МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ,
МОЛОДЕЖИ И СПОРТА УКРАИНЫ

ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ РАДИОЭЛЕКТРОНИКИ

ISSN 0135-1710

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ И ПРИБОРЫ АВТОМАТИКИ

**Всеукраинский межведомственный
научно-технический сборник**

Основан в 1965 г.

Выпуск 156

Харьков
2011

УДК 62-50

В сборнике представлены результаты исследований, касающихся компьютерной инженерии, управления, технической диагностики, автоматизации проектирования, оптимизированного использования компьютерных сетей и создания интеллектуальных экспертных систем. Предложены новые подходы, алгоритмы и их программная реализация в области автоматического управления сложными системами, оригинальные информационные технологии в науке, образовании, медицине.

Для преподавателей университетов, научных работников, специалистов, аспирантов.

У збірнику наведено результати досліджень, що стосуються комп'ютерної інженерії, управління, технічної діагностики, автоматизації проектування, оптимізованого використання комп'ютерних мереж і створення інтелектуальних експертних систем. Запропоновано нові підходи, алгоритми та їх програмна реалізація в області автоматичного управління складними системами, оригінальні інформаційні технології в науці, освіті, медицині.

Для викладачів університетів, науковців, фахівців, аспірантів.

Свидетельство о государственной регистрации
печатного средства массовой информации КВ № 12073-944ПР от 07.12.2006 г.

Адрес редакционной коллегии: Украина, 61166, Харьков, просп. Ленина, 14, Харьковский национальный университет радиоэлектроники, комн. 321, тел. 70-21-326

СОДЕРЖАНИЕ

УДК 681.3.06

И.В. ЛИСИЦКАЯ

МЕТОДОЛОГИЯ ОЦЕНКИ СТОЙКОСТИ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

Излагается новый подход к оценке показателей доказуемой стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа, который основывается на результатах изучения свойств шифров как случайных подстановок. Для преодоления вычислительных трудностей, свойственных анализу показателей стойкости больших шифров, развивается методика, которая строится на результатах изучения свойств уменьшенных версий больших прототипов. В соответствии с этой методикой максимумы полных дифференциалов и линейных корпусов шифров могут быть получены расчетным путем из формул, выведенных для случайных подстановок. В отличие от известных результатов, связывающих показатели стойкости шифров с дифференциальными и линейными свойствами входящих в шифры нелинейных преобразований, делается вывод, что максимальные значения полных дифференциалов и линейных корпусов современных шифров не зависят (при достаточном числе цикловых преобразований) ни от свойств используемых в шифрах подстановочных конструкций, ни от методов введения в цикловые функции подключей, ни от способа построения расширяющего линейного преобразования, а являются функцией только размера битового входа в шифр (степени подстановки).

Введение

В последнее время появился ряд публикаций, в которых обсуждаются подходы к получению оценок доказуемой безопасности блочных симметричных шифров (БСШ) к атакам дифференциального и линейного криптоанализа [1-8 и др.].

Мы здесь не будем детально рассматривать сущность каждого из этих предложений, а приведем сразу итоговые выводы, следующие из анализа этих работ [9].

Первый вывод состоит в том, что в основе всех известных подходов к оценке показателей стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа лежит процедура определения максимумов средних значений дифференциальных вероятностей (MADP) и максимумов средних значений вероятностей линейных корпусов (MALHP).

Второй вывод заключается в том, что результирующие показатели стойкости шифров практически во всех работах связываются с соответствующими показателями, входящими в шифры S-блоковых конструкций.

Третий вывод состоит в том, что предлагаемые в отмеченных работах оценки доказуемой стойкости отличаются в значительных пределах.

Формулируется общий вывод о том, что существующая методика оценки показателей стойкости БСШ является все еще не совершенной. Более того, в работе будет показано, что известные подходы и их результаты не могут претендовать на объективность.

В данной статье мы хотим ещё раз высказать свою точку зрения по вопросу оценки безопасности БСШ, концептуально отличающуюся от известных, хотя в конечном итоге речь опять будет идти об определении максимальных значений полных дифференциалов и линейных корпусов (оболочек) БСШ. Основой здесь станут материалы нашей работы [9], дополненные уточнениями и разъяснениями.

1. Краткая сущность известных подходов к оценке стойкости и идеи, на которых строится новый подход

Прежде всего отметим, что все существующие подходы к оценке показателей стойкости БСШ опираются скорее на интуитивные соображения, подкрепленные результатами анализа под определенным углом зрения (субъективного) уменьшенных по числу циклов или упрощенных версий рассматриваемых БСШ.

И такой подход многим исследователям представляется вполне оправданным, так как полный анализ дифференциальных и линейных свойств современного шифра при реальной

длине битового размера входа является сегодня невыполнимой задачей. Собственно говоря, разработчики шифров и идут по пути увеличения размеров битового входа шифров именно для того, чтобы сделать задачу полного перебора ключей или текстов заведомо не реализуемой в обозримом будущем. Поэтому многие оценки показателей стойкости больших шифров строятся больше на основе накопленного опыта и некоторых соображений и оценок, позволяющих получить аргументы и данные для подтверждения предполагаемых высоких показателей стойкости предлагаемых решений. По этому же пути пошли и разработчики шифра Rijendael. Они действительно предложили достаточно прозрачную для понимания и анализа конструкцию шифрующего преобразования, строящуюся на реализации популярной теперь стратегии широкого следа и допускающую достаточно убедительное прогнозирование ожидаемых показателей стойкости.

Стремясь реализовать максимально возможные показатели преобразования по стойкости, они постарались использовать в своей конструкции и S-блоки с предельными дифференциальными и линейными показателями, даже допустив регулярность (алгебраичность) в построении нелинейных преобразований.

Интуиция их, правда, подвела при выборе конструкции S-блоков. Они посчитали, что показатели S-блоков оказывают решающее влияние на итоговые показатели стойкости шифра. На самом деле, как мы покажем, это не так и, соответственно, обоснованные ими показатели стойкости к атакам дифференциального и линейного криптоанализа несколько иные.

Излагаемые далее соображения и результаты строятся исходя из развиваемого нами нового подхода в теории и методах криптоанализа, ориентированного, с одной стороны, на использование при определении ожидаемых результатов стойкости больших шифров результатов анализа уменьшенных их версий, а с другой – на развитую на основе изучения свойств и показателей случайных подстановок и уменьшенных моделей шифров, рассматриваемых как подстановочные преобразования, концепцию (новую методологию) определения показателей стойкости БСШ к атакам дифференциального и линейного криптонализа.

Итак, для преодоления трудностей анализа полномасштабных моделей (алгоритмов) шифрования мы пошли по пути разработки и исследования уменьшенных моделей прототипов, для которых имеющихся вычислительных ресурсов оказывается уже вполне достаточно. Наши проработки показывают, что большое число хорошо известных алгоритмов шифрования допускают масштабирование. Удается во многих случаях построить уменьшенные модели, которые сохраняют (с учетом масштабирования) все свойства своих прототипов и позволяют решить многие задачи анализа и сравнения по показателям стойкости больших версий шифров [10-13 и др.].

Самый главный и неожиданный результат изучения уменьшенных моделей состоит в том, что общепринятая точка зрения, разрабатываемая во многих работах и состоящая в том, что линейные и дифференциальные свойства шифров непосредственно связаны со свойствами S-блоков, используемых при их построении, оказалась не верной или не совсем верной. На самом деле результирующие (т.е. получающиеся при использовании полного набора цикловых преобразований) показатели стойкости шифров определяются практически только размером битового входа в шифр.

Другой важный вывод, следующий из выполненных исследований, приводит к тому, что показатели стойкости больших (полных реализаций) шифров к атакам дифференциального и линейного криптоанализа (таких шифров, как Rijndael и многих других известных шифров, а также шифров Лабиринт, Калина, Мухомор, ADE [14-16], представленных на украинский конкурс по выбору национального стандарта шифрования) могут быть получены расчетным путем.

Этот вывод сделан на основе установленного в ходе исследований факта, что практически все известные шифры (большие и малые их версии) с увеличением числа циклов шифрования приходят к установившимся (стационарным) состояниям, свойственным случайным подстановкам соответствующей степени, для которых сегодня уже определены аналитические выражения для законов распределения переходов XOR таблиц и смещений таблиц линейных аппроксимаций. В результате появилась возможность найти максимумы интересующих нас распределений из формул путём расчётов (для шифров с операциями

введения цикловых подключей, отличными от XOR, необходимо рассматривать соответствующие таблицы для ключенезависимых переходов).

В работе обобщаются результаты по обоснованию предлагаемой методологии.

2. Понятийный аппарат линейного и дифференциального криптоанализа

Напомним кратко основной понятийный аппарат линейного и дифференциального криптоанализа. Следуя работе [17], введем ряд определений.

Определение 1 (Дифференциальная и Линейная вероятность). *Дифференциальная вероятность* DP^{f} *и линейная вероятность* LP^{f} *соответственно для ключезависимой функции* f *с* n*-битным входом* x *и* n*-битным выходом* y ($\mathrm{x}, \mathrm{y} \in \mathrm{GF}(2^{\mathrm{n}})$) *есть*

$$\mathrm{DP}^{\mathrm{f}}(\Delta \mathrm{x} \to \Delta \mathrm{y}) = \frac{\#\{\mathrm{x} \in \mathrm{GF}(2^{\mathrm{n}}) \mid \mathrm{f}(\mathrm{x}) \oplus \mathrm{f}(\mathrm{x} \oplus \Delta \mathrm{x}) = \Delta \mathrm{y}\}}{2^{\mathrm{n}}}, \tag{1}$$

$$\mathrm{LP}^{\mathrm{f}}(\Gamma \mathrm{y} \to \Gamma \mathrm{x}) = \left(\frac{\#\{\mathrm{x} \in \mathrm{GF}(2^{\mathrm{n}}) \mid \mathrm{x} \cdot \Gamma \mathrm{x} = \mathrm{f}(\mathrm{x}) \cdot \Gamma \mathrm{y}\}}{2^{\mathrm{n}-1}} - 1 \right)^2, \tag{2}$$

где Δx *и* Δy *являются входным и выходным различием* (*разностью*), *а* Γx и Γy – *входной и выходной масками*; x·Γx *обозначает результат побитного произведения* x и Γx.

Определение 2 ($\mathrm{DP}^{\mathrm{f}}_{\max}$ и $\mathrm{LP}^{\mathrm{f}}_{\max}$). *Максимальное значение дифференциальной и линейной вероятности для ключезависимой функции f определяется соответственно как*

$$\mathrm{DP}^{\mathrm{f}}_{\max} = \max_{\Delta \mathrm{x} \neq 0, \Delta \mathrm{y}} \mathrm{DP}^{\mathrm{f}}(\Delta \mathrm{x} \to \Delta \mathrm{y}),$$

$$\mathrm{LP}^{\mathrm{f}}_{\max} = \max_{\Gamma \mathrm{x}, \Gamma \mathrm{y} \neq 0} \mathrm{LP}^{\mathrm{f}}(\Gamma \mathrm{y} \to \Gamma \mathrm{x}).$$

Напомним также выражения для средних вероятностей ADP, ALHP, MADP и MALHP ключезависимой функции $f = f[k](x)$ с n-битным входом x и n-битным выходом y, $(\mathrm{x}, \mathrm{y} \in \mathrm{GF}(2^{\mathrm{n}}))$, параметризованной ключом k, используемых во многих публикациях по обоснованию показателей стойкости блочных шифров.

Определение 3. *Среднее значение дифференциальной вероятности* (ADP) *функции* f[k](x) *есть* $\mathrm{ADP}^{\mathrm{f}} = \operatorname{ave}_{\mathrm{k}} \mathrm{DP}^{\mathrm{f[k]}}(\Delta \mathrm{x} \to \Delta \mathrm{y})$.

Определение 4. *Среднее значение вероятности линейного корпуса* (ALHP*) функции* f[k](x) *есть* $\mathrm{ALHP}^{\mathrm{f}} = \operatorname{ave}_{\mathrm{k}} \mathrm{LP}^{\mathrm{f[k]}}(\Gamma \mathrm{x} \to \Gamma \mathrm{y})$.

Определение 5. *Максимум среднего значения дифференциальной вероятности* (MADP) *и максимум среднего значения вероятности линейного корпуса* (MALHP) *функции* f[k](x) *есть*

$$\mathrm{MADP}^{\mathrm{f}} = \max_{\Delta \mathrm{x} \neq 0, \Delta \mathrm{y}} \mathrm{ADP}^{f}(\Delta \mathrm{x} \to \Delta \mathrm{y}).$$

$$\mathrm{MALHP}^{\mathrm{f}} = \max_{\Gamma \mathrm{x}, \Gamma \mathrm{y} \neq 0} \mathrm{ALHP}^{\mathrm{f}}(\Gamma \mathrm{x} \to \Gamma \mathrm{y}).$$

В наших разработках [18 и др.] развивается новая точка зрения к формированию оценок стойкости БСШ к атакам дифференциального и линейного криптоанализа, которая формализуется как два новых метода (подхода).

Предлагается для оценки стойкости БСШ к атакам дифференциального и линейного криптоанализа пользоваться не MADP (максимумом средней дифференциальной вероятности) для некоторого фиксированного перехода входной разности Δx в выходную разность Δy, а средним (по множеству ключей) значением максимумов дифференциальных

вероятностей (AMDP) ключезависимой функции f[k](x), а для линейного криптоанализа - соответственно пользоваться не MALHP, а AMLHP.

Определение 6 (AMDP)**.** *Среднее* (*по множеству из* 2^h *ключей*) *значение максимальной дифференциальной вероятности ключезависимой функции* f[k](x) *есть*

$$\mathrm{AMDP}^f = \operatorname*{ave}_k \mathrm{DP}_{\max}^{f[k]} = \frac{1}{2^h}\sum_{k=1}^{2^h} \mathrm{DP}_{\max}^{f[k]}.$$

Определение 7 (AMPLH)**.** *Среднее* (*по множеству из* 2^h *ключей*) *значение максимальной вероятности линейных корпусов функции* f[k](x) *есть*

$$\mathrm{AMLHP}^f = \operatorname*{ave}_k \mathrm{LP}_{\max}^{f}(\Gamma x \to \Gamma y) = \frac{1}{2^h}\sum_{k=1}^{2^h} \mathrm{LP}_{\max}^{f[k]}.$$

В обоих случаях 2^h - мощность множества ключей зашифрования, использованных при вычислениях.

Можно также отметить, что очевидны неравенства:

$$\mathrm{MADP}^f < \mathrm{AMDP}^f,\ \mathrm{MALHP}^f < \mathrm{AMLHP}^f.$$

Помимо большей адекватности формируемых оценок их значения совпадают с соответствующими дифференциальными и линейными показателями случайных подстановок и характеризуют максимально достижимые значения дифференциальных и линейных вероятностей. В последнем случае обеспечиваются и значительные вычислительные преимущества (нет необходимости запоминать полностью все таблицы, а достаточно только определить и запомнить их максимальные значения).

Важным для дальнейшего является понятие случайной подстановки. Мы на нем остановимся отдельно.

3. Математическая модель случайных подстановок

Напомним, что ранее в нашей работе [19] понятие случайной подстановки было определено следующим образом.

Определение 8. *Под случайной понимается подстановка, которая удовлетворяет одновременно трем критериям случайности*:

Число инверсий h_n *в подстановке степени* n *приблизительно равно числу "антиинверсий", а практически*

$$\left|\eta_n - \frac{n(n-1)}{4}\right| \le a\sigma_\eta,\ \ \sigma_\eta = \frac{n^{3/2}}{6}.$$

Число циклов x_n *в подстановке степени* n *близко к* ln*n, а практически, находится в границах*

$$\left|\xi_n - \ln n\right| \le a\sigma_\xi,\quad \sigma_\xi = \sqrt{\ln n}.$$

Число возрастаний q_n *в подстановке степени* n *приблизительно равно числу убываний, а практически*

$$\left|\theta_n - \frac{n}{2}\right| \le a\sigma_\theta,\ \ \sigma_\theta = \sqrt{n/12}.$$

В этих соотношениях a – параметр, выбираемый в значительной степени из субъективных соображений (по крайней мере, из условия, что множество допустимых подстановок не станет меньше некоторого практически оправданного числа – использовались значения $a \le 1$).

В других наших публикациях [20,21], посвященных исследованию дифференциальных и линейных свойств случайных подстановок и подстановочных преобразований, развивающих результаты работ Luka O'Connor [22-24], мы определили еще два утверждения,

которые справедливы для случайных подстановок. Напомним здесь их, так как они являются важными для дальнейшего.

В обозначениях работ [20,22] пусть $\Pr(\Lambda_\pi(\Delta X,\Delta Y)=2k$ будет вероятностью того, что значение ячейки дифференциальной таблицы случайно взятой подстановки p порядка 2^n для перехода входной разности ΔX в соответствующую выходную разность ΔY будет равно 2k. Эта вероятность определяется теоремой.

Утверждение 1. *Для любых ненулевых фиксированных* ΔX, $\Delta Y \in Z_2^n$ *в предположении, что подстановка p выбрана равновероятно из множества* S_2^n *и* $0 \le k \le 2^{n-1}$,

$$\Pr(\Lambda(\Delta X,\Delta Y)=2k)=\binom{2^{n-1}}{k}^2 \cdot \frac{k!\cdot 2^k \cdot \Phi(2^{n-1}-k)}{2^n!}, \qquad (3)$$

где функция $\Phi(d)$ *определяется выражением*

$$\Phi(d)=\sum_{i=0}^{d}(-1)^i \cdot \binom{d}{i}^2 \cdot 2^i \cdot i!(2d-2i)!.$$

Закон распределения вероятностей (5) получен для полного множества подстановок, однако замечательным его свойством является то, что он оказывается справедливым и для усеченного (причем, существенно) множества подстановок, формируемых симметричными шифрами. Такие преобразования, осуществляемые на различных ключах зашифрования, формируют множество подстановок случайного типа. Об этом свидетельствуют многочисленные результаты экспериментов. И это еще не все! Оказывается, что закон распределения (5), полученный на основе анализа всего множества $2^n!$ равновероятных подстановок, является справедливым и для множества ячеек таблицы XOR разностей каждой отдельно взятой случайной подстановки степени 2^n.

Подтверждением этого факта является то, что для закона вероятностей $\Pr(\Lambda_\pi(\Delta X,\Delta Y)=2k$, рассматриваемого применительно к отдельной подстановке, с высокой точностью выполняется условие нормировки, характерное для полной группы событий:

$$\sum_{k=1}^{k^*}\Pr(\Lambda_\pi(\Delta X,\Delta Y)=2k)=1.$$

Здесь $\Lambda_\pi(\Delta X,\Delta Y)$ – значение XOR таблицы для пары значений разностей входов и выходов ΔX, $\Delta Y \in Z_2^n$: $\Delta X = X + X'$, $\Delta Y \in \pi(X)+\pi(X')$ подстановки $\pi \in S_2^n$. Значение k* представляет собой половину от максимального числа переходов XOR таблицы случайной подстановки.

Совершенно аналогичное по содержанию утверждение справедливо для вероятности смещений линейных аппроксимационных таблиц $LAT_\pi^*(\alpha,\beta)$ случайных подстановок [21,23].

Утверждение 2. *Пусть* $\lambda^*(\alpha,\beta)$ *будет случайным значением распределения* $LAT_\pi^*(\alpha,\beta)=\left|LAT_\pi(\alpha,\beta)-2^{n-1}\right|$, *когда подстановка p выбрана равновероятно из множества* 2^n *и маски* α,β *не нулевые. Тогда* $\lambda^*(\alpha,\beta)$ *принимает только четные значения и*

$$\Pr(\lambda^*(\alpha,\beta)=2k)=\frac{(2^{n-1}!)}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}+|k|}^2 \qquad (4)$$

для $|k| \le 2^{n-2}$.

Связь новых обозначений с представленными выше устанавливается равенством $LAT_\pi^*(\alpha,\beta)=LP^f(\Gamma y \to \Gamma x)$.

И для этого распределения справедлива нормировка

$$\sum_{k=0}^{k^*} \Pr\left(\lambda^*(\alpha,\beta) = 2k^*\right) = 1 .$$

Здесь k^* – половинное значение максимального для таблицы $LAT_\pi^*(\alpha,\beta)$ смещения.

На основе полученных результатов представляется логичным в дополнение к уже известным подходам сформировать (сформулировать) новое (или уточненное) определение случайной подстановки [25].

Определение 9. *Подстановка является случайной, если вместе с выполнением критериев случайности* 1-3 *для ячеек её XOR таблицы и таблицы линейных аппроксимаций выполняются законы распределения вероятностей* (3) (*критерий случайности* 4) *и* (4) (*критерий случайности* 5).

С использованием предложенных критериев случайности был выполнен достаточно широкий объём исследований по реализации конкретных значений критериев отбора случайных подстановок [25-27 и др.], подтвердивших практическую возможность реализации подстановочных преобразований с показателями, которые повторяют весьма близко распределения, следующие из теоретических результатов (имеющих комбинаторные, дифференциальные и линейные характеристики, полученные из теоретических расчётов).

Таким образом, приведенные определения и утверждения можно считать теоретической и практической базой для формирования понятия математической модели случайной подстановки.

4. Обоснование методологии оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа на основе моделей случайных подстановок

В основе развиваемого подхода лежит рассмотрение шифрующих преобразований как случайных подстановок.

Самый важный вывод работ [21, 23 и др.] состоит в том, что приведенные выше критерии случайности подстановок выполняются и для шифрующих преобразований всех современных блочных симметричных шифров, рассматриваемых как подстановочные преобразования.

Само по себе отдельное шифрующее преобразование (отдельный цикл) не является случайной подстановкой, так как для него не выполняются законы распределения вероятностей (3) и (4). Оно не укладывается в рамки случайных подстановок и по инверсиям, и по возрастаниям, и по циклам (хотя бы потому, что имеются множества входов в подстановку, которые влияют не на все значения выходов). Однако при реализации механизмов перемешивания (линейных преобразований), используемых в каждом цикле, последовательность шифрующих преобразований приобретает свойства случайной подстановки (к чему как раз и стремятся все разработчики шифров). Этот, казалось бы, тривиальный вывод остался не замеченным разработчиками шифров и криптоаналитиками при формировании оценок показателей стойкости шифров к атакам дифференциального и линейного криптоанализа (они не могли правильно интерпретировать результаты, так как были связаны полномасштабными версиями шифров, не поддающимися вычислительным экспериментам). Как уже отмечалось выше, во всех известных работах показатели многоцикловых преобразований (стойкость к атакам дифференциального и линейного криптоанализа) непосредственно связывались и связываются с соответствующими показателями S-блоковых конструкций, используемых в качестве нелинейных преобразований каждой цикловой функции.

Наша позиция состоит в том, что итоговые (асимптотические) показатели стойкости, максимумы полных дифференциалов таблицы XOR разностей последовательности шифрующих преобразований, также как и максимумы линейных аппроксимационных таблиц этих же преобразований, зависят только от числа циклов шифрующего преобразования и размера его битового входа.

Этот вывод зафиксирован в виде утверждения.

Утверждение 3. *Для каждого блочного симметричного шифра* (*из числа известных итеративных БСШ*) *существует вполне определенное число циклов, после которого шифр приобретает свойства случайной подстановки. Дальнейшее наращивание числа циклов не влияет на итоговые дифференциальные и линейные свойства шифра. Это значение является одним и тем же для всех шифрующих преобразований с одинаковым битовым размером входа.*

Это утверждение в первой части представляется в известном смысле достаточно очевидным (в том смысле, что каждый реальный шифр строится так, чтобы набор его цикловых преобразований в той или иной мере обладал свойствами случайной подстановки), при нашем подходе это свойство определяется как промежуточный результат, переходящий в асимптотическое значение, одинаковое для всех шифров (с одинаковым битовым размером входа), поддающийся расчету.

Выполним обоснование справедливости этого утверждения на примере рассмотрения дифференциальных показателей шифра-подстановки. В качестве одного из таких показателей в нашем случае будет выступать максимальное значение полного дифференциала.

Начнем доказательство приведенного утверждения (скорее не доказательство, а объяснение его правомерности) с конца, т.е. предположим, что БСШ имеет некоторое определенное число циклов, после которых шифр становится случайной подстановкой, т.е. обладает законом распределения вероятностей переходов разностей (3).

Покажем, что дальнейшее наращивание числа циклов не влияет на итоговые дифференциальные свойства этого шифра.

Важно сразу отметить, что особенностью случайной подстановки, удовлетворяющей критерию 4, является то, что мы имеем дело не с фиксированным распределением переходов наборов разностей $\Delta x \to \Delta y$ (закрепленным распределением значений входов (ячеек) таблицы XOR разностей), а со случайным. Таблица XOR разностей случайной подстановки определяется тем, что для нее являются фиксированными числа ячеек каждого типа, определяемых с помощью закона распределения $\Pr(\Lambda_f(\Delta x, \Delta y) = 2k$ в виде [21]

$$\Lambda_{m,2k} = (2^m - 1)^2 \cdot \Pr(\Lambda_f(\Delta x, \Delta y)) = \frac{(2^m - 1)^2}{2^m!} \begin{pmatrix} 2^{m-1} \\ k \end{pmatrix}^2 \cdot k! 2^k \cdot \Phi(2^{m-1} - k) \ . \qquad (5)$$

В соответствии с этим соотношением таблица XOR разностей случайной подстановки имеет λ_0 ячеек, имеющих значение $\Lambda_{m,0}$, λ_1 ячеек, имеющих значение $\Lambda_{m,2}$, λ_2 ячеек, имеющих значение $\Lambda_{m,4}$, и т.д., $\lambda_{k_f^*}$ ячеек, имеющих значение $\Lambda_{m,2k^*}$. Все эти значения вместе дают общее число ненулевых входов (ячеек) в подматрицу таблицы XOR разностей, равное $2^{n-1} \times 2^{n-1}$, причем сами числа $\lambda_0, \lambda_1, \lambda_2, \ldots, \lambda_{k_f^*}$ определяются однозначно из (5).

Поэтому применительно к шифрующим многоцикловым преобразованиям-случайным подстановкам дифференциальные вероятности DP^f должны теперь интерпретироваться в обозначениях подстановочных преобразований для ключезависимой функции *f* как

$$DP^f(\Delta x, \Delta y) = DP^f(\Delta x \to \Delta y) = \Pr(\Lambda_f(\Delta x, \Delta y) = 2k) \ ,$$

причем эти вероятности следует считать одинаковыми для всех ячеек таблицы дифференциальных разностей (для всех вариантов сочетаний входных и выходных разностей).

Возвратимся к нашей задаче. Итак, пусть r-цикловое шифрующее преобразование (последовательность r цикловых преобразований) f_r с n-битным размером входа (и выхода) обладает свойством 4, т.е. закон распределения $DP^{f_r}(\Delta x, \Delta y)$ переходов входных разностей Δx в выходные разности Δy имеет вид (3) с нормировкой

$$\sum_{k=0}^{k^*} DP^{f_r}(\Delta x, \Delta y) = 1 \ .$$

Тогда если на входы очередного циклового преобразования (подстановки) поступают некоторые сочетания пар выходов предшествующего преобразования случайного типа

(предшествующей случайной подстановки), подчиняющиеся закону распределения XOR разностей таблицы полных дифференциалов (3), то цикловое преобразование может осуществить лишь переименование выходов и соответствующих им разностей, оставляя результирующий закон распределения разностей неизменным (для операции XOR подстановка вместе с линейным цикловым преобразованием является детерминированным преобразованием и произведение случайной в оговоренном смысле подстановки на любую другую подстановку является случайной). Приведем математическое обоснование этого факта, который подтверждается многочисленными экспериментами с малыми шифрами.

Нас интересует закон распределения вероятностей $DP^{f_{r+1}}(\Delta x, \Delta z)$ для r + 1 цикла преобразований, где Δz является выходной разностью r + 1-го циклового преобразования. У нас имеется цепочка $\Delta x \to \Delta y \to \Delta z$ разностей, совместный закон распределения вероятностей для которой обозначим $DP^{f_{r+1}}(\Delta x, \Delta y, \Delta z) = DP^{f_{r+1}}(\Delta x \to \Delta y \to \Delta z)$. В соответствии с формулой умножения вероятностей можем записать представление для этой вероятности в виде

$$DP^{f_{r+1}}(\Delta x, \Delta y, \Delta z) = DP^{f_r}(\Delta x, \Delta y) DP^{f_1}(\Delta z / \Delta x, \Delta y).$$

И тогда дифференциальная вероятность $DP^{f_{r+1}}(\Delta x, \Delta z)$ для r + 1-го циклового преобразования может быть определена из совместной вероятности $DP^{f_{r+1}}(\Delta x, \Delta y, \Delta z)$ путем ее усреднения по множеству промежуточных значений $\Delta y \in Z_2^n$, т.е.

$$DP^{f_{r+1}}(\Delta x, \Delta z) = \sum_{\Delta y \in Z_{2^n}} DP^{f_r}(\Delta x, \Delta y) DP^{f_1}(\Delta z / \Delta x, \Delta y).$$

Но в нашем случае закон распределения $DP^{f_r}(\Delta x, \Delta y) = \Pr\left(\Lambda_f(\Delta x, \Delta y) = 2k\right)$ является одним и тем же для каждой выходной разности r-циклового преобразования (для каждой ячейки таблицы дифференциальных разностей случайной подстановки), поэтому

$$DP^{f_{r+1}}(\Delta x, \Delta z) = DP^{f_r}(\Delta x, \Delta y) \sum_{\Delta y \in Z_{2^n}} DP^{f_1}(\Delta z / \Delta x, \Delta y).$$

Очевидно далее, что при фиксированных значениях Δy выходные разности Δz не зависят от того, какие значения принимают входные разности Δx и, следовательно,

$$\sum_{\Delta y \in Z_{2^n}} DP^{f_1}(\Delta z / \Delta x, \Delta y) = \sum_{\Delta y \in Z_{2^n}} DP^{f_1}(\Delta z / \Delta y) = \sum_{\Delta y \in Z_{2^n}} DP^{f_1}(\Delta y \to \Delta z).$$

Но в соответствии с (5) для подстановочного одноциклового преобразования f_1

$$\sum_{\Delta y \in Y} DP^{f_1}(\Delta x, \Delta y) = \sum_{\Delta y \in Y} DP^{f_r}(\Delta x \to \Delta y) = 1,$$

и, в итоге, приходим к результату

$$DP^{f_{r+1}}(\Delta x, \Delta z) = DP^{f_r}(\Delta x, \Delta y) \Rightarrow DP^{f_{r+1}}(\Delta x \to \Delta z) = DP^{f_r}(\Delta x \to \Delta y),$$

где $DP^{f_r}(\Delta x \to \Delta y) = \Pr\left(\Lambda_f(\Delta x, \Delta y) = 2k\right)$.

Последнее и обозначает, что дополнительные цикловые преобразования уже не изменяют закона распределения разностей на выходе шифра.

Остановимся теперь на одном из принципиальных моментов рассматриваемого подхода – приходу шифров к стационарному состоянию, свойственному случайной подстановке. Здесь мы опять будем вести речь о дифференциальных характеристиках.

Заметим для начала, что для R-циклового шифра SPN структуры формирование результирующего закона распределения вероятностей переходов таблицы полных дифференциалов сводится к последовательному выполнению R однотипных (одноцикловых) преобразований (R итераций). Для иллюстрации процесса прихода шифров к стационарным состояниям в табл. 1 представлены результаты экспериментов с малыми их версиями. Значение

максимума таблиц разностей, равное 19-20, как раз соответствует показателю случайной подстановки. Представленные результаты свидетельствуют, что произведение одноцикловых преобразований после небольшого начального числа их повторений приобретает свойства случайной подстановки, соответствующей степени независимо от показателей случайности исходного одноциклового преобразования.

Таблица 1

Средние значения максимумов таблиц XOR разностей ($AMDPr2^{16}$) малых версий шифров вместе со среднеквадратическими отклонениями

Шифр / г	Шифр Хейса		Мини-AES	Мини-ADE	Мини-Лабиринт	Мини-Мухомор		Мини-Калина	
Число циклов	S-блок δ = 8	S-блок δ = 4	S-блок δ = 4	S-блок δ = 4	S-блок δ = 4	S-блок δ = 8	S-блок δ = 4	S-блок δ = 8	S-блок δ = 4
1	32768	16384	16384	16384	-	65536	65536	6082,56	3732,48
2	12288	4096	3036,16	3353,6	-	14187,5	5770,24	826,88	382,4
3	2326,81	439	274,24	307,2	37,5	2496,32	1802,24	24,8	19,36
4	216,803	56,964	19,326	20,54	19,04	542,72	125,53	19,04	19,14
5	65,38	26,18	19,02	19,08	19,24	46,28	29,7	19,14	19,2
6	24,108	19,108	18,812	19,24	19,04	19,48	18,88	19,14	19,36
7	19,021	19,086	18,87	19,00	19,14	19,47	18,87	19,27	18,73
8	19,16	19,1	19,27	18,93	19,24	19,33	19,27	19,02	19,00

В работе [9] мы не смогли привести теоретического обоснования утверждения 3 (была доказана только приведенная выше часть о том, что если шифр пришёл к стационарному состоянию, то дальнейшее наращивание числа циклов этого состояния не меняет). Поэтому здесь представляется дополнительное обоснование самого перехода шифра к стационарному состоянию.

Мы заинтересовались процессами, происходящими при последовательном выполнении подстановочных преобразований вообще, а не только шифрующих преобразований.

Были рассмотрены подстановки 256-й степени (байтовые подстановки). В табл. 2 представлены результаты вычислительного эксперимента по определению максимумов XOR таблиц последовательности (произведения) подстановочных преобразований для двух различных байтовых подстановок. Одна подстановка взята с показателем d-равномерности, равным 4, а вторая с показателем d-равномерности, равным 8. Видно, что обе подстановки уже на втором IциклеI приходят к максимуму дифференциала, равному 10-12, характерному для случайной подстановки степени 2^8 [20]. Интересно отметить, что результат не зависит от ключевых значений, если их ввести после каждого подстановочного преобразования.

Таблица 2

Распределение максимумов XOR таблиц последовательности подстановочных преобразований байтовой подстановки

Число циклов (повторов)	1	2	3	4	5	6	7	8	9	10	11
Значение максимума XOR таблицы для AES S-блока	4	12	12	10	12	12	10	12	12	12	12
Значение максимума XOR таблицы для S-блока Мухомор	8	10	10	12	10	14	12	12	10	12	12

Конечно, по законам комбинаторики этот процесс должен быть периодическим, но для интересующих нас значений мы, как правило, оказываемся очень далеко от циклового периода подстановки.

Таким образом, действительно произведение (последовательность) подстановочных преобразований нетривиального типа (а не только шифров) является с большой вероятностью случайной подстановкой, независимо от свойств подстановки, участвующей в формировании этого преобразования.

Мы посчитали, что это и приведенное выше утверждение является неким “законом природы”, который выполняется независимо от нашего желания (может, здесь надо было бы более строго оговорить, какие подстановки удовлетворяют этому правилу, но это предмет отдельного исследования).

Подобным же образом к стационарному распределению, свойственному случайной подстановке, приходит и любой шифр. Переход к стационарному распределению как раз соответствует тому моменту, с которого шифр начинает повторять свойства случайной подстановки.

А вот тот факт, что произведение подстановок (и без случайной компоненты), как и последовательность шифрующих преобразований с нулевыми цикловыми подключами, становится случайной подстановкой, оказался всё же неожиданным. Объяснением этому факту может быть лишь то, что сами по себе подстановки (исключая тривиальные их конструкции), как правило, представляют собой набор случайных переходов (уже в самой подстановке заложен механизм случайного перемешивания) и именно этим определяется важнейшая роль подстановочных преобразований в шифрах.

Аналогичные аргументы могут быть приведены по отношению к линейным показателям многоцикловых итеративных процедур шифрования.

В результате мы приходим к тому, что утверждение 3 оказывается справедливым практически для всех современных блочных симметричных шифров. Но раз так, то для оценки показателей доказуемой стойкости этих шифров можно воспользоваться расчётными соотношениями, справедливыми для математических моделей случайных подстановок. Приведём их далее.

5. Расчетные соотношения для определения показателей стойкости шифров к атакам дифференциального и линейного криптонализа

Расчетные соотношения для определения максимальных значений полных дифференциалов и максимальных значений линейных корпусов могут быть получены применением законов (3) и (4), справедливых для случайных подстановок, к шифрам, рассматриваемым как случайные подстановки, что и сделано в работах [20] и [21].

Как показано в [20], среднее значение максимума таблицы дифференциальных разностей случайной подстановки порядка 2^n находится путем определения максимального значения $k = k_{max}$, при котором выполняется соотношение

$$\frac{(2^n-1)^2}{2^n!}\cdot\binom{2^{n-1}}{k}^2\cdot k!2^k\cdot\Phi(2^{n-1}-k)\approx 1. \qquad (6)$$

Если это соотношение применить к шифру с n-битовым размером входа, то для интересующего нас максимального значения дифференциальной вероятности (максимальной вероятности полного дифференциала) DP^f_{max} можем записать выражение

$$DP^f_{max}=\frac{k_{max}}{2^n}. \qquad (7)$$

В работе [20] также приведено расчетное соотношение, являющееся хорошей аппроксимацией соотношений (6) и (7):

$$DL^f_{max}=\frac{n+4}{2^n}.$$

В [21] показано, что среднее значение максимума таблицы линейных аппроксимаций для случайной подстановки определяется аналогично предыдущему случаю путем нахождения значения k^*, являющегося целым решением уравнения

$$\frac{(2^n-1)^2\cdot\left(2^{n-1}!\right)^2}{2^n!}\cdot\binom{2^{n-1}}{2^{n-2}+|k^*|}^2=1. \qquad (8)$$

Соответственно для шифра с n-битовым размером входа максимальное значение линейной вероятности (максимальной вероятности линейного корпуса) DL^{f}_{max} представляется в виде

$$DL^{f}_{max} = \left(\frac{k_{max}}{2^{n-1}} \right)^2 .$$

Приведем здесь также соотношение, полученное на основе обработки результатов вычислительных экспериментов, являющееся удобной заменой выполнению расчетов по соотношению (8):

$$DL^{f}_{max} = \left(\frac{\left(\frac{3}{2} \right)^2}{2^{n-1}} \right)^2$$

Выводы

На основе накопленных результатов и обоснований можно утверждать следующее.

1. Современные блочные симметричные шифры при полном наборе шифрующих многоцикловых преобразований обладают свойствами случайных подстановок, т.е. для них справедливы законы распределения вероятностей для комбинаторных показателей (инверсий, возрастаний и циклов), а также законы распределения вероятностей полных дифференциалов и линейных корпусов, свойственные случайным подстановкам соответствующей степени.

2. Максимальные значения полных дифференциалов и линейных корпусов блочных симметричных шифров, определяющие по современным меркам показатели их доказуемой стойкости к атакам дифференциального и линейного криптоанализа, могут быть получены расчетным путем. Они не зависят (при достаточном числе цикловых преобразований) ни от свойств используемых в шифрах подстановочных конструкций, ни от методов введения в цикловые функции цикловых подключей, ни от способа построения расширяющего линейного преобразования цикловой функции, а являются функцией только размера битового входа в шифр.

3. Впервые предложена и обоснована методология оценки стойкости блочных симметричных шифров к атакам линейного и дифференциального криптоанализа, которая предусматривает использование для формирования выводов относительно уровня доказуемой безопасности шифров показателей их уменьшенных моделей, что позволило существенно ускорить процесс выполнения экспертизы и сравнения решений по построению алгоритмов блочного симметричного шифрования.

4. Впервые установлен принцип определения максимумов дифференциальной и линейной вероятностей современных БСШ на основе использования показателей случайных подстановок соответствующей степени, не связанный с показателями нелинейных преобразований (S-блоков) шифров, что позволило значительно упростить процесс нахождения показателей доказуемой безопасности шифров к атакам линейного и дифференциального криптоанализа.

Список литературы: **1.** *Thomas Baignoires and Serge Vaudenay*. Proving the Security of AES Substitution-Permutation Network. http://lasecwww.epfl.ch. 2004. p. 16. **2.** *Liam Keliher.* Toward Provable Security Against Differential and Linear Cryptanalysis for Camellia and Related Ciphers, International Journal of Network Security. Vol.5, No.2. P.167–175, Sept. 2007. **3.** *L. Keliher, H. Meier, and S. Tavares.* New method for upper bounding the maximum average linear hull prodadility for SPNs, Advances in Cryptology - EUROCRYPT 2001, LNCS 2045, Springer-Verlag. 2001. P. 420-436. **4.** *L. Keliher, H. Meijer, and S. Tavares*, Improving the upper bound on the maximum average linear hull probability for Rijndael, Eighth Annual International Workshop on Selected Areas in Cryptography (SAC 2001), LNCS 2259, pp. 112-128, Springer-Verlag, 2001. **5.** *Алексийчук А.Н.* Оценки практической стойкости блочного шифра ІКалинаІ относительно методов разностного, линейного криптоанализа и относительно алгебраических атак, основанных на гомоморфизмах / А.Н. Алексийчук, Л.В. Ковальчук, Е.В. Скрыпник, А.С. Шевцов // Прикладная радиоэлектроника. 2008. Т.7, №3. С. 203-209. **6.** Final report of European project number IST-1999-12324, named New

European Schemes for Signatures, Integrity, and Encryption, April 19, 2004. Version 0.15 (beta), Springer-Verlag. **7.** *K. Nyberg and L. Knudsen*, Provable security against differential cryptanalysis, Journal of Cruptology. 1995.Vol.8. No.1. **8.** *M. Matsui*. On a Structure of Block Ciphers with Provable Security against Differential and Lintar Cryptanalysis. IEICE TRANS. FUNDAMENTALS, Vol. E82-A, NO. 1 JANUARY 1999. P. 117-122. **9.** *Горбенко І.Д.* Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / Горбенко І.Д., Долгов В.И., Лисицкая И.В., Олейников Р.В. // Прикладная радиоэлектроника. 2010. Т. 9, № 3. С. 312-320. **10.** *Лисицкая И.В.* Криптографические свойства уменьшенной версии шифра IМухоморI. / И.В. Лисицкая, О.И. Олешко, С.Н. Руденко, Е.В. Дроботько, А.В. Григорьев // Спеціальні телекомунікаційні системи та захист інформації. Збірник наукових праць. Київ, 2010. Вип. 2(18). С. 33-42. **11.** *Кузнецов А.А.* Линейные свойства блочных симметричных шифров, представленных на украинский конкурс / А.А. Кузнецов, И.В. Лисицкая, С.А. Исаев // Прикладная радиоэлектроника. 2011. Т.10, №2. С. 135-140.**12.** *Долгов В.И.* Криптографические свойства уменьшенной версии шифра "Калина" / В.И. Долгов, Р.В. Олейников, А.Ю. Большаков, А.В. Григорьев, Е.В. Дробатько // Прикладная радиоэлектроника. 2010. Т.9, № 3. С. 349-354.**13.** *Головашич С.А.* Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Прикладная радиоэлектроника. Харьков: ХТУРЭ. 2007. Том. 6, №2, С. 230-240. **14.** *Горбенко І.Д.* Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація / І.Д. Горбенко, М.Ф. Бондаренко, В.І. Долгов, Р.В. Олійников, В.І. Руженцев, М.С. Михайленко , Ю.І. Горбенко, О.І. Олешко, С.В. Казьміна // Прикладная радиоэлектроника. Харьков: ХТУРЭ. 2007. Том. 6, №2. С. 147-157. **15.** *Горбенко І. Д.* Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікації / І.Д. Горбенко, В.І. Долгов, Р.В. Олейніков, В.І. Руженцев, М.С. Михайленко, Ю.І. Горбенко, О.С. Тоцкій, С.В. Казьміна // Прикладная радиоэлектроника. 2007. Т.6, № 2. С. 195-208. **16.** *Кузнецов А.А.* Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) / А.А. Кузнецов, Р.В. Сергиенко, А.А. Наумко // Прикладная радиоэлектроника. 2007. Том 6, №2. С. 241-249. **17.** *F. Sano, K. Ohkuma, H. Chimisu, and S. Rawamura.* On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis, IEISE Trans. Fundamentals. Janiary 2003.Vol. E86-A. No.1. P. 37-46. **18.** *Долгов В.И.* Новая методика оценки двухциклового дифференциала уменьшенной версии супер блока AES. / В.И. Долгов, И.В. Лисицкая, В. А. Феськов, К.Е. Лисицкий // Сборник трудов Второй Международной научно-технической конференции IКомпьютерные науки и технологииI, 8-10 октября, Белгород. 2011. С. 418-422.**19.** *Горбенко И.Д.* Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 28147-89 / Горбенко И.Д., Лисицкая И.В. // Радиотехника. 1997. Вып 103. С. 121-130. **20.** *Олейников Р.В.* Дифференциальные свойства подстановок / Р.В. Олейников, О.И. Олешко, К.Е. Лисицкий, А.Д. Тевяшев // Прикладная радиоэлектроника. 2010. Т.9, № 3. С. 326-333. **21.** *Долгов В.И.* Свойства таблиц линейных аппроксимаций случайных подстановок / В.И. Долгов, И.В. Лисицкая, О.И. Олешко / / Прикладная радиоэлектроника. Харьков: ХНУРЭ. 2010. Т. 9, № 3. С. 334-340. **22.** *L. J. O'Connor*. On the Distribution of Characteristics in Bijective Mappings. Advances in Cryptology. EUROCRIPT 93, Lecture Notes in Computer Science, vol. 795, T. Helleseth ed., Springer-Verlag, pages 360-370, 1994. **23.** *Luke O'Connor*. Properties of Linear Approximation Tables. Email: oconnor@dsts. Edu. au, 1995. **24.** *Luke O'Connor*. On Linear Approximation Tables and Ciphers secure against Linear Cryptanalysis. Email: oconnor@dsts. Edu. au, 1995. **25.** *Долгов В.И.* Случайные подстановки в криптографии / В.И. Долгов, И.В. Лисицкая, К.Е. Лисицкий // Радіоелектронні та комп'ютерні системи. 2010. № 5 (46). С. 79-85. **26.** *Лисицкая И.В.* Экспериментальная проверка работоспособности новых критериев отбора случайных подстановок / И.В. Лисицкая, К.Е. Лисицкий, А.В. Широков, Е.Д. Мельничук // Радіоелектронні та комп'ютерні системи. 2010. № 6 (47). С. 87-93. **27.** *Лисицкая И.В.* Оценка числа случайных подстановок с заданным распределением парных разностей XOR таблиц и смещений таблиц линейных аппроксимаций / И.В. Лисицкая, А.В. Широков, Е.Д. Мельничук, К.Е. Лисицкий // Прикладная радиоэлектроника. Харьков: ХНУРЭ. 2010. Т. 9, № 3. С. 341-345.

Поступила в редколлегию 10.09.2011

Лисицкая Ирина Викторовна, канд. техн. наук, доцент кафедры БИТ ХНУРЭ. Научные интересы: защита информации, методы криптоанализа блочных шифров. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 340-84-60.

УДК 621.315.592

А.П. ОКСАНИЧ, И.В. ШЕВЧЕНКО, Ю.А. КРАСНОПОЛЬСКАЯ

ВИРТУАЛЬНЫЙ ДАТЧИК ДЛЯ МОНИТОРИНГА ТЕМПЕРАТУРЫ ФОНОВОГО НАГРЕВАТЕЛЯ В ТЕПЛОВОМ УЗЛЕ УСТАНОВКИ ДЛЯ ВЫРАЩИВАНИЯ МОНОКРИСТАЛЛОВ АРСЕНИДА ГАЛЛИЯ

Разрабатывается математическая модель – виртуальный датчик температуры фонового нагревателя, используемого для формирования оптимальных тепловых условий в зоне, примыкающей к фронту кристаллизации при выращивании слитков полуизолирующего GaAs по LEC-технологии. Выполняется проверка адекватности модели в ходе экспериментов на различных стадиях процесса выращивания. Модель используется как составная часть информационной технологии мониторинга качества процесса выращивания монокристаллов полупроводников.

1. Введение

Выращивание монокристаллов GaAs по LEC-технологии является сложным, многофакторным процессом, и для обеспечения выполнения требований к структурному совершенству и другим параметрам кристаллов требует применения эффективных технологий контроля и управления. Существующие системы контроля параметров процесса выращивания используют прямые измерения температуры основного нагревателя, потребляемой фоновым нагревателем (ФН) мощности, скорости вращения кристалла и тигля, а также косвенные измерения уровня расплава в тигле и диаметра слитка [1]. Однако для мастера-технолога важным является температура фонового нагревателя, которая во многом определяет температурные градиенты в зоне кристаллизации. Измерять температуру ФН и определять параметры температурного поля в расплаве путем прямых измерений при помощи термопар допустимо только в ходе специально поставленных экспериментов, связанных с научно-техническими исследованиями. Это обусловлено тем, что согласно методу Чохральского слиток, вращаясь, вытягивается из расплава, который в свою очередь находится во вращающемся тигле. Расплав имеет температуру более 1000°C. Во время вытягивания монокристалла постоянно держать в расплаве какой либо датчик температуры практически невозможно. Температуру расплава на его поверхности в принципе можно определять косвенным методом, например пирометрическим. Однако при выращивании монокристаллов арсенида галлия над расплавом располагается слой герметизатора (Ba_2O_3), который, имея низкую теплопроводность, искажает результаты пирометрических измерений. Таким образом, мастер-технолог вынужден субъективно оценивать температуру ФН, ориентируясь на значение потребляемой мощности и свой опыт.

Реализовать косвенные измерения температуры ФН и вычислять температурные градиенты в зоне кристаллизации можно, используя специальные методики и комплекс предназначенных для этого математических моделей, которые служат виртуальными датчиками параметров теплового поля. Основным компонентом в этом комплексе является численная модель расчета температурного поля в расплаве и слитке на основе метода конечных разностей. Вспомогательные модели, построенные на основе нейронных сетей и нечетких клеточных автоматов, позволяют повысить адекватность результатов расчета температурного поля [2, 3].

Поскольку при выращивании монокристаллов полуизолирующего GaAs используется фоновый нагреватель, помещенный в слой герметизатора, в упомянутый комплекс моделей необходимо включать и виртуальный датчик измерения температуры фонового нагревателя, как источника теплоты в расчетной сетке метода конечных разностей. Кроме того, постоянный контроль температуры фонового нагревателя представляет отдельную проблему, связанную с необходимостью оптимизации значения его температуры на разных этапах процесса выращивания в автоматизированной системе управления качеством процесса выращивания.

Целью данного исследования является разработка математической модели – виртуального датчика температуры ФН и усовершенствование функциональной модели системы "Советчик мастера", использующей информационную технологию виртуального мониторинга параметров процесса выращивания монокристаллов GaAs по LEC-технологии.

2. Постановка задачи и её связь с научными проблемами

Регулировать отток тепла от боковой поверхности слитка в районе фронта кристаллизации и тем самым влиять на радиальные температурные градиенты можно путем регулирования температуры (мощности) дополнительного (фонового) нагревателя, размещенного в слое герметизатора [4, 5] (рис. 1). Конструкция фонового нагревателя выбрана таким образом, чтобы обеспечить локальное воздействие на поверхность расплава в области формирования растущего слитка и создание температур на нагревателе от 800 до 1300°С. Следует сказать, что технологические условия выращивания, обеспечивающие получение монокристаллов с требуемой плотностью дислокаций $N \leq 5Ч10^3 см^{-2}$, являются весьма жесткими. Например, повышение температуры ФН свыше 1200°С приводит к сильному поверхностному разложению монокристалла и срыву монокристаллического роста. Снижение температуры ФН ниже 850°С незамедлительно сказывается на возрастающей плотности дислокаций. Уменьшение скорости подъема затравки также приводит к сильному поверхностному разложению кристалла, а увеличение скорости подъема приводит к ухудшению монокристаллического роста и двойникованию. Такая жесткость требует корректировки теплового режима у фронта кристаллизации в процессе выращивания и непрерывного контроля температуры ФН.

Поскольку условия теплоотдачи от ФН в окружающую среду в процессе выращивания меняются из-за изменения расположения деталей теплового узла, непосредственное вычисление температуры ФН по потребляемой мощности при помощи простой линейной аппроксимации не дает адекватного результата. Методика косвенного измерения температуры ФН и соответствующая математическая модель должны учитывать эти особенности. Наиболее подходящим для построения адекватной математической модели косвенного измерения температуры ФН следует признать регрессионный метод.

Таким образом, для разработки адекватной математической модели и методики измерения, пригодной для косвенного измерения температуры ФН на разных стадиях выращивания, необходимо решить следующие задачи:

1. Выделить факторы, по мнению экспертов влияющие на температуру ФН.
2. Сформировать стратегию и план эксперимента и провести все необходимые опыты.
3. Проверить результаты на воспроизводимость.
4. Определить коэффициенты регрессионного уравнения.
5. Оценить значимость коэффициентов.
6. Проверить адекватность модели.
7. Сформировать методику косвенных измерений температуры ФН.

3. Эксперименты и результаты

Прежде всего, определим факторы, влияющие на изменение температуры ФН, и обсудим на качественном уровне влияние и взаимосвязь этих факторов. Эта предварительная работа заметно упрощает дальнейшие действия исследователя.

Главным фактором, несомненно, является потребляемая ФН электрическая мощность, значение которой вычисляется по известному напряжению питания и потребляемому постоянному току.

К другим рассматриваемым факторам относятся температура основного нагревателя (ОН), теплопроводность герметизатора, конвекция в расплаве и в среде над слоем герметизатора, скорость вращения затравки и тигля, уровень расплава в тигле, скорость вытягивания затравки.

Считаем электрическую мощность ФН независимым фактором, так как потребляемый нагревателем ток и напряжение питания поддерживаются на заданном уровне вне зависимости от других рассматриваемых факторов.

Температура ОН косвенно влияет на температуру ФН, создавая основное тепловое поле. Чем выше температура ОН, тем выше (при прочих равных условиях) температура в

зоне расположения ФН, меньше теплоотдача самого ФН и выше его температура. Считаем температуру ОН фактором, который не зависит от других перечисленных выше факторов.

Для расчета температуры ФН нужно также определить факторы, влияющие на теплоотдачу с поверхности герметизатора в окружающую среду. К этим факторам относятся:

– теплопроводность герметизатора (примем её постоянной, так как диапазон температур, в которых производится эксперимент, небольшой);

– теплообмен поверхности герметизатора с окружающей средой за счет излучения;

– конвективный теплообмен поверхности герметизатора с окружающей средой.

Тепловой поток с единицы поверхности герметизатора можно представить в виде трех слагаемых:

$$q_{\text{пгі}} = \sigma\varepsilon_i T_i^4 + p_i H_i + \alpha(T_i - T_{\text{ср}}), \qquad (1)$$

где σ – постоянная Больцмана; ε_i – коэффициент излучения с единичной i-й поверхности герметизатора; Ti – температура единичной i-й поверхности герметизатора; p_i – отражательная способность единичной поверхности; H_i – внешний теплопоток на единичную поверхность от поверхностей теплового узла и слитка; α – коэффициент конвективной теплоотдачи; $T_{\text{ср}}$ – температура среды над герметизатором.

Рассмотрим на качественном уровне изменения составляющих этого теплового потока в течение процесса выращивания. Измерения показали, что распределение температуры по высоте стенки тигля практически линейно и её максимум наблюдается в верхней рабочей области, примыкающей к поверхности расплава в начале процесса выращивания. Перегрев по сравнению с температурой кристаллизации составляет $\approx 45°C$. Для сохранения неизменными тепловых условий на уровне фронта кристаллизации в течение всего процесса вытягивания тигель, по мере опускания уровня расплава, перемешается вверх. Фоновый нагреватель при этом перемещается вглубь тигля, чтобы расстояние между его нижней кромкой и уровнем расплава оставалось неизменным. Однако при этом изменяются условия лучистого теплообмена поверхности герметизатора со стенкой тигля, так как площади слитка и внутренней поверхности тигля, участвующие в теплообмене излучением, увеличиваются. Это приводит к изменению второго слагаемого в выражении (1), т.е. к изменению условий теплоотдачи с поверхности герметизатора.

По мере заглубления ФН и герметизатора в тигель величина $T_{\text{ср}}$ растет. Таким образом, конвективный тепловой поток уменьшается, что служит еще одним подтверждением того, что фактор “уровень расплава” является качественно значимым и его влияние следует оценить количественно.

Рассмотрим тепловой эффект, возникающий при увеличении скорости подъема затравки. Увеличение этой скорости приводит к мгновенному возрастанию объемной скорости кристаллизации. Выделяющаяся на фронте кристаллизации скрытая теплота плавления не будет успевать “уходить теплопроводностью” через кристалл. Поэтому она в основном будет рассеиваться в примыкающем столбике расплава, температура в нем повысится, а это повлечет за собой уменьшение теплоотдачи ФН и снижение его температуры.

Вращение затравки и тигля создаёт вынужденную конвекцию в слое герметизатора и дополнительный отток тепла от ФН. Поскольку ФН имеет кольцевую форму, то заметный отток теплоты могут создать только радиальные токи в слое герметизатора. Если учесть, что толщина этого слоя составляет не более 20 мм, а плотность герметизатора мала по сравнению с плотностью расплава, то становится ясно, что радиальные токи незначительны. Тем не менее, влияние скорости вращения затравки и тигля с нашей точки зрения было необходимо исследовать, чтобы априори не ухудшить адекватности модели. Естественная конвекция в слое герметизатора мала из-за его малой глубины и ею можно пренебречь. Следует также учесть, что коэффициент теплопроводности герметизатора (0,02 Вт/смК) в семь раз ниже теплопроводности расплава GaAs (0,14 Вт/смК), что уменьшает кондуктивную тепловую связь между ФН и примыкающим к герметизатору слоем расплава.

Таким образом, можно составить перечень варьируемых факторов, которые следует учесть в модели вычисления температуры ФН: X1 – потребляемая мощность ФН; X2 – температура ОН; X3 – скорость вытягивания; X4 – скорость вращения затравки; X5 – скорость вращения тигля; X6 – уровень расплава.

В табл. 1 приведены обозначения, названия и уровни перечисленных факторов.

Таблица 1

Перечень и уровни изменения факторов

	Факторы	Уровни действия факторов				
		1	2	3	4	5
1	Мощность, потребляемая ФН, Вт	1500	2300	–	–	–
2	Температура основного нагревателя, °С	1100	1300	–	–	–
3	Скорость вытягивания, мм/мин	0,07	0,14	–	–	–
4	Скорость вращения затравки, об/мин	10	20	–	–	–
5	Скорость вращения тигля, об/мин	5	10	–	–	–
6	Уровень расплава, %	100	80	60	40	20

Уровни факторов нумеровались и кодировались в соответствии с общепринятой практикой по формуле:

$$x_j = \frac{\tilde{x}_j - \tilde{x}_{0j}}{\Delta\tilde{x}_j},$$

где x_j – кодированные значения факторов; $\tilde{x}_j$ – натуральные значения факторов на верхнем, основном и нижнем уровнях; $\vec{x}_{oj}$ – натуральные значения факторов на основном уровне; $\Delta\tilde{x}_j$ – натуральное значение интервалов варьирования факторов; j – номер фактора.

Для натурного исследования влияния перечисленных факторов на температуру фонового нагревателя был составлен предварительный план эксперимента, структура которого показана в табл. 2, где указаны номера уровней.

Специфика экспериментов на ростовой установке заключается в следующем:

1. Каждый эксперимент по измерению температуры ФН, температуры в отдельных точках расплава и окружающей слиток среды требует неоднократного механического вмешательства в сложный процесс роста монокристалла и, как правило, приводит к ухудшению его качества, т.е. к значительным материальным потерям. Поэтому количество экспериментов на ростовой установке приходится ограничивать.

2. Смена уровней факторов X1 и X2 предполагает выдержку времени, в течение которой затухает переходный процесс и устанавливается новый тепловой режим. Учитывая тот факт, что фактор X6 (уровень расплава) является динамическим, строгая фиксация его уровня предполагает, что факторы X1 и X2 должны быть изменены заблаговременно.

3. Процесс выращивания является необратимым во времени и, следовательно, при планировании эксперимента приходится это учитывать. А именно – во время вытягивания кристалла уровень расплава в тигле (фактор X6) последовательно проходит все указанные в табл. 1 ступени, и изменить их порядок невозможно.

Все эти условия определили стратегию проводимых экспериментов. Были проведены 7 процессов выращивания, в которых исследуемые факторы X1...X5 изменялись так, чтобы строки табл. 2 чередовались случайным образом, но без нарушения чередования уровней фактора X6. Для всех точек плана проводились параллельные измерения в одинаковом количестве k = 3. Таким образом, общее число опытов, результаты которых легли в основу многофакторного анализа, составило 105. Для проверки адекватности модели впоследствии были проведены дополнительные эксперименты.

Для измерения температуры ФН и окружающих его элементов использовали алундированные микротермопары ТПР (тип В) диаметром 100 мкм, спаи их вваривали в кварцевые чехлы, которые, в свою очередь, крепили к специальному кронштейну. С помощью специального координатного устройства осуществляли перемещение термопар как вдоль поверхности герметизатора и расплава, так и под поверхностью на стадиях разращивания, вытягивания цилиндрической части и сведения слитка на конус в конце процесса. Погрешность измерения составляла ±3°С.

Схема размещения точек измерения температуры в тепловом узле приведена на рис. 1. Обработка данных эксперимента и синтез регрессионной модели проводились в пакетах MS Excel и StatGraphics 3.

Таблица 2

План факторного эксперимента

Номер опыта	X1	X2	X3	X4	X5	X6
1	1	1	1	1	1	1
2	1	1	1	1	2	2
3	1	1	1	2	1	3
4	1	1	1	2	2	4
5	1	1	2	1	1	5
6	1	1	2	1	2	1
7	1	1	2	2	1	2
8	1	1	2	2	2	3
9	1	2	1	1	1	4
10	1	2	1	1	2	5
11	1	2	1	2	1	1
12	1	2	1	2	2	2
13	1	2	2	1	1	3
14	1	2	2	1	2	4
15	1	2	2	2	1	5
16	1	2	2	2	2	1
17	2	1	1	1	1	2
18	2	1	1	1	2	3
18	2	1	1	2	1	4
20	2	1	1	2	2	5
21	2	1	2	1	1	1
22	2	1	2	1	2	2
23	2	1	2	2	1	3
24	2	1	2	2	2	4
25	2	2	1	1	1	5
26	2	2	1	1	2	1
27	2	2	1	2	1	2
28	2	2	1	2	2	3
29	2	2	2	1	1	4
30	2	2	2	1	2	5
31	2	2	2	2	1	1
32	2	2	2	2	2	2
33	1	2	1	1	1	3
34	2	2	1	1	2	4
35	2	1	1	2	1	5

При предварительной обработке данных эксперимента проведена проверка однородности дисперсии воспроизводимости. Для оценки воспроизводимости эксперимента проводилась статистическая обработка его результатов. Проверка воспроизводимости или постоянства дисперсии отклика сводится к проверке гипотезы об однородности дисперсий $S_1^2, S_2^2, ..., S_N^2$, найденных по результатам N опытов. Уточнённая величина выборочной дисперсии отклика S_i^2 для i-го опыта равна [6]:

$$S_i^2 = (\sum_{q=1}^{m} (y_{iq} - \overline{y}_u)^2)/(m-1), i = 1, 2, ..., N,$$

где y_{iq} – отклики i-го опыта при q-м его повторе; m – количество повторов опыта; $\overline{y}_i$ – среднее значение отклика в i-м опыте.

Для проверки гипотезы об однородности многих дисперсий при одинаковом для каждого опыта числе повторов применяется критерий Кохрена (*G* - критерий):

$$G = S_{max}^2 / \sum_{i=1}^{N} S_i^2,$$

где S_{max}^2 – наибольшая найденная выборочная дисперсия.

Гипотеза об однородности дисперсий подтверждается, если вычисленное значение *G* – критерия не превышает критического, определённого по соответствующим таблицам [2] в зависимости от числа степеней свободы k_{G1}=m-1, k_{G2}=N и выбранного уровня значимости. При заданном числе степеней свободы каждого измерения k_{G1} =2 и общем числе опытов N=35 оценка по числу Кохрена составила $G_{эксп}$=0,092537, что существенно меньше соответствующего интерполированного табличного значения (0,2152) для уровня значимости 0,01 [5].

Уравнение регрессии строилось в виде линейного полинома в истинных координатах:

$$Y = a_0 + \sum_{i=1}^{p} a_i X_i,$$

где p – число независимых переменных.

На первом этапе в модель были включены все 6 независимых переменных. Несмотря на то, что R2 статистика показала, что модель объясняет 99,2194% изменчивости отклика Y, оценка стандартной ошибки показывает отклонение остатков 6,07478, что не является удовлетворительным при точности прямых измерений платиновой термопарой ± 1°C и желательной точности косвенных измерений не хуже ±3°C.

Статистический анализ исходной модели показал, что переменными X4 и X5 можно пренебречь, так как P-значение (P-value – граничный уровень значимости) для X4 и X5 больше или равно 0,10 (0,4634 и 0,5273 соответственно). Другими словами, эти факторы не

являются статистически значимыми на 90% или более доверительном уровне и их можно удалить.

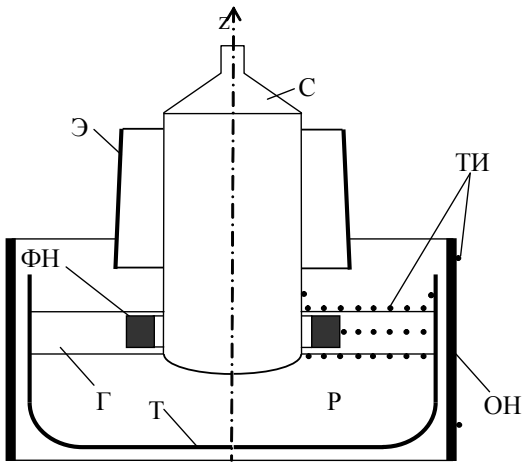


Рис. 1. Схема размещения точек измерения температуры: С – слиток; ОН – основной нагреватель; ФН – фоновый нагреватель; Э – экран; Т – тигель; Г – герметизатор; Р – расплав; ТИ – точки измерения

Дальнейшие исследования велись с переменными X1, X2, X3, X6**.** Регрессионный анализ выявил структуру линейной модели следующего вида:

$$Y = 765{,}14 + 0{,}143649*X1 + 0{,}0512563*X2 + 48{,}9129*X3 - 0{,}079936*X6. \quad (2)$$

Как известно, качество регрессионной модели зависит от значимости коэффициентов модели и от качества регрессионного уравнения в целом. В табл. 3 показаны параметры качества коэффициентов модели, включая константу.

Таблица 3

Оценки коэффициентов модели и их значимости

Параметр	Стандартная оценка	Ошибка	t – Статистика	P-Value
Константа	763,982	5,97353	127,895	0,0000
X1	0,150982	0,00105857	142,628	0,0000
X2	0,038372	0,00426022	9,00704	0,0000
X3	89,1859	12,1232	7,35662	0,0000
X6	-0,0330345	0,0150132	-2,20036	0,0036

Сравнивая значения коэффициента с его стандартной ошибкой, можно судить о значимости коэффициента. В данном случае сравнение указанных значений по t-статистике при уровне значимости P-Value не более 0,05 показывает, что все коэффициенты статистически значимы.

В табл. 4 приведена матрица оценок коэффициентов парной корреляции между переменными модели. Значимой корреляции с абсолютными значениями более 0,5 не выявлено.

Таблица 4

Оценки взаимной корреляции факторов

	X1	X2	X3	X6
X1	1,0000	0,0750	-0,0764	-0,0250
X2	0,0750	1,0000	0,0698	0,1130
X3	-0,0764	0,0698	1,0000	-0,0692
X6	-0,0250	0,1130	-0,0692	1,0000

Общие результаты регрессионного анализа таковы:

– R^2 -статистика составляет 99,855%, т.е. более 99% изменчивости отклика обусловлено изменением четырех указанных переменных;

– скорректированная величина R^2 (с учетом числа переменных регрессии – adjusted for d.f.) составляет 99,836%;

– стандартная ошибка остатков (SEE) составляет 2,48652;

– среднее значение остатков – 1,90981.

Статистика Дарбина-Уотсона (DW) составляет 0,928572 (P=0,0000). Она является результатом тестирования остатков для определения, есть ли существенная корреляция с порядком расположения данных в таблице. Так как P-значение для DW меньше 0,05, есть вероятность "сериальной" корреляции. Это, на наш взгляд, связано с тем, что переменная X6 в ходе опытов изменялась в одном и том же порядке.

С учетом того, что самое высокое P-значение независимых переменных составляет 0,0336, что меньше, чем уровень 0,05, то все независимые переменные являются статистически значимыми на уровне достоверности 95%.

Для проверки качества уравнения регрессии (2) использовалась F-статистика, представляющая собой отношение объясненной суммы квадратов остатков (в расчете на одну переменную) к остаточной сумме квадратов (в расчете на одну степень свободы). Результаты расчета F-статистики показаны в табл. 5. Значения F-отношения и P-Value показывают, что уравнение (2) имеет достаточный уровень адекватности.

Таблица 5

Результаты вычисления F-статистики

Источник	Суммарная квадратичная ошибка	Число степеней свободы	Средняя кв. ошибка на одну степень свободы	F-отношение	P-Value
Модель	127963,0	4	31990,8	5174,18	0,0000
Остатки	185,483	30	6,18277		
Общая	128149,0	34			

Статистическая значимость (F-статистика) для каждой переменной показана в табл. 6. Все включенные переменные статистически значимы.

Таблица 6

Результаты вычисления F-статистики по каждой переменной

Параметр	Суммарная квадратичная ошибка	Число степеней свободы	Средняя кв. ошибка на одну степень свободы	F-отношение	P-Value
X1	127134,0	1	127134,0	20562,70	0,0000
X2	476,251	1	476,251	77,03	0,0000
X3	322,449	1	322,449	52,15	0,0000
X6	29,9345	1	29,9345	4,84	0,0036
Модель	127963,0	4			

Верхний и нижний пределы оценок коэффициентов модели в доверительном интервале 95% с учетом объема имеющихся данных и наличия шума показаны в табл. 7. Пределы изменения значений коэффициентов на 95%-ном доверительном уровне достаточно узкие.

Таблица 7

Предельные оценки коэффициентов модели в доверительном интервале 95%

Параметр	Стандартная оценка	Отклонение	Нижний предел	Верхний предел
Константа	765,14	2,04244	760,969	769,311
X1	0,143649	0,000363361	0,142907	0,144391
X2	0,0512563	0,00144461	0,048306	0,0542066
X3	48,9129	4,12283	40,493	57,3329
X6	-0,079936	0,00508686	-0,0903248	-0,0695472

Была вычислена также DFITS-статистика – диагностика влияния всех отдельно взятых наблюдений, которая показывает, насколько сильно данное наблюдение "оттягивает" на себя линию регрессии. Анализ не выявил точек с необычно большими значениями "рычага" DFITS [7].

На рис. 2 приведен график стьюдентизированных остатков (нормированных разностей между модельными и наблюдаемыми значениями) в зависимости от номера наблюдения. Стьюдентизированный остаток – это остаток, деленный на оценку своего стандартного отклонения, меняющегося от одного наблюдения к другому, в зависимости от расстояния между Xi и средним значением X [8]. Стьюдентизированные остатки точнее отражают различия в дисперсиях истинных ошибок для разных наблюдений. Различимого криволинейного тренда остатков не наблюдается, что позволяет говорить о том, что гипотеза о линейности модели подтверждается.

Если рассматривать целевое предназначение модели, то под адекватностью понимают степень соответствия модели этому предназначению. Проверка адекватности проводится на основании экспериментальной информации. В данном случае проверка адекватности заключается в доказательстве факта, что точность результатов измерения температуры ФН, полученных по модели, будет не хуже требуемой.

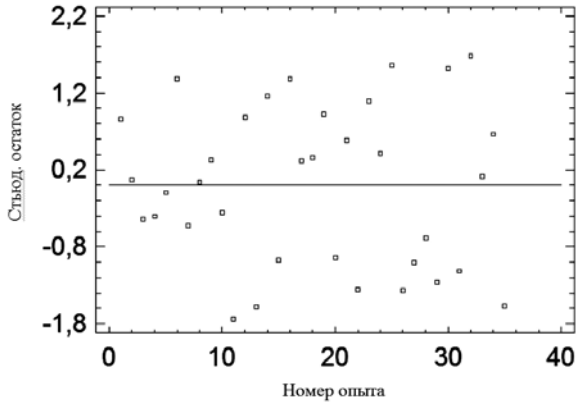


Рис. 2. График стьюдентизированных остатков в зависимости от номера наблюдения.

Стандартные ошибки структурных параметров уравнения (2) и значение коэффициента детерминации R^2 свидетельствуют о статистической адекватности модели. Однако при наличии возможности физического моделирования была осуществлена и верификация модели путем сравнения получаемых на ней данных и измеренных значениях температуры фонового нагревателя в процессе выращивания. Для этого были задействованы аппаратные средства существующей системы автоматизированного контроля и управления ростовой установки “Арсенид–1М”. Верификация разработанной математической модели проведена путем сравнения значений температуры ФН, полученных от виртуального датчика и значений, полученных путём прямого измерения термопарой. Значения независимых переменных задавали в произвольных точках поверхности отклика. Эти же значения факторов использованы в модели для определения температуры ФН. Таблица 8 включает в себя: модельные значения Y, °C; стандартную ошибку для каждого модельного значения; 95,0%-й доверительный интервал модельных значений; 95,0%-й доверительный интервал для среднего отклика. В табл. 9 сравниваются округленные до 1°C модельные и экспериментальные значения температуры ФН и показана ошибка модели относительно результатов реальных измерений. На рис. 3 приведен график ошибок (остаточных компонент) модели относительно измеренных термопарой значений. Несмотря на небольшое число опытов, можно утверждать, что систематической составляющей остатки не содержат. Анализ табличных данных показывает, что погрешность измерений при помощи виртуального датчика температуры в проведенных экспериментах не превышает ±3°C, т.е. сравнима с погрешностью измерений при помощи термопары с учётом неизбежных влияний динамики процесса вытягивания и нестабильности температуры расплава.

С использованием полученной математической модели была сформирована методика косвенного измерения температуры фонового нагревателя при различных сочетаниях значений параметров технологического режима. Методика включает следующие этапы:

1. Для каждой конкретной ростовой установки виртуальный датчик верифицируется на типовом процессе выращивания. Для верификации достаточно одного пробного прогона процесса с измерением температуры ФН на трех этапах выращивания при помощи термопары, как это описано выше.

2. Если выявлена систематическая ошибка, оператор компенсирует её, регулируя значение постоянной составляющей модели в диалоговом окне программы контроля температуры.

3. В течение последующих процессов выращивания температура ФН вычисляется по следующим параметрам:

– температура основного нагревателя, °С (измеряется в реальном времени прямым методом);

– скорость вытягивания, мм/мин (значение задаётся оператором);

– уровень расплава, вычисляемый в реальном времени по формуле:

$$h_р = (\frac{m_з - m_с}{\rho_р \pi R_т^2} + h_г) \cdot 100\% ,$$

где $m_з$ – масса загрузки; $m_с$ – измеренная в реальном времени масса выращенного на данный момент слитка; $\rho_р$ – плотность расплава; $R_т$ – радиус тигля; $h_г$ – высота слоя герметизатора;

– потребляемая мощность ФН, кВт (измеряется в реальном времени прямым методом).

Таблица 8

Прогнозные значения отклика модельной функции в доверительном интервале 95%

Номер опыта	Модельное значение, °С	Стандартная ошибка модельного значения	Нижний 95%-й доверительный уровень модельного значения	Верхний 95%-й доверительный уровень модельного значения	Нижний 95%-й доверительный уровень для среднего модельного значения	Верхний 95%-й доверительный уровень для среднего модельного значения
1	1034,38	0,907361	1032,53	1036,24	1033,72	1035,04
2	1056,94	0,886822	1055,13	1058,75	1056,4	1057,47
3	1062,65	0,923769	1060,76	1064,54	1061,9	1063,4
4	1083,74	0,892662	1081,92	1085,56	1083,17	1084,31
5	1106,53	0,901888	1104,69	1108,37	1105,9	1107,16
6	1106,21	0,894386	1104,38	1108,03	1105,62	1106,79
7	1128,76	0,879739	1126,97	1130,56	1128,28	1129,25
8	1134,48	0,917574	1132,6	1136,35	1133,76	1135,19
9	1040,65	0,909207	1038,79	1042,5	1039,97	1041,32
10	1063,44	0,909215	1061,58	1065,29	1062,76	1064,11
11	1063,11	0,897792	1061,28	1064,95	1062,51	1063,72
12	1085,67	0,879503	1083,87	1087,46	1085,19	1086,15
13	1091,38	0,916987	1089,51	1093,25	1090,67	1092,1
14	1112,47	0,888918	1110,65	1114,29	1111,92	1113,02
15	1135,26	0,9043	1133,41	1137,11	1134,62	1135,91

Таблица 9

Сравнение модельных и экспериментальных значений температуры ФН

Номер опыта	1	2	3	4	5	6	7	8	9	10	11	12
Модель, °С	1034	1057	1063	1084	1107	1106	1129	1134	1041	1063	1063	1086
Эксперимент, °С	1035	1057	1062	1084	1108	1105	1127	1136	1043	1064	1062	1085
Остаток, °С	1	0	-1	0	1	-1	-2	2	2	1	-1	-1
Номер опыта	13	14	15									
Модель, °С	1091	1112	1135									
Эксперимент, °С	1091	1110	1133									
Остаток, °С	0	-2	-2									

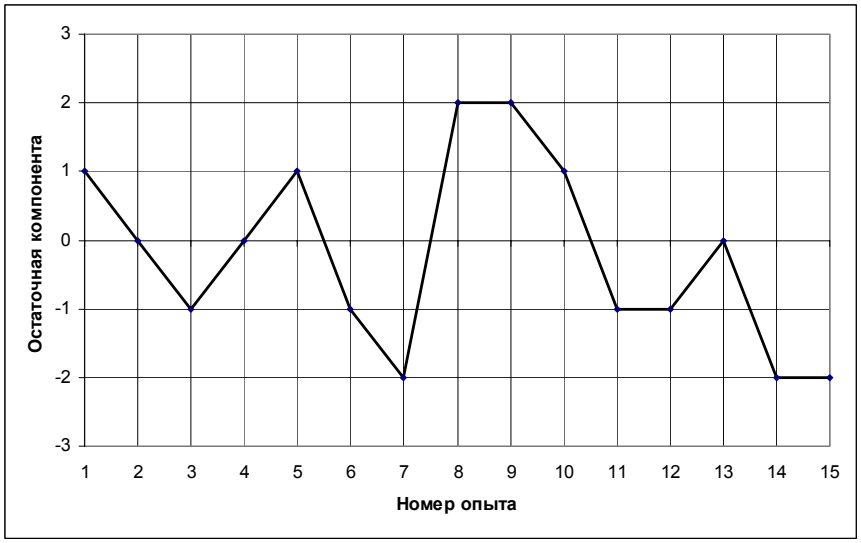


Рис. 3. График остаточных компонент модели в сравнении с прямым измерением температуры ФН

Методика прошла испытания в условиях производства монокристаллов GaAs диаметром 75...100 мм. Подтверждена валидность методики, т.е. точность измерений температуры и повторяемость (воспроизводимость) результатов измерения. Применение методики в 34-х процессах выращивания показало повышение стабильности плотности дислокаций на уровне $N \leq 5 \cdot 10^3 см^{-2}$. Данные по температуре ФН используются в подсистеме "Советчик мастера", основная функция которой – поддержка принятия оперативных решений по коррекции параметров процесса выращивания монокристаллов GaAs.

Выводы

Впервые предложена математическая модель для определения температуры фонового нагревателя теплового узла, которая учитывает значение потребляемой нагревателем мощности, значение скорости вытягивания, значение температуры основного нагревателя и значение уровня расплава, что позволяет обеспечить погрешность косвенного измерения не превышающую ±3°С, и использовать в технологическом процессе виртуальный мониторинг теплового поля в зоне кристаллизации.

Контроль температуры фонового нагревателя позволяет ввести дополнительный контур автоматического регулирования в автоматизированную систему управления процессом выращивания монокристаллов GaAs по LEC-технологии.

Разработанная модель является прикладной основой для построения информационной технологии реализации полнофункциональной системы "Советчик мастера", которая позволяет в режиме реального времени процесса выращивания контролировать температурное поле в зоне кристаллизации, оптимизировать температурный режим и повышать структурное совершенство монокристаллов GaAs.

Список литературы: 1. *Оксанич А.П.* Архітектура та функціональність дворівневої системи управління вирощуванням злитків кремнію / А.П. Оксанич, В.Р. Петренко, С.Э. Притчин // Радіоелектроніка та інформатика. 2007. № 4 (39). С. 49 – 53. **2.** *Нейросетевая* модель расчета температурного поля слитка в процессе выращивания монокристаллов методом Чохральского / И.В. Шевченко, Ю.А. Краснопольская, Е.А. Глушков, М.В. Репин // Нові технології. 2009. № 2 (24). С. 3-9. **3.** *Моделирование* процесса выращивания полупроводниковых материалов на основе нейронной сети и нечеткого клеточного автомата / И.В. Шевченко, Ю.А. Краснопольская, Е.А. Глушков, С.Л. Шкатуло // Нові технології. 2010. № 1 (27). С. 169–177. **4.** *Ковтун Г.П.* Технологические приемы улучшения теплового режима выращивания кристаллов GaAs методом Чохральского / Г.П. Ковтун, А.И. Кравченко, А.И. Кондрик, А.П. Щербань. Технология и конструирование в электронной аппаратуре. 2004. №6. С. 3–6. **5.** *Оксанич А.П.* Моделирование процессов образования дислокаций под действием термических напряжений в слитках GaAs, выращиваемых из расплава методом Чохральского с жидкостной герметизацией / А.П. Оксанич, Л.Г. Шепель, В.В. Батареев. Прикладная радиоэлектроника. 2005. Т. 4, № 2. С. 185–194. **6.** *Хартман К., Лецкий Э., Шефер В.* Планирование эксперимента в исследовании технологических процессов. М.: Мир, 1977. 552 с. **7.** *Монтгомери Д. К.* Планирование эксперимента и анализ данных:

Пер. с англ. Л.: Судостроение, 1980. 384 с. **8.** *Афифи А., Эйзен С.* Статистический анализ. Подход с применением ЭВМ. М.: Мир, 1982. 484 с.

Поступила в редколлегию 11.09.2011

Оксанич Анатолий Петрович, д-р техн. наук, профессор, заведующий кафедрой информационно-управляющих систем, директор НИИ технологии полупроводников и информационно-управляющих систем Кременчугского национального университета им. М. Остроградского. Научные интересы: методы и аппаратура контроля структурно совершенных полупроводниковых монокристаллов. Адрес: Украина, 39600, Кременчуг, ул. Первомайская, 20, тел.: (05366) 30157. E-mail: oksanich@kdu.edu.ua.

Шевченко Игорь Васильевич, канд. техн. наук, доцент кафедры информационно-управляющих систем Кременчугского национального университета им. М. Остроградского. Научные интересы: интеллектуальные информационные технологии контроля и управления в производстве полупроводниковых материалов. Адрес: Украина, 39600, Кременчуг, ул. Первомайская, 20, E-mail: athome050@yandex.ru.

Краснопольская Юлия Алексеевна, аспирант кафедры информационно-управляющих систем Кременчугского национального университета им. М. Остроградского. Научные интересы: интеллектуальные информационные технологии мониторинга технологического процесса производства полупроводниковых материалов. Адрес: Украина, 39600, Кременчуг, ул. Первомайская, 20, E-mail: ulya.k@mail.ru.

681.325.53: 37: 004.5

Н.Я.КАКУРИН, Ю.В.ЛОПУХИН, В.В. ВАРЕЦА, С.Н. САРАНЧА, А.Н. МАКАРЕНКО

СХЕМОТЕХНИЧЕСКОЕ ПРОЕКТИРОВАНИЕ НА ЯЗЫКЕ VHDL ПРЕОБРАЗОВАТЕЛЕЙ КОДОВ ПО МЕТОДУ ДОСЧЕТА

Рассматривается структура и функционирование многосекционных преобразователей кодов по методу досчета. Обосновывается выбор языка VHDL и рассматривается реализация преобразователя двоичного кода в двоично-двенадцатиричный код по методу досчета .

1. Постановка задачи

Рост быстродействия высокопроизводительных вычислительных систем в настоящее время невозможен без использования быстродействующих методов и средств обработки первичной информации.

Особая группа функционально-ориентированных устройств (ФОУ) применяется в качестве предпроцессоров и постпроцессоров. Предпроцессор ведет обработку информации до основного (центрального) процессора, постпроцессор – после.

Известно, что в современных универсальных ЭВМ преобразование чисел выполняется программным способом, что снижает их производительность. Переход на быстродействующие аппаратурные способы преобразования кодов позволяет значительно увеличить быстродействие вычислительной системы и является перспективным.

Достоинством преобразователей кодов по методу досчета (ПК ДСЧ), относящихся к аппаратурным способам преобразования, является схемная простота, малые аппаратурные затраты, низкая стоимость и линейный рост аппаратурных затрат от разрядности входного кода [1-3].

Основными параметрами ПК ДСЧ являются: система счисления на входе и выходе, разрядность входного и выходного кодов, быстродействие, аппаратурные затраты и стоимость. Реализация ПК ДСЧ на БИС или СБИС улучшает их основные параметры.

Быстродействие ПК ДСЧ в дальнейшем будем оценивать не по абсолютным единицам времени (нс, мкс, мс), а по относительным (по количеству тактов преобразования максимального числа).

Характеристика стоимости является вторичной по отношению к параметру аппаратурных затрат и отражает влияние на нее типа применяемых элементов.

Целью настоящей работы являются:

– анализ структурных особенностей и основных характеристик ПК ДСЧ;

– алгоритмизация нахождения структуры ПК ДСЧ с наибольшим быстродействием;

– рассмотрение результатов схемотехнического проектирования на языке VHDL многосекционной структуры ПК ДСЧ двоичного кода в двоично-двенадцатиричный код.

2. Односекционная и многосекционная схемы ПК ДСЧ

Простейшим преобразователем по методу досчета является односекционная схема, содержащая один входной вычитающий счетчик и один выходной суммирующий.

Недостатком односекционного ПК ДСЧ есть значительное число тактов на преобразование максимального числа.

Пусть система счисления на входе – p; число входных разрядов nZ; длительность периода импульсов генератора – $T_Г$.

Тогда при p=2; nZ=20 время преобразования определяется формулой:

$$t_{пр} = T_Г \cdot N_{макс} = T_Г \cdot (p^{nZ} - 1), \qquad (1)$$

при $T_Г = 1 \cdot 10^{-6}$ с.; $t_{пр} = 1 \cdot 10^{-6}(2^{20} - 1) = 1 \cdot 10^{-6} \cdot 1{,}048575 \cdot 10^{6} \approx 1{,}05$с.

Для ускорения процесса преобразования чисел можно использовать различные приемы, в частности разбиение входных и выходных счетчиков на две [1] или на большее число секций [2-4].

Перевод чисел в многосекционных ПК ДСЧ происходит путем последовательно-возвратного обнуления каждого входного счетчика. При этом способе обнуление входного счетчика второй секции начинается только после полного обнуления входного счетчика первой секции, обнуление третьей секции возможно после полного обнуления предыдущих входных секций, т.е. второй и первой.

Структура многосекционного ПК ДСЧ показана на рис.1.

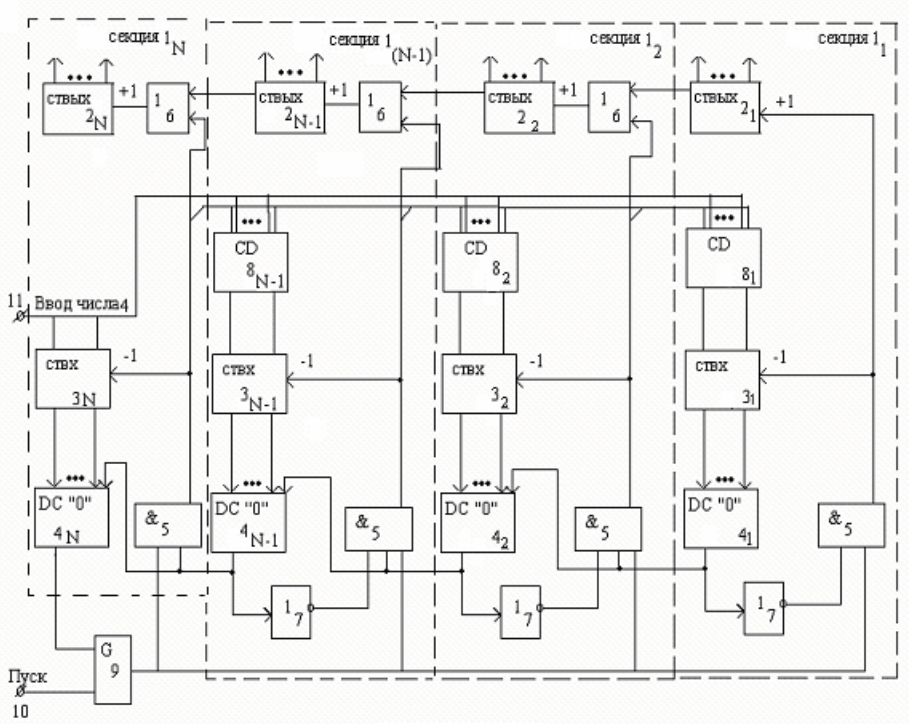


Рис. 1. Структура многосекционного ПК ДСЧ

Преобразователь содержит N преобразующих секций I; каждая преобразующая секция I – декаду (при К =10) двоично-десятичного счетчика 2, двоичный счетчик 3, дешифратор нуля 4, элемент И 5. Все секции I, кроме младшей, содержат элемент ИЛИ 6; все секции,

кроме старшей, – элемент НЕ 7. Все преобразующие секции, кроме двух старших, содержат шифраторы 8.

Преобразователь содержит генератор импульсов 9 и вход пуска 10. Обозначим коэффициент пересчета двоичных счетчков 3_i через $M_i(i=\overline{1,N})$. Устройство работает следующим образом. В исходном состоянии в двоичных счетчиках $3_i(i=\overline{1,N})$ записаны числа $a_1, a_2, \ldots, a_n$ преобразуемого двоичного кода, а декады двоично-К-ичных счетчиков $2_i(i=\overline{1,N})$ установлены в нуль. При этом на выходе дешифратора нуля 4_i появляется запрещающий потенциал, если в двоичном счетчике 3_i записано какое-либо число, отличное от нуля. По сигналу "Пуск" импульсы с выхода генератора 9 поступают через элемент $И5_1$ на счетный вход вычитания счетчика 3_i и на счетный вход сложения счетчика 2_1 и производят вычитание единиц из счетчика 3_1 и прибавление единиц в счетчик 2_1 (по единице на каждый импульс) до тех пор, пока в счетчике 3_1 не установятся нули. Таким образом, число a_1 будет перенесено в счетчик 2_1. Если $a_1 \geq 10$, то возникает единица переноса, которая поступает через элемент ИЛИ 6_2 на счетный вход счетчика 2_2, а в счетчике 2_1 останется число $m_1 = a_1 - 10$.

Если $a_1 < 10$, то в счетчике 2_1 остается число $m_1 = a_1$.

Преобразование называется возвратно-поступательным, так как прохождение одного импульса на обнуление второй секции приводит к записи корректирующей поправки R_{21} в первый входной счетчик. Затем вновь начинается обнуление первого входного счетчика. При этом первый импульс с выхода генератора 9, пройдя через элемент И 5_i $(i=\overline{2,N})$ и шифратор $8_i(i=\overline{1,N-2})$, при p=2 и K=10 устанавливает число R_i, представленное формулой:

$$R_i = R_{i,i-1}R_{i,i-2}\ldots R_{i,1} = \prod_{l=1}^{l=i-1} M_1 - K^{i-1} = 2^{\sum_{l=1}^{l=i-1} n_l} - 10^{i-1} \qquad (2)$$

(n_l – количество двоичных разрядов в двоичном счетчике секции l) в двоичные счетчики $3_l(l=\overline{1,i-1})$ соответствующих предыдущих секций. После вычитания последней единицы из счетчика 3_N и последнего числа R_N из счетчиков $3_l(l=\overline{1,i-1})$ на выходе дешифратора нуля 4_N появляется сигнал, останавливающий работу генератора импульсов 9. На этом преобразование кода заканчивается.

3. Метод определения основных параметров многосекционного ПК ДСЧ

Разбиение ПК по методу досчета на секции выполняется таким образом, чтобы сохранилась счетчиковая структура выходных счетчиков (чтобы перенос был строго равен 1). При p=2 и $K \neq 10$ требуется выполнение общего условия:

$$2^{n_1} = (1a)_K; 2^{n_1+n_2} = (1ab)_K; 2^{n_1+n_2+n_3} = (1abc)_K. \qquad (3)$$

Это возможно в случае выполнения неравенства:

$$p^L \geq K^{i-1}, (i=\overline{2,N}), \qquad (4)$$

где i – номер секции; N – максимальное число секций; L – наименьшее целое число, при котором выполняется неравенство (4). При этом L не должно превышать заданное число разрядов nZ.

Как только $L \geq nZ$, процесс разделения на секции прекращается. В результате получим:

$$L = \sum_{l=1}^{l=N} n_l, \qquad (5)$$

здесь n_l - число входных p-ичных разрядов в секции l. Если обозначить $M_l = p^{n_l}$, то корректирующие поправки из i-ой секции i-1,i-2,….., 1 определяются по формуле:

$$R_i = R_{i,i-1}R_{i,i-2}\cdot\cdot R_{i,1} = \prod_{l=1}^{l=i-1} M_l - K^{i-1} = p^{\sum_{l=1}^{l=i-1} n_l} - K^{i-1}. \quad (6)$$

Например, при p=2; K=10; nZ=10 имеем $2^4 \geq 10^1$ и $n_1 = 4$; $R_2 = R_{21} = 16 - 10 = 6$.

Далее $2^7 \geq 10^2$; $n_2 = 7 - 4 = 3$; $R_3 = 128 - 100 = 28_{10}$. Для нахождения поправок $R_{32}; R_{31}$ число 28_{10} переводится в двоичную систему счисления $28_{10} = 0011\ 1100_2$ и разделяется на секции по числу входных разрядов и переводится вновь в десятичную систему $R_{32} = 1; R_{31} = 12$.

На следующем шаге имеем $2^{10} \geq 10^3; n_3 = 3$.

Поправки $R_4 = 2^{10} - 1000 = 1024 - 1000 = 24_{10} = 000\,0011100$ и $R_{43} = 0; R_{42} = 1; R_{41} = 8$.

На последнем шаге разбиения на секции, если $L > nZ$, число p-ичных разрядов секции n_N находят по формуле:

$$n_N = n_z - \sum n_i (i = \overline{1, N-1}). \quad (7)$$

Преобразование числа в многосекционной схеме ПК ДСЧ аналогично счету импульсов в неоднородной позиционной системе счета с весами $Q_i (i = \overline{1, N})$.

Весовые коэффициенты секций Q_i определяют по формуле:

$$Q_i = 1 + \sum_{j=1}^{i-1} R_{ij} Q_j, \ (i = \overline{1, N}), \quad (8)$$

где R_{ij} – корректирующая поправка из секции i в секцию j.

При числе разрядов каждой входной секции n_i и p=2 максимальное число тактов преобразования ПК ДСЧ рассчитывается по формуле:

$$T_N = \sum_{i=1}^{N} (2^{n_i} - 1) \cdot Q_i \quad (9)$$

Величины поправок R_{ij} определяют системой счисления p на входе, K на выходе, числом разрядов nZ на входе и числом разрядов n_i каждой секции.

При разбиении ПК ДСЧ на секции указывают число выходных m_i и входных n_i разрядов каждой секции в виде:

$$\begin{matrix} m_N, m_{N-1}, m_{N-2}, \cdots, m_2, m_1, \\ n_N, n_{N-1}, n_{N-2}, \cdots\cdots, n_2, n_1 \end{matrix} \quad (10)$$

Многосекционное разбиение называют фундаментальным (основным), если в каждой секции находится по одному выходному разряду. Фундаментальному разбиению(ФР) соответствует минимальное число тактов.

Все другие разбиения ПК ДСЧ на секции можно получить из фундаментального. ФР можно отобразить в виде:

$$\begin{matrix} 1,1,\cdots,1,1 \\ n_N, n_{N-1}, \cdots, n_2, n_1 \end{matrix} \quad (11)$$

4. Алгоритм нахождения фундаментального разбиения ПК ДСЧ

Анализ рассмотренной выше методики позволяет сформулировать алгоритм нахождения ФР в виде:

1. Находится разрядность каждой секции и число секций всего ПК по заданным основаниям входной и выходной систем счисления и разрядности на входе.
2. Строится матрица корректирующих поправок R_{ij} $(i = \overline{2, N}; j = \overline{1, N-1})$.

3. Вычисляются весовые коэффициенты $Q_i (i = \overline{1, N})$ секций.

4. Определяется максимальное число тактов преобразования фундаментального разбиения T_N.

В соответствии с приведенным выше алгоритмом для p=2; nZ=21; K=12 найдем, что $2^4 \geq 12^1$, следовательно $n_1 = 4$. Далее $2^{4+4} \geq 12^2$; $n_2 = 4$; $2^{4+4+3} \geq 12^3$; $n_3 = 3$; $2^{4+4+3+4} \geq 12^4$; $n_4 = 4$; $2^{4+4+3+4+3} \geq 12^5$; $n_5 = 3$; $2^{4+4+3+4+3+3} \geq 12^6$; $n_6 = 3$.

Таким образом, ФР в данном случае имеет вид:

1,1,1,1,1,1,
3,3,4,3,4,4.

Корректирующие поправки R_{ij} находят способом вычисления общей поправки R_i и разделение ее на поправки по секциям $j = \overline{1, i-1}$. Общая поправка R_i вычисляется по формуле (6).

Затем поправку R_i переводят во входную систему счисления p и представляют $n_1 + n_2 + ... + n_i$ разрядными числами. Полученное число разбивается на группы по n_i разрядов в каждой. Каждая группа двоичных разрядов представляет собой чистую поправку R_{ij}, которая для удобства вычислений переводится в десятичную систему счисления.

Поправочные коэффициенты в общем виде записываются по матрице:

$$R_{ij} = \begin{array}{c|cccccc} R_2 & 0 & 0 & \cdots & 0 & 0 & R_{21} \\ R_3 & 0 & 0 & \cdots & 0 & R_{32} & R_{31} \\ R_4 & 0 & 0 & \cdots & R_{43} & R_{42} & R_{41} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ R_N & R_{N,N-1} & R_{N,N-2} & \cdots & R_{N,3} & R_{N,2} & R_{N,1} \end{array}. \qquad (12)$$

Для рассматриваемого примера с p=2; K=12; N=6 получим

$$R_2 = 2^4 - 12^1 = 4_{10} = 0100_2;$$

$$R_{21} = 0100_2 = 4_{10}\ R_3 = 2^{4+4} - 12^2 = 112_{10} = 01110000_2;$$

$$R_{32} = 7_{10}; R_{31} = 0_{10}; R_4 = 2^{4+4+3} - 12^3 = 320_{10} = 00101000000_2; R_{43} = 1_{10};$$

$$R_{42} = 4_{10}; R_{41} = 0_{10};$$

$$R_5 = 2^{4+4+3+4} - 12^4 = 12032_{10} = 010111100000000_2; R_{54} = 5_{10}; R_{53} = 7_{10};$$

$$R_{52} = 0_{10}; R_{51} = 0_{10};$$

$$R_6 = 2^{4+4+3+4+3} - 12^5 = 13312_{10} = 000011010000000000_2;$$

$$R_{65} = 0_{10}; R_{64} = 6_{10}; R_{63} = 4_{10}; R_{62} = 0_{10}; R_{61} = 0_{10}.$$

В итоге получим следующую матрицу корректирующих поправок:

$$R_{ij} = \begin{array}{c|ccccc} 2 & & & & & 4 \\ 3 & & & & 7 & 0 \\ 4 & & & 1 & 4 & 0 \\ 5 & & 5 & 7 & 0 & 0 \\ 6 & 0 & 6 & 4 & 0 & 0 \end{array} \qquad (13)$$

и следующие веса секций $Q_1 = 1; Q_2 = 5; Q_3 = 36; Q_4 = 57; Q_5 = 538; Q_6 = 487$.

Максимальное число тактов преобразования ПК ДСЧ составит 8372 такта.

Все основные параметры ПК ДСЧ можно быстро определить с помощью программного средства «PREOBRAZOVATEL 2-K », реализованного на языке программирования C# [4]. Результаты расчета для p=2; K=12 ; nz =21 приведены на рис.2.

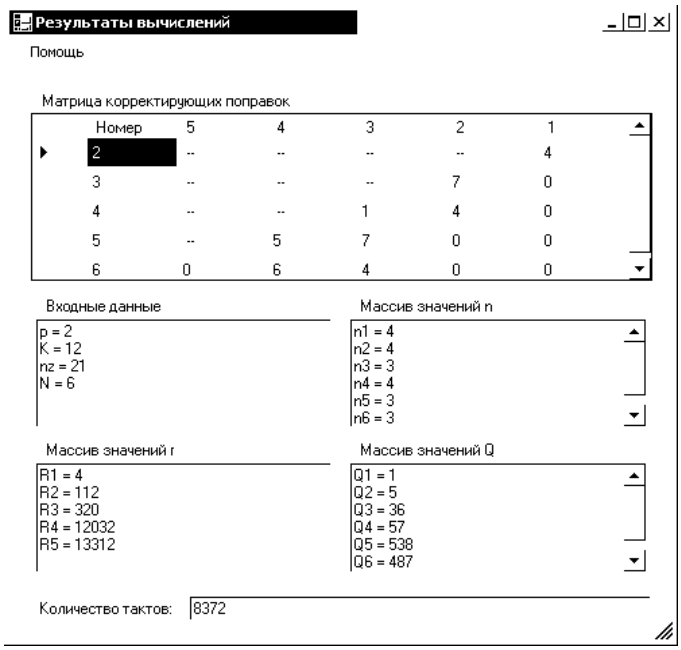


Рис.2. Пример расчета параметров 6-секционного ПК ДСЧ

5 . Назначение и возможности VHDL-модели ПК ДСЧ

Суть данной работы заключается в создании универсальной модели ПК ДСЧ, которая могла бы быть описана на языке VHDL.

Актуальность проектирования состоит в подготовке формализованного задания для проектирования ПК на ПЛИС с созданием модели на языке VHDL.

VHDL – это мощный язык, который позволяет описывать поведение цифровых схем, а также проводить иерархическое функционально-структурное описание больших интегральных систем и в то же время имеет все признаки языка программирования высокого уровня – позволяет создавать свои типы данных, имеет широкий набор арифметических и логических операций .

Задачей системы синтеза на данном этапе является эффективное распределение RTL-схемы в целях создания нового списка соединений с минимальным количеством использованных схемных компонентов. Каждый компонент нового списка будет соответствовать физическому аппаратному блоку в используемой микросхеме FPGA (элементы конфигурируемых логических блоков, логика ускоренного переноса).

Иерархические проекты синтезируются в восходящем режиме, когда компоненты нижнего уровня синтезируются до компонентов верхнего уровня.

Модель устройства, разработанная на языке описания аппаратуры VHDL, должна быть адаптирована для синтеза и реализации на кристалле FPGA фирмы XILINX.

Задача выбора аппаратной платформы чрезвычайно важна для проектировщика. Правильный выбор позволит:

– снизить материальные затраты при реализации устройства;

– добиться оптимального функционирования и быстродействия.

Согласно техническому заданию, модель ПК должна быть адаптирована для синтеза и реализации на FPGA фирмы Xilinx. При выборе серии ПЛИС основное внимание уделяется соотношению ее стоимости и производительности. Также необходимо учитывать площадь кристалла, которая будет занята синтезированным устройством.

Программируемые пользователем вентильные матрицы (Field Programmable Gate Arrays – FPGA) впервые были разработаны фирмой Xilinx в 1985 г. Настройка FPGA на заданное функционирование выполняется каждый раз перед началом ее работы. Необходимая для этого программа настройки предварительно записывается в ПЗУ (ОЗУ). Сразу после включения питания производится загрузка информации из ПЗУ и осуществляется автоматическая инициализация FPGA. Возможно также выполнение настройки FPGA под

управлением микропроцессора или микроконтроллера. FPGA имеет типичную структуру вентильной матрицы.

ПЛИС типа FPGA фирмы Xilinx выполнены по SRAM КМОП технологии. Характеризуются высокой гибкостью структуры и изобилием на кристалле триггеров. При этом логика реализуется посредством матрицы так называемых LUT - таблиц (Look Up Table), а внутренние межсоединения - посредством разветвлённой иерархии металлических линий, коммутируемых специальными быстродействующими транзисторами.

Большая стоимость микросхем FPGA с встроенной RAM по сравнению со стоимостью заказных микросхем ограничивает использование FPGA для изготовления опытных образцов или мелкосерийной продукции. Этот недостаток FPGA устранен фирмой Xilinx выпуском новой серии микросхем FPGA - серий Spartan и Spartan-II. Параметры микросхем семейства FPGA Spartan-II (модель XC2S30) имеют рекордно низкую стоимость в расчете на один вентиль при плотности упаковки до 200 тысяч вентилей. В кристалле имеется четыре блока ОЗУ каждый по 4 КБита, также возможна реализация 16 бит памяти на каждом 4-входовом функциональном генераторе.

Устройства Spartan-II сочетают черты гибкой, регулярной архитектуры, которая охватывает матрицу конфигурируемых логических блоков (CLB), окруженную программируемыми блоками ввода-вывода, связанными между собой иерархией быстрых, многосторонних ресурсов межсоединений.

Устройства Spartan-II имеют более высокую производительность по сравнению с предыдущими семействами FPGA. Проекты могут работать с системной частотой синхронизации до 200 МГц, включая блоки ввода/вывода (Input/Output-I/O).

Кроме этого, чипы Spartan-II отличает целый ряд достоинств:

– относительно низкая стоимость кристалла;

– большая размерность чипа (до 200 000 системных вентилей);

– высокое быстродействие.

Программируемая пользователем вентильная матрица Spartan-II охватывает: конфигурируемые логические блоки (configurable logic blocks – CLBs) и блоки ввода – вывода (IOBs). CLB блоки служат для создания функциональных логических элементов, а блоки I/O создают интерфейс между контактами микросхемы и CLB

Ниже приведен фрагмент текста программы на VHDL-языке для генерации RTL-схемы трехсекционного ПК ДСЧ из двоичной системы счисления в двоично-двенадцатиричную:

```
library ieee;
use  ieee.std_logic_1164.all;
use  ieee.std_logic_unsigned.all;
component ie7 is
generic(n:natural:=10);
port(
   clk  :  in STD_LOGIC;
   rst  :  in STD_LOGIC;
   ce_in  :  in STD_LOGIC;
   ce_out  :  out STD_LOGIC;
   q  :  out STD_LOGIC_VECTOR(3 downto 0)
);
end  component;
     begin
       process(clk) is
     begin
        if rising_edge(clk) then
                    if load='1' then reg<=din;
                    elsif clk_en='1' then
                            if section1/=0 then section1<=section1-1;
                            elsif section2/=0 then section2<=section2-1; section1<="0100";
                            elsif section3/=0 then section3<=section3-1; section2<="0111";
                                        section1<="0000";
                            elsif section4/=0 then section4<=section4-1; section3<="001";
                                                section2<="0100";  section1<="0000";
                            —elsif section5/=0 then section5<=section5-1; section4<="0110";
                            section3<="001";  section2<="111";  section1<="0000";
                            end if;
```

```
                    end if;
        end if;
      end process;
        ce_out<=ce_in when cnt=n-1 else '0';
    q<=cnt;
  end architecture ie7;
```

В целях проверки функционирования ПК ДСЧ 2-12 получена временная диаграмма преобразования числа 298 из двоичной системы в двенадцатиричную (рис.3).

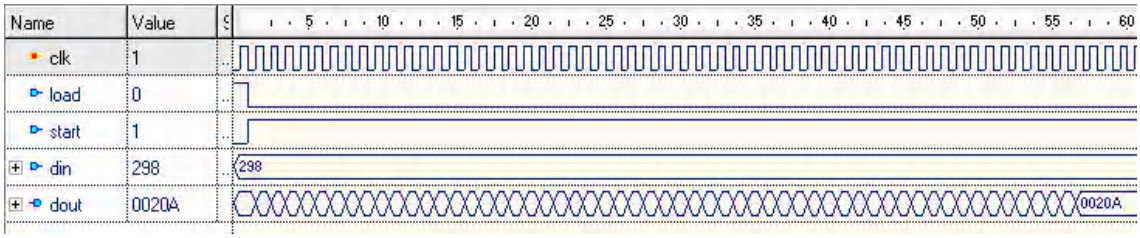


Рис. 3. Временная диаграмма функционирования трехсекционного ПК ДСЧ

СБИС семейства Spartan-II отличает целый ряд достоинств: относительно низкая стоимость кристалла; большая размерность чипа (до 200 000 системных вентилей); высокое быстродействие. Схемотехническая реализация трехсекционного ПК ДСЧ 2-12 приведена на рис.4.

Программируемая пользователем вентильная матрица Spartan-II охватывает: конфигурируемые логические блоки (configurable logic blocks - CLBs) и блоки ввода - вывода (IOBs). CLB блоки служат для создания функциональных логических элементов, а блоки I/O создают интерфейс между контактами микросхемы и CLB

Выводы

1. Рассмотрена структура и функционирование многосекционного преобразователя кодов по методу досчета.

2. Предложены методика и алгоритм нахождения фундаментального разбиения ПК ДСЧ, реализованные на языке программирования C# в программном средстве «PREOBRAZOVATEL 2-K», позволяющем автоматизировать этапы системного проектирования и ускорять нахождение основных характеристик многосекционного ПК ДСЧ .

3. Разработана на языке описания аппаратуры VHDL программная модель многосекционного ПК ДСЧ и получена временная диаграмма функционирования трехсекционного ПК ДСЧ двоичного кода в двоично-двенацатиричный код.

Научная новизна исследования состоит в разработке и апробации программной модели многосекционного ПК ДСЧ и реализации этой модели на языке VHDL .

Практическая значимость результатов заключается в возможности автоматизированного синтеза RTL-схем ПК ДСЧ, что позволяет на порядок ускорить их проектирование и реализацию на СБИС.

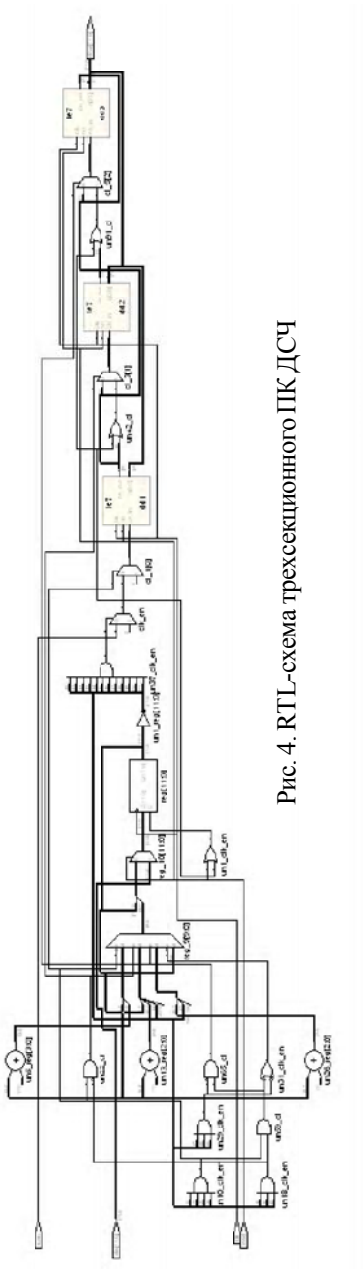


Рис. 4. RTL-схема трехсекционного ПК ДСЧ

Список литературы: **1.** А.С. 468236 5G06F 5/02. Устройство для преобразования кодов / В.М.Гусятин, Н.В.Алипов, А.П.Руденко // Открытия, изобретения. 1975. №15. С.108. **2.** А.С. 1153323 5G06F 5/00. Преобразователь двоичного кода в двоично-К-ичный код /Н.Я.Какурин, Ю.К. Кирьяков, В.М. Гусятин // Открытия, изобретения.1985. №16. С.167. **3.** *Макаренко А.Н.* Алгоритмизация разбиений преобразователей кодов // АСУ и приборы автоматики. 1990. Вып. 94. С.103-109. **4.** *Какурин Н.Я., Лопухин Ю.В., Вареца В.В., Катасонов В.В., Мака-*

ренко А.Н. Программное средство для анализа характеристик преобразователей кодов по методу досчета // АСУ и приборы автоматики. 2010. Вып. 152. С.41-48.

Поступила в редколлегию 29.08.2011

Какурин Николай Яковлевич, канд. техн. наук, профессор кафедры АПВТ ХНУРЭ. Научные интересы: прикладная теория цифровых автоматов, автоматизация проектирования цифровых устройств. Адрес: Украина, 61166, Харьков, пр.Ленина, 14, тел. 70-21-326.

Лопухин Юрий Владимирович, ст. преподаватель кафедры АПВТ ХНУРЭ. Научные интересы: проектирование программного обеспечения, автоматизация проектирования цифровых устройств. Адрес: Украина, 61166, Харьков, пр.Ленина, 14, тел. 70-21-326.

Вареца Виталий Викторович, аспирант кафедры АПВТ ХНУРЭ. Научные интересы: проектирование программного обеспечения, автоматизация проектирования цифровых устройств. Адрес: Украина, 61166, Харьков, пр.Ленина, 14, тел. 70-21-326.

Саранча Сергей Николаевич, канд. техн. наук, доцент кафедры ЭВМ ХНУРЭ. Научные интересы: системы автоматизированного проектирования, моделирование цифровых систем. Адрес: Украина, 61166, Харьков, пр.Ленина, 14, тел. 70-21-354.

Макаренко Анна Николаевна, канд. техн. наук, доцент кафедры информационных технологий Харьковского банковского института. Научные интересы: информационные технологии, анализ и синтез преобразователей код-код. Адрес:. Украина, 61074, Харьков, пр. Победы, 55, тел. 336-05-64.

УДК 681.518:004.93.1’

А.О. ПАНИЧ, О.Б. БЕРЕСТ

ОПТИМІЗАЦІЯ ПАРАМЕТРІВ НАВЧАННЯ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ КЕРУВАННЯ ЕЛЕКТРОПРИВОДОМ ПЛАТФОРМИ ЛЕТУЧОЇ ПИЛИ

Розглядається категорійна модель та інформаційно-екстремальний алгоритм навчання системи підтримки прийняття рішень для керування летучою пилою. Будуються в процесі навчання вирішальні правила, які дозволяють підвищити точність різання довговимірних матеріалів, що рухаються.

Вступ

Летучі пили (ЛП) використовуються в технологічних лініях для порізу довговимірних матеріалів, що рухаються. Оброблюваними виробами, наприклад, можуть бути труби, сортовий прокат, гнуті профілі, деревні плити [1,2]. Несучим органом ЛП є платформа, на якій розміщене обладнання різальної системи. Робочий цикл привода платформи має періоди робочого та зворотного ходу, перший з яких містить ділянки розгону з переслідуванням перерізу різання оброблюваного виробу та руху з постійною швидкістю з виконанням технологічної операції різання [3,4]. Електропривод платформи працює з високою частотою вмикань і характеризується великими витратами електроенергії в перехідних процесах, тому до нього пред’являються жорсткі вимоги щодо виконання технологічних обмежень. Попередній аналіз та модельні дослідження процесів керування ЛП з врахуванням випадкових змін параметрів приводів платформи та оброблюваного виробу показують, що запропоновані у працях [5,6] закони руху та способи їх реалізації не завжди забезпечують необхідну точність порізу та, відповідно, потребують застосування методів її підвищення.

Одним із шляхів підвищення точності роботи електропривода платформи ЛП є використання інтелектуальної системи керування ЛП на основі машинного навчання та розпізнавання образів [7,8], яка функціонує роздільно у часі у двох режимах: навчання, на якому будуються вирішальні правила, і екзамену, на якому здійснюється оцінка поточного функціонального стану системи.

У статті розглядається математична модель та інформаційно-екстремальний алгоритм навчання системи керування електроприводом платформи ЛП.

1. Постановка задачі інформаційно-екстремального навчання

Нехай алфавіт $\{X_m^o\}$ складається з трьох класів розпізнавання, що характеризують отримані в результаті послідовності робочих циклів довжини відрізаних виробів (за умови виконання синхронізації за швидкістю) за такою трьохальтернативною системою оцінок: клас X_1^o – "Норма" (точність порізу ±3 мм), клас X_2^o – "Більше норми" і клас X_3^o – "Менше норми". За результатами моделювання цих трьох режимів функціонування системи керування сформовано вхідну навчальну матрицю $\| y_{m,i}^{(j)} \mid m = 1,3 \|$, в якій рядок є реалізацією образу $\{y_{m,i}^{(j)} \mid i = \overline{1, N}\}$, де N – кількість ознак розпізнавання, а стовпчик матриці - випадкова навчальна вибірка $\{y_{m,i}^{(j)} \mid j = \overline{1, n}\}$, де n – обсяг вибірки. Дано структурований вектор просторово-часових параметрів функціонування g=<g_1, …, gx , …, g_Ξ>, які впливають на функціональну ефективність системи керування з відповідними на них обмеженнями $Rx(g_1, \ldots, g_\Xi) \le 0$.

У режимі навчання необхідно побудувати вирішальні правила шляхом відновлення в радіальному базисі простору ознак контейнерів класів розпізнавання в процесі оптимізації параметрів функціонування $\{g_\xi^*\}$, які забезпечують максимум інформаційного критерію функціональної ефективності (КФЕ) в робочій (допустимій) області визначення його функції:

$$E_m^* = \max_G E_m,$$

де E_m – КФЕ процесу навчання розпізнавати реалізації класу X_m^o; G – область допустимих значень параметрів функціонування системи керування.

У режимі екзамену, тобто безпосередньої оцінки поточного стану ЛП, необхідно визначити належність реалізації, що розпізнається, одному із класів заданого алфавіту $\{X_m^o \mid m = \overline{1,3}\}$.

Таким чином, задача інформаційно-екстремального навчання полягає у побудові оптимального (тут і далі в інформаційному розумінні) розбиття простору ознак на класи розпізнавання.

2. Математична модель

Вхідний математичний опис інтелектуальної системи керування подамо у вигляді теоретико-множинної структури:

$$\Delta_B = <G, T, \Omega, Z, Y; X; \Pi, \Phi_1, \Phi_2>,$$

де G – множина факторів, які діють на систему керування; T – множина моментів часу зняття інформації; Ω – простір ознак розпізнавання; Z – простір можливих станів системи керування; Y – вибіркова множина (вхідна навчальна матриця); X – вхідна бінарна навчальна матриця; П: $G \times T \times \Omega \to Z$ – оператор переходів, що відбиває механізм зміни станів системи під впливом внутрішніх і зовнішніх факторів; $\Phi_1 : G \times T \times \Omega \times Z \to Y$ – оператор формування вибіркової множини Y на вході СППР; $\Phi_2 : Y \to X$ – оператор формування бінарної навчальної матриці.

На рис.1 показано категорійну модель у вигляді діаграми відображення множин, що застосовуються в процесі навчання системи керування електроприводом платформи ЛП з оптимізацією контрольних допусків на ознаки розпізнавання [7]. Оператор $\theta : X \to \tilde{\Re}^{|M|}$ відновлює у загальному випадку нечітке розбиття $\tilde{\Re}^{|M|}$, а оператор класифікації у: $\tilde{\Re}^{|M|} \to I^{|I|}$ перевіряє основну статистичну гіпотезу про належність реалізацій $\{x_m^{(j)} | j = \overline{1, n}\}$ нечіткому класу X_m^o, де l – кількість статистичних гіпотез. Оператор $\gamma : I^{|I|} \to \Im^{|q|}$ шляхом оцінки статистичних гіпотез формує множину точнісних характеристик $\Im^{|q|}$, де $q=l^2$ – кількість точнісних характеристик. Оператор $\varphi : \Im^{|q|} \to E$ обчислює множину значень інформаційного КФЕ, який є функціоналом точнісних характеристик.

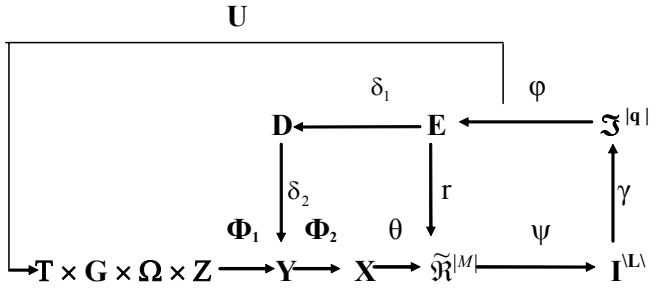


Рис. 1.Діаграма відображення множин у процесі навчання СППР

У діаграмі (див.рис.1) контур оптимізації геометричних параметрів розбиття $\widetilde{\Re}^{|M|}$ замикається оператором r: $E \to \widetilde{\Re}^{|M|}$, оператори якого показано на рис. 2.

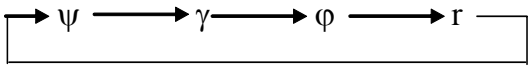


Рис. 2. Контур оптимізації геометричних параметрів контейнерів класів розпізнавання

У діаграмі (див.рис.1) терм-множина D складається із допустимих значень СКД, а контур операторів, показаних на рис.3, безпосередньо оптимізує контрольні допуски на ознаки розпізнавання.

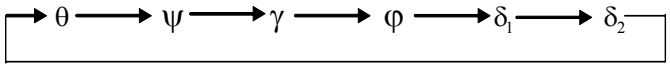


Рис.3. Контур оптимізації контрольних допусків на ознаки розпізнавання

Оператор U: $E \to G \times T \times \Omega \times Z$ регламентує процес навчання і дозволяє оптимізувати параметри його плану, які визначають, наприклад, обсяг і структуру випробувань, черговість розгляду класів розпізнавання тощо.

Таким чином, використання показаної на рис. 1 категорійної моделі достатньо адекватно відбиває слабоформалізований динамічний процес навчання СППР і, крім того, суттєво спрощує побудову структурної схеми інформаційно-екстремального алгоритму навчання.

3. Алгоритм навчання СППР

Алгоритм навчання СППР з оптимізацією контрольних допусків на ознаки розпізнавання розглянемо відносно показаного на рис. 4 двобічного симетричного поля допусків для і-ї ознаки розпізнавання y_i із вхідної навчальної матриці $\| y_{m,i}^{(j)} \|$.

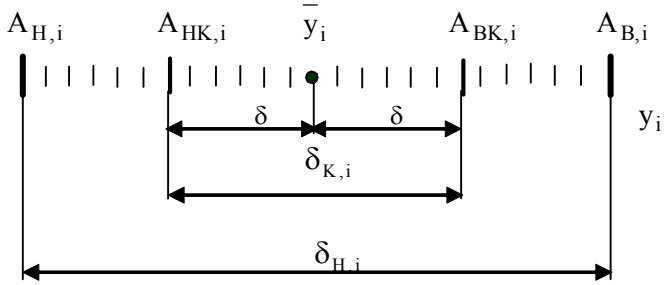


Рис. 4. Симетричне поле допусків

На рис. 4 прийнято такі позначення: $\bar{y}_i$ – номінальне (усереднене) значення ознаки y_i; $A_{H,i}$, A_{B_i} – нижній і верхній нормовані допуски відповідно; $A_{HK,i}$, $A_{BK,i}$ – нижній і верхній контрольні допуски відповідно; $\delta_{H,i}$ – поле нормованих допусків; $\delta_{K,i}$ – поле контрольних допусків; δ – параметр поля контрольних допусків.

Розглянемо алгоритм навчання СППР з паралельною оптимізацією контрольних допусків на ознаки розпізнавання. При цьому зміна контрольних допусків, які формуються відносно базового (найбільш бажаного) класу X_1^o, здійснюється для всіх ознак одночасно

за такою двохциклічною ітераційною процедурою пошуку глобального максимуму інформаційного КФЕ навчання СППР у робочій (допустимій) області визначення його функції:

$$\delta^* = \arg\max_{G_\delta} \{ \max_{G_E \cup G_d} \overline{E} \}, \quad (1)$$

де $\overline{E}$ – усереднене за алфавітом класів розпізнавання значення інформаційного КФЕ навчання СППР; G_δ, G_E, G_d – допустимі області значень параметра поля контрольних допусків на ознаки розпізнавання; КФЕ навчання СППР і радіусів контейнерів класів розпізнавання, що у процесі навчання відновлюються в радіальному базисі простору ознак відповідно.

Вхідними даними є масив реалізацій образу $\{y_m^{(j)} \mid m = \overline{1,M};\ j = \overline{1,n}\}$ і система нормованих допусків на ознаки розпізнавання $\{\delta_{H,i}\}$, яка визначає область значень відповідних контрольних допусків. При цьому за область значень параметра δ_i береться інтервал $[1; \delta_{H,i}/2]$, де $\delta_{H,i}$ – ширина нормованого поля допусків для і-ї ознаки розпізнавання.

Розглянемо основні етапи реалізації алгоритму навчання СППР з паралельною оптимізацією контрольних допусків на ознаки розпізнавання:

1. Обнулюється лічильник кроків зміни параметра δ : l:=0.
2. Запускається лічильник: l:=l+1 і обчислюються нижні та верхні контрольні допуски для всіх ознак:

$$\{A_{HK,i}[l] := y_{1,i} - \delta[l]\} \ \text{ і } \ \{A_{BK,i}[l] = y_{1,i} + \delta[l]\}, \quad i = \overline{1,N}, \quad (2)$$

де $y_{1,i}$ – вибіркове середнє значення i-ї ознаки для векторів-реалізацій класу X_1^o, який є найбільш бажаним для ОПР .

3. Реалізується базовий алгоритм навчання [8]:

а) формується бінарна навчальна матриця $\| x_{m,i}^{(j)} \|$ за правилом

$$x_1^{(j)} = \begin{cases} 1, & \text{if } \ y_{1,i} - \delta \le y_{1,i}^{(j)} \le y_{1,i} + \delta, \\ 0, & \text{if else}; \end{cases}$$

б) формується масив еталонних двійкових векторів $\{x_{m,i} \mid m = \overline{1,M},\ i = \overline{1,N}\}$, елементи якого визначаються за правилом

$$x_{m,i} = \begin{cases} 1, & \text{if } \ \frac{1}{n} \sum_{j=1}^{n} x_{m,i}^{(j)} > \rho_m; \\ 0, & \text{if else}, \end{cases}$$

де ρ_m – рівень селекції координат вектора $x_m \in X_m^o$;

в) розбиваються множини еталонних векторів на пари найближчих “сусідів”: $\Re_m^{|2|} = < x_m, x_l >$, де x_l – еталонний вектор сусіднього класу X_l^o, за такою схемою:

– структурується множина еталонних векторів, починаючи з вектора x_1 базового класу X_1^o, який характеризує найбільшу функціональну ефективність СППР;

– будується матриця кодових відстаней між еталонними векторами розмірності *M*×*M;*

– для кожного рядка матриці кодових відстаней знаходиться мінімальний елемент, який належить стовпчику вектора, найближчого до вектора, що визначає рядок. За наявності декількох однакових мінімальних елементів вибирається з них будь-який, оскільки вони є рівноправними;

– формується структурована множина елементів попарного розбиття $\{\Re_m^{|2|} \mid m = \overline{1,M}\}$, яка задає план навчання;

г) змінюється кодова відстань d_m за рекурентною процедурою

$$d_m(k) = [d_m(k-1) + h \mid d_m(k) \in G_m^d],$$

де k – змінна числа збільшень радіуса контейнера $K_m^o \in X_m^o$; h – крок збільшення радіуса; G_m^d – область допустимих значень радіуса d_m;

д) обчислюється значення інформаційного КФЕ навчання СППР за модифікованою формулою критерію Кульбака [8]:

$$E_m = \log_2\left(\frac{2-(\alpha_m^{(k)}+\beta_m^{(k)})}{\alpha_m^{(k)}+\beta_m^{(k)}}\right)*[1-(\alpha_m^{(k)}+\beta_m^{(k)})], \qquad (3)$$

тут $\alpha_m^{(k)}$, $\beta_m^{(k)}$ – точнісні характеристики: помилки першого і другого роду, що обчислюються на k-му кроці відновлення контейнера класу X_m^o;

е) процедура закінчується при знаходженні глобального максимуму КФЕ в робочій області його визначення: $E_m^* = \max_{\{d\}} E_m$, де $\{d\} = \{d_1,...,d_k,...,d_{max}\} \in [0; d(x_m \oplus x_1)-1]$ – множина радіусів концентрованих гіперсфер, центр яких визначається вершиною еталонного вектора $x_m \in X_m^o$.

4. Якщо $\delta \le \delta_H / 2$, то виконується пункт 2, інакше – пункт 5.

5. Визначається максимальне значення КФЕ, обчислене за l кроків навчання СППР:

$$E_m^* = \max_{\{l\}} E_m$$

і визначається оптимальне значення параметра поля контрольних допусків, яке дорівнює екстремальній сумі l^* лічильника кроків зміни параметра δ.

6. Визначаються оптимальні нижні та верхні контрольні допуски для ознак розпізнавання

$$\{A^*_{HK,i} := A_{HK,i}[l^*]\}; \quad \{A^*_{BK,i} := A_{BK,i}[l^*]\}, \; i = \overline{1,N}.$$

7. ЗУПИН.

Таким чином, алгоритм навчання СППР з оптимізацією системи контрольних допусків полягає в реалізації двохциклічної ітераційної процедури пошуку глобального максимуму інформаційного КФЕ навчання системи в робочій (допустимій) області визначення його функції.

4. Приклад реалізації алгоритму

Для формування навчальних матриць використана комп'ютерна модель системи керування електроприводом платформи ЛП [6] профілезгинального стану, яка оснащена двигуном постійного струму Д32 потужністю 18 кВт, маса платформи 1200 кг. Модель доповнена блоками, що реалізують випадкові збурення за нормальним законом розподілення сигналів статичного моменту M_c, зворотних зв'язків по струму i_2 та швидкості обертання ω_2 якоря двигуна електропривода платформи ЛП; сигналу виміряної швидкості оброблюваного виробу V_1; сигналу тривалості спрацьовування механізму зчеплення (після зчеплення закінчується розгін-синхронізація). Відповідно до використовуваних на практиці, при моделюванні встановлена швидкість руху оброблюваного виробу V_1=0,9 м/с, мірна довжина порізу $L_м$=4 м, прискорення при розгоні $a_{зад.в}$=2,34 м/с^2. Згідно з працею [6], значення похідної моменту електроприводу прийняте рівним 20 (у відносних одиницях). При цьому задана точність мірного порізу дорівнювала $\pm$3 мм. Оптимальний за енерговитратами закон руху привода платформи ЛП в режимі робочого ходу містить ділянки розгону-синхронізації, на яких швидкість V_2 платформи змінюється від 0 до швидкості V_{OB} виробу й відбувається її синхронізація з перерізом різання, та руху з постійною швидкістю V_2=V_{OB} під час обробления виробу. На ділянці розгону-синхронізації реалізується рівноприскорений рух з обмеженням похідної моменту двигуна привода платформи. Ділянка розгону-синхронізації, у свою чергу, містить ділянки зміни моменту M_2 двигуна згідно з заданою похідною $\dot{M}_{зад}$ моменту та ділянку рівноприскореного руху платформи з заданим прискоренням $a_{зад.в}$. Привод платформи ЛП запускається в момент досягнення точкою обробки на виробі (перерізом різання) наперед визначеного значення координати, що пов'язане з початковим положенням

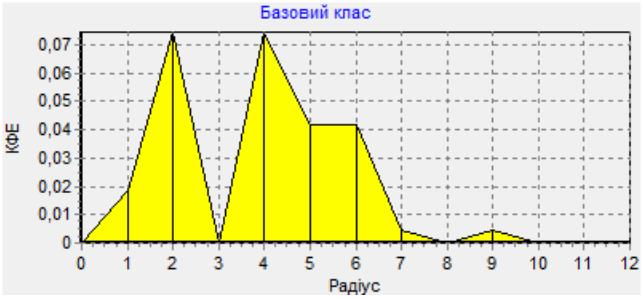
платформи, швидкістю $V_{ОВ}$ та шляхом переміщення, який проходить платформа під час розгону-синхронізації. Запропонований у [6] закон руху привода платформи ЛП реалізований у комп'ютерній моделі системи керування електроприводом платформи ЛП [7], яка містить контури швидкості та моменту, налаштовані на модульний оптимум. Задана тахограма руху платформи ЛП формується у моделі контроллера ЛП та передається на вхід електропривода.

На тахограмі сигналу завдання швидкості, що надходить з контроллера ЛП до електропривода платформи, виділено 5 характерних точок ($n = \overline{1,5}$). Перша точка відповідає моменту запуску платформи (V_2=0); друга – початку зміни завдання швидкості з заданим прискоренням $a_{зад.в}$; третя – початку зміни прискорення від $a_{зад.в}$ до 0; четверта – завданню швидкості, що дорівнює V_1; п'ята – спрацюванню механізму зчеплення. Для другої, третьої та четвертої ділянок тахограми на випробувальному стенді було сформовано масиви навчальних матриць $\{y^{(j)}_{s,m,i} \mid s = \overline{2,4}; m = \overline{1,3}; i = \overline{1,23}; j = \overline{1,40}\}$ відповідно для класів $X^{o}_{s,1}$, $X^{o}_{s,2}$ і $X^{o}_{s,3}$.

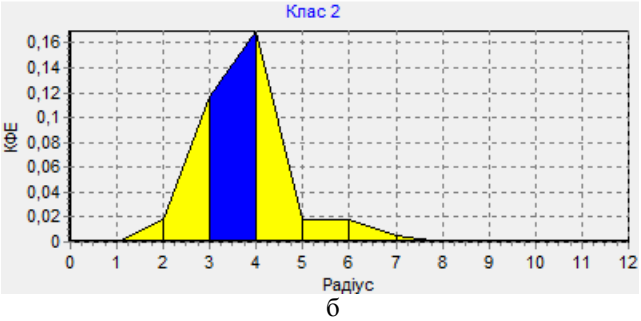
Словник ознак розпізнавання складався з 23 параметрів, з яких 5 безпосередньо зчитуються з датчиків на об'єкті: переміщення і швидкості виробу та платформи – відповідно, l_1 і V_1 та l_2 і V_2; момент приводу платформи M_2. Крім того, враховано поточний час; різниці переміщень $(l_1 - l_2)$ та швидкостей $(V_1 - V_2)$; похідні моменту $\dot{M}_2$ та швидкостей $\dot{V}_1, \dot{V}_2$ і $\ddot{V}_2$; виміряне значення статичного моменту M_c; виміряне значення тривалості спрацьовування механізму зчеплення; задані від контроллера ЛП значення моменту та швидкості привода платформи; задані значення корекції швидкості синхронізації та положення запуску платформи, які використовуються у керуючому алгоритмі; розраховано значення миттєвої потужності та роботи току на нагрівання якоря двигуна електропривода платформи ЛП; миттєва механічна потужність, механічна робота та кінетична енергія електропривода платформи ЛП.

На рис. 5 показано одержані в процесі реалізації базового алгоритму навчання графіки залежності критерію (3) від радіусів контейнерів класів розпізнавання для алфавіту $\{X^{o}_{2,m}\}$, побудованого на другій ділянці тахограми, для неоптимального параметра $\delta_i = \pm 40$ (у відсотках від усередненого значення і-ї ознаки), обчисленого для першого класу $X^{o}_{2,1}$ і для рівня селекції координат еталонного вектора $y_{2,1} \in X^{o}_{2,1}$, який дорівнював $\rho_{2,1} = 0{,}5$.

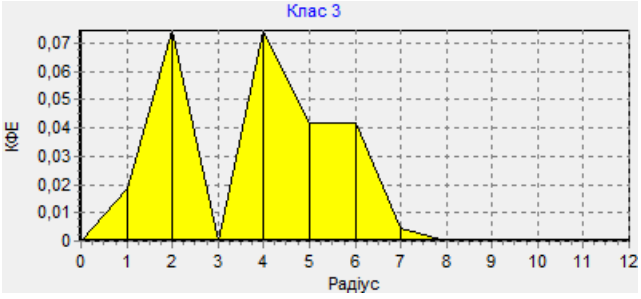
Аналіз рис.5 показує, що тільки в одному випадку (рис.5,б) існує робоча область, яку тут і далі на графіку позначено темною ділянкою. Цей факт пояснюється тим, що вибрана система контрольних допусків є неоптимальною. Тому для підвищення функціональної ефективності навчання СППР доцільно застосувати ітераційний алгоритм навчання (1) з паралельною оптимізацією контрольних допусків на ознаки розпіз-



а



б



в

Рис.5. Графіки залежності КФЕ від радіусів контейнерів класів розпізнавання: а – клас $X^{o}_{2,1}$; б – клас $X^{o}_{2,2}$; в – клас $X^{o}_{2,3}$

навання. На рис.6 показано одержаний в процесі паралельної оптимізації графік залежності усередненого за алфавітом класів розпізнавання КФЕ (2) від параметра поля контрольних допусків δ.

Аналіз рис.6 показує, що оптимальне значення параметра поля контрольних допусків на ознаки розпізнавання дорівнює $\delta^* = \pm 89$ при максимальному середньому значенні КФЕ $E^* = 0{,}41$, що суттєво перебільшує значення критерію при реалізації базового алгоритму навчання (рис. 5,б).

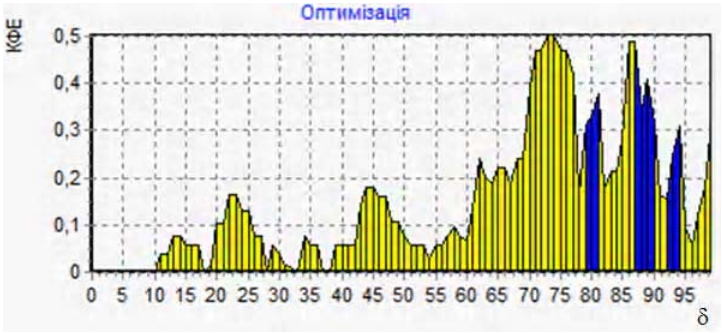
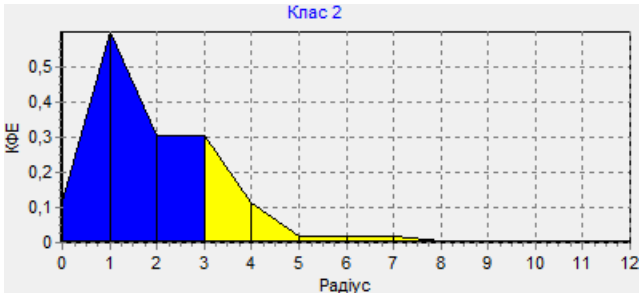


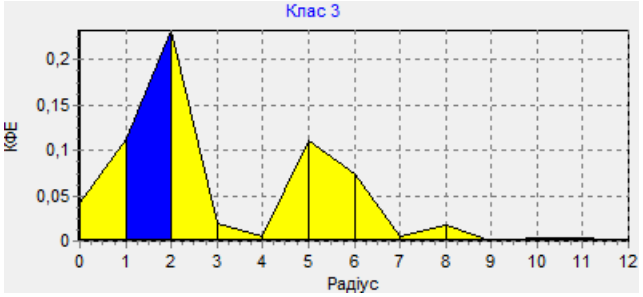
Рис. 6. Графік залежності КФЕ навчання СППР від параметра поля контрольних допусків на ознаки розпізнавання

На рис. 7 показано графіки залежності КФЕ (2) від радіусів контейнерів класів розпізнавання, одержані в процесі оптимізації контрольних допусків на ознаки розпізнавання.

а



б



в

Рис. 7. Графіки залежності критерію Кульбака від радіусів контейнерів класів розпізнавання в процесі оптимізації контрольних допусків: а – клас $X^o_{2,1}$; б – клас $X^o_{2,2}$; в – клас $X^o_{2,3}$

Аналіз рис. 7 показує, що при оптимальному параметрі δ^* поля контрольних допусків для всіх класів розпізнавання існують робочі області визначення КФЕ і при цьому оптимальні радіуси контейнерів класів розпізнавання дорівнюють у кодових одиницях відповідно $d^*_{2,1} = 3$, $d^*_{2,2} = 1$ і $d^*_{2,3} = 2$.

Таким чином, у процесі навчання відновлено оптимальні контейнери класів розпізнавання, центрами яких є еталонні двійкові вектори-реалізації образів, що забезпечують оптимальні радіуси відповідних контейнерів.

Аналогічно формувалися в процесі навчання вирішальні правила для інших ділянок тахограми сигналу завдання швидкості ЛП.

Висновки

1. Розроблено інформаційно-екстремальний алгоритм навчання інтелектуальної СППР з оптимізацією системи контрольних допусків на ознаки розпізнавання, що дозволяє сформувати базу знань для керування ЛП в робочому режимі функціонування.

2. У процесі навчання СППР побудовано оптимальні в інформаційному розумінні вирішальні правила у вигляді відновлених в радіальному базисі контейнерів класів розпізнавання, центрами яких є екстремальні еталонні двійкові вектори-реалізації образів, які дозволяють в робочому режимі коригувати швидкість ЛП з метою підвищення точності нарізки довговимірних матеріалів.

Список літератури: 1. *Червяков В.Д.* Летучие механизмы как класс рабочих машин в аспекте задач управления / В.Д. Червяков, А.А. Паныч // Электротехнические системы и комплексы: Межвузовский сборник научных трудов. Магнитогорск: МГТУ. 1998. Вып. 3. С. 176-182. **2.** *Червяков В.Д.* Задачи ресурсосберегающего управления электроприводом несущего органа летучей пилы / В.Д. Червяков, А.А. Паныч // Вісник Національного технічного університету "Харківський політехнічний інститут". Збірка наукових праць. Тематичний випуск 10. Харків, НТУ ХПІ, 2001. С.370-371. **3.** *Белов М.П.* Автоматизированный электропривод типовых производственных механизмов и технологических комплексов: учебник для студ. высш. учеб. заведений/ М.П. Белов, В.А. Новиков, Л.Н. Рассудов // М.: Издательский центр "Академия", 2007. 576 с. **4.** *Лимонов Л.Г.* Автоматизированный электропривод промышленных механизмов / Л.Г. Лимонов // Х.: Изд-во "ФОРТ", 2009. 272 с. **5.** *Паныч А.А.* Оптимальное по энергозатратам управление процессом рабочего хода платформы летучей пилы / А.А. Паныч, В.Д. Червяков // Вісник Національного технічного університету "Харківський політехнічний інститут". Харків: НТУ "ХПІ", 2008. №30. С.500-502. **6.** *Червяков В.Д.* Анализ законов движения электропривода несущего органа летучей пилы методом компьютерного моделирования / В.Д. Червяков, А.А. Паныч // Збірник наукових праць Дніпродзержинського державного технічного університету (технічні науки). Тематичний випуск "Проблеми автоматизованого електропривода. Теорія і практика". Дніпродзержинськ: ДДТУ, 2007. С.289-291. **7.** *Краснопоясовський А.С.* Інформаційний синтез інтелектуальних систем керування: Підхід, що ґрунтується на методі функціонально-статистичних випробувань / А.С. Краснопоясовський // Суми: Видавництво СумДУ, 2004. 261 с. **8.** *Довбиш А.С.* Основи проектування інтелектуальних систем: Навчальний посібник / А.С. Довбиш // Суми: Видавництво СумДУ, 2009. 171 с.

Надійшла до редколегії 11.09.2011

Панич Андрій Олександрович, ст. викладач кафедри комп'ютерних наук, факультет електроніки та інформаційних технологій, Сумський державний університет. Наукові інтереси: інтелектуальні системи управління. Адреса: Україна, 40007, Суми, вул. Римського-Корсакова, 2. E-mail: info@ksu.sumdu.edu.ua.

Берест Олег Борисович, аспірант кафедри Комп'ютерних наук, факультет Електроніки та інформаційних технологій, Сумський державний університет, Україна. Наукові інтереси: інформаційний аналіз і синтез інтелектуальних систем, що навчаються. Адреса: Україна, 40007, Суми, вул. Римського-Корсакова, 2. E-mail: Berest_Oleg@mail.ru.

УДК 681.518:004.93.1’

В.В. МОСКАЛЕНКО, І.В. ШЕЛЕХОВ, О.В. СОБОЛЄВ

ІНФОРМАЦІЙНО-ЕКСТРЕМАЛЬНИЙ УНІМОДАЛЬНИЙ КЛАСИФІКАТОР З ПАРАЛЕЛЬНО-ПОСЛІДОВНОЮ ОПТИМІЗАЦІЄЮ КОНТРОЛЬНИХ ДОПУСКІВ НА ОЗНАКИ РОЗПІЗНАВАННЯ

Пропонується інформаційно-екстремальний алгоритм оптимізації контрольних допусків на ознаки розпізнавання для унімодального класифікатора, який характеризується єдиним центром розсіювання векторів-реалізацій образів. При цьому одержані за процедурою паралельної оптимізації квазіоптимальні контрольні допуски використовуються як стартові для послідовної процедури. Як приклад розглядається реалізація унімодальної системи підтримки прийняття рішень для керування технологічним процесом вирощування сцинтиляційних монокристалів.

Вступ

Один із прогресивних способів підвищення функціональної ефективності АСК вирощуванням великогабаритних сцинтиляційних монокристалів (СМК) полягає в наданні їй властивості адаптивності на основі машинного навчання та розпізнавання образів [1]. Перспективною розробкою в галузі аналізу і синтезу здатних навчатися АСК є інформаційно-есктремальна інтелектуальна технологія (ІЕІ-технологія) [2]. Основна ідея ІЕІ-технології полягає в оптимізації в процесі навчання структурованих просторово-часових параметрів функціонування системи шляхом трансформації апріорного нечіткого розбиття простору ознак розпізнавання у чітке розбиття відношення еквівалентності класів. При цьому оптимізація параметрів функціонування здійснюється за ієрархічною ітераційною процедурою шляхом пошуку глобального максимуму інформаційного критерію функціональної ефективності навчання в робочій області визначення його функції. У праці [3] розглядалася оптимізація контрольних допусків на ознаки розпізнавання в процесі навчання мультимодального класифікатора за паралельним алгоритмом, який передбачає одночасну зміну контрольних допусків на всі ознаки. Але в цій праці не вдалося побудувати безпомилкові вирішальні правила, оскільки одержані екстремальні параметри навчання слід розглядати як квазіоптимальні.

У статті в рамках ІЕІ-технології розглядаються алгоритми паралельно-послідовної оптимізації системи контрольних допусків (СКД) на ознаки розпізнавання в процесі навчання унімодальної системи підтримки прийняття рішень (СППР), яка є складовою частиною системи керування вирощуванням сцинтиляційних монокристалів.

1. Постановка задачі

Розглянемо АСК вирощуванням монокристалів, складовою частиною якої є здатна навчатися СППР. Нехай за інтервал часу τ_r, $r = \overline{1,R}$, де R – кількість інтервалів спостереження технологічного процесу, сформовано впорядкований алфавіт параметричних класів розпізнавання $\{X^o_m(\tau_r) \mid m = \overline{1,M}\}$, що характеризують функціональні стани технологічного процесу,непрямим показником якості якого є діаметр монокристала, що вирощується, («Норма», «Менше норми» і «Більше норми») на інтервалі τ_r, і відповідну навчальну багатовимірну (векторну) матрицю типу «об’єкт-властивість» $\| y^j_{m,i}(\tau_r) \mid i = \overline{1,N}, j = \overline{1,n} \|$, де N, n – кількість ознак розпізнавання і векторів-реалізацій образу відповідно. Відомий структурований вектор параметрів функціонування СППР $g = <d_m, \delta>$, де d_m – радіус контейнера класу $X^o_m(\tau_r)$, що відновлюється в радіальному базисі дискретного простору ознак розпізнавання відносно центру розсіювання, який визначається вершиною еталонного вектора x_m; δ – параметр поля контрольних допусків на ознаки розпізнавання. При цьому задано такі обмеження: вершина вектора x_m, що визначає геометричний центр розсіювання векторів-реалізацій всіх класів у бінарному просторі $\Omega_Б$ ознак розпізнавання і має

одиничні координати; $d_m > d_{m-1}$. При цьому радіус класу X_M^o дорівнює $d_M = N$ і $\delta \in [0; \delta_H / 2]$, де δ_H – нормоване поле допусків, що визначає область значень параметра δ.

Необхідно в процесі навчання СППР визначити оптимальні значення координат вектора g, що забезпечують на кожному інтервалі аналізу даних τ_r максимальне значення усередненого за алфавітом класів розпізнавання критерію функціональної ефективності (КФЕ) навчання СППР:

$$\bar{E}^*(\tau_r) = \frac{1}{M} \sum_{m=1}^{M} \max_{\{k\}} E_m(\tau_r), \tag{1}$$

де $E_m(\tau_r)$ – інформаційний КФЕ навчання СППР розпізнавати реалізації класу X_m^o; $\{k\}$ – впорядкована множина кроків навчання (відновлення контейнерів класів розпізнавання).

При функціонуванні СППР в режимі екзамену, тобто безпосереднього розпізнавання, необхідно прийняти рішення про належність реалізації, що розпізнається, одному із класів сформованого на етапі навчання алфавіту $\{X_m^o(\tau_r) \mid m = \overline{1, M}\}$ і таким чином дефазіфікувати функціональний стан системи керування і, при необхідності, внести коригуючі команди для стабілізації діаметра монокристала.

2. Алгоритми навчання та екзамену унімодального класифікатора

Алгоритм навчання унімодальної СППР з оптимізацією СКД на ознаки розпізнавання, як і для мультимодальної [2,3], полягає у реалізації структурованої двоциклічної ітераційної процедури пошуку глобального максимуму інформаційного КФЕ (1) в робочій області визначення його функції. Для інформаційно-екстремального алгоритму паралельної оптимізації СКД, при якому параметр поля контрольних допусків δ_K змінюється одночасно для всіх ознак розпізнавання, така процедура має вигляд:

$$\delta_K^* = \arg \max_{G_\delta} \{\max_{G_E} \bar{E}\}, \tag{2}$$

де G_δ – область допустимих значень відповідних контрольних допусків на ознаки розпізнавання; G_E – область допустимих значень інформаційного КФЕ (1) навчання СППР.

У процедурі (2) внутрішній цикл реалізує базовий алгоритм навчання [2], основними задачами якого є обчислення інформаційного КФЕ навчання СППР; пошук глобального максимуму КФЕ в робочій (допустимій) області визначення його функції; оптимізація геометричних параметрів контейнерів класів розпізнавання.

При цьому специфіка базового алгоритму навчання унімодальної СППР полягає у відсутності процедури визначення для кожного класу найближчого сусіда, оскільки класи розпізнавання апріорно є впорядкованими, що суттєво підвищує оперативність навчання.

Оптимізацію контрольних допусків на ознаки доцільно здійснювати за паралельно-послідовним алгоритмом, що забезпечує прийнятну оперативність та високу точність обчислення КФЕ. При цьому за алгоритмом паралельної оптимізації СКД на ознаки визначаються квазіоптимальні контрольні допуски, які для послідовного алгоритму приймаються як стартові.

Розглянемо у рамках ІЕІ-технології алгоритм навчання унімодальної СППР на етапі паралельної оптимізації контрольних допусків на ознаки розпізнавання (2). Вхідні дані: масив реалізацій класів розпізнавання $\{y_{m,i}^{(j)} \mid m = \overline{1, M};\ i = \overline{1, N};\ j = \overline{1, n}\}$; система нормованих допусків $\{\delta_{H,i} \mid \overline{i = 1, N}\}$, що визначає область значень відповідних контрольних допусків. Попередньо для кожної ознаки визначається ціна градації її шкали виміру, що дозволяє обчислювати на кожному кроці навчання нижній і верхній контрольні допуски відповідно:

$$A_{KH,i} = y_{1,i} - \delta;\ A_{KB,i} = y_{1,i} + \delta, \tag{3}$$

де $y_{1,i}$ – вибіркове середнє значення і-ї ознаки розпізнавання у векторах-реалізаціях базового класу X_1^o.

Реалізація алгоритму навчання унімодальної СППР з паралельною оптимізацією контрольних допусків на ознаки розпізнавання здійснюється за такою схемою:

1) обнулюється лічильник кроків зміни параметра δ (кроків навчання): l:=0;

2) δ : l:=l+1;

3) на кожному кроці навчання за формулами (3) обчислюються нижній $A_{HK,i}[l]$ і верхній $A_{HK,i}[l]$ контрольні допуски для всіх ознак розпізнавання;

4) реалізується базовий алгоритм навчання і визначається поточний глобальний максимум усередненого за алфавітом класів розпізнавання інформаційного критерію $\overline{E}[l]$ в робочій області визначення його функції;

5) якщо в робочій області визначення функції інформаційного критерію має місце $\overline{E}[l] \le \text{extr}\max \overline{E}$, де $\text{extr}\max \overline{E}$ – граничний максимум усередненого за алфавітом класів розпізнавання інформаційного критерію (1), то виконується пункт 6, інакше – пункт 7 ($\overline{E}[0] = 0$);

6) якщо $\delta \le \delta_H / 2$, то виконується пункт 2, інакше– пункт 6;

7) $\text{extr}\max \overline{E} := \max\limits_{\{l\}} \overline{E}^*[l]$, $\delta^* := \arg\ \text{extr}\max \overline{E}$;

8) для парметра δ^* обчислюються оптимальні нижні $\{A^*_{HK,i}\}$ і верхні $\{A^*_{BK,i}\}$ контрольні допуски на ознаки розпізнавання;

9) ЗУПИН.

Одержані в процесі паралельної оптимізації квазіоптимальні допуски використовуються як стартові для алгоритму послідовної оптимізації контрольних допусків на ознаки розпізнавання.

Алгоритм послідовної оптимізації контрольних допусків на ознаки розпізнавання здійснювався за ітераційною процедурою

$$\{\delta^*_{K,i}\} = \arg\{\max_{G_{\delta_i}}\{\max_{G_E}[\overset{S}{\underset{s=1}{\otimes}} \max_{G_d} \overline{E}^{(s)}]\}\},\ i = \overline{1,N}, \tag{4}$$

де $\overline{E}^{(s)}$ – усереднений за алфавітом класів КФЕ навчання СППР на s-му прогоні послідовної процедури оптимізації; G_{δ_i} – область допустимих значень поля контрольних допусків для і-ї ознаки; G_E – область допустимих значень критерію оптимізації; G_d – область допустимих значень радіусів контейнерів; $\otimes$ – символ операції повторення.

Як КФЕ навчання СППР використано модифіковану інформаційну міру Кульбака [2,4], в якій розглядається відношення правдоподібності у вигляді відношення повної ймовірності правильного прийняття рішень P_t до повної ймовірності помилкового прийняття рішень P_f. Для рівноймовірних двохальтернативних гіпотез, що характеризує найбільш складний у статистичному розумінні випадок прийняття рішень, міру Кульбака подамо у вигляді:

$$E^{(k)}_m = \log_2 \frac{P^{(k)}_{t,m}}{P^{(k)}_{f,m}}[P^{(k)}_{t,m} - P^{(k)}_{f,m}] = \left| \begin{matrix} P^{(k)}_{t,m} = 0{,}5 \cdot D_{1,m} + 0{,}5 \cdot D_{2,m} \\ P^{(k)}_{f,m} = 0{,}5 \cdot \alpha_m + 0{,}5 \cdot \beta_m \end{matrix} \right| =$$

$$= 0{,}5 \log_2 \left(\frac{D^{(k)}_{1,m} + D^{(k)}_{2,m}}{\alpha_m{}^{(k)} + \beta_m{}^{(k)}}\right) \cdot [(D^{(k)}_{1,m} + D^{(k)}_{2,m}) - (\alpha_m{}^{(k)} + \beta_m{}^{(k)})] =$$

$$= \log_2 \left(\frac{1 + (D^{(k)}_{1,m} - \beta_m{}^{(k)})}{1 - (D^{(k)}_{1,m} - \beta_m{}^{(k)})}\right) \cdot [D^{(k)}_{1,m} - \beta_m{}^{(k)}], \tag{5}$$

де $D^{(k)}_{1,m}$ – перша достовірність, обчислена на k-му кроці навчання розпізнавати реалізації класу X^o_m; $D^{(k)}_{2,m}$ – друга достовірність; $\alpha_m{}^{(k)}$ – помилка першого роду; $\beta_m{}^{(k)}$ – помилка другого роду.

Визначення належності деякої реалізації $x^{(j)}$, наприклад, класу X_m^o для унімодального класифікатора здійснюється за правилом

$$\text{if } d_{m-1} < d[x_m \oplus x^{(j)}] < d_m \text{ then } x^{(j)} \in X_m^o \text{ else } x^{(j)} \notin X_m^o,$$

де d_{m-1} – визначенний в процесі навчання оптимальний радіус контейнера внутрішнього класу (вкладеного), для першого(базового) класу $d_{m-1} = 0$; $d[x_m \oplus x^{(j)}]$ – кодова відстань вектора $x^{(j)}$ до центра розсіювання реалізацій x_m; $\oplus$ – символ операції складання за модулем два; d_m – поточний радіус контейнера класу X_m^o.

Нормовану модифікацію критерію (5) подамо у вигляді

$$E_m^{*(k)} = \frac{E_m^{(k)}}{E_{max}}, \tag{6}$$

тут E_{max} – значення критерію (5) при $D_{l,m}^{(k)} = 1$ *і* $\beta_m{}^{(k)} = 0$.

Наведений вище алгоритм навчання системи може не забезпечити досягнення граничного максимум інформаційного критерію (1), що згідно з принципом відкладених рішень [5] з метою побудови безпомилкового за навчальною матрицею класифікатора потребує оптимізації інших параметрів навчання, наприклад словника ознак розпізнавання.

Алгоритм екзамену за IEI-технологією базується на аналізі значень функції належності, наприклад, до класу X_m^o, яка обчислюється для кожної реалізації, що розпізнається, і для унімодального класифікатора має простий вигляд:

$$\mu_{m,j} = \begin{cases} 1, \text{ if } d_{m-1}^* < d[x_1 \oplus x^{(j)}] < d_m^*; \\ 0, \text{ if else}, \end{cases} \tag{7}$$

де $d(x_1 \oplus x^{(j)})$ – кодова відстань між еталонним вектором x_1 і реалізацією класу, що розпізнається; d_{m-1}^*, d_m^* – оптимальні радіуси контейнерів класу X_{m-1}^o, X_m^o відповідно.

Алгоритм екзамену має такі вхідні дані: M – кількість класів, які СППР навчена розпізнавати; $\{d_m^*\}$ – масиви оптимальних радіусів контейнерів та $\{\delta_{k,i}^* \mid i = \overline{1, N}\}$ – масив контрольних допусків, визначені на етапі навчання; $\{x^{(j)}\}$ – масив двійкових векторів-реалізацій образу, що розпізнається.

Розглянемо основні етапи реалізації алгоритму екзамену:

1) формування лічильника класів розпізнавання: $m := m + 1$;

2) формування лічильника числа реалізацій, що розпізнаються: $j := j + 1$;

3) обчислення кодової відстані $d(x_1 \oplus x^{(j)})$;

4) обчислення функції належності (7);

5) порівняння: якщо $j \le n$, то виконується крок 2, інакше – крок 6;

6) порівняння: якщо $m \le M$, то виконується крок 1, інакше – крок 7;

7) визначення класу X_m^o, до якого належить реалізація образу, наприклад, за умови $\bar{\mu}_m^* = \max_{\{m\}} \bar{\mu}_m$, де $\bar{\mu}_m = \frac{1}{n} \sum_{j=1}^{n} \mu_{m,j}$ – усереднене значення функцій належності для реалізацій класу X_m^o, або видача повідомлення: «Клас не визначено», якщо $\bar{\mu}_m^* \le c$. Тут c – порогове значення.

Таким чином, алгоритми екзамену у рамках IEI-технології є детермінованими і відрізняються відносно малою обчислювальною трудомісткістю, що дозволяє їх реалізовувати у реальному темпі часу.

3. Приклад реалізації алгоритму навчання унімодальної СППР

Розглянемо результати реалізації запропонованого алгоритму на прикладі навчанні СППР для керування вирощуванням монокристала на установці типу "РОСТ"[6,7] за методом Чохральського в НТК «Інститут монокристалів» (м. Харків). Тривалість часового інтерва-

лу дорівнювала п'яти годинам від початку вирощуванняю За архівною історією декількох вирощувань та даними кінцевого лабораторного контролю якості оптичних характеристик та діаметра монокристала вздовж вирощеної булі для даного інтервалу було сформовано вхідну апріорно класифіковану навчальну матрицю для трьох класів, що характеризували якість монокристала за трьохалтернативною системою оцінок: «Норма», «Менше норми» і «Більше норми». При цьому кількість ознак розпізнавання дорівнювала 35, із них 10 первинних ознак, взяті з трендів котролю за тепловими умовами росту та станом розплаву в тиглі, решта – вторинні ознаки – є різницями першого та другого порядків над динамічними трендами первинних ознак розпізнавання. Як базовий було обрано клас X_1^o, що характеризував стан діаметра монокристала «Більше норми». Клас X_2^o «Норма» характеризував незначні відхилення діаметр монокристала від заданого і клас X_3^o – «Менше норми».

На рис. 1 показано графік залежності нормованого критерію Кульбака (6) від параметра поля контрольних допусків δ (*delta*), одержаний в процесі навчання СППР з паралельною оптимізацією контрольних допусків на ознаки розпізнавання. На графіку штрихована ділянка позначає робочу область визначення функції інформаційного критерію, в якій одночасно виконуються умови: $D_{1,m} > 0{,}5$, $D_{2,m} > 0{,}5$, і $d_m > d_{m-1}$.

Аналіз рис.1 показує, що оптимальний параметр поля контрольних допусків дорівнює $\delta^* = \pm 1$ (у відносних одиницях) при значенні максимуму усередненого критерію $\overline{E}^* = 0{,}1$.

Таким чином, відновлений в процесі навчання класифікатор не є безпомилковим за навчальною матрицею і для підвищення його функціональної ефективності було реалізовано алгоритм послідовної оптимізації СКД на ознаки розпізнавання (4). При цьому одержані в процесі паралельної оптимізації квазіоптимальні контрольні допуски в алгоритмі послідовної оптимізації приймаються як стартові, що дозволяє суттєво підвищити оперативність навчання СППР через те, що оптимізація параметрів плану навчання здійснюється тільки в робочій області визначення функції інформаційного КФЕ (6).

Динаміку зміни значення максимуму усередненого критерію $\overline{E}^*$ при оптимізації СКД за послідовним алгоритмом показано на рис. 2.

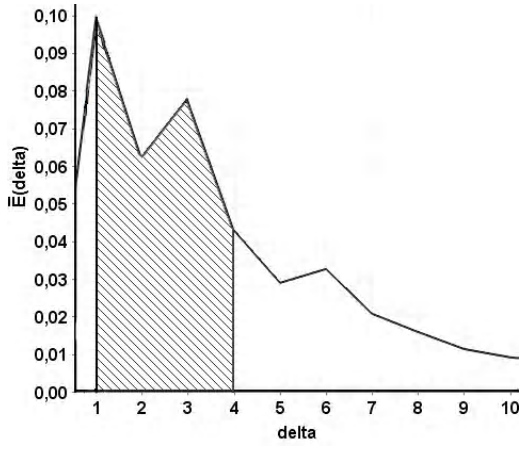


Рис. 1. Графік залежності критерію Кульбака параметра поля контрольних допусків

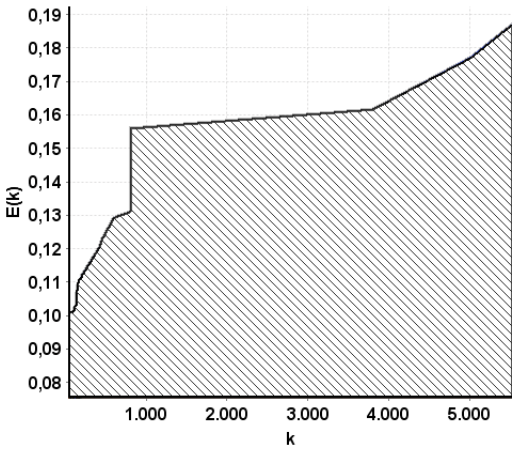


Рис. 2. Графік зміни максимального усередненого від значення КФЕ при оптимізації СКД за послідовним алгоритмом

Оскільки метою навчання СППР є відновлення в просторі ознак оптимальних контейнерів класів розпізнавання, то на рис.3 і 4 наведено графіки залежності нормованого КФЕ (6) від радіусів контейнерів класів X_1^o і X_2^o.

Аналіз рис.3 показує, що оптимальний радіус контейнера класу X_1^0 дорівнює $d_1^* = 28$ кодових одиниць при максимальному значенні КФЕ $E_1^* = 0{,}208$.

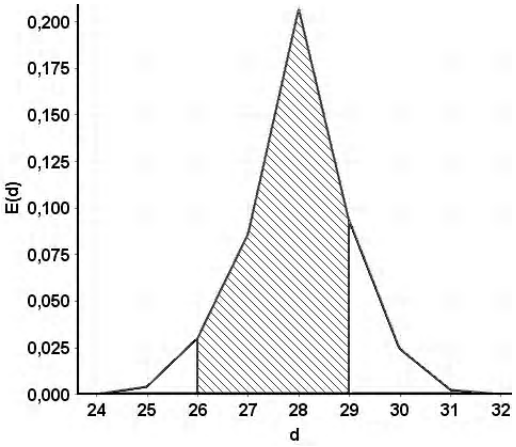


Рис. 3. Графік залежності критерію Кульбака від радіуса контейнера класу X_1^0

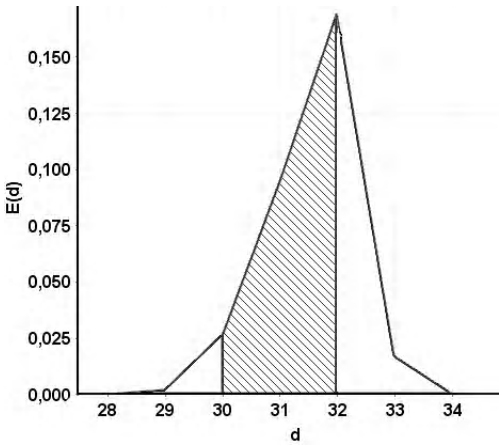


Рис. 4. Графік залежності критерію Кульбака від радіуса контейнера класу X_2^0

Аналіз рис. 4 показує, що для класу X_2^0 оптимальний радіус його контейнера дорівнює $d_2^* = 32$ кодових одиниць при максимальному значенні КФЕ $E_2^* = 0{,}170$.

Таким чином, порівняльний аналіз рис.1 і 2 показує, що паралельно-послідовна оптимізація контрольних допусків дозволила майже вдвічі підвищити функціональну ефективність навчання СППР.

Висновки

1. У рамках IEI-технології розроблено інформаційне, алгоритмічне та програмне забезпечення унімодального класифікатора для оцінки діаметра монокристала за трьохальтернативною системою оцінок: «Норма», «Менше норми» і «Більше норми», яке дозволяє надати АСК властивість адаптивності через навчання СППР за рахунок збільшення частоти та точності оцінок в процесі вирощування.

2. Поєднання паралельного та послідовного алгоритму в оптимізації дозволяє підвищити достовірність прийняття рішень на етапі екзамену, проте для побудови безпомилкового за навчальною матрицею класифікатора згідно з принципом відкладених рішень необхідна оптимізація інших параметрів навчання, наприклад словника ознак розпізнавання.

3. Основна відмінність унімодального класифікатора від мультимодального полягає у відновленні в процесі навчання контейнерів класів розпізнавання з єдиним геометричним центром, що у більшій мірі відповідає реальному розподілу векторів-реалізацій впорядкованих класів розпізнавання у бінарному просторі ознак.

Список літератури: 1. *Симанков В.С.* Адаптивное управление сложными системами на основе теории распознавания образов / В.С. Симанков, Е.В. Луценко. Краснодар: Техн. ун-т Кубан. гос. технол. ун-та. 1999. 318 с. **2.** *Довбиш А.С.* Основи проектування інтелектуальних систем: Навчальний посібник / А.С. Довбиш. Суми: Видавництво Сум ДУ, 2009. 171 с. **3.** *Довбиш А.С.* Інтелектуальна система підтримки прийняття рішень для керування вирощуванням монокристалів / А.С. Довбиш, В.С. Суздаль, В.В Москаленко // Вісник СумДУ. Серія технічні науки. 2011. №2. С. 39-47. **4.** *Кульбак С.* Теория информации и статистика: Пер. с англ./ С. Кульбак. М.: Наука, 1967. 408 с. **5.** *Ивахненко А.Г.* О принципах построения обучающихся систем управления сложными процесами / А.Г. Ивахненко. М.: Наука. 1970. 252 с. **6.** *Горилецкий В.И.* Рост кристаллов / В.И. Горилецкий, Б.В. Гринёв, Б.Г. Заславский, Н.Н. Смирнов, В.С. Суздаль. Харків: Акта, 2002. 536с. **7.** *Суздаль В.С.* Сцинтилляционные монокристаллы: автоматизированное выращивание / В.С.Суздаль, П.Е. Стадник, Л.И. Герасимчук, Ю.М. Епифанов. Харьков: «ИСМА», 2009. 260 с.

Надійшла до редколегії 02.09.2011

Москаленко В'ячеслав Васильович, аспірант каф. комп'ютерних наук СумДУ. Наукові інтереси: інтелектуальні системи автоматизованого керування. Адреса: Україна, 40007, Суми, вул. Римського-Корсакова, 2, e-mail: systemscoders@gmail.com.

Шелехов Ігор Володимирович, канд. техн. наук, ст. викладач каф. комп'ютерних наук СумДУ. Наукові інтереси: аналіз і синтез інтелектуальних адаптивних СППР, що навчаються. Адреса: Україна, 40007, Суми, вул. Римського-Корсакова,2, e-mail: igor-i@ukr.net.

Соболєв Олександр Вікторович, канд. техн. наук, науковий співробітник НТК "Інститут монокристалів". Наукові інтереси: системи багатовимірного робастного керування. Адреса: Україна, 61178, Харків, пр. Леніна, 60, e-mail: sobolev@isma.kharkov.ua.

УДК 681.323

П.О. КРАВЧЕНКО

УДОСКОНАЛЕНИЙ МЕТОД ГЕНЕРАЦІЇ ТА ВИДАЧІ КЛЮЧІВ ДЛЯ КОМБІНОВАНИХ ІНФРАСТРУКТУР ВІДКРИТИХ КЛЮЧІВ

Описується удосконалений метод генерації таємного ключа для комбінованої інфраструктури відкритих ключів, який відрізняється паралельними запитами користувача до розподіленого уповноваженого на генерацію ключів та формуванням особистого ключа користувачем, що дозволяє збільшити показники доступності для розподіленого уповноваженого на генерацію ключів.

Вступ

Однією з альтертатив інфраструктурі відкритих ключів (ІВК) на базі X.509 є ІВК на базі ідентифікаторів та комбіновані ІВК, що поєнують переваги обох інфраструктур. Однак одним з важливих проблемних питань, яке потребує рішення, є низька криптоживучість такої ІВК. Це пояснюється тим, що при компрометації майстер-ключа ІВК на ідентифікаторах зловмисник може обчислити усі особисті ключі користувачів. Для вирішення цього проблемного питання застосовують криптоживучі ІВК на ідентифікаторах, що характеризуються розподіленим уповноваженим на генерацію ключів (УГК). Майстер-ключ розподіляється між декількома серверами за деяким алгоритмом, що дозволяє відновити його тільки у разі участі необхідної кількості серверів. Архітектура криптоживучої комбінованої ІВК наведена на рис. 1.

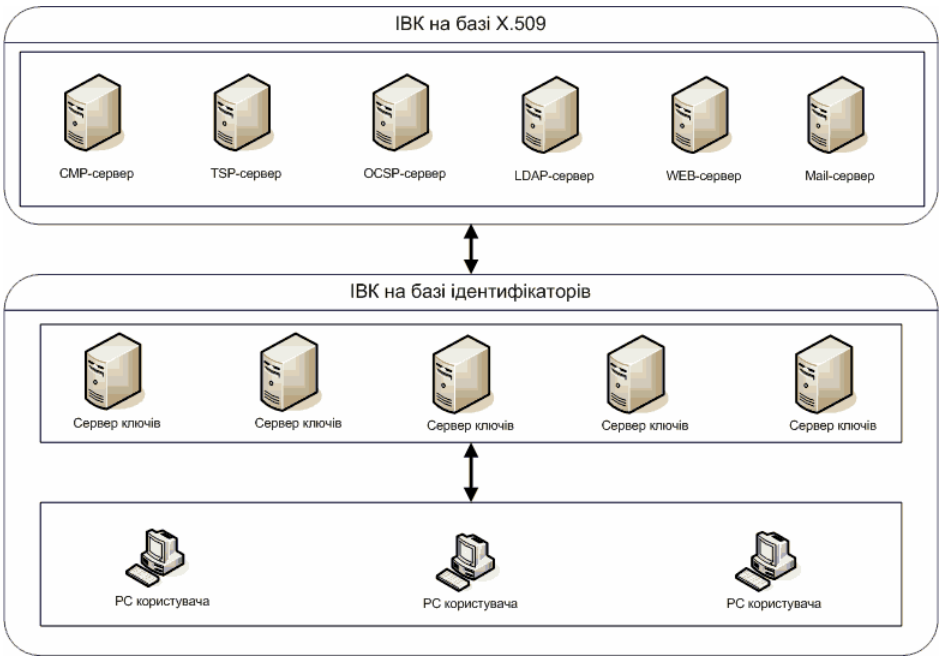


Рис. 1. Архітектура криптоживучої комбінованої ІВК

Для генерації особистого ключа користувача у криптоживучій комбінованій ІВК застосовують методи генерації та видачі ключів. Наведемо вимоги, яким повинні задовільняти протоколи, що є реалізацією таких методів:

– експоненційна складність атаки “груба сила” зі сторони уповноваженого на генерацію ключів;

– неможливість обчислення особистого ключа меншою, ніж порогова, кількістю серверів;

– відсутність автентифікованого та конфіденційного каналу зв’язку;

– забезпечення доступності розподіленого уповноваженого на генерацію ключів.

Ціль – розробка удосконаленого методу генерації та видачі ключів для комбінованої ІВК, який би задовольняв висунутим вимогам.

Об'єкт дослідження – процеси криптографічних перетворень у ІВК при реалізації процесів генерації ключів.

Предмет дослідження – метод генерації та видачі особистих ключів користувачів для криптоживучої комбінованої ІВК.

1. Існуючі рішення відносно генерації та видачі ключів

Розглянемо протоколи, що не потребують конфіденційного каналу зв'язку між користувачем та розподіленим уповноваженим на генерацію ключів.

У роботі [1] Lee запропонував протокол, який дозволяв виробляти особистий ключ без необхідності у конфіденційному каналі звязку. Користувачу необхідно реєструватися тільки у одному з множини розподілених УГК. При подальших дослідженнях Gangishetti [2] знайшов серйозні вразливості такого протоколу, на основі яких були проведені успішні атаки. Також Chunxiang [3] показав, що центр генерації може успішно провести атаку, яка дозволить йому отримати особистий ключ будь-якого користувача.

Протокол Kumar [4] використовує ідею, запропоновану Lee, але в ньому використана схема, що дозволяє генерувати особистий ключ користувача t серверам з n (t<n), але процесом генерації керує єдиний уповноважений на генерацію ключів. Суттєвим недоліком цього протоколу є те, що УГК може імітувати користувача при умові компрометації хоча б одного з серверів генерації [5].

Протокол Мелецького використовує схожу на Lee схему (рис. 2), але стійкий до усіх відомих атак. Недоліком такого протоколу є те, що у разі виведення з ладу хоча б одного сервера уся система перестане функціонувати.

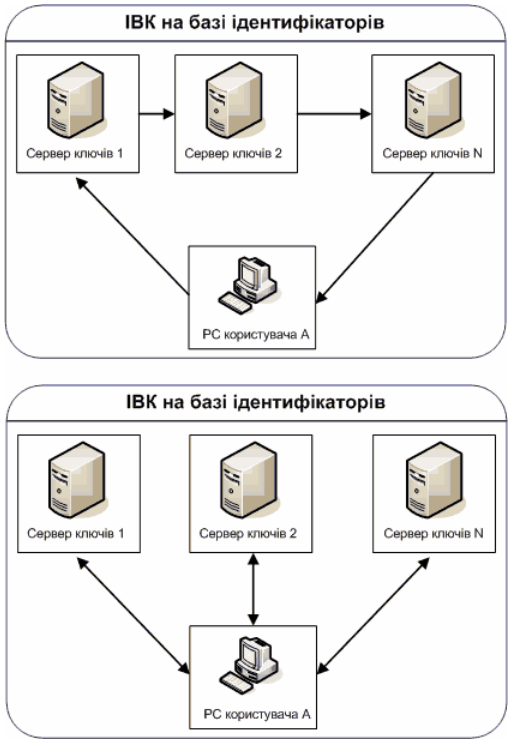


Рис. 2. Схема методу генерації ключів Lee, Мелецького

Відзначимо, що даний недолік властивий усім наведеним протоколам, тому що особистий ключ користувача виробляє уповноважений на генерацію ключів, і його доступність критична для роботи системи.

2. Удосконалений метод генерації та видачі ключів

Відзначимо, що основними відмінностями удосконаленого методу є паралельні запити до уповноважених на генерацію ключів та формування особистого ключа користувачем самостійно (рис. 3).

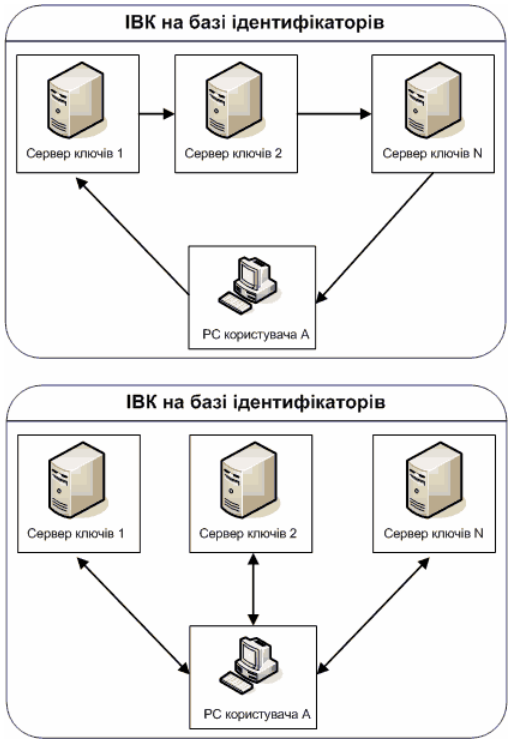


Рис. 3. Схема удосконаленого методу генерації ключів

Удосконалений метод генерації ключів характеризується такими етапами.

Етап 1. Ініціалізація. Здійснюється у такій послідовності:

– налаштування та установка параметрів серверів генерації;

– налаштування забезпечення користувача та реєстрація його в системі;

– виконання протоколу та вироблення по необхідності ключів.

Налаштування та системна установка усіх УГК виконується так:

Усі n УГК разом обирають просте число q, дві групи G_1, G_2 порядку q_i та білінійне відображення Вейля або Тейта $e : G_1 \times G_1 \to G_2$ та генератор групи $P \in G_1$. Далі обираються криптографічні геш-функції $H_1 : \{0,1\}^* \to G_1$ та $H_2 : G_2 \to \{0,1\}^l$ для деякого l.

Генерується майстер-ключ системи $S < p$, де p – просте число, порядок групи точок ЕК. Будується многочлен $a_{n-1}x_i^{\left\lfloor \frac{n+1}{2} \right\rfloor - 1} + ... + a_1 x_i + S = 0$. Згідно зі схемою Лагранжа, обчислюються частки s_i ключа для кожного сервера генерації. Кожен сервер генерації обчислює його відкритий ключ $P_i = s_i P$. Таким чином, будь-які $\left\lfloor \frac{n+1}{2} \right\rfloor$ з n УГК.

Обчислюється загальносистемний відкритий ключ $Y_N = SP$. Номери k_i кожного сервера запам'ятовуються.

Отже, публікуються або є доступними для усіх користувачів такі загальносистемні параметри: $Params = \{G_1, G_2, e, H_1, H_2, P, P_0, P_1, ...P_n, k_1, k_2, k_n, Y_N\}$.

Етап 2. Реєстрація користувача. Користувач обирає відкритий ідентифікатор ID, обчислює відповідний відкритий ключ Q_{ID} та виробляє довгостроковий секрет x. Далі користувач проходить реєстрацію на кожному сервері генерації та надає йому шляхом, що забезпечує цілісність, параметр xQ_{ID}, xP_i. Центр генерації перевіряє його правильність за допомогою обчислення та перевірки умов: $e(xQ_{ID}, P_i) = e(Q_{ID}, xP_i)$ та зберігає дані, отримані від користувача у власній базі даних. Як результат, користувачу видається доказ реєстрації у вигляді $prf_{ID} = s_i H(ID \| xQ_{ID})$.

Користувач перевіряє доказ реєстрації за допомогою рівності $e(prf_{ID}, P) = e(H(ID \| xQ_{ID}), P_i)$. При позитивному результаті процедура реєстрації вважається успішною.

Етап 3. Паралельний запит часткових ключів користувачем. Користувач здійснює запит до кожного ЦГ, надсилаючи йому кортеж $\{ID, x^{-1}P\}$.

Отримавши кортеж, ЦГ вибирає зі своєї БД xQ_{ID}, яке відповідає даному ID, та перевіряє справжність отриманої інформації: $e(x^{-1}P, xQ_{ID}) = e(P, Q_{ID})$. Якщо кортеж справжній, то ЦГ множить значення xQ_{ID} на свій таємний ключ s_i та надсилає повідомлення $\{ID, s_i xQ_{ID}\}$ користувачу.

Етап 4. Вироблення та перевірка особистого ключа користувачем. Користувач, отримавши $t \geq k$ відповідей, обирає з них будь-які k, множить кожне на x^{-1} та отримує кортеж $(s_0 Q_{ID}, s_1 Q_{ID}, s_N Q_{ID})$. Користувач будує систему рівнянь:

$$\begin{cases} a_{n-1}k_i^{n-1} + ... + a_1 k_i + a_0 = s_i Q_{ID} \pmod p, \\ a_{n-1}k_j^{n-1} + ... + a_1 k_j + a_0 = s_j Q_{ID} \pmod p, \\ a_{n-1}k_t^{n-1} + ... + a_1 k_t + a_0 = s_t Q_{ID} \pmod p, \end{cases} \quad (1)$$

де s_i, s_j, s_t – особисті ключі серверів генерації, до яких звертався користувач; $a_0 = S$ – таємний ключ системи (що був розподілений серверами генерації).

Користувач будує многочлен Лагранжа:

$$F(x) = \sum_i l_i(x) y_i \pmod p,$$

тут $l_i(x) = \prod \frac{x - x_j}{x_i - x_i} \pmod p$.

Користовач виконує підстановку значень k_i замість x_i, розв'язує систему (1) та отримує коєфіцієнт многочлена $a_{n-1}Q_{ID}, ... a_1 Q_{ID}, a_0 Q_{ID}$. Коєфіцієнт $a_0 Q_{ID} = SQ_{ID}$ буде таємним ключем користувача.

Користувач перевіряє справжність отриманого особистого ключа SQ_{ID} за допомогою рівності $e(SQ_{ID}, P) = e(Q_{ID}, P_{sys})$. При позитивному результаті перевірки він приймає отриманий ключ як особистий.

3. Обчислення показників стійкоті та доступності

Стійкість протоколу базується на інтерполяційній формулі Лагранжа, а також залежить від довжини модуля перетворень P і довжин S_i -х часток секрету. Розглянемо можливі атаки на схему Шаміра. Основною задачею атак є визначення загального секрету $S = a_0$. Величину a_0 можна визначити безпосередньо або через приватні секрети $f(l_i), ..., f(l_k)$. Якщо $a_0 = S$ і формується довіреною стороною випадково, то складність атаки типу "груба сила" за визначенням a_0 можна оцінити через імовірність P_0 її здійснення:

$$P_0 = \frac{1}{p-2} \approx \frac{1}{p} = p^{-1}. \quad (2)$$

Складність атаки "груба сила" за визначенням a_0 через $f(i_1), ..., f(i_k) \in GF(p)$ можна оцінити як

$$P_f = \left(\frac{1}{(p-1)^k} \right) = (p-1)^{-k} \approx p^{-k}. \quad (3)$$

Попередні порівняння (2) і (3) показують, що краща є атака за безпосереднім визначенням a_0. Складність цієї атаки залежить тільки від величини модуля p. Якщо p – відкритий загальносистемний параметр, відомий криптоаналітику, то складність атаки можна визначити також через безпечний час:

$$T_б = \frac{I_0}{\zeta K} \approx \frac{p}{\zeta K}, \qquad (4)$$

де $I_0 \approx p$ – число спроб підбору значення a_0 з імовірністю 1; ζ – продуктивність криптоаналітичної системи; $K = 3{,}1 \cdot 10^7$ с/рік – кількість секунд у році.

Доведемо твердження.

Твердження. Припустимо, що майстер-ключ S розподілений між n об'єктами, з яких $\left\lfloor \frac{n+1}{2} \right\rfloor$ мають змогу відтворити ключ, тобто використовується порогова схема Лагранжа $(\left\lfloor \frac{n+1}{2} \right\rfloor, n)$. Приймемо, що ймовірність успішної атаки на відмову в обслуговуванні на об'єкт дорівнює p та що усі атаки на об'єкти незалежні. Тоді ймовірність P ненадання послуги доступність $\left\lfloor \frac{n+1}{2} \right\rfloor$ об'єктами оцінюється, відповідно для базового та удосконаленого методу, співвідношеннями $P = 1 - (1-p)^n$ та $P = \sum_{k=\left\lfloor \frac{n+1}{2} \right\rfloor}^{n} C_n^k \cdot p^k \cdot (1-p)^{n-k}$.

Доведення. Для випадку базового методу обчислимо ймовірність неуспішності атаки $P_{неусп}$. Очевидно, що $P_{неусп} = (1-p)$. Враховуючи, що атаки на усі n обєктів незалежні, отримаємо ймовірність неуспішності атаки на n обєктів як $P^n{}_{неусп} = (1-p)^n$. Тоді ймовірність успішної атаки хоча б на один з n обєктів дорівнює $P = 1 - (1-p)^n$. Для удосконаленого методу використаємо формулу Бернуллі та розрахуємо ймовірність виведення з ладу $\left\lfloor \frac{n+1}{2} \right\rfloor, \left\lfloor \frac{n+1}{2} \right\rfloor + 1, .. n$ серверів. Ймовірність виведення з ладу $\left\lfloor \frac{n+1}{2} \right\rfloor$ серверів дорівнює $P_{неусп} = C_n^{\left\lfloor \frac{n+1}{2} \right\rfloor} \cdot p^{\left\lfloor \frac{n+1}{2} \right\rfloor} \cdot (1-p)^{\left(n - \left\lfloor \frac{n+1}{2} \right\rfloor\right)}$. Тоді ймовірність ненадання послуги доступність буде визначатися співвідношенням $P = \sum_{k=\left\lfloor \frac{n+1}{2} \right\rfloor}^{n} C_n^k \cdot p^k \cdot (1-p)^{n-k}$.

Показники доступності та конфіденційності для ймовірності $P = 0.1$ успішної атаки на відмову в обслуговуванні та ймовірності компрометації $P = 0.0001$ системи наведені у таблиці. За прототип візьмемо метод Мелецького.

Прототип			**Удосконалений метод**		
Кількість серверів	Ймовірність виходу з ладу	Ймовірність компрометації	Кількість серверів	Ймовірність виходу з ладу	Ймовірність компрометації
2	0.19	1.00E-008	2	0.19	1.00E-008
3	0.27	1.00E-012	3	0.028	1.00E-008
4	0.34	1.00E-016	4	0.0523	1.00E-012
5	0.41	1.00E-020	5	0.0085	1.00E-012

На рис. 4 наведено графік залежності ймовірності виходу з ладу системи від ймовірності успішності атаки на відмову в обслуговуванні для 5 серверів відповідно для базового (верхній) та удосконаленого (нижній) методу.

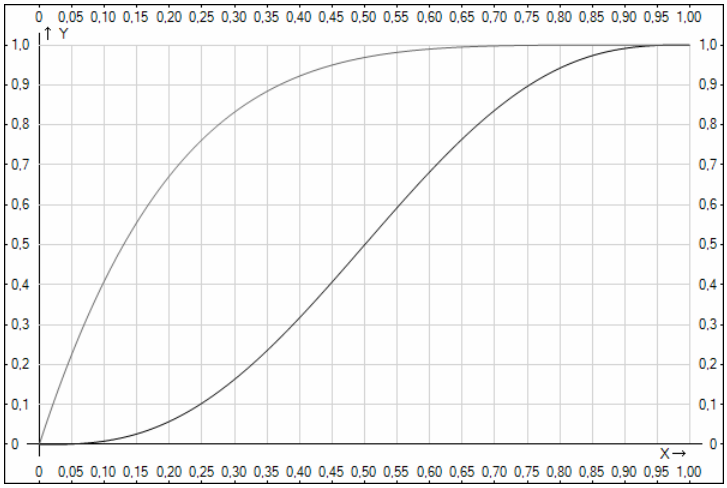


Рис. 4. Схема удосконаленого методу генерації ключів

Висновки

Наукова новизна представлена методом генерації таємного ключа для комбінованої інфраструктури відкритих ключів, який відрізняється паралельними запитами користувача до розподіленого уповноваженого на генерацію ключів та формуванням особистого ключа користувачем, що дозволяє збільшити показники доступності для розподіленого уповноваженого на генерацію ключів.

Практична значущість полягає у можливості побудови криптоживучої комбінованої ІВК, що відповідає вимогам наданню послуги доступність.

Зазначимо, що основними недоліками системи є збільшення її компонентів для досягнення тієї ж ймовірності компрометації. Проте рішення про застосування такої системи буде прийнято згідно з вимогами, що пред'являються до неї.

Перелік літератури: **1**. *Lee B., Boyd C., Dawson E., Kim K., Yang J., Yoo S.* Secure key issuing in ID-based cryptography, ACS Conferences in Research and Practice in Information Technology 32. 2004. P. 69-74. **2**. *Gangishetti R., Choudary Gorantla M., Lal Das M., Saxena A*. Cryptoanalysis of key issuing protocols in ID-based cryptosystems, IMSCCS, 2006. P. 8-12. **3**. *Chunxiang X., Junhui Z., Zhiguang Q.* A note on secure key issuing in ID-based cryptography. Technical report, 2005, http://eprint.iacr.org/2005/180.pdf. 4 p. **4**. *Kumar K.P., Shailaja G., Saxena A*. Secure and efficient threshold key issuing protocol for ID-based cryptosystems. IACR Cryptology ePrint Archive, 2006, 10 p. **5**. *Горбенко І.Д.* Удосконалений протокол вироблення ключів з асиметричними криптографічними перетвореннями зі спарюванням точок еліптичних кривих на базі ідентифікаторів / І.Д. Горбенко, П.О. Кравченко, О.П. Мелецький // Радиотехника. Харьков, 2006. Вып. 147. С.99-106.

Надійшла до редколегії 27.08.2011

Кравченко Павло Олександрович, аспірант каф. БІТ ХНУРЕ. Наукові інтереси: інфраструктури відкритих ключів. Адреса: Україна, 61166, Харків, пр. Леніна, 14, тел: 702-18-07, E-mail: kravchenkopo@gmail.com.

УДК 519.7

Н.Е. РУСАКОВА

МОДЕЛЬ ЛОГИЧЕСКОГО ОПЕРАТОРА С УПРАВЛЯЕМЫМ ЯДРОМ

Рассматриваются линейные логические операторы с управляемым ядром, являющиеся основным решающим средством в реляционных сетях, которые в свою очередь рекомендуются на роль универсального решателя высокопроизводительных мозгоподобных структур. Приводится модель логического оператора с управляемым ядром, которая характеризуется введением в вычисление этого оператора множителей и благодаря которой появляется возможность построения схемы отдельной ветви реляционной сети для переменных множеств и соответствий.

Введение

Язык алгебры предикатов представляет собой универсальное средство формального описания любых механизмов интеллекта человека и машин. Разработчики, проектирующие средства искусственного интеллекта, используют алгебру предикатов для начального формального описания моделей. Следующим этапом является алгебра предикатных операций, на которой выражаются любые действия над отношениями. Отношения выражают свойства предметов и связи между ними. Они представляют собой универсальное средство формального описания любых объектов [1].

Каждая модель логической сети характеризуется своим предикатом модели. Однако предикаты лишь описывают конкретную модель логических сетей. А для того, чтобы сеть функционировала, т.е. чтобы из нее можно было извлечь некоторые знания, необходимо решать систему логических уравнений [2]. Для решения логических уравнений часто используют линейные логические операторы [1,3].

Целью исследования является разработка модели логического оператора с управляемым ядром, которая позволяет понять процесс, происходящий в ветвях реляционной сети и построить схему отдельной ветви.

1. Линейные логические операторы

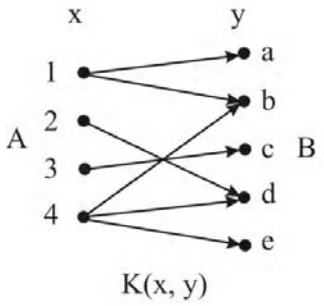
Механизм, решающий уравнения алгебры предикатов, называется реляционной сетью. Такое название мотивировано тем, что, во-первых, мозг человека реализует нейронную сеть; во-вторых, с психологической точки зрения механизм мышления представляется как ассоциативная сеть; в-третьих, с математической точки зрения механизм мышления предстает как устройство для обработки отношений (по англ. relation). Реляционная сеть состоит из полюсов и ветвей, соединяющих полюсы. Пара полюсов x и y, соединенных ветвью $K(x, y)$, реализуют линейный логический оператор первого и второго рода. Сеть называется первого рода, если в ней действуют лишь операторы первого рода. Аналогично определяются сети второго рода. Если в сети используются операторы обоих видов, сеть называется комбинированной.

Существует взаимно-однозначное двумерное соответствие между всеми предикатами $K(x, y)=1$ на $A\times B$ и всеми соответствиями $K(x, y)$ на $A\times B$. Соответствиями называются отношения, задаваемые бинарными предикатами. Алгебру одноместных предикатов можно содержательно рассматривать как алгебру множеств, двуместных – как алгебру соответствий.

Вычисление СДНФ двуместного предиката производится по следующей формуле:

$$K(x, y) = \bigvee_{(\sigma,\varepsilon)\in A\times B} K(\sigma,\varepsilon)x^{\sigma}y^{\varepsilon}. \qquad (1)$$

Пусть $x \in A,\ y \in B$, $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d, e\}$. Представим пример двудольного графа двуместного предиката и соответствующую ему таблицу предиката (рис.1).



x	y	a	b	c	d	e
	1	1	1	0	0	0
	2	0	0	0	1	0
	3	0	0	1	0	0
	4	0	1	0	1	1

K(x, y)

Рис. 1. Представление предиката в виде таблицы и двудольного графа

СДНФ предиката согласно формуле (1) имеет вид:

$$K(x,\ y) = K(1,a)x^1y^a \vee ... \vee K(3,b)x^3y^b \vee ... \vee K(4,e)x^4y^e = 1\cdot x^1y^a \vee ... \vee 0\cdot x^3y^b \vee ... \vee 1\cdot x^4y^e =$$
$$= x^1y^a \vee x^1y^b \vee x^2y^d \vee x^3y^c \vee x^4y^b \vee x^4y^d \vee x^4y^e . \qquad (2)$$

Равенство $K(1,a) = 1$ равносильно утверждению, что предмет $y = a$ есть образ предмета $x = 1$ относительно соответствия $K(x,\ y)$. Полный образ предмета x может быть вычислен с помощью дизъюнктивного разложения предиката:

$$\exists\sigma \in A(x^\sigma \cdot K(\sigma,\ y)) = Q(y) . \qquad (3)$$

Приведем пример отыскания полного образа $Q(y)$ предмета $x = 1$ для соответствия (3):

$$Q(y) = \exists\sigma \in \{1,\ 2,\ 3,\ 4\}(x^\sigma \cdot (x^1(y^a \vee y^b) \vee x^2y^d \vee x^3y^c \vee x^4(y^b \vee y^d \vee y^e))) =$$
$$= (1^1 \cdot (1^1(y^a \vee y^b) \vee 1^2y^d \vee 1^3y^c \vee 1^4(y^b \vee y^d \vee y^e))) \vee (1^2 \cdot (1^1(y^a \vee y^b) \vee 1^2y^d \vee 1^3y^c \vee 1^4(y^b \vee y^d \vee y^e))) \vee$$
$$\vee (1^3 \cdot (1^1(y^a \vee y^b) \vee 1^2y^d \vee 1^3y^c \vee 1^4(y^b \vee y^d \vee y^e))) \vee$$
$$\vee\ (1^4 \cdot (1^1(y^a \vee y^b) \vee 1^2y^d \vee 1^3y^c \vee 1^4(y^b \vee y^d \vee y^e))) = y^a \vee y^b .$$

Следовательно, $Q = \{a,\ b\}$ – полный образ предмета $x = 1$. Полный прообраз P предмета y может быть вычислен по формуле

$$\forall\sigma \in B(y^\sigma \supset K(\sigma, y)) = P(x) . \qquad (4)$$

Приведем пример отыскания полного образа $P(x)$ предмета $y = b$ для соответствия (2):

$$P(x) = \forall\sigma \in \{a,\ b,\ c,\ d,\ e\}(y^\sigma \supset (x^1(y^a \vee y^b) \vee x^2y^d \vee x^3y^c \vee x^4(y^b \vee y^d \vee y^e))) =$$
$$= (b^a \supset (x^1(b^a \vee b^b) \vee x^2b^d \vee x^3b^c \vee x^4(b^b \vee b^d \vee b^e))) \wedge$$
$$\wedge\ (b^b \supset (x^1(b^a \vee b^b) \vee x^2b^d \vee x^3b^c \vee x^4(b^b \vee b^d \vee b^e))) \wedge$$
$$\wedge (b^c \supset (x^1(b^a \vee b^b) \vee x^2b^d \vee x^3b^c \vee x^4(b^b \vee b^d \vee b^e))) \wedge$$
$$\wedge\ (b^e \supset (x^1(b^a \vee b^b) \vee x^2b^d \vee x^3b^c \vee x^4(b^b \vee b^d \vee b^e))) = x^1 \vee x^4 .$$

Полным прообразом предмета $y = b$ будет множество $P = \{1,\ 4\}$.

Максимальным образом множества $P \subseteq A$ относительно соответствия $K(x,\ y) = 1$ называется множество $Q_{max} \subseteq B$, представляющее собой объединение образов всех предметов $x \in P$. Этот образ вычисляется по формуле:

$$\exists x \in A(P(x) \cdot K(x,\ y)) = Q_{max}(y) . \qquad (5)$$

Минимальным образом множества $P \subseteq A$ относительно соответствия $K(x,\ y) = 1$ называется множество $Q_{min} \subseteq B$, представляющее собой пересечение образов всех предметов $x \in P$ и вычисляется по формуле:

$$\forall x \in A(P(x) \supset K(x,\ y)) = Q_{min}(y) . \qquad (6)$$

Преобразование $\mathcal{F}(P) = Q_{max}$ вида (5) обладает аддитивностью $\mathcal{F}(P_1 \vee P_2) = \mathcal{F}(P_1) \vee \mathcal{F}(P_2)$ относительно операции дизъюнкции и однородностью $\mathcal{F}(\alpha P) = \alpha\mathcal{F}(P)$ относительно операции конъюнкции, $\alpha \in \{0,\ 1\}$. Это преобразование называется линейным логическим оператором

первого рода. Преобразование $\Upsilon(P) = Q_{min}$ вида (6) обладает аддитивностью $\Upsilon(P_1 \wedge P_2) = \Upsilon(P_1) \wedge \Upsilon(P_2)$ относительно операции конъюнкции и однородностью $\Upsilon(\alpha \vee P) = \alpha \vee \Upsilon(P)$ относительно операции дизъюнкции. Такое преобразование называется линейным логическим оператором второго рода. Предикат $K(x, y)$ называется ядром линейного логического оператора. Именно они описывают основные действия реляционной сети, реализующей процессы мышления в числовой природе и в технике.

Найдем значения линейных логических операторов первого и второго рода для соответствия (2). Подадим на вход линейного логического оператора множество $P = \{1, 4\}$. Согласно формуле (5) имеем:

$$Q_{max}(y) = \exists x \in \{1,\ 2,\ 3,\ 4\}((x^1 \vee x^4) \wedge\ (x^1(y^a \vee y^b) \vee x^2 y^d \vee x^3 y^c \vee x^4(y^b \vee y^d \vee y^e))) =$$
$$= ((1^1 \vee 1^4) \cdot (1^1(y^a \vee y^b) \vee 1^2 y^d \vee 1^3 y^c \vee 1^4(y^b \vee y^d \vee y^e))) \vee$$
$$\vee\ ((2^1 \vee 2^4) \cdot (2^1(y^a \vee y^b) \vee 2^2 y^d \vee 2^3 y^c \vee 2^4(y^b \vee y^d \vee y^e))) \vee$$
$$\vee((3^1 \vee 3^4) \cdot (3^1(y^a \vee y^b) \vee 3^2 y^d \vee 3^3 y^c \vee 3^4(y^b \vee y^d \vee y^e))) \vee$$
$$\vee((4^1 \vee 4^4) \cdot (4^1(y^a \vee y^b) \vee 4^2 y^d \vee 4^3 y^c \vee 4^4(y^b \vee y^d \vee y^e))) = y^a \vee y^b \vee y^d \vee y^e.$$

Преобразование по фомуле (6) имеет вид:

$$Q_{min}(y) = \forall x \in \{1,\ 2,\ 3,\ 4\}((x^1 \vee x^4) \supset$$
$$\supset (x^1(y^a \vee y^b) \vee x^2 y^d \vee x^3 y^c \vee x^4(y^b \vee y^d \vee y^e))) =$$
$$= ((1^1 \vee 1^4) \supset (1^1(y^a \vee y^b) \vee 1^2 y^d \vee 1^3 y^c \vee 1^4(y^b \vee y^d \vee y^e))) \wedge$$
$$\wedge ((2^1 \vee 2^4) \supset (2^1(y^a \vee y^b) \vee 2^2 y^d \vee 2^3 y^c \vee 2^4(y^b \vee y^d \vee y^e))) \wedge$$
$$\wedge((3^1 \vee 3^4) \supset (3^1(y^a \vee y^b) \vee 3^2 y^d \vee 3^3 y^c \vee 3^4(y^b \vee y^d \vee y^e))) \wedge$$
$$\wedge ((4^1 \vee 4^4) \supset (4^1(y^a \vee y^b) \vee 4^2 y^d \vee 4^3 y^c \vee 4^4(y^b \vee y^d \vee y^e))) =$$
$$(1 \supset y^a \vee y^b) \cdot (0 \supset y^d) \cdot (0 \supset y^c) \cdot (1 \supset y^b \vee y^d \vee y^e) = y^b.$$

Представим наглядно при помощи двудольных графов приведенные выше вычисления (рис. 2).

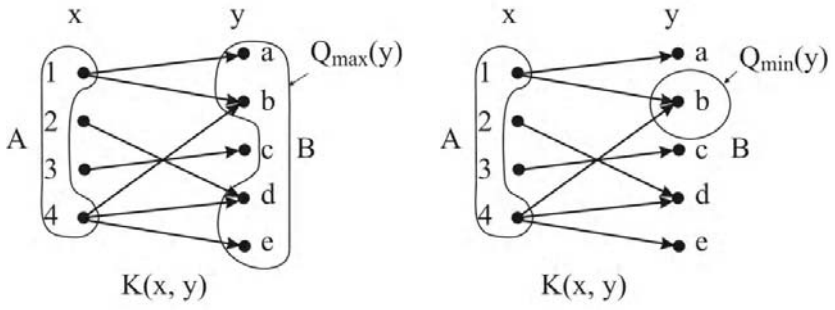


Рис. 2. Двудольные графы для вычислений $Q_{max}(y)$ и $Q_{min}(y)$

Если поменять в двудольном графе направление всех стрелок на обратные, получим дуальный граф с тем же ядром $K(x, y)$. Дуальному графу соответствуют линейный логический оператор первого рода

$$\exists y \in B(Q(y)K(x, y)) = P_{max}(x) \tag{7}$$

и второго рода

$$\forall x \in B(Q(y) \supset K(x, y)) = P_{min}(y), \tag{8}$$

называемые дуальными по отношению к операторам (5) и (6). Важно отметить, что дуальные логические операторы далеко не всегда возвращают исходное множество к первоначальному виду. Так, множество $Q_{max} = Q$, формируемое оператором (5), возвращается дуальным оператором (6) в виде более широкого множества P_{max}, чем исходное множество P (рис.3).

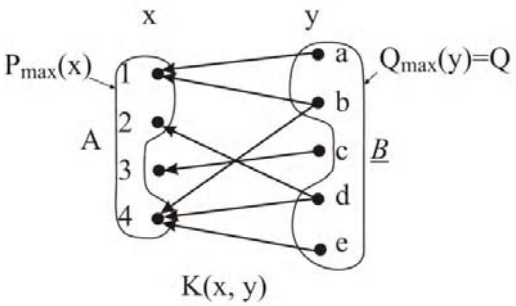


Рис.3. Дуальный двудольный граф для соответствия (2)

Линейные логические операторы представляют собой операции над переменными предикатами. Они входят составной частью в более обширную систему, называемую алгеброй предикатных операций. Алгебра предикатов служит формальным средством для записи мыслей, алгебра же предикатных операций, будучи материализована в виде решающего устройства, может служить средством искусственного воспроизведения процесса мышления.

2. Модель логического оператора с управляемым ядром

Для формирования математического действия, которое происходит в ветвях реляционной сети, разработана модель логического оператора с управляемым ядром, которая характеризуется введением в вычисление линейного логического оператора первого и второго рода множителей ξ_{a_i}, ζ_{b_j}, $\eta_{a_i b_j}$, $(i = \overline{1,k},\ j = \overline{1,l})$. Благодаря этой модели появилась возможность выполнять обсчет логических операторов для переменных множеств и соответствий.

Задав множества $A = \{a_1,\ a_2, ..., a_k\}$; $B = \{b_1,\ b_2, ..., b_l\}$, имеем следующие выражения формул (5), (6):

$$Q_{max}(y) = \bigvee_{i=1}^{k} (P(a_i) K(a_i,\ y)),\ a_i \in A, \tag{9}$$

$$Q_{min}(y) = \bigwedge_{i=1}^{k} (P(a_i) \supset K(a_i,\ y)),\ a_i \in A. \tag{10}$$

Уравнения (9) и (10), в которых переменное множество $P(a_i) = \xi_{a_i}$ и управляемое ядро $K(a_i,\ b_j) = \eta_{a_i b_j}$ заменены на соответствующие множители, будут иметь следующий вид:

$$Q_{max}(y) = \bigvee_{i=1}^{k} (\xi_{a_i} (\bigvee_{j=1}^{l} \eta_{a_i b_j} b_j^{b_j})),\ Q_{min}(y) = \bigwedge_{i=1}^{k} (\xi_{a_i} \supset (\bigvee_{j=1}^{l} \eta_{a_i b_j} b_j^{b_j})),$$

где $\xi_{a_i},\ \eta_{a_i b_j} \in \{0,\ 1\}$.

Схемы линейных логических операторов первого и второго рода представлены на рис. 4,5.

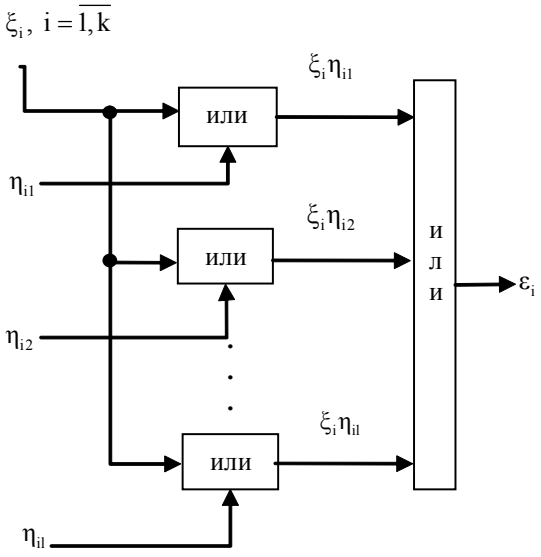


Рис. 4. Схема линейного логического оператора первого рода

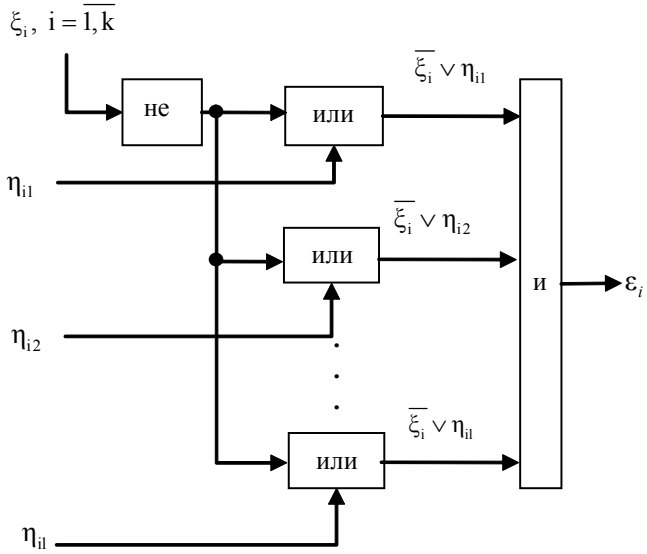


Рис. 5. Схема линейного логического оператора второго рода

Выводы

В течение каждого такта работы реляционной сети одновременно срабатывают все линейные логические операторы. В сети первого рода после каждого такта осуществляется пересечение всех множеств Q_{max}, сходящихся со всех сторон к каждому из полюсов. В сети второго рода множества Q_{min}, наоборот, объединяются. Сеть первого рода может формировать лишние решения, а второго – может не найти некоторые из действительных решений. В статье впервые предложена модель логического оператора с управляемым ядром, которая характеризуется введением в вычисление этого оператора множителей и благодаря которой появляется возможность построения схемы отдельной ветви реляционной сети для переменных множеств и соответствий. Эта модель дает возможность решать любую задачу без необходимости обучения.

Список литературы: 1. *Бондаренко М.Ф.* О реляционных сетях / М.Ф. Бондаренко, И.А. Лещинская, Н.П. Кругликова, Н.Е. Русакова, Ю.П. Шабанов-Кушнаренко // Бионика интеллекта. 2010. № 3. С. 8–13. **2.** *Закревский А.Д.* Логические уравнения. Минск: Наука и техника, 1975. 96 с. **3.** *Вечирская И.Д.* Линейные логические операторы в виде схем и графов / И.Д. Вечирская, З.В. Дударь, А.А. Иванилов, В.А. Лещинский // Бионика интеллекта. 2004. №1(61). С.38-41.

Поступила в редколлегию 29.08.2011

Русакова Наталия Евгеньевна, м.н.с. каф. программной инженерии ХНУРЭ. Научные интересы: логическая алгебра, реляционные сети, искусственный интеллект. Увлечения: спортивные бальные танцы, катание на коньках, вышивка. Адрес: Украина, 61166, Харьков, пр.Ленина, 14, тел.р.702-11-52, т. моб. 068-606-64-22. E-mail: natalium@mail.ru.

УДК 004.896

С. ЛАГА, В.А. ТИМОФЕЕВ, А.А. ШАМРАЕВ

АДАПТИВНЫЙ КРИТИЧЕСКИЙ РЕГУЛЯТОР СИСТЕМЫ УПРАВЛЕНИЯ ПРОЦЕССОМ ТРАВЛЕНИЯ ПОЛОСОВОЙ СТАЛИ

Предлагается подход к реализации цифровых регуляторов в системах управления процессом травления полосовой стали, основанный на применении моделей и методов адаптивного критического управления, позволяющих учесть характер неопределенностей объектов рассматриваемого класса. Результаты моделирования полученных цифровых алгоритмов (с использованием программной среды SCILAB) подтверждают снижение ошибки отклонения характеристик полосовой стали на выходе линии травления от заданных значений.

1. Введение

Одним из перспективных путей повышения эффективности непрерывных широкополосных станов прокатки является совершенствование систем автоматического управления ключевыми стадиями, определяющими качество выпускаемой продукции – стального проката [1]. К их числу относится технологическая линия травления полосовой стали, формирующая важные физико-механические характеристики проката. Эта линия функционирует в специфических условиях неопределенности, существенно осложняющих управление режимом травления. Часть переменных (температура конца прокатки и травильного раствора) измеряются с большой погрешностью, а некоторые возмущающие переменные и факторы (точный химсостав травильного раствора, забивка шламом углублений на поверхности проката) вообще не поддаются измерению и контролю. Наконец, существуют измеряемые возмущающие переменные (толщина и скорость движения полосы), которые оказывают существенное влияние на динамические характеристики объекта. Эффективное управление такими объектами возможно на основе математического моделирования объекта и системы управления. Математические модели должны быть нечувствительными к большим помехам и погрешностям измерения, легко адаптироваться к часто меняющимся динамическим характеристикам линии травления и удовлетворять принятым условиям адекватности. Указанным требованиям наиболее полно удовлетворяют адаптивные критические методы контроля, идентификации и управления динамическими объектами, функционирующими в условиях существенной неопределенности о характеристиках объекта и окружающей среды на основе объединения принципов теории адаптивного и критического управления [2]. При использовании критических регуляторов в системах микроконтроллерного управления процессом травления последние также приобретают аналогичные полезные свойства, отсутствующие в существующих системах управления и приводящие к снижению качества полосовой стали. Такой подход позволит в значительной мере устранить недостатки, присущие традиционным системам управления, построенным на основе детерминированных или статистических моделей.

Применение микроконтроллерной системы нагрева рабочих сред травильных ванн в высокоэффективных управляемых энергоблоках, используемых в технологических линиях травления полосовой стали, позволяет отказаться от высокопотенциального перегретого пара и перейти к использованию низкопотенциального насыщенного пара, что в свою очередь значительно уменьшает потребление природного газа при выполнении этого технологического процесса.

Целью данной работы является решение задачи синтеза цифровых регуляторов в системах управления процессом травления полосовой стали, основанным на применении моделей и методов адаптивного критического управления, позволяющих учесть характер неопределенностей объектов рассматриваемого класса.

2. Принцип критического управления динамическими объектами

Рассмотрим динамический SISO-объект, функционирующий в замкнутой системе управления $S_D(P,C)$, описываемый разностным уравнением

$$A(q)y(k) = q^{-d}B(q)u(k) + w(k), \quad (1)$$

где полиномы $A(q) \in R[q,n]$ $a_0 = 1$, $B(q) \in R[q,m]$; d – время чистого запаздывания; y, u и w – выходной, управляющий и возмущающий сигналы соответственно; $C : (y^*, y) \to u$ – аналитический закон управления; y^* – внешнее задающее воздействие; P – совокупность параметров закона управления.

В общем случае критическое управление динамическими нестационарными объектами может быть реализовано в условиях их нормального функционирования и существенной априорной и текущей неопределенности о возмущениях, действующих на объект с использованием обучающих моделей и при наличии различного типа ограничений (на амплитуды, скорость изменения, энергию) управляющих и выходных сигналов.

При этом предполагается, что целью управления объектом вида (1) является нахождение управляющего воздействия $u(k)$, поддерживающего выполнение в реальном времени системы целевых неравенств

$$J_i^c(p) \le \varepsilon_i, \; i = 1, 2, ..., n, \quad (2)$$

где $p \in P$ – параметры закона управления, принадлежащие ограниченному множеству P; ε_i – некоторые границы (пороговые значения) целевых функций, полученные на основе параметрического и структурного синтеза адаптивной замкнутой системы управления.

В настоящей работе рассматривается задача критического управления динамическим объектом (1) в предположении, что параметры объекта априори неизвестны и должны уточняться в реальном времени по ходу функционирования системы управления. При этом относительно объекта принимаются стандартные предположения, применяемые в теории адаптивного управления: нули полинома лежат вне единичного круга; верхняя граница порядков полиномов $A(q)$ и $B(q)$ известна; время чистого запаздывания d также известно. Первое предположение обеспечивает устойчивость замкнутой системы критического управления; второе позволяет избежать нежелательный эффект переобучения, достаточно часто возникающий в процессе адаптивной идентификации; третье – обеспечивает необходимое условие $b_0 \neq 0$, делающее возможным синтез закона управления [3].

Алгоритм критического управления состоит из двух последовательных шагов: идентификации параметров объекта и расчета управляющих воздействий.

В качестве процедур идентификации можно использовать модификации рекуррентного метода наименьших квадратов либо проекционные алгоритмы, в той или иной степени связанные с квадратичными критериями. В связи с этим возникает необходимость синтеза адаптивных алгоритмов идентификации, не связанных ни с какими статистическими предпосылками, обладающих высокой скоростью сходимости, вычислительной простотой и пригодных для работы в реальном времени в контуре критической системы управления динамическим объектом.

Рассмотрим полином

$$G(q) = 1 - \Delta A(q), \quad (3)$$

где $G(q) = g_1 q^{-1} + g_2 q^{-2} + ... + q^{-n-1}$, и преобразуем уравнение объекта (1) к виду

$$y(k) = \Theta^T \psi(k-1) + \Delta w(k), \quad (4)$$

здесь $\Theta = (g_1, g_2, ..., g_{n+1}, b_0, b_1, ..., b_m)^T$, $\Delta u(k) = u(k) - u(k-1)$; $\Delta w(k) = w(k) - w(k-1)$,

$$\psi(k-1) = (y(k-1), y(k-2), ..., y(k-n-1), \Delta u(k-d), \Delta u(k-d-1), ..., \Delta u(k-d-m))^T.$$

Параметры уравнения (4) уточняются с помощью одного из адаптивных алгоритмов идентификации. При этом в дальнейших расчетах вместо этого уравнения используется настраиваемая модель

$$\hat{y}(k) = \hat{\Theta}^T(k-1)\psi(k-1). \quad (5)$$

Если параметры объекта априори известны и неизменны, задача критического управления может быть решена с помощью регулятора, удовлетворяющего уравнению

$$\Delta F(q) B(q) u(k) = -E(q) y(k), \tag{6}$$

где оценки полиномов $F(q) \in R[q,d-1]$ с $f_0 = 1$ и $E(q) \in R[q,n)$ можно получить с помощью следующих систем рекурсивных уравнений:

$$\begin{cases} \hat{f}_1(k) = \hat{g}_1(k); \\ \hat{f}_2(k) = \hat{g}_2(k) + \hat{f}_1(k)\hat{g}_1(k-1); \\ \vdots \\ \hat{f}_{d-1}(k) = \hat{g}_{d-1}(k) + \hat{f}_1(k)\hat{g}_{d-1}(k-1) + \cdots + \hat{f}_{d-2}(k)\hat{g}_1(k-d+2) \end{cases} \tag{7}$$

и

$$\begin{cases} \hat{e}_0(k) = \hat{g}_d(k) + \hat{f}_1(k)\hat{g}_{d-1}(k-1) + \cdots + \hat{f}_{d-1}(k)\hat{g}_1(k-d+1); \\ \hat{e}_1(k) = \hat{g}_{d+1}(k) + \hat{f}_1(k)\hat{g}_d(k-1) + \cdots + \hat{f}_{d-1}(k)\hat{g}_2(k-d+1); \\ \vdots \\ \hat{e}_n(k) = \hat{f}_{d-1}(k)\hat{g}_{n+1}(k-d+1). \end{cases} \tag{8}$$

На основании полученных оценок на этом же этапе решается полиномиальное уравнение

$$\hat{F}(q,k)(1-\hat{G}(q,k)) + \hat{E}(q,k)q^{-d} = 1, \tag{9}$$

где $\hat{F}(q,k)$, $\hat{G}(q,k)$, $\hat{E}(q,k)$ – оценки полиномов, полученные в соответствии с зависимостями (7) и (8) к k -му моменту времени; $\hat{f}_0(k)=1$.

Адаптивный критический регулятор C_R^k реализуется на основе закона управления, в котором неизвестные параметры объекта заменены оценками, полученными на предыдущем шаге, т.е.

$$\hat{E}(q,k)y(k) + \hat{F}(q,k)\hat{B}(q,k)\Delta u(k) = 0,$$

при этом d -шаговый прогноз выходного сигнала объекта имеет вид

$$\hat{y}(k+d) = \hat{E}(q,k)y(k) + \hat{F}(q,k)\hat{B}(q,k)\Delta u(k),$$

где используются полученные выше оценки $\hat{E}(q,k)$, $\hat{F}(q,k)$, $\hat{B}(q,k)$.

При этом предполагается, что параметры закона управления априори неизвестны и непредсказуемым образом могут меняться во времени, а внешние возмущения $w(k)$ имеют неизвестный характер (стохастический, детерминированный, хаотический) и ограничены по амплитуде. Цель управления считается достигнутой, если удовлетворяются все n неравенств вида (2).

В работе [3] доказаны следующие свойства адаптивного критического регулятора:

– если входные и выходные сигналы объекта $u(k)$ и $y(k)$ являются ограниченными последовательностями, то ошибка идентификации также является ограниченной последовательностью:

$$\lim_{k\to\infty} \sup |e(k)| \le \delta; \tag{10}$$

– выходной сигнал объекта ограничен условием

$$\lim_{k\to\infty} \sup |y(k)| \le \|\hat{F}(q)\| \delta, \tag{11}$$

т.е. обеспечивается устойчивость замкнутой системы, выходной сигнал которой асимптотически ограничен «трубкой» $\pm\left\|\hat{F}\right\|\delta$.

3. Моделирование критического цифрового регулятора системы управления процессом травления

Общая схема системы управления технологическим процессом травления полосовой стали с использованием последовательно соединенных высокоэффективных управляемых энергоблоков содержит целый ряд локальных контуров микроконтроллерного регулирования. К наиболее важным из таких контуров относятся подсистемы управления температурой травильного раствора и поддержания заданного уровня его кислотности, определяемого суммарным влиянием целого ряда факторов (в первую очередь концентрацией серной кислоты H_2SO_4 и солей $FeSO_4$, находящихся в травильном растворе). При этом состав и температура раствора существенно влияют на конечный результат работы технологической линии травления – при недостаточном уровне кислотности на поверхности проката остается окалина, а при избыточном уровне снимается лишний слой металла и возникает отклонение толщины стальной полосы от заданной величины. В идеальном случае управление процессом травления на протяжении цикла обработки полосы должно обеспечивать поддержание графика, приведенного на рис.1.

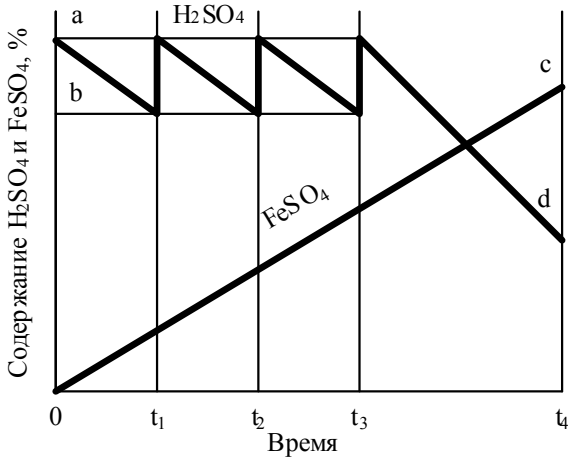


Рис. 1. Диаграмма изменения состава травильного раствора

В соответствии с рис.1 концентрация кислоты в растворе (с начальным уровнем a%) не должна быть ниже уровня b% (в противном случае темп работы линии будет существенно снижен), а в конце технологического цикла (к моменту t_4) концентрации кислоты и соли должны составлять d% и c% соответственно. Ввиду наличия специфических неопределенностей, присущих рассматриваемому технологическому процессу, применение традиционных регуляторов не позволяет получить высокое качество управления режимами травления. В связи с этим целесообразным является разработка описанного выше критического регулятора для некоторых контуров системы управления процессом травления полосовой стали.

Исследования показали, что динамика влияния расхода кислоты ($u(k)$) на плотность травильного раствора ($y(k)$) может быть (для рассмотренной в модельном эксперименте технологической линии) описана ARMAX – моделью вида:

$$(1+1.9q^{-1}+0.92q^{-2})y(k)=q^{-1}(1+0.85q^{-1})u(k)+w(k), \qquad (12)$$

возмущаемой сигналом

$$w(k)=w(k-1)+0.1\operatorname{sign} v(k), \qquad (13)$$

где $v(k)$ – дискретный белый шум с нулевым математическим ожиданием и ограниченной дисперсией.

В соответствии с описанным выше подходом было получено следующее уравнение критического регулятора:

$$u(k)=0.9y(k)-0.98y(k-1)-0.92y(k-2)+0.15u(k-1)+0.85u(k-2), \qquad (14)$$

приводящего к получению гарантированной точности идентификации и приемлемого уровня отклонения выходного сигнала от значений, определяемых технологическим режимом

травления. На рис. 2-4 представлены некоторые результаты моделирования работы синтезированного регулятора (с использованием программной среды SCILAB). В частности, на рис. 2 приведен график текущего отклонения плотности травильного раствора от задания, на рис. 3 показан характер возмущений, а рис.4 иллюстрирует процесс уменьшения нормы ошибки идентификации.

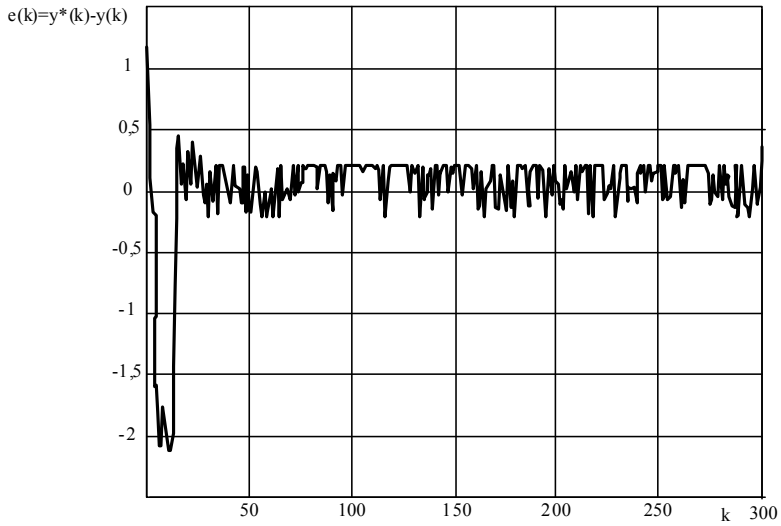


Рис. 2. Ошибка управления (текущее отклонение плотности травильного раствора от задания)

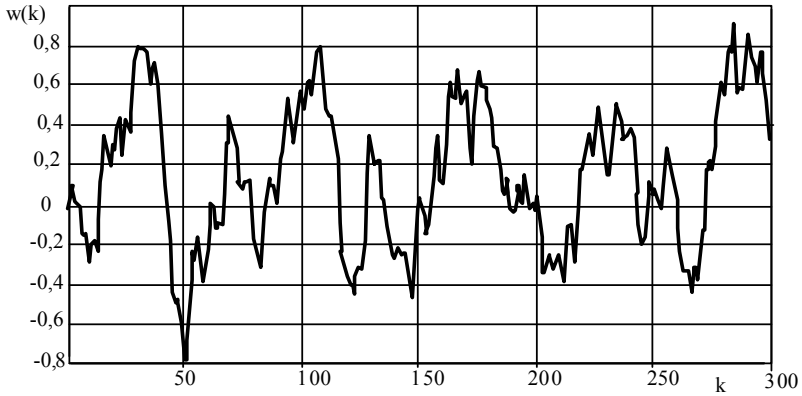


Рис. 3. Возмущающий сигнал системы управления

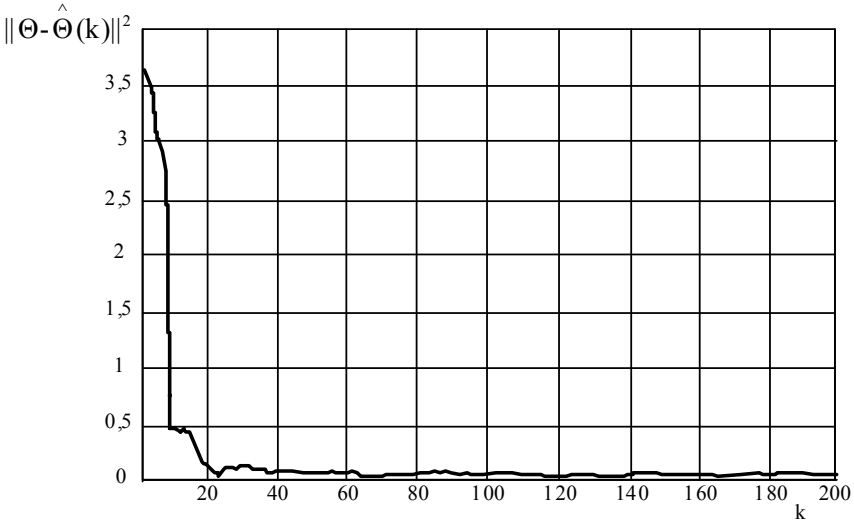


Рис. 4. Качество идентификации (изменение нормы ошибки $\|\Theta-\hat{\Theta}(k)\|^2$)

Синтезированная система управления удовлетворяет условиям (10) и (11) для значения δ=0,05 . Результаты моделирования подтверждают работоспособность предложенного критического адаптивного регулятора, что свидетельствует о возможности его практического использования в составе автоматизированной системы управления технологическими процессами травления полосовой стали.

4. Выводы

Научная новизна полученных результатов заключается в модификации подхода к синтезу адаптивных критических регуляторов для цифровых систем управления с высоким уровнем неопределенности. Суть предложенной модификации состоит в применении рекурсивной процедуры пересчета параметров расширенной ARMAX – модели и последующем определении управляющих воздействий, гарантирующих ограниченность ошибки управления в соответствии с заданными условиями. При этом возмущения могут иметь различный характер (стохастический, детерминированный, хаотический) и быть ограничены лишь по амплитуде.

Практическая значимость заключается в теоретическом и экспериментальном подтверждении возможности и целесообразности применения адаптивных критических регуляторов для создания системы управления технологическим процессом травления полосовой стали с использованием последовательно соединенных высокоэффективных управляемых энергоблоков. В частности, в статье приведены результаты моделирования контуров критического управления температурой травильного раствора и поддержания заданного уровня его кислотности.

Перспективным представляется развитие теоретических и экспериментальных исследований по разработке критических регуляторов для общего технологического цикла прокатки полосовой стали на металлургических предприятиях.

Список литературы: 1.*Балюта С.Н.* Система управления широкополосным станом горячей прокатки / С.Н. Балюта, И.Н. Богаенко, В.Д. Йовбак // Промислова електроенергетика та електротехніка. 2009. №44. С.23-29. **2.** *Skogestad S., Ppostlethwaire I.* Multivariable feedback control: analysis and design. Chichester: Wiley, 2005. 574 p. **3.** *Тимофеев В.А., Илюнин О.О., Самер Лага.* Синтез модифицированного критического регулятора для управления нестационарными объектами // Вестник Херсонского национального технического университета. Херсон, 2010. №38. С.398-401.

Поступила в редколлегию 17.08.2011

Самер Лага, аспирант кафедры экономической кибернетики ХНУРЭ. Научные интересы: идентификация нелинейных систем, цифровое управление. Адрес: Украина, 61166, Харьков, пр. Ленина, 14.

Тимофеев Владимир Александрович, д-р техн. наук, заведующий кафедрой экономической кибернетики ХНУРЭ. Научные интересы: адаптивное управление стохастическими процессами, методы динамической оптимизации. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 70-21-354.

Шамраев Анатолий Анатольевич, канд. техн. наук, доцент кафедры электронных вычислительных машин ХНУРЭ. Научные интересы: нейро-нечеткое управление, разработка и оптимизация микроконтроллерных систем. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 7021354.

УДК 681.518.2

И.А. БОЖИНСКИЙ

ОПЕРАТИВНОЕ УПРАВЛЕНИЕ СЕТЕВЫМИ СИСТЕМАМИ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

Исследуются математические модели оперативного управления сетевыми системами в условиях неопределенности. Разрабатываются инструментальные средства принятия управленческих решений в условиях неопределенности.

Введение

Актуальность состояния проблемы. Сетевые системы характеризуются рядом специфических свойств, к которым относятся: распределение элементов системы на значительном расстоянии друг от друга; иерархическая структура объекта управления и управляющей системы; наличие общности протекающих процессов в различных элементах системы и общности математических описаний исследуемых элементов сетевой системы [1].

К классу сетевых систем относятся водопроводные и тепловые сети, металлургические и транспортно-технологические комплексы, требующие применения инструментальных средств многосвязного и автономного регулирования и управления.

Важная роль в повышении эффективности функционирования сетевых систем отводится методам искусственного интеллекта, которые позволяют повысить качество принимаемых решений в условиях неопределенности исходных данных, проявления внешней среды и цели функционирования [2].

Постановка цели и задач исследования. Процедура исследования сетевых систем включает в себя следующие задачи: содержательная постановка проблемы оперативного управления сетевыми системами; построение математической модели функционирования компонент сетевых систем; разработка алгоритмов оперативного управления производственными процессами в условиях неопределенности. Решения, принимаемые в условиях неопределенности проявления внешней среды, всегда приводят к худшим результатам, чем при полной определенности. В этом случае отыскивается квазиоптимальное решение, лучшее в смысле максимальной близости к некоторому предпочтительному решению.

Сущность выполненных исследований

1. Математическое моделирование сетевых систем

Математическое описание сетевых систем с иерархическими уровнями принятия управленческих решений представим следующим образом [1 - 3]:

– На первом (верхнем) уровне иерархии расположим статическую детерминированную операторную гипермодель без учета свойств стохастичности, неопределенности, нечеткости данных и нечеткости логики. На этом уровне решается прямая задача анализа хода производства:

$$Ax = y,\ x \in R_x^m,\ y \in R_y^n,$$

где x и y – элементы метрических пространств R_x^m и R_y^n; A – оператор, переводящий элементы $x \in R_x^m$ в элементы $y \in R_y^n$.

– На втором сверху уровне иерархии расположим детерминированную статическую векторно-матричную модель без учета отмеченных свойств. На этом уровне осуществляется декомпозиция оператора A для получения математической модели решаемой задачи. Например, для линейных задач оператор **A** можно представить двумя составляющими – структурой S_A и параметрами P_A:

$$A = [P_A, S_A].$$

Чтобы перейти от операторной модели Ax = y к векторно-матричной модели, заменим элементы x и y метрических пространств R_x^2 и R_y^2 вектором $x = [x_1\ x_2]$ и транспонирован-

ным вектором $y^T = [y_1\ y_2]^T$, а оператор А заменим оператором A^M матричного преобразования

$$a_{11}\ x_1 + a_{12}\ x_2 = y_1,$$
$$a_{21}\ x_1 + a_{22}\ x_2 = y_2.$$

– На третьем уровне расположим детерминированную динамическую модель без учета части отмеченных свойств. На этом уровне располагаются модели процесса управления, которые представляют собой последовательную непрерывную во времени смену состояний сетевой системы вида:

$$\dot{x}\ (t) = A(t)x(t) + B(t)u(t),$$
$$y(t) = C(t)\ x(t) + D(t)u(t),$$

где x – n-мерный вектор состояния системы; u – r-мерный вектор входных (управляющих) воздействий; y – m-мерный вектор выходных переменных; t – время. Характерным признаком динамических систем является явная зависимость переменных или параметров системы от времени t.

– На четвертом уровне расположим стохастическую динамическую модель без учета части отмеченных свойств. На этом уровне располагаются стохастические модели, которые представляются двумя компонентами:

$$y = f(x, \theta) + \eta,$$

здесь y – выходной показатель процесса; $f(x, \theta)$ – вектор-функция производственных факторов; η – стохастическая составляющая модели.

– На пятом уровне расположим статическую модель с учетом неопределенности. На этом уровне иерархии располагается модель динамической регрессии с учетом неопределенности вида:

$$y(t) = r(a, x, t, \gamma) = r(a, x, t; \gamma) + \xi\ ,$$

где γ – неопределенность, учитывающая неадекватность модели и проявление внешней среды; ξ – стохастическая составляющая модели.

– На шестом уровне расположим статическую модель с учетом нечеткости. На этом уровне располагаются модели процессов в сетевых системах, представленных на множестве отношений «условие-действие», которые базируются на нечеткой логике или интегрированных нечетких сетях Петри.

Наиболее характерным признаком сетевых систем является наличие топологической структуры модели, представленной графом сети. Граф представляет собой совокупность двух множеств G = (X, Y): множества элементов $x \in X$ и множества отношентий между этими элементами $y \in Y$.

Для описания топологии сетевой системы можно воспользоваться вторым законом сетей и выполнить такие операции:

1. Заменить схему сетевой системы графом сети, причем любая вершина должна содержать не менее трех инцидентных (входящих или выходящих) дуг, а две вершины соединяются между собой только одной дугой.

2. Подсчитать количество вершин n – 1 и дуг m графа сети и определить цикломатическое число сети – количество независимых ресурсных потоков (газа, воды, воздуха) s=m–n.

3. Выбрать дерево графа сети таким образом, чтобы после удаления всех связей ветви графа не образовывали ни единого замкнутого контура: в качестве связей принять дуги с независимыми расходами (потоками), а в качестве ветвей принять дуги с заданными напорами (давлениями).

4. Выполнить упорядоченную нумерацию дуг – сначала связей, а затем ветвей; первые порядковые номера присваиваются связям с заданными расходами, а последние порядковые номера – ветвям с заданными напорами.

5. Выбрать направление обхода контура, совпадающее с направлением единственной связи, входящей в контур.

6. Составить матрицу независимых контуров ||1 B|| в виде прямоугольной таблицы, над которой пишутся возрастающие слева направо порядковые номера дуг, а слева от таблицы

пишутся возрастающие сверху вниз порядковые номера связей, совпадающие с порядковыми номерами ветвей.

Элементами матрицы контуров являются: 1, если направление дуги совпадает с направлением контура; -1, если направление дуги противоположно направлению обхода контура; 0, если дуга не входит в контур. Подматрица контуров $\|B\|$, состоящая из $n \times s$ элементов, содержит всю информацию о топологии (геометрии) S_A сети (Мэзон и Циммерман).

2. Оперативное управление сетевыми системами

Оперативное управление сетевыми системами часто сводится к определению управляющих воздействий, которые переводят систему в желаемое состояние с учетом предъявляемых требований и ограничений при наличии возмущающих воздействий. Возмущения проявляются в виде внутренних факторов и внешней среды. Все внутренние и внешние возмущения учесть невозможно. Поэтому в поле зрения попадают лишь входные величины x, которые оказывают влияние на выходные координаты y.

Входные воздействия подразделяются на управления и и возмущения f. Управления и обеспечивают желаемое функционирование объекта и должны быть изменяемыми. Если таких воздействий нет, то задача оперативного управления не имеет решения. Возмущения f препятствуют нормальному функционированию объекта управления. В системах автоматического регулирования (САР) используются три основных принципа управления: по возмущению, по отклонению и комбинированный.

Принцип управления по возмущению состоит в том, чтобы уменьшить влияние возмущения f на выходные величины объекта y. При изменении возмущения f необходимо так изменять управление и, чтобы скомпенсировать влияние возмущения. В инвариантной системе выходная величина y не зависит от возмущающего воздействия f. Для изменения выходной величины y в управляющее устройство подается дополнительный сигнал y*, который представляет задающее воздействие.

Принцип управления по отклонению состоит в том, что при отклонении управляемой величины y от заданного значения y* подключается обратная связь, которая обеспечивает зависимость управления и (входной величины) от управляемой (выходной) величины y. Отклонение управляемой величины Δy от заданного значения y может быть вызвано разными причинами, в том числе изменением задающего воздействия y*. Его наличие является командой для изменения управления и до тех пор, пока Δy не снизится до допустимого значения. Наличие обратной связи вызывает запаздывание информации в силу инерционности объекта.

Принцип комбинированного управления сочетает в себе лучшие свойства разомкнутых и замкнутых систем и применяется для улучшения динамических свойств САР. В этом случае сильные возмущения в основном компенсируются по разомкнутому контуру, а неучтенные возмущения и ошибки, возникающие из-за отсутствия полной информации о поведении объекта, компенсируются посредством обратной связи в замкнутой системе.

Одним из основных элементов сетевых систем газоснабжения являются регуляторы давления, которые обеспечивают редуцирование и стабилизацию давления газа между различными уровнями газораспределительной сети. В зависимости от типа используемого регулятора системы автоматического регулирования также делятся на:

– системы статического регулирования, обеспечивающие однозначную зависимость между регулируемым давлением и расходом газа;

– системы астатического регулирования, обеспечивающие стабилизацию давления в статике независимо от величины расхода газа, если расход не выходит за установленные пределы;

– системы изодромного регулирования, которые в динамическом режиме обеспечивают свойства, характерные для статических систем, а в статике – свойства астатических систем.

При автоматическом управлении сетевыми системами широко распространены следующие законы регулирования [1 – 3]:

1) Закон статического регулирования, который также называется законом пропорционального регулирования $u = K_1 \varepsilon$ и реализуется статическим П-регулятором с параметром настройки K_1.

При пропорциональном законе регулирования каждому значению регулируемого параметра соответствует строго определенное положение регулирующего органа, т.е. в зависимости от изменения нагрузки регулируемая величина принимает в статике различные значения.

Усредненная статическая характеристика таких регуляторов (РД-50М) без учета зоны нечувствительности имеет вид, представленный на рис. 1.

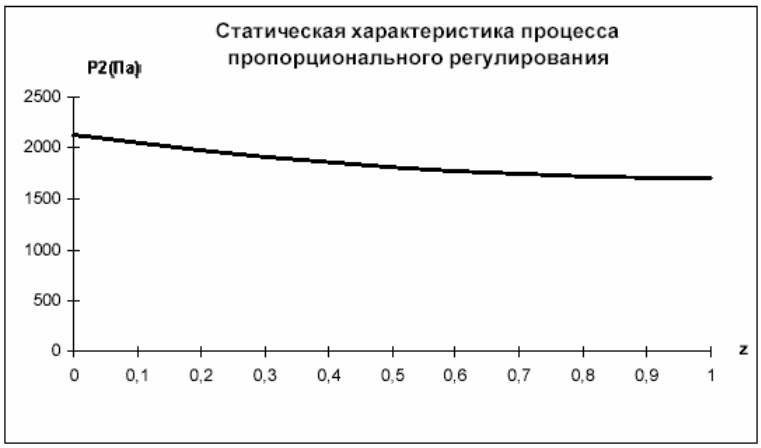


Рис. 1. Характеристика системы статического регулирования

2) Закон астатического регулирования, который также называется законом интегрального регулирования $u = K_2 \int \varepsilon \, dt$ и реализуется астатическим И-регулятором с параметром настройки K_2.

Закон астатического регулирования применяют для устранения статической ошибки стабилизации давления газа. При этом отклонение величины регулируемого параметра от заданного значения стремится к нулю.

Если бы регулятор не обладал некоторой зоной нечувствительности, то характеристика системы астатического регулирования представляла бы горизонтальную линейную зависимость стабилизируемого давления на выходе сетевой системы от расхода газа.

Однако таких регуляторов на практике нет. Все они обладают определенной зоной нечувствительности. Для астатических регуляторов это приводит к тому, что регулируемый параметр находится в пределах зоны нечувствительности, которая заштрихована на рис. 2.

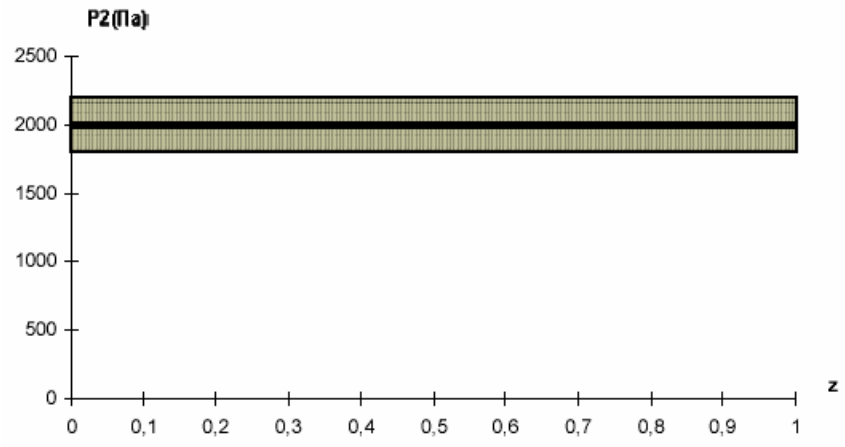


Рис. 2. Характеристика системы астатического регулирования

3) Закон изодромного регулирования, который также называется законом пропорционально-интегрального регулирования

$$u = K_1 \varepsilon + K_2 \int \varepsilon \, dt$$

и реализуется изодромным пропорционально-интегральным ПИ-регулятором с параметрами настройки K_1 и K_2. Изодромное регулирование объединяет лучшие свойства статических и астатических систем. ПИ-регуляторы обеспечивают плавное повышение давления газа на выходе сетевой системы при увеличении расхода с отрицательной неравномерностью процесса регулирования, как показано на рис. 3.

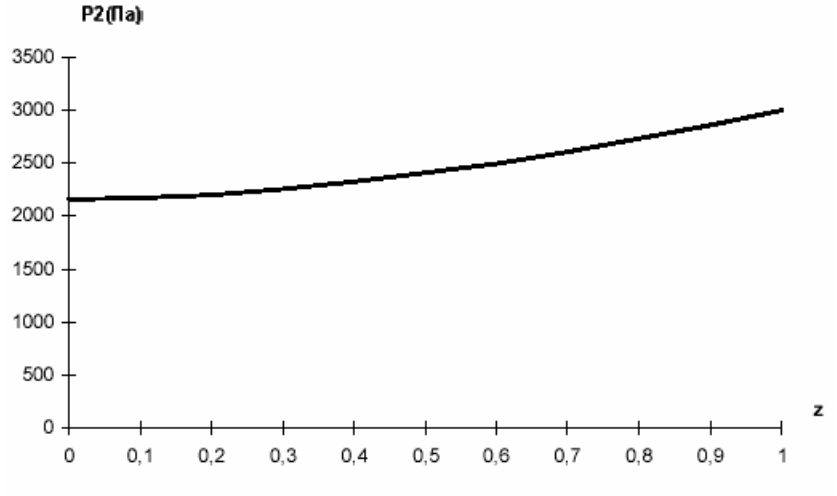


Рис. 3. Характеристика системы изодромного регулирования

4) Закон пропорционально-интегрально-дифференциального регулирования

$$u = K_1\varepsilon + K_2\int \varepsilon dt + K_3(d\varepsilon / dt)),$$

который реализуеется изодромным с предварением ПИД-регулятором с параметрами настройки K_1, K_2 и K_3.

Желание повысить качество управления сетевых систем наталкивается на предельные возможности имеющихся методов оперативного управления. Возникающие при этом трудности объясняются не только большой размерностью управляемых процессов, но и характером неопределенности и нечеткости исходной информации.

3. Оперативное управление в условиях неопределенности

Большинство задач принятия управленческих решений решаются в условиях неопределенности. К существующим видам и формам проявления относятся неопределенности:

1) вызванные недостаточным количеством информации;
2) связанные с ограничениями по времени принятия решения;
3) обусловленные высокой платой за повышение определенности;
4) возникающие из-за неадекватности модели по разным причинам;
5) порождаемые действиями людей в процессе принятия решений;
6) преднамеренно организованные для сокрытия ресурсов системы.

Учет неопределенности осуществляется с целью определить степень влияния внешнего проявления на качество получаемых решений и по возможности принять меры, ослабляющие это влияние. Существует несколько путей “избавления” от неопределенности. Одним из них является замена в модели случайно изменяющихся компонент их усредненными характеристиками.

Желание избавиться от вероятностной неопределенности приводит к постановкам задач в классе стохастического программирования, решение которых сопряжено со значительными трудностями и внесением новых неопределенностей. Поэтому целесообразно вначале решить задачу детерминированной оптимизации при фиксированных значениях, а затем исследовать устойчивость и чувствительность полученного решения к проявлениям внешней среды.

Неопределенность многокритериальной оптимизации резко усиливается, поскольку она включает в себя неопределенность от локальных задач оптимизации, неопределенность вычислительных процедур и неопределенность свертки локальных критериев.

При выработке управленческих решений часто встречаются задачи, в которых исходные данные нечетко сформулированы и плохо определены. Такие задачи содержат большое число неопределенностей типа *много, мало, плохо, хорошо,* которые не имеют аналогов в языке традиционной математики. Поэтому подобные описания средствами традиционной математики сильно огрубляют математическую модель принятия решений.

Для решения такого класса задач разработаны алгоритмы регуляризации и аппарат нечеткой математики, которыми оперирует лицо, принимающее решение, при описании своих желаний и целей. Такой математический аппарат получил название теории нечетких или размытых множеств.

Выводы

Научная новизна сформулированных и реализованых задач оперативного управления сетевыми системами с нечетко заданной информацией состоит в разработке следующих подходов:

1) задачи достижения поставленной цели для случая пересечения нечеткого множества целей G(X) и четкого множества допустимых альтернатив C(X);

2) задачи достижения поставленной цели для случая пересечения нечеткого множества целей G(X) и нечеткого множества допустимых альтернатив C(X);

3) задачи достижения поставленной цели для случая непересечения нечеткого множества целей G(X) и нечеткого множества допустимых альтернатив C(X) методом взаимной "подтяжки" друг к другу области целей и ограничений;

4) задачи достижения четко поставленной цели G(X) на заданном нечетком множестве допустимых альтернатив C(X);

5) нечеткий вариант задач математического программирования, которые решаются по принципу многоальтернативной оптимизации.

Практическая значимость выполненных научно-исследовательских работ состоит во внедрении полученных результатов в региональные газораспределительные сети государственной компании «Укртрансгаз».

Перспективы исследований вытекают из дуализма решаемой проблемы. Множественность эффективных решений является скорее достоинством, а не недостатком, поскольку "жесткие" схемы получения единственного решения неадекватны сущности многокритериальной оптимизации, а свобода выбора предпочтительного решения из множества эффективных позволяет учесть неопределенность целей и критериев. В настоящее время остается актуальной проблема проведения дополнительных исследований, направленных на создание адаптивной иерархической системы принятия оперативного управления в условиях неопределенности.

Решение задач оперативного управления с учетом нечеткости внешней среды и нарушения исходных предпосылок требует разработки регуляризованных процедур принятия управленческих решений с ориентацией на вид неопределенности и нечеткость исходной информации.

Список литературы: 1. *Божинский И.А.* Информационно-аналитическая система управления газосбытового предприятия. Трубопроводные системы энергетики: Управление развитием и функциониро-ванием / И.А. Божинский, В.Ф. Ткаченко. Новосибирск: Наука, 2004. С. 271-286. **2.** *Божинский И.А.* Оперативное диспетчерское управление в распределительных системах газоснабжения //Комунальное хозяйство городов. Серия: Архитектура и технические науки / И.А. Божинский, В.Ф. Ткаченко. Киев: Техника, 2002. Вып. 6. С. 367-370. **3.** *Божинський І.А.* Автоматизована система керування об'єктами газопостачання області //Нафтова і газова промисловість. № 3. 2001. С. 49 – 52.

Поступила в редколлегию 22.08.2011

Божинский Иван Андреевич, канд. техн. наук, зам. начальника НДЧ ХНУРЭ. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 70-21-378.

УДК 681.3

Р.М. ДУБАН, І.В.ШЕЛЕВИЦЬКИЙ

СПЛАЙН-МОДЕЛІ ПРОФІЛІВ СКЛАДНОСТІ ПИТАНЬ ТА ЗНАНЬ РЕСПОНДЕНТІВ В ТЕСТОВОМУ КОНТРОЛІ ЗНАНЬ

Пропонується як функція профілів питань і учасників тестування застосовувати сплайни з фіксованими краями. Описуються вирази та особливості роботи з такими моделями. Завдяки новій моделі автоматизується процес розрахунку профілів моделей IRT за даними тестування. Показуються результати оцінювання IRT-профілів.

1. Вступ

Застосування інформаційних комп'ютерних технологій у навчальному процесі - одна з найбільш важливих і стійких тенденцій розвитку світової освіти. У вітчизняній освіті питання поширення застосування інформаційних технологій входить до пріоритетних напрямів соціально-економічного та культурного розвитку держави. Зокрема створення умов для здобуття громадянами якісної освіти входить до пріоритетного напрямку "Нова якість життя"[1]. Розпочато реалізацію національного проекту «Відкритий світ», до задач якого входить стандартизація та уніфікація методик навчання, а також створення централізованої системи навчання і оцінки знань учнів.

Важливим елементом освітніх інформаційних комп'ютерних технологій є системи тестового контролю. Повноцінна система комп'ютерного тестування повинна містити модуль обробки даних, що базується на тій чи іншій теоретичній моделі тестування. Система також має вирішувати задачі визначення рівня складності тестових завдань, що в свою чергу дозволить більш об'єктивно визначити рівень знань осіб, які проходять тестування. На сьогодні відомі та використовуються для визначення характеристик тестових завдань дві основні теорії: класична теорія тестів (Classical Theory of mental tests) та сучасна теорія тестів IRT (Item Response Theory) [2].

Класична теорія тестів розвивалась та вдосконалювала свій математичний апарат із середини минулого сторіччя і дозволяє отримати статистичне обґрунтування якості тесту. Але, незважаючи на добре розроблений математичний апарат, прозорість та ясність висновків, які можна отримати, має принципові недоліки. Зокрема, тестові бали учнів, що проходили тестування, залежать від складності завдань в тесті, а складність завдань залежить від вибірки учнів. Таким чином, великий недолік класичної теорії пов'язаний з наявністю нелінійної залежності між рівнем складності тестових завдань та балами учнів, що пройшли тестування [3].

Натомість, останнім часом у вітчизняній освіті набула популярності сучасна теорія тестування, що розвивається за кордоном протягом вже декількох десятиріч - Item Response Theory[4]. В порівнянні з класичною теорією, IRT має такі переваги: оцінка складності тестових завдань мало залежить від вибірки респондентів, на яких вона була отримана; оцінка рівня підготовленості учнів не залежить від набору тестових завдань, що використовуються; неповнота даних (пропуск деяких комбінацій рівня знань учня – рівня складності завдання) не є критичним [2].

Суть IRT полягає в тому, що тестові питання та респонденти характеризуються деякою функціональною залежністю від складності питання та рівня знань респондента. Ці складові є латентними, прихованими, а теорія встановлює зв'язок між множинами цих характеристик. Теорія базується на математичних моделях, що дозволяють будувати профілі складності тестів та рівнів знань респондентів. Кількість математичних моделей постійно збільшується. Більш відомими є логістичні моделі Г. Раша та А. Бірнбаума. Основою для багатьох моделей IRT, в тому числі і моделей Бірнбаума, є однопараметрична модель Раша – Rasch measurement [5]. В ній використовується термін ймовірності P_{ij} правильного виконання і-м учасником тестування j-го тестового завдання, що залежить від їх параметрів. Ця залежність називається функцією успіху. Ймовірність визначається за різницею рівнів знань учасника тестування θ_i та рівня складності завдання β_j:

$$P_{ij}=\frac{1}{1+e^{-(\theta_i-\beta_j)}}. \quad (1)$$

Модель Раша базується на найбільш важливому параметрі $(\theta_i-\beta_j)$ – різниці знань респондента та складності завдання. Оскільки ще в класичній теорії тестів було з'ясовано, що завдання мають різну диференційною здатність, в двопараметричну модель Бірнбаума додатково увійшла диференційну здатність завдання, і функція успіху прийняла вигляд

$$P_{ij}=\frac{1}{1+e^{-d_j(\theta_i-\beta_j)}}, \quad (2)$$

де d_j – диференційна здатність завдання, що характеризує нахил (крутизну) його профілю. Для більшої відповідності емпіричним даним А. Бірнбаум розробив трипараметричну модель, де третій параметр відповідає ймовірності вгадування [6].

Окрім вказаних двох основних моделей в IRT використовуються ще й інші моделі і їх кількість збільшується [7]. Причиною цього є насамперед значний інтерес до цих питань в освіті і бажання отримати більш точну, надійну та просту у використанні модель. Різні автори в IRT пропонують нові параметри та їх комбінації, обґрунтовуючи необхідність їх врахування і застосування. Питання вибору оптимальної моделі залишається актуальним і сьогодні.

Значного поширення і застосування серед моделей IRT набула саме однопараметрична модель Г.Раша, хоча і її застосування є досить складним процесом [8]. Нелінійна залежність моделі від параметрів значно ускладнює оцінювання функцій за емпіричними даними. Так, якщо модель не може адекватно описати емпіричні дані, то вони вибраковуються і не використовуються. Такий підхід є малопродуктивним й фактично реалізує принцип "якщо дані не відповідають теорії, то тим гірше для даних".

Існують математичні функції з лінійною залежністю від параметрів, які дозволяють описувати функціональні залежності достатньо складної форми – це сплайни. В роботі пропонується як моделі профілів тестів та респондентів використовувати сплайн-функції, що дозволяють більш точно описати емпіричні дані складної залежності. Розглядається ермітів кубічний сплайн з фіксованими краями. *Метою* є створення інформаційної технології автоматичного оцінювання профілів тестового контролю. Для досягнення мети необхідно адаптувати сплайн-модель до апріорних умов профілів тестового контролю, оцінити параметри моделі за емпіричними даними результатів випробовування тесту та реалізувати алгоритми автоматичного оцінювання з оптимізацією розміщення вузлів сплайна. Отримані результати перевіряються на реальних даних випробовування тесту.

2. Виклад основного матеріалу

В практиці обробки даних найбільш часто застосовують кубічні сплайни з двома неперервними похідними[9]. Для їх розрахунку необхідно вирішить систему інтерполяційних рівнянь. Зручніше користуватись кубічними ермітовими сплайнами, що мають неперервність лише першої похідної і локальні розв'язки інтерполяційних рівнянь.

В загальному вигляді сплайни розраховуються за формулою:

$$P_n(x)=\sum_{i=0}^{R-1} a_i H_i(x), \quad (3)$$

де $H_i(x)$ – базисна функція сплайна; a_i – числові коефіцієнти; R – кількість вузлів сплайна.

В ермітового сплайна базисні функції побудовані так, що числові коефіцієнти є значеннями сплайна та його похідними у вузлах:

$$S(x)=\sum_{i=0}^{R-1} f(u_i)H_i(x)+\sum_{i=0}^{R-1} f'(u_i)\hat{H}_i(x), \quad (4)$$

тут u – вузли сплайна.

Для точки x_k, що належить фрагменту, і вираз (4) можна записати так:

$$S(x_k)=f(u_i)^0 h_i(x_k)+f(u_{i+1})^1 h_{i+1}(x_k)+f'(u_i)^0 \hat{h}_i(x_k)+f'(u_{i+1})^1 \hat{h}_{i+1}(x_k), \quad (5)$$

де h – складові базисних сплайнів $H_i(x)$, $H_{i+1}(x)$, $H_i(x)$, $H_{i+1}(x)$ (рис. 1).

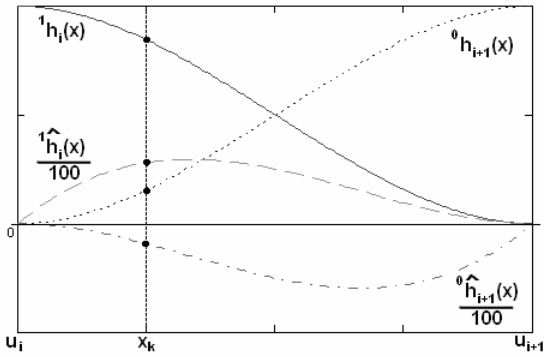


Рис. 1. Складові ермітових базисних сплайнів на інтервалі

Аби не мати справу із похідними та двома видами базисних функцій $H_i(x)$ та $\hat{H}_i(x)$, похідні замінюють центральними розділеними різницями у вузлах сплайна:

$$f'(u_i) \approx \frac{u_{i+1}-u_i}{u_{i+1}-u_{i-1}}\frac{f(u_i)-f(u_{i-1})}{u_i-u_{i-1}} + \frac{u_{i-1}-u_i}{u_{i-1}-u_{i+1}}\frac{f(u_{i+1})-f(u_i)}{u_{i+1}-u_i}. \quad (6)$$

Загальні вирази (7.1)-(7.4) для таких сплайнів отримано в [10]:

$$^0h_i(x)=\frac{2x^3-3x^2(u_i+u_{i+1})+6u_iu_{i+1}x-u_{i+1}^2(3u_i-u_{i+1})}{(u_i^2-2u_iu_{i+1}+u_{i+1}^2)(u_{i+1}-u_i)}, \quad (7.1)$$

$$^1h_{i+1}(x)=\frac{(x-u_i)^2(2x+u_i-3u_{i+1})}{(u_i-u_{i+1})(u_i^2-2u_iu_{i+1}+u_{i+1}^2)}, \quad (7.2)$$

$$^0\hat{h}_i(x)=\frac{(x-u_i)(x^2-2u_{i+1}x+u_{i+1}^2)}{(u_i-u_{i+1})^2}, \quad (7.3)$$

$$^1\hat{h}_{i+1}(x)=\frac{(x-u_i)^2(x-u_{i+1})}{(u_i-u_{i+1})^2}. \quad (7.4)$$

Важливим аспектом моделі є компактне представлення профілів тестових питань та учасників тестування. Вся інформація про модель міститься в значеннях вузлових точок сплайна або пов'язаних з ними параметрах. Однак модель-профіль має важливі особливості, які явно повинна врахувати сплайн-модель. Для профілів питань сплайн-модель має бути "зафіксованою" на краях згідно з умовами: f(0) = 0; f(1)=1. Для профілів респондентів властиві зворотні умови: f(0) = 1; f(1)=0. Крайові умови для профілів питань та учасників тестування схематично зображені на рис. 2. Якщо не враховувати ці особливості, то сплайн модель може суттєво порушувати ці умови й буде неадекватною процесу. Будемо називати далі такі ермітові кубічні сплайни фіксованими $F^+(x)$ для першого випадку і $F^-(x)$ – для другого випадку.

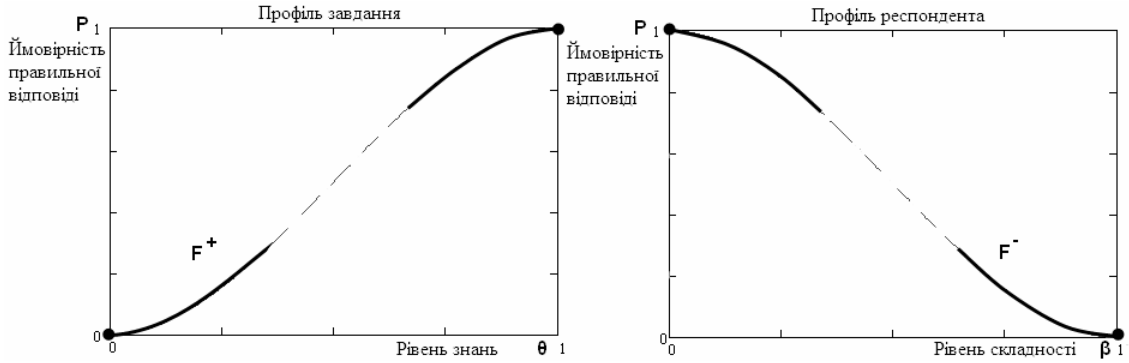


Рис.2. Фіксовані на краях значення профілів

Отримаємо розрахункові вирази для $F^+(x)$ на проміжку $x \in [u_0, u_{R-1})$. У цьому випадку з виразу (5) отримаємо для першого фрагмента, де $x \in [u_0, u_1)$, вираз:

$$F_1^+(x)=f(u_1)\,{}^1h_1(x)+f'(u_1)\,{}^1\hat{h}_1(x). \quad (8)$$

Для побудови сплайна кількість вузлів R має бути не менше трьох. Якщо вузлів сплайна лише три, тобто проміжок лише два, то другий проміжок є останнім, а вузол u_1 збігається з вузлом u_{R-2}. Після підстановки значень крайніх вузлів у (5) функція для останнього фрагмента прийме вигляд (9), де $x \in [u_{R-2}, u_{R-1})$:

$$F_{R-1}^+(x)=f(u_{R-2})\,{}^0h_{R-2}(x)+{}^1h_{R-1}(x)+f'(u_{R-2})\,{}^0\hat{h}_{R-2}(x). \quad (9)$$

Графічно в загальному вигляді функції першого (8) та останнього (9) фрагментів сплайна зображено на рис. 3.

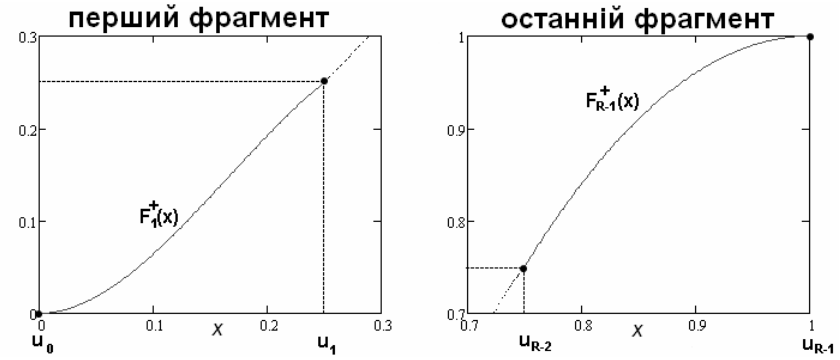


Рис.3. Перший $F^+_1(x)$ та останній $F^+_{R-1}(x)$ фрагменти фіксованого сплайна $F^+(x)$

У випадку R=4 середній фрагмент фіксованого сплайна матиме вигляд:

$$F_2^+(x)=f(u_1)\,{}^0h_1(x)+f(u_2)\,{}^1h_2(x), \quad (10)$$

де $x \in [u_1, u_{R-2})$.

Якщо вузлів сплайна більше трьох, то другий фрагмент прийме вигляд

$$F_2^+(x)=f(u_1)\,{}^0h_1(x)+f(u_2)\,{}^1h_2(x)+f'(u_2)\,{}^1\hat{h}_2(x), \quad (11)$$

тут $x \in [u_1, u_2)$, а передостанній –

$$F_{R-2}^+(x)=f(u_{R-3})\,{}^0h_{R-3}(x)+f(u_{R-2})\,{}^1h_{R-2}(x)+f'(u_{R-3})\,{}^0\hat{h}_{R-3}(x), \quad (12)$$

де $x \in [u_{R-3}, u_{R-2})$.

Якщо ж вузлів більше чотирьох, то усі фрагменти з другого до передостаннього розраховуються за загальною формулою ермітового кубічного сплайна (5).

В загальному вигляді сплайн-модель $F^+(x)$ профілів тестових завдань на проміжку $x \in [u_0, u_{R-1})$ для R=3 матиме вигляд

$$F^+(x)\begin{cases} F_1^+(x), \text{якщо } x \in [u_0, u_1); \\ F_{R-1}^+(x), \text{якщо } x \in [u_1, u_{R-1}); \end{cases} \quad (13)$$

для R=4:

$$F^+(x)\begin{cases} F_1^+(x), \text{якщо } x \in [u_0, u_1); \\ F_2^+(x), \text{якщо } x \in [u_1, u_2); \\ F_{R-1}^+(x), \text{якщо } x \in [u_2, u_{R-1}); \end{cases} \quad (14)$$

для $R \geq 5$:

$$F^+(x)\begin{cases} F_1^+(x), \text{якщо } x \in [u_0, u_1); \\ F_2^+(x), \text{якщо } x \in [u_1, u_2); \\ F_{i+1}^+(x), \text{якщо } x \in [u_i, u_{i+1}),\ i \in [2, R-3), R>5; \\ F_{R-2}^+(x), \text{якщо } x \in [u_{R-3}, u_{R-2}]; \\ F_{R-1}^+(x), \text{якщо } x \in [u_{R-2}, u_{R-1}). \end{cases} \quad (15)$$

Це графічно зображено на рис. 4.

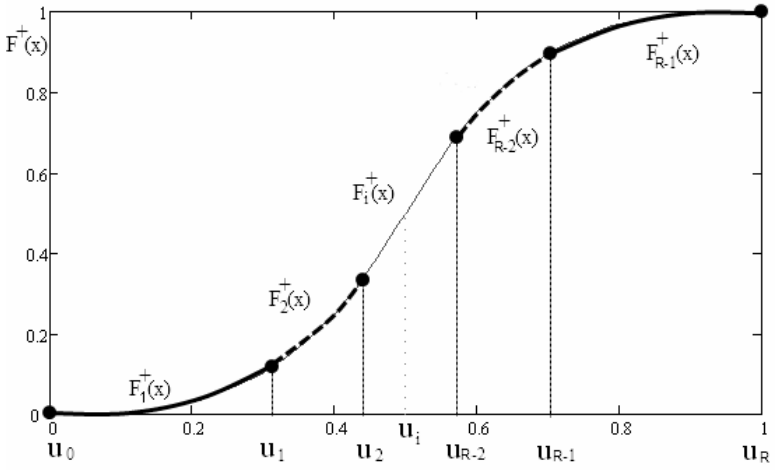


Рис.4. Сплайн-модель профілів тестових завдань

Для побудови профілю рівня знань особи, що проходить тестування, використовується сплайн-функція $F^-(x)$, отримана з виведеної функції $F^+(x)$:

$$F^-(x)=F^+(1-x). \qquad (16)$$

Отримана сплайн-модель враховує специфіку профілів, лінійно залежить від параметрів, що є значеннями сплайна у точках стикування – вузлах. Конкретні значення визначаємо за даними тестового контролю в контрольних групах, де отримуємо емпіричні оцінки профілів у точках. Оцінки параметрів сплайна шукаємо за методом найменших квадратів на фіксованій сітці вузлів, так що для профілів питань досягається:

$$D=\sum_{i=1}^{N}(d_i-F^+(\theta,U))^2 \to \min .$$

Зменшення похибки наближення досягається також за рахунок оптимізації числа та схеми розміщення вузлів сплайна. Завдяки хорошим наближуючим властивостям сплайна та лінійній залежності від параметрів відпадає необхідність участі оператора-експерта в побудові кожного профілю.

Розроблена модель входить в модуль розрахунку профілів складності тестових завдань та рівня знань учнів, що проходять тестування, в авторській інформаційній системі “Logit”. Приклад профілів питань, що надає система, зображено для питань на рис. 5, для респондентів – на рис. 6.

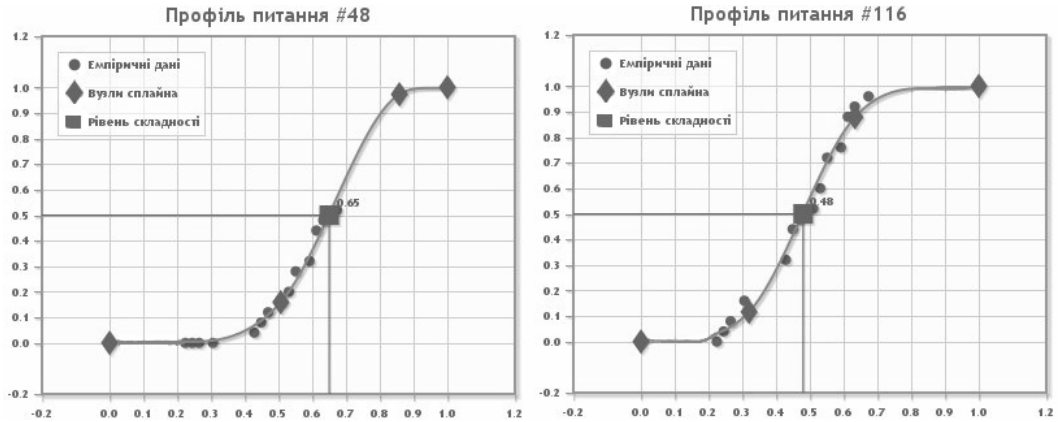


Рис.5. Профілі питань, побудовані в системі “Логіт”

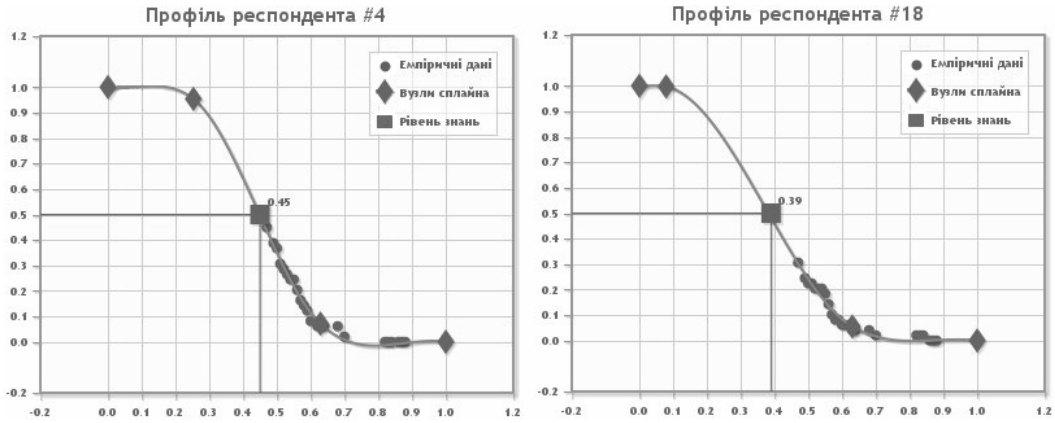


Рис .6. Профілі респондентів, побудовані в системі “Логіт”

На рис. 5 зображені довільні питання з тесту, за яким проводилось тестування на контрольній групі. Вибіркові профілі респондентів зображені на рис. 6. Рівень складності питань та рівень знань учасників тестування визначається за IRT на рівні P = 0,5.

3. Висновки

Незначним ускладненням моделі зменшується кількість вхідних параметрів та вирішується проблема фіксації крайніх точок, але швидкість розрахунків комп’ютером підвищується. У порівнянні з моделями IRT отримана модель є загалом більш надійною, універсальною та простою, не потребує участі експертів у побудові профілів.

Модель, що побудована з використанням складеної сплайн-функції з фіксованими краями, має такі переваги:

– враховує апріорні посилки,

– має лінійну залежність від параметрів,

– оцінку за МНК,

– дає можливість оптимізувати профіль.

Але, як і всі моделі, що входять до IRT, сплайн-модель має свої недоліки. Одним із найбільших недоліків є те, що функція не враховує неспадаючий характер при побудові профілів питань. Цю проблему можна вирішити, підібравши ще більш вдалий базис сплайна. Перед тим, як рекомендувати використовувати модель як вимірювальну систему в тестовому контролі знань, необхідне проведення її апробації на великій кількості емпіричних даних. Для спрощення процесу апробації модель інтегровано у web-систему “Logit”(http://kdpu.edu.ua/logit/), а процес створення профілів автоматизовано.

Наукова новизна полягає в тому, що вперше запропоновано як профіль у тестовому контролі використовувати ермітові кубічні сплайни з фіксованими краями.

Практичне значення роботи в тому, що з допомогою нової моделі вдалося реалізувати автоматичне оцінювання профілів питань та респондентів тесту. Завдяки цьому суттєво скорочується час на оцінювання якісних характеристик тесту, немає необхідності у залученні до процесу оцінювання фахівця-статистика, зростає точність та достовірність оцінювання.

Предметом подальших досліджень є вдосконалення сплайн-моделі для більш точного врахування особливості профілів (а саме їх неспадаючий характер) та завершення роботи над інформаційною системою, що втілює продемонстровані результати.

Список літератури: 1. *Указ* Президента України від 08.09.2010 року № 895 “Про заходи щодо визначення і реалізації проектів із пріоритетних напрямів соціально-економічного та культурного розвитку”. **2.** *Ким В.С.* Тестирование учебных достижений. Монография. Уссурийск. УГПИ, 2007. 214 с. **3.** *Аванесов В.С.* Основы научной организации педагогического контроля в высшей школе. М., 1989. 167 с. **4.** *C. DeMars.* Item Response Theory. Oxford University Press: 2010. 144 p. **5.** *Rasch G.* Probabilistic Model for Some Intelligence and Attainment Tests. Chicago: Univ. of Chicago Press, 1981. 199 p. **6.** *Birnbaum A.* Some Latent Trait Models and Their Use in Inferring and Examinee’s Ability. In Lord F.M., Novick M. Statistical Theories of Mental Test Scores. Addison-Wesley Publ. Co. Reading, Mass, 1968. P.397-479. **7.** *Baker F.B.* The Basics of Item Response Theory. ERIC, 2001. 172p. **8.** *Wilson M.* Constructing Measures: An Item

Response Modeling Approach. Mahwah, New Jersey: Lawrence Erlbaum associates, 2005. 228 p. **9.** *Шелевицький І. В.* Методи та засоби сплайн-технології обробки сигналів складної форми /М.О.Шутко. Кривий Ріг: Європейський університет, 2002. 304 с. **10.** *Шелевицький І.В.* Сплайни в цифровій обробці даних і сигналів /І.В. Шелевицький, М.О.Шутко, В.М.Шутко, О.О. Колганова. Кривий Ріг, 2008. 232 с.

Надійшла до редколегії 25.08.2011

Дубан Роман Миколайович, аспірант Національного авіаційного університету. Наукові нтереси: web-технології. Адреса: Україна, 50093, Кривий Ріг, вул. Гутовського 27-1, тел. (067)9018237.

Шелевицький Ігор Володимирович, д-р техн. наук, доцент, заступник директора з наукової роботи Криворізького педагогічного інституту ДВНЗ "Криворізький національний університет". Наукові інтереси: сплайни і їх застосування. Адреса: Україна, 50086, Кривий Ріг, пр. Гагаріна 54, тел. (096)5320143.

УДК 621.391

Д.Г. МЕДВЕДЄВ

ТЕХНОЛОГІЯ КЛАСИФІКАЦІЇ ЕОЗИНОФІЛІВ НА ОСНОВІ СПЛАЙН-ПАРАМЕТРИЗАЦІЇ

Описуються спеціалізовані способи та алгоритми параметризації цифрових зображень біологічних об'єктів для задач медичної діагностики. Розробляються алгоритми отримання контуру еозинофіла як сплайн-функції та знаходження його морфологічних параметрів. Пропонується дискримінантна функція для параметризованих еозинофілів. Створюється інформаційна технологія параметризації еозинофілів.

Постановка проблеми

За даними Міністерства охорони здоров'я України протягом останніх 10 років в Україні спостерігається поширення та ускладнення перебігу алергічних захворювань у дітей. Близько 18-20% їх мають різні за локалізацією та формами прояву алергічні захворювання. Рівень поширеності бронхіальної астми в різних регіонах коливається від 0,9 до 6,8; атопічного дерматиту – від 2,1 до 12,8 на 1000 дитячого населення [1].

Від виявлення цих захворювань на початковій стадії залежить їх лікування і подальший прогноз. На кафедрі педіатрії Дніпропетровської медичної академії розроблено метод прогнозування імунного статусу новонароджених за морфологічними ознаками імунних клітин крові (еозинофілів) [2]. Метод дозволяє економити час і кошти на аналізи та оптимізувати диспансеризацію дітей групи ризику. Проте візуальне визначення морфологічних параметрів трудомістке й суб'єктивне і тому реалізоване лише для якісно-кількісних показників (наприклад, відсоток еозинофілів неправильної форми) [3]. Для реалізації кількісних вимірювань з метою діагностики була поставлена задача автоматизації, тобто створення інформаційної системи оконтурювання та параметризації еозинофілів за цифровим зображенням.

Аналіз останніх досліджень і публікацій

Питаннями розпізнавання й параметризації клітин крові, шкіри займаються Адамов В.Г., Коков А.А (Донецький національний технічний університет). В роботах [4,5] для оконтурювання застосовують метод активних контурів, де мінімізується потенційна енергія сплайн-кривої. Однак метод погано описує фрагменти з великою кривизною. У роботі [6] алгоритм вдосконалено введенням локальних параметрів гладкості. Проте слід відзначити, що ефективність методу знижується при наявності шумів.

У Biomedical Imaging Group для оконтурювання каплеподібних об'єктів розроблено алгоритм «Змійка» [7], де контур описує експоненційний сплайн мінімальної енергії.

Розглянуті методи мало придатні для оконтурювання саме еозинофілів через нечіткість їх контурів та високу варіабельність зображень за формою та забарвленням.

Метою роботи є створення стійких до варіабельності зображень алгоритмів параметризації еозинофілів для підвищення якості діагностики імунного статусу.

В процесі створення інформаційної системи розпізнавання та параметризації еозинофілів розв'язано такі *задачі*:

1. Попередня обробка зображення з метою покращення його якості.
2. Розпізнавання еозинофіла за його цифровим зображенням.
3. Побудова сплайн-моделі контуру еозинофіла за методом найменших квадратів та оптимізація поділу сплайна на фрагменти.
4. Визначення геометричних параметрів клітини.
5. Визначення дискримінантної функції для отриманих коефіцієнтів параметризованих еозинофілів.

Цифрові зображення еозинофілів отримано за зразками мазків крові, наданими кафедрою педіатрії Дніпропетровської медичної академії у Кривому Розі. Для фотографування застосовувалася камера DCM510 5Mpixels з мікроскопом Konus Academy #5304 при збільшенні у 500 разів. Розмір пікселя зображення складає 0,04826±0,00049 мкм.

Знімки мазків крові (рис. 1), як правило, недостатньо чіткі і контрастні, а також несуть в собі багато непотрібної інформації – шумів (пил, що осів на скельця препаратів, сторонні включення). Еозинофіл вирізняється специфічним забарвленням.

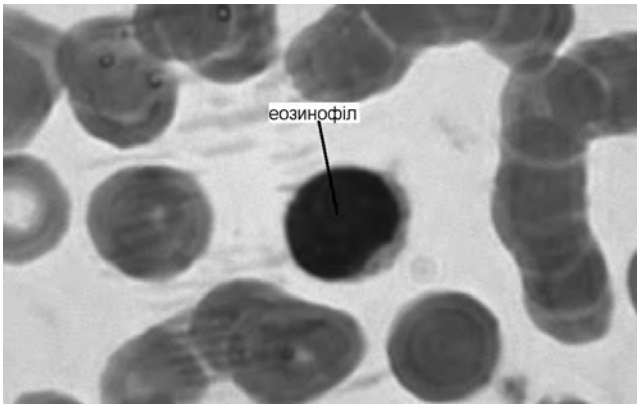


Рис 1. Зображення еозинофіла

Придушення ізольованих перешкод з мінімальним розмиванням контрасту отримано шляхом одновимірної медіанної фільтрації по 5 точках.

Для виділення контуру використовується оператор Собеля. Для розрахунку порогового значення оператора зображення переводиться у формат YUV. Оператор застосовується до сигналу яскравості Y.

Еозинофіл відрізняється від загального фону більшою яскравістю, а від інших клітин – забарвленням (навіть візуально його можна виокремити від фону). Враховуючи лише яскравість, не можна відрізнити еозинофіл та визначити його важливі характеристики. Тому необхідно брати до уваги разом із бінарним компонентом яскравості й компоненти кольоровості U (синьо-жовта) V (червоно-блакитна). Отримуємо кольорове зображення з іншим розподілом кольорів за рахунок бінарного перетворення яскравості. На ньому чітко виділені ті ж контури, але еозинофіл стане білого кольору, а фон має жовтуватий колір.

Завдяки різниці в кольорі виділяємо еозинофіл. Для цього розроблено алгоритм послідовної стратегії перебору. Знаходяться приблизні межі «білого тіла» – контур еозинофіла. Знаходяться білі точки, навколо яких є достатня кількість (не менше 5) таких же білих точок. Це виключає окремі білі точки серед кольорового фону. Далі рухаємось в чотирьох напрямках, шукаючи чорні точки – контур й описуємо навколо нього прямокутник. Особливість контура еозинофіла в тому, що він є замкнутою лінією. Тому для подальшої апроксимації сплайном зручніше перейти до полярної системи координат з початком координат у центрі прямокутника (рис. 2).

Як видно на рис. 2, контур еозинофіла не є гладкою однозначною послідовністю ряду точок. Його можна розглядати як множину значень деякої гладкої кривої контура f(a) разом з адитивним білим шумом з нульовим середнім $r(\alpha_i) = f(\alpha_i) + \varepsilon_i$, $i = \overline{1, N}$, $M(\varepsilon) = 0$, $D(\varepsilon) = \sigma^2$.

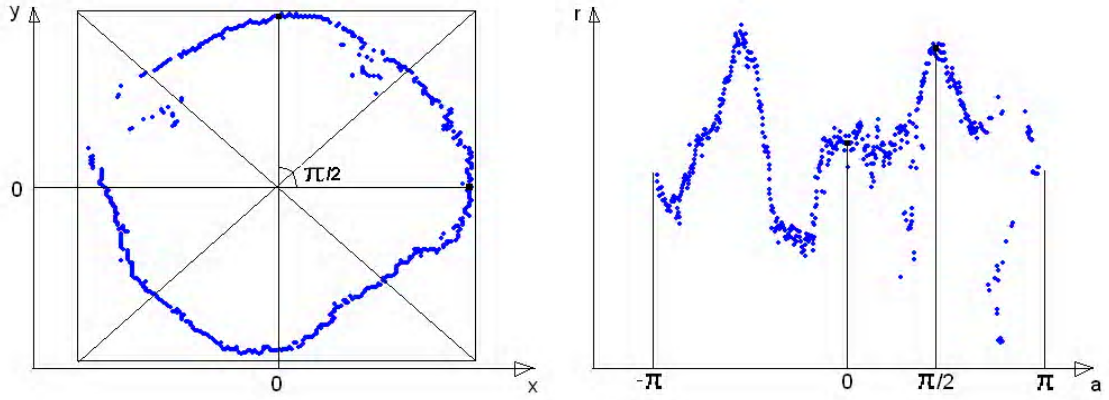


Рис. 2. Виділений контур еозинофіла в декартовій та полярній СК

Для апроксимації кривої контура f(a) за даними $r(a_i)$, $i = \overline{1, N}$ застосуємо кубічний ермітів сплайн [8], значення якого розраховуються як

$$S(\alpha) = \sum_{j=0}^{R} f(\alpha_j) H_j(\alpha), \tag{1}$$

де k_j – параметр сплайна, що є значенням сплайна у вузлах; $H_j(a)$ – базисні ермітові сплайни; R – число фрагментів сплайна.

Ермітові базисні сплайни – локальні й складаються з 4-х ненульових фрагментів:

$$H_j(\alpha) = \begin{cases} H_{0,j-1}(\alpha), \alpha \in [u_{j-1}, u_j), \\ H_{1,j}(\alpha), \alpha \in [u_j, u_{j+1}), \\ H_{2,j+1}(\alpha), \alpha \in [u_{j+1}, u_{j+2}), \\ H_{3,j+2}(\alpha), \alpha \in [u_{j+2}, u_{j+3}), \\ 0, x \notin [u_{j-1}, u_{j+3}). \end{cases} \tag{2}$$

Значення сплайна в довільній точці, що належить j-му фрагменту, дорівнює

$$S_j(\alpha) = f(u_{j-1}) H_{0,j-1}(\alpha) + f(u_j) H_{1,j}(\alpha) + f(u_{j+1}) H_{2,j+1}(\alpha) + f(u_{j+2}) H_{3,j+2}(\alpha). \tag{3}$$

Оскільки функцію контура в полярній системі координат можна розглядати як періодичну, розрахункові вирази [8] кубічного ермітового сплайна модифіковано для періодичних крайових умов. Особливістю періодичного сплайна є те, що перед першим фрагментом знаходиться останній, а за останнім фрагментом іде перший.

Для заданої множини вузлових точок сплайна $U = \{U_0, U_1, \ldots, U_R\}$ оцінки значень у вузлах шукаємо за методом найменших квадратів. При цьому мінімізується енергія похибки апроксимації (в методах активних контурів енергія сплайна):

$$E = \sum_{i=1}^{N} (r_i - S(\alpha_i))^2 \to \min. \tag{4}$$

Вектор оцінок отримуємо як

$$A = (P^T P)^{-1} (P^T r), \tag{5}$$

де P – матриця планування специфічного блочно-діагонального виду розмірності NxR; r – вектор даних розмірності N.

Завдяки локальним властивостям базису система рівнянь добре обумовлена, а розрахунки швидкі.

Оскільки сплайн-модель отримана за методом найменших квадратів для заданого вектора вузлів (рис. 3), залишається можливість подальшої оптимізації шляхом підбору оптимального числа і схеми розміщення вузлів.

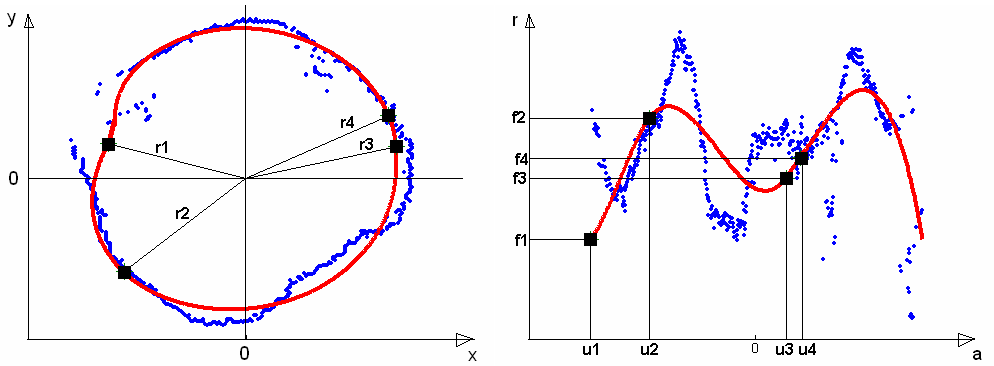


Рис. 3. Апроксимація еозинофіла на початку оптимізації

Оптимізація починається з чотирьох рівномірно розміщених вузлів із застосуванням спрощеного методу покоординатного спуску. Якщо оптимізація дає середньоквадратичне відхилення більше 2 пікселів, то в фрагмент з найбільшою похибкою додаємо вузол й процес повторюємо. Як правило, для досягнення точності достатньо 10-13 вузлів (рис. 4).

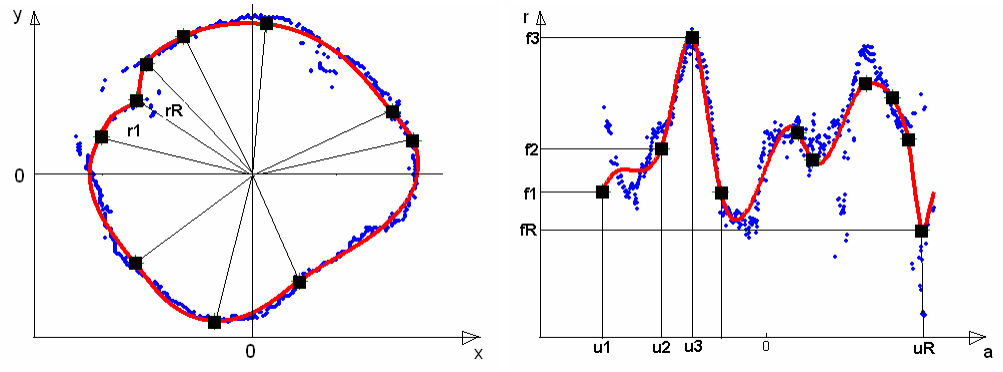


Рис. 4. Оптимізований контур еозинофіла

Фактично гладкістю сплайна керуємо, змінюючи число вузлів та їх розміщення.

Подальша параметризація еозинофіла полягає у визначенні таких його морфологічних ознак, які визначають імунний статус дитини, а саме:

1) форма клітини (кругла, овальна, неправильна),
2) індекс видовженості клітини (відношення великого до малого діаметрів клітини),
3) площа еозинофіла,
4) довжина контура.

Великим діаметром еозинофіла вважатимемо найдовший серед відрізків кінці якого належать контуру досліджуваного тіла. Пошук великого діаметра виконується перебором довжин всіх вказаних відрізків.

Малим діаметром, за аналогією з еліпсом, буде найдовший відрізок, серед перпендикулярних до великого діаметра. Його пошук також виконується перебором. Перпендикулярність перевіряється за допомогою скалярного добутку.

Індекс видовженості клітини визначається відношенням великого діаметра до малого. Якщо індекс видовженості еозинофіла належить проміжку (1, 1.1) і довжина контура еозинофіла приблизно дорівнює πd_y, де d_y – великий діаметр, то форма є круглою. Якщо діаметри точкою перетину діляться навпіл, то форма є овальною. Форма є неправильною у всіх останніх випадках.

Площа досліджуваної клітини дорівнює інтегралу від сплайна в полярній системі координат:

$$S = \sum_{j=1}^{R} \int_{u_j}^{u_{j+1}} S_j(\alpha) d\alpha . \qquad (6)$$

Довжина лінії визначається за формулою:

$$l = \int_{m}^{n} \sqrt{r^2 + (r')^2}\, dx = \sum_{j=1}^{R} \int_{u_j}^{u_{j+1}} ((S_j(\alpha))^2 + (S_j^{'}(\alpha))^2) d\alpha \,. \quad (7)$$

Для зручності розрахунків для фрагментів розраховуються коефіцієнти кубічних поліномів, що підставляються в знайдені аналітичні вирази.

Вказані вище морфологічні ознаки застосовуються в дискримінантному аналізі. За навчальною вибіркою розраховуються коефіцієнти дискримінантної функції [9]

$$D(q) = \sum_{i=1}^{5} \beta_i q_i \,, \quad (8)$$

де q_i – морфологічний параметр.

За встановленою дискримінантною функцією новий зразок можна класифікувати як норму або патологію.

Таким чином, розроблено інформаційну технологію, що втілюється в діагностичну інформаційну систему (рис. 5).

Рис. 5. Інформаційна система параметризації еозинофілів

Інформаційна система включає блоки первинного збору інформації: отримання зображень (1) та історії хвороб (діагнозів) (2). Параметризовані зображення, отримані разом з історією, зберігаються в навчальній базі даних (4), що використовується для розрахунку або уточнення дискримінантної функції.

Параметри зображень, що не мають первісного діагнозу, підлягають діагностиці (6).

Користувачами такої системи з одного боку мають бути практикуючі лікарі, що потребують прогнозної діагностики, а з іншого – медики – наукові працівники, що формують навчальну базу й уточнюють дискримінантну функцію.

На даний час система знаходиться на стадії розробки.

Початкова вибірка досліджуваних об’єктів складається з 300 зображень (приблизно 70 пацієнтів). Всі зображення були отримані та опрацьовані автором самостійно за допомогою даної технології в системі MatLab. Мазки крові та їхній опис, розподіл зображень за класами, був отриманий на кафедрі педіатрії Дніпропетровської медичної академії.

Висновки

Наукова новизна роботи полягає в тому, що вперше запропоновано метод оконтурювання, який поєднує оцінювання ермітової кубічної сплайн-моделі за методом найменших квадратів з покоординатною оптимізацією розміщення вузлів сплайна. На відміну від методів активних контурів не потрібно встановлювати компроміс між гладкістю та наближенням, параметри моделі мають очевидну інтерпретацію, а оцінки параметрів стійкі до білого шуму.

Створена інформаційна технологія, що використовує оконтурювання та параметризацію еозинофілів для морфологічної діагностики імунного статусу. Практичне значення технології в тому, що з її допомогою можна реалізувати метод оцінки імунного статусу дитини за морфологічними показниками еозинофілів. Метод діагностики за морфологічними показниками оперативніший за інші та мало травматичний.

Технологічність процедури перевірено на 300 реальних зображеннях. Предметом подальшої роботи є втілення технології у спеціалізованій інформаційній діагностичній системі.

Список літератури: 1.*Наказ* від 20.02.1995 № 33 Про розвиток та удосконалення лікувально-профілактичної допомоги дітям з алергічними захворюваннями. Режим доступу: www.moz.gov.ua/ua/main/?docID=9606 **2.** *Литвинова Т.В.* Профілактика респіраторних захворювань у дітей, хворих на бронхіальну астму, що одержують базисну терапію: дис. канд. мед. наук: 14.01.10 // Д. – ДМА, 2006. 193с. **3.** *Пат.* на винахід № 62672. Україна. Спосіб прогнозування імунного статусу новонароджених / Мокія С.О., Шелевицький І.В., Василенко Н.В. Опубл.15.12.2005, Бюл.№12. **4.** *Чудовська А.К.* Порівняльний аналіз алгоритмів виділення контурів //Матеріали XIII Всеукраїнської (VIII Міжнародної) студентської наукової конференції з прикладної математики та інформатики. Львів, 22 – 23 квітня 2010 року. **5.** *Коков А.А.* Автоматизированная подсистема распознавания и оконтуривания клеток. Режим доступу: http://www.masters.donntu.edu.ua/2003/kita/kokov/library/pub1.htm **6.** *Бедзір А.О., Лютак І.З.* Автоматичне знаходження контурів дефектів шляхом аналізу зображень, отриманих ультразвуковими методами контролю // Науковий вісник Івано-Франківського національного технічного університету нафти і газу 2009. №22. С.28-32. **7.** *Delgado-Gonzalo R., Thévenaz P., Seelamantula C.S., Unser M.* Snakes with Ellipse-Reproducing Property // IEEE Transactions on Image Processing, in press. http://bigwww.epfl.ch/algorithms/esnake. **8.** *Шелевицький І.В., Шутко М.О., Шутко В.М., Калганова О.О.* Сплайни в цифровій обробці даних і сигналів. Кривий Ріг: Видавничий дім. 2008. 232с. **9.** *Афифи А.* Статистический анализ: Подход с использованием ЭВМ / А Афифи., С. Эйзен. Пер. с англ. М.: Мир, 1982. С. 322-324.

Надійшла до редколегії 12.08.2011

Медведєв Дмитро Геннадійович, аспірант Національного авіаційного університету сплайни. Адреса: Україна, 50055, Дніпропетровська обл., м. Кривий ріг, вул. Кокчетавська, 29, кв. 84, тел.: (093)4205340, (068)8535681.

УДК 621.37/39.029.3

А.А. АНДРУСЕВИЧ, И.Ш. НЕВЛЮДОВ, А.Н. ДОНСКОВ

РАЗРАБОТКА И ПРИМЕНЕНИЕ МЕТОДОВ МОНИТОРИНГА ПРОЦЕССОВ ПРОЕКТИРОВАНИЯ, ПРОИЗВОДСТВА И ЭКСПЛУАТАЦИИ ЖЦ РЭС

Излагаются результаты усовершенствования методов и средств мониторинга производственной среды при изготовлении РЭС в направлении совершенствования систем технического обслуживания технологического оборудования, использующего цифровые системы управления и контроля. Приводятся основы теории и новая концепция мониторинга жизненного цикла РЭС на этапах проектирования, производства и эксплуатации, в основе которой положено отображение информации на основе визуализации процессов. Показывается, что реализация такой концепции является существенным дополнением информационной поддержки жизненного цикла, обеспечивая решение задач принятия решений в условиях неопределенности и включение человека в управление жизненным циклом.

1. Ведение

Современный уровень развития техники характеризуется повышением сложности, наукоемкости, качества техники и появлением в связи с этим новых проблем. Действенным средством решения подобных проблем в последнее десятилетие выступают новые технологии сквозной информационной поддержки сложной наукоемкой продукции на всех этапах ее жизненного цикла (ЖЦ) от маркетинга до утилизации, базирующиеся на моделировании, электронном представлении и использовании информации для обеспечения ЖЦ. Мониторинг, выполняя по своему определению функции по надзору за состоянием объектов, предполагает сбор и обработку информации о ЖЦ и, следовательно, является частью этих технологий.

К числу наиболее важных функций мониторинга, реализуемых в настоящее время, относится контроль и прогнозирование состояния РЭС и процессов обеспечения ее ЖЦ. Для сложных систем, в том числе и ЖЦ РЭС, возникает необходимость принятия решений в ситуации отсутствия формальных методов постановки и решения задач, возникающих в ЖЦ РЭС. Наиболее эффективными становятся человеко-машинные процедуры, основанные на интеллектуальных возможностях систем, реализующих эти процедуры в «диалоге» человека с ЭВМ. Здесь мониторинг, способный отображать суть происходящих в ЖЦ РЭС процессов, и, следовательно, дающий возможность реализовать интеллектуальные возможности для построения математических и логических моделей, становится действенным инструментом обеспечения ЖЦ РЭС.

Таким образом, разработка теоретических основ мониторинга, дающего возможность оценивать и прогнозировать состояние процессов ЖЦ РЭС в условиях отсутствия формальных методов моделирования для обеспечения возможности принятия эффективных решений при поддержке ЖЦ РЭС, является актуальной научно-технической проблемой.

2. Разработка методов мониторинга технологических процессов (ТП) в производстве РЭС

Контроль (наблюдение изображения) монтажных соединений при мониторинге ЖЦ РЭС на этапе производства можно рассматривать как часть технологического процесса, включающего последовательность операций изменения состояния предмета производства (T_i) и операций технического контроля (K_i). Методы рассматриваемого мониторинга встраиваются в систему межоперационного контроля, получаемая информация может быть использована в системе технического обслуживания и профилактики ТП сборки и монтажа РЭС. Совершенствование такой системы [1,2] является необходимым условием улучшения показателей производства, характеризующих стабильность и надежность ТП, отсутствие простоев. Реальные технологические процессы характеризуются необходимостью постоянной настройки режимов и оборудования ввиду наличия большого количества объективных и субъективных факторов, вызванных изменением характеристик исходных материалов и энергоносителей, износом и нестабильностью работы оборудования, технологической оснастки, инструмента, квалификацией исполнителей и т.д.

Появление изображения соединения, не соответствующего эталонному, можно рассматривать как отказ ТП, вызванный его разладкой, уместно в этом случае рассматривать мониторинг как мероприятие по обеспечению показателей безотказности ТП. Задачей, требующей теоретического обоснования, является определение количества и периодичности проверок соединений в соответствии с ограничениями на технико-экономические показатели ТП.

Основная цель регламентных и других профилактических работ, обеспечивающих настройку ТП, – уменьшение параметров потока отказов до их минимальных значений. Интуитивно должно быть ясно, что если бы регламентные работы не уменьшали параметр потока отказов, то в их проведении не было бы смысла.

Все операции можно разделить на несколько групп в зависимости от скорости изменения параметра потока отказов (рис. 1).

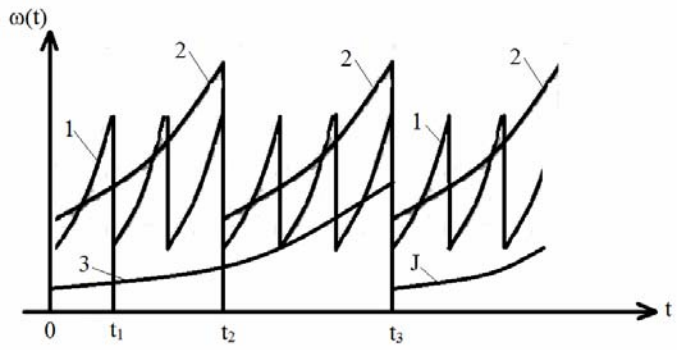


Рис. 1. Изменение параметра потока отказов сгруппированных ТП

К первой группе относятся те ТП, параметр потока отказов которых возрастает до предельно допустимых значений за время наработки t_1. После выполнения регламентных работ на этих ТП их параметры потока отказов восстанавливаются (кривая 1).

Ко второй группе относятся ТП, параметр потока отказов которых возрастает до предельно допустимых значений за время t_2 (например, $t_2 = 3t_1$, кривая 2). К третьей группе относятся ТП, предельные значения параметра потока отказов которых достигаются за время t_3, равное, например, $t_3 = 2t_2$ (кривые 3). К нулевой группе можно отнести ТП, параметры потока отказов которых за весь срок эксплуатации остаются постоянными.

Имея данные о характере изменения параметра потока отказов операций (частей) ТП, можно оценить периодичность выполнения регламентных работ (в случае метода техобслуживания по наработке) или работ по контролю состояния ТП. Оценку периодичности выполнения работ целесообразно произвести из условия получения максимального коэффициента работоспособности ТП.

Можно рассмотреть коэффициент работоспособности ТП в виде

$$K_и = \frac{t_н + t_{пи}}{t_o} = 1 - \frac{t_{рр} + t_в}{t_o}, \qquad (1)$$

где $t_o = t_н + t_{пи} + t_{рр} + t_в$; $t_н$ – среднее время наработки за время t_o; $t_{пи}$ – среднее время простоя ТП, сюда входят и подготовительное время; $t_{рр}, t_в$ – средние времена, затраченные соответственно на регламентные работы и на восстановление ТП; t_o – суммарное время (в часах) эксплуатации ТП за рассматриваемый календарный отрезок времени (исключая плановые настройки и восстановление работоспособности ввиду разладки ТП).

Тщательный анализ причин отказов, установление дополнительных операций контроля и соответствующих результатам контроля профилактических операций иногда могут обеспечить снижение уровня параметра потока (интенсивности) отказов. В данном случае речь идет не об оптимальном межрегламентном периоде, а о выполнении профилактических работ в зависимости от состояния ТП.

Для расчета потока отказов (интенсивности) ТП необходимо определить плотность вероятности распределения времени до отказа $f(t)$.

Будем рассматривать процесс изменения состояния ТП (имеется в виду совокупность технологических операций) как однородный, т.е. с постоянной средней скоростью и постоянным средним квадратическим отклонением скорости или постоянным коэффициентом вариации скорости изменения наблюдаемого в процессе мониторинга параметра (особенности геометрии поверхности). В таком случае кинетическое уравнение процесса можно записать в виде

$$dx(t) = adt + bd\eta(t), \qquad (2)$$

где a – коэффициент сноса (средняя скорость изменения параметра, наблюдаемого в процессе проверок); b^2 – средняя скорость изменения дисперсии параметра.

Если марковский процесс определяется уравнением вида (2), то условная переходная плотность $w(t_0, x_0; t, x)$ этого процесса описывается уравнением Фоккера-Планка-Колмогорова следующего вида:

$$\frac{\partial w(t_0, x_0; t, x)}{\partial t} + a\frac{\partial w(t_0, x_0; t, x)}{\partial x} - \frac{b^2}{2}\frac{\partial^2 w(t_0, x_0; t, x)}{\partial x^2} = 0. \quad (3)$$

Тогда плотность распределения времени достижения границы изучаемым процессом – плотность распределения времени до отказа имеет следующую связь с условной плотностью перехода процесса из одного состояния в другое:

$$f(t) = -\int_{-\infty}^{1} \frac{\partial w(t_0, x_0; t, x}{\partial t} dx . \quad (4)$$

Чтобы определить плотность вероятности распределения времени до отказа $f(t)$, необходимо получить выражение для $\varpi\ (t_0, x_0; t, x)$, решив уравнение (3), затем найти частную производную по времени от функции $w(t_0, x_0; t, x)$ и полученное выражение проинтегрировать по параметру x.

Если реализации имеют немонотонный характер, то после первого достижения границы заданной области (физически это соответствует отказу и снятию наблюдения) немонотонная реализация может снова возвратиться в заданную область и участвовать в наблюдаемом процессе.

Для того чтобы первое достижение границы немонотонной реализацией моделировало отказ и дальнейшая реализация не участвовала в наблюдаемом процессе и не влияла на $w(t, x)$, необходимо на границе заданной области поставить граничное условие типа «поглощающий экран». В таком случае любая реализация, впервые достигнув его, навсегда остается на границе, вне заданной области.

Поскольку выше было установлено, что реализации процесса могут иметь немонотонный характер, в качестве граничных условий при решении уравнения (3) принимаются условия

$$w(t, x)\ \big|_{x=-\infty} = 0 , \quad (5)$$

$$w(t, x)\ \big|_{x=1} = 0 . \quad (6)$$

Первое граничное условие (5) чисто формально. Поскольку изучаемый процесс (определяющий параметр изделий) не может принимать отрицательных значений, установленная левая граница является недостижимой (естественной) и никак не влияет на процесс в заданной области. Принятие формального условия (5) необходимо для решения уравнения (3). Граничное условие (6) вытекает из приведенных соображений и соответствует поглощающему экрану в точке x=1.

Решение уравнения (3) для краевых условий (4) – (6) и последующие оценки распределения параметров отказов и расстроек ТП можно найти в

$$w(t, x) = \frac{1}{b\sqrt{2\pi t}}\left[e^{-\frac{(x-at)^2}{2b^2 t}} - e^{-\frac{(x-at-2)^2-4at}{2b^2 t}}\right]. \quad (7)$$

Вычислим производную

$$\frac{\partial w(t, x)}{\partial t} = \frac{(x^2 - a^2t^2 - b^2 t)}{2b^3 t^2\sqrt{2\pi t}} e^{-\frac{(x-at)^2}{2b^2 t}} -$$

$$- \frac{[(x-2)^2 - a^2t^2 - b^2 t]}{2b^3 t^2\sqrt{2\pi t}} e^{-\frac{(x-at-2)^2 - 4at}{2b^2 t}}.$$

Подставив последнее выражение в (5), проинтегрируем и получим выражение для плотности распределения времени до первого отказа:

$$f(t) = -\int_{-\infty}^{1} \{\frac{(x^2 - a^2t^2 - b^2t)}{2b^3t^2\sqrt{2\pi t}} e^{-\frac{(x-at)}{2b^2t}} -$$

$$-\frac{[(x-2)^2 - a^2t^2 - b^2t}{2b^3t^2\sqrt{2\pi t}} e^{-\frac{(x-at-2)^2}{2b^2t}} \} dx.$$

Окончательно выражение для плотности распределения времени до отказа ТП

$$f(t) = \frac{1}{bt\sqrt{2\pi t}} e^{-\frac{(1-at)^2}{2b^2t}}. \quad (8)$$

Полученное распределение может быть использовано для описания расстройки ТП при нелинейном изменении среднего значения параметра. При этом неоднородный процесс квантуется на однородные участки и время выхода за предельный уровень получается в результате свертки времени наработки на линеаризованных участках.

Например, процесс расстройки позволяет выделить два однородных участка. На первом участке до наработки некоторого условного значения параметра процесс протекает со средней скоростью a_1 и коэффициентом вариации ν_1. При этом время наработки на первом участке имеет некоторую случайную величину T_1. Далее, до разрушения процесс имеет характеристики a_2 и ν_2. Время наработки на втором участке составляет случайную величину T_2. Тогда, при условии независимости времени наработки на линеаризованных участках, распределение времени общей наработки $t = T_1 + T_2$ примет следующий вид:

$$f^*(t) = \int_0^{\infty} f(t - T_1) f(T_1) dT_1, \quad (9)$$

где $f(T_1) = \frac{1}{\nu_1 T_1 \sqrt{2\pi a_1 T_1}} e^{-\frac{(1-a_1T_1)^2}{2\nu_1^2 a_1 T_1}}$ – плотность распределения наработки T_1 на первом участке; $f(T_2) = f(t - T_1) = \frac{1}{\nu_2 T_2 \sqrt{2\pi a_2 T_2}} e^{-\frac{(1-a_2T_2)^2}{2\nu^2 2a_2 T_2}}$ – плотность распределения наработки T_2 на втором участке.

Математическое ожидание распределения (9)

$$M[T] == \frac{1}{a_1} + \frac{1}{a_2} = \frac{a_1 + a_2}{a_1 a_2}. \quad (10)$$

Дисперсия искомого распределения (9)

$$D[T] == \frac{\nu^2_1}{a^2_1} + \frac{\nu^2_2}{a^2_2}. \quad (11)$$

Можно рассмотреть монотонное течение процесса расстройки. Если процесс имеет монотонные реализации, то первое пересечение границы любой реализацией будет одновременно и последним, т.е. реализация в дальнейшем уже больше никогда и никак не будет влиять на наблюдаемый процесс. Это означает, что нет необходимости в установлении каких-либо условий на границе заданной области. В связи с последним в качестве граничных условий принимаются

$$w(t,x)\big|_{x=-\infty} = w(t,x)\big|_{x=+\infty} = 0. \quad (12)$$

Границы (12) являются недостижимыми для изучаемого процесса и никак не влияют на процесс в заданной области. Это чисто формальные граничные условия, необходимые для решения уравнения (3).

В качестве начального условия используется (4). Аналогично без потери общности приняты нулевые начальные условия $(t_0 = 0, x_0 = 0)$.

Решение уравнения (3) с краевыми условиями (12) записывается в виде

$$w(t,x) = \frac{1}{b\sqrt{2\pi t}} e^{-\frac{(x-at)^2}{2b^2 t}}. \quad (13)$$

Математическое ожидание

$$M[T] = (1/a)(1+\nu^2/2). \quad (14)$$

Дисперсия

$$D\{T] = (\nu^2/a^2)(1+5\nu^2/4). \quad (15)$$

Полученные распределения позволяют вычислить зависимость интенсивности отказов от времени. Кривые интенсивностей монотонных $\lambda_1(t)$ и немонотонных распределений $\lambda_2(t)$ начинаются с нуля, т.е. $\lambda_1(0) = \lambda_2(0) = 0$. Определим поведение интенсивностей при $t \to \infty$:

$$\lim_{t\to\infty} \lambda_1(t) = \lim_{t\to\infty} \frac{f(t)}{1-F(t)} = \lim[\frac{\partial \ln f(t)}{\partial t}] = \frac{a}{2\nu^2}.$$

Основным вопросом, возникающим при обработке опытных данных, является оценка параметров распределений. Они могут быть вычислены как на основе статистики отказов, так и на основе физических характеристик процессов расстройки ТП, а также путем совместного использования обоих типов информации.

3. Практические приложения результатов исследований

Унифицированный комплекс мониторинга цифровых модулей систем ЧПУ.

Были апробированы в производстве РЭС разработанные средства мониторинга технологической среды, которые позволяют наблюдать состояния систем ЧПУ. Основными характеристиками средств мониторинга являются: использование усовершенствованных устройств предварительной обработки информации; применение устройств сжатия диагностической информации; модификация алгоритмов обработки диагностической информации на основе идей последовательного анализа; построение гибких автоматизированных систем диагностики и контроля на основе мультипроцессорных систем с развитыми интерактивными средствами и возможностью модификации.

В связи с этим апробация проведена в направлении проверки информационного, математического и программного обеспечения комплекса диагностики и контроля, обеспечивающего оптимизацию процесса поиска дефектов. Выполненное при этом моделирование необходимо, так как фактически ни одна микропроцессорная система ЧПУ, применяемая в технологическом оборудовании, не имеет исчерпывающего математического описания.

При моделировании микропроцессорных систем использовалось три уровня описания: алгоритмический; функциональный; вентильный.

Такая последовательность, как показала практика, является наиболее оптимальной с точки зрения снижения трудоемкости и уменьшения временных характеристик процесса мониторинга систем ЧПУ.

Для мониторинга таких систем апробировано создание целостного технологического процесса контроля и прогнозирования цифровых систем технологического оборудования. При таком подходе значительно (в 10-12 раз) снижается трудоемкость мониторинга, уменьшается вероятность появления ошибок, существенно снижается стоимость аппаратных средств диагностики, понижается себестоимость процесса контроля. Определена возможность реализации процесса мониторинга цифровых модулей систем СУТО в условиях полной или частичной неопределенности при высокой сложности объекта мониторинга.

Апробация проводилась на цифровых модулях следующих систем УЧПУ: 2С42, НЦ-31, BOSCH CC-300, CNC-600, ELSA-1000, SINUMERIC-8.5M, SIMATIC-S5. Она показала существенное увеличение эффективности процесса обнаружения неработоспособного состояния цифровых модулей с применением разработанных методов. При этом трудоем-

кость процесса с применением разработанного унифицированного комплекса диагностики и контроля снизилась в 3,6 раза.

Разработанные теоретические основы мониторинга позволили создать новые эффективные технологии производства и контроля РЭС [3-7], усовершенствовать систему технического обслуживания и профилактики ТП, которая обеспечивает своевременную настройку ТП, уменьшая тем самым простои и количество брака. Усовершенствование осуществлено в направлении создания аппаратного, математического и программного обеспечения приведенных ниже подсистем.

Подсистема повышения надежности ТП. Основные функции подсистемы: обработка статистической информации о расстройках и отказах; оценка реального технического состояния и надежности ТП; выбор теоретической модели надежности и системы на основе информации, получаемой в процессе функционирования ТП.

Подсистема первичной обработки статистической информации для сортировки и накопления статистических данных о работе ТП. Входными данными подсистемы являются компоненты информационного вектора, поступающего из диагностической зоны мониторинга ТП, а именно: технологическая операция и связанные с ней оперативные характеристики. Разработанное математическое и программное обеспечение осуществляет формирование общих данных о расстройках режимов, отказах и сбоях оборудования и оснастки. Граф-схема алгоритма программы представлена на рис. 2.

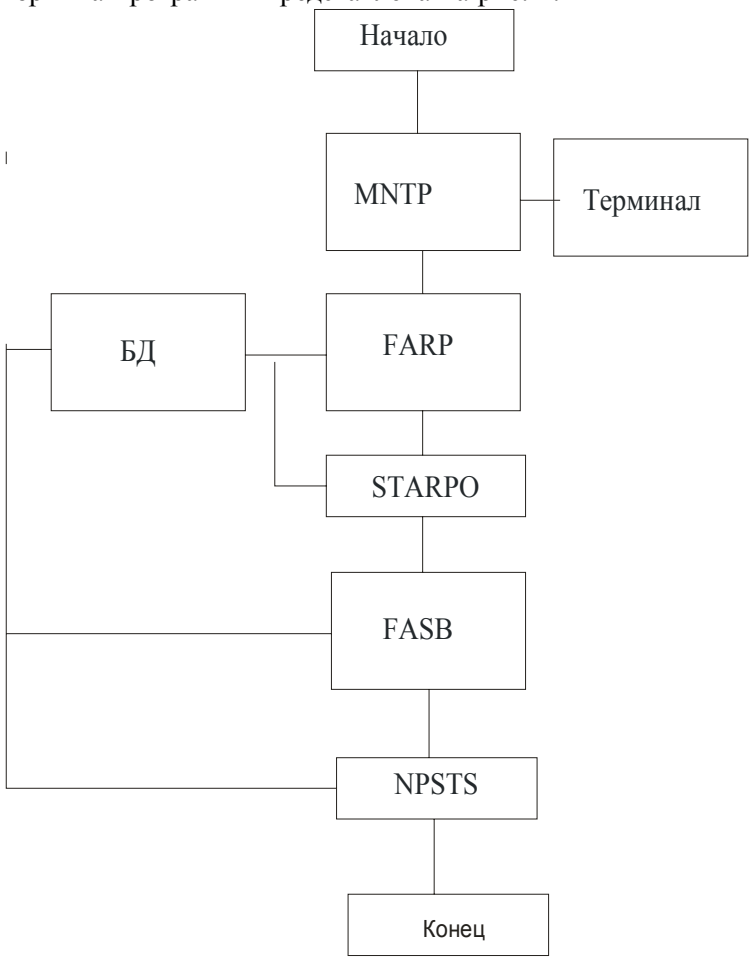


Рис. 2. Граф-схема алгоритма программы обработки статистической информации

В подсистеме выбора модели и прогнозирования расстроек ТП осуществляется анализ наиболее адекватной теоретической модели, описывающей изменение характеристик ТП. В качестве исходных данных используется информация, содержащаяся в БД, созданных предыдущими подсистемами. Здесь решаются следующие задачи: оценка характеристик выборочного распределения отказов (расстроек); оценка параметров и характеристик

конкурирующих теоретических моделей; вычисление обобщенного критерия согласия теоретической модели с эмпирическими данными; выбор наиболее адекватной теоретической модели. Работа программы начинается с ввода номера ТП, статистика отказов (расстроек) которого будет подвергнута анализу. Если имеется состоятельная статистика (n>15), то для оценки характеристик выборочного распределения оцениваются параметры эмпирической функции изменения и прогнозирования характеристик ТП.

4. Выводы

Усовершенствованы методы и средства мониторинга производственной среды при изготовлении РЭС в направлении совершенствования систем технического обслуживания технологического оборудования, использующего цифровые системы управления и контроля. Приведены основы теории и новая концепция мониторинга жизненного цикла РЭС на этапах проектирования, производства и эксплуатации, в основе которой положено отображение информации на основе визуализации процессов. Показано, что реализация такой концепции является существенным дополнением информационной поддержки жизненного цикла, обеспечивая решение задач принятия решений в условиях неопределенности и включением человека в управление жизненным циклом.

Апробация показала существенное увеличение эффективности процесса обнаружения неработоспособного состояния цифровых модулей с применением разработанных методов. При этом трудоемкость процесса с применением разработанного унифицированного комплекса диагностики и контроля снизилась в 3,6 раза. Разработанные теоретические основы мониторинга позволили создать новые эффективные технологии производства и контроля РЭС, усовершенствовать систему технического обслуживания и профилактики ТП, которая обеспечивает своевременную настройку ТП, уменьшая тем самым простои и количество брака.

Список литературы: 1. *Андрианов А.С.* Ремонтное обслуживание промышленного оборудования на основе корпоративной информационной системы // Вестник саратовского государственного технического университета. 2009. Вып. 1, №2 (38). С. 187-192. **2.** *Андрианов А.С.* Процессный подход к управлению техническим обслуживанием и ремонтом промышленного оборудования // Сб. научных трудов «Труды соискателей и аспирантов». Саратов. Научная книга. 2008. С. 19-35. **3.** *Андрусевич А.А., Невлюдов И.Ш.* Оценивание технологических свойств основных и вспомогательных материалов в производстве электронной техники / Вісті Академії інженерних наук України. Харків: «ХАИ», 2004. №4(24). С. 120-124. **4.** *Андрусевич А.А., Невлюдов И.Ш., Второв Е.П.* Оценивание физико-химической активности материалов для монтажа электронной техники. Науч.-техн. журнал. «Технология приборостроения» 2004. № 1. С. 32-37. **5.** *Андрусевич А.А., Невлюдов И.Ш., Жупинский В.А.* Исследование показателей качества монтажных материалов // Технология приборостроения. 2004. №2. С. 24-29. **6.** *Андрусевич А.А., Невлюдов И.Ш., Роздоловский Ю.М., Второв Е.П., Сотник С.В.* Оценивание свойств материалов, образующих монтажные соединения электронной техники // Технология приборостроения. 2005. №2. С. 51-59. **7.** *Андрусевич А.А., Невлюдов И.Ш. Стародубцев Н.Г., Роздоловський Ю.М.* Залучення засобів технічного зору для технологічного моніторингу монтажних з'єднань у виробництві електронної техніки // Науково-технічний та громадянський часопис Президії Академії інженерних наук України Вісті Академії інженерних наук України. Харків: «ХАИ», 2006. № 3(30). С. 167-172.

Поступила в редколлегию 02.09.2011

Андрусевич Анатолий Александрович, директор Криворожского авиационного колледжа. Научные интересы: технология приборостроения, мониторинг процессов изготовления радиоэлектронных систем, проблемы повышения надёжности функционирования радиоэлектронных систем. Адрес: Украина, 50045, Кривой Рог, ул. Туполева, 1, тел. (0564) 27-56-79. E-mail: uchebotdel@kk.nau.edu.ua

Невлюдов Игорь Шакирович, д-р техн. наук, проф., зав. каф. ТАПР ХНУРЭ. Научные интересы: технология приборостроения, гибкие производственный системы, робототехника. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. (057) 702-14-86. E-mail: tapr@khture.kharkov.ua

Донсков Александр Николаевич, аспирант каф. ТАПР ХНУРЭ. Научные интересы: технология приборостроения, технология микроструктурированных оптических волокон. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. (057) 702-14-86. E-mail: tapr@khture.kharkov.ua

УДК 658.512.011:681.326:519.713

В.И. ХАХАНОВ, МУРАД АЛИ А., BAGHDAD AMMAR AVNI ABBAS, О.А. ГУЗЬ, И.В. ХАХАНОВА

МЕТРИКА И КРИТЕРИИ АНАЛИЗА КИБЕРПРОСТРАНСТВА

Предлагаются метрика и критерии качества взаимодействия объектов при анализе киберпространства, представленного в двоичном и многозначном исчислении. Показываются направления использования оценок для задач поиска, распознавания и принятия решений.

1. Введение

Инфраструктура киберпространства должна иметь развитую сеть сервисов, обеспечивающих быстрый поиск необходимых данных распараллеливания вычислительных процессов путем имплементации функциональностей в кристаллы специализированных цифровых систем. Такая плата в настоящее время вполне допустима, поскольку существуют проблемы заполнения площадей силиконового кристалла, который содержит до 1 миллиарда вентилей при толщине пластины, равной 5 микрон. При этом современные технологии допускают создание пакета или «сэндвича», содержащего до 7 кристаллов, что соизмеримо с объемом нейронов головного мозга человека. Практически «беспроводное» соединение таких пластин основывается на технологической возможности сверления порядка 10 тысяч сквозных отверстий (vias) на 1 квадратном сантиметре. Наполнить полезной функциональностью такой объем допустимых на кристалле вентилей в настоящее время проблематично. Поэтому можно и нужно использовать «жадные» к аппаратуре модели и методы для создания быстродействующих средств параллельного решения практических задач. Имея в виду дискретность и многозначность алфавитов описания информационных процессов, свойство параллелизма является особенно востребованным при создании эффективных и интеллектуальных «движков» для киберпространства или интернета [1].

Проблема создания эволюционирующего кибернетического пространства (Evolutive Cyber Space) и его инфраструктуры в последние годы является весьма привлекательной темой для крупного IT–бизнеса. Принципиальная позиция ECS – генерирование новых сервисов на основе мирового опыта, скрытого в информационном пространстве. Согласно запрету Геделя, адаптированному для информационного пространства, нельзя создать интеллектуальную структуру, которая решит любые задачи, формально представленные спецификацией. Тем не менее, принцип Геделя предоставляет методологическую основу эволюции (саморазвития) киберпространства на основе синтеза полезных спецификаций, которые не покрываются существующими у человечества примитивами решений, что обусловливает создание нового функционального или технологического компонента для его последующего использования в новых сервисах. ECS закономерно повторяет эволюцию человечества, только в тысячи раз более быстрыми темпами, с точностью до изоморфизма создавая виртуальный киберобраз нашего мира со всеми его позитивными и негативными свойствами. Соотношение реального мира и виртуального киберпространства можно представить симметрической разностью (xor-операция на замкнутом теоретико-множественном алфавите), не равной пустому множеству $W \oplus C \neq \varnothing$. Более того, всегда будет существовать между двумя мирами степень различия, показывающая и определяющая стремление обоих миров к сближению через совершенство, которое уменьшает степень различия (рис.1):

$$W \oplus C = D,$$
$$D = \{W^*, C^*\}, W^* \in W, C^* \in C,$$
$$W = \{W^c, W^*\}, C = \{C^c, C^*\}.$$

Здесь $W^* \in W$ – интеллект человека и человечества, еще не имплементированный в киберпространство; $C^* \in C$ – интеллект (вычислительный, запоминающий, технологический, коммуникационный) киберпространства, которого (еще) нет у человечества.

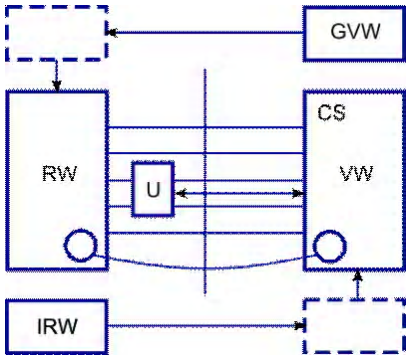
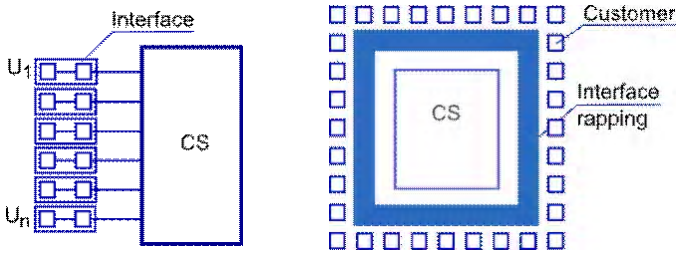


Рис. 1. Взаимодействие реального мира и киберпространства

Пространства (кибернетического) всегда будет мало! Как памяти и производительности компьютера. При этом пользователь всегда будет платить за ненужные функциональности. Понятие персонального компьютера теряет свою актуальность ввиду появления облачных сервисов в киберпространстве, временная аренда которых становится экономически более выгодной по сравнению с покупкой программных продуктов. Компьютер, на пути к созданию интерфейсной оболочки глобального киберпространства, трансформируется в гаджет, типа IPhone, а затем – в электронную таблетку (tablet) – идентификатор. Сегодня необходим лишь любой, пока что аппаратный, интерфейс связи с киберпространством (рис. 2,а). Завтра будет создана непрерывная и глобальная инфраструктура киберпространства, не предусматривающая наличия у пользователя «тяжелых» интерфейсных гаджетов для входа в интернет (рис. 2,б).



а б

Рис. 2. Трансформирование инфраструктуры киберпространства

Агрессивность интернета и прозрачность общего «дома» порождает естественное желание каждого пользователя создать свой собственный микромир. Необходима личная киберячейка или квартира, где человек может и должен быть один. Виртуальный индивидуальный киберкомпьютер ($C^v = \{D,S,C^i,I,M\}$ – данные, сервисы, интеллектуальная система управления, инфраструктура и монитор для ввода-вывода информации) – возможное решение данной проблемы.

Новое свойство возникает при взаимодействии (суперпозиции) не менее двух различных компонентов $W \oplus C = D \neq \varnothing$. Если же $W \oplus C = \varnothing$, то $W = C$. Если в качестве компонентов выступают примитивы, то степень их различия равна объединению таких компонентов.

Доказательство. Пусть имеются два примитива, входящие в универсум $\{a,b\} \in U$. Тогда на основании определения симметрической разности можно получить $a \oplus b = (a \cap \bar{b}) \cup (\bar{a} \cap b) = (a \cap U \setminus b) \cup (U \setminus a \cap b) = (a \cup b)$, поскольку $a \in (U \setminus b), b \in (U \setminus a)$.

Иначе – фиксируется результат $a \oplus b = (a \cup b) = \{a,b\}$. Если объекты в пространстве не имеют общих точек (не пересекаются), то степень их различия равна объединению объектов. Сказанное выше в равной степени относится и к примитивам.

Цель – усовершенствование метрики и критериев качества взаимодействия объектов при анализе киберпространства, представленного в двоичном и многозначном исчислении.

Задачи: 1) Показать направления использования оценок для поиска, распознавания и принятия решений в киберпространстве [1-5]. 2) Определить критерии качества (скалярный и векторный) взаимодействия информационных объектов для анализа и синтеза двоичных и многозначных данных в кибернетическом пространстве [1, 6, 7].

2. Метрика и критерии взаимодействия объектов в киберпространстве

Основываются на использовании бета-метрики [1-3] измерения расстояний в киберпространстве. Киберпространство – дискретное векторно-логическое пространство – совокупность взаимодействующих по соответствующей метрике информационных процессов и явлений, описываемых векторами логических переменных и использующих в качестве носителя компьютерные системы и сети. Метрика – способ измерения расстояния в пространстве между компонентами процессов или явлений, описанных векторами логических переменных. Расстояние (булева производная, степень изменения, различия или близости) в киберпространстве определяется xor-отношением векторов, обозначающих компоненты процесса или явления, что отличает его от кодового расстояния по Хэммингу. Процедуры сравнения, измерения, оценивания, распознавания, тестирования, диагностирования, оперируют xor-отношением объектов. Компонент пространства представлен k-мерным вектором $a = (a_1, a_2, ..., a_j, ..., a_k)$, $a_j \in \{0,1\}$, где каждая его координата определена в двоичном алфавите, 0 – «ложь», 1 – «истина». Нуль-вектор есть k-мерный кортеж, все координаты которого равны нулю: $a_j = 0, j = \overline{1,k}$.

Метрика β кибернетического пространства определяется равенством

$$\beta = \bigoplus_{i=1}^{n} d_i = 0,$$

которое формирует нуль-вектор для xor-суммы расстояний d_i между ненулевым и конечным числом объектов, замкнутых в цикл. Здесь n – количество расстояний между компонентами (векторами) пространства, составляющими цикл $D = (d_1, d_2, ..., d_i, ..., d_n)$, d_i – есть вектор расстояния, соответствующий ребру цикла, соединяющему два компонента (вектора) a, b пространства, который далее обозначается без индекса как $d(a,b)$. Расстояние между двумя объектами a и b есть производный вектор: $d(a,b) = (a_j \oplus b_j)_1^k$. Векторному значению расстояния соответствует норма (скаляр), определяемая кодовым расстоянием по Хэммингу между двумя векторами в виде числа единиц вектора $d(a,b)$. Метрика β векторного логического двоичного пространства есть равная нуль-вектору xor-сумма расстояний между конечным числом вершин графа, образующих цикл. Теперь можно дать более формальное определение киберпространства, как векторно-логическое, нормируемое β-метрикой, где xor-сумма расстояний между конечным числом точек цикла равна нуль-вектору. Определение метрики через отношения позволяет сократить систему аксиом (тождественности, симметрии и транзитивности треугольного замыкания) с трех до одной и распространить ее действие на сколь угодно сложные структуры n-мерного логического пространства. Классическое задание метрики для определения взаимодействия одной, двух и трех точек в векторном логическом пространстве является частным случаем β-метрики при $i = 1,2,3$ соответственно:

$$M \subset \beta = \begin{cases} d_1 = 0 \leftrightarrow a = b; \\ d_1 \oplus d_2 = 0 \leftrightarrow d(a,b) = d(b,a); \\ d_1 \oplus d_2 \oplus d_3 = 0 \leftrightarrow d(a,b) \oplus d(b,c) = d(a,c). \end{cases}$$

Векторно-логический транзитивный треугольник имеет полную аналогию численному измерению расстояния в метрическом M-пространстве, которое задается системой аксиом, определяющей взаимодействие одной, двух и трех точек в любом пространстве:

$$M = \begin{cases} d(a,b) = 0 \leftrightarrow a = b; \\ d(a,b) = d(b,a); \\ d(a,b) + d(b,c) \geq d(a,c). \end{cases}$$

Специфика аксиомы треугольника (метрического) М-пространства заключается в численном (скалярном) сравнении расстояний трех объектов. При этом интервальная неопределенность ответа – две стороны треугольника могут быть больше либо равны третьей – малопригодна для определения точной длины последней стороны. Бета-метрика устраняет данный недостаток и исключает неопределенность бинарного отношения детерминированных процессов или явлений. Третья сторона треугольника в векторном логическом пространстве определяется двоичным вектором-расстоянием между двумя вершинами путем вычисления xor-суммы расстояний двух других сторон треугольника: $d(a,b) \oplus d(b,c) = d(a,c) \rightarrow d(a,b) \oplus d(b,c) \oplus d(a,c) = 0$.

Метрика β кибернетического многозначного векторно-логического пространства, есть вектор, равный значению $\varnothing$ по всем координатам, полученный путем применения симметрической разности расстояний между конечным числом точек, образующих цикл:

$$\beta = \underset{i=1}{\overset{n}{\Delta}} d_i = \varnothing .$$

Здесь каждая координата вектора, соответствующего объекту, определена в алфавите, составляющем булеан на универсуме примитивов мощностью p:

$$a_j = \{\alpha_1, \alpha_2, ..., \alpha_r, ..., \alpha_m\}, m = 2^p .$$

На основе введенной метрики анализа киберпространства вводятся критерии оценивания взаимодействия конечного числа объектов между собой [1-3]. Скалярный критерий взаимодействия двух объектов (процессов) в дискретном булевом пространстве, представленных k-мерными многозначными векторами

$$m = (m_1, m_2, ..., m_j, ..., m_k),\ m_j \in \{0,1,x\} \text{ и } A = (A_1, A_2, ..., A_j, ..., A_k),\ A_j \in \{0,1,x\},$$

необходим для сравнения и последующего выбора, лучшего в некотором смысле, решения. Степень принадлежности m-вектора к A обозначается как $\mu(m \in A)$, непринадлежности – $\overline{\mu}(m \in A)$. Существует 5 типов теоретико-множественного взаимодействия двух векторов:

1) $m = A$; 2) $m \subset A$; 3) $A \subset m$; 4) $m \cap A \neq \{m, A, \varnothing\}$; 5) $m \cap A = \varnothing$.

Цель скалярного критерия – оценить любое из указанных взаимодействий интервальной оценкой [0,1] путем совместного использования трех параметров: кодового расстояния $d(m,A)$ и двух функций непринадлежности $\overline{\mu}(m \in A) = 1 - \mu(m \in A)$, $\overline{\mu}(A \in m) = 1 - \mu(A \in m)$:

$$Q = \frac{1}{3}\left[\frac{1}{k} d(m,A) + [1 - \mu(m \in A)] + [1 - \mu(A \in m)]\right],$$

$$d(m,A) = \text{card}\,(m_i \underset{i=1}{\overset{k}{\cap}} A_i = \varnothing);$$

$$\mu(m \in A) = 2^{c-a};$$

$$\mu(A \in m) = 2^{c-b};$$

$$a = \text{card}\,(A_i = x), i = \overline{1,k};$$

$$b = \text{card}\,(m_i = x), i = \overline{1,k};$$

$$c = \text{card}\,(m_i \underset{i=1}{\overset{k}{\cap}} A_i = x).$$

Здесь $d(m,A)=\mathrm{card}\,(m_i \overset{k}{\underset{i=1}{\cap}} A_i=\varnothing)$ – мощность или количество пустых координатных пересечений двух взаимодействующих векторов, составляющих расстояние по Хэммингу; $\mu(m\in A)=2^{c-a}$ $(\mu(A\in m)=2^{c-b})$ – отношение общего для m и A пространства к пространству вектора A (m), что формирует указанную функцию принадлежности. Операции координатного пересечения (and), симметрической разности (xor) определены для символов алфавита Кантора $A=\{0,1,x=\{0,1\},\varnothing\}$, кодируемых векторами (01,10,11,00) соответственно:

$\cap$	0	1	x	$\varnothing$
0	0	$\varnothing$	0	$\varnothing$
1	$\varnothing$	1	1	$\varnothing$
x	0	1	x	$\varnothing$
$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$

$\wedge$	01	10	11	00
01	01	00	01	00
10	00	10	10	00
11	01	10	11	00
00	00	00	00	00

Δ	0	1	x	$\varnothing$
0	$\varnothing$	x	1	0
1	x	$\varnothing$	0	1
x	1	0	$\varnothing$	x
$\varnothing$	0	1	x	$\varnothing$

$\oplus$	0	1	x	$\varnothing$
0	00	11	10	01
1	11	00	01	10
x	10	01	00	11
$\varnothing$	01	10	11	00

Нормирование параметров критерия (кодового расстояния и функций непринадлежности) позволяет оценить уровень взаимодействия векторов в численном интервале [0,1]. С учетом изоморфизма теоретико-множественных и логических операций критерий качества можно трансформировать к виду:

$$Q=\frac{1}{3}\left[\frac{1}{k}d(m,A)+[1-\mu(m\in A)]+[1-\mu(A\in m)]\right],$$

$$d(m,A)=\mathrm{card}\,(m_i \overset{k}{\underset{i=1}{\oplus}} A_i=U);$$

$$\mu(m\in A)=\mathrm{card}\,(A_i=U)-\mathrm{card}\,(m_i \overset{k}{\underset{i=1}{\wedge}} A_i=U);$$

$$\mu(A\in m)=\mathrm{card}\,(m_i=U)-\mathrm{card}\,(m_i \overset{k}{\underset{i=1}{\wedge}} A_i=U);$$

$$U=\begin{cases}1\leftarrow\{m_i,A_i\}\in\{0,1\};\\ x\leftarrow\{m_i,A_i\}\in\{0,1,x\}.\end{cases}$$

Если векторы m и A – двоичные по всем координатам, то переменная U=1 и вычисления проводятся по правилам двоичной $\oplus$–операции. Если векторы m и A определены в троичном алфавите, то переменная U = x инициирует вычисления на основе использования теоретико-множественной операции симметрической разности Δ. Первый компонент $\frac{1}{n}d(m,A)$ критерия формирует степень несовпадения k-мерных векторов в виде кодового расстояния по Хэммингу, отнесенного к длине вектора, путем выполнения операции xor над всеми координатами; второй и третий компоненты $[1-\mu(m\in A)]+[1-\mu(A\in m)]$ определяют степени непринадлежности результата конъюнкции к пространству каждого из двух взаимодействующих векторов. Если такие степени равны нулю $\frac{1}{n}d(m,A)=0,\ [1-\mu(m\in A)]=0,\ [1-\mu(A\in m)]=0$, то объекты идентичны друг другу. Понятия принадлежности и непринадлежности являются взаимодополняющими, но в данном случае технологичнее вычислять непринадлежность, поскольку общепринятым в литературе является понятие нулевого расхождения объектов, свидетельствующее об их полной идентичности. Данный критерий работает в интервале [0,1]. Полное совпадение двух объектов $d(m,A)=0,\ \mu(m\in A)=1,\ \mu(A\in m)=1$ характеризуется нулевой оценкой крите-

рия $Q = \frac{1}{3}\left[\frac{1}{k}0 + [1-1] + [1-1]\right] = 0$. Противоположным вариантом является максимальное несовпадение двух объектов: $d(m, A) = k,\ \mu(m \in A) = 0,\ \mu(A \in m) = 0$, которое определяется оценкой взаимодействия: $Q = \frac{1}{3}\left[\frac{1}{k}k + [1-0] + [1-0]\right] = 1$. Если параметры взаимодействия равны $d(m, A) = 0,\ \mu(m \in A) = \frac{1}{2},\ \mu(A \in m) = \frac{1}{2}$, то критерий будет иметь следующую оценку: $Q = \frac{1}{3}\left[\frac{1}{k}0 + [1-\frac{1}{2}] + [1-\frac{1}{2}]\right] = \frac{1}{3}$. Взаимодействие (пересечение) двух векторов: A = (XXX1X) и m = (XX0X0) дает общее пространство, равное (XX010) = {00010, 01010, 10010, 11010}. Критерий качества взаимодействия при параметрах $d(m, A) = 0,\ \mu(m \in A) = \frac{1}{2},\ \mu(A \in m) = \frac{1}{4}$ будет иметь следующую оценку: $Q = \frac{1}{3}\left[\frac{1}{k}0 + [1-\frac{1}{2}] + [1-\frac{1}{4}]\right] = \frac{1}{4}$.

Достоинство введенного критерия (непринадлежности, различия) заключается в линейности изменения его численного значения от 0 до 1 по мере увеличения «расстояния» от полного совпадения двух объектов до максимально возможного, когда кодовое расстояние равно $d(m, A) = k$.

Критерий может быть использован в задачах отслеживания цели, движения по заданному маршруту, диагностирования функциональных нарушений, поиска, распознавания и принятия решений. Критерий качества Q, используемый для выполнения регуляторной функции при оценивании взаимодействия объектов в реальном масштабе времени, необходимо минимизировать.

Тем не менее, скалярная оценка имеет только интегральные свойства взаимодействия двух объектов, что позволяет осуществлять сравнение нескольких расстояний, чаще меры близости одного объекта по отношению к конечному множеству других. Недостатком интегральной оценки является неоднозначность ее приведения к исходному векторному эквиваленту, как и любого другого функционального отношения: прямая импликация однозначна, обратная – многозначна. Поэтому полная картина анализа взаимодействия объектов должна содержать не только интегральный скалярный критерий Q, но и результат их векторного отношения $Q(m, A) = m \oplus A$, который более информативен для последующей коррекции направления решения задач синтеза или анализа процессов взаимодействия в рамках существующей системы. Как получить векторный критерий качества взаимодействия двух объектов? Формула скалярного критерия качества после проведения векторных операций использует процедуры вычисления трех компонентов: кодовое расстояние, определяемое числом единиц в координатах результирующего вектора, полученного на основе xor-операции $d(m, A) = m \oplus A$, и две функции принадлежности $\mu = \mu(m \in A) \vee \mu(A \in m) = (A \wedge \overline{m \wedge A}) \vee (m \wedge \overline{m \wedge A})$, которые в совокупности также определяются xor-операцией, в общем случае на замкнутом теоретико-множественном алфавите:

$$\mu = (A \wedge \overline{m \wedge A}) \vee (m \wedge \overline{m \wedge A}) = [A \wedge (\overline{m} \vee \overline{A})] \vee [m \wedge (\overline{m} \vee \overline{A})] =$$
$$= [(A \wedge \overline{m}) \vee (A \wedge \overline{A}) \vee (m \wedge \overline{m}) \vee (m \wedge \overline{A})] =$$
$$= (A \wedge \overline{m}) \vee (m \wedge \overline{A}) = m \oplus A.$$

Логическое объединение двух векторных функций, формирующих кодовое расстояние и взаимную принадлежность друг другу, дает, естественно, искомый результат:

$$Q = d(m, A) \vee [\mu(m \in A) \vee \mu(A \in m)] = (m \oplus A) \vee (m \oplus A) = m \oplus A.$$

Это означает, что по существу взаимодействие любых объектов в киберпространстве определяется выполнением симметрической разности в многозначном алфавите (xor-операции в двоичном):

Δ	0	1	x	∅
0	∅	x	1	0
1	x	∅	0	1
x	1	0	∅	x
∅	0	1	x	∅

0=01; 1=10
x=11; ∅=00 →

⊕	0	1	x	∅
0	00	11	10	01
1	11	00	01	10
x	10	01	00	11
∅	01	10	11	00

Но при кодировании символов алфавита двоичными векторами-примитивами операция симметрической разности между символами в координатах векторов превращается в xor-операцию двоичных векторов. Другие логические операции при формировании векторной оценки взаимодействия объектов в киберпространстве, согласно приведенным выше формулам, не используются. В качестве примера ниже предложены процедуры выполнения операции симметрической разности и xor над двумя формами объектов, представленными в виде символов алфавита Кантора и двоичных кодов:

m =	x	x	x	x	1	0	1	0
A =	1	0	0	x	x	x	1	0
Δ =	0	1	1	∅	0	1	∅	∅
m =	11	11	11	11	10	01	10	01
A =	10	01	01	11	11	11	10	01
⊕ =	01	10	10	00	01	10	00	00

Второй пример иллюстрирует вычисление взаимодействия векторов в двухтактном алфавите описания автоматных переменных $B^2(Y)$ в форматах символьного и двоичного описания координат:

m =	Y	A	B	S	P	L	E	Q
A =	H	S	J	L	E	L	F	C
Δ =	L	B	H	E	H	∅	Y	Y
m =	1111	1100	0011	1001	0110	1101	0100	1000
A =	0010	1001	0001	1101	0100	1101	1011	0111
⊕ =	1101	0101	0010	0100	0010	0000	1111	1111

Здесь интересен факт, что в кубитном формате описания символьных переменных теоретико-множественные, в общем случае последовательно выполняемые, операции над элементами множеств заменяются параллельными операциями, что существенно повышает быстродействие вычислительных процессов анализа моделей за счет соответствующего увеличения объема памяти. Для создания кубитных структур данных вычислительных процессов необходимо определить: 1) универсум примитивов (процессов или явлений) с последующим их унитарным кодированием в пределах кубита; 2) компактную систему (структуру) отношений (функциональных), задающих поведение объекта; 3) последовательность обработки компонентов структуры на основе параллельного выполнения векторных логических операций, заменяющих теоретико-множественные, последовательные во времени, вычислительные процедуры.

Две формы (скалярная и векторная) существования критерия качества $q = \{Q, Q(m, A)\}$ направлены на выбор лучшего решения (для пользователя) и детализацию различий между объектами (для компьютера) соответственно. Численный эквивалент удобен для человека, который не способен оперировать лингвистическими (многозначными) переменными при оценке взаимодействия объектов, представленных векторами. К тому же две одинаковые численные оценки не означают идентичности двух расстояний при взаимодействии трех объектов в пространстве. Например: d(a,b) = 0011 = 2, d(a,c) = 1100 = 2, при a = 0000, b = 1100, c = 0011. Поэтому к скалярной оценке необходимо иметь векторный эквивалент критерия качества взаимодействия, который показывает структуру сходства и различия по всем параметрам (переменным) векторов.

Вычислить критерий – значит определить степень принадлежности или непринадлежности данного процесса или явления, в том числе к некоторому классу объектов. Такая классификация, путем сравнения анализируемого объекта с семейством, но представленным в форме одного обобщенного вектора, дает возможность существенно повысить быстродействие задач анализа структур данных. Для этого необходимо создавать иерархические форматы структур данных, ориентированные на компактное представление специальным образом закодированных объектов. При представлении объекта киберпространства совокупностью теоретико-множественных или кубитных переменных структура вектора делится на сегменты, соответствующие кубиту. Кубитная переменная (кубит) – совокупность n двоичных разрядов, необходимых для унитарного кодирования n примитивов и булеана порожденных символов. Формы представления вектора кубитных переменных: символьная и/или кубитно-двоичная, ориентированы на параллельное выполнение теоретико-множественных операций $(\cap,\cup,\tilde{m})$ с помощью алгебры векторной логики $(\wedge,\vee,\overline{m})$ [11]. Примеры таких операций в упомянутых форматах представлены ниже:

m =	Y	A	B	S	P	L	E	Q
A =	H	S	J	L	E	L	F	C
$\cap$ =	H	Q	J	S	E	L	∅	∅
m =	1111	1100	0011	1001	0110	1101	0100	1000
A =	0010	1001	0001	1101	0100	1101	1011	0111
$\vee$ =	0010	1000	0001	1001	0100	1101	0000	0000
m =	Y	A	B	S	P	L	E	Q
$\tilde{m}$ =	∅	B	A	P	S	H	F	C
m =	1111	1100	0011	1001	0110	1101	0100	1000
$\overline{m}$ =	0000	0011	1100	0110	1001	0010	1011	0111

При анализе кубитно-двоичных форм представления объектов в целях определения расстояний между ними необходимо учитывать: 1) Кодовое расстояние формируется при наличии хотя бы одного кубита, равного нулю по всем его координатам. 2) В противном случае вычисляются функции принадлежности на основании подсчета общего числа единиц, полученного при выполнении векторной операции конъюнкции, отнесенных к количеству единиц каждого из векторов, соответствующих двум различным объектам киберпространства. 3) Xor-сумма расстояний объектов, составляющих цикл, равна вектору, составленному из нулевых кубитов. 4) Xor-сумма всех примитивов кубита равна вектору, имеющему все единичные координаты. 5) Формирование многозначных сигнатур на основе кубитных структур данных может существенно расширить область применения аппарата xor-полиномов с нелинейными обратными связями. 6) Неструктурированное множество примитивов, самоорганизующееся в процессе моделирования или решения конкретной задачи, существенно уменьшает объем моделей и время их создания. 7) Реализация дерева классификации и процедур его анализа значительно сокращает объем структур данных, а также время решения соответствующих задач. Пример такого дерева представлен на рис. 3, которое, благодаря бинарности, выполняет классификацию (спуск по дереву) за минимальное число шагов вычислительной процедуры.

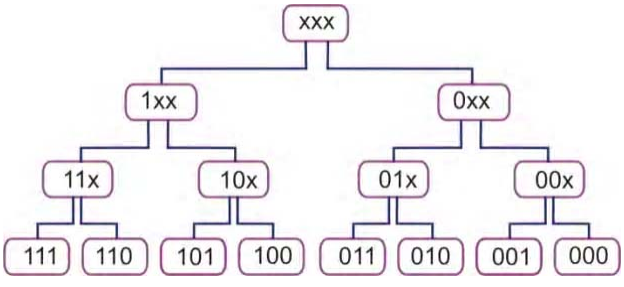


Рис.3. Пример классификационного бинарного дерева

Процедура классификации: 1) Анализ i-го разряда входного вектора m по правилам

$$P = \begin{cases} P^0 \leftarrow m_i \oplus A_i = 0; \\ P^1 \leftarrow m_i \oplus A_i = 1 \end{cases}$$

для выбора левой или правой ветви вершины дерева. Здесь множество A определяет обобщенные коды-сигнатуры, а также конечные вершины дерева. 2) Анализ заканчивается положительно, если обработаны все разряды входного вектора, который идентифицирован существующим аналогом в библиотеке. В противном случае объект не может быть идентифицирован в рамках системы, которая должна быть расширена. 3) Если результат анализа имеет неоднозначность по отношению к 0 и 1, то объект идентифицируется уже не примитивом, а классом (подклассом). Время выполнения процедуры классификации определяется выражением: $T = \log_2 N$, что является заслугой избыточных вершин, позволяющих систему из N отношений (нижний уровень кодов) представить в виде древовидной структуры.

3. Заключение

Предложена модифицированная модель критерия скалярного и векторного качества оценивания бинарных отношений, которая отличается использованием функции непринадлежности и кодового расстояния Хэмминга, что обеспечивает линейность изменения численного значения критерия от 0 до 1 по мере увеличения «расстояния» от полного совпадения двух объектов до максимально возможного, когда кодовое расстояние равно $d(m, A) = k$. Критерий может быть использован при оценивании взаимодействия объектов в реальном масштабе времени в задачах отслеживания цели, движения по заданному маршруту, диагностирования функциональных нарушений, поиска, распознавания и принятия решений.

Практическая значимость – существенное повышение быстродействия при решении задач анализа процессов и явлений в киберпространстве и других задач дискретной оптимизации упрощения системы команд и процедур при вычислении критериев путем параллельного выполнения векторных логических операций.

Список литературы: 1. *Инфраструктура* мозгоподобных вычислительных процессов / М.Ф. Бондаренко, О.А. Гузь, В.И. Хаханов, Ю.П. Шабанов-Кушнаренко. Харьков: Новое слово, 2010. 160 с. **2.** *Хаханов В. И., Литвинова Е. И., Чумаченко С. В., Гузь О.А.* Логический ассоциативный вычислитель. Электронное моделирование. 2011. № 1. С. 73-90. **3.** *Hahanov V., Wajeb Gharibi, Litvinova E., Chumachenko S.* Information analysis infrastructure for diagnosis. Information. An international interdisciplinary journal. 2011. Japan. Vol. 14. No 7. P. 2419-2433. **4.** *Хаханов В.И.* Проектирование и тестирование цифровых систем на кристаллах / В.И. Хаханов, Е.И. Литвинова, О.А. Гузь. Харьков: ХНУРЭ, 2009. 484с. **5.** *Stig Stenholm, Kalle-Antti Suominen.* Quantum approach to informatics. Published by John Wiley & Sons, Inc., Hoboken, New Jersey. 2005. 238p. **6.** *Акритас А.* Основы компьютерной алгебры с приложениями: Пер. с англ. / А. Акритас. М.: Мир, 1994. 544 с. **7.** *Аттетков А.В.* Методы оптимизации / А.В. Аттетков, С.В. Галкин, В.С. Зарубин. Москва: Издательство МГТУ им. Н.Э. Баумана. 2003. 440 с.

Поступила в редколлегию 22.09.2011

Хаханов Владимир Иванович, декан факультета компьютерной инженерии и управления, д-р техн. наук, профессор кафедры АПВТ ХНУРЭ. Научные интересы: техническая диагностика цифровых систем, сетей и программных продуктов. Увлечения: баскетбол, футбол, горные лыжи. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 70-21-326. E-mail: hahanov@kture.kharkov.ua.

Мурад Али А., аспирант кафедры АПВТ ХНУРЭ. Научные интересы: компьютерные системы и сети. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 70-21-326.

Baghdad Ammar Avni Abbas, аспирант кафедры АПВТ ХНУРЭ. Научные интересы: компьютерные системы и сети. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 70-21-326.

Гузь Олеся Алексеевна, канд. техн. наук, доцент кафедры СКС Донецкой Академии автомобильного транспорта. Научные интересы: техническая диагностика цифровых систем. Адрес: Украина, 83086, Донецк, пр. Дзержинского, 7.

Хаханова Ирина Витальевна, д-р техн. наук, профессор кафедры АПВТ ХНУРЭ. Научные интересы: техническая диагностика цифровых систем. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 70-21-326.

УДК 378.147

Н.А.БОНДАРЕНКО, В.И.ШЕХОВЦОВА

СОЗДАНИЕ НОВОГО КЛАССА PIXEL И ЭЛЕМЕНТА УПРАВЛЕНИЯ TEXTBOX С НОВЫМ СВОЙСТВОМ BLANKNUMBER В СИСТЕМЕ ОБЪЕКТНО-ОРИЕНТИРОВАННОГО ПРОГРАММИРОВАНИЯ

Разрабатывается новый элемент управления TextBox с новым свойством BlankNumber и новый пользовательский класс Pixel в системе объектно-ориентированного программирования Visual Basic. Приводятся результаты разработки и программирования нового элемента управления и нового класса объектов. Показываются результаты тестирования нового элемента управления и нового класса, демонстрирующие корректность их работы.

1. Введение

Система объектно-ориентированного программирования Visual Basic (ООП VB) [1] дает возможность создания собственных элементов управления, которые получили название «элементы управления ActiveX», или «элементы управления пользователя» (*User Control*). При этом программист должен самостоятельно определить свойства, методы и события нового элемента управления. Однако имеющихся элементов управления бывает недостаточно или же использование их стандартных свойств методов громоздко и неудобно. В этом случае было бы целесообразно добавить к стандартным собственные свойства и методы.

Другой особенностью системы ООП VB [2] является возможность создания собственных классов. Прикладная программа создается путем задания необходимых объектов и определения их взаимодействия между собой и операционной системой.

Класс – это абстракция, объединяющая различные объекты в одну группу в соответствии с их свойствами и поведением. Например, все командные кнопки являются объектами класса CommandButton, все метки – объектами класса Label. Класс отличается от элемента управления тем, что объекты класса могут реально существовать в программе, хотя и не иметь визуального отображения.

Цель – разработать элемент управления ActiveX, который состоит из стандартного текстового поля с новым свойством.

Задачи для достижения цели. Элемент управления ActiveX должен иметь следующие параметры:

– стандартные свойства: Text, BackColor, ForeColor, Font, MultiLine;
– новое свойство BlankNumber, показывающее количество пробелов в текстовом поле.

Это свойство должно быть доступно только для чтения во время проектирования и выполнения программы.

2. Основное содержание

Новый класс Pixel разрабатывается для формирования и отображения на экране точек заданного размера и цвета. Это позволяет легко отображать результаты в графическом виде с необходимым разрешением.

Для удобства и гибкости работы с объектами такого класса необходимо предусмотреть возможность задания ряда свойств и методов.

Свойства класса:

1) X – горизонтальная координата отображаемой точки. Тип данных – Integer;
2) Y – вертикальная координата отображаемой точки. Тип данных – Integer;
3) Size – размер отображаемой точки. Тип данных – Integer;
4) Color – цвет отображаемой точки. Тип данных – Long.

Методы класса: Show – отображает точку на экране в соответствии с заданными свойствами. Метод является процедурой без параметров.

Внешний вид разработанного элемента управления показан на рис. 1. Он основан на стандартном текстовом поле.

Рис. 1. Внешний вид элемента управления TextBox

Для программирования событий инициализации и изменения размеров элемента управления выбраны следующие параметры:

– ширина и высота текстового поля равна ширине и высоте контейнера соответственно;

– горизонтальная и вертикальная координата текстового поля относительно контейнера равна 0.

Программирование свойств и методов было осуществлено при помощи специальной программы ООП VB – *ActiveX Control Interface Wizard*. В соответствии с поставленной задачей выбраны необходимые свойства и методы разрабатываемого элемента управления (рис. 2).

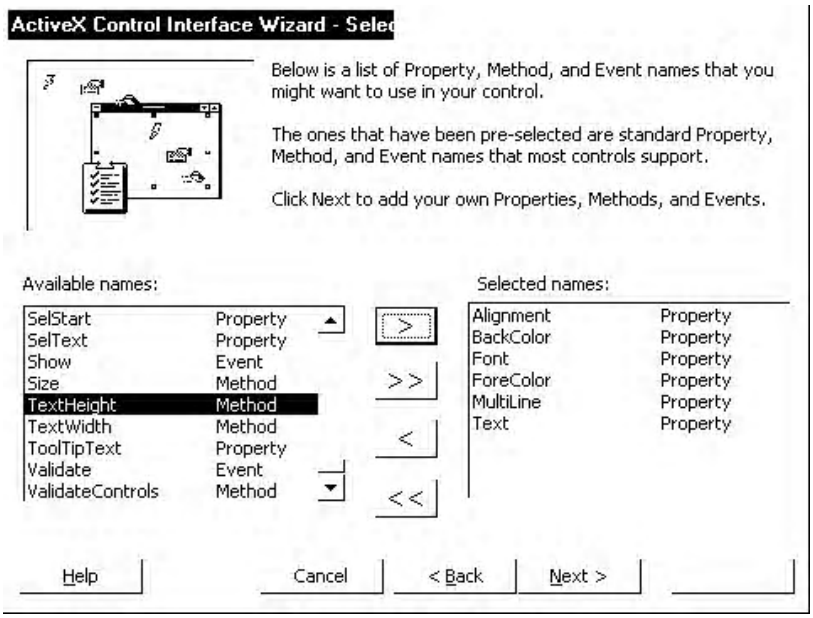


Рис. 2. Выбор свойств и методов разрабатываемого элемента управления

Добавлено новое свойство BlankNumber и определены его параметры (рис. 3).

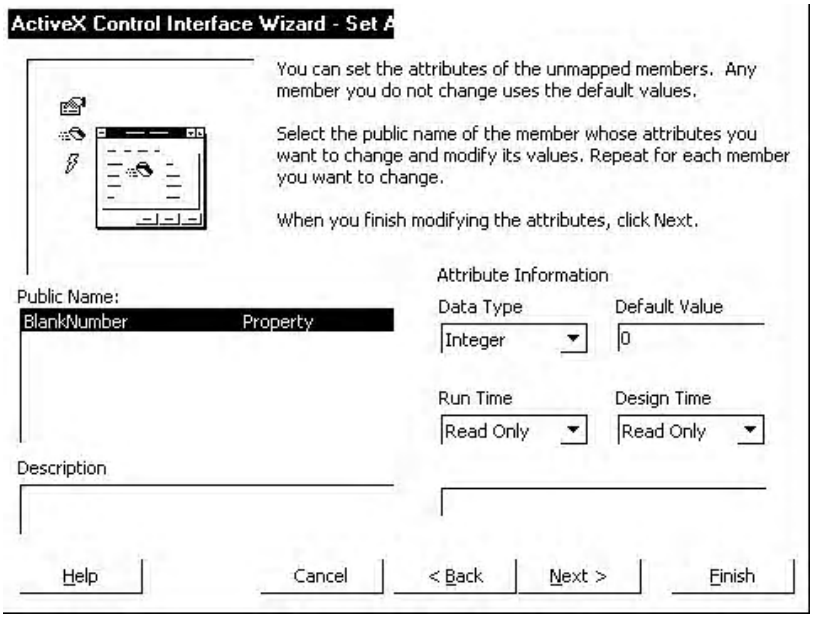


Рис. 3. Определение параметров нового свойства

В результате программой ActiveX Control Interface Wizard был сгенерирован программный код, реализующий работу выбранных свойств и методов.

В процедуру Public Property Get BlankNumber() As Integer, реализующую доступ к новому свойству BlankNumber, добавлен программный код для подсчета количества пробелов в текстовом поле.

Для тестирования разработанного элемента управления на этапе выполнения прикладной программы (*run time*) на форме была размещена командная кнопка Command1 с надписью «BlankNumber». При нажатии на эту кнопку выводится сообщение о количестве пробелов в текстовой строке путем обращения к свойству BlankNumber. Полученный результат представлен на рис. 4.

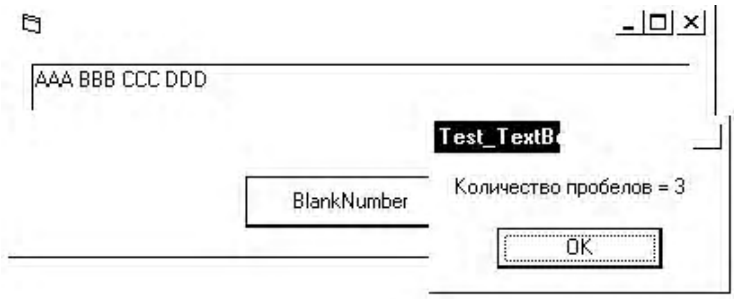


Рис. 4. Результат тестирования нового свойства

В третьем случае производилась проверка возможности записи значения нового свойства на этапе выполнения программы Для этого на форме была размещена вторая командная кнопка с надписью «Установка BlankNumber».

Программа была запущена на выполнение и нажата кнопка «Установка BlankNumber». В результате было получено сообщение об ошибке «Set not supported at runtime» (Установка не поддерживается на этапе выполнения).

Таким образом, проведенное тестирование свойств и методов разработанного элемента управления на этапе выполнения прикладной программы показало корректность их работы в соответствии с заданными параметрами.

Разработка нового класса осуществлялась с помощью специальной программы ООП VB 6 – *Class Builder Utility*. В соответствии с поставленной задачей было задано имя нового класса и его свойства (рис. 5).

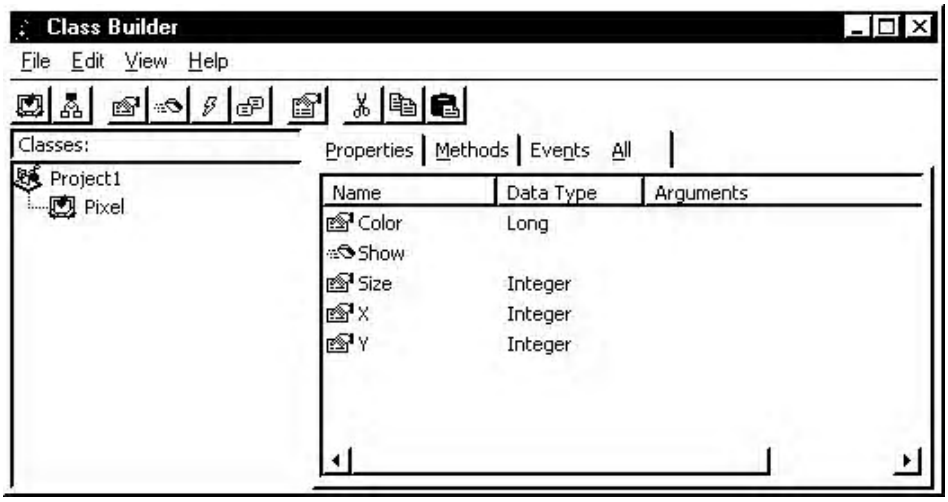


Рис. 5. Задание свойств нового класса

Программой Class Builder Utility для нового класса был сформирован программный код, реализующий доступ к его свойствам и методам.

Создана коллекция объектов класса Pixel (рис. 6).

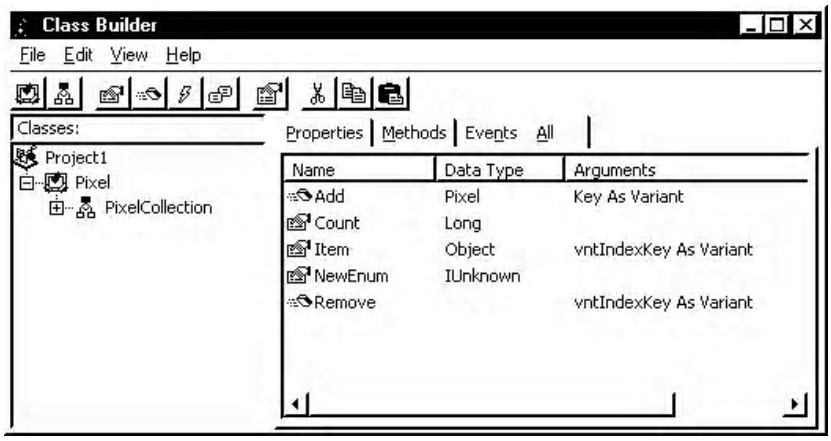


Рис. 6. Коллекция объектов класса Pixel

Для тестирования нового класса и коллекции его объектов был создан новый проект Standard EXE, к которому были подключены разработанные модуль класса Pixel и коллекция.

После запуска программы был введен размер точки и нажата кнопка «Создать коллекцию», а затем «Показать коллекцию» (рис. 7).

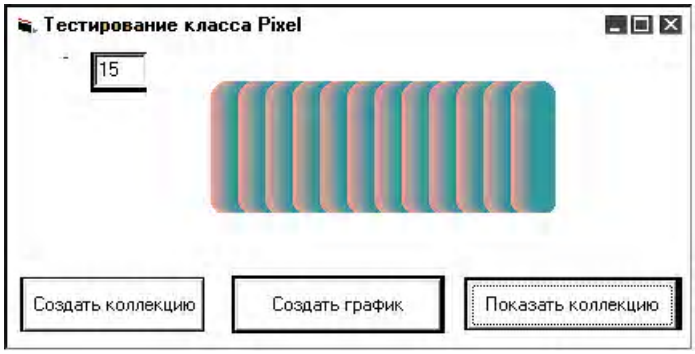


Рис. 7. Отображение коллекции на экране

После запуска программы был введен размер точки и нажата кнопка «Создать график». После получения сообщения о создании графика была нажата кнопка «Показать коллекцию». Результат показан на рис. 8.

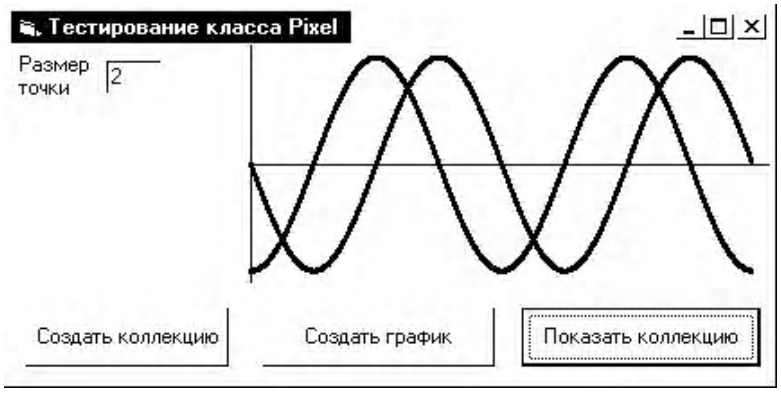


Рис. 8. Отображение графиков на экране

Таким образом, из проведенного тестирования можно сделать вывод, что свойства и методы нового класса и коллекции работают корректно и в соответствии с заданными параметрами.

Научная новизна. Разработан новый компонент ActiveX (элемент управления TextBox с новым свойством BlankNumber) и новый пользовательский класс Pixel в системе объектно-ориентированного программирования Visual Basic.

Список литературы: 1. *Бондаренко М.А.* Програмування у середовищі Visual Basic. Частина 1. Харків: Канком, 2004. 496 с. **2.** *Бондаренко М.А.* Програмування у середовищі Visual Basic. Частина 2. Харків: Канком, 2005. 664 с.

Поступила в редколлегию 12.09.2011

Бондаренко Николай Андреевич, канд. техн. наук, профессор Украинской инженерно-педагогической Академии. Научные интересы: проектирование технических систем. Адрес: Украина, 61000, Харьков, ул. Клочковская, 195 г, кв. 44, тел. 7 19 50 01.

Шеховцова Виктория Ивановна, канд. пед. наук, ст. преподаватель Украинской инженерно-педагогической Академии. Научные интересы: проектирование технических и информационных систем. Адрес: Украина, 61140, Харьков, пр. Гагарина, 92, кв. 15, тел. 7 37 52 90.

РЕФЕРАТИ

УДК 681.3.06

Методологія оцінки стійкості блокових симетричних шифрів / І.В. Лисицька // АСУ та прилади автоматики. 2011. Вип. 156. С.4-15.

Запропонована нова методологія оцінки стійкості блокових симетричних шифрів до атак диференціального та лінійного криптоаналізу, що будується на основі аналізу показників зменшених моделей шифрів та показників розроблених моделей випадкових підстановок. Рівень доказової стійкості шифрів визначено з допомогою їх математичного моделювання випадковими підстановками відповідного степеня.

Табл. 2. Бібліогр.: 27 назв.

UDC 681.3.06

Methodology for estimation of security of symmetric block cipher / I.V. Lisitskaya // Management Information System and Devices. 2011. N 156. P.4-15.

A new methodology for estimation of security of symmetric block cipher to differential and linear attacks, which is based on analysis of properties of model ciphers and properties developed models of random permutations. The level of provable of security ciphers defined by their the mathematical modeling of random permutations corresponding degree.

Tab. 2. Refs.: 27 titles.

УДК 621.315.592

Віртуальний датчик для моніторингу температури фонового нагрівача в тепловому вузлі установки для вирощування монокристалів арсеніду галію / А.П. Оксаніч, І.В. Шевченко, Ю.О. Краснопольска // АСУ та прилади автоматики. 2011. Вип. 156. С. 16-26.

Удосконалено математичну модель визначення температури фонового нагрівача теплового вузла, що, на відміну від існуючої, враховує не тільки значення споживаної нагрівачем потужності, але й значення інших технологічних параметрів, що впливають на тепловіддачу нагрівача, що дозволяє підвищити об'єктивність виміру, довести погрішність виміру до рівня ±3°С і використовувати в технологічному процесі інформаційну технологію віртуального моніторингу теплового поля в зоні кристалізації.

Табл. 9. Іл. 3. Бібліогр.: 8 назв.

UDC 621.315.592

Virtual sensor for temperature monitoring of background heater in a node for growing single crystals of gallium arsenide/ A.P. Oksanich, I.V Shevchenko, U.A. Krasnopolskaya // Management Information System and Devices. 2011. N 156. P.16-26.

Improved mathematical model for determining the temperature of an additional heater, which is located in a thermal node. The model takes into account the value of the power consumption, as well as the values of other process parameters that affect heat transfer. It allows to increase the objectivity of measurement and measurement error to less than ±3°C. The model is used for virtual monitoring of the thermal field in the crystallization zone.

Tab. 9. Fig. 3. Ref.: 8 items.

УДК 681.325.53: 37 : 004.5

Схемотехнічне проектування на мові VHDL перетворювачів кодів за методом долічення / М.Я. Какурін, Ю.В. Лопухін, В.В.Вареца, С.М. Саранча , Г. М. Макаренко // АСУ та прилади автоматики. 2011. Вип. 156. С.26-34.

Розглянута структура і функціонування багатосекційних перетворювачів кодів за методом " долічення до нуля ". Запропоновано алгоритм знаходження фундаментального розбиття перетворювачів кодів і програмний засіб для їх реал і зації та аналізу основних характеристик.

Іл. 4. Бібліогр.: 4 назви.

UDC 681.325.53:37 : 004.5

Schemetical design with VHDL of code transformers by the method "to accounting to zero"N.Ya.Kakurin, Yu.V.Lopuhin, V.V.Varetsa, S .M. Sarancha, A. N. Makarenko // Management Information System and Devices. 2011. N 156. P.26-34.

The structure and functioning of multiblockes of code transformers by the method "to accounting to zero" are examined. The algorithm for searching of fundamental breaking up of code transformers and software for its implementation and analysis of basic characteristics are offered.

Fig. 4. Ref.: 4 items.

УДК 681.518:004.93.1’

Оптимізація параметрів навчання інтелектуальної системи керування летучою пилкою / А.О.Панич, О.Б.Берест // АСУ та прилади автоматики. 2011. Вип. 156. С.34-41.

Розглянута категорична модель і інформаційно - екстремальний алгоритм навчання системи підтримки ухвалення рішення для керування летучою пилкою. Побудовано в процесі навчання вирішальні правила, які дозволили збільшити точність різання довгомірних матеріалів, що рухаються.

Іл.7. Бібліогр.: 8 назв.

UDC 681.518:004.93.1’

The optimization of learning intellectual control system parameters of flying saw / A.O.Panych, O.B.Berest // Management Information System and Devices. 2011. N 156. P.34-41.

Categorical model and information-extreme learning algorithm of the decision making support system for flying saw control are under consideration. Decision rules were developed during the learning process, that let to increase the cutting precision of long-size moving materials.

Fig.7. Ref.:8 items.

УДК 681.518:004.93.1’

Інформаційно-екстремальний унімодальний класифікатор з паралельно-послідовною оптимізацією контрольних допусків на ознаки розпізнавання / В.В. Москаленко, І.В. Шелехов, О.В. Соболєв // АСУ та прилади автоматики. 2011. Вип. 156. С.42-47.

Запропоновано інформаційно-екстремальний алгоритм оптимізації контрольних допусків на ознаки розпізнавання для унімодального класифікатора, який характеризується єдиним центром розсіювання векторів-реалізацій образів. При цьому одержані за процедурою паралельної оптимізації квазіоптимальні контрольні допуски використовуються як стартові для послідовної процедури. Як приклад розглянуто реалізацію унімодальної системи підтримки прийняття рішень для керування технологічним процесом вирощування сцинтиляційних монокристалів.

Іл. 4. Бібліогр.: 7 назв.

UDC 681.518:004.93.1’

Information-extreme unimodal classifier with parallel-sequential optimization of the control permits for identification signs / V.V. Moskalenko, I.V. Shelehov, O.V. Sobolev // Management Information System and Devices. 2011. N 156. P.42-47.

This paper proposes information-extreme algorithm with optimization coltrol permits of identification signs for unimodal classifier characterized by single center of pattern vector-realizations distribution. Quasi optimal coltrol permits uses as initial parameters for sequential optimization. On the example of unimodal DSS, the article considers implementation of the algorithm for control of growing scintillate single crystals.

Fig. 4. Ref.: 7 items.

УДК 681.323

Удосконалений метод генерації та видачі ключів для комбінованих інфраструктур відкритих ключів /П.О. Кравченко // АСУ та прилади автоматики. 2011. Вип. 156. С.48-53.

Удосконалено метод генерації таємного ключа для комбінованої інфраструктури відкритих ключів, який відрізняється паралельними запитами користувача до розподіленого уповноваженого на генерацію ключів та формуванням особистого ключа користувачем, що дозволяє збільшити показники доступності для розподіленого уповноваженого на генерацію ключів.

Табл. 1. Іл. 4. Бібліогр.: 5 назв.

UDC 681.323

The improved key issuing method for the combined public key infrastructure / P.O. Kravchenko // Management Information System and Devices. All-Ukr. Sci. Interdep. Mag. 2011. N. 156. P.48-53.

The key issuing method for the combined public key infrastructure was improved. The method differs from existing in parallel requests to the distributed private key generator and calculation of private key on user side and allows to increase rate of availability of distributed private key generator.

Tab. 1. Fig. 4. Ref.: 5 items.

УДК 519.7

Модель логічного оператора з керованим ядром/ Н.Є. Русакова // АСУ та прилади автоматики. 2011. Вип. 156. С.54-58.

Розглянуті реляційні мережі та лінійні логічні оператори, які є основним вирішувачем у роботі реляційних мереж. Також вперше запропоновано модель логічного оператора з керованим ядром, яка дає можливість побудови окремої гілки реляційної мережі.

Іл. 5. Бібліогр.: 3 назви.

UDC 519.7

Model of logical operator with the guided kernel / N.E.Rusakova // Management Information System and Devices. 2011. N 156. P.54-58.

Relation networks and linear logical operators are examined in the article. Also in-process a model is first offered logical operator with the guided kernel, which enables construction of separate branch of relation network.

Ref.: 3 items.

УДК 004.896

Адаптивний критичний регулятор системи керування процесом травлення смугової сталі / Самер Лага, В.О. Тімофєєв, А.А. Шамраєв // АСУ та прилади автоматики. 2011. Вип. 156. С.59-64.

Розглянуто підхід до керування технологічними процесами прокатки смугової сталі за допомогою критичних регуляторів. Запропоновано процедури рекурентного обчислення параметрів розширеної ARMAX – моделі об'єктів цифрового керування. Наведено результати моделювання системи критичного керування процесом травлення, що підтверджують ефективність застосування запропонованого методу для отримання гарантованої точності ідентифікації та зменшення відхилення вихідних параметрів від заданих значень.

Іл. 4. Бібліогр.: 3 назви.

UDC 004.896

Adaptive crinical controller of control system for pickling of strip steel /Samer Laga, V.O. Timofeyev, A.A. Shamraev // Management Information System and Devices. 2011. N 156. P.59-64.

In this paper the approach to the control of technological processes of strip steel rolling mill by means of critical controllers was considered. The recursive parameters calculation procedures of the extended ARMAX - model of digital control objects were proposed. The simulation results of the critical control system process digestion were shown, witch confirming the effectiveness of the proposed method for guaranteed accuracy for identification and to reduce the deviation of output parameters from the given values.

Fig. 4. Ref.: 3 items.

УДК 681.518.2

Оперативне управління сітковими системами в умовах невизначеності / І.А. Божинський // АСУ та прилади автоматики. 2011. Вип. 156. С.65-70.

Досліджено математичні моделі оперативного управління сітковими системами в умовах невизначеності. Розроблено інструментальні засоби прийняття управлінських рішень в умовах невизначеності.

Іл. 3. Бібліогр.: 3 назви.

UDK 681.518.2

On-line analitical processing for net systems in the indefinite conditions / I.A. Bozhinskiy // Management Information System and Devices. 2011. N 156. P.65-70.

This article deels with on-line analitical processing for net systems in the indefinite conditions. The instrumental devises for net systems operation control tools in the indefinite conditions were put into operation.

Fig. 3. Ref.: 3 items.

УДК 681.3

Сплайн-моделі профілів складності питань та знань респондентів у тестовому контролі знань / Р.М. Дубан, І.В. Шелевицький // АСУ та прилади автоматики. 2011. Вип. 156. С.71-77.

Відомі моделі IRT тестового контролю знань для побудови профілів потребують індивідуальної роботи експерта з кожним питанням й респондентом. Запропоновано як модель застосовувати кубічний ермітів сплайн із фіксованими краями. Завдяки універсальності моделі автоматизовано групові розрахунки профілів. Розроблені алгоритми втілено в інформаційну системі "Logit", показано приклади розрахованих профілів питань та респондентів.

Іл. 6. Бібліогр.: 10 назв.

UDC 681.3

Comlpex issues and respondent knowledge profile spline models in knowledge testing. / R.N. Duban, I.V. Shelevitskiy // Management Information System and Devices. 2011. N 156. P.71-77.

Famous IRT models of knowledge test control used for building profiles require expert's individual work on each issue and each respondent. The model of cubic Hermite spline with fixed edges is proposed for wide usage. Due to its universality, calculations of group profiles are automatized. The developed algorithms are embodied in an information system "Logit" and demonstrate examples of calculated profile issues and respondents.

Fig. 6. Ref.: 10 items.

УДК 621.391

Технологія класифікації еозинофілів на основі сплайн-параметризації / Д.Г. Медведєв // АСУ та прилади автоматики. 2011. Вип. 156. С.77-82.

Існують методи діагностики імунного статусу дітей, що потребують морфологічного аналізу клітин крові – еозинофілів. Для оконтурювання та параметризації цифрових зображень еозинофілів розроблено інформаційну технологію, що ґрунтується на оцінках сплайн-моделі контуру за методом найменших квадратів. Технологія апробована на 300 знімках. Показано приклади оконтурювання та параметризації. Технологію втілено в інформаційну систему діагностики імунного статусу.

Іл. 5. Бібліогр.: 9 назв.

UDC 621.391

Technology classification of eosinophils on the basis spline parameterization / D. Medvedev // Management Information System and Devices. 2011. N 156. P.77-82.

There are methods of diagnosing immune status of children in need of morphological analysis of blood cells - eosinophils. For contouring and parameterization of digital images eosinophils developed information technology, based on estimates of spline contour model by the method of least squares. The technology has been tested on 300 images. Shown examples of contouring and parameterization. The technology embodied in the information system diagnosis of immune status.

Fig. 5. Ref.: 9 items.

УДК 621.37/39.029.3

Розробка та застосування методів моніторингу процесів проектування, виробництва та експлуатації ЖЦ РЕЗ/ А.О. Андрусевич, І.Ш. Невлюдов, О.М. Донсков // АСУ та прилади автоматики. 2011. Вип. 156. С.82-89.

Удосконалено методи та засоби моніторингу виробничого середовища при виготовленні РЕЗ в напрямку вдосконалення систем технічного обслуговування технологічного обладнання, що використовує цифрові системи управління і контролю. Наведено основи теорії і нову концепцію моніторингу життєвого циклу РЕЗ на етапах проектування, виробництва та експлуатації, в основі якої покладено відображення інформації на основі візуалізації процесів.

Іл. 2. Бібліогр.: 7 назв.

UDC 621.37/39.029.3

Development and application of methods monitoring processes designing, manufacture and operation of LC REM / A.A. Andrusevich, I. Sh. Nevlyudov, O.M. Donskov // Management Information System and Devices. 2011. N 156. P.82-89.

Methods and tools for environmental monitoring in the manufacture of RES in the direction of improving the system of maintenance of process equipment using digital control systems and control improved. Presents basic theory and a new concept for monitoring the life cycle of the RECs during the design, manufacture and operation, which laid the basis for the map-based information visualization process.

Fig. 2. Ref.: 7 items.

УДК 658.512.011:681.326:519.713

Метрика та критерії аналізу кіберпростору/ В.І. Хаханов, Мурад Алі, Baghdad Ammar Avni Abbas, О.О. Гузь, І.В. Хаханова // АСУ та прилади автоматики. 2011. Вип. 156. С.90-98.

Запропоновано метрику й критерії якості взаємодії об'єктів при аналізі кіберпростору, представленого у двійковому та багатозначному вирахуванні. Показуються напрямки використання оцінок для завдань пошуку, розпізнавання й прийняття рішень.

Іл. 3. Бібліогр.: 7 назв.

UDC 658.512.011:681.326:519.713

The metrics and criteria of the analysis cyberspace / V.I. Hahanov, Murad Ali, Baghdad Ammar Avni Abbas, O.O. Guz, I.V. Hahanova // Management Information System and Devices. 2011. N 156. P.90-98.

The metrics and criteria of quality interaction objects are offered at the analysis the cyberspace submitted in binary and multiple-valued calculation. Directions of use estimations for tasks of search, recognition and decision-making are shown.

Fig. 3. Ref.: 7 items.

УДК 378.147

Утворення нового класу pixel та елемента керування textbox з новою властивістю blanknumber в системі об'єктно-орієнтованого програмування / М. А. Бондаренко, В.І. Шеховцова // АСУ та прилади автоматики. 2011. Вип. 156. С.99-103.

Розглянуті питання розробки програмного та інформаційного забезпечення роботи в системі об'єктно-орієнтованого програмування Visual Basic. Розроблено новий елемент керування TextBox з новою властивістю BlankNumber та новий клас користувача Pixel. Наведено результати розробки та тестування нового елемента керування та нового класу об'єктів користувача. Результати демонструють коректність їх роботи.

Іл. 8. Бібліогр.: 2 назви.

UDK 378.147

Formation of new class of pixel and custom of textbox control is with new property of blanknumber in the system of the objective oriented programming / H. A. Bondarenko,V. I. Shehovtcova // Management Information System and Devices. 2011. N 156. P.99-103.

The questions of development of the programmatic and informative providing of work in the system of the objective oriented programming of Visual Basic are considered. New custom of TextBox control is developed with new property of BlankNumber and new class of user Pixel. The results of development and testing of new custom and new class of objects of user control are resulted. Results demonstrate correctness of their work.

Fig. 8. Ref.: 2 items.

ПРАВИЛА

оформления рукописей для авторов научно-технического сборника *"АСУ и приборы автоматики"*

Формат страницы — А4 (210х297мм), поля: сверху, справа, слева, снизу – 30 мм. Редактор: Pagemaker 6.0, 6,5 (можно, но нежелательно Word), гарнитура Times New Roman Cyr, кегль – 11 пунктов, межстрочное расстояние — 110 %, табуляция — 5 мм.

Объем рукописи – до 10 с. (языки: русский, украинский, английский). Содержание должно отражать актуальность исследования, постановку задачи, цель, сущность, научные и практические результаты, сравнение с лучшими аналогами, выводы.

Структура рукописи: заголовок, аннотация, текст, литература, реферат на украинском и английском языках, сведения об авторах.

ОБРАЗЕЦ ОФОРМЛЕНИЯ

УДК 519.713

И.О. ФАМИЛИЯ

НАЗВАНИЕ РУКОПИСИ

Аннотация (абзац 5-10 строк, кегль 10) помещается в начале статьи и содержит информацию о результатах описанных исследований.

Основной текст можно разделять на 2 и более подразделов с заголовками, выделенными полужирным шрифтом, пронумерованными арабскими цифрами, как показано в следующей строке.

1. Название раздела

Рисунки и таблицы (черно-белые, контрастные) помещаются в текст после первой ссылки в виде *переносимых объектов* и раздельно нумеруются, при наличии более одного рисунка (таблицы), арабскими цифрами. Рисунок содержит подрисуночную центрированную подпись (текстовая строка, расположенная вне рисунка, кегль 10) под иллюстрацией, как показано на рис. 1.

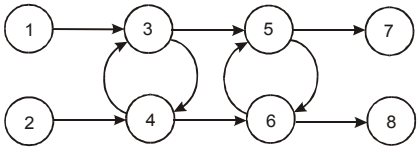


Рис. 1. Граф с контурами

Табличный заголовок располагается справа над таблицей, что иллюстрируется табл.1. Редакторы: CorelDraw, Table Editor и др.

Таблица 1

Шаг i	1	2	3	4	5	6
Ф1(1,3)	1	2	2	4	6	1

Формулы нумеруются при наличии ссылок на них в рукописи. Рекомендуемый кегль формульного набора: обычный (переменная) – 11 пунктов, крупный индекс – 8, мелкий индекс (над- и подиндекс) – 8, крупный символ (основной) – 12, мелкий (индексный) математический символ – 10:

$$F_{i+j} = \sum_{i=1}^{b^k} F_j^i - \prod_{j=1}^{l+h^2} P_{R\,j+i} + F^{j-1} + X^{\Sigma n^k} . \qquad (1)$$

Формат переменных (желательно не курсивом – без наклона) в тексте и формулах должен быть идентичным. В тексте над- и подиндексы составляют 70 % от кегля, которые рекомендуется опускать (поднимать) на 17 (33) % относительно основной строки.

Список литературы (включает опубликованные источники, на которые имеются ссылки в тексте, заключенные в квадратные скобки) печатается без отступа, кегль 9 пунктов.

Образец окончания текста рукописи (литература, сведения об авторах, реферат) представлен ниже.

Список литературы: 1. *Фамилия И.О.* Название книги. Город: Издательство, 1900. 000 с. 2. *Название* сборника / Под ред. И.О. Фамилия. Город: Издательство, 1900. 000 с. 3. *Фамилия И.О.* Название статьи / / Название журнала. Название серии. 1997. Т. 00, № 00. С. 00-00 .

Поступила в редколлегию 00.00.00

Фамилия, имя, отчество, ученая степень, звание, должность и место работы. Научные интересы. Адрес, контактный телефон.

Рефераты на украинском и английском языках:

УДК 000.000.00

Назва статті українською мовою / Ініціали. Прізвище // АСУ та прилади автоматики. 2000. Вип. 00. С. 000-000.

Текст реферату.

Табл. 00. Іл. 00. Бібліогр.: 00 назв.

UDC 000.000.00

Title of paper / Initials. Surname // Management Information System and Devices. All-Ukr. Sci. Interdep. Mag. 2000. N 00. P. 000-000.

Text.

Tab. 00. Fig. 00. Ref.: 00 items.

Представление материалов

Рукопись, реферат, сведения об авторах — в одном файле, *поименованном фамилией первого автора*, на дискете 3,5 дюйма. Твердая копия материалов – для граждан Украины — в одном экземпляре: рукопись, подписанная авторами, рефераты, акт экспертизы, внешняя рецензия, подписанная доктором наук, заявление на имя главного редактора со сведениями об авторах.

Адрес редакции: Украина, 61166, Харьков, пр. Ленина, 14, ХНУРЭ, комната 321, тел. 70-21-326, e-mails: ri@kture.kharkov.ua; hahanov@kture.kharkov.ua. http://www.ewdtest.com/ri

Тематика статей, публикуемых в сборнике:

– Компьютерная инженерия
– Математическое моделирование
– Оптимизация и процессы управления
– Автоматизация проектирования и диагностика
– Информационные интеллектуальные системы
– Проектирование интегральных схем и микросистем
– Компьютерные технологии в образовании

Відповідальний випусковий В.І. Хаханов
Редактор О.П. Гужва
Комп'ютерна верстка Г.В. Хаханова, С.В. Чумаченко

Підп. до друку 27.09.2011. Формат 60x841/8. Умов. друк. арк. .
Обл.-вид. арк. 9,8. Тираж 300 прим.
Зам. № б/н. Ціна договірна.

Харківський національний університет радіоелектроніки (ХНУРЕ).
Україна, 61166, Харків, просп. Леніна, 14.

Оригінал-макет підготовлено в навчально-науковому видавничо-поліграфічному центрі ХНУРЕ
Україна, 61166, Харків, просп. Леніна, 14.
Надруковано у видавництві ПП "Степанов В.В."
61168, Харків, вул. Акад. Павлова, 311