ISSN 2078-9181

РОССИЙСКАЯ АКАДЕМИЯ НАУК
Отделение нанотехнологий и информационных технологий

САНКТ-ПЕТЕРБУРГСКИЙ
ИНСТИТУТ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РАН

ТРУДЫ СПИИРАН

proceedings.spiiras.nw.ru

ВЫПУСК 3(40)

Санкт Петербург
2015

18+

Труды СПИИРАН

Выпуск № 3(40), 2015

Научный, научно-образовательный, междисциплинарный журнал с базовой специализацией в области информатики, автоматизации и прикладной математики

Журнал основан в 2002 году

Учредитель и издатель

Федеральное государственное бюджетное учреждение науки
Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)

Адрес редакции

199178, Санкт-Петербург, 14-я линия, д. 39,
e-mail: publ@iias.spb.su, сайт: http://www.proceedings.spiiras.nw.ru/

Подписано к печати 15.06.2015. Формат 60×90 1/16. Усл. печ. л. 13,8. Заказ № 196. Тираж 200 экз., цена свободная
Отпечатано в Редакционно-издательском центре ГУАП, 190000, Санкт-Петербург, Б. Морская, д. 67

Журнал зарегистрирован Федеральной службой по надзору в сфере связи и массовых коммуникаций, свидетельство ПИ № ФС77-41695 от 19 августа 2010 г.
Подписной индекс 29393 по каталогу «Почта России»

Журнал входит в «Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук»

SPIIRAS Proceedings

Issue № 3(40), 2015

Scientific, educational, and interdisciplinary journal primarily specialized
in computer science, automation, and applied mathematics

Trudy SPIIRAN ♦ Founded in 2002 ♦ Труды СПИИРАН

Founder and Publisher

Federal State Budget Institution of Science
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences
(SPIIRAS)

Editorial Board's address

14-th line VO, 39, SPIIRAS, St. Petersburg, 199178, Russia,
e-mail: publ@iias.spb.su, web: http://www.proceedings.spiiras.nw.ru/

Signed to print 15.06.2015
Printed in Publishing center GUAP, 67, B. Morskaya, St. Petersburg, 190000, Russia

The journal is registered in Russian Federal Agency for Communications and Mass-Media Supervision,
certificate ПИ № ФС77-41695 dated August 19, 2010 г.
Subscription Index 29393, Russian Post Catalog

СОДЕРЖАНИЕ

CONTENTS

УДК 621.376.9

И.А. Саитов, Н.И. Мясин, К.И. Мясин

ОПРЕДЕЛЕНИЕ ПРИГОДНОСТИ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ СВЯЗИ ДЛЯ ПЕРЕДАЧИ МНОГОУРОВНЕВЫХ СИГНАЛОВ

Саитов И.А., Мясин Н.И., Мясин К.И. **Определение пригодности волоконно-оптических систем связи для передачи многоуровневых сигналов.**
Аннотация. Для решения задач проектирования и оперативного управления волоконно-оптическими системами передачи информации необходимо значение вероятности ошибки в додетекторной области. Оптимизация систем передачи по этому параметру особенно актуальна для фрагментов полностью оптических сетей связи. В статье представлена оценка вероятности битовой ошибки для наихудшего случая при оптической обработке сигнала. Полученная аналитическая модель легла в основу способа оценивания возможности применения многоуровневых оптических сигналов в волоконно-оптических системах передачи. Способ позволяет определить пригодность системы передачи с требуемой достоверностью принимать сигналы с заданным размером ансамбля.
Ключевые слова: волоконно-оптические системы передачи, сигналы с многоуровневой модуляцией интенсивности, вероятность ошибки, отношение сигнал/помеха.

Saitov I.A., Mjasin N.I., Mjasin K.I. **Determining the Suitability of the Fiber-Optic Communication Systems for Transmission of Multi-Level Signals.**
Abstract. To solve the problems of design and operational management of fiber-optic communication systems a value of error probability in subdetector area sometimes is necessary. Optimization of transmission systems for this parameter is particularly relevant for fragments of all-optical networks. In article, the estimation of bit error probability is presented for the worst case of optical signal processing. The obtained analytical model was the basis of a method for estimating the possibility of using multi-level optical signals in fiber-optic communication systems. The method allows to determine the suitability of a transmission system with the required reliability to receive signals with a given size of the ensemble.
Keywords: fiber-optic communication systems, signals with multilevel intensity modulation, error probability, signal-to-disturbance ratio.

1. Введение.

Внедрение волоконно-оптических систем передачи (ВОСП) со спектральным разделением каналов (СР) позволяет значительно улучшить оперативные и технико-экономические характеристики транспортной сети связи, существенно расширить перечень услуг связи. Вместе с этим использование ВОСП-СР сопровождается усложнением программно-аппаратных средств и комплексов оптической связи, повышением требований к свойствам отдельных компонентов и общесистемных параметров волоконно-оптических линий связи.

Вместе с развитием систем со спектральным разделением каналов усложняются оптические сигналы. Сигналы с многоуровневой модуляцией интенсивности позволяют многократно увеличить скорость передачи информации [1] по ВОСП-СР, сохраняя длительность импульсов не достигающую порогов возникновения нелинейных эф-

фектов и поляризационной модовой дисперсии. Исследования [1–5] продемонстрировали перспективность данного научного направления в предметной области. Применительно к ВОСП с некогерентным приемом, сигналы с многоуровневой модуляцией интенсивности (*IM-M – M-ary intensity modulation*) в отечественной и зарубежной литературе [1, 4, 5] называют многоуровневыми оптическими сигналами (МОС).

Бурное развитие телекоммуникационных технологий приводит к некоторому отставанию научно-методического инструментария от потребностей практики в отдельных направлениях отрасли. Известные модели и методики не в полной мере позволяют реализовать все преимущества многоволновых волоконно-оптических линейных трактов (ВОЛТ) с МОС, так как не достаточно адекватно отражают специфику современных мультипротокольных транспортных сетей связи. Так, первые опыты эксплуатации ВОСП нового поколения, в том числе с МОС, показали, что в гетерогенных мультипротокольных ВОЛТ существенно повышается совместное влияние дисперсии и нелинейных эффектов [4, 6]. Приближенная оценка квантового шума, присущего всем средствам математического моделирования оптических систем связи приводит к несостоятельности полученных результатов. Проектировщики вынуждены использовать грубые оценки влияния квантового шума [7], упрощающие проектные решения [8], но являющиеся причиной существенных погрешностей при решении поставленных задач. Это снижает качество управления, ограничивает эффективность использования ресурсов оптических направляющих сред.

2. Показатель качества передачи информации. Важным системным показателем ВОЛТ является отношение мощности оптического сигнала к мощности оптического шума, а в общем случае к мощности оптической помехи (ООСП, *OSDR – optical signal-to-disturbance ratio*). ООСП является тем параметром, который характеризует достижимую помехоустойчивость [6, 9, 10] при использовании тех или иных приемных устройств, помехоустойчивых и манипуляционных кодов. ООСП позволяет определить «чистый» выигрыш от применения конкретного ансамбля сигналов и/или линейного кода. Именно мощности сигнала и помехи определяют дальность передачи по оптическому волокну [6, 9]. В то же время ООСП позволяет рассчитать коэффициент (или вероятность) ошибок.

Дискретный МОС, вводимый в световод, за счет влияния шумов, хроматической дисперсии и нелинейных эффектов на фотодетекторе может быть представлен бесконечным числом подуровней, определяемых стохастическими процессами. Рассматриваемый оптический канал оканчивается до демодулятора и является дискретно-

непрерывным. В таких случаях в теории связи [9, 10], как правило, показателем качества передачи информации выбирают отношение сигнал-шум или сигнал/помеха.

Исходя из изложенного, далее показателем качества передачи информации выбрано отношение мощности оптического сигнала к мощности оптической помехи (ООСП).

3. Граница вероятности ошибки многоуровневого оптического сигнала. Для решения задач оптимизации параметров ВОЛТ требуется значение показателя качества для конкретной мощности сигнального созвездия. Так как МОС в отличие от сигналов с амплитудно-импульсной модуляцией принципиально не могут быть отрицательны, математический аппарат теории электрической связи не может быть применен к МОС без модернизации. В общем случае применения многоуровневых сигналов функциональная зависимость вероятности ошибки от ООСП не установлена.

Аналогично размышлениям, изложенным в [10] для противоположных сигналов с амплитудно-импульсной модуляцией, выведем выражение для определения граничного значения вероятности ошибки МОС с равновероятным формированием координат точек ансамбля сигналов.

В силу стохастичности процесса передачи правомочно говорить о вероятностном характере расположения точек ансамбля сигналов на выходе канала связи. Строго говоря, евклидово расстояние между математическим ожиданием координат соседних точек сигнала с многоуровневой модуляцией интенсивности на приеме не одинаково. Физическая природа данного различия заключается во влиянии нелинейных эффектов оптического волокна на распространяющийся сигнал. Минимальное евклидово расстояние на приеме – между точками с максимальной мощностью, так как степень искажения вследствие фазовой самомодуляции и вынужденного комбинационного рассеяния пропорциональна мощности сигнала:

$$dE_{\min} = P_{\text{вых}_{i,M}} - P_{\text{вых}_{i,M-1}}, \qquad (1)$$

где $P_{\text{вых}_{i,m}}$ – средняя мощность сигнала с уровнем m (принимает целочисленные значения в диапазоне от 1 до размера ансамбля сигналов M) на выходе оптического волокна в i-м спектральном канале.

Дисперсия уровней МОС так же различна, в силу наличия квантовых шумов, коррелированных с сигналом. Вместе с тем, в силу близости закона Пуассона [7] и нормального распределения при больших значениях параметра первого, а так же учитывая центральную предельную

теорему правомочно рассматривать гауссов характер отклонения сигнальных точек на приеме. Другими словами, положим, что на приеме действует гауссов шум с мощностью равной сумме мощностей квантового и аддитивного гауссова шумов. Данное допущение позволяет вычислить вероятность символьной ошибки для наихудшего случая.

Пусть приемник функционирует по правилу минимального евклидового расстояния между принятой и опорной сигнальными точками. Учитывая выражение (1), ошибка наиболее вероятна между двумя верхними уровнями. Тогда максимальная вероятность символьной ошибки оценивается как:

$$p_{s_i} \le \frac{1}{\sqrt{2\pi}\sigma_{M-1}} \int\limits_{P_{\text{вых}_{i,M}} - \frac{dE_{\min}}{2}}^{\infty} \exp\left(\frac{-(x - P_{\text{вых}_{i,M-1}})^2}{2\sigma_{M-1}^2}\right) dx + \\ + \frac{1}{\sqrt{2\pi}\sigma_M} \int\limits_{-\infty}^{P_{\text{вых}_{i,M}} - \frac{dE_{\min}}{2}} \exp\left(\frac{-(x - P_{\text{вых}_{i,M}})^2}{2\sigma_M^2}\right) dx, \quad (2)$$

где σ_m – среднеквадратическое отклонение (СКО) для m-й точки ансамбля сигналов. Учитывая пропорциональность мощности квантового шума мощности сигнала справедливо записать неравенство: $\sigma_n > \sigma_m$ если $n > m$, $n, m \in [1; M]$. При вычислении граничной вероятности ошибки с некоторой погрешностью можно принять $\sigma_M \approx \sigma_{M-1}$, тогда вероятность символьной ошибки удовлетворяет неравенству:

$$p_{s_i} < erfc\left(\frac{dE_{\min}}{\sigma_M \sqrt{8}}\right). \quad (3)$$

Допущение о равенстве СКО двух верхних уровней оптического сигнала, безусловно, несколько огрубляет результат (3). Полученное по (3) значение оказывается несколько выше реального, образуется некоторый запас по достоверности передачи. Вместе с тем, если при проектировании ВОСП есть возможность определения СКО для каждой точки ансамбля сигналов, то необходимо использовать более точное выражение (2).

Эквивалентную вероятность ошибки на бит для сигналов *IM-M* затруднительно вычислить с учетом ее зависимости от отображения символа в соответствующее значение энергии сигнала. Если использу-

ется манипуляционный код Грея, то два символа, соответствующие сигналам с соседними энергиями, отличаются не более чем на один бит. Поскольку наиболее вероятные ошибки, обусловленные влиянием помехи, приводят к выбору сигнала с соседним значением амплитуды вместо верного, то большинство битовых блоков содержат ошибки только в одном бите. Следовательно, эквивалентная вероятность ошибки на бит для сигналов *IM-M* может быть аппроксимирована по верхней границе выражением:

$$p_{b_i} = \frac{1}{\log_2 M} p_{s_i} \cdot \tag{4}$$

В работах [6, 9] отмечается незначительное влияние нелинейных эффектов в стандартном телекоммуникационном диапазоне вводимых мощностей. Таким образом, при условии соблюдения ограничений на максимальную вводимую мощность, можно сделать допущение о равномерном расположении математических ожиданий мощностей уровней сигнала на приеме. В этом случае евклидово расстояние между точками ансамбля сигналов равно:

$$dE = \frac{P_{\text{вых}_{i,M}}}{M-1} \cdot \tag{5}$$

При равновероятном и равномерном формировании символов учитывая (5) и потенциальную гетерогенность ВОСП:

$$p_{b_i} < \frac{1}{\log_2 M_i} erfc\left(\frac{OSDR_i}{\sqrt{8}M_i(M_i-1)}\right), \tag{6}$$

где $OSDR_i$ – отношение средней мощности оптического сигнала к средней мощности оптической помехи для *i*-го спектрального канала.

Зависимость вероятности ошибки от ООСП представлена на рисунке 1, *а*. Для фиксированного значения вероятности ошибки $p_b = 10^{-12}$ при постоянном уровне аддитивных шумов можно вычислить требуемые значения ООСП (рисунок 1, *б*) для передачи конкретной мощности сигнального созвездия. График имеет ступенчатый характер в виду дискретного значения числа точек ансамбля сигналов, которыми удобно кодировать двоичные последовательности, а так же ограничением на вероятность ошибки.

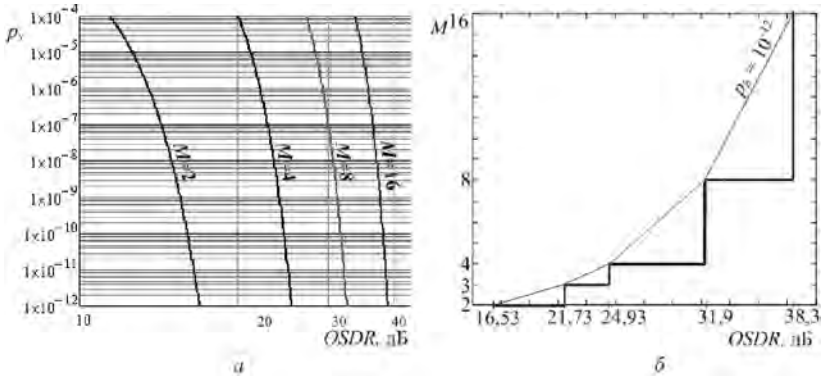


Рис. 1. Зависимости, полученные с помощью выражения (6): *а)* граница вероятности ошибки на символ для сигналов *IM-M*; *б)* зависимость передаваемого числа уровней сигнала от ООСП

Полученная граничная зависимость связывает показатель достоверности передачи информации с параметрами ВОЛТ через уравнение распространения сигнала.

4. Способ оценивания возможности применения МОС в ВОСП. Многоуровневый амплитудно-модулированный сигнал, вследствие ограничений на мощность вводимого в оптическое волокно излучения, использует тот же бюджет мощности, что и бинарный *IM*-сигнал. Этот фактор существенно сокращает дальность передачи такого сигнала. Евклидово расстояние *dE* между нижними уровнями определяет достижимую помехоустойчивость – порог чувствительности фотоприемного устройства (ФПУ) должен быть ниже второго уровня многоуровневого сигнала (рисунок 2,*а*).

Учитывая обратно пропорциональную зависимость дальности передачи от количества уровней сигнала *M* можно сделать вывод о предпочтительности оптического сигнала с количеством уровней от четырех до восьми, сигналы с большим количеством уровней целесообразно применять в приложениях с небольшими расстояниями: локальных сетях, межблочных интерфейсах, на последней миле и др.

На рисунке 2 представлены сигнальные созвездия, соответствующие оптическому сигналу с модуляцией интенсивности. Случай равномерной плотной укладки сфер (рисунок 2,*б*) описан в [9] и представляет интерес с точки зрения увеличения скорости передачи.

Из рисунка 2,*б*, что ошибочное принятие решения относительно уровня сигнала имеет разный вес. Так ошибочное принятие решения при распознавании первого и второго уровней приводит к потере двух

бит информации притом, что вероятность ошибки в распознавании соседних уровней максимальна.

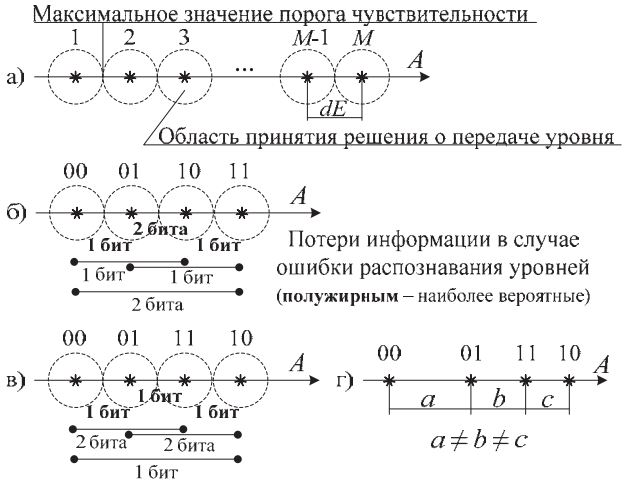


Рис. 2. Схематичное изображение укладки сигнальных сфер: а) общее представление многоуровневого кода на сигнальной плоскости; б) расположение символов 4-х уровневого кода; в) расположение символов после применения манипуляционного кодирования; г) размещение уровней через неравномерные интервалы

Для уравнивания функций потерь при наиболее вероятных ошибках, учитывая расположение сигнальных точек, можно применить манипуляционный код Грея (рисунок 2,*в*). В этом случае, Хеммингово расстояние от любой сигнальной точки до соседних минимально и равно единице, что означает потерю только одного бита при наиболее вероятных ошибках.

Расстояние между двумя нижними уровнями определяет дальность передачи с точки зрения энергетического запаса. Таким образом, для увеличения дальности передачи многоуровневого сигнала, казалось бы, можно применить неравномерное расположение точек сигнального созвездия (рисунок 2,*г*). Однако, исследования [5, 7] показывают, что вследствие влияния квантового шума сигнала различение M-го и (M–1)-го уровней затруднительно (см. рисунок 3). За счет чего расположение уровней в соответствии с рисунком 2,*г* влечет увеличение вероятности ошибки. Для стандартных телекоммуникационных приложений компромиссным является вариант с равномерным расположением уровней сигнала.

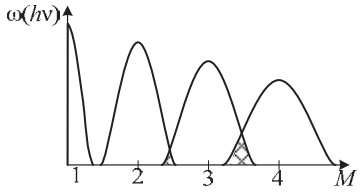


Рис. 3. Распределение вероятностей появления фотонов МОС

Таким образом, качество приема МОС определяется ООСП и возможностью различения двух нижних уровней. ООСП показывает, насколько легко сигнал может быть выделен на фоне помех, а условие превышения вторым уровнем МОС уровня чувствительности приемника характеризует энергетические соотношения параметров принимаемого сигнала и приемника.

Вместе с тем, вводимую мощность нельзя увеличивать бесконечно – при увеличении мощности сигнала начинают проявляться нелинейные эффекты. В виду многообразия видов оптических волокон, а так же отраслевых стандартов значение суммарной вводимой мощности в световод может варьироваться [3, 13]. Ввиду того, что на повышение ООСП расходуется общий ресурс вводимой в главный оптический трат мощности, необходимо обеспечение условий нормального функционирования систем передачи, работающих в спектральных каналах (СК), не подверженных оптимизации. Для этого следует наложить ограничение на вероятность ошибки в каждом СК. Вместе с тем, различные абсолютные значения мощности помехи и шума могут давать равные значения ООСП. Возможна ситуация, когда нижние уровни сигнала окажутся за порогом чувствительности приемника. В связи с данным физическим ограничением необходимо рассматривать возможность применения многоуровневого сигнала при условии превышения вторым уровнем сигнала на приеме граничного значения чувствительности.

Учитывая связь вероятности ошибки и ООСП (выражение (6)), указанные условия записываются следующим образом:

$$\begin{cases} OSDR_i \geq OSDR_{\text{ТР}_i}, \\ P_{\text{вых}_{i,2}} > P_{\text{РЧ}_i} \end{cases} \quad (7)$$

где $P_{\text{вых}_{i,2}}$ – мощность импульса для второго уровня МОС на выходе световода, Вт; $P_{\text{РЧ}_i}$ – реальная чувствительность ФПУ i-го СК, Вт; $OSDR_{\text{ТР}_i}$ – требуемое для нормального функционирования системы в i-м СК ООСП. В данном случае рассматривается реальная чувствительность как минимальный поток излучения, который может быть

обнаружен на фоне собственных шумов безотносительно требуемой вероятности ошибки.

Для проверки возможности применения МОС той или иной размерности в конкретной ВОСП необходимо и достаточно проверить условия (7).

Сущность способа оценивания возможности применения МОС в ВОСП заключается в том, что оценивают мощность второго уровня МОС на фотоприемнике, и сравнивают с чувствительностью ФПУ. Затем вычисляют ООСП на выходе световода и сравнивают с требуемым для нормального функционирования ООСП. Если хотя бы одно неравенство из выражения (7) не выполняется, то делают вывод о непригодности данной ВОСП для передачи МОС интересующей размерности.

Исходными данными для рассматриваемого способа являются параметры световода, необходимые для решения нелинейного уравнения Шредингера (уравнения распространения сигнала), используемого для получения описания сигнала на выходе световода; вектор размеров ансамблей сигналов, на пригодность к передаче которого оценивается ВОСП; чувствительность ФПУ; мощность аддитивных шумов и длительность импульса оптического сигнала при соответствующем M_i.

Предлагаемый способ может быть использован для произвольного числа спектральных каналов. Соответствующие процедуры начала и окончания цикла с постусловием представлены шагами 2 и 10.

Вычисление шага 3 – менее ресурсоемкая процедура, чем вычисление шагов 5 и 6, так как не требует реализации метода секущих. За счет такого порядка проверки условий (7) удалось достичь снижения вычислительных затрат в случае непригодности СК ВОСП к работе МОС.

