраивается под конкретную возрастную группу путем использования специальных инструментальных средств, осуществляющих конвертацию описаний МедО в соответствующие таблицы статических сведений базы данных.

Таким образом, для адаптивной ИС можно выделить инвариантную часть, реализующую функциональные возможности АССД; средства адаптации (инструментальные средства), осуществляющие настройку инвариантной части для новой области применения; множество описаний областей применения на языке представления метаинформации. При этом БД инвариантной части должна содержать группу таблиц статических сведений об области применения. В качестве области применения можно рассматривать список профилей патологии. Следует отметить, что в состав инсталляционного пакета АКДО средства адаптации и описания областей применения не входят. Конечному пользователю поставляется только универсальная ИС и инвариантная часть, настроенная для конкретной области применения.

Для представления метаинформации необходима соответствующая модель. Разработанная и используемая в настоящее время во множестве приложений базовая модель представления метаинформации (БМПМ) по способу представления знаний наиболее близка к иерархическим семантическим сетям. Дескриптивные знания в БМПМ представляются в виде иерархически организованной сети понятий (дерева понятий). В качестве понятий выступают сущности (объекты), атрибуты, значения атрибутов и отношения. В качестве языка представления метаинформации целесообразно использовать расширяемый язык разметки XML (Extensible Markup Language), соответствующий БМПМ [1].

Адаптивная часть АКДО состоит из нескольких уровней представления метаинформации, используемой для описания области применения. Описания на всех уровнях относятся к одному классу XML-описаний, который состоит из следующих секций:

— паспорта описания, который содержит:
  наименование;
  глобальный уникальный идентификатор (ГУИ);

— содержательной части, представляющей описание структуры сведений.

Содержательная часть описывается при помощи информационных элементов (ИЭ) и информационных секций (ИнС), соответствующих сущностям.

Информационный элемент представляет собой кортеж вида

$$IE = (N, \{A\}, R_c, ED),$$

где N — наименование сущности; $\{A\}$ — множество свойств (атрибутов) сущности; R_c — правило, определяющее допустимое количество экземпляров сущности ($R_c \in$ {П1, П+, П*, Н}); ED — внешние данные, связанные с сущностью.

Информационная секция представляет собой кортеж вида

$$IS = (N, \{A\}, R_u, R_c, ED, \{Ch\}),$$

где R_u — правило, определяющее возможные сочетания экземпляров подчиненных сущностей ($R_u \in$ {И, ИЛИ, МИЛИ}); $\{Ch\}$ — множество дочерних (подчиненных) ИЭ и/или ИнС.

Информационные секции используются для описания составных (сложных) сущностей, такие сущности раскрываются (объясняются) посредством подчиненных ИнС и ИЭ: ИЭ соответствуют листьям, а ИнС — узлам и корню дерева сущностей.

Правило R_c определяет допустимое количество экземпляров сущности, соответствующей ИЭ или ИнС, а правило R_u определяет состав списка подчиненных ИЭ и/или ИнС, указывая возможные сочетания экземпляров соответствующих сущностей при описании сведений об области применения на уровне представления метаинформации. Обозначения правил R_c и R_u имеют и более развернутую запись: «П1» — «повтор один раз», «П+» — «повтор хотя бы один раз», «П*» — «повтор один раз, несколько раз или ни разу»; «Н» — «необязательно»,»И» — «все из», «ИЛИ» — «одно из», «МИЛИ» — «несколько из».

Если правило R_c не указано, то по умолчанию принимается правило «П1», если правило R_u не указано, то по умолчанию принимается правило «И».

Механизм связи между сущностями реализован отношениями «предок — потомок» и посредством специальной сущности типа «ссылка». В наименовании такой сущности указывают наименование объекта ссылки. Для реализации механизма ссылок каждая сущность, ссылка на которую допустима, должна иметь уникальный идентификатор. Таким сущностям добавляется свойство «локальный идентификатор» (ЛИН). Механизм реализации ссылок описывается на уровне представления структуры метаинформации и на уровне представления метаинформации.

Медицинское обеспечение АССД, и АКДО в частности, служит основой для последующей разработки информационного, алгоритмического, программного, методического и организационного обеспечения АССД как автоматизированной системы и определяет функциональные возможности создаваемой системы скрининга, ее состоятельность в решении задач диагностики и область ее эффективного применения [5]. Структура МедО АССД и соотношение его элементов с компонентами формальной модели АССД приведены в работе [2].

Исходя из места, роли и способа использования МедО в процессах создания и эксплуатации АССД [3], следует различать первичное и вторичное МедО АССД.

Первичное МедО представляет собой описание функциональных требований к АССД (обычно в форме документа «Постановка задачи на разработку МедО АССД»), включая:

— контингент пациентов, подлежащих обследованию;

— периодичность обследований;

— цель, достигаемую в результате обследования;

— ведущую функцию системы (и ее подсистем), т. е. функцию, обеспечивающую достижение сформулированной цели АССД;

— нозологическую ориентацию обследования, т. е. состав профилей патологии и диагнозов, выделяемых в процессе обследования.

Таким образом, первичное МедО содержит требования и служит основой для формирования вторичного МедО, а по мере разработки последнего непосредственно входит в его различные компоненты.

В структуре вторичного МедО (рис. 1) основными являются блоки описания объектов и описания решающих правил.

Структура описания объектов МедО представлена на рис. 2. Секция установочных признаков описывает характеристики объекта обследования (пациента), важные с точки зрения состава первичных медицинских данных (ПМД) и решающих правил. Секция опросников описывает структуру обследования, состав ПМД и их взаимодействие. В секции выходных данных описываются обобщенные медицинские показатели (ОМП), которые подлежат определению посредством решающих правил. Секция шкал типов данных является вспомогательной и определяет логический тип данных ПМД и ОМП. Также следует отметить, что описание опросников и выходных данных определяет состав и структуру таблиц БД.

Структура описания решающих правил показана на рис. 3. Структура секции решающих правил напрямую зависит от структуры выходных данных. В секции таблиц нормативов описываются различные нормативные данные табличной структуры, используемые в решающих правилах.

В АКДО с использованием формального описания МедО (рис. 4) входят следующие функциональные блоки:

— регистратура;

— медицинская карта, обследование;

— подсистема расчета выходных данных по решающим правилам и формирования индивидуального заключения о состоянии здоровья;

— подсистема электронного документооборота;

— подсистема передачи данных.

Программная реализация каждого блока основана на интерпретации заранее подготовленных xml-описаний, поступающих на вход комплекса. Блок документооборота позволяет пользователям самостоятельно описывать и формировать требуемые документы. Структура документа описывается при помощи трех типовых элементов: надписи, списка и таблицы. Описание правил отбора сведений из информационной базы производится с использованием понятий предметной области и на интуитивно понятном для врача языке. Сформированное описание документа при необходимости может быть передано в подчиненные организации. На основании документов, полученных от подчиненных организаций, можно сформировать результирующий документ. Таким образом, блок документооборота позволяет:

— описывать структуру документа, правила получения и интеграции данных;

— формировать документы по БД;

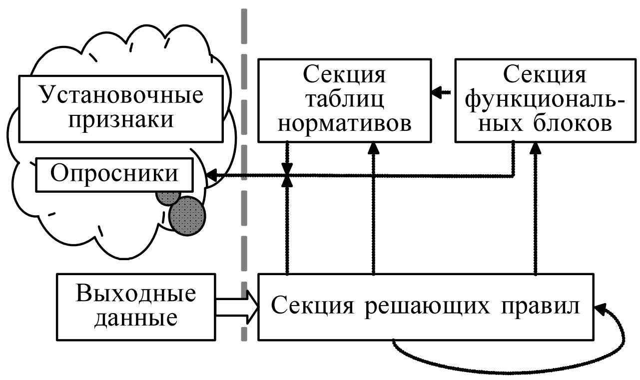
— формировать документы по другим, заранее сформированным, документам;

— осуществлять обмен документами и описаниями документов между организациями.

Таким образом, применение описанной методики при создании АКДО позволило значительно сократить временные затраты на:

■ *Рис. 1. Структура описания МедО*

■ *Рис. 2. Структура описания объектов МедО*

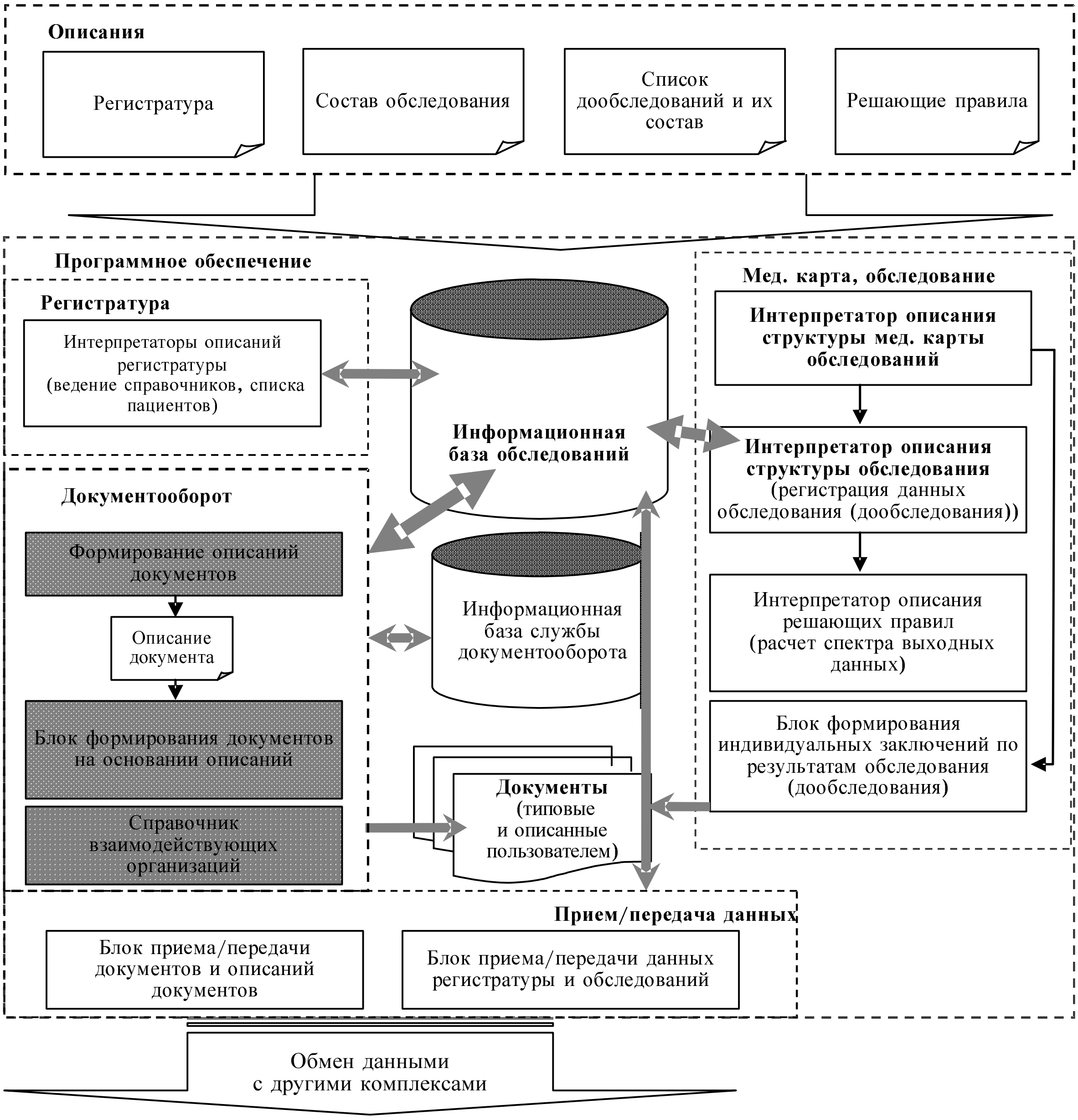


■ *Рис. 3. Структура описания решающих правил*

— расширение/изменение состава базового обследования;

— добавление новых видов дообследований;

— формирование отчетной документации в соответствии с требованиями и распоряжениями руководящих органов.



■ *Рис. 4. Базовая структура АКДО*

Литература

1. **Шерстюк Ю. М.** Основы метауправления функциональностью в информационных системах. СПб.: СПИИРАН, 2000.
2. **Шаповалов В. В., Шерстюк Ю. М.** Формальная модель автоматизированной системы скринирующей диагностики здоровья населения // Информационные технологии в здравоохранении. 2001. № 8–9. С. 8–10.
3. **Воронцов И. М., Шаповалов В. В.** Стандартизированные технологии — настоящее и будущее профилактической медицины // Медицина Петербурга. 2005. № 2 (199). С. 7.
4. **Романенко А. И., Шаповалов В. В., Шерстюк Ю. М.** Структура и формирование медицинского обеспечения программных систем и комплексов для здравоохранения // Современные информационные технологии: Тр. Междунар. науч.-техн. конф. Пенза: Пензенский технологический ин-т, 2003. С. 89–91.
5. **Шаповалов В. В., Шерстюк Ю. М.** Автоматизированный скрининг — проблема экспертных знаний // Инновации. 2003. № 10 (67). С. 89–91.

УДК 615.471:617.7

ВЛИЯНИЕ ЧАСТОТЫ ДИСКРЕТИЗАЦИИ ЭКГ НА ТОЧНОСТЬ ВЫЧИСЛЕНИЯ СПЕКТРАЛЬНЫХ ПАРАМЕТРОВ ВАРИАБЕЛЬНОСТИ СЕРДЕЧНОГО РИТМА

А. Н. Калиниченко,
канд. техн. наук, доцент
О. Д. Юрьева,
аспирант
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

Представлены результаты экспериментальной оценки зависимости ошибки вычисления спектральных параметров вариабельности сердечного ритма от частоты дискретизации при использовании трех различных методов определения опорной точки QRS-комплекса: по абсолютному максимуму, по равенству площадей под кривой и по равенству сумм квадратов модулей значений кривой, описывающей QRS-комплекс.

Введение

Анализ вариабельности сердечного ритма (ВСР) представляет собой один из наиболее распространенных методов количественной оценки активности вегетативной нервной системы. Метод основан на распознавании и измерении временных интервалов межу R-зубцами ЭКГ (RR-интервалов), построении динамических рядов кардиоинтервалов и последующем анализе полученных числовых рядов математическими методами.

Первым шагом при анализе ритма всегда является измерение RR-интервала. Оценка значений RR-интервалов по дискретизованному сигналу ЭКГ приводит к появлению ошибки, связанной с конечностью величины шага дискретизации. Низкая частота дискретизации (ЧД) может привести к неточному определению опорной точки R-зубца, что существенно изменяет измеряемые спектральные показатели ВСР. Международными стандартами измерения ВСР [1] рекомендован диапазон выбора ЧД от 250 до 500 Гц. Более низкая ЧД может дать удовлетворительные результаты только в случае, если используется какой-либо алгоритм интерполяции (например, параболический) для более точного определения опорной точки R-зубца [2].

Выбор ЧД зависит от диапазона частот ЭКГ, от конечных целей исследования и от используемого метода анализа. Выбор ЧД определяется тем, что спектральная плотность мощности ЭКГ находится в диапазоне частот 0,5÷30 Гц [3]. Согласно теореме Котельникова, достаточна частота дискретизации, равная 100 Гц. Однако Американское общество кардиологов рекомендует использовать ЧД 500 Гц. Кроме того, в последнее время появляется все больше статей, приводящих доказательства необходимости использования ЧД, равной 1 кГц [2]. Это связано с тем, что при невысокой вариабельности относительная ошибка вычисления спектральных параметров ВСР оказывается достаточно большой [4].

Для вычисления значения ВСР предложено много разнообразных методов, основанных на различных подходах к анализу сигналов. В частности, методы статистического анализа, спектральный анализ, методы нелинейной динамики, корреляционные методы. В данной работе представлены результаты исследования с использованием методов спектрального анализа.

Анализ спектральной плотности мощности позволяет получить базовую информацию о том, как распределена мощность в зависимости от частоты. В спектре различают три основные спектральные компоненты [1]: VLF (very low frequency, 0,0003÷0,04 Гц), LF (low frequency, 0,04÷0,15 Гц), HF (high frequency, 0,15÷0,4 Гц).

Целью исследования, представленного в настоящей работе, являлась сравнительная оценка различных подходов к определению опорной точки QRS-комплекса — по максимуму и «центру тяжести». Проводилась количественная оценка ошибки вычисления параметров ВСР в зависимости от выбранного значения ЧД и алгоритма определения опорной точки QRS-комплекса с целью обоснования выбора ЧД.

Исследование проводилось на модельном сигнале и реальных записях ЭКГ. Зубцы ЭКГ моделировались фрагментами синусоид.

Для проведения исследования был сформирован набор реальных записей ЭКГ в трех отведениях. Для автоматического анализа проведена верификация данных с целью определения местоположения QRS-комплексов. Общее число записей — 10. Общее число QRS-комплексов — 3210. Длительность модельного сигнала и каждой записи — 5 мин. Исходная частота дискретизации модельного сигнала и реальных записей — 500 Гц. Все расчеты выполнялись с использованием пакета MATLAB.

Определение опорной точки по максимуму QRS-комплекса

При прореживании сигнала может происходить смещение точки максимума, что в свою очередь приводит к появлению ошибки в определении опорной точки и, соответственно, к неверному измерению RR-интервалов. Из примера (рис. 1) видно, что прореживание сигнала приводит к появлению ошибки.

Вычисление номера отсчета, соответствующего максимальному значению QRS-комплекса, выполнялось по формуле

$$k_i = T_{\max i} F_d,$$

где $T_{\max i}$ — время, соответствующее максимуму QRS-комплекса; F_d — частота дискретизации.

Длительность RR-интервалов определялась по формуле

$$RR_i = (k_i - k_{i-1})T,$$

где T — интервал дискретизации.

Расчет среднеквадратической ошибки определения опорной точки QRS-комплекса выполнялся по следующей формуле:

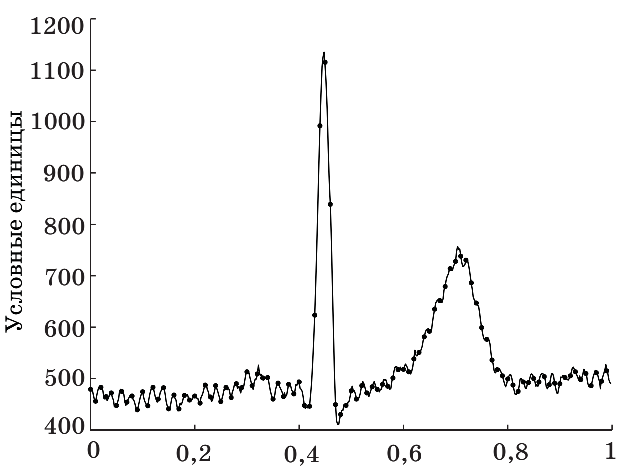
$$SQ = \frac{\sum_{i=1}^{N}(RR_{0i} - RR_{pi})^2}{N-1},$$

где RR_0 и RR_p — длительность RR-интервала исходного и прореженного сигнала соответственно (p — коэффициент прореживания); N — количество QRS-комплексов.

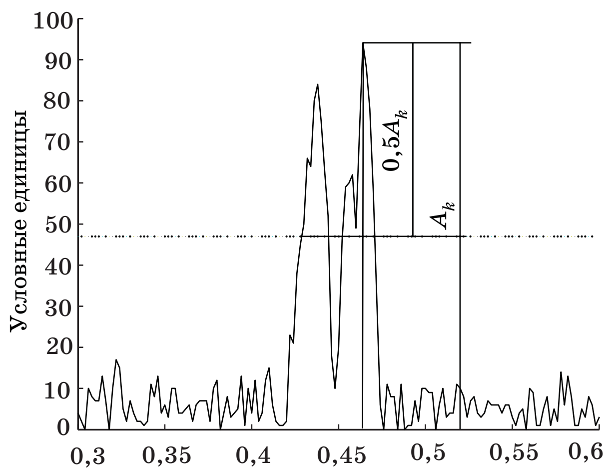
Определение опорной точки по «центру тяжести» QRS-комплекса

На первом этапе для удаления постоянной составляющей сигнала вычисляется модуль первой производной сигнала. Далее, для того чтобы устранить влияние колебаний, вызванных помехами, устанавливается некоторый порог, равный произведению коэффициента k (где $k < 1$) на максимальное значение QRS-комплекса. Опорная точка определяется двумя методами: по равенству площадей под кривой, описывающей анализируемый QRS-комплекс и ограниченной снизу порогом, и по равенству сумм квадратов модулей значений для той же кривой. На рис. 2 проиллюстрирована работа алгоритма определения опорной точки QRS-комплекса по «центру тяжести». На первом этапе работы алгоритма определяется предварительная опорная точка I_{ak}, соответствующая максимуму QRS-комплекса, а затем в соответствии с формулами, указанными ниже, определяется опорная точка I_k.

Расчет площади под кривой выполнялся по следующей формуле:



■ *Рис. 1. Отсчеты исходного сигнала и сигнала, прореженного в 5 раз (показаны жирными точками)*



■ *Рис. 2. Иллюстрация работы алгоритма определения опорной точки QRS-комплекса по «центру тяжести»*

$$Q_k = \sum_{I_{l_k}}^{I_{r_k}} q_i,$$

где $q_i = \begin{cases} 0, \ x_i \le 0{,}5A_k \\ x_i - 0{,}5A_k, \ x_i > 0{,}5A_k \end{cases}$, A_k — максимум QRS-комплекса; I_{rk} и I_{lk} — соответственно правая и левая границы анализируемого участка. На предыдущих этапах работы было показано, что точность определения опорной точки QRS-комплекса зависит от значения порога [5]. Проведенные исследования позволили утверждать, что порог $0{,}5A_k$ является оптимальным.

За опорную точку k-го комплекса принимается первый отсчет I_k, для которого выполняется условие:

$$\sum_{I_{l_k}}^{I_k} q_i \ge \frac{1}{2} Q_k$$ — для метода определения опорной точки по равенству площадей;

$$\sum_{I_{l_k}}^{I_k} |q_i|^2 \ge \frac{1}{2} Q_k$$ — для метода определения опорной точки по равенству сумм квадратов модулей значений кривой.

Методика эксперимента и результаты

В ходе эксперимента оценивалась ошибка, за которую принимался модуль разности между истинными значениями параметров ВСР и значениями параметров ВСР, измеренными для определенного коэффициента прореживания. В качестве истинных значений параметров ВСР были выбраны значения ВСР, рассчитанные по результатам ручной верификации сигнала при максимальном значении ЧД. Вычислялась абсолютная ошибка при изменении коэффициентов прореживания от 2-х до 5.

На первом этапе исследования проводилась сравнительная оценка указанных выше методов определения опорной точки на модельном сигнале. Были исследованы зависимости величины абсолютной ошибки вычисления параметров HF, LF и VLF эталонного сигнала от коэффициента прореживания. Полученные результаты представлены в табл. 1.

На втором этапе проводилось аналогичное исследование на реальных записях ЭКГ. В табл. 2 показаны результаты исследования зависимости величины абсолютной ошибки вычисления параметров HF, LF и VLF реального сигнала от коэффициента прореживания для трех методов.

■ *Таблица 1*

Параметры ВСР	Коэффициент прореживания k	Абсолютная ошибка $\times 10^3$, мс^2 (модельный сигнал)	
		Равенство площадей	Равенство модулей
VLF	2	3,5	4,0
	3	3,5	4,4
	4	5,1	4,4
	5	5,7	4,5
LF	2	15,4	13,6
	3	16,9	18,1
	4	8,5	8,0
	5	7,9	3,8
HF	2	22,9	16,7
	3	56,1	24,5
	4	79,4	69,8
	5	87,5	77,4

■ *Таблица 2*

Параметры ВСР	Коэффициент прореживания k	Абсолютная ошибка $\times 10^{-2}$, мс^2 (реальный сигнал)		
		Максимум	Равенство площадей	Равенство модулей
VLF	2	1,1	0,7	0,6
	3	1,3	1,2	0,7
	4	1,4	2,0	1,8
	5	1,4	2,3	1,4
LF	2	9,55	8,8	7,4
	3	11,4	12,0	9,5
	4	12,1	10,8	8,9
	5	12,5	11,7	7,4
HF	2	3,5	4,2	4,1
	3	4,4	4,6	5,4
	4	4,6	4,7	5,6
	5	4,7	4,6	5,2

Анализ результатов и выводы

Проведенные эксперименты показали, что метод определения опорной точки по максимуму, который используется большинством исследователей, очень чувствителен к уменьшению ЧД. Для определения опорной точки могут служить альтернативные методы, основанные на «центре тяжести»: по равенству площадей под кривой и по равенству сумм квадратов модулей значений кривой. Второй из указанных алгоритмов является более устойчивым к снижению частоты и дает лучшие результаты. Кроме того, из табл. 2 видно, что при уменьшении ЧД в 2 раза существенно возрастает ошибка измерения параметров ВСР для всех трех алгоритмов. Таким образом, остается актуальной задача дальнейшего исследования зависимости точности вычисления параметров ВСР от ЧД и создания единых рекомендаций по выбору ЧД.

На следующем этапе исследования планируется провести аналогичные исследования для других способов определения опорной точки QRS-комплекса. Вероятно, наилучшими для определения опорной точки являются методы, основанные на интегральных характеристиках описания QRS-комплекса.

Литература

1. Heart Rate Variability. Standards of Measurement, Physiological Interpretation, and Clinical Use, Task Force of the European Society of Cardiology and the North American Society of Pacing and Electrophysiology // Circulation. 1996. N 93. P. 1043–1065.
2. **Abboud S., Barnea O.** Errors due to sampling frequency of the electrocardiogram in spectral analysis of heart rate signals with low variability // Computers in Cardiology. IEEE Press, 1995. P. 461–464.
3. **Merri M. et al.** Sampling frequency of the electrocardiogram for spectral analysis of the heart rate variability // IEEE Transaction on Biomedical Engineering. 1990. P. 99.
4. **Ward S. et al.** Electrocardiogram sampling frequency errors in PR-interval spectral analysis: Proc. IEEE PGBIOMED’04. Southampton, U.K., August 2004.
5. **Юрьева О. Д.** Исследование помехоустойчивости методов измерения длительности RR-интервалов // Известия ГЭТУ. В печати.

Институт проблем управления имени В. А. Трапезникова РАН
Отделение нанотехнологий и информационных технологий
Отделение энергетики, машиностроения, механики и процессов управления РАН
Российский Национальный Комитет по автоматическому управлению
Научный совет по теории управляемых процессов и автоматизации

МУЛЬТИКОНФЕРЕНЦИЯ «ТЕОРИЯ И СИСТЕМЫ УПРАВЛЕНИЯ»
с 26 по 30 января 2009 г.

Место проведения: институт проблем управления имени В. А. Трапезникова РАН,
адрес: 117997, ГСП-7, Россия, Москва, улица Профсоюзная, 65;
институт проблем механики им. А. Ю. Ишлинского РАН,
адрес: 119526, Москва, просп. Вернадского, 101, корп. 1.

Мультиконференция «Теория и системы управления» объединяет четыре конференции

IV Международная конференция по проблемам управления (МКПУ-IV)
URL: http://www.ipu.ru
E-mail: iccpripu@ipu.ru
Тел./ факс: +7 (495) 334-89-69

Направления работы
Общие вопросы современной теории управления
Устойчивость, робастность, инвариантность, адаптация в управляемых динамических системах
Управление в междисциплинарных моделях социально-экономических и медико-биологических систем
Управление в организационных системах
Управление в промышленности, энергетике и на транспорте
Управление в гибридных и других сложных моделях динамических и интеллектуальных систем; групповое управление и мультиагентные системы
Информационные технологии в управлении; управление в вычислительных и телекоммуникационных системах
Управление подвижными объектами
Профессиональная подготовка специалистов в области управления

«Управление динамическими системами»
URL: http://www.ipmnet.ru
E-mail: kostin@ipmnet.ru
Тел.: +7 (495) 434-92-63; факс: +7 (499) 739-95-31

Направления работы
Теория управления динамическими системами
Оптимальное управление
Управление и оценивание в условиях неопределенности
Игровые задачи динамики
Управление летательными аппаратами и транспортными средствами
Управление в робототехнике и мехатронике, включая микро- и наномеханические системы

«Математическая теория систем»
URL: http://www.isa.ru
E-mail: znat@isa.ru
Тел./ факс: +7 (499) 135-51-64

Направления работы
Математические методы теории систем
Проблемы неопределенности и риски в теории систем
Самоорганизация в сложных системах
Методы и алгоритмы принятия решений
Нелинейные управляемые системы
Статистические методы в теории систем
Теория макросистем
Динамические системы, использующие экспертные знания
Математическое моделирование сложных систем

VIII Международная конференция «Идентификация систем и задачи управления» (SICPRO’09) — см. с. 8 данного издания.

УДК 519.862.6

ОСНОВЫ ЛОГИКО-ВЕРОЯТНОСТНОЙ ТЕОРИИ РИСКА С ГРУППАМИ НЕСОВМЕСТНЫХ СОБЫТИЙ

И. В. Машканцев,
системный разработчик
Е. Д. Соложенцев,
доктор техн. наук, профессор
Институт проблем машиноведения РАН

Дается краткое описание основных положений логико-вероятностной теории риска с группами несовместных событий, ее приложений и особенностей для проблемы моделирования и анализа риска в сложных системах в областях управления и эконометрики. Описывается основная идея — введение в статистическую табличную базу данных групп несовместных событий или конечных множеств, что позволяет получить систему логических уравнений или базу знаний, использовать логико-вероятностное исчисление и решать задачи риска, эффективности и управления.

Введение

Вероятностная (В) логика Дж. фон Неймана и логико-вероятностное (ЛВ) исчисление И. А. Рябинина для решения прямых задач риска появились в 50–60-х гг. XX века независимо друг от друга для разных приложений [1, 2]. В принципе, можно было использовать один термин, считая ЛВ-исчисление развитием В-логики. Однако ЛВ-исчисление породило целое научное направление и стало основой ЛВ-теории риска. Решение обратных задач риска с оценкой вероятностей по набору Л-суждений впервые рассмотрел Нильс Нилссон, но аналитическое решение удалось получить только для простейших случаев. Обратные задачи риска без каких-либо ограничений успешно решаются в ЛВ-теории риска с группами несовместных событий (ГНС) [2, 3].

Современная ЛВ-теория риска включает в себя: ЛВ-исчисление И. Рябинина, структурно-логическое моделирование А. Можаева и ЛВ-теорию риска с ГНС Е. Соложенцева. ЛВ-теорию риска следует рассматривать как новую научную дисциплину для изучения в экономических и технических университетах со своими разделами, правилами, областями применения, примерами и Software.

Основы ЛВ-теории риска с ГНС для целей управления создавались в течение 10 лет [2—5]. ЛВ-теория риска с ГНС использовалась для решения важных экономических проблем, таких как:

— классификация — кредитные риски, рейтинги, мониторинг;

— ивестирование — портфель ценных бумаг;

— эффективность — управление социальными процессами;

— качество — управление качеством функционирования;

— менеджмент — управление риском неуспеха менеджмента компании по функциям, предметным областям и достижению целей;

— взятки и коррупция — выявление взяток по статистике параметров функционирования учреждения, поведения чиновников, обслуживания;

— управление развитием и испытаниями — организационные и экономические системы, машины и технологии.

При решении названных выше проблем выявились достоинства ЛВ-теории риска с ГНС:

— в два раза большая точность в распознавании плохих и хороших объектов;

— в семь раз большая робастность (стабильность) в распознавании объектов;

— абсолютная прозрачность в оценке и анализе риска и ЛВ-модели риска;

— решение новых задач анализа риска объектов и модели риска;

— возможность управлять риском и эффективностью.

ЛВ-теория риска с ГНС отличается: видом используемой информации, типом связей между переменными, законами распределений переменных, методами решения обратных задач, сложностью логических функций и описаний объектов, использованием статических и динамических моделей риска, методами оценивания, использованием комбинированных моделей риска, способами управления и научными основами (табл. 1).

На основе ЛВ-теории риска с ГНС разработаны ЛВ-модели риска неуспеха для проблем классифи-

■ ***Таблица 1.*** *Отличия ЛВ-теории риска с ГНС*

ЛВ-теорией риска используются	Другими теориями используются
База знаний (БЗ)	База данных (БД)
Логические зависимости между переменными	Функциональные и корреляционные зависимости между переменными
Дискретные табличные распределения	Нормальное и аналитические распределения
Алгоритмические итеративные методы решения обратных и оптимизационных задач	Аналитические методы решения обратных и оптимизационных задач
Л-функции любой сложности с любым числом объектов в статистике, параметров и градаций параметров	Функции ограниченной сложности с небольшим числом объектов, параметров и градаций параметров
Статические и динамические модели риска	Статические модели риска
Оценки по статистическим данным	Экспертные оценки
Комбинированные Л-модели риска	Отдельные модели риска
Управление по вкладам инициирующих событий в риск и эффективность	Управление по значениям риска и эффективности
Логика и дискретная математика	Теория статистики и непрерывная математика

кации, инвестирования, эффективности, менеджмента, взяток и коррупции [2—5]. Изложим ЛВ-теорию риска с ГНС с примерами из наиболее характерной и «продвинутой» проблемы классификации (кредитных рисков).

Переход от базы данных к базе знаний

Общим для проблем классификации, инвестирования, эффективности, менеджмента, взяток и коррупции является одинаковое табличное представление статистических данных (БД) [2, 3].

База данных табличного типа (табл. 2) содержит статистическую информацию об однородных объектах (кредитах) или состояниях одного объекта в разные моменты времени (портфель ценных бумаг). В таблице БД количество столбцов может достигать нескольких десятков, а количество строк — нескольких сотен. В БД значения даже для одного параметра могут иметь бесконечное множество рациональных значений.

В ячейках таблицы — значения параметров (количественные или качественные), характеризующих объект или состояние объекта. Для измерения параметров используются шкалы: логическая, качественная, числовая и др. Последний столбец таблицы — параметр эффективности объекта или состояния объекта. Параметры, описывающие объект, обозначим строчными буквами $z_1, ..., z_j, ..., z_n$, а параметр эффективности объекта — строчной буквой y_i, $i = 1, 2, ..., N$. В клетках табл. 2 находятся значения параметров z_{ij} и для последнего столбца — значения параметра эффективности y_i.

База знаний. Изменим исходное представление БД, заменив значения параметров на их градации (нумерованные интервалы) (табл. 3). В сценариях и ЛВ-моделях риска проблем классификации, инвестирования, эффективности, менеджмента, коррупции и взяток имеется большое число объектов N (до 1000 и более), событий-параметров n (до 20 и более), событий-градаций в каждом событии-параметре (от 2-х до 40).

Таким образом, в табл. 3 для каждого параметра введены множества с конечным числом элемен-

■ ***Таблица 2.*** *Объекты и значения параметров*

Объект	Параметр 1 z_1	...	Параметр j z_j	...	Параметр n z_n	Параметр эффективности y_i
1		...		...		
...	...	...	...	...	...	
i		...	z_{ji}	...	...	y_i
...	...	...	...	...	...	
N		...		...		

■ ***Таблица 3.*** *Объекты и градации параметров*

Объект	Параметр 1 Z_1	...	Параметр j Z_j	...	Параметр n Z_n	Параметр эффективности Y
1		...		...		
...	...	...	...	...	...	
i		...	Z_{jr}	...	...	Y_r
...	...	...	...	...	...	
N		...		...		

тов (градаций). Если в табл. 2 параметры могли принимать несчетное количество разных значений, то теперь каждый параметр имеет конечное число элементов.

Теперь параметры объекта будем называть событиями-параметрами и Л-переменными и обозначать прописными буквами $Z_1, ..., Z_j, ..., Z_n$, а параметр эффективности объекта — событием-параметром эффективности и обозначать прописной буквой Y. В клетках табл. 3 находятся события-градации Z_{jr}, $j = 1, 2, ..., n$; $r = 1, 2, ..., N_j$ параметров $Z_1, ..., Z_j, ..., Z_n$. В последнем столбце — события-градации Y_r, $r = 1, 2, ..., N_y$ параметра эффективности Y. В общем случае градации линейно неупорядочены и нельзя сказать, что градация 3 лучше или хуже градации 4.

Для проблемы классификации получим систему Л-уравнений риска:

$$\begin{cases} Z^1_{1\ r_1\in N_1} \vee \cdots \vee Z^1_{j\ r_j\in N_j} \vee \cdots \vee Z^1_{n\ r_n\in N_n} = Y^1_{\ r_y\in N_y} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ Z^i_{1\ r_1\in N_1} \vee \cdots \vee Z^i_{j\ r_j\in N_j} \vee \cdots \vee Z^i_{n\ r_n\in N_n} = Y^i_{\ r_y\in N_y} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ Z^N_{1\ r_1\in N_1} \vee \cdots \vee Z^N_{j\ r_j\in N_j} \vee \cdots \vee Z^N_{n\ r_n\in N_n} = Y^N_{\ r_y\in N_y} \end{cases}, \quad (1)$$

где $i = 1, 2, ..., N$; $j = 1, 2, ..., n$; $r_j \in N_j$; $r_y \in N_y$.

Систему Л-уравнений типа (1) и будем называть базой знаний, а также рассматривать как систему Л-высказываний и использовать для получения новых знаний. Для БЗ легко вычислить частоты (вероятности) событий-градаций. Они равны отношению числа объектов или состояний с градацией к общему числу объектов или состояний в БЗ, равному N. С каждой Л-переменной свяжем вероятность ее истинности. Обозначим для события-параметра: p — вероятность неуспеха; $q = 1-p$ — вероятность успеха.

Систему Л-уравнений (1) после ее ортогонализации можно преобразовать в следующую систему В-полиномов:

$$\begin{cases} P^1_{1\ r_1\in N_1} + P^1_{2\ r_2\in N_2}(1 - P^1_{1\ r_1\in N_1}) + \\ + P^1_{3\ r_3\in N_3}(1 - P^1_{1\ r_1\in N_1})(1 - P^1_{2\ r_2\in N2}) + \cdots = P^1_{\ r_y\in N_y} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ P^i_{1\ r_1\in N_1} + P^i_{2\ r_2\in N_2}(1 - P^i_{1\ r_1\in N_1}) + \\ + P^i_{3\ r_3\in N_3}(1 - P^i_{1\ r_1\in N_1})(1 - P^i_{2\ r_2\in N2}) + \cdots = P^i_{\ r_y\in N_y} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ P^N_{1\ r_1\in N_1} + P^N_{2\ r_2\in N_2}(1 - P^N_{1\ r_1\in N_1}) + P^N_{3\ r_3\in N_3} \times \\ \times (1 - P^N_{1\ r_1\in N_1})(1 - P^N_{2\ r_2\in N2}) + \cdots = P^N_{\ r_y\in N_y} \end{cases}. \quad (2)$$

В ЛВ-теории риска с ГНС события-параметры связаны Л-операциями AND, OR, NOT и могут иметься циклы. В общем случае получим другие записи уравнений (1) и (2). Событиям-параметрам соответствуют Л-переменные, которые могут быть зависимыми, но не изначально, а только потому, что они содержатся в Л-формуле, которая и определяет зависимость между ними. События-градации для параметра являются зависимыми и образуют ГНС [2—3].

Вероятности в ГНС

Запишем в общем виде Л-функцию риска

$$Y = Y(Z_1, Z_2, ..., Z_n) \quad (3)$$

и В-функцию риска для объекта таблицы

$$P_i\{Y_i = 1|Z(i)\} = P(P_1, ..., P_j, ..., P_n),\ i = 1, 2, ..., N. \quad (4)$$

Для каждого события-градации в ГНС рассматриваются три вероятности (рис. 1): $P2_{jr}$ — относительная частота в статистике; $P1_{jr}$ — вероятность в ГНС; P_{jr} — вероятность, подставляемая в (4) вместо вероятности P_j для события-параметра. Определим эти вероятности для j-й ГНС:

$$P2_{jr} = P\{Z_{jr} = 1\};\ \sum_{r=1}^{N_j} P2_{jr} = 1,\ r = 1, 2, \ldots, N_j; \quad (5)$$

$$P1_{jr} = P\{Y = 1 \mid Z_j = 1\};\ \sum_{r=1}^{N_j} P1_{jr} = 1,\ r = 1, 2, \ldots, N_j; \quad (6)$$

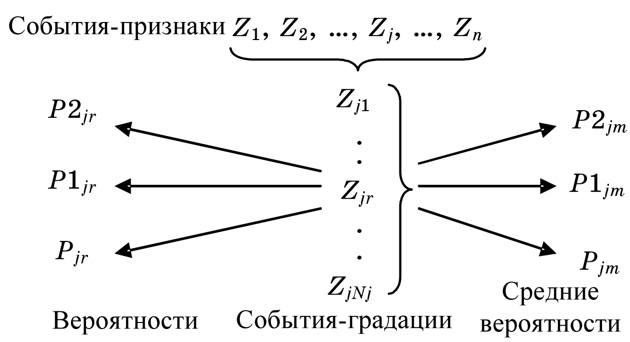
$$P_{jr} = P\{Y = 1|Z_{jr} = 1\};\ r = 1, 2, ..., N_j,\ j = 1, 2, ..., n, \quad (7)$$

где n, N_j — числа признаков и градаций в j-признаке, черточка '|' читается «при условии».

Средние значения вероятностей $P2_{jr}$, $P1_{jr}$ и P_{jr} для градаций в ГНС равны:

$$P2_{jm} = 1/N_j;\ P_{jm} = \sum_{r=1}^{N_j} P_{jr} P2_{jr};$$

$$P1_{jm} = \sum_{r=1}^{N_j} P1_{jr} P2_{jr}. \quad (8)$$



■ ***Рис. 1.*** *Вероятности в группе несовместных событий*

Вероятности P_{jr} будем оценивать при алгоритмической итеративной идентификации В-модели риска по статистическим данным. Вначале нужно определить вероятности $P1_{jr}$, удовлетворяющие (6), и перейти от вероятностей $P1_{jr}$ к вероятностям P_{jr}. Число независимых вероятностей

$$N_{ind} = \sum_{j=1}^{n} N_j - n. \qquad (9)$$

Вероятности P_{jr} и $P1_{jr}$ связаны по формуле Байеса для случая ограниченного количества информации [2—4] через средние вероятности P_{jm} и $P1_{jm}$:

$$P_{jr} = \frac{P1_{jr} P_{jm}}{P1_{jm}},\ r = 1,\ 2,\ \ldots,\ N_j;\ j = 1,\ 2,\ \ldots,\ n. \qquad (10)$$

Системы логических и вероятностных уравнений базы знаний

Успех объекта из табл. 3, описываемого параметрами (Л-переменными) $Z_1, Z_2, ..., Z_n$, определяется следующей Л-функцией (конъюнкцией) [2, 3]:

$$Y = Z_1 \wedge Z_2 \wedge \ldots \wedge Z_j \wedge \ldots \wedge Z_n. \qquad (11)$$

Неуспех определяется по правилу де Моргана (отрицание конъюнкции)

$$\bar{Y} = \bar{Z}_1 \vee \bar{Z}_2 \vee \bar{Z}_3 \vee \ldots \vee \bar{Z}_n. \qquad (12)$$

Вместо Л-переменных Z_1, Z_2, ..., Z_n в Л-выражения (11) и (12) следует подставить Л-переменные для градаций этих переменных. Из Л-функции (11) и (12) получают В-полиномы. Обозначим для события-параметра: p_1 — вероятность успеха; $1 - p_1 = q_1$ — вероятность неуспеха. Тогда В-полином для Л-функции (11)

$$P\{Y = 1\} = p_1 p_2 p_3 \times \ldots \times p_n. \qquad (13)$$

Для перехода от Л-функции (12) к В-функции нужно в общем случае (когда Л-функция — сложное выражение) выполнить ортогонализацию этой функции:

$$\tilde{Y} = \bar{Z}_1 \vee \bar{Z}_2 Z_1 \vee \bar{Z}_3 Z_2 Z_1 \vee \ldots \qquad (14)$$

Тогда В-полином можно записать

$$P\{\bar{Y} = 1\} = q_1 + q_2 p_1 + q_3 p_2 p_1 + \ldots \qquad (15)$$

Так как приведенные Л-функции очень просты (последовательное соединение для успеха и параллельное соединение для неуспеха), то вместо (15) известно также другое простое выражение для В-полинома:

$$P\{\bar{Y} = 1\} = 1 - (1 - p_1)(1 - p_2) \times \ldots \times (1 - p_n). \qquad (16)$$

Арифметика В-модели риска такова, что риск по формулам (15) и (16) находится в интервале [0, 1] при любых значениях вероятностей инициирующих событий.

В соответствии с табл. 3 строится система из N Л-уравнений типа (12). Число возможных разных объектов или состояний объекта в табл. 3 равно

$$N_{\max} = N_1 N_2 \times \ldots \times N_j \times \ldots \times N_n, \qquad (17)$$

где $N_1, ..., N_j, ..., N_n$ — число градаций в событиях-параметрах.

Если число параметров равно $n = 20$ и каждый имеет $N_j = 5$ градаций, то число возможных разных объектов (комбинаций) равно астрономическому числу $N_{\max} = 5^{20}$, что объясняет вычислительные трудности решения задач риска.

Запишем Л-функцию для объектов в табл. 3:

$$Y = Y_1 \vee Y_2 \vee \ldots \vee Y_i \vee \ldots \vee Y_N, \qquad (18)$$

где каждый объект определяется Л-функцией (11), включающей все Л-переменные.

В табл. 3 каждая Л-переменная в (18) принимает много значений по числу градаций, на которые она разбита. Л-функции для двух разных объектов, например:

$$Y_i = Z_1 \wedge Z_2 \wedge \ldots \wedge Z_{jr} \wedge \ldots \wedge Z_n; \qquad (19)$$

$$Y_k = Z_1 \wedge Z_2 \wedge \ldots \wedge Z_{jr+1} \wedge \ldots \wedge Z_n, \qquad (20)$$

ортогональны

$$Y_i \wedge Y_k = 0, \qquad (21)$$

так как $Z_{jr} \wedge Z_{jr+1} = 0$, ибо Z_{jr} и Z_{jr+1} принадлежат одной ГНС.

Свойство ортогональности Л-слагаемых Л-функции риска (20) позволяет перейти от Л-функций к алгебраическим выражениям для вероятностей, т. е. Л-переменные заменить на вероятности и знаки '$\vee$' на знаки '+'.

Для названных выше приложений предложены следующие типы ЛВ-моделей риска с ГНС: с полным и ограниченным числом событий, динамические и комплексные (табл. 4).

■ ***Таблица 4.*** *Типы ЛВ-моделей риска с ГНС*

Тип ЛВ-модели риска	Содержание
С полным числом событий	Л-функция риска в совершенной дизъюнктивной нормальной форме (СДНФ)
С ограниченным числом событий	Л-функция риска в виде: кратчайших путей успеха, минимальных сечений неуспеха и ограниченного (сценарием) числа событий
Динамический	С изменяющимися вероятностями событий и временем — параметром (в техническом анализе)
Комбинированный	С логическим объединением связями OR, AND, NOT отдельных сценариев и Л-функций риска

Идентификация ЛВ-модели риска с ГНС по статистическим данным

Задача идентификации В-модели риска по статистическим данным — обратная оптимизационная задача, является основной и сложной в проблемах риска [2—5]. Для ее решения систему из Л-уравнений типа (12) заменяют на систему из В-полиномов типа (15). Вероятности в левой части системы неизвестны.

Предложена следующая схема решения задачи. Пусть известны в первом приближении вероятности для градаций P_{jr}, $r = 1, 2, ..., N_j$, $j = 1, 2, ..., n$ и вычислены риски P_i, $i = 1, ..., N$ для объектов в статистике из N_g хороших и N_b плохих объектов. Определим допустимый риск P_{ad} так (рис. 2), чтобы принятое расчетное число хороших объектов N_{gc} имело риск меньше допустимого и соответственно число плохих объектов $N_{bc} = N - N_{gc}$ имело риск больше допустимого. На шаге оптимизации изменим так вероятности P_{jr}, $r = 1, 2, ..., N_j$, $j = 1, 2, ..., n$, чтобы число корректно распознаваемых объектов увеличилось.

Переменные P_{ad} и N_{gc} связаны однозначно. В алгоритме задачи удобнее задавать N_{gc} и определять допустимый риск P_{ad}.

Условие $P_i > P_{ad}$ выделяет следующие типы объектов: N_{gg} — хорошие по модели и статистике; N_{gb} — хорошие по модели и плохие по статистике; N_{bg} — плохие по модели и хорошие по статистике; N_{bb} — плохие по модели и статистике. Риски объектов N_{gg}, N_{bg}, N_{gb}, N_{bb} перемещаются относительно P_{ad} при изменении P_{jr}. При переходе одних объектов вправо от P_{ad} такое же число объектов переходит влево. Оптимальным будет такое изменение P_{jr}, которое переводит объекты N_{gb} и N_{bg} через P_{ad} навстречу друг другу.

Задача идентификации В-модели риска сформулирована так [2—4].

Заданы: статистика по объектам, имеющая N_g хороших и N_b плохих объектов, и В-модель риска типа (15).

Требуется определить: вероятности P_{jr}, $r = 1, 2, ..., N_j$, $j = 1, 2, ..., n$ событий-градаций и допустимый риск P_{ad}, разделяющий объекты на хорошие и плохие.

Критерий оптимизации: число корректно классифицируемых объектов должно быть максимальным:

$$F = N_{bb} + N_{gg} \to \max_{P_{jr}}. \qquad (22)$$

Важно, что критерий оптимизации, в отличие от скоринговых и других методик, использует прямой прозрачный целочисленный критерий оптимизации. Из выражения (22) следует, что точность В-модели риска в классификации хороших E_g и плохих E_b объектов и в целом E_m равна:

$$E_g = N_{gb}/N_g;\ E_b = E_{bg}/E_b;\ E_m = (N - F)/N. \qquad (23)$$

Ограничения:

1) вероятности P_{jr} должны удовлетворять условию

$$0 < P_{jr} < 1,\ j = 1, 2, ..., n;\ r = 1, 2, ..., N_j; \qquad (24)$$

2) средние риски объектов по В-модели риска и статистике должны быть равны; при обучении В-модели риска будем корректировать вероятности P_{jr} на шаге итеративного процесса идентификации по формуле

$$P_{jr} = P_{jr}(P_{av}/P_m);\ j = 1, 2, ..., n;\ r = 1, 2, ..., N_j, \qquad (25)$$

где $P_{av} = N_b / N$ — средний риск по статистике; P_m — средний риск по модели;

3) допустимый риск P_{ad} определяется при заданном коэффициенте асимметрии распознавания хороших и плохих объектов, равном

$$E_{gb} = N_{gb}/N_{bg}. \qquad (26)$$

Потери неэквивалентны при ошибочном распознавании хорошего и плохого объектов.

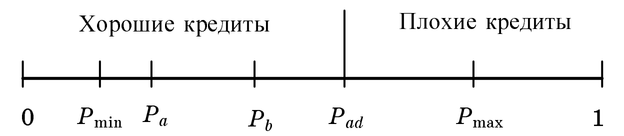
Формула для итеративной алгоритмической идентификации ЛВ-модели риска

$$\Delta P1_{jr} = K_1 \frac{N_{\text{opt}} - N_v}{N_{\text{opt}}} K_3 P1_{jr},$$
$$j = 1, 2, \ldots, n,\ r = 1, 2, \ldots, N_j, \qquad (27)$$

где K_1 — коэффициент, равный ~ 0,05; N_{opt}, N_v — число оптимизаций и номер текущей оптимизации; K_3 — случайное число в интервале [−1, +1]. В процессе итеративной алгоритмической оптимизации $\Delta P1_{jr}$ стремится к нулю. Формула (27) обеспечивает простое задание максимального приращения вероятностей и определение точности оценки вероятностей по величине приращений на шаге последней оптимизации.

Оценка риска нового объекта выполняется на В-модели риска при известных вероятностях P_{jr}, $j = 1, 2, ..., n$; $r = 1, 2, ..., N_j$, где вместо вероятностей событий-признаков P_1, P_2, P_3, ... подставляются вероятности их событий-градаций P_{jr}, $j = 1, 2, ..., n$; $r = 1, 2, ..., N_j$.

В работах [2, 4] приведены результаты идентификации ЛВ-модели кредитных рисков по реальным статистическим данным банка. Имелось $N = 1000$ логических уравнений, оценивались 94 вероятности P_{jr}, $j = 1, 2, ..., 20$, $r = 1, 2, ..., N_j$ и допустимый риск P_{ad}. ЛВ-модели кредитного риска с ГНС показали в два раза большую точность и в семь раз большую робастность, а также абсолютную прозрачность в распознавании плохих



■ ***Рис. 2.** Схема классификации объектов* и хороших кредитов, чем известные западные и скоринговые методики.

Алгоритмический итеративный метод идентификации ЛВ-модели риска с ГНС позволяет извлекать из БЗ или системы Л-уравнений новые знания (вероятности и вклады событий-градаций, допустимый риск, асимметрию распознавания и др.) при любой сложности ЛВ-функции риска и любых числах объектов в статистике, параметров объекта и градаций в каждом параметре.

Анализ риска

Вклады событий и градаций в риск объекта. Пусть В-модель риска идентифицирована по статистическим данным и известны вероятности P_{jr}. Определим вклады событий-признаков и событий-градаций в риск объекта и средний риск множества объектов, а также в точность ЛВ-модели риска, вычисляя разности между значениями названных характеристик для В-модели риска после ее идентификации и при условии (|) придания соответствующим вероятностям событий-признаков нулевых значений [2, 3].

Вклад признака (всех градаций признака) в риск объекта i

$$\Delta P_j = P(i) - P(i)\big|_{P_j=0},\ j=1,\ 2,\ \ldots,\ n. \qquad (28)$$

Вклад признака в средний риск P_m множества объектов

$$\Delta P_{jm} = P_{jm} - P_{jm}\big|_{P_j=0},\ j=1,\ 2,\ \ldots,\ n. \qquad (29)$$

Вклад признака в целевую функцию $F_{\max}$

$$\Delta F_j = F_{\max} - F\big|_{P_j=0},\ j=1,2,\ \ldots,\ n. \qquad (30)$$

Вычисление вкладов градаций ΔP_{jrm} и ΔF_{jr} по предложенной схеме было бы некорректно, ибо не ясно, как корректировать частоты других градаций $P2_{jr}$ в ГНС, если одной из них придается нулевое значение. Поэтому вместо вкладов ΔF_{jr} будем вычислять ошибки классификации объектов по каждому событию-градации:

$$E_{jrg} = (N_{jrg} - N_{jrgg})/N_{jrg};\ E_{jrb} = (N_{jrb} - N_{jrbb})/N_{jrb};$$

$$E_{jrm} = (N_{jr} - N_{jrgg} - N_{jrbb})/N_{jr}, \qquad (31)$$

где N_{jrg}, N_{jrb}, N_{jr} — числа хороших, плохих и всего объектов с градацией; N_{jrgg}, N_{jrbb} — числа хороших и плохих объектов с корректной классификацией.

Опасные элементы и их комбинации. Другое важное применение ЛВ-анализа риска состоит в следующем. Если рассматривать Л-функцию риска, то при $P_j = 1$ для элемента j (вероятности отказов остальных элементов принять равными 0,5) может произойти отказ объекта или, что то же самое, значение риска параметра эффективности Y будет равняться 1. Последовательно исключая только один параметр из множества Z_j, $j = 1, 2, \ldots, n$ или два параметра из этого множества (все различные комбинации по два), просто установить самые опасные элементы системы или их комбинации по два, по три и т. д. Примеры такого определения самых опасных элементов системы приведены в работах Н. А. Махутова и В. В. Ярошенко по выбору целей бесконтактных войн 6-го и 7-го поколений.

Атрибуты риска и управление риском

Из системы Л-уравнений и соответствующей системы В-полиномов получают методом алгоритмической итеративной идентификации следующие новые знания: вероятности P_{jr}, $j = 1, 2, \ldots, n$, $r = 1, 2, \ldots, N_j$; вклады событий-градаций Z_{jr}, $j = 1, 2, \ldots, n$, $r = 1, 2, \ldots, N_j$ в риск каждого объекта и всего множества объектов; точность ЛВ-модели риска; допустимый риск P_{ad}.

Атрибутами риска события-градации являются: вероятность неуспеха для объекта, относительная вероятность неуспеха среди градаций события-параметра, вероятность-частота в множестве объектов, вклад в точность модели.

Атрибутами риска события-параметра являются: вероятность неуспеха для объекта, структурный вес и значимость в модели риска, вклад в средний риск множества объектов.

Атрибутами риска объекта являются: риск неуспеха, возможные потери, цена за риск, вклад в риск множества объектов.

Атрибутами риска множества объектов являются: допустимый риск, средний риск, средние потери, допустимые потери, асимметрия распознавания хороших и плохих объектов, число объектов, число опасных объектов, энтропия рисков.

Рассмотрим управление кредитным риском, исходя из количественных значений описанных атрибутов. Целью управления является снижение финансовых потерь банка и повышение точности распознавания плохих и хороших кредитов. Параметрами управления риском кредита и кредитной деятельностью банка являются: риск кредита, который сравнивают с допустимым риском и принимают решение о выдаче кредита; коэффициент асимметрии распознавания хороших и плохих кредитов; цена за кредит, зависящая от риска кредита и его отличия от допустимого риска; число признаков, описывающих кредит; число градаций для каждого признака; ширина интервалов при выделении градаций для таких признаков, как сумма кредита, его срок, возраст клиента и др.

Приложения ЛВ-теории риска с ГНС

Приложениями ЛВ-теории риска с ГНС, кроме кредитных рисков, являются проблемы инвестирования, эффективности, менеджмента, взяток и коррупции, которые отличаются, по существу, только постановкой задач оптимизации [2—4].

Инвестирование. Разработана ЛВ-модель риска инвестиций, в которой определяются оптималь-

■ ***Таблица 5.*** *Особенности ЛВ-теории риска с ГНС*

Параметр	Содержание
Объекты исследования	Структурно-сложные, многокомпонентные и многоуровневые системы: банковские, экономические и организационные
ЛВ-модели риска с ГНС	С полным числом событий, с ограниченным числом событий, комплексные модели риска, динамические модели риска
Области применения	Проблемы классификации, инвестирования, эффективности, менеджмента, взяток и коррупции
Решаемые задачи	Количественная оценка и анализ риска объекта и множества объектов, управление риском, управление портфелем и эффективностью, моделирование риска неуспеха менеджмента, выявление взяток и коррупции
Методические основы ЛВ-теории риска с ГНС	Логика, теории множеств и вероятностей, комбинаторика, дискретная математика, ЛВ-исчисление с логическими связями элементов OR, AND, NOT и циклами
Переход от БД к БЗ	Вводят ГНС или конечные множества и преобразуют статистическую БД в БЗ в виде системы Л-уравнений (Л-высказываний), что позволяет использовать ЛВ-исчисление и решать задачи риска, эффективности и управления
Определение риска	Вводится допустимый риск, разделяющий объекты на плохие и хорошие. Риск каждого уровня определяется своими атрибутами
Критерии качества Л-модели риска	Точность (ошибки классификации), робастность, прозрачность результатов и анализа риска и модели риска
Распределения переменных	Дискретные табличные распределения случайных переменных
Связанность и зависимость переменных	Л-переменные могут быть зависимыми, но не изначально, а только потому, что они содержатся в определенной Л-формуле, которая и определяет зависимость между ними. События-градации для каждого параметра зависимы и рассматриваются как ГНС
Тип вычислений	Алгоритмические итеративные методы. Это обеспечивает возможность решения обратной оптимизационной задачи риска независимо от количеств объектов в статистической БД, параметров, описывающих объект, градаций в каждом параметре, Л-сложности модели риска
Построение модели риска	Сценарий, граф-модель риска, Л-функция риска, ортогональная Л-функция, В-функция риска, идентификация В-функции риска
Идентификация ЛВ-модели риска	Идентификации В-модели риска по статистическим данным сведена к решению задачи оптимизации с целочисленной целевой функцией, большим числом неизвестных параметров-вероятностей и локальными экстремумами. Решают алгоритмическими итеративными методами (случайного поиска и градиентов). Используют формулу Байеса для связи вероятностей в ГНС
Логические разности	На каждом шаге оптимизации нужно определить приращение каждой вероятности. При этом следует нормировать вероятности в ГНС, т. е. их сумма должна равняться 1
Анализ риска	Вычисляют вклады в риск объекта, всего множества объектов и целевую функцию событий-параметров и событий-градаций. Эти вклады — атрибуты риска — и позволяют управлять риском и эффективностью
Управление риском	Активное управление риском по вкладам событий-признаков и событий-градаций в риск и эффективность
Программные средства	Специальные Software для идентификации В-модели риска, выбора портфеля ценных бумаг, структурно-логического моделирования

ные доли капитала в ценные бумаги портфеля. В этой модели, в отличие от теорий Марковица и VaR, не используется допущение о нормальности законов распределения доходности ценных бумаг и всего портфеля.

Используется переход от табличной статистической БД по доходностям акций портфеля к БЗ в виде системы Л-уравнений (Л-высказываний). Для этого диапазон изменения доходности каждой акции и портфеля разбивается на интервалы (события-градации). Наряду с допустимой доходностью портфеля Y_{ad} и риском портфеля $Risk$ вводятся понятия числа опасных состояний N_{ad} и энтропии H_{ad} рисков опасных состояний в «хвосте» распределения доходности портфеля. Это позволяет анализировать риск портфеля и управлять им.

Эффективность. Разработана ЛВ-модель риска эффективности социальных процессов, в которой оцениваются весомости инициирующих случайных процессов для итогового случайного процесса параметра эффективности. Используется переход от табличной статистической БД значений влияющих параметров и итогового параметра эффективности к БЗ в виде системы Л-уравнений (Л-высказываний). Для этого диапазоны изменения влияющих и итогового параметра разбиваются на интервалы (события-градации). Для параметра эффективности вводятся понятия: допустимое значение Y_{ad} , риск $Risk$, число опасных состояний N_{ad} и энтропия H_{ad} рисков опасных состояний в «хвосте» распределения параметра эффективности. Это позволяет анализировать риск и эффективность и управлять ими. В отличие от работ лауреата Нобелевской премии Дж. Хекмана, задача решается при произвольных распределениях влияющих параметров и параметра эффективности.

Менеджмент. Разработаны ЛВ-модели риска неуспеха менеджмента компании по функциям, по направлениям деятельности; по управлению компанией как сложным объектом; по достижению одной и группы целей; по качеству функционирования. В рассмотренных моделях статистические данные не используются и не осуществляется переход от БД к БЗ. Демонстрируется построение и использование комплексных ЛВ-моделей риска, построенных из частных моделей. На необходимость разработки моделей риска для управления менеджментом указывал в своих работах великий американский экономист Питер Ф. Друкер.

Взятки. Разработаны следующие ЛВ-модели риска взяток [5]: в учреждении по параметрам успешности его функционирования, чиновников по параметрам их поведения, в учреждении и чиновников по параметрам обслуживания, в комплексе на основе Л-сложения первых трех моделей. Для построения названных ЛВ-моделей риска используется переход от табличных статистических БД к БЗ в виде системы Л-уравнений (Л-высказываний).

ЛВ-модели риска взяток предназначены для использования в департаменте «Экономические преступления» города, в службах внутренней безопасности компаний и банков и для разработки стандартов на параметры обслуживания.

Особенности ЛВ-теории риска с ГНС

Приведем в табличной форме особенности ЛВ-теории риска с ГНС (табл. 5), учитывая также результаты работ [2—5].

Проблемы ЛВ-теории риска с ГНС

Наряду с вышеизложенными основами ЛВ-теории риска с ГНС разработаны:

— *формальное изложение ЛВ-теории риска с ГНС* по академику Мальцеву, включающее в себя описание множеств и отношений на множествах, атрибутов элементов множеств, сигнатуры и аксиом, аппарата вывода;

— *учебный курс по ЛВ-теории риска с ГНС в экономике*, включающий в себя лекции, лабораторные работы на компьютере и предметные индексы;

— *программное обеспечение для ЛВ-теории риска с ГНС*, включающее в себя Software для идентификации, оценки и анализа кредитных рисков; для выбора, оценки и анализа риска портфеля ценных бумаг; для автоматизированного структурно-логического моделирования рисков.

Определено полное решение проблемы разработки и использования ЛВ-теории риска с ГНС для целей управления:

— разработка ЛВ-моделей риска с ГНС для разных приложений;

— разработка учебного курса по ЛВ-теории риска с ГНС в экономике;

— разработка Software для ЛВ-моделирования и управления риском;

— экспертиза и сертификация ЛВ-моделей риска и программных средств.

Литература

1. **Рябинин И. А.** Надежность и безопасность структурно-сложных систем. 2-е изд. СПб.: Изд-во СПбГУ, 2007. 276 с.
2. **Соложенцев Е. Д.** Сценарное логико-вероятностное управление риском в бизнесе и технике. 2-е изд. СПб.: Бизнес-пресса, 2006. 560 с.
3. **Solojentsev E. D.** Scenario Logic and Probabilistic Management of Risk in Business and Engineering. Springer, 2004. 391 p.
4. **Соложенцев Е. Д., Степанова Н. В., Карасев В. В.** Прозрачность методик оценки кредитных рисков и рейтингов. СПб.: Изд-во СПбГУ, 2005. 197 с.
5. **Соложенцев Е. Д.** Сценарные логико-вероятностные модели риска взяток // Финансы и Бизнес. 2007. № 1. С. 125–138.

СВЕДЕНИЯ ОБ АВТОРАХ

АНАНЬЕВ
Михаил
Юрьевич

Аспирант Санкт-Петербургского государственного университета водных коммуникаций.
В 2005 году окончил Санкт-Петербургский государственный университет водных коммуникаций.
Область научных интересов — информационная безопасность, криптография.

ГОРТИНСКАЯ
Лидия
Вячеславовна

Научный сотрудник научного филиала ФГУП НИИ «Вектор» — специализированного центра программных систем «Спектр».
В 2004 году окончила Санкт-Петербургский государственный университет информационных технологий, механики и оптики.
Является автором 48 научных публикаций.
Область научных интересов — информационная безопасность, криптография.

КНЯЗЕВ
Евгений
Геннадьевич

Старший разработчик программного обеспечения ЗАО «Транзас Технологии».
В 2005 году окончил Санкт-Петербургский государственный университет информационных технологий, механики и оптики.
Является автором четырех научных публикаций.
Область научных интересов — применение методов Data Mining к анализу исходного кода программ.

ВОРОБЬЕВ
Станислав
Николаевич

Доцент Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1962 году окончил Ленинградский институт авиационного приборостроения.
В 1971 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 50 научных публикаций.
Область научных интересов — моделирование систем и процессов.

КАЛИНИЧЕНКО
Александр
Николаевич

Доцент кафедры биомедицинской электроники и охраны среды Санкт-Петербургского государственного электротехнического университета «ЛЭТИ».
В 1977 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина).
В 1989 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 80 научных публикаций.
Область научных интересов — методы цифровой обработки и анализа биомедицинских сигналов.

КОРШУНОВ
Геннадий
Иванович

Профессор кафедры инноватики и управления качеством Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1970 году окончил Ленинградский политехнический институт.
В 2002 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором 90 научных публикаций.
Область научных интересов — автоматизация и управление технологическими процессами, качество сложных систем, экологические системы.

КУБАЙЧУК
Александр
Борисович

Начальник отдела медицинских информационных систем Федерального государственного научного учреждения «Научно-исследовательский конструкторско-технологический институт биотехнических систем».
В 1994 году окончил Санкт-Петербургское высшее военное инженерное училище связи по специальности «Программное обеспечение вычислительной техники и автоматизированных систем».
Является автором восьми научных публикаций.
Область научных интересов — метауправление в сфере информационных технологий.

ЛАЗАРЕВ
Игорь
Владимирович

Студент пятого курса Санкт-Петербургского государственного университета аэрокосмического приборостроения, стипендиат Правительства Санкт-Петербурга.
Является автором четырех научных публикаций.
Область научных интересов — прикладная статистика.

МАРКОВСКИЙ
Станислав
Георгиевич

Старший преподаватель кафедры вычислительных машин и комплексов Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1986 году окончил Ленинградский институт авиационного приборостроения по специальности «Электронные вычислительные машины».
Является автором 26 научных публикаций.
Область научных интересов — протоколы случайного множественного доступа, нетрадиционные архитектуры компьютеров.

МАШКАНЦЕВ
Иван
Владимирович

Системный разработчик лаборатории «Интегрированные системы автоматизированного проектирования» Института проблем машиноведения РАН.
В 2004 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения по специальности «Системы автоматизированного проектирования».
Является автором четырех научных публикаций.
Область научных интересов — финансовые риски.

МОЛДОВЯН
Николай
Андреевич

Главный научный сотрудник научного филиала ФГУП НИИ «Вектор» — специализированного центра программных систем «Спектр». Заслуженный изобретатель Российской Федерации, профессор.
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.

ПЕРЕВАРЮХА
Андрей
Юрьевич

Аспирант Санкт-Петербургского института информатики и автоматизации РАН.
В 2004 году окончил Астраханский государственный технический университет по специальности «Автоматизированные системы обработки информации и управление».
Является автором одиннадцати научных публикаций.
Область научных интересов — применение нелинейных динамических моделей в математической биологии, математическая теория динамики популяций, проблемы хаоса и стабильности в экосистемах.

СОЛОЖЕНЦЕВ
Евгений
Дмитриевич

Заведующий лабораторией интегрированных интеллектуальных систем автоматизированного проектирования Института проблем машиноведения РАН, профессор кафедры информационных технологий в экономике Санкт-Петербургского государственного университета аэрокосмического приборостроения. Заслуженный деятель науки РФ.
В 1960 году окончил Харьковский политехнический институт.
В 1983 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 180 научных публикаций.
Область научных интересов — моделирование, анализ и управление риском на стадиях проектирования, испытаний и эксплуатации банковских, организационных, экономических и технических систем.

СОЛЬНИЦЕВ
Ремир
Иосифович

Профессор кафедры компьютерного проектирования информационно-измерительных систем Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1956 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина).
В 1970 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором 300 научных публикаций.
Область научных интересов — системы автоматизации проектирования, системы управления, экологические системы.

ТЮРЛИКОВ
Андрей
Михайлович

Доцент кафедры информационных систем Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1980 году окончил Ленинградский институт авиационного приборостроения по специальности «Информационные системы управления».
В 1986 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 60 научных публикаций.
Область научных интересов — многоабонентные системы связи, системы дистанционного обучения, протоколы передачи данных в реальном масштабе времени, алгоритмы сжатия видеоинформации.

ШАБАЛОВ
Александр
Александрович

Ассистент кафедры инноватики и управления качеством Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2005 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения.
Является автором шести научных публикаций.
Область научных интересов — системный анализ, моделирование систем.

ШОПЫРИН
Данил
Геннадиевич

Доцент кафедры компьютерных технологий Санкт-Петербургского государственного университета информационных технологий, механики и оптики.
В 2002 году окончил Оренбургский государственный университет.
В 2005 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором одиннадцати научных публикаций.
Область научных интересов — объектно-ориентированное и автоматное программирование.

ЮРЬЕВА
Ольга
Дмитриевна

Аспирант кафедры биомедицинской электроники и охраны среды Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В. И. Ульянова (Ленина).
В 2006 году окончила Санкт-Петербургский государственный электротехнический университет «ЛЭТИ».
Является автором пяти научных публикаций.
Область научных интересов — методы цифровой обработки и анализа биомедицинских сигналов.

УДК 629.78

Алгоритм распознавания конфигураций звезд

Воробьев С. Н., Лазарев И. В. Информационно-управляющие системы, 2008. № 2. С. 2–8.

Предлагается процедура распознавания звезд, основанная на сравнении наблюдаемой конфигурации звезд с множеством эталонных конфигураций, задаваемых по каталогу. Показано, что при произвольной ориентации искусственного спутника Земли алгоритм вычисления угловых расстояний между звездами конфигурации и ускоренного перебора эталонов реализуется в режиме реального времени и не требует больших объемов памяти.

Список лит.: 7 назв.

UDK 629.78

Algorithm of star configurations recognition

Vorobiev S. N., Lazarev I. V. IUS, 2008. N 2. P. 2–8.

Suggested is a star recognition procedure that is based on comparing the observed star configuration with a set of the standard configurations defined in a catalog. It is shown that star recognition by analyzing angles in an observed configuration and accelerated enumeration of predefined set of configurations can be processed in real time and does not have large memory requirements for an arbitrary oriented artificial satellite in space.

Refs: 7 titles.

УДК 629.075

Нелинейная динамическая модель системы запас-пополнение

Переварюха А. Ю. Информационно-управляющие системы, 2008. № 2. С. 9–14.

Исследуется динамическая система, основанная на модели запас-пополнение Рикера. Делается вывод об ограниченности применения известных дискретных моделей пополнения популяций. Предлагается модифицированная непрерывно-дискретная модель воспроизводства, качественно отличающаяся от модели Рикера.

Список лит.: 11 назв.

UDK 629.075

A non-linear dynamic model of the stock-recruitment system

Perevaryukha A. Yu. IUS, 2008. N 2. P. 9–14.

The author analyzes a dynamic system based on the stock-recruitment Ricker Map and makes some suggestions about restrictions in using well-known discrete maps of population recruitment. Also suggested is a modified hybrid model of reproduction qualitatively different from the Ricker Map.

Refs: 11 titles.

УДК 004.412; 004.413.5

Использование автоматизированной классификации изменений программного кода в управлении процессом разработки программного обеспечения

Князев Е. Г., Шопырин Д. Г. Информационно-управляющие системы, 2008. № 2. С. 15–21.

Описывается метод автоматизированной классификации изменений в контексте контроля развития программного кода, основанный на статистической кластеризации метрик изменений исходного кода. Показано применение автоматизированной классификации изменений для оптимизации процесса просмотра исходного кода и автоматизации контроля изменений на ответственных стадиях разработки. Приведен способ построения отчета по параметрам процесса разработки.

Список лит.: 20 назв.

UDK 004.412; 004.413.5

Using automatic classification of source code changes in software development process management

Knyazev E. G., Shopyrin D. G. IUS, 2008. N 2. P. 15–21.

Described is a method of using automatic source code changes classification aimed at control source code evolution. The method is based on statistical clustering of code change metrics. In this work, we show how automatic classification of code changes could be used for code review process optimization and for code changes control automation at final development stages. A development process of parameters report building is also shown.

Refs: 20 titles.

УДК 681.3

Протоколы коллективной подписи на основе свертки индивидуальных параметров

Ананьев М. Ю., Гортинская Л. В., Молдовян Н. А. Информационно-управляющие системы, 2008. № 2. С. 22–27.

Предлагается новый протокол коллективной подписи, устраняющий недостаток ранее известных протоколов такого типа, заключающийся в участии в протоколе доверенной стороны, которой передаются личные секретные ключи пользователей, подписывающих электронный документ.

Список лит.: 6 назв.

UDK 681.3

Collective digital signature protocols based on de-escalation of the individual parameters

Ananiev M. Yu., Gortinskaya L. V., Moldovyan N. A. IUS, 2008. N 2. P. 22–27.

The paper introduces a new collective digital signature protocol that is free of the shortcoming of the known protocols of this type, which consists in signers' disclosing their private keys to a trusted party participating in the protocol.

Refs: 6 titles.

УДК 004.728.3.057.4

Использование идентификаторов абонентов для резервирования канала множественного доступа

Марковский С. Г., Тюрликов А. М. Информационно-управляющие системы, 2008. № 2. С. 28–35.

Рассмотрены режимы передачи запросов, используемые в стандарте IEEE 802.16, для резервирования канала множественного доступа. Вводится способ передачи запросов с использованием идентификаторов абонентов. Показано, что предложенный способ позволяет уменьшить среднюю задержку передачи запроса и может быть реализован в рамках режима multicast polling стандарта IEEE 802.16.

Список лит.: 6 назв.

UDK 004.728.3.057.4

Using subscriber identifiers for multiple access channel reservation

Markovskij S. G., Tyurlikov A. M. IUS, 2008. N 2. P. 28–35.

Bandwidth request transmission for multiple access channel reservation in the IEEE 802.16 standard is discussed. A subscriber identifier-based method of request transmission is introduced. It is shown that this method allows for decreasing the average request transmission delay and may be implemented as part of the multicast polling scheme of the IEEE 802.16.

Refs: 6 titles.

УДК 551.46.08

Моделирование замкнутой системы управления «Природа-техногеника»

Сольницев Р. И., Коршунов Г. И., Шабалов А. А. Информационно-управляющие системы, 2008. № 2. С. 36–41.

Рассмотрены вопросы создания замкнутой системы управления «Природа-техногеника», предназначенной для эффективного снижения загрязняющих веществ, выбрасываемых промышленными предприятиями в атмосферу. Представлена математическая модель замкнутой системы управления и модели составляющих ее звеньев. Приведены результаты анализа системы на основе моделирования.

Список лит.: 6 назв.

UDK 551.46.08

Modeling the ‘nature-technogenic’ closed control system

Solnitsev R. I., Korshunov G. I., Shabalov A. A. IUS, 2008. N 2. P. 36–41.

Design issues of the ‘nature-technogenic’ closed control system used for efficient pollution decrease (dispersion into the atmosphere from the industrial enterprises) are discussed. A mathematical model of the closed control system, as well mathematical models of its components, are presented. Parametric parameter used for modeling are given, and analysis results on the base of modeling are presented.

Refs: 6 titles.

УДК 004.435 + 004.4’423

Структура медицинской информационной системы многопрофильного скрининга с унифицированным формальным представлением медицинского обеспечения

Кубайчук А. Б. Информационно-управляющие системы, 2008. № 2. С. 42–45.

Рассматривается класс адаптивных информационных систем и методика их построения. Предлагается типовая архитектура, многоуровневая модель представления метаинформации и описывается процедура адаптации для подобных систем. В качестве примера системы, разработанной по указанной методике, приводится информационная система многопрофильного скрининга.

Список лит.: 5 назв.

UDK 004.435 + 004.4’423

Structure of medical computer-based diagnostic screening systems with unified formal provision of medical care

Kubaychuk A. B. IUS, 2008. N 2. P. 42–45.

The class of adaptive information systems and their construction principles are discussed. The article suggests a typical architecture and multi level model of meta information presentation, as well as an adaptation process for such systems. The computer-based systems for diagnostic screening is proposed as an example of a system that has been developed using these principles.

Refs: 5 titles.

УДК 615.471:617.7

Влияние частоты дискретизации ЭКГ на точность вычисления спектральных параметров вариабельности сердечного ритма

Калиниченко А. Н., Юрьева О. Д. Информационно-управляющие системы, 2008. № 2. С. 46–49.

Представлены результаты экспериментальной оценки зависимости ошибки вычисления спектральных параметров вариабельности сердечного ритма от частоты дискретизации при использовании трёх различных методов определения опорной точки QRS-комплекса: по абсолютному максимуму, по равенству площадей под кривой и по равенству сумм квадратов модулей значений кривой, описывающей QRS-комплекс.

Список лит.: 5 назв.

УДК 519.862.6

Основы логико-вероятностной теории риска с группами несовместных событий

Машканцев И. В., Соложенцев Е. Д. Информационно-управляющие системы, 2008. № 2. С. 50–57.

Дается краткое описание основных положений логико-вероятностной теории риска с группами несовместных событий, ее приложений и особенностей для проблемы моделирования и анализа риска в сложных системах в областях управления и эконометрики. Описывается основная идея — введение в статистическую табличную базу данных групп несовместных событий или конечных множеств, что позволяет получить систему логических уравнений или базу знаний, использовать логико-вероятностное исчисление и решать задачи риска, эффективности и управления.

Список лит.: 5 назв.

UDK 615.471:617.7

Influence of the ECG sampling rate on the accuracy of heart rate variability spectral parameters estimation

Kalinichenko A. N., Yurieva O. D. IUS, 2008. N 2. P. 46–49.

The results of experimental estimation of the heart rate variability calculation error are presented. Three different methods are considered: one based on R-wave maximum, another using QRS area criterion, and one more with the use of QRS area square criterion.

Refs: 5 titles.

UDK 519.862.6

The basics of logical-and-probabilistic risk theory with groups of incompatible events

Mashkantsev I. V., Solozhentsev E. D. IUS, 2008. N 2. P. 50–57.

A brief description of basic statements of the logical-and-probabilistic risk theory with groups of incompatible events, its applications and its features in the context of the modeling problem and risk analysis in complex systems in the areas of management and econometrics is given. The main idea of the approach is introduction into the statistical data base groups of incompatible events or finite sets, that allows to receive the LP-equation system or the knowledge base, use the logical-and-probabilistic calculus, and resolve new tasks - risks, efficiency and management.

Refs: 5 titles.

Уважаемые авторы журнала «ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ»!

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». Статьи проходят обязательное рецензирование и публикуются бесплатно. Мы будем рады сотрудничеству с Вами и надеемся, что Вы порекомендуете библиотеке Вашей организации подписаться на наш журнал.

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, заглавие, инициалы и фамилия автора (авторов), ученая степень, звание, полное название организации, аннотация (5–7 строк) 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:

— отпечатанный (формат А4) текст статьи, подписанный всеми авторами с указанием даты предоставления, и иллюстрации, пронумерованные с подрисуночными подписями (в двух экземплярах);

— полностью совпадающий с распечаткой текст в виде файла Microsoft Word (шрифт Times New Roman, тексты программ — Courier New) на дискетах 1,44 Mb или CD;

— название статьи и аннотация (5–7 строк) на русском и английском языках;

— фамилия, имя, отчество автора (ов) на английском языке;

— 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 (при необходимости).

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.

Адрес редакции:
190000, Санкт-Петербург, Б. Морская ул., 67, ГУАП, РИЦ
Редакция журнала «Информационно-управляющие системы»
Факс: (812) 494 70 18
Тел.: (812) 494 70 36
E-mail: 80x@mail.ru
Сайт: www.i-us.ru