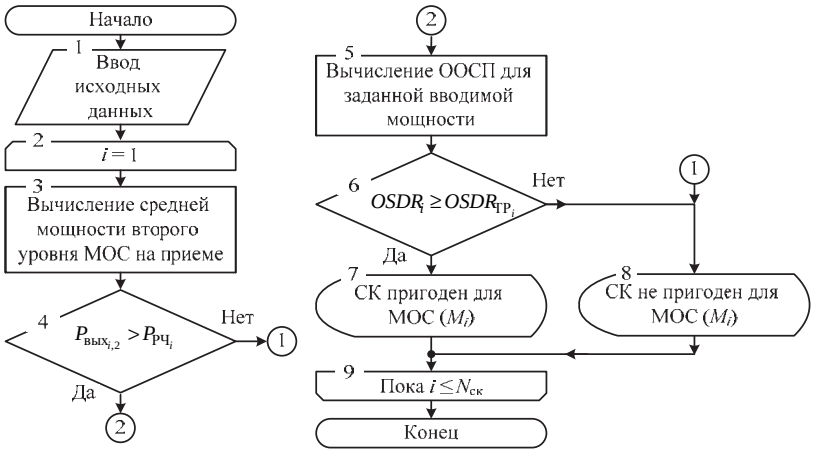


Рис. 4. Блок-схема способа оценивания возможности применения МОС в ВОСП

Решение о пригодности СК главного оптического тракта выносится индивидуально для каждого канала. Ввиду неоднородности группового спектра, как по предъявляемым требованиям, так и по ООСП не все СК могут быть переведены на работу МОС.

5. Заключение. Ввиду высокой актуальности вопросов повышения пропускной способности имеющихся ВОСП, а следовательно, удешевления затрат на передачу единицы информации активно исследуются МОС.

Граничное значение эквивалентной вероятности ошибки на бит для МОС (6) является верхней вероятностью ошибки для оптической обработки сигнала с многоуровневой модуляцией интенсивности. В то же время, оценка (6) асимптотически наилучшая для вероятности ошибки в постдетекторной области: за счет квантового выхода и шум-фактора ФПУ вероятность ошибки может только увеличиваться.

Сформулированные необходимое и достаточное условия применимости МОС в СК ВОСП-СР легли в основу способа оценивания возможности применения МОС в ВОСП.

Полученные решения обобщены на случай МОС и многоволновых ВОЛТ, но могут быть применены и к традиционным бинарным сигналам (для случая $M = 2$), в том числе в одноволновых ВОСП.

Литература

1. *Avlonitis N.S., Nikolas N.S., Yeatman E.M.* Performance of 4-ary ASK in Nonlinear, Multi-Channel Environments. URL: http://www.ee.ucl.ac.uk/lcs/previous/LCS2004/46.pdf (дата обращения 01.02.2015).
2. *Qian D., Huang M-F., Ip E., Huang Y-K., Shao Y., Hu J., Wang T.* 101,7 Tb/s (370x294-Gb/s) PDM-128QAM-OFDM transmission over 3x55 km SSMF using pilot-based phase noise mitigation // Optical Fiber Communication Conference and Exposition (OFC/NFOEC). 2011. PDPB5. pp. 1345–1351.
3. *Новиков А.Г., Трещиков В.Н., Плаксин С.О., Плоцкий А.Ю., Наний О.Е.* Перспективные *DWDM* системы связи со скоростью 20 Тбит/с на соединение // Фотон-экспресс. 2012. №3. С. 34–37.
4. *Величко М.А., Наний О.Е., Сусьян А.А.* Новые форматы модуляции в оптических системах связи // Lightwave Russian edition. 2005. №4. С. 21–30.
5. *Мясин К.И.* Модель М-го симметричного канала с квантовым шумом // Науковедение: интернет-журнал. 2014 №1 (20). URL: http://www.naukovedenie.ru/pdf/11tvn114.pdf (дата обращения 01.02.2015).
6. *Саитов И.А., Щекотихин В.М.* Теоретические основы построения средств связи оптического диапазона // Орел: Академия ФСО России. 2008. 491 с.
7. *Wei H., Plant D.V.* Quantum noise in optical communication systems // Optical modeling and performance predictions // Proceedings of SPIE. 2003. vol. 5178. pp. 139-147.
8. *Drummond P.D., Corney J.F.* Quantum noise in optical fibers I: stochastic equations // Journal of the Optical Society of America B. 2001. vol. 18(2). pp. 139-152.
9. *Слепов Н.Н.* Современные технологии цифровых оптоволоконных сетей связи // М.: Радио и Связь. 2005. 468 с.

10. Прокис Дж. Цифровая связь: перевод с англ. / под общ. ред. Д.Д. Кловского // М.: Радио и связь. 2000. 800 с.
11. *Перина Я.* Квантовая статистика линейных и не линейных оптических явлений // М.: Мир, 1987. 368с.
12. *Агравал Г.П.* Применение нелинейной волоконной оптики: учебное пособие // СПб.: Лань. 2011. 591 с.
13. *Листвин В.Н., Трещиков В.Н.* DWDM системы: научное издание // М.: Наука. 2013. 300 с.

References

1. Avlonitis N.S., Nikolas N.S., Yeatman E.M. Performance of 4-ary ASK in Nonlinear, Multi-Channel Environments. Available at: http://www.ee.ucl.ac.uk/lcs/previous/LCS2004/46.pdf (accessed 01.02.2015).
2. Qian D., Huang M-F., Ip E., Huang Y-K., Shao Y., Hu J., Wang T. 101,7 Tb/s (370x294-Gb/s) PDM-128QAM-OFDM transmission over 3x55 km SSMF using pilot-based phase noise mitigation. Optical Fiber Communication Conference and Exposition (OFC/NFOEC). 2011 PDPB5. pp. 1345–1351.
3. Novikov A.G., Treshhikov V.N., Plaksin S.O., Plockij A.Ju., Nanij O.E. [Future DWDM communication systems with a speed 20 Tbit/with on connection]. *Fotonjekspress – Photon-express Journal*. 2012. vol. 3. pp. 34–37. (In Russ.).
4. Velichko M.A., Nanij O.E., Sus'jan A.A. [New formats of modulation in optical communication systems]. *Lightwave Russian edition*. 2005. vol. 4. pp. 21–30. (In Russ.).
5. Mjasin K.I. [Model of M-ary symmetric channel with quantum noise]. *Naukovedenie : Internet-zhurnal – On-line Journal "Naukovedenie"*. 2014. vol. 1(20). Available at: http://naukovedenie.ru/pdf/11tvn114.pdf (accessed 01.02.2015). (In Russ.).
6. Saitov I.A., Shhekotihin V.M. *Teoreticheskie osnovy postroenija sredstv svjazi opticheskogo diapazona* [Theoretical bases of construction of a communication facility of an optical range]. Orel: Akademija FSO Rossii. 2008. 491 p. (In Russ.).
7. Wei H., Plant D.V. Quantum noise in optical communication systems. Optical modeling and performance predictions. *Proceedings of SPIE*. 2003. vol. 5178. pp. 139-147.
8. Drummond P.D., Corney J.F. Quantum noise in optical fibers I: stochastic equations. *Journal of the Optical Society of America B*. 2001. vol. 18(2). pp. 139-152.
9. Slepov N.N. *Sovremennye tehnologii cifrovyh optovolokonnyh setej svjazi* [Modern technologies of digital fibre-optical communication networks]. M.: Radio i Svjaz'. 2005. 468 p. (In Russ.).
10. Proakis J.G. *Digital communications. 4th edition*. McGraw Hill Higher Education. 2000. 1024 p. (Russ. ed.: Prokis J. *Cifrovaja svjaz'*. M.: Radio i Svjaz'. 2000. 800 p.).
11. Perina Ja. *Kvantovaja statistika linejnyh i ne linejnyh opticheskih javlenij* [The quantum statistics linear and nonlinear optical phenomena]. M.: Mir. 1987. 368 p. (In Russ.).
12. Agrawal G.P. *Primenenie nelinejnoj volokonnoj optiki: uchebnoe posobie* [Application of nonlinear fiber optics: tutorial]. SPb. : Lan'. 2011. 591 p. (In Russ.).
13. Listvin V.N., Treshhikov V.N. DWDM sistemy [DWDM systems]. M.: Nauka. 2013. 300 p. (In Russ.).

Саитов Игорь Акрамович — д-р техн. наук, профессор, начальник факультета, Академия Федеральной службы охраны Российской Федерации. Область научных интересов: оптическая связь, транспортные сети связи. Число научных публикаций — 160. Akramovish@mail.ru; ул. Приборостроительная, 35, Орел, 302034, РФ; р.т.:+7(4862)549801.

Saitov Igor' Akramovich — Ph.D., Dr. Sci., professor, chief of faculty, The Academy of Federal Security Guard Service of the Russian Federation. Research interests: optical communication, transport communication networks. The number of publications — 160. Akramovish@mail.ru; 35, Priborostroitelnaya Street, Orel, 302034, Russia; office phone: +7(4862)549801.

Мясин Николай Игоревич — к-т техн. наук, доцент, Академия Федеральной службы охраны Российской Федерации. Область научных интересов: волоконно-оптические системы передачи с усилителями, нелинейные эффекты в оптических волокнах, технические средства охраны и контроля доступа. Число научных публикаций — 50. staryi_nik@mail.ru; Приборостроительная, 35, Орел, 302034; р.т.: +7(486)2549913.

Mjasin Nikolaj Igorevich — Ph.D., associate professor, The Academy of Federal Security Guard Service of the Russian Federation. Research interests: fiber-optical communication systems with amplifiers, nonlinear effects in optical fibers, means of protection and the access control. The number of publications — 50. staryi_nik@mail.ru; 35, Priborostroitelnaya Street, Orel, 302034, Russia; office phone: +7(486)2549913.

Мясин Константин Игоревич — преподаватель, Академия Федеральной службы охраны Российской Федерации. Область научных интересов: волоконно-оптические системы передачи с многоуровневыми сигналами, квантовый шум, искажения оптического сигнала. Число научных публикаций — 30. fmmc@mail.ru; Приборостроительная, 35, Орел, 302034; р.т.: +7(486)2549912.

Mjasin Konstantin Igorevich — lecturer, The Academy of Federal Security Guard Service of the Russian Federation. Research interests: fiber-optical communication systems with multilevel modulation, quantum noise, distortion optic signal. The number of publications — 30. fmmc@mail.ru; 35, Priborostroitelnaya Street, Orel, 302034, Russia; office phone: +7(486)2549912.

РЕФЕРАТ

Саитов И.А., Мясин Н.И., Мясин К.И. **Определение пригодности волоконно-оптических систем связи для передачи многоуровневых оптических сигналов.**

Статья посвящена оцениванию пригодности волоконно-оптической линии связи к работе многоуровневыми оптическими сигналами с целью увеличения скорости передачи информации.

Во введении представлено обоснование актуальности исследования. Целесообразность изложенного материала заключается в повышении точности решения задач проектирования и управления за счет учета свойств оптических многоуровневых сигналов и особенностей их распространения.

Далее, авторы обосновывают выбор показателя «отношение средней мощности оптического сигнала к средней мощности оптической помехи» в додетекторной области с учетом специфики модели волоконно-оптического канала связи. Такой показатель позволяет наиболее адекватно сравнивать волоконно-оптические системы передачи и формулировать оптимизационные задачи в додетекторной области.

В третьем параграфе работы представлено оригинальное авторское видение проблемы вычисления вероятности ошибки оптического сигнала. По известной методике, описанной Дж. Прокисом, получено граничное значение для вероятности ошибки при оптической обработке сигнала. Данная оценка может быть использована для полностью оптических линий связи или для сравнения систем додетекторной обработки сигнала.

Четвертый параграф непосредственно посвящен разработке способа определения пригодности системы передачи для работы многоуровневыми оптическими сигналами. Для решения задачи оценивания возможности применения многоуровневых оптических сигналов в волоконно-оптической системе передачи авторы выдвигают необходимое и достаточное условия. Эти условия положены в основу способа проверки пригодности системы передачи к приему с заданной достоверностью сигналов с многоуровневой модуляцией интенсивности. Итеративное применение представленного способа с размером ансамбля сигналов в качестве параметра позволяет находить максимально допустимое число уровней модуляции интенсивности.

В заключении обобщены результаты и представлены основные положения работы.

Представленный материал адресован аспирантам, ученым и инженерам, работающим в области разработки и модернизации волоконно-оптических систем связи.

SUMMARY

Saitov I.A., Mjasin N.I., Mjasin K.I. **Determining the Suitability of the Fiber-Optic Communication Systems for Transmission of Multi-Level Signals.**

The article is devoted to assessing the suitability of a fiber-optic link to work of the multi-level optical signals, for the purpose of increase in information transmission rate.

In the introduction substantiation of relevance of the research is presented. The expediency of the material is to increase the accuracy of the design and operational management problems solution by taking into consideration properties of multi-level optical signals and their distribution characteristics.

Further, the authors justified the choice of parameter «optical signal-to-disturbance ratio» in subdetection area, taking into account the specifics of the model fiber optic link. This parameter allows the most adequate to compare the fiber-optic communication systems and to formulate optimization tasks in subdetection area.

In the third paragraph of the paper an original author's vision of the bit error probability calculation problem for the optical signal is presented. By the known technique described by J. Proakis the boundary value for the error probability in optical signal processing is obtained. This estimate can be used for all-optical communication lines or comparison subdetektor signal processing systems.

The fourth paragraph is directly devoted to development of determining suitability method of a transmission system for multi-level optical signals. To solve the problem of estimating the possibility of using multi-level optical signals in a fiber optic communication system, the authors formulate the necessary and sufficient conditions. These conditions are the basis for a method for checking the suitability of the transmission system to the reception given to the reliability of signals with multilevel modulation intensity. Iterative application of the present method with the signals ensemble size of as a parameter allows finding the maximum number of levels of intensity modulation.

In conclusion the results are summarized and the main theses of work are resented.

The material is addressed to graduate students, scientists and engineers working in the development of the fiber-optic communication systems.

УДК 621.3.089.2

М.С. Григоров, О.О. Басов

МЕТОДИКА МУЛЬТИЭНЕРГЕТИЧЕСКОЙ РЕНТГЕНОГРАФИИ ИЗДЕЛИЙ МИКРОЭЛЕКТРОНИКИ С НЕОДНОРОДНОЙ СТРУКТУРОЙ

Григоров М.С., Басов О.О. **Методика мультиэнергетической рентгенографии изделий микроэлектроники с неоднородной структурой.**

Аннотация. Анализ существующих систем неразрушающего рентгеновского контроля изделий микроэлектроники, их основных возможностей и характеристик свидетельствует о необходимости внедрения метода мультиэнергетической рентгенографии, позволяющего расширить возможности цифровой рентгенографии на изделия микроэлектроники с неоднородной структурой. Разработанная методика позволяет получить минимальный набор цифровых рентгеновских изображений изделия микроэлектроники с неоднородной структурой за счет обоснованного выбора команд источнику рентгеновского излучения для запуска «рабочих» режимов экспозиции. Указанный набор изображений обеспечивает возможность проведения контроля дефектов изделия по результатам визуализации внутренней структуры всех его функциональных элементов с требуемым качеством.

Ключевые слова: мультиэнергетическая рентгенография, изделие микроэлектроники, рентгеновское изображение, показатель качества рентгеновского изображения.

Grigorov M.S., Basov O.O. **Technique of a Multipower X-Ray Analysis of Products of Microelectronics with Non-Uniform Structure.**

Abstract. The analysis of the existing systems of nondestructive x-ray control of products of microelectronics, their main opportunities and characteristics testifies to need of introduction of a multipower X-ray analysis method allowing to expand possibilities of a digital X-ray analysis for microelectronics products with non-uniform structure. The developed technique allows us to receive the minimum set of digital x-ray images of a product of microelectronics with non-uniform structure due to a reasonable choice of commands to a source of x-ray radiation in order to actuate the "working" modes of exposition. The specified set of images provides the possibility of monitoring product defects by results of visualization of the internal structure of all its functional elements with the demanded quality.

Keywords: multipower x-ray analysis, microelectronics product, x-ray image, indicator of quality of the x-ray image.

1. Введение. Современное производство изделий микроэлектроники (ИМ) предъявляет высокие требования к контролю качества выпускаемой продукции. При этом оценка качества изделий, для которых применение "традиционных" методов диагностики и локализации дефектов малоэффективно или невозможно в силу различных причин, может быть произведена только с использованием неразрушающего рентгеновского контроля (НРК).

Современные ИМ характеризуются сложной, многослойной, а, следовательно, неоднородной (с точки зрения ослабления рентгеновских лучей) структурой. Большое количество разнородных функциональных элементов (ФЭ) в составе ИМ обуславливает необходимость

проведения нескольких рентгеновских экспозиций, обеспечивающих для каждого типа ФЭ (уровня неоднородности) ИМ формирование рентгеновского изображения (РИ) требуемого качества. Увеличение числа формируемых РИ требует обработки и анализа каждого из них, что приводит к возрастанию количества итераций и, соответственно, времени реализации задач НРК, в частности, по расшифровке дефектов ИМ.

Поэтому в настоящее время объективно существует противоречие между необходимостью получения изображения всех ФЭ ИМ с требуемым качеством, и необходимостью снижения затрат времени на проведение НРК. Его разрешение лежит в области автоматизации существующих систем НРК за счет совершенствования математического и программного обеспечения процедуры формирования РИ ИМ с неоднородной структурой. Указанный подход представляет собой сложную научно-техническую задачу и обуславливает актуальность исследований.

2. Существующие подходы к реализации мультиэнергетической рентгенографии. Процесс формирования набора РИ в описанных выше условиях принято называть мультиэнергетической рентгенографией.

В медицине известен метод двухэнергетической рентгенографии [1, 2], согласно которого из двух изображений, сделанных при разных анодных напряжениях на рентгеновской трубке, путем субтракции получают изображения мягких и костных тканей. Указанный метод также получил широкое распространение для выявления опасных вложений в ручной клади и багаже [3, 4].

Для исследования возможности повышения точности разделения веществ с близкими эффективными атомными номерами в [5] был предложен метод трехэнергетической рентгенографии, где решение поставленной задачи осуществлялось двумя способами:

1) используя энергоселективные свойства трех линеек детекторов, за одно сканирование формируется три изображения объекта контроля в различных энергетических диапазонах при одном выбранном анодном напряжении источника рентгеновского излучения. Достоинством этого способа можно считать высокую скорость получения изображений, недостатком – существенное перекрытие энергетических диапазонов при получении изображения;

2) используя высокую точность позиционирования механизма перемещения объекта контроля последовательно получают три его изображения при трех разных анодных напряжениях и различных условиях фильтрации с последующим совмещением изображений, полу-

ченных в трех энергетических диапазонах. В этом случае достигается лучшее энергетическое разделение.

Опираясь на известные методы рентгенографии, нашедшие применение в других областях, разработана методика мультиэнергетической рентгенографии, позволившая расширить возможности цифровой рентгенографии на изделия микроэлектроники с неоднородной структурой.

3. Методика мультиэнергетической рентгенографии изделий микроэлектроники с неоднородной структурой. Разработанная методика включает в себя следующие шаги.

1. Установление зависимости интенсивности излучения $J^{\text{И}}(\lambda)$ от параметров источника рентгеновского излучения (анодного напряжения U^{A} и анодного тока i^{A} рентгеновской трубки).

2. Интерполяция полученных значений интенсивности для обеспечения большей точности установки параметров источника рентгеновского излучения.

3. Формирование набора команд $\left\{C_j(U^{\text{A}}, i^{\text{A}})\right\}, j = \overline{1...N}$ источнику рентгеновского излучения на основе анализа зависимости значений количественного показателя качества $Q_{\text{кол}}$ от режима работы источника.

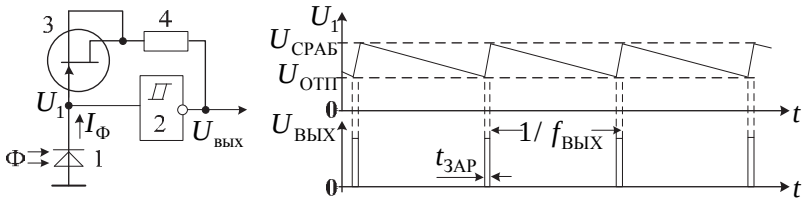
4. Формирование первого (опорного) РИ ИМ с неоднородной структурой.

5. Выбор набора команд $\left\{C_j(U^{\text{A}}, i^{\text{A}})\right\}, j = \overline{1...N},$ обеспечивающих получение для каждого типа ФЭ ИМ изображения требуемого качества.

6. Формирование РИ в моменты действия анодных напряжения U^{A} и тока i^{A}, соответствующих командам из набора $\left\{C_j(U^{\text{A}}, i^{\text{A}})\right\}$.

Для реализации методики предложено ввести в контур регулирования источника рентгеновского излучения звено обратной связи на основе датчика (детектора) рентгеновского излучения (рисунок 1).

В качестве приемника излучения в данном датчике применен фотодиод (1), снабженный металлическим экраном, установленным для защиты схемы от излучения большой мощности, и триггер Шмитта (2) с нелинейной цепью обратной связи, содержащей сопротивление $R_{\text{ОС}}$ (4) и полевой транзистор (3) в диодном включении. При сравнительной простоте построения такой фотодатчик обеспечивает линейное преобразование потока излучения Φ_J в частоту f_X выходных импульсов за счет цепи отрицательной обратной импульсной связи.



а) *б)*

Рис. 1. Микромощный датчик рентгеновского излучения: *а* – принципиальная электрическая схема; *б* – временные диаграммы работы

Принцип действия детектора рентгеновского излучения основан на медленном заряде собственной емкости $C_Д$ фотодиода в зоне гистерезиса $\Delta U_Г$ триггера Шмитта фототоком $I_Ф = \Phi_J S_\lambda$, прямо пропорциональным измеряемому потоку излучения Φ_J и световой чувствительности S_λ фотодиода, с последующим быстрым разрядом емкости фотодиода до исходного уровня током обратной связи. Если пренебречь длительностью времени разряда $t_{РАЗ}$ емкости $C_Д$ фотодиода по сравнению со временем ее заряда $t_{ЗАР}$, то при выполнении неравенства $t_{ЗАР} \gg t_{РАЗ}$ частота выходных импульсов определяется соотношением:

$$f_X \approx \frac{I_Ф}{\Delta U_Г C_Д} \approx \frac{\Phi_J S_\lambda}{\Delta U_Г C_Д} = \Phi_J K_Ф,$$

где $K_Ф = S_\lambda / \Delta U_Г C_Д$ – коэффициент преобразования фотодетектора.

Для преобразования частоты f_X выходных импульсов детектора излучения в цифровой код N_X разработана следующая схема (рисунок 2). В данном преобразователе реализован принцип цифрового измерения частоты, согласно которому число выходных импульсов детектора излучения суммируется в счетчике на постоянном интервале измерения $T_{ИЗМ} = const$, в конце которого на выходах счетчика формируется код

$$N_X = f_X T_{ИЗМ} = \Phi_J K_Ф T_{ИЗМ},$$

прямо пропорциональный измеряемому потоку рентгеновского излучения Φ_J.

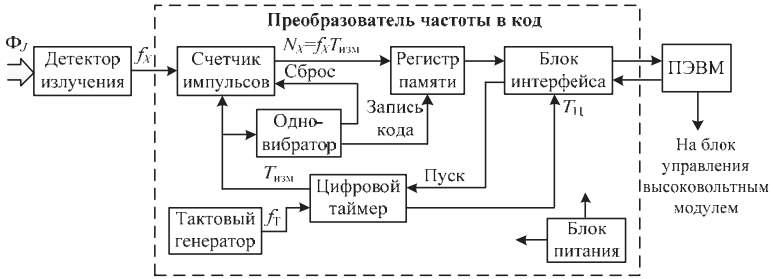


Рис. 2. Структурная схема преобразователя частоты импульсов в цифровой код

В схеме преобразователя частоты в код (рисунок 2) применены цифровой таймер с номинальной емкостью счета $N_{\text{НОМ}}$ и кварцевый генератор импульсов высокой тактовой частоты $f_{\text{Т}} \gg f_X$, служащие для формирования такта измерения постоянной длительности, составляющей $T_{\text{ИЗМ}} = N_{\text{НОМ}} / f_{\text{Т}} = (0{,}1...0{,}5)$ с.

Выбор длительности такта измерения, равной целому числу периодов частоты 50 Гц, позволяет значительно ослабить влияние помех промышленной частоты на результат преобразования фототока. Процесс заполнения интервала $T_{\text{ИЗМ}}$ импульсами измеряемой частоты f_X эквивалентен ее интегрированию на данном участке времени, что приводит к значительному (в сотни раз) ослаблению влияния периодических помех на результат измерения [6].

В схеме преобразователя частоты в цифровой код используются регистр памяти, служащий для запоминания выходного кода N_X в конце такта измерения $T_{\text{ИЗМ}}$, и блок интерфейса для связи с управляющей ЭВМ. Блок интерфейса преобразует параллельный цифровой код, снимаемый с выходов регистра памяти, в последовательный код, который передается на ЭВМ по линии связи. Соответствующие команды для регулирования и установки анодного напряжения и тока в высоковольтном источнике анодного напряжения поступают от ЭВМ на блок управления высоковольтным модулем, обеспечивающим гальваническую разделение выходов ЭВМ от высоковольтных электрических цепей.

Измерение потока излучения Φ_J начинается при подаче импульса "Пуск" от ПЭВМ, который поступает через блок интерфейса на управляющий вход цифрового таймера. При этом цифровой таймер формирует импульс заданной длительности $T_{\text{ИЗМ}}$, поступающий на вход "Разрешение счета" счетчика, в течение которого выходные импульсы

датчика излучения частоты f_X суммируются в счетчике и непрерывно увеличивают значение его выходного кода. По окончанию интервала измерения $T_{\text{ИЗМ}}$, т. е. по срезу импульса на выходе цифрового таймера срабатывает одновибратор и формирует короткий импульс, который поступает на С-вход записи регистра памяти и на R-вход сброса счетчика. По фронту этого импульса выходной код N_X счетчика записывается в регистр памяти, после чего высоким уровнем этого импульса выполняется сброс счетчика, при котором все его выходы устанавливаются в нулевое состояние. После окончания такта измерения $T_{\text{ИЗМ}}$ подается сигнал от цифрового таймера на ЭВМ через блок интерфейса, который является сигналом разрешения на считывание полученного значения выходного кода и его запись в память ЭВМ.

Для повышения точности управления интенсивностью потока рентгеновского излучения в устройстве выполняется автоматическая аддитивная коррекция погрешности от влияния темнового тока $I_{\text{ФТ}}$ фотодиода. Особенность работы системы НРК заключается в том, что рентгеновский источник из-за большой рассеиваемой мощности работает в периодическом режиме. При этом формирование высокого напряжения на аноде рентгеновской лампы выполняется на коротком интервале времени, не превышающем 8 с, в течение которого формируется рентгенограмма объекта контроля, после чего напряжение на рентгеновской лампе отключается. Циклы измерения и остановки лампы задаются командами ЭВМ, что позволяет измерять темновой ток $I_{\text{ФТ}}$ фотодиода в детекторе излучения и формировать начальный код $N_{\text{НАЧ}} = I_{\text{ФТ}} T_{\text{ИЗМ}} / \Delta U_{\text{Г}} C_{\text{Д}}$, который автоматически вычитается из последующих результатов измерения потока рентгеновского излучения при работе системы НРК в активном режиме. Такая цифровая коррекция результатов преобразования позволяет практически исключить влияние темнового тока фотодиода на точность детектора излучения в широком температурном диапазоне.

Введение предложенного звена обратной связи в состав системы НРК позволяет установить зависимость интенсивности от параметров источника рентгеновского излучения рентгеновской трубки при значительно высокой точности ее установки.

При реализации опытного образца устройства использовались цифровые КМОП микросхемы серии К561: в детекторе излучения в генераторе тактовых импульсов и в одновибраторе применены микросхемы триггера Шмитта типа К561ТЛ1, в счетчике импульсов и таймере использовались микросхемы типа К561ИЕ11, К561ИЕ8, а регистр памя-

ти собран на микросхемах К561ИР9, и т. п. При изготовлении промышленной партии преобразователь частоты в код можно реализовать на простом микроконтроллере, а в канале связи с ЭВМ использовать стандартную микросхему приемопередатчика типа USB.

С использованием опытного образца устройства (рис. 2) был проведен натурный эксперимент по установлению искомой зависимости интенсивности $J^{\text{И}}(\lambda)$ рентгеновского излучения от анодного напряжения $U^{\text{А}}$ и анодного тока $i^{\text{А}}$ (таблица 1) для автономной просвечивающей полнокадровой рентгеновской установки «Калан-4У».

Таблица 1. Параметры излучения вне объекта контроля

$U^{\text{А}}/i^{\text{А}}$ (кВ/мА)	$J^{\text{И}}(\lambda)$, отн. ед.	$\overline{I_j}$	$C_{0,99}$	$Q_{\text{кол.}}$
80/1	1,76	35,21	0,0391	900,51
80/2	3,69	73,72	0,0273	2700,37
80/3	5,77	115,44	0,0273	4228,57
100/1	2,60	51,91	0,0273	1901,47
100/2	5,77	115,33	0,0273	4224,54
100/3	8,80	175,96	0,0273	6445,42
120/1	3,55	71,07	0,0273	2603,30
120/2	8,33	166,51	0,0234	7115,81
120/3	12,42	248,45	0,0273	9100,73
140/1	4,54	90,71	0,0273	3322,71
140/2	10,71	214,11	0,0273	7842,86
140/3	12,70	254	0,0273	9304,03
160/1	5,55	110,97	0,0273	4064,84
160/2	12,66	253,29	0,0273	9278,02
160/3	12,70	254	0,0234	10854,70
180/1	6,05	121	0,0273	4432,23
180/2	12,70	254	0,0234	10854,70
180/3	12,70	254	0,0273	9304,03

Для реализации второго шага методики предложено использовать кубическую интерполяцию полученных значений зависимости интенсивности $J^{\text{И}}(\lambda)$ рентгеновского излучения от анодного напряжения $U^{\text{А}}$ и анодного тока $i^{\text{А}}$. Это позволяет обеспечить большую точность установки заданной интенсивности рентгеновского излучения.

Аналогичным образом может быть установлена искомая зависимость для любого источника рентгеновского излучения. Она позво-

ляет сформировать набор команд $\left\{C_j(U^{\text{A}}, i^{\text{A}})\right\}, j = \overline{1...N}$, обеспечивающих получение области:

$$G^Q = \bigcup_{j=1}^{N} \bigcup_{i=1}^{O_j} G_{ji}^Q ,$$

где G_{ji}^Q – отдельные области рентгеновского изображения, сформированные по результатам сегментации и процедуры анализа качества.

Реализация третьего шага метода основана на анализе зависимости количественного показателя качества $Q_{\text{кол},ji}$ вне объекта контроля (таблица 1), упорядоченного в порядке возрастания, от режима работы (рисунок 3). В качестве количественного показателя качества области РИ ИМ использована величина:

$$Q_{\text{кол},ji} = \frac{\overline{I}_{G_{ji}}}{C_{G_{ji}}},$$

где $\overline{I}_{G_{ji}}$ – средняя яркость области G_{ji}; $C_{G_{ji}}$ – сосредоточенность долей энергии области G_{ji} при значении доли суммарной энергии m = 0,99 [7-11]. Об инвариантности сосредоточенности $C_{0,99}$ долей энергии РИ ИМ к яркости $\overline{I_j}$ его элементов свидетельствуют данные, приведенные в таблице 1.

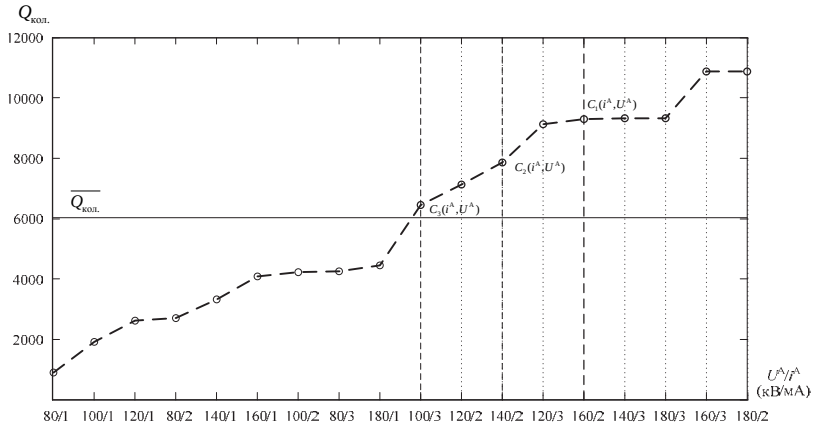


Рис. 3. Зависимость интенсивности рентгеновского излучения от режима работы рентгеновского источника

Сопоставление зависимости количественного показателя качества $Q_{\text{кол}.ji}$ от режима работы источника рентгеновского излучения с результатами экспертной оценки позволило сделать ряд важных выводов.

1. В качестве "рабочих" следует выбирать такие режимы работы рентгеновского излучателя (параметры $(U^{\text{A}}, i^{\text{A}})$), которые обеспечивают получение значений показателя $Q_{\text{кол.}} > \overline{Q_{\text{кол.}}}$, где $\overline{Q_{\text{кол.}}}$ – среднее значение данного показателя по множеству режимов работы излучателя. Это позволит реализовать пятый шаг разработанной методики.

2. Для формирования опорного РИ (четвертый шаг методики) следует использовать "средний" режим работы рентгеновского излучателя, попавший в диапазон "рабочих". В рассматриваемом случае такой режим формируется командой $C_1(160, 2)$, т.е. рентгеновский излучатель работает при следующих параметрах: $U_1^{\text{A}} = 160$ кВ, $i_1^{\text{A}} = 2$ мА.

3. В предположении, что источник рентгеновского излучения питается переменным (пульсирующим) анодным напряжением U^{A} и через него протекает переменный (пульсирующий) анодный ток i^{A}, получение РИ (шестой шаг методики) следует осуществлять в моменты времени действия анодных напряжения и тока, соответствующих значениям из "рабочего" диапазона режимов функционирования. Так для рассматриваемого случая (рисунок 3) моменты формирования команд $\left\{C_j(U^{\text{A}}, i^{\text{A}})\right\}, j = \overline{2...N},$ представлены на рисунке 4.

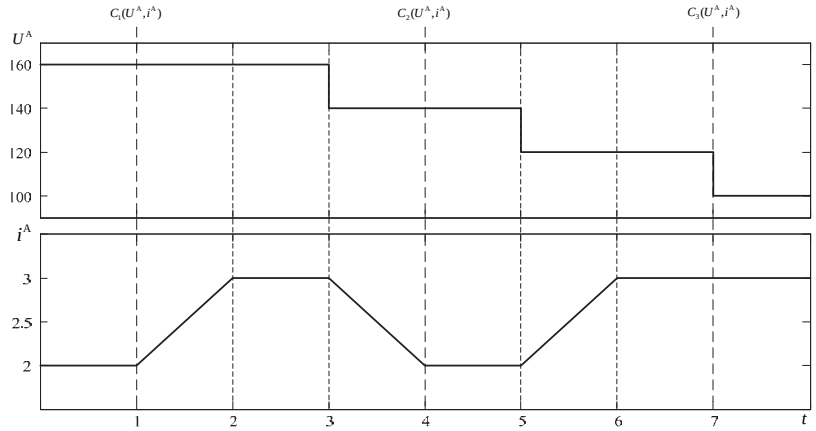


Рис. 4. Формирование команд источнику рентгеновского излучения

Реализация методики с учетом указанных рекомендаций позволяет получить набор рентгеновских изображений, обеспечивающий возможность провести контроль дефектов по результатам визуализации его внутренней структуры с требуемым качеством изображения для всех ФЭ ИМ [12, 13].

4. Заключение. В процессе исследования была решена задача внедрения метода мультиэнергетической рентгенографии в системы неразрушающего рентгеновского контроля, расширив возможности данных систем на изделия микроэлектроники с неоднородной структурой. Разработанная методика позволяет получить минимальный набор цифровых рентгеновских изображений изделия микроэлектроники с неоднородной структурой за счет обоснованного выбора команд источнику рентгеновского излучения для запуска "рабочих" режимов экспозиции.

Литература

1. *Мазуров А.И.* Последние достижения в цифровой рентгенотехнике // Медицинская техника. 2010. № 5(263). С. 10-14.
2. *Jens Ricke, et al*. Clinical results of Csl-detector-based dual-exposure dual energy in chest radiography // Eur Radiol. 2003. vol. 13. pp. 2577–2582.
3. *Macdonald R.* Design and implementation of a dual-energy X-ray imaging system for organic material detection in airport security application // Proc. SPIE. 2001. vol. 4301. pp. 31–41.
4. Способ улучшения распознаваемости материала в рентгеновской контрольной установке и рентгеновская контрольная установка // патент № 2462702. РФ. 2012. 11 с.
5. *Рыжиков В.Д., Ополонин А.Д., Волков В.Г., Лисецкая Е.К., Галкин С.Н., Воронкин Е.Ф.* Трехэнергетическая цифровая радиография для разделения веществ с малым эффективным атомным номером // Вісник НТУ «ХПІ». 2013. № 34(1007). С. 43–51.
6. *Орнатский П.П.* Автоматические измерения и приборы // Киев: Высш.шк. 1988. 486 с.
7. *Жиляков Е.Г., Черноморец А.А., Лысенко И.В.* Метод определения точных значений долей энергии изображений в заданных частотных интервалах // Вопросы радиоэлектроники. Сер. РЛТ. 2013. Вып. 4. С. 115–123.
8. *Черноморец А.А. Голощапова В.А., Лысенко И.В., Болгова Е.В.* О частотной концентрации энергии изображений // Научные ведомости БелГУ. Сер. История. Политология. Экономика. Информатика. 2011. №1(96). Вып. 17/1. С. 146–151.
9. *Жиляков Е. Г., Черноморец А.А., Белов А.С., Болгова Е.В.* О субполосных свойствах изображений // Научные ведомости БелГУ. Сер. История. Политология. Экономика. Информатика. 2013. №8(151). Вып. 26/1. С. 175–182.
10. *Черноморец А.А., Иванов О.Н.* Метод анализа распределения энергий изображений по заданным частотным интервалам // Научные ведомости БелГУ. Сер. История. Политология. Экономика. Информатика. 2010. №19(90). Вып.16/1. С. 161–166.
11. *Григоров М.С., Басов О.О.* Анализ распределения энергии рентгеновского изображения по частотным интервалам // Наукоемкие технологии и инновации (XXI научные чтения): Сборник научных трудов Международной научно-

практической конференции, посвященной 60-летию БГТУ им. В.Г. Шухова. 2014. С. 160–165.
12. *Григоров М.С., Басов О.О.* Применение мультиэнергетической цифровой рентгенографии для контроля качества изделий микроэлектроники с неоднородной структурой // Информационные технологии в науке, образовании и производстве: Сборник научных трудов VI Международной научно-технической конференции. Орел. 2014. URL: http://youconf.ru/itnop2014/materials/ manager/view/61.
13. *Григоров М.С., Басов О.О.* Автоматизация неразрушающего рентгеновского контроля изделий микроэлектроники при применении мультиэнергетической рентгенографии // Прогрессивные технологии и процессы: Сборник научных статей Международной молодежной научно-технической конференции. Курск: Юго-Зап. гос. ун-т. 2014. Том 1. С. 97–100.

References

1. Mazurov A.I. [Latest advances in digital rentgenotechnika]. *Medicinskaya tehnika – Medical equipment*. 2010. vol.5(263). pp. 10–14. (In Russ.).
2. Jens Ricke, et al. Clinical results of Csl-detector-based dual-exposure dual energy in chest radiography. *Eur Radiol*. 2003. vol. 13. pp. 2577–2582.
3. Macdonald R. Design and implementation of a dual-energy X-ray imaging system for organic material detection in airport security application. Proc. SPIE. 2001. vol. 4301. pp. 31–41.
4. [Method for improving ability to recognise materials in x-ray inspection system, and x-ray inspection system]. Patent no. 2462702. Russian Federation. 2012. 11 p. (In Russ.).
5. Rizikov V.D., Opolonin A.D., Volkov V.G., Liseckaya E.K., Galkin S.N., Voronkin E.F. [Three-power digital radiography for division of substances with small effective atomic number]. *Vestnik NTU «HPI» – Messenger of NTU «HPI»*. 2013. vol. 34(1007). pp. 43–51. (In Russ.).
6. Ornatskiy P.P. *Avtomaticheskie izmereniya i pribori* [Automatic measurements and devices]. Kiev: Highschool. 1988. 486 p. (In Russ.).
7. Zilyakov E.G., Chernomorets A.A., Lisenko I.V. [Method of determination of exact values of shares of energy of images in the set frequency intervals]. *Voprosi radioelektroniki. Ser. RLT – Questions electronics. Ser. RLT*. 2013. vol. 4. pp. 115–123. (In Russ.).
8. Chernomorets A.A., Goloshapova V.A., Lisenko I.V., Bolgova E.V. [About frequency concentration of energy of images]. *Nauchnie vedomosti BelGU. Ser. Istoriya. Politologiya. Economika. Informatika – Scientific sheets of BelSU. Ser. History. Political science. Economy. Informatics*. 2011. vol. 1(96). Issue 17/1. pp. 146–151. (In Russ.).
9. Zilyakov E.G., Chernomorets A.A., Belov A.S., Bolgova E.V. [About subband properties of images]. *Nauchnie vedomosti BelGU. Ser. Istoriya. Politologiya. Economika. Informatika. – Scientific sheets of BelSU. Ser. History. Political science. Economy. Informatics*. 2013. vol. 8(151). Issue 26/1. pp. 175–182. (In Russ.).
10. Chernomorets A.A., Ivanov O.N. [Method of the analysis of distribution of energiya of images on the set frequency intervals]. *Nauchnie vedomosti BelGU. Ser. Istoriya. Politologiya. Economika. Informatika. – Scientific sheets of BelSU. Ser. History. Political science. Economy. Informatics*. 2010. vol. 19 (90). Issue 16/1. pp. 161–166. (In Russ.).
11. Grigorov M.S., Basov O.O. [The analysis of distribution of energy of the x-ray image on frequency an interval]. *Naukoemkie tehnologii I innovacii (XXI nauchnie chteniya): Sbornik nauchnih trudov Mezdunarodnoy nauchno-praktecheskoy konferencii, posvyasennoy 60-letiu BGTU im. V.G. Shuhova* [High Tech and Innova-

tion (XXI Scientific Reading): Collection of scientific papers of International scientific-practical conference]. Belgorod. 2014. pp. 160–165. (In Russ.).
12. Grigorov M.S., Basov O.O. [Application of a multipower digital X-ray analysis for quality control of products of microelectronics with non-uniform structure]. *Informacionnie tehnologii v nauke, obrazovanii I proizvodstve: Sbornik nauchnih trudov VI Mezdunarodnoy nauchno-tehnicheskoy konferencii* [Information technology in science, education and production: Collection of scientific papers of VI International scientific-practical conference]. 2014. Available at: http://youconf.ru/itnop2014/materials/manager/ view/61. (In Russ.).
13. Grigorov M.S., Basov O.O. [Automation of nondestructive x-ray control of products of microelectronics at application of a multipower X-ray analysis]. *Progressivnie tehnologii I processi: Sbornik nauchnih statey Mezdunarodnoy molodeznoy nauchno-tehnicheskoy konferencii* [Progressive technology and processes: Collection of scientific papers of International youth scientific and technical conference]. Kursk. 2014. vol. 1. pp. 97–100. (In Russ.)

Григоров Михаил Сергеевич — научный сотрудник, Академия Федеральной службы охраны Российской Федерации. Область научных интересов: системы рентгеновского контроля, обнаружение сигналов побочных электромагнитных излучений технических средств, проектирование систем контроля. Число научных публикаций — 45. gms.orel@mail.ru; Приборостроительная, 35, Орел, 302034; р.т.: +7(4862)549579.

Grigorov Mihail Sergeevich — researcher, Academy of Federal Agency of protection of Russian Federation. Research interests: systems of x-ray control, detection of signals of compromising emanations of technical equipment, engineering of control systems. The number of publications — 45. gms.orel@mail.ru; 35, Priborostroitelnaya Street, Orel, 302034, Russia; office phone: +7(4862)549579.

Басов Олег Олегович — к-т техн. наук, докторант, Академия Федеральной службы охраны Российской Федерации. Область научных интересов: обработка и кодирование речевых и иконических сигналов, проектирование полимодальных инфокоммуникационных систем. Число научных публикаций — 165. oobasov@mail.ru; Приборостроительная, 35, Орел, 302034; р.т.: +7(4862)549533.

Basov Oleg Olegovich — Ph.D., doctoral student, The Academy of Federal Security Guard Service of the Russian Federation. Research interests: processing and coding of speech and iconic signals, polymodal infocommunicational systems design. The number of publications — 165. oobasov@mail.ru; 35, Priborostroitelnaya Street, Orel, 302034, Russia; office phone: +7(4862)549533.

РЕФЕРАТ

Григоров М.С., Басов О.О. **Методика мультиэнергетической рентгенографии изделий микроэлектроники с неоднородной структурой.**

В условиях устойчивого развития цифровых рентгеновских систем повышаются возможности проведения неразрушающего рентгеновского контроля изделий микроэлектроники. При этом для изделий микроэлектроники, которые обладают неоднородной структурой, возникает противоречие между необходимостью оперативно проводить контроль и получать рентгеновское изображение каждого элемента изделия с требуемым качеством.

По этой причине возникают задачи по автоматизации формирования минимального набора рентгеновских изображений изделия микроэлектроники с неоднородной структурой за счет обоснованного выбора команд источнику рентгеновского излучения для запуска "рабочих" режимов экспозиции.

Опираясь на известные методы рентгенографии, нашедшие применение в других областях, в работе была решена задача по внедрению метода мультиэнергетической рентгенографии в системы неразрушающего рентгеновского контроля, позволяющего расширить возможности цифровой рентгенографии на изделия микроэлектроники с неоднородной структурой.

Предложенная методика основана:

– на установлении зависимости интенсивности излучения от параметров источника рентгеновского излучения;

– интерполяции полученных значений интенсивности излучения;

– формировании набора команд источнику рентгеновского излучения на основе анализа зависимости значений количественного показателя качества от режима работы источника;

– формировании опорного рентгеновского изображения изделия микроэлектроники с неоднородной структурой;

– выборе набора команд, обеспечивающих получение изображения требуемого качества для каждого типа функциональных элементов изделия микроэлектроники;

– формировании рентгеновских изображений изделия микроэлектроники в моменты действия анодных напряжения и тока, соответствующих командам из предопределенного набора.

Разработанная методика позволяет получить минимальный набор рентгеновских изображений изделия микроэлектроники с неоднородной структурой, обеспечивающий возможность провести контроль дефектов изделия по результатам визуализации его внутренней структуры с требуемым качеством изображения для всех его функциональных элементов, за счет обоснованного выбора команд источнику рентгеновского излучения для запуска «рабочих» режимов экспозиции.

SUMMARY

Grigorov M.S., Basov O.O. **Technique of a Multipower X-Ray Analysis of Products of Microelectronics with Non-Uniform Structure.**

In the conditions of a sustainable development of digital x-ray systems possibilities of carrying out nondestructive x-ray control of products of microelectronics raise. Thus for microelectronics products, which possess non-uniform structure, there is a contradiction between the need to carry out control quickly and to receive the x-ray image of each element of a product with the demanded quality.

For this reason, there are tasks of automation of formation of the minimum set of x-ray images of a product of microelectronics with non-uniform structure due to a reasonable choice of teams to a source of x-ray radiation in order to actuate the "working" modes of an exposition.

Based on the known methods of a X-ray analysis, which found application in other areas in work, the task of introduction of a multi-power X-ray analysis method allowing to expand possibilities of a digital X-ray analysis on microelectronics products with non-uniform structure was solved.

The offered technique is based on:

– establishment of dependence of radiation intensity on parameters of a source of x-ray radiation;

– interpolation of the received values of intensity of radiation;

– formation of a set of commands to a source of x-ray radiation on the basis of the analysis of dependence of values of a quantitative quality index on a source operating mode;

– formation of the basic x-ray image of a product of microelectronics with non-uniform structure;

– a choice of a set of the commands providing the image of the demanded quality for each type of functional elements of a product of microelectronics;

– formation of x-ray images of a product of microelectronics at the moments of action of anode tension and current corresponding to the commands from the predetermined set.

The developed technique allows us to receive the minimum set of x-ray images of a product of microelectronics with non-uniform structure. This set provides the opportunity to carry out control of product defects by results of visualization of its internal structure with the demanded quality of the image for all its functional elements, due to a reasonable choice of commands to a source of x-ray radiation in order to actuate the "working" modes of exposition.

УДК 004.94

И.И. Лившиц, А.В. Полещук

ПРАКТИЧЕСКАЯ ОЦЕНКА РЕЗУЛЬТАТИВНОСТИ СМИБ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ РАЗЛИЧНЫХ СИСТЕМ СТАНДАРТИЗАЦИИ – ИСО 27001 И СТО ГАЗПРОМ

Лившиц И.И., Полещук А.В. **Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации – ИСО 27001 и СТО Газпром.**

Аннотация. В данной публикации кратко рассмотрена оценка результативности систем менеджмента информационной безопасности (СМИБ) в соответствии с требованиями различных систем стандартизации, например ГОСТ Р ИСО/МЭК серии 27001 и Системы обеспечения информационной безопасности СТО Газпром серии 4.2 (СОИБ). Данная проблема имеет важное значение для минимизации рисков нарушения ИБ и обеспечения стабильности процессов обработки информации. Обращено внимание на методические сложности совмещения требований различных систем стандартизации (ГОСТ Р ИСО/МЭК и СОИБ), которые необходимо учитывать при оценке постоянного улучшения результативности СМИБ. Предложены формулы для расчета результативности СМИБ и рассмотрены практические примеры (кейсы), поясняющие расчет для конкретных ситуаций. Данные результаты могут найти применение при создании моделей и методов обеспечения аудитов СМИБ и мониторинга состояния объектов, находящихся под воздействием угроз нарушения ИБ, а также при создании моделей и методов оценки защищенности информации и ИБ объектов СМИБ и/или СОИБ Газпром.

Ключевые слова: система менеджмента информационной безопасности (СМИБ), система обеспечения информационной безопасности (СОИБ), метрики ИБ, объект защиты (ОЗ), меры (средства) информационной безопасности.

Livshits I.I., Poleshuk A.V. **Practical Assessment of the ISMS Effectiveness in Accordance with the Requirements of the Various Standardization Systems both ISO 27001 and STO Gazprom.**

Abstract. This issue briefly covers the need of numerical evaluation for Information Security Management Systems (ISMS) effectiveness in accordance with the requirements of two or more different standardization systems, such as ISO / IEC 27001 series of standards and Information Security Providing System STO Gazprom series 4.2 (ISPS). This problem is important to minimize the violation of IT-security risks and ensure the information processes stability in the information systems. This issue describes methodological difficulties in reconciling the requirements of different Standardization systems both ISO / IEC and ISPS that must be considered when assessing the ISMS effectiveness. The formulas have been proposed to solve the problem for calculating the ISMS effectiveness and discussed practical examples (cases), explaining the calculation for specific situations. These results can be used to create models and methods to provide the ISMS audits and monitoring IT-security facilities both ISMS and / or ISPS Gazprom.

Keywords: Information Security Management System (ISMS), Information security providing system (ISPS), metrics, object of protection (ObP), controls.

1. Введение.

Проблема оценки результативности СМИБ в соответствии с требованиями стандартов ГОСТ Р ИСО/МЭК серии 27001 [1–2] является достаточно известной. Значительно более

сложной проблемой является обеспечение постоянного улучшения результативности СМИБ, созданной с учетом дополнительных отраслевых стандартов (например, СОИБ Газпром [4 – 9]). Решение поставленной выше проблемы может быть затруднено объективными различиями в требованиях СОИБ, которые могут усложнить успешное внедрение СМИБ (например, различия в понятиях «актив» и «объект защиты»). В равной мере это относится и к требованиям по менеджменту рисков [2], а также правилам проведения аудитов в соответствии со стандартом ИСО серии 19011 [3]. В случае, когда высшее руководство организации принимает решение о внедрении и подготовке СМИБ к внешнему аудиту, представляется необходимым проанализировать требования текущей реализации СОИБ (оценить уровень, на котором они реализованы) и выработать решение о комплексе мероприятий, которые следует предпринять для целей обеспечения соответствия СМИБ требованиям стандарта [1]. Одним из важнейших требований, включенных в цикл PDCA, является требование повышения результативности (см. п. 7.1, 8.1 стандарта [1]). Эти оценки должны быть представлены высшему руководству (ЛПР) для принятия адекватных («разумных» в терминах [10]) управленческих решений. Предлагается несколько примеров расчета результативности СМИБ, прошедших практическую апробацию.

2. Необходимые термины и определения. Для решения поставленной проблемы рассмотрим несколько необходимых терминов из [1] и [11]:

1. *Событие информационной безопасности* (*information security event*): идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью. Отметим, что это определение точно совпадает по п. 3.5 в [1]и по п. 3.2 [11].

2. *Инцидент информационной безопасности* (*information security incide*nt): Появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ (п. 3.3. по [11]). Но в стандарте [1] представлено иное определение: «*Инцидент информационной безопасности* (*information security incident*): Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность» (п. 3.6. по [1]).

Обратим внимание, что «целевой» стандарт по сертификации СМИБ [1] трактует термин «инцидент ИБ» иначе, чем стандарт по управлению инцидентами ИБ [11]. Прежде всего, стандарт [11] устанавливает четкую логическую последовательность – инцидент ИБ является следствием события (событий) ИБ. В тоже время определение по [11] объективно более емкое – дает четкую «привязку» на бизнес-активы и угрозы ИБ, что подразумевает некоторый «операционный» анализ, выполняемой в организации, исходя из внутренних потребностей, технических возможностей и целей ИБ.

Следующие термины важны для ясного и однозначного понимания «предмета измерения». Расчет результативности СМИБ [1] выполняется в точном соответствии в терминах по ГОСТ Р ИСО серии 9000, в котором приведены следующие два термина:

3. *Результативность* (*effectiveness*): степень реализации запланированной деятельности и достижения запланированных результатов (п. 3.2.14)

4. *Эффективность* (*efficiency*): Связь между достигнутым результатом и использованными ресурсами (п. 3.2.15)

В методическом плане представляется рациональным говорить именно об оценке результативности СМИБ, т.к. для оценки эффективности нужно оперировать дополнительно затраченными ресурсами: финансовыми параметрами деятельности организации и, детально, динамикой их изменения (бюджет службы ИБ, штатная численность, стоимость технических средств (ТС), внешние услуги и пр.) [12 – 15]. Дополнительно принимается во внимание, что выбор мер (средств) обеспечения ИБ (“controls”) для ИС является важной задачей, которая может иметь значительные последствия в отношении бизнес-операций и защищаемых активов организации, а также вовлеченного персонала, что также вносит существенные бюджетные решения и процесс капиталовложений [2, 16 – 17].

3. Определение сущностей для расчета результативности. Для практической реализации выбранных ключевых сущностей и достоверной оценки результативности СМИБ потребуются выполнить определенные предположения. Появляется роль «оператора», который в режиме, близком к режиму реального времени (РРВ), анализирует совокупность событий (их может быть несколько тысяч в достаточно краткий период) и принимает решение о фиксации события ИБ и/или инцидента ИБ – в случае если нанесен ущерб. В расчете результативности СМИБ предлагается применять три ключевые сущности: Событие, Событие ИБ и Инцидент ИБ.

1. *Событие* – любое изменение установленного состояния контролируемых объектов. (event, alert, «сработка» ТС и/или СЗИ). События фиксируются в журналах (проход сотрудника через КПП), в log-файлах (межсетевые экраны), в архивах (системы видеонаблюдения) и пр. Важно, что событие всегда «идентифицировано», т.е. является материальным фактом, может быть извлечено, проанализировано «оператором», передано на дальнейшую обработку, протестировано на стенде и пр. Важно также, что событие само по себе не приводит к угрозам ИБ, тем более – к ущербу ИБ (бизнесу). Предполагается, что число событий может быть велико и достигать нескольких тысяч в день, это обстоятельство накладывает определенные ограничения на «глубину» архива и временной лимит для анализа (обработки) «сырых» событий со стороны оператора. *Должно выполняться*: Кол-во событий > 0.

2. *Событие ИБ* – результат анализа множества «сырых» событий со стороны оператора. Анализ событий ИБ выполняется на основании определенных критериев (например, количество ошибок при вводе пароля, количество просроченных сертификатов ЭЦП и пр.). Важно, что в качестве событий ИБ могут выступать записи аудитов – внутренних и внешних, которые также являются фиксированными событиями (см. выше). Предполагается, что по факту события ИБ может быть предпринято расследование (при эскалации как инцидент ИБ). Предполагается, что число событий ИБ может достигать сотни в год. *Должно выполняться*: Кол-во событий > Кол-во событий ИБ.

3. *Инцидент ИБ* – в нотации ГОСТ 18044 [11] это следствие проявления событий ИБ, что возможно приведет к компрометации бизнеса или угрозе ИБ. Важно, что инцидент является именно следствием события ИБ, на основании решения «оператора» по итогам анализа события ИБ. Для каждого идентифицированного инцидента ИБ принимается решение о вероятности реализации угроз и возникновения ущерба (например, угроза финансовых потерь при передаче носителя с сертификатом ЭЦП неуполномоченному лицу). По инциденту ИБ всегда проводится расследование с отражением факта преодоления (попытки) существующих мер и средств обеспечения ИБ (“*controls*”), оценке конкретного ущерба ИБ. Предполагается, что число инцидентов ИБ может достигать десятков в год. *Должно выполняться*: Кол-во событий ИБ > Кол-во инцидентов ИБ.

4. Установленные дополнительные ограничения для расчета. Практическая реализация выбранных сущностей требует

фиксации дополнительных ограничений по выполненным ранее предположениям:

1. *Область сертификации СМИБ (“scope”)* – если выбрано на определенный период только несколько процессов (например, обеспечение ИБ для работы в сети интернет), то ошибки ввода паролей в АСУТП не принимаются при расчетах ни количества событий ИБ, ни инцидентов ИБ.

2. *Временной интервал* – необходимо выполнять сравнение между состоянием «*до СМИБ*», т.е. когда ТС были внедрены, но сама система СМИБ формально не вводилась в действие, персонал не проходил должного обучения и определенные дополнительные нормативные документы (регламенты) не разрабатывались и текущим состоянием, отсчитываемым, например, по годам.

3. *Техническая возможность* – необходимо обеспечить техническую возможность по обработке значительного количества событий в режиме, близком к режиму реального времени (РРВ) по структурным подразделениям и «селекции» событий ИБ, которые попадают в *scope* текущей конфигурации СМИБ.

4. *Оператор* – необходимо обеспечить наличие «оператора», доступность, компетентность и оснащенность которого позволяет принимать решения в фиксированном временном интервале о назначении события ИБ и/или инцидента ИБ в силу достоверной и объективной информации по множеству входных событий.

5. *Норма допустимой результативности* – необходимо обеспечить учет «порогового» допустимого значения, которое является ориентиром для расчета текущего уровня результативности СМИБ (в текущей конфигурации ***scope***). В расчете «порогового» допустимого значения участвует плановый (задаваемый ЛПР) показатель повышения результативности СМИБ, например, 10%.

6. *Зрелость СМИБ* – необходимо принять во внимание, что для СМИБ, находящихся на разных уровнях зрелости, представляется целесообразным применять разные формулы определения результативности. В частности, на первом этапе «приработки» СМИБ могут применяться простые формулы, с увеличением опыта и технического оснащения (“***controls***”) могут применяться полиномы с системой весовых коэффициентов, расчет которых представляют отдельную задачу.

5. Формулы расчета результативности СМИБ. С учетом сказанного выше для СМИБ рекомендуются к применению следующие формулы, учитывающие, например, раздельно события ИБ и инциденты ИБ. В этом варианте особую роль приобретает техническая

оснащенность «оператора», о чем указывалось выше. В частности, реализованный в СМИБ комплекс ТС должен позволять «селектировать» из многих тысяч событий в режиме, близком к РРВ, события, относящиеся к сотрудникам одной службы, даже если они находятся в разных подсетях (VLAN). Соответственно, результативность СМИБ рассчитывается следующим образом:

Расчет результативности событий ИБ:

$$\text{К с} = \left(\mathbf{1} - \left(\frac{\text{С тек.}}{\text{С } max}\right)\right) * \mathbf{100}\%, \quad (1)$$

где:

Кс – коэффициент результативности идентификации событий ИБ;

С***тек*** – идентифицированное количество событий ИБ в текущей конфигурации ***scope***;

С***max*** – максимально возможное количество событий ИБ за предыдущий период.

Расчет результативности инцидентов ИБ:

$$\text{К и} = \left(\mathbf{1} - \left(\frac{\text{И тек.}}{\text{И } max}\right)\right) * \mathbf{100}\%, \quad (2)$$

где:

Ки – коэффициент результативности идентификации инцидентов ИБ;

И ***тек*** – идентифицированное количество инцидентов ИБ в текущей конфигурации scope;

И ***max*** – максимально возможное количество инцидентов ИБ за предыдущий период.

С учетом положений (1) и (2) общий показатель результативности СМИБ рассчитывается:

$$\text{К смиб} = (\text{К с} * \boldsymbol{\alpha} + \text{К и} * \boldsymbol{\beta}), \quad (3)$$

где:

К смиб – общий показатель результативности СМИБ

Кс – коэффициент результативности идентификации событий ИБ;

Ки – коэффициент результативности идентификации инцидентов ИБ;

α – весовой коэффициент определения важности Кс;

β – весовой коэффициент определения важности Ки.

Формула (3) обладает рядом особенностей:

1. При С***тек*** = 0 и И***тек*** = 0 мы получаем абсолютный 100% уровень ИБ, несмотря на ведущийся «лог» многочисленных «сырых» событий. Если «оператор» не выделил события ИБ (нет «видимых»

нарушений ИБ), не определил инциденты ИБ (нет ущерба ИБ или компрометации бизнес-процессов).

2. Весовые коэффициенты α и β нормируются к единице (α + β= 1) и определяют значимость для конкретного объекта (процесса СМИБ) значимость событий и инцидентов ИБ. В простейшем случае α = β = 0,5.

6. Примеры кейсов для расчета результативности СМИБ. Рассмотрим несколько практических примеров расчета результативности СМИБ по формуле (3) для случая зрелой СМИБ.

Кейс 1.

Для С***тек*** = 54, С ***max*** = 60, И ***тех***. = 18 и И***max*** = 21, α = β = 0,5 получаем:

$$\text{К смиб} = \left(\left(1 - \left(\frac{54}{60}\right) * 100\%\right) * 0{,}5 + \left(1 - \left(\frac{18}{21}\right) * 100\%\right) * 0{,}5\right) = 12{,}14\%.$$

Вывод: При установленной ЛПР К смиб ≥ 10 %, цель достигнута.

Кейс 2.

Для С***тек*** = 70, С ***max*** = 60, И ***тех***. = 18 и И***max*** = 23, α = β = 0,5 получаем:

$$\text{К смиб} = \left(\left(1 - \left(\frac{70}{60}\right) * 100\%\right) * 0{,}5 + \left(1 - \left(\frac{18}{23}\right) * 100\%\right) * 0{,}5\right) = -8{,}33 + 10{,}86 = 2{,}53\%.$$

Вывод: При установленной ЛПР К смиб ≥ 10 %, цель не достигнута.

Кейс 3.

Для С***тек*** = 70, С ***max*** = 60, И ***тех***. = 18 и И***max*** = 23, α = 0,3 β = 0,7 получаем:

$$\text{К смиб} = \left(\left(1 - \left(\frac{70}{60}\right) * 100\%\right) * 0{,}3 + \left(1 - \left(\frac{18}{23}\right) * 100\%\right) * 0{,}7\right) == -5 + 15{,}21 = 10{,}21\ \%.$$

Вывод: При установленной ЛПР К смиб ≥ 10 %, цель достигнута.

7. Дополнительные метрики ИБ, применяемые для оценки результативности СМИБ. С целью снижения ущерба и потери ценных для бизнеса активов, для службы ИБ предлагаются метрики, показывающие степень достижения возможного максимума (плана продаж, выполнения в срок проектов и пр.) [12, 15–17]. Соответственно, могут быть предложены различные типы метрик:

— простые метрики (например, количество выявленных инцидентов ИБ, предотвращенных утечек);

— сложные метрики (например, отношение стоимости мер защиты к стоимости ИТ активов);

— комплексные метрики (например, число произошедших инцидентов ИБ, приведших к ущербу (вынужденному простою) в ИС, определенных как критичные для бизнеса).

В качестве практических метрик ИБ рекомендуются к применению:

— Кс = (1 – С тек * 100% / С макс) – для оценки динамики событий ИБ;

— Кр = (1 – Кс (повторных) * 100% / Кс) – для оценки динамики повторных событий ИБ (рецидив);

— Кд = (С макс – С тек) / (К макс – К тек) – для оценки динамики приращений событий ИБ и инцидентов ИБ.

8. Выводы:

1. Для оценки результативности СМИБ (вне зависимости от целей, типов и частоты аудитов), необходимо обеспечить управление достоверными и удобными для анализа численными метриками ИБ. Представляется важным, что оценки результативности СМИБ явным образом влияют на изменение статуса службы ИБ, и соответствующего технического оснащения (бюджета). В то же время предоставление «слабых» оценок ИБ может быть расценено как несоответствие понимания роли службы ИБ в обеспечении успешного достижения бизнес-целей организации.

2. При создании СМИБ, соответствующих множеству требований (отраслевой сертификации, национальным стандартам ГОСТ Р, международным стандартам ISO) в общем случае, необходимо учитывать и уникальные отраслевые особенности – например, с помощью весовых коэффициентов. Но в этом случае, как было показано в практических примерах (кейсах), существует сложность выделения по значимости какой-либо одной сущности, группы активов или набора технических средств.

3. При прогнозировании и обеспечения постоянного повышения результативности СМИБ необходимо формировать сопоставимые метрики ИБ, которые позволят оценить сделанные предварительно предположения и допущения и сформировать обоснованные цели в области СМИБ, направленные на обеспечение стабильного развития бизнеса организации.

Литература

1. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования // М.: ФАТРиМ России. 2008.
2. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности // М.: ФАТРиМ России. 2011.
3. ГОСТ Р ИСО 19011-2011 Руководящие указания по проведению аудитов систем менеджмента // М.: ФАТРиМ России. 2013.
4. СТО Газпром 4.2-1-001-2009 Система обеспечения информационной безопасности ОАО «Газпром». Основные термины и определения // М.: ОАО «Газпром». 2009.
5. СТО Газпром 4.2-2-002-2009 Система обеспечения информационной безопасности ОАО «Газпром». Требования к автоматизированным системам управления технологическими процессами // М.: ОАО «Газпром». 2009.
6. СТО Газпром 4.2-3-002-2009 Требования по технической защите информации при использовании информационных технологий // М.: ОАО «Газпром». 2009.
7. СТО Газпром 4.2-3-003-2009 Система обеспечения информационной безопасности ОАО «Газпром». Анализ и оценка рисков // М.: ОАО «Газпром». 2009.
8. СТО Газпром 4.2-3-004-2009 Классификация объектов защиты // М.: ОАО «Газпром». 2009.
9. СТО Газпром 4.2-3-005-2013 Управление инцидентами информационной безопасности // М.: ОАО «Газпром». 2013.
10. *Ногин В.Д.* Принятие решений при многих критериях // Государственный Университет – Высшая школа экономики. Санкт-Петербург. 2007. 103 с.
11. ГОСТ Р ИСО/МЭК 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности // М.: ФАТРиМ России, 2008.
12. *Карпенко М.С.* Учет факторов риска и неопределенности при реализации энергосберегающих проектов // Энергобезопасность и Энергосбережение. 2014. Вып. 6. С. 13–16.
13. *Лившиц И.И.* Совместное решение задач аудита информационной безопасности и обеспечения доступности информационных систем на основании требований международных стандартов BSI и ISO // Информатизация и Связь. 2013. Вып. 6. С. 62–67
14. *Лившиц И.И.* Практические применимые методы оценки систем менеджмента информационной безопасности // Менеджмент качества. 2013. Вып. 1. С. 22–34.
15. *Лившиц И.И.* Актуальность применения метрик информационной безопасности для оценки результативности проектов систем менеджмента информационной безопасности // Менеджмент качества. 2015. Вып. 1. С. 74–81
16. NIST.SP.800-53Ar4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations. URL: http://dx.doi.org/10.6028/
17. *Брукс П.* Метрики для управления ИТ-услугами // Альпина Бизнес Букс. 2007. 270 с.

References

1. GOST R ISO/IEC 27001:2005. [Information technology. Security techniques. Information security management systems. Requirements].M.: FATRiM Rossii. 2008. (In Russ.).
2. GOST R ISO/IEC 27005:2010. [Information technology. Security techniques. Information technology. Security techniques. Information security risk management]. M.: FATRiM Rossii. 2011. (In Russ.).
3. GOST R ISO 19011:2011. [Guidelines for auditing management systems]. M.: FATRiM Rossii. 2013. (In Russ.).

4. STO Gazprom 4.2-1-001-2009. [IT-Security Providing System. Terms and Definition]. M.: OAO Gazprom. 2009. (In Russ.).
5. STO Gasprom 4.2-2-002-2009. [IT-Security Providing System. Requirements for automated process control system]. M.: OAO Gazprom. 2009. (In Russ.).
6. STO Gasprom 4.2-3-002-2009. [IT-Security Providing System. Requirements for technical protection of information when using information technology]. M.: OAO Gazprom, 2009. (In Russ.).
7. STO Gasprom 4.2-3-003-2009. [IT-Security Providing System. Analyses and assessment of Risk]. M.: OAO Gazprom. 2009. (In Russ.).
8. STO Gasprom 4.2-3-004-2009. [IT-Security Providing System. Object of protection classification]. M.: OAO Gazprom. 2009. (In Russ.).
9. STO Gasprom 4.2-3-005-2013. [IT-Security Providing System. IT-Security Incident Management]. M.: OAO Gazprom. 2009. (In Russ.).
10. Nogin V.D. *Prinyatie resheniy pri mnogih kriteriyah* [Decision-making in many criteria]. St. University, St. Petersburg, 2007. 103 p. (In Russ.).
11. GOST R ISO/IEC 18044-2007. [Information technology. Security techniques. Information security incident management]. M.: FATRiM Rossii, 2008. (In Russ.).
12. Karpenko M. [Managing the risks and uncertainties in the implementation of energy saving projects]. *Jenergobezopasnost' i Jenergosberezhenie – Energy Security and Energy Saving.* 2014. vol. 6. pp. 13–16 (In Russ.).
13. Livshitz I.I. [Joint problem solving information security audit and ensure the availability of information systems based on the requirements of international standards BSI / ISO]. *Informatisatia i Svyaz' – Informatization and Communication.* 2013. vol. 6. pp 48–51 (In Russ.).
14. Livshitz I.I. [Practical purpose methods for ISMS evaluation]. *Menedzhment kachestva – Quality Management*. 2013. vol. 1. pp. 22–34 (In Russ.)..
15. Livshitz I.I [Actuality of IT-security metrics appliance for ISMS evaluation]. *Menedzhment kachestva – Quality Management.* 2015. vol. 1. pp. 74–81 (In Russ.).
16. NIST.SP.800-53Ar4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations. Available at: http://dx.doi.org/10.6028.
17. Bruks P. *Metriki dlja upravlenija IT-uslugami* [Metrics for IT-service management]. Alpina Business Books. 2007. 270 p. (In Russ.).

Лившиц Илья Иосифович — к-т техн. наук, ведущий аналитик, ООО "Газинформсервис". Область научных интересов: системный анализ, защита информации, риск-менеджмент. Число научных публикаций — 50. Livshitz.il@yandex.ru; 198188, Санкт-Петербург, а/я 35; р.т.: +7(812) 677-20-50, Факс: +7(812) 677-20-51.

Livshitz Ilya Iosifovich — Ph.D., lead analyst, LLC “Gasinformservice”. Research interests: system analyses, IT-security, risk-management. The number of publications — 50. Livshitz.il@yandex.ru; 198188, Saint-Petersburg, a/ja 35; office phone: +7(812) 677-20-50, Fax: +7(812) 677-20-51.

Полещук Александр Владимирович — к-т техн. наук, эксперт по информационной безопасности, ООО «Академия Информационных Систем». Область научных интересов: системный анализ, защита информации, управление событиями и инцидентами ИБ. Число научных публикаций — 50. sailor1981@rambler.ru; ул. Плеханова, 4а, Москва, 111141; р.т.: +7 (495) 817-08-70.

Poleshuk Alexander Vladimirovich — Ph.D., IT-Security expert, JSC "IT-System Academia". Research interests: system analyses, IT-security, IT-security incident and events management. The number of publications — 50. sailor1981@rambler.ru; 4a, Plehanova, Moscow, 111141, Russia; office phone: +7 (495) 817-08-70.

РЕФЕРАТ

Лившиц И.И., Полещук А.В. **Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации – ИСО 27001 и СТО Газпром.**

В данной публикации рассмотрена проблема оценки результативности СМИБ в соответствии с требованиями стандартов ИСО серии 27001. Более сложной проблемой является проблема обеспечение постоянного улучшения результативности СМИБ, созданной с учетом дополнительных отраслевых стандартов (например, СОИБ Газпром). Решение поставленной выше проблемы может быть затруднено объективными различиями в требованиях СОИБ, которые могут усложнить успешное внедрение СМИБ (например, различия в понятиях «актив» и «объект защиты»). В равной мере это относится и к требованиям по менеджменту рисков, а также правилам проведения аудитов в соответствии со стандартом ИСО серии 19011.

Стандарт ИСО 27001 трактует термин «инцидент ИБ» иначе, чем стандарт ИСО 18044, отмечено, что стандарт по управлению инцидентами устанавливает четкую логическую последовательность – инцидент ИБ является следствием события (событий) ИБ. Это определение по ИСО 18044 объективно более емкое – дает четкую «привязку» на бизнес-активы и угрозы ИБ, что подразумевает некоторый «операционный» анализ, выполняемой в организации, исходя из внутренних потребностей и целей ИБ.

Для СМИБ рекомендуются к применению следующие формулы, учитывающие, например, раздельно события ИБ и инциденты ИБ. В этом варианте особую роль приобретает техническая оснащенность «оператора». В частности, реализованный в СМИБ комплекс технических средств должен позволять «селектировать» из многих тысяч событий в режиме, близком к реальному времени, события, относящиеся к сотрудникам одной службы, даже если они находятся в разных подсетях (VLAN). Соответственно, результативность СМИБ рассчитывается с учетом уникальных отраслевых особенностей – например, с помощью весовых коэффициентов. Представляется важным, что оценки результативности СМИБ явным образом влияют на изменение статуса службы ИБ, и соответствующего технического оснащения (бюджета). В то же время предоставление «слабых» оценок ИБ может быть расценено как несоответствие понимания роли службы ИБ в обеспечении успешного достижения бизнес-целей организации. Данные результаты могут найти применение при создании моделей и методов обеспечения аудитов СМИБ и мониторинга состояния объектов, находящегося под воздействием угроз нарушения ИБ, а также при создании моделей и методов оценки защищенности информации и ИБ объектов СМИБ и/или СОИБ Газпром.

SUMMARY

Livshits I.I., Poleshuk A.V. **Practical Assessment of the ISMS Effectiveness in Accordance with the Requirements of the Various Standardization Systems both ISO 27001 and STO Gazprom.**

This issue covers the problem of assessing ISMS effectiveness in accordance with the requirements of ISO 27001 series and more complex problems – concerning ensuring the continuous improvement for ISMS effectiveness, created with the additional industry standards (eg, STO ISPS Gazprom). The solution of the above problems can be complicated by objective differences in the requirements ISPS that can complicate the successful ISMS implementation (eg, differences in terms of "asset" and "object of protection"). This equally applies to the requirements for risk management, as well as the rules of the audits in accordance with ISO 19011 series.

ISO 27001 interprets the term "security incidents" other than ISO 18044, it is noted that the standard incident management establishes a clear logical sequence – the IT-security incident is a consequence of the IT-Security event (s). This definition is in accordance with ISO 18044 objectively more capacious - gives a clear "links" on the business assets and threats to IT-Security, which implies a certain "operational" analysis performed by the organization on the basis of domestic needs and IT-Security objectives.

For ISMS it recommended to use the following formulas, taking into account, for example, separate IT-Security incidents and IT-Security events. In this embodiment, a special role is played by the technical equipment of "operator". In particular, implemented in ISMS set of technical tools should allow to "select" more than thousands of events per short period related to a single service employees, even if they are on different subnets (VLAN). Accordingly, the ISMS effectiveness is calculated with taking into account the unique features of the sector - for example, using weighting factors. It is important that the assessment of ISMS effectiveness explicitly affect the change in the status of IT-Security department, and the appropriate technical equipment (budget). At the same time providing the "weak" estimates of IT-Security can be regarded as inconsistent with the understanding of the role of IT-Security department to ensure the successful achievement of the business objectives of the organization. These results can be used to create models and methods to ensure the ISMS audits and monitoring of objects under the influence of threats to IT-Security violations, as well as the creation of models and methods of estimation of IT-Security facilities ISMS and / or ISPS Gazprom.

УДК 006.72

А.Ю. Коваленко

БАЛЛИСТИЧЕСКОЕ ПРОЕКТИРОВАНИЕ РАЗНОРОДНОЙ СИСТЕМЫ КА С ЗАДАННЫМ ЦИКЛОМ ЗАМЫКАНИЯ ТРАССЫ

Коваленко А.Ю. **Баллистическое проектирование разнородной системы КА с заданным циклом замыкания трассы.**
Аннотация. Разработан подход к формированию устойчивой разнородной системы КА. Сформировано требование обеспечения кратности квазисинхронных орбит. Произведена декомпозиция задачи формирования орбит с заданным циклом замыкания трассы. Разработана методика формирования кратных квазисинхронных орбит различных геометрических характеристик с единым циклом замыкания трассы в заданных условиях движения.
Ключевые слова: разнородная система КА, квазисинхронные орбиты, уточнение параметров движения, цикл замыкания трассы.

Kovalenko A. **Ballistic Design of Heterogeneous System of the Spacecraft with a Given Cycle of Track Circuit.**
Abstract. An approach to the formation of a stable heterogeneous system of the spacecraft is developed. Requirement to provide quasi-synchronous orbits multiplicity is formed. Decomposition of problem of formation of orbits with a given cycle of track circuit is carried out. Method of forming multiple quasi-synchronous orbits of various geometric characteristics of a single cycle of track circuit in the given operating conditions is developed.
Keywords: heterogeneous system spacecraft, quasi-synchronous orbit, clarification of motion parameters, cycle of track circuit.

1.Введение. Формирование разнородной системы КА возможно как на основе уже функционирующих в космическом пространстве КА [1], так и на основе вновь запускаемых КА, то есть система изначально проектируется как разнородная.

В первом случае формируется временно-устойчивая структура системы КА, в которой по истечении заданного времени баллистическое построение изменится относительно начального [2]. Во втором случае, при проектировании разнородной системы КА, возможно формирование системы устойчивого баллистического построения с постоянным временным интервалом (периодом повторяемости системы), через который взаимное положение КА в системе повторяется.

Под периодом повторяемости системы понимается промежуток времени относительно начального момента времени, через который относительное положение всех КА системы в космическом пространстве повторяется.

Формирование системы устойчивого баллистического построения осуществляется с использованием квазисинхронных орбит [3],

которые обеспечивают стабильное положение орбиты относительно земной поверхности.

На квазисинхронную орбиту может быть наложено условие кратности, под которым понимается равенство с заданной точностью координат и проекций вектора скорости центра масс КА в Гринвичской системе координат через постоянный интервал времени ($T_{\text{ЦЗТ}}$), называемый циклом замыкания трассы (ЦЗТ).

При использовании квазисинхронных орбит для построения системы обеспечивается не только повторяемость положения КА относительно земной поверхности, но и взаимное положение между КА системы в моменты времени отличающиеся на $T_{\text{ЦЗТ}}$. Поэтому использование квазисинхронных орбит позволяет сформировать устойчивую структуру разнородной системы КА, в которой КА находятся на разных орбитах, но имеют единый или близкий по величине ЦЗТ, который выбирается исходя из решаемых целевых задач, возможностей выведения КА и маневренных возможностей КА.

Баллистическое проектирование системы устойчивого баллистического построения разнородной системы КА начинается с выбором базовой квазисинхронной орбиты. Цикл замыкания трассы данной орбиты принимается в качестве циклов замыкания трассы для всех КА разнородной системы.

$$T_{\text{ЦЗТ}}^{\text{Б}} = T_{\text{ЦЗТ}}^{\text{КА}1} = \ldots = T_{\text{ЦЗТ}}^{\text{КА}j}, \qquad (1)$$

где $T_{\text{ЦЗТ}}^{\text{Б}}$ – базовый цикл замыкания трассы;

$T_{\text{ЦЗТ}}^{\text{КА1}}, \ldots T_{\text{ЦЗТ}}^{\text{КА}j}$ –циклы замыкания трасс соответственно КА_1 ,…, КА_j разнородной системы.

Выбор базовой орбиты производится исходя из минимизации энергетических затрат на создание разнородной системы по отдельному алгоритму, который выходит за рамки данной статьи и поэтому не рассматривается.

2. Методика формирование кратных квазисинхронных орбит. Задача формирования орбит с заданным $T_{\text{ЦЗТ}}^{\text{Б}}$ разделяется на две подзадачи, а именно формирование квазисинхронных орбит на множестве орбит КА, входящих в состав разнородной системы, относительно проектной базовой квазисинхронной орбиты, и уточнение параметров движения КА с целью обеспечения требуемого $T_{\text{ЦЗТ}}^{\text{Б}}$ в заданных условиях движения. Под условиями движения понимается физическое состояние среды движения и движущегося в ней КА [4].

Условие кратности квазисинхронных орбит может быть представлено следующим равенством [3]:

$$\frac{T_{\text{зв}}}{T_{\Omega}} = \frac{T_{\text{ЦЗТ}}}{N}, \qquad (2)$$

где $T_{\text{зв}}$ – продолжительность звездных суток;

T_{Ω} – драконический период обращения;

$T_{\text{ЦЗТ}}$ – продолжительность ЦЗТ в сутках;

N – количество целых витков за ЦЗТ.

Драконический период обращения для круговой орбиты с учетом второй зональной гармоники [5] в восходящем узле орбиты рассчитывается по формуле

$$T_{\Omega} = \frac{2\pi}{\sqrt{\mu}} R_0^{\frac{3}{2}} \left[1 - \frac{3}{4} c_{20} \left(\frac{R_{\text{Э}}}{R_0} \right)^2 \left(1 + 5\cos^2 i_0 \right) \right], \qquad (3)$$

где R_0 – радиус-вектор в восходящем узле орбиты;

i_0 – наклонение в восходящем узле орбиты;

$R_{\text{Э}} = 6378{,}136\,\text{км}$ – экваториальный радиус Земли.

При баллистическом проектировании системы устойчивого баллистического построения принимается условие, что все КА имеют одинаковое наклонение.

Формирование квазисинхронных орбит КА с единым ЦЗТ $T_{\text{ЦЗТ}}^{\text{Б}}$ осуществляется на основе выражения (2) методом последовательного увеличения или уменьшения количества витков (в зависимости уменьшения или увеличения высоты орбиты относительно начальной проектной квазисинхронной орбиты), укладывающихся в ЦЗТ.

Количество витков за ЦЗТ квазисинхронной орбиты 1-го КА на соответствующей итерации приближения определяется следующим выражением:

$$N_i^{\text{КА1}} = N_{\text{пр}} \pm \Delta N \cdot i, \quad i = 1, 2, 3, \ldots \qquad (4)$$

где $N_{\text{пр}}$ – количество витков за ЦЗТ начальной проектной квазисинхронной орбиты;

ΔN – шаг изменения витков в ЦЗТ.

Драконический период обращения на данной итерации определяется из следующего соотношения:

$$T_{\Omega i}^{\text{КА1}} = \frac{T_{\text{зв}} N_i^{\text{КА1}}}{T_{\text{ЦЗТ}}^{\text{Б}}}.$$

Подставляя полученное значение периода обращения $T_{\Omega i}^{\text{КА1}}$ в выражение (3) методом половинного деления получается значение радиус-вектора КА (R_0^i) для заданного отношения количества витков к продолжительности ЦЗТ. На основании полученного значения R_0^i осуществляется проверка пригодности орбиты по критерию требуемой высоты полета КА (R_{mp}) с заданной точностью ε:

$$\left| R_{mp} - R_0^i \right| = \varepsilon. \qquad (5)$$

В случае выполнения равенства (5) с заданной точностью (ε) квазисинхронная орбита является сформированной, в противном случае выполняется следующее приближение по количеству витков в выражении (4).

Таким образом формируется множество квазисинхронных орбит одинакового наклонения для каждого $КА_1,\ldots,КА_j$ разнородной системы, удовлетворяющее требованию единого ЦЗТ равного или близкого по величине ЦЗТ начальной проектной квазисинхронной орбиты, т.е. критерию (1).

В результате применения данного подхода к формированию системы устойчивого баллистического построения у квазисинхронных орбит формируются только их геометрические характеристики без изменения элементов орбиты, характеризующих ориентацию плоскости орбиты в пространстве.

Для управления группировкой КА необходимы параметры движения КА в проекциях на оси Гринвичской относительной системы координат для восходящего узла орбиты $(\vec{q}_0)$.

Рассчитанные по проектным параметрам значения параметров $\vec{q}_0$ имеют сравнительно низкую точность. Уточнение параметров движения КА, с целью обеспечения требуемого $T_{\text{ЦЗТ}}^{\text{Б}}$ в заданных условиях движения, а именно, совпадение с заданной точностью пара-

метров движения КА в проекциях на оси ГСК через $T^{\text{Б}}_{\text{ЦЗТ}}$ осуществляется при наличии следующих исходных данных:

– приближенные начальные условия движения $(\vec{q}_0)$, получаемые после выведения КА на заданную орбиту;

– набор возмущающих факторов, учитываемых при моделировании движения КА, которые составляют вектор условий движения $(\vec{\lambda})$.

При заданных начальных условиях замыкание трасс через $T^{\text{Б}}_{\text{ЦЗТ}}$ обеспечивается уточнением (корректировкой) параметров движения в начальной точке. Задача сводится к отысканию таких поправок $\Delta\vec{q}_0$ к начальным значениям параметров движения $\vec{q}_0$, при которых обеспечивается совпадение параметров движения КА в проекциях на оси гринвичской геоцентрической системы координат на моменты времени t_0 и $(t_0 + T^{\text{Б}}_{\text{ЦЗТ}})$, соответствующие прохождению восходящего узла орбиты с заданной точностью:

$$\vec{q}(t_0 + T_{\text{ЦЗТ}}) - \vec{q}_0(t_0) \le \varepsilon,$$

где ε – заданная точность.

В общем случае, при осуществлении прогнозирования движения КА на основе динамической модели вида, связь между параметрами движения $\vec{q}$ и начальными условиями $\vec{q}_0$ любого КА осуществляется нелинейной функцией f [4] вида:

$$\vec{q}(t) = f(\vec{q}_0, \vec{\lambda}, t). \qquad (6)$$

Решение поставленной задачи может быть достигнуто при её формализации в рамках линейной теории.

Линеаризуем выражение (6) в окрестностях точки начального приближения $\vec{q}_0$ и отнимем все нелинейные члены ряда, для этого разложим указанное выражение в ряд Тейлора:

$$\vec{q} = \vec{q}_0 + \frac{\partial q}{\partial q_0}\Delta\vec{q}. \qquad (7)$$

В векторном виде выражение (7) принимает вид СЛУ:

$$\delta\vec{q} = A\Delta\vec{q}, \tag{8}$$

где $\delta\vec{q}$ – вектор невязок параметров движения в моменты времени t_0 и $t_0 + T_{\text{ЦЗТ}}$;

$\Delta\vec{q}$ – вектор неизвестных поправок к уточняемому вектору q_0;

$A_{[6]} = \left[\dfrac{\partial q}{\partial q_0}\right]$ – матрица частных производных.

Решение СЛУ возможно при условии, что матрица А неособенная, тогда:

$$\Delta\vec{q} = A^{-1}\delta\vec{q}.$$

В связи с принятым допущением о линейном характере функции f полученное решение системы (8) будет иметь некоторую невязку:

$$\vec{\vartheta} = \delta\vec{q} - A\Delta\vec{q}.$$

Минимизация полученной невязки осуществляется итерационным способом путём последовательного уточнения начальных условий $\vec{q}_0$:

$$\vec{q}_{0,i} = \vec{q}_{0,i-1} + \Delta\vec{q}, \tag{9}$$

где i – номер итерации.

Итерационный процесс прекращается при достижении требуемой точности ε, т.е. до выполнения условия $\Delta\vec{q} \le \varepsilon$.

Таким образом, параметры движения КА, удовлетворяющие требованию обеспечения замыкания трасс с заданной точностью через заданное время $T_{\text{ЦЗТ}}$ определяются соотношением (9).

В связи с тем, что параметры движения ($\vec{q}_0$) определяются для восходящего узла орбиты, то для повышения точности определения параметров движения на момент времени прохождения плоскости экватора СЛУ (8) может быть представлена в следующем виде [6]:

$$\delta\vec{q} = A\Delta\vec{q} - \dot{\vec{q}}\Delta t, \tag{10}$$

где $\dot{\vec{q}}$ – производная вектора параметров движения по времени;

Δt – поправка к времени прохождения восходящего узла орбиты.

Решение СЛУ (10) осуществляется таким же образом как и системы (8), за исключением того, что для каждого приближения итера-

ционного процесса (9) поправка к координате z_0 определяется следующим выражением:

$$\Delta z_0 = \frac{z_0}{x_0^2 + y_0^2}(x_0 \Delta x_0 + y_0 \Delta y_0)$$

где x_0, y_0, z_0 – координаты на момент прохождения восходящего узла орбиты;

$\Delta x_0, \Delta y_0, \Delta z_0$ – поправки к координатам на момент прохождения восходящего узла орбиты.

3. Заключение. Применение квазисинхронных орбит позволяет проектировать разнородные системы КА, включающие в себя орбиты с различными геометрическими характеристиками, но, в то же время, имеющими единую временную кратность повторяемости относительно Земли. Исходя из предложенного подхода к проектированию квазисинхронных орбит разнородной системы КА возможно формирование параметров орбит системы устойчивого баллистического построения разнородной системы КА, а также уточнять их для заданных условий движения.

Проведенное моделирование показывает существование квазисинхронных орбит с единым ЦЗТ для различных высот над поверхностью Земли. В качестве начальной проектной квазисинхронной орбиты использована квазисинхронная шестисуточная околокруговая орбита с наклонением 67.1^0 и высотой 1079.396 км.

Результаты моделирования квазисинхронных орбит с $T_{\text{ЦЗТ}} = 6$ суток с учетом второй зональной гармоники гравитационного поля Земли представлены в виде графика на рисунке 1.

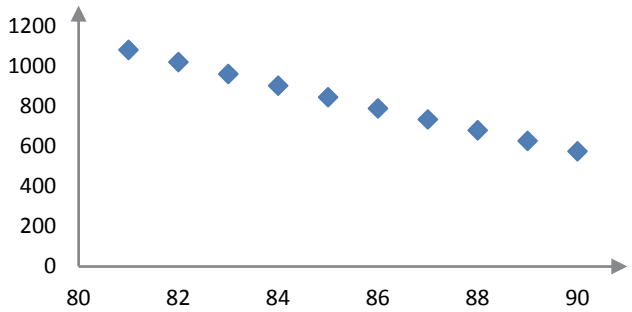


Рис. 1. Зависимость высоты квазисинхронной орбиты от количества витков в ЦЗТ

В результате уточнения одной из полученных квазисинхронных орбит высотой 913.25 км получен вектор параметров движения КА в

ГСК, соответствующий уточненной высоте 913.005 км, с учетом вторых зональных и тессеральных гармоник гравитационного поля Земли.

Литература

1. *Коваленко А.Ю., Мосин Д.А.* Формирование баллистических структур спутниковых систем в ближней операционной зоне на основе функционирующих космических аппаратов // Актуальные проблемы защиты и безопасности: Труды пятнадцатой Всероссийской научно-практической конференции. Санкт-Петербург. 2012. Том 1. С. 470–474.
2. *Коваленко А.Ю.* Анализ структурной устойчивости разнородной системы КА // Труды СПИИРАН. 2014. №4(35). С. 108–116.
3. *Власов С.А., Кульвиц А.В., Кубасов И.Ю., Мосин Д.А.* Баллистическое проектирование систем космических аппаратов: учебное пособие // СПб.: ВКА имени А.Ф.Можайского. 2007. 86 с.
4. *Ломако Г.И.* Экспериментальная баллистика КА // СПб.: ВИКА имени А.Ф.Можайского. 1997. 454 с.
5. *Баринов К.Н., Мамон П.А.* Теория полета космических аппаратов // М.: МО СССР. 1974. 346 с.
6. *Агаджанов П.А., Дулевич В.Е., Коростылев А.А.* Космические траекторные измерения. Радиотехнические методы измерений и математическая обработка данных // М.: Советское радио. 1969. 504 с.

References

1 Kovalenko A.Ju., Mosin D.A. [Formation of ballistic structures satellite systems operating in the near area on the basis of a functioning spacecraft]. *Aktual'nye problemy zashhity i bezopasnosti: Trudy pjatnadcatoj Vserossijskoj nauchno-prakticheskoj konferencii* [Actual problems of protection and security: Collected papers]. Sankt-Peterburg. 2012. vol 1. pp. 470-474. (In Russ.).

2 Kovalenko A.Ju. [Analysis of the structural stability of the heterogeneous system KA]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2014. no. 4(35). pp. 108-116. (In Russ.).

3 Vlasov S.A., Kul'vic A.V., Kubasov I.Ju., Mosin D.A. *Ballisticheskoe proektirovanie sistem kosmicheskih apparatov* [Ballistic design of spacecraft systems]. SPb.: VKA imeni A.F.Mozhajskogo. 2007. 86 p. (In Russ.).

4 Lomako G.I. *Jeksperimental'naja ballistika kosmicheskih apparatov* [Experimental ballistics spacecraft]. SPb.: VIKA imeni A.F.Mozhajskogo, 1997. 454 p. (In Russ.).

5 Barinov K.N., Mamon P.A. *Teorija poleta kosmicheskih apparatov* [Theory of flight spacecraft]. M.: MO SSSR. 1974. 346 p. (In Russ.).

6 Agadzhanov P.A., Dulevich V.E., Korostylev A.A. *Kosmicheskie traektornye izmerenija. Radiotehnicheskie metody izmerenij i matematicheskaja obrabotka dannyh* [Space trajectory measurement. Electronic measurement techniques and mathematical processing of data]. M.: Sovetskoe radio. 1969. 504 p. (In Russ.).

Коваленко Алексей Юрьевич — к-т техн. наук, старший преподаватель кафедры навигационно-баллистического обеспечения применения космических средств и теории полета летательных аппаратов, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: экспериментальная баллистика, теория полета космических аппаратов, математическое моделирование. Число научных публикаций — 25. al_nex_239@mail.ru; ул. Ждановская 13, Санкт-Петербург, 197198; р.т.: +7(812)23719-60.

Kovalenko Aleksey Yuryevich — Ph.D., senior lecturer of navigation and ballistic support of the use of space assets and the theory of the flight of aircraft department, Mozhaisky Military Space Academy. Research interests: experimental ballistics, theory of flight spacecraft, mathematical modeling. The number of publications — 25. al_nex_239@mail.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

РЕФЕРАТ

Коваленко А.Ю. **Баллистическое проектирование разнородной системы КА с заданным циклом замыкания трассы.**

В данной статье рассматривается вопрос проектирования орбит КА, входящих в состав разнородной системы, с единым циклом замыкания трассы.

Формирование системы устойчивого баллистического построения осуществляется с использованием квазисинхронных орбит, которые обеспечивают стабильное положение орбиты относительно земной поверхности. В такой системе КА находятся на разных орбитах, но имеют единый или близкий по величине цикл замыкания трассы, который выбирается исходя из решаемых целевых задач, возможностей выведения КА и маневренных возможностей КА.

Предложен подход к формированию квазисинхронных орбит. Необходимым условием формирования структуры разнородной системы КА является наличие проектной базовой квазисинхронной орбиты. Цикл замыкания трассы данной орбиты принимается в качестве циклов замыкания трассы для всех КА разнородной системы.

Задача формирования орбит с заданным циклом замыкания трассы разделена на две подзадачи, а именно формирование квазисинхронных орбит на множестве орбит КА, входящих в состав разнородной системы, относительно проектной базовой квазисинхронной орбиты, и уточнение параметров движения КА с целью обеспечения требуемого цикла замыкания трассы в заданных условиях движения.

Проведено численное моделирование, подтверждающее существование квазисинхронных орбит разной высоты с единым по времени циклом замыкания трассы, а также уточнение параметров движения КА в условиях движения отличных от расчетных.

SUMMARY

Kovalenko A. **Ballistic Design of Heterogeneous Systems of the Spacecraft with a Given Cycle of Track Circuit.**

This article discusses the design of spacecraft orbits that are part of a heterogeneous system with a single cycle of track circuit.

Formation of sustainable construction of ballistic is carried out using quasi-synchronous orbits, which provide a stable position relative to the Earth's orbit. In this system, the spacecraft are in different orbits, but have the same or close to the value of the cycle of track circuit, which is selected from the solved targets, opportunities of spacecraft injection and maneuver capabilities of spacecraft.

The paper suggests an approach to the formation of quasi-synchronous orbits. A necessary condition for the formation of a heterogeneous structure of the spacecraft is the presence of a base design quasi-synchronous orbit. Cycle of track circuit of this orbit is taken as the track circuit cycles for all spacecraft heterogeneous systems.

The task of forming the orbit with a given cycle of track circuit is divided into two sub-tasks, namely the formation of quasi-synchronous orbits on the set of orbits of the satellites belonging to the hybrid system with respect to the project base quasi-synchronous orbit, and refinement of the parameters of motion of spacecraft in order to provide the desire cycle of track circuit in the given operating conditions
A numerical simulation is conducted, confirming the existence of quasi-synchronous orbits of different heights with a single time-cycle of track circuit, along with the specification of the parameters of spacecraft motion in operating conditions different from the calculated ones.

УДК 159.953:004.8:007.3

Д.Н. Бирюков

КОГНИТИВНО-ФУНКЦИОНАЛЬНАЯ СПЕЦИФИКАЦИЯ ПАМЯТИ ДЛЯ МОДЕЛИРОВАНИЯ ЦЕЛЕНАПРАВЛЕННОГО ПОВЕДЕНИЯ КИБЕРСИСТЕМ

Бирюков Д.Н. **Когнитивно-функциональная спецификация памяти для моделирования целенаправленного поведения киберсистем.**
Аннотация. Отмечается роль памяти в моделировании упреждающего поведения. Приводятся наиболее изученные возможности памяти человека и особенности протекания когнитивных и рефлекторных процессов в ней. Формулируются требования к памяти киберсистемы, способной в ходе антиципации синтезировать сценарии упреждающего поведения в конфликте.
Ключевые слова: антиципация, киберсистема, моделирование, память человека, упреждающее поведение.

Biryukov D.N. **The Cognitive and Functional Specification of Memory for Modeling of Purposeful Behavior of Cybersystems.**
Abstract. The memory role in modeling of anticipatory behavior is noted. The article depicts the most studied human memory capabilities and features of the occurrence of cognitive and reflexive processes in it. Requirements to memory of the cybersystem capable of synthesizing scenarios of anticipatory behavior in the conflict during an anticipation are formulated.
Keywords: anticipation, cybersystem, modelling, human memory, anticipatory behavior.

1. Введение. На начальном этапе проектирования киберсистем предотвращения компьютерных атак, наделенных способностью антиципации, видится необходимым проанализировать наиболее изученные возможности памяти человека и функции работы с ней. Это связано с тем, что именно человек способен синтезировать сценарии упреждающего поведения на разных уровнях, используя для этого различные механизмы, основанные на возможностях его нервной системы в общем и головного мозга в частности. Возможно, что реализация подобных механизмов в киберсистеме сможет способствовать порождению ею моделей поведения, направленного на предотвращение возможных негативных последствий.

Основным элементом системы раннего обнаружения возможного нападения и его превентивного пресечения является модуль синтеза сценариев упреждающего поведения в информационно-техническом конфликте – Гиромат. А сама система представляет собой частично упорядоченную иерархию гироматов с поуровневой координацией, что должно позволить решить вопрос непротиворечивости в условиях модельной полноты теории, положенной в основу проектируемой системы. Каждый отдельно взятый гиромат должен состоять из четырех основных элементов: Интерпретатора, Планировщика, Генератора и

Памяти. Память является одним из важнейших элементов, так как через нее осуществляется глобальное и локальное взаимодействие первых трех (базовых) элементов (см. рисунок 1). Ввиду этого можно предположить, что чем большей функциональностью, направленной на порождение стратегий упреждающего поведения в конфликте, будет обладать Память, тем более результативной может быть деятельность всей системы.

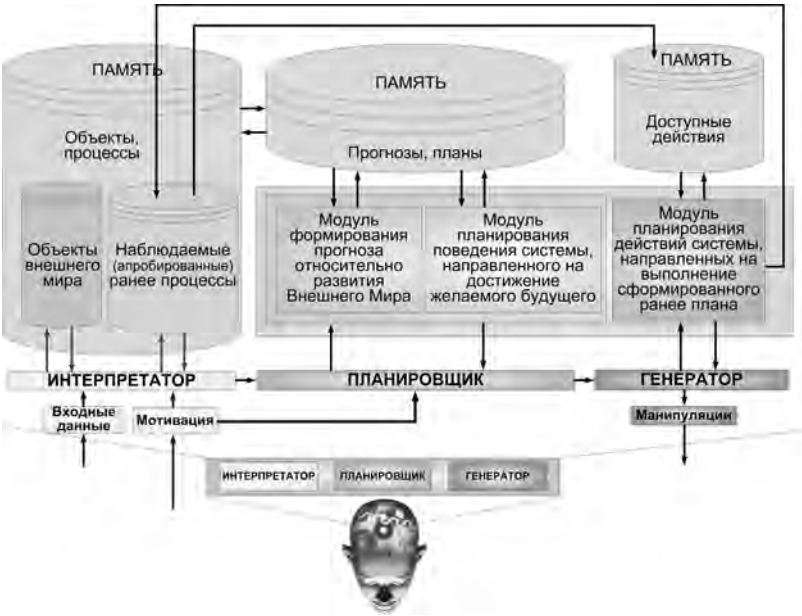


Рис.1. Проект организации памяти киберсистемы

2. Память – основа интеллекта киберсистемы. По результатам анализа ряда работ [1–7], можно сделать вывод о том, что память человека можно разделить на долговременную (ДП) и рабочую (кратковременную) память (РП), хотя кратковременную и рабочую память чаще всего разделяют. Так термин *кратковременная память* (КП) используют для характеристики исполнения заданий, требующих удержания в памяти небольшого объема информации. А термин *рабочая память* используют [8, 9] для обозначения системы, которая не только временно хранит информацию, но и использует ее, позволяя выполнять такие сложные действия, как логическое мышление, научение и понимание (на самом деле, специалисты выделяют еще *сенсорную па-*

мять [10], которую рассматривают как границу раздела восприятия и памяти).

В рамках ДП, следует обратить внимание на отличия недекларативной (имплицитной) и декларативной (эксплицитной) долговременной памяти [1].

Недекларативная память относится к ситуациям, в которых проявляются формы научения, претворяющиеся скорее в действия, нежели в явные воспоминания (пример: езда человека на велосипеде). Ярким примером задействования недекларативной памяти являются примеры формирования условных рефлексов [4, 5]. Можно утверждать, что человек в состоянии контролировать достаточно сложные системы без очевидного сознательного обращения к правилам, лежащим в их основе. Если же говорить об эксплицитном научении, то нельзя отвергать тот факт, что на его результаты влияет глубина осознания наблюдаемых явлений и процессов.

Декларативная память – это память о событиях, фактах, объектах и т.п. Для воспроизведения информации об окружающем мире, хранящейся в декларативной памяти, и о прошлом опыте необходимо участие сознания.

В 1972 году Эндел Тульвиг выделил [2] в рамках декларативной памяти семантическую (СП) и эпизодическую память (ЭП):

– СП – это система, хранящая знания о мире; она выходит за пределы простого знания смысла слов и охватывает сенсорные признаки; она также может включать общие знания о протекании наблюдаемых процессов, функционировании определенных объектов и т.п.;

– ЭП содержит информацию, на основании которой можно вспомнить отдельно взятые явления (события), «заново пережить» их и, при необходимости, использовать эту информацию для планирования дальнейших действий.

В настоящее время достаточно широкое развитие приобретает сенсорно-функциональная теория организации СП [11–13], согласно которой выдвигается предположение о том, что в СП информация об объектах организована на основе различий между сенсорными или зрительными свойствами и функциональными свойствами. В то же время, согласно подходу, учитывающему многие свойства памяти [14], мозг организован так, что память о любом свойстве (например, о цвете, о движении) хранится в его отдельном участке [15]. Данный подход весьма перспективен, так как он основан на признании того, что большинству понятий присущи ряд свойств, и что эти свойства определяют сходства и различия между категориями.

Знания в семантической памяти представлены в виде *схем* [16]. Схемы включают то, что часто называют *сценариями* и *каркасами*. Сценарии имеют дело со знаниями о событиях и о последовательности событий [17, 18]. Каркасы – это структуры знаний, имеющие отношение к какому-то аспекту (объекту) мира и содержащие зафиксированную структурированную информацию. Схематические знания весьма полезны ввиду того, что они позволяют *формировать ожидания*.

Доказано [19], что чем глубже обработка информации при ее поступлении, тем лучше она сохраняется в памяти [20] и тем лучше ее последующее воспроизведение. Обработка информации может заключаться в многократном повторении материала или в его связывании с материалом, имеющемся в памяти [20].

В 1969 году была предложена системная модель СП [21], сводящаяся к тому, что СП представляет собой серию иерархических сетей. Из предложенных моделей [21] также вытекает, что человек часто успешно использует СП, *прибегая к умозаключениям*. При этом время принятия решения относительно более типичных, или представительных членов категории, меньше, чем для сравнительно нетипичных членов [22, 23].

В 1975 году была предложена [24], а далее подтверждена [25, 26] модель распространяющейся активации, согласно которой, в момент, когда человек воспринимает какое-то понятие или думает о нем, в семантической памяти активируется соответствующая точка. Затем эта активация с наибольшим эффектом распространяется на другие понятия, тесно связанные с ним, и менее заметно – на понятия, семантически удаленные от него.

Д. Хебб предположил [27], что долговременное научение основано на нейронных сетях, возникающих и изменяющих свои параметры при одновременном возбуждении двух или более нервных клеток. Уже доказано [28–30], что различная интеллектуальная деятельность (научение) приводит к различным физическим изменениям в структуре мозга, а как следствие к различной результативности при решении одних и тех же задач.

Извлечение же информации из памяти (в общем виде) – это продвижение от одного или нескольких стимулов к целевым воспоминаниям (в результате распространения активации) с целью сделать эти целевые воспоминания доступными и способными влиять на последующее распознавание. Уровень активации – величина переменная, определяющая доступность следа в памяти и возрастающая, когда воспринимается нечто ассоциирующееся с ним (или при непосредственном обращении к нему).

Подтверждено предположение о том, что практика воспроизведения и дополнительное изучение в одинаковой мере улучшают запоминание «практикуемых» объектов, но только практика воспроизведения ухудшает запоминание «непрактикуемых» конкурентов [31, 32]. Связь же между забыванием и временем описывается скорее логарифмической функцией, нежели линейной [33].

Важным элементом при работе человека с памятью является его возможность подавлять воспоминания [34]. Подтверждено [35], что в основе остановки нежелательных моторных действий и подавления воспоминаний лежит один и тот же процесс торможения. В зависимости от того, хочет ли человек вспомнить о чем-то в ответ на предъявление стимула, он способен проконтролировать активацию гиппокампа, оказывая тем самым влияние на последующее воспроизведение [35].

В составе РП выделяют: центральный процессор (далее – «центральный процессор памяти» – ЦПП), фокус внимания (ФВ) и эпизодический буфер (ЭБ). Основная функция ЦПП – концентрация внимания. ЦПП обеспечивает способность человека направлять внимание на то, чем он в данный момент занимается. Контроль внимания может осуществляться автоматически – на основе существующих привычек, а может зависеть от исполнителя, внимание которого ограничено [36]. Когда автоматическое разрешение конфликтной ситуации невозможно (или при возникновении новой ситуации), в действие вступает контролирующая система внимания, которая может вмешаться и принять решение в пользу одного из конкурирующих вариантов или активизировать стратегии поиска альтернативных решений.

Эпизодический Буфер представляет собой систему хранения, в которой может содержаться около четырех [37, 38] (семи [39]) порций многомерной информации. Благодаря этой своей способности ЭБ может играть роль связующего звена между разными подсистемами рабочей памяти, а также связывать их с вводом информации из ДП и от подсистем, осуществляющих восприятие данных. Предполагают [37], что информация из ЭБ извлекается с помощью сознательного понимания. Это связывает модель РП с такой влиятельной точкой зрения, как точка зрения на функцию сознания. Так, Б. Баарс [40] полагает, что роль сознательного понимания заключается в объединении разных потоков информации от разных органов чувств и связывании их в воспринимаемые объекты и сцены. Он предположил, что сознание играет роль ментального рабочего пространства, участвующего в выполнении сложных когнитивных действий, т.е. – рабочей памяти, в то же время есть предположения, что сознание только отображает информацию из разных источников.

Понятие *фокуса внимания* в своих работах широко использует Н. Коуэн [38] и считает, что рабочая память зависит от активации, имеющей место в ДП и контролируемой процессом внимания (собственно через ФВ). Активированная память многомерна и в этом плане она похожа на ЭБ А.Баддли [37]; основное отличие заключается в том, что у А. Баддли объекты скачиваются в ЭБ из ДП, а Н. Коуэн полагает, что «они удерживаются в ДП».

На основе данных о принципах функционирования памяти человека, изложенных выше, предлагается сформулировать ряд требований (Т) к памяти киберсистемы.

Т.1. Структурно память должна состоять из:

Т.1.1. Долговременной памяти [1] (базы знаний), состоящей из [2, 4, 5]:

Т.1.1.1. Ассоциативно-семантической (декларативной / эксплицитной) ДП;

Т.1.1.2. Ассоциативно-рефлекторной (недекларативной / имплицитной) ДП;

Т.1.2. Рабочей (оперативной) памяти, состоящей из:

Т.1.2.1. Ограниченной области памяти с оперативным доступом [37,40];

Т.1.2.2. Контроллера, осуществляющего задание направления для перемещения фокуса внимания в памяти [38];

Т.1.2.3. ЦПП [41], определяющего необходимость семантического вмешательства и осуществляющего логическую (интеллектуальную) обработку информации, помещенной в оперативную память;

Т.2. Память должна содержать данные об окружающем мире (СП) [2] в виде схем [16]:

Т.2.1. Об объектах и их свойствах [2, 3]:

Т.2.1.1. Информация о различных свойствах объектов, должна храниться раздельно [11-15] в виде каркасов [16];

Т.2.1.2. Информация о свойствах должна храниться на самом высоком из возможных уровней иерархии представления данных об объектах (принцип когнитивной экономии [21]);

Т.2.2. О протекании процессов в виде сценариев [16–18];

Т.3. Память должна содержать данные о наблюдаемых (пережитых) явлениях и уметь вспоминать конкретные отдельные явления/процессы (эпизодическая память) [2];

Т.4. Процесс накопления данных в памяти должен сопровождаться ее структурными изменениями [28–30];

Т.5. На качество сохранения данных в памяти должно влиять:

Т.5.1. Многократное повторение поступающих в память данных (чем больше количество повторений, тем лучше память) [42, 19, 43];

Т.5.2. Количество связей между поступившими данными и информацией, хранящейся в памяти (чем больше связей, тем лучше память) [19, 20, 43];

Т.5.3. Наличие иерархической структурированности запоминаемых данных [44–47], например, в виде иерархических сетей [21];

Т.6. Концепты, представленные в памяти, при одновременном их «возбуждении» должны объединяться ассоциативной связью, чем больше подобных возбуждений, тем “крепче” должна становиться эта связь [27];

Т.7. Доступность конкретных данных в памяти должна зависеть от уровня их активации:

Т.7.1. Уровень активации должен быть величиной переменной;

Т.7.2. Чем выше уровень активации данных, тем выше должна быть их доступность (если уровень активации достаточно высок – выше определенного значения, то данные должны быть извлечены из памяти, в противном случае – нет);

Т.7.3. «Яркость» концепта в памяти должна возрастать при активации какого-либо ассоциированного с ним концепта или при непосредственной его активации;

Т.8. Извлечение информации из памяти должно осуществляться за счет продвижения от стимулированных концептов к целевым:

Т.8.1. При обращении к данным, хранящимся в памяти (при занесении данных), от них должно происходить распространение активации:

Т.8.1.1. Активация должна в наибольшей степени распространятся в сторону понятий, с которыми данные в наибольшей степени ассоциируются, и в наименьшей – в сторону отдаленных понятий [48–50];

Т.8.1.2. Чем «крепче» связь между стимулируемым и стимулирующим концептами, тем больший уровень активации должен получать стимулируемый концепт;

Т.8.2. Организация памяти должна позволять осуществлять извлечение информации из памяти на основе накопленного опыта, логики и целей, стоящих перед системой («вычислять» нужную информацию);

Т.8.3. Должен быть реализован механизм, позволяющий подавлять «нежелательное» извлечение данных из памяти [34, 35];

Т.8.4. Извлеченные целевые/промежуточные концепты должны быть способны оказывать влияние на результаты последующего извлечения информации;

Т.9. На качество построения «правдоподобных» выводов (в ходе умозаключений) на основании информации, хранящейся в памяти, должно влиять:

Т.9.1. «Расстояние» между концептами, представляющими объект и его свойство (чем больше «расстояние», тем больше время принятия решения о наличии/отсутствии свойства у объекта) [21];

Т.9.2. Степень известности ассоциативной связи между концептами (чем выше величина ассоциативной связи, тем быстрее находится ассоциация) [22, 23];

Т.10. Связь между забыванием данных, представленных в памяти, и временем должна описываться логарифмической функцией [33];

Т.11. Многократное воспроизведение определенных концептов (а также попытки воспроизведения [51]) должно ухудшать воспроизведение конкурирующих концептов [52];

Т.12. В рамках ассоциативно-рефлекторной памяти должна быть реализована возможность выработки условных рефлексов с учетом того, что [4,5]:

Т.12.1. Многократное заблаговременное предъявление условного стимула без подкрепления безусловным стимулом должно приводить к затруднению выработки условного рефлекса;

Т.12.2. Предъявление условного стимула без подкрепления его безусловным (после выработки условного рефлекса), должно приводить к постепенному угасанию условного рефлекса.

3. Уровни синтеза сценариев поведения интеллектуальной системы. Рассмотрев типовые сценарии поведения в конфликте [53–55], можно утверждать, что деление памяти на уровни можно осуществлять и по основанию, связанному с глубиной обработки данных, поступающих на вход интеллектуальной системы. В этом случае можно говорить о двух основных уровнях поведения: о рефлекторном и интеллектуальном (в рамках которого производится семантическая обработка информации). Оба эти уровня предполагают непосредственное применение памяти в процессе синтеза сценариев поведения киберсистемы.

Далее предлагается недекларативную память называть ассоциативно-рефлекторной памятью (АРП), а декларативную память – ассоциативно-семантической памятью (АСП). Естественно предположить, что и АРП, и АСП могут в той или иной мере способствовать построению сценариев упреждающего поведения.

Обобщенные схемы рефлекторного поведения представлены на рисунке 2, где «*В*» – модуль восприятия, а «*Р*» – модуль реакции.

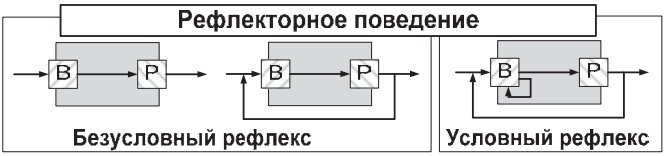


Рис. 2. Основные схемы рефлекторного поведения

Основным отличием схемы интеллектуального поведения от схем рефлекторного поведения является наличие в ней модуля прогнозирования – «*П*», функционирование которого основано на обработке семантической информации (см. рисунок 3).

Рис.3. Обобщенная схема интеллектуального поведения

Детализация схемы интеллектуального поведения приведена на рисунке 4, на котором используются следующие обозначения:

$В_Ф$ – «Физическое» восприятие через систему сенсоров (Внешнее),

$В_{МС}$ – Восприятие модели поведения Системы (Внутреннее),

$В_{МВМ}$ – Восприятие модели развития «Внешнего Мира» (Внутреннее),

$В_\Sigma$ – Оценивание («Восприятие Восприятия»),

$П_С$ – Прогнозирование поведения Системы,

$П_{ВМ}$ – Прогнозирование поведения “Внешнего Мира”.

Пояснение операций, входящих в типовые сценарии поведения в конфликтах, основанные на интеллектуальном поведении (см. рисунок 4), приведены ниже:

01. Рефлекторная реакция на раздражитель;

02. Восприятие системой самой себя через систему сенсоров;

1. «Физическое» («Внешнее») восприятие через систему сенсоров, построение первичной модели наблюдаемого явления;

2. Оценивание модели, построенной по результатам «Физического» («Внешнего») восприятия;

3. Построение моделей, описывающих потенциальное развитие наблюдаемых явлений (Прогноз дальнейших «физических» восприятий Внешнего Мира);

4. Определение наличия задачи (идентификация задачи);

5. Оценивание степени критичности задачи;

6. Построение моделей потенциально реализуемого поведения, направленного на решение идентифицированной задачи;

7. Определение наличия решения идентифицированной задачи;

8. Оценивание пригодности (оптимальности) решения;

9. Определение порядка реагирования для решения задачи.

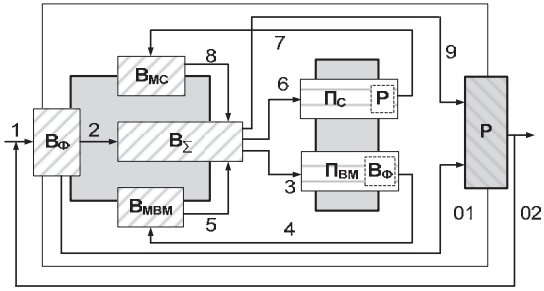


Рис. 4. Детализация схемы интеллектуального поведения

К безусловным рефлексам, способствующим упреждению в конфликте, следует отнести механизмы, напрямую заложенные в систему при ее создании. Такие механизмы должны быть способными однозначно реагировать на явления, наблюдаемые в киберпространстве. Очевидно, что перечень таких механизмов будет конечен и неизменен для каждой конкретной реализации киберсистемы.

Если рассматривать механизмы поведения, реализуемые на уровне условных рефлексов, то следует отметить тот факт, что на данном уровне система должна быть способной вырабатывать все новые и новые механизмы собственного поведения. Однако, для того, чтобы был порожден новый механизм поведения, система должна пройти этап обучения (формирования условного рефлекса). Этап обучения может занять длительный промежуток времени, в ходе которого система, порождающая спецификации наблюдаемых процессов, а также спецификации процессов собственного поведения, может пропустить атакующие воздействия от противоборствующей стороны.

К системам, способным формировать механизмы собственного поведения на уровне условных рефлексов, можно отнести системы обнаружения вторжений, функционирующие на основе нейронных

сетей и предназначенные для распознавания аномалий в сетевом трафике, передаваемом в защищаемом сегменте. Одной из «слабых» сторон подобных систем является то, что они чаще всего не в состоянии пояснить оператору порядок формирования принятого решения, а так же аргументировать его.

При рассмотрении условных рефлексов через призму моделирования сценариев упреждающего поведения следует отметить, что в основе условных рефлексов лежит способность установления ассоциативных связей. Как видится, данная способность весьма важна и должна быть реализована в интеллектуальной системе синтеза сценариев упреждающего поведения в конфликте. Наличие ассоциативных связей должно позволить системе накапливать опыт и учитывать контексты, а способность учитывать контексты – один из шагов в направлении создания поистине интеллектуальных систем.

Наибольший интерес представляет уровень, на котором система способна порождать сценарии упреждающего поведения с учетом семантики наблюдаемых явлений, процессов и взаимодействующих (противоборствующих) объектов.

4. Модель памяти для формирования сценариев упреждения. Для воплощения рассмотренных выше функций памяти в разрабатываемой интеллектуальной системе не обойтись без языковых средств описания, представления и манипулирования знаниями о предметной области конфликта. В связи с этим, предлагается построить абстрактную систему знаний в виде структурированной модели взаимодополняющих формальных семантик: денотационной семантики структур, аксиоматической семантики свойств и операционной семантики действий.

Все знания, которыми будет манипулировать система в ходе своего функционирования, необходимо каким-то образом представить в ее памяти (в Базе Знаний системы). Для этого предлагается использовать формализмы, подобные семантическим сетям или фреймам, как видится, их применение должно позволить описывать произвольные предметные области с необходимой степенью детализации.

Для формализации *денотационной семантики* при конструировании сколь угодно сложных онтологических построений предлагается использовать теорию типов данных и функциональных пространств Д. Скотта, основанную на использовании частично упорядоченных свойством аппроксимации множеств.

Для формализации *аксиоматической семантики* представления знаний, их логической интерпретации и порождения однозначных следствий из них, видится возможным использовать семейство машин логиче-

ского вывода, функционирующих на основе дескрипционных логик, дополненных непротиворечивыми аксиомами концептологии предметной области конфликта.

В ходе формализации *операционной семантики* сценариев поведения при выборе концептов атомарных действий видится целесообразным использовать систему весовых коэффициентов для указания того, в каких контекстах и как часто применялись те или иные концепты (аналог синаптических связей между нейронами коры головного мозга). При этом динамику изменения значений предложенных коэффициентов предлагается моделировать аппаратом ассоциативной ресурсной сети [56].

Для построения и представления моделей сценариев поведения самой системы, предлагается использовать функциональную парадигму, предложенную Дж. Бэкусом [57] и позволяющую формировать из базовых функций (действий, процедур, программ и т.п.) и функциональных форм (которые в свою очередь задаются исходя из семантики предметной области) более сложные функциональные конструкции. На вход процедуры, формирующей более сложные функции, предлагается подавать данные, извлеченные из онтологии с учетом значений предложенных коэффициентов.

Учитывая вышесказанное, общую модель формирования сценариев упреждающего поведения можно представить следующим образом: см. рисунок 5.

В центральной части рисунка 5 выделены элементы, участвующие в порождении сценариев поведения системы на рефлекторном уровне. Верхняя и нижняя часть рисунка отражает специфику синтеза сценариев на семантическом уровне.

На вход системы, способной осуществлять построение сценариев упреждающего поведения, могут поступать как данные от обучающей системы, так и данные от системы сенсоров (в общем случае «вход» может быть одним). Поступившие данные предлагается помещать в БЗ. В то же время данные (результаты измерений), поступившие на вход системы, должны инициировать срабатывание определенных условных рефлексов, направленных на разрешение идентифицированной, но семантически неосознанной задачи. В этом случае реализация условного рефлекса и есть решение задачи. Если соответствующий условный рефлекс не сформирован, то система должна осуществлять идентификацию задачи и поиск решения на основе знаний, имеющихся у системы.

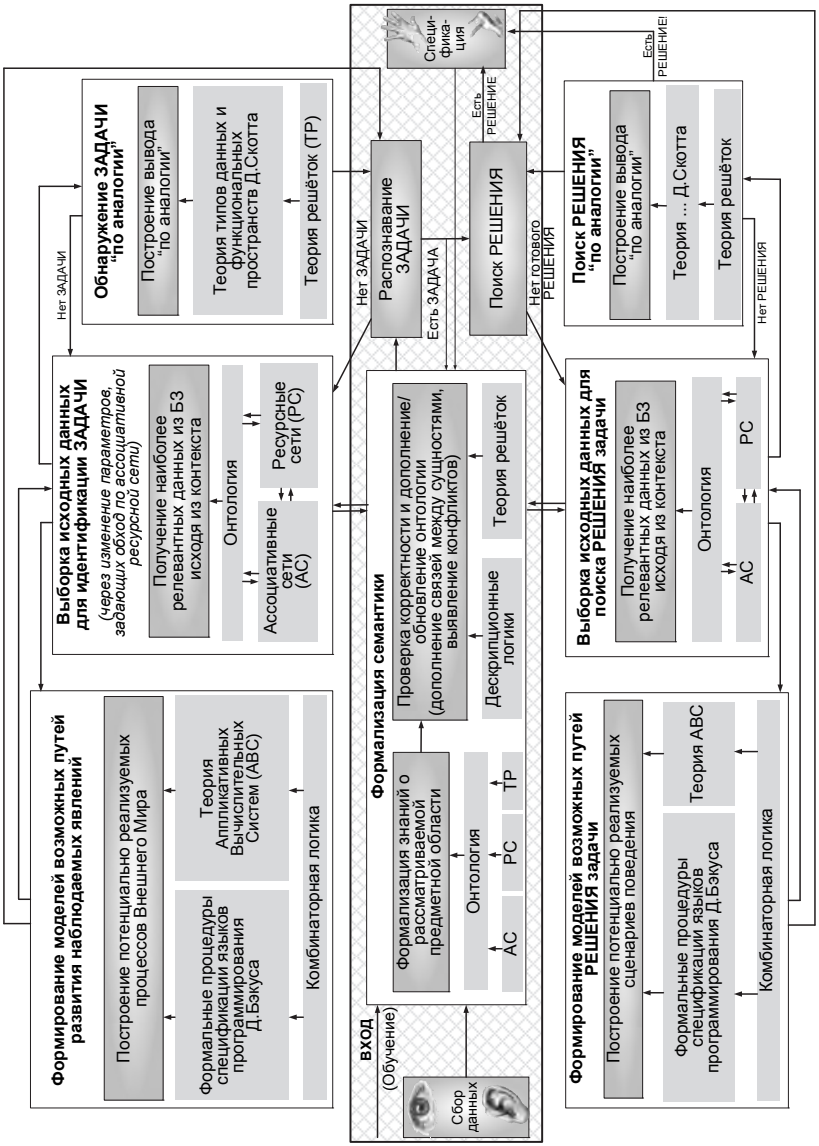


Рис. 5. Модель формирования спецификаций «Задач» и «Решений»

Как идентификацию потенциальных задач, так и поиск способов их решения, система должна осуществлять как минимум двумя спосо-

бами. Первый способ – поиск по аналогии (Д. Пойа, например, писал [58]: «Возможно, не существует открытий ни в элементарной, ни в высшей математике, ни даже, пожалуй, в любой другой области, которые могли бы быть сделаны… без аналогии»). Очевидно, что может сложиться такая ситуация, при которой в системе могут отсутствовать знания, позволяющие осуществить вывод новых знаний по аналогии. В этом случае система должна иметь возможность конструировать новые знания о возможных процессах, путем комбинирования моделями имеющихся допустимых функций (действий) – второй способ.

Независимо от того, какой из перечисленных способов будет использовать система при порождении новых знаний о потенциально возможных задачах и способах их решения, она должна иметь возможность осуществлять навигацию по данным, представленным в ее ассоциативно-семантической памяти. В основу данного механизма предлагается заложить идею направленного распространения ассоциативного сигнала по ассоциативным связям.

Как видится, предложенная модель формирования сценариев упреждения должна быть реализована в Гиромате [59], способном в процессе своего функционирования строить в своей памяти модель окружающей киберсреды и синтезировать программу действий в соответствии с заложенными в него целями, состоящими в поддержании должного уровня защищенности критической информационной инфраструктуры от компьютерных атак, сообразуясь с этой моделью.

3. Заключение. Проведенный анализ результатов большого количества исследований, посвященных изучению памяти человека, позволил выделить основные правила ее построения и функционирования. Выделенные правила были положены в основу когнитивно-функциональной спецификации памяти проектируемой киберсистемы, призванной в ходе антиципации синтезировать сценарии упреждающего поведения в конфликте.

Сделан вывод о том, что способность системы к упреждающему поведению может быть реализована на двух уровнях: на уровне ассоциативно-рефлекторной и ассоциативно семантической памяти. При этом, важное место отводится механизмам:

– выработки системой условных рефлексов;

– иерархического представления данных в памяти системы (об объектах, их свойствах и процессах);

– изменения доступности данных, находящихся в памяти системы (для реализации возможности учета контекстов, а также процедуры «забывания» ложных и устаревших данных);

– направления фокуса внимания (для выделения из памяти необходимых знаний, исходя из решаемых системой задач и поступающих данных);

– осуществления “правдоподобных” умозаключений на основе информации, хранящейся в памяти системы (в том числе, путем осуществления выводов по аналогии).

Реализация в системе указанных механизмов необходима для того, чтобы она была способна к упреждающему поведению в конфликте.

Литература

1. *Squire L.R.* Declarative and nondeclarative memory: Multiple brain systems supporting learning and memory // Journal of Cognitive Neuroscience. 1992. vol. 4. pp. 232–243.
2. *Tulving E.* Episodic and semantic memory // Organization of Memory. New York: Academic Press. 1972. pp. 381–403.
3. *Tulving E.* Episodic memory: From mind to brine // Annual Review of Psychology. 2002. vol. 53. pp. 1–25.
4. *Weiskrantz E., Warrington E.K.* Conditioning in amnesic patients // Neuropsychologia. 1979. vol. 8. pp. 281–288.
5. *Brooks D.N., Baddeley A.D.* What can amnesic patients learn? // Neuropsychologia. 1976. vol. 14. pp. 111–122.
6. *Neath I., Surprenant A.* Human Memory: An Introduction to Research, Data and Theory (2nd ed.) // Belmont. CA: Wadsworth. 2003.
7. *Engle R.W., Kane M.J.* Executive attention, working memory capacity and two-factor theory of cognitive control // The Psychology of Learning and Motivation. New York: Elsevier. 2004. pp. 145–199.
8. *Miller G.A., Galanter E., Pribram K.H.* Plans and the Structure of Behavior // New York: Holt. Rinehart & Winston. 1960.
9. *Baddeley A.D., Hitch G.J.* Working memory // Recent Advances in Learning and Motivation. New York: Academic Press. 1974. vol. 8. pp. 47–89.
10. *Atkinson R.C., Shiffrin R.M.* Human memory: A proposed system and its control processes // The Psychology of Learning and Motivation: Advances in Research and Theory. New York: Academic Press. 1968. vol. 2. pp. 89–195.
11. *Sitnicova T., West W.C., Kuperberg G.R., Holcomb P.J.* The neural organization of semantic memory: Electropsychological activity suggests feature-based segregation // Biological Psychology. 2006. vol. 71. pp. 326–340.
12. *Lee A.C.H., Graham K.S., Simons J.S., Hodges J.R., Owen A.M., Patterson K.* Regional brain activations differ for semantic features but not for categories // NeuroReport. 2002. vol. 13. pp. 1497–1501.
13. *Marques J.F., Canessa N., Siri S., Catricala E., Cappa S.* Conceptual knowledge in the brain: fMRI evidence for a featural organization // Brain Research. 2008. vol. 1194. pp. 90–99.
14. *Cree G.S., McRae K.* Analyzing factors underlying the structure and computation of the meaning of chipmunk, cherry, chisel, cheese, and cello (and many other such concrete nouns) // Journal of Experimental Psychology: General. 2003. vol. 132. no. 2. pp. 163–201.
15. *Martin A., Chao L.L.* Semantic memory and the brain: Structure and Processes // Current Opinion in Neurobiology. 2001. vol. 11. pp. 194–201.

16. *Barlett F.C.* Remembering: A Study in Experimental and Social Psychology // New York: Cambridge University Press. 1932.
17. *Schank R.C., Abelson R.P.* Scripts, Plans, Goals and Understanding // Hillsdale. NJ: Lawrence Erlbaum Associates. 1977.
18. *Bower G.H., Black J.B., Turner T.J.* Scripts in memory for test // Cognitive Psychology. 1979. vol. 11. pp. 177–220.
19. *Craik F.I.M., Tulving E.* Depth of processing and the retention of words in episodic memory // Journal of Experimental Psychology: General. 1975. vol. 104(3). pp. 268–294.
20. *Craik F.I.M., Lochart R.S.* Levels of processing. A framework for memory research // Journal of Verbal Learning and Verbal Behavior. 1972. vol. 11(6). pp. 671–684.
21. *Collins A.M., Quillian M.R.* Retrieval time from semantic memory // Journal of Verbal Learning and Verbal Behavior. 1969. vol. 8. pp. 240–247.
22. *Rosh E., Mervis C.B.* Family resemblances: Studies in the internal structure of categories // Cognitive Psychology. 1975. vol. 7. pp. 573–605.
23. *Rosh E.* Natural categories // Cognitive Psychology. 1973. vol. 4. pp. 328–350.
24. *Collins A.M., Loftus E.* A spreading activation theory of semantic memory // Psychological Review. 1975. vol. 82. pp. 407–428.
25. *Meyer D.E., Schaneveldt R.W.* Meaning, memory structure, and mental processes // Science. 1976. vol. 192. pp. 27–33.
26. *McNamara T.P.* Priming and constraints it places on theories of memory and retrieval // Psychological Review. 1992. vol. 99. pp. 650–662.
27. *Hebb D.O.* The Organization of Behavior // New York: Wiley. 1949.
28. *DeZeeuw C.I.* Plasticity: A pragmatic compromise // Science of Memory: Concepts. New York: Oxford University Press. 2007. pp. 83–86.
29. *Hartley T., Maguire E.A., Spiers H.J., Bugress N.* The well-worn route and the path less traveled: Distinct neural bases of route following and wayfinding in humans // Neuron. 2003. vol. 37. pp. 877–888.
30. *Maguire E.A., Woollett K., Spiers H.J.* London taxi drivers and bus drivers: A structural MRI and neuropsychological analysis // Hippocampus. 2006. vol. 16. pp. 1091–1101.
31. *Anderson M.C.* Rethinking interference theory: Executive control and the mechanisms of forgetting // Journal of Memory and Language. 2003. vol. 49(4). pp. 415–445.
32. *Strom B.C., Bjork E.L., Bjork R.A., Nestojko J.F.* Is retrieval success a necessary condition for retrieval-induced forgetting? // Psychonomic Bulletin and Review. 2006. vol. 13. pp. 1023–1027.
33. *Ebbinghaus H.* Memory: A Contribution to Experimental Psychology // New York: Teachers College. Columbia University. 1913.
34. *Levy B.J., Anderson M.C.* Individual differences in the suppression of unwanted memories: The executive deficit hypothesis // Acta Psycbologica. 2008. vol. 127. pp. 623–635.
35. *Anderson M.C., Ochsner K.N., Cooper J., Robertson E, Gabrieli S.W., Glover G.H.* Neural systems underlying the suppression of unwanted memories // Science. 2004. vol. 303. pp. 232–235.
36. *Norman D.A., Shallice T.* Attention to action: Willed and automatic control of behavior // Consciousness and Self-regulation. Advances in Research and Theory. New York: Plenum Press. 1986. vol. 4. pp. 1–18.
37. *Baddeley A.D.* The episodic buffer: A new component of working memory? // Trends in Cognitive Sciences. 2000. vol. 4(11). pp. 417–423.
38. *Cowan N.* Working Memory Capacity // Hove. UK: Psychology Press. 2005.
39. *Miller G.A.* The magical number seven, plus or minus two: Some limits on our capacity for processing information // Psychological Review. 1956. vol. 63. pp. 81–97.

40. *Baars B.J.* The conscious access hypothesis: Origins and recent avidence // Trends in Cognitive Science. 2002. vol. 6(1). pp. 47–52.
41. *Norman D.A., Shallice T.* Attention to action: Willed and automatic control of behavior // Consciousness and Self-regulation. Advances in Research and Theory. New York: Plenum Press. 1986. vol. 4. pp. 1–18.
42. *Craik F.I.M., Lochart R.S.* Levels of processing. A framework for memory research // Journal of Verbal Learning and Verbal Behavior. 1972. vol. 11. pp. 671–684.
43. *Glenberg A.M., Smith S.M., Green. C.* Type I rehearsal: Maintenance and more // Journal of Verbal Learning and Verbal Behavior. 1977. vol. 16. pp. 339–352.
44. *Tulving E.* Subjective organization in free recall of «unrelated» words // Psychological Review. 1962. vol. 69. pp. 344–354.
45. *Bower G.H., Clark M.C.* Narrative stories as mediators for serial learning // Psychonomic Science. 1969. vol. 14. pp. 181–182.
46. *Bower G.H., Clark M.C., Lesgold A.M., Winzen D.* Hierarchical retrieval schemes in recall of categorized word list // Journal of Verbal learning and Verbal Behavior. 1969. vol. 8. pp. 323–343.
47. *Broadbent D.E., Cooper P.J, Broadbent M.H.* A comparison of hierarchical retrieval schemes in recall // Journal of Psychology: Human Learning and Memory. 1978. vol. 4. pp. 486–497.
48. *Collins A.M., Loftus E.* A spreading activation theory of semantic memory // Psychological Review. 1975. vol. 82. pp. 407–428.
49. *Meyer D.E., Schaneveldt R.W.* Meaning, memory structure, and mental processes // Science. 1976. vol. 192. pp. 27–33.
50. *McNamara T.P.* Priming and constraints it places on theories of memory and retrieval // Psychological Review. 1992. vol. 99. pp. 650–662.
51. *Strom B.C., Bjork E.L., Bjork R.A., Nestojko J.F.* Is retrieval success a necessary condition for retrieval-induced forgetting? // Psychonomic Bulletin and Review. 2006. vol. 13. pp. 1023–1027.
52. *Anderson M.C.* Rethinking interference theory: Executive control and the mechanisms of forgetting // Journal of Memory and Language. 2003. vol. 49(4). pp. 415–445.
53. *Бирюков Д.Н., Ломако А.Г.* Построение систем информационной безопасности: от живых организмов к киберсистемам // Защита информации. INSIDE. 2013. №2. С. 2–6.
54. *Бирюков Д.Н., Ломако А.Г.* Подход к построению системы предотвращения киберугроз // Проблемы информационной безопасности. Компьютерные системы. С-Пб.: Издательство Политехнического университета. 2013. №2. С. 13–19.
55. *Бирюков Д.Н.* Анализ способностей живых организмов при проектировании систем кибербезопасности // Методы обеспечения информационной кибербезопасности. Труды ИСА РАН. М.: КомКнига. 2013. Т.27 (доп. выпуск). С. 431–446.
56. *Жилякова Л.Ю.* Процессы изменения проводимостей в ассоциативной ресурсной сети // X международная конференция имени Т.А. Таран Интеллектуальный анализ информации ИАИ-2010. Киев: Просвіта. 2010. С. 85–91.
57. *Бэкус Дж.* Можно ли освободить программирование от стиля фон Неймана? Функциональный стиль и соответствующая алгебра программ // М.: Мир. 1993.С. 84–158.
58. *Пойа Д.* Математика и правдоподобные рассуждения. М.: Наука. 1975. 462 с.
59. *Поспелов Д.А.* Мышление и автоматы // М.: Советское радио. 1972. 224 с.

References

1. Squire L.R. Declarative and nondeclarative memory: Multiple brain systems supporting learning and memory. *Journal of Cognitive Neuroscience*. 1992. vol. 4. pp. 232–243.

2. Tulving E. Episodic and semantic memory. *Organization of Memory*. New York: Academic Press. 1972. pp. 381–403.
3. Tulving E. Episodic memory: From mind to brine. *Annual Review of Psychology*. 2002. vol. 53. pp. 1–25.
4. Weiskrantz E., Warrington E.K. Conditioning in amnesic patients. *Neuropsychologia*. 1979. vol. 8. pp. 281–288.
5. Brooks D.N., Baddeley A.D. What can amnesic patients learn? *Neuropsychologia*. 1976. vol. 14. pp. 111–122.
6. Neath I., Surprenant A. Human Memory: An Introduction to Research, Data and Theory (2nd ed.). Belmont. CA: Wadsworth. 2003.
7. Engle R.W., Kane M.J. Executive attention, working memory capacity and two-factor theory of cognitive control. *The Psychology of Learning and Motivation.* New York: Elsevier. 2004. pp. 145–199.
8. Miller G.A., Galanter E., Pribram K.H. Plans and the Structure of Behavior. New York: Holt. Rinehart & Winston. 1960.
9. Baddeley A.D., Hitch G.J. Working memory. *Recent Advances in Learning and Motivation*. New York: Academic Press. 1974. vol. 8. pp. 47–89.
10. Atkinson R.C., Shiffrin R.M. Human memory: A proposed system and its control processes. *The Psychology of Learning and Motivation: Advances in Research and Theory*. New York: Academic Press. 1968. vol. 2. pp. 89–195.
11. Sitnicova T., West W.C., Kuperberg G.R., Holcomb P.J. The neural organization of semantic memory: Electropsychological activity suggests feature-based segregation. *Biological Psychology*. 2006. vol. 71. pp. 326–340.
12. Lee A.C.H., Graham K.S., Simons J.S., Hodges J.R., Owen A.M., Patterson K. Regional brain activations differ for semantic features but not for categories. *NeuroReport*. 2002. vol. 13. pp. 1497–1501.
13. Marques J.F., Canessa N., Siri S., Catricala E., Cappa S. Conceptual knowledge in the brain: fMRI evidence for a featural organization. *Brain Research*. 2008. vol. 1194. pp. 90–99.
14. Cree G.S., McRae K. Analyzing factors underlying the structure and computation of the meaning of chipmunk, cherry, chisel, cheese, and cello (and many other such concrete nouns). *Journal of Experimental Psychology: General*. 2003. vol. 132. no. 2. pp. 163–201.
15. Martin A., Chao L.L. Semantic memory and the brain: Structure and Processes. *Current Opinion in Neurobiology*. 2001. vol. 11. pp. 194–201.
16. Barlett F.C. Remembering: A Study in Experimental and Social Psychology. New York: Cambridge University Press. 1932.
17. Schank R.C., Abelson R.P. Scripts, Plans, Goals and Understanding. Hillsdale. NJ: Lawrence Erlbaum Associates. 1977.
18. Bower G.H., Black J.B., Turner T.J. Scripts in memory for test. *Cognitive Psychology*. 1979. vol. 11. pp. 177–220.
19. Craik F.I.M., Tulving E. Depth of processing and the retention of words in episodic memory. *Journal of Experimental Psychology: General*. 1975. vol. 104(3). pp. 268–294.
20. Craik F.I.M., Lochart R.S. Levels of processing. A framework for memory research. *Journal of Verbal Learning and Verbal Behavior*. 1972. vol. 11(6). pp. 671–684.
21. Collins A.M., Quillian M.R. Retrieval time from semantic memory. *Journal of Verbal Learning and Verbal Behavior*. 1969. vol. 8. pp. 240–247.
22. Rosh E., Mervis C.B. Family resemblances: Studies in the internal structure of categories. *Cognitive Psychology*. 1975. vol. 7. pp. 573–605.
23. Rosh E. Natural categories. *Cognitive Psychology*. 1973. vol. 4. pp. 328–350.

24. Collins A.M., Loftus E. A spreading activation theory of semantic memory. *Psychological Review*. 1975. vol. 82. pp. 407–428.
25. Meyer D.E., Schaneveldt R.W. Meaning, memory structure, and mental processes. *Science*. 1976. vol. 192. pp. 27–33.
26. McNamara T.P. Priming and constraints it places on theories of memory and retrieval. *Psychological Review*. 1992. vol. 99. pp. 650–662.
27. Hebb D.O. The Organization of Behavior. New York: Wiley. 1949.
28. DeZeeuw C.I. Plasticity: A pragmatic compromise. *Science of Memory: Concepts*. New York: Oxford University Press. 2007. pp. 83–86.
29. Hartley T., Maguire E.A., Spiers H.J., Bugress N. The well-worn route and the path less traveled: Distinct neural bases of route following and wayfinding in humans. *Neuron*. 2003. vol. 37. pp. 877–888.
30. Maguire E.A., Woollett K., Spiers H.J. London taxi drivers and bus drivers: A structural MRI and neuropsychological analysis. *Hippocampus*. 2006. vol. 16. pp. 1091–1101.
31. Anderson M.C. Rethinking interference theory: Executive control and the mechanisms of forgetting. *Journal of Memory and Language*. 2003. vol. 49(4). pp. 415–445.
32. Strom B.C., Bjork E.L., Bjork R.A., Nestojko J.F. Is retrieval success a necessary condition for retrieval-induced forgetting? *Psychonomic Bulletin and Review*. 2006. vol. 13. pp. 1023–1027.
33. Ebbinghaus H. Memory: A Contribution to Experimental Psychology. New York: Teachers College. Columbia University. 1913.
34. Levy B.J., Anderson M.C. Individual differences in the suppression of unwanted memories: The executive deficit hypothesis. *Acta Psycbologica*. 2008. vol. 127. pp. 623–635.
35. Anderson M.C., Ochsner K.N., Cooper J., Robertson E, Gabrieli S.W., Glover G.H. Neural systems underlying the suppression of unwanted memories. *Science*. 2004. vol. 303. pp. 232–235.
36. Norman D.A., Shallice T. Attention to action: Willed and automatic control of behavior. *Consciousness and Self-regulation. Advances in Research and Theory*. New York: Plenum Press. 1986. vol. 4. pp. 1–18.
37. Baddeley A.D. The episodic buffer: A new component of working memory? *Trends in Cognitive Sciences*. 2000. vol. 4(11). pp. 417–423.
38. Cowan N. Working Memory Capacity. Hove. UK: Psychology Press. 2005.
39. Miller G.A. The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*. 1956. vol. 63. pp. 81–97.
40. Baars B.J. The conscious access hypothesis: Origins and recent avidence. *Trends in Cognitive Science*. 2002. vol. 6(1). pp. 47–52.
41. Norman D.A., Shallice T. Attention to action: Willed and automatic control of behavior. *Consciousness and Self-regulation. Advances in Research and Theory*. New York: Plenum Press. 1986. vol. 4. pp. 1–18.
42. Craik F.I.M., Lochart R.S. Levels of processing. A framework for memory research. *Journal of Verbal Learning and Verbal Behavior*. 1972. vol. 11. pp. 671–684.
43. Glenberg A.M., Smith S.M., Green. C. Type I rehearsal: Maintenance and more. *Journal of Verbal Learning and Verbal Behavior*. 1977. vol. 16. pp. 339–352.
44. Tulving E. Subjective organization in free recall of «unrelated» words. *Psychological Review*. 1962. vol. 69. pp. 344–354.
45. Bower G.H., Clark M.C. Narrative stories as mediators for serial learning. *Psychonomic Science*. 1969. vol. 14. pp. 181–182.
46. Bower G.H., Clark M.C., Lesgold A.M., Winzen D. Hierarchical retrieval schemes in recall of categorized word list. *Journal of Verbal learning and Verbal Behavior*. 1969. vol. 8. pp. 323–343.

47. Broadbent D.E., Cooper P.J, Broadbent M.H. A comparison of hierarchical retrieval schemes in recall. *Journal of Psychology: Human Learning and Memory*. 1978. vol. 4. pp. 486–497.
48. Collins A.M., Loftus E. A spreading activation theory of semantic memory. *Psychological Review*. 1975. vol. 82. pp. 407–428.
49. Meyer D.E., Schaneveldt R.W. Meaning, memory structure, and mental processes. *Science*. 1976. vol. 192. pp. 27–33.
50. McNamara T.P. Priming and constraints it places on theories of memory and retrieval. *Psychological Review*. 1992. vol. 99. pp. 650–662.
51. Strom B.C., Bjork E.L., Bjork R.A., Nestojko J.F. Is retrieval success a necessary condition for retrieval-induced forgetting? *Psychonomic Bulletin and Review*. 2006. vol. 13. pp. 1023–1027.
52. Anderson M.C. Rethinking interference theory: Executive control and the mechanisms of forgetting. *Journal of Memory and Language*. 2003. vol. 49(4). pp. 415–445.
53. Biryukov D.N., Lomako A.G. [Design and construction of information security from living organisms to cybersystems]. *Zashita informatiyi – Data protection. INSIDE*. 2013. vol. 2. pp. 2–6. (In Russ.).
54. Biryukov D.N., Lomako A.G. [Approach to creation of system of cyber-threats preventing]. *Problemy informatsionnoy bezopasnosty. Kompyuternie sistemy – Problems of information security. Computer systems*. SPB: St. Petersburg Polytechnical University. 2013. vol. 2. pp. 13–19. (In Russ.).
55. Biryukov D.N. [Analysis of the ability of living organisms in the design of systems cybersecurity]. *Metody obespeceniya informatsionnoy kiberbezopasnosty. Trudy ISA RAN. – ISA RAS proceedings Methods of providing information cybersecurity.* M.: KomKniga. 2013. vol. 27 (add. issue). pp. 431–446. (In Russ.).
56. Gilyakova L.Y. [Processes of change of provodimost in an associative resource network]. *X megdunarodnaya konferenciya imeni T.A.Taran Intellektualniy analiz informacii IAI-2010* [X international conference of name T.A. Taran Intellectual analysis of information of IAI-2010]. pp. 85–91. (In Ukraine).
57. Backus J. [Whether it is possible to exempt programming from style Neumann's background? Functional style and corresponding algebra of programs]. M.: Nauka. 1993. pp. 84–158. (In Russ).
58. Polya G. *Matematika i pravdopodobnye rassuzhdenija* [Mathematics and plausible reasonings]. M.: Nauka. 1975. 462 p. (In Russ.).
59. Pospelov D.A. *Myshlenie i avtomaty* [Thinking and machines]. M.: Sovetskoe radio. 1972. 224 p. (In Russ.).

Бирюков Денис Николаевич — к-т техн. наук, профессор кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: системный анализ, защита информации, интеллектуальная поддержка принятия решений. Число научных публикаций — 70. Biryukov.D.N@yandex.ru; ул. Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: (812)237-19-60.

Biryukov Denis Nikolaevich — Ph.D., professor of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: system analyses, IT-Security, intelligent decision support. The number of publications — 70. Biryukov.D.N@yandex.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: (812) 237-19-60.

РЕФЕРАТ

Бирюков Д.Н. **Когнитивно-функциональная спецификация памяти для моделирования целенаправленного поведения киберсистем.**

Для того чтобы система была способной к упреждающему поведению в условиях конфликта, она должна обладать свойством антиципации. Свойство антиципации присуще биосистемам и наиболее ярко проявляется в деятельности человека. Для обнаружения механизмов, способствующих появлению свойства антиципации у человека, предложено уделить особое внимание структуре и порядку функционирования его памяти. Выдвинуто предположение о том, что чем большей функциональностью, направленной на порождение стратегий упреждающего поведения в конфликте, будет обладать память, тем более результативной может быть деятельность всей системы предотвращения вторжений.

На начальном этапе был произведен обзор и анализ работ ряда ученых, занимающихся изучением строения и принципов функционирования памяти человека. По результатам проведенного анализа построена когнитивно-функциональная спецификация памяти системы, способной к упреждающему поведению. Сделан вывод о том, что сценарии упреждающего поведения могут формироваться на дух уровнях: на уровне рефлексов и на уровне, предполагающем семантическую обработку знаний. Отмечена важность реализации в проектируемой системе механизмов функционирования памяти, направленных на:

– выработку системой условных рефлексов;

– иерархическое представление данных в памяти системы (об объектах, их свойствах и процессах);

– изменение доступности данных, находящихся в памяти системы (для реализации возможности учета контекстов, а также процедуры “забывания” ложных и устаревших данных);

– направление фокуса внимания (для выделения из памяти необходимых знаний, исходя из решаемых системой задач и поступающих данных);

– осуществление “правдоподобных” умозаключений на основе информации, хранящейся в памяти системы (в том числе, путем осуществления выводов по аналогии).

Как видится, реализация указанных механизмов необходима для того, чтобы проектируемая система была способна к упреждающему поведению в конфликте. Также в статье предложен первичный облик языковых средств описания, представления и манипулирования знаниями о предметной области конфликта.

SUMMARY

Biryukov D.N. **The Cognitive and Functional Specification of Memory for Modeling of Purposeful Behavior of Cybersystems.**

For the system to be capable of anticipatory behavior in the conditions of the conflict, it has to possess property of an anticipation. Property of anticipation is inherent in biosystems and is most brightly shown in activity of the person. For detection of the mechanisms promoting emergence of property of anticipation in the person it is offered to pay special attention to structure and an order of functioning of his memory. It is suggested that the more memory possesses functionality, directed on generation of strategy of anticipatory behavior in the conflict, the more productive the activity of the whole system of prevention of invasions can be.

At the initial stage the review and the analysis of works of a number of the scientists who are engaged in studying of a structure and the principles of functioning of memory of the person were made. By the results of the analysis, cognitive-functional specification of memory system, capable of anticipatory behavior, has been built. It is concluded that scenarios of anticipatory behavior can be formed on two levels: at the level of reflexes and at the level assuming semantic processing of knowledge. There has been noted the importance of the implementation in the designed system mechanisms of memory functioning, aimed at:

– development of conditioned reflexes by system;

– hierarchical data presentation in memory of system (about objects, their properties and processes);

– Change in the availability of data stored in the system memory (for the realization of the possibility of taking into account the context and the procedures for "forgetting" false and outdated data);

– The direction of the focus of attention (to select from memory the necessary knowledge, based on the tasks solved by the system and receiving data);

– implementation of "plausible" conclusions on the basis of information stored in memory of system (including, by implementation of conclusions by analogy).

Apparently, the implementation of these mechanisms is needed so that the designed system was capable of anticipatory behavior in the conflict. In addition, the article suggests the primary appearance of linguistic means of description, presentation and manipulation of knowledge of the subject area of conflict.

УДК 681.3

М.А. Еремеев, И.Е. Горбачев

СВОЙСТВА УПРАВЛЯЕМЫХ ПОДСТАНОВОЧНО-ПЕРЕСТАНОВОЧНЫХ СЕТЕЙ ДЛЯ БЛОЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ НА ОСНОВЕ ОДНОГО КЛАССА ПОДСТАНОВОК

Еремеев М.А., Горбачев И.Е. **Свойства управляемых подстановочно-перестановочных сетей для блочных алгоритмов шифрования на основе одного класса подстановок.**

Аннотация. Статья посвящена исследованию управляемых подстановочно-перестановочных сетей на основе управляемых элементов $F_{4/2}$ в качестве примитива блочных алгоритмов шифрования. Актуальность исследований связана с их ориентацией на проектирование скоростных аппаратных шифров. Научная и практическая значимость полученных результатов заключается в повышении эффективности аппаратной реализации скоростных алгоритмов шифрования, предназначенных для защиты информации в информационно-телекоммуникационных системах и сетях.

Ключевые слова: защита информации, блочные шифры, управляемые подстановочно-перестановочные сети, криптографический примитив.

Eremeev M.A., Gorbachev I.E. **Properties of the Controlled Substitution-Permutation Network for Block Encryption Algorithm Based on One Class of Permutations.**

Abstract. Article is devoted to investigation of the controlled substitution-permutation network based on managed elements $F_{4/2}$ as a primitive block encryption algorithms. Relevance of research is related to their focus on the design of high-speed hardware ciphers. The scientific and practical significance of the results is to improve the efficiency of high-speed hardware implementation of encryption algorithms, designed to protect information in information and telecommunication systems and networks.

Keywords: information security, block ciphers, controlled substitution-permutation network, cryptographic primitive.

1. Введение.

Постоянно увеличивающийся объем конфиденциальной информации, циркулирующей в информационно-телекоммуникационных сетях (ИТКС), предъявляет повышенные требования к современным шифрам. Характерным является повышение требований одновременно по стойкости, скорости и простоте реализации.

Любой блочный шифр представляет собой большое множество подстановок заданного размера, выбираемых в зависимости от секретного ключа. Однако такое непосредственное задание шифра на практике не реализуется, поскольку требует неимоверно большого количества памяти. Но такие подстановки можно генерировать. Соответствующий генератор и представляет собой блочный алгоритм шифрования. Построение блочных шифров на практике осуществляется путем многократного применения относительно простых криптографических преобразований (примитивов). В современных блочных шифрах наиболее широко используются

следующие примитивы: перестановки, подстановки, циклический сдвиг, побитовое сложение по модулю 2 (гаммирование), сложение по модулю 2^n. Использование управляемых операций в качестве криптографического примитива давно привлекает внимание разработчиков шифров. Под управляемой операцией преобразования понимается операция, управляемая некоторым двоичным вектором. При фиксированном значении управляющего вектора реализуются преобразования, относящиеся к одному из вариантов (модификаций) операции. Иными словами, управляемую операцию можно охарактеризовать как множество различных модификаций, каждая из которых соответствует конкретному значению управляющего вектора. Управляющий вектор в таких операциях может формироваться по секретному ключу и/или по преобразуемому блоку данных. Использование такого рода операций открывает большие перспективы для построения стойких и высокоскоростных блочных шифров.

В работах [1–6] была показана эффективность использования управляемых подстановочно-перестановочных сетей (УППС) для синтеза блочных шифров, ориентированных на программную реализацию, в том числе и реализацию в программируемых интегральных схемах. В настоящее время в массовом масштабе выпускаются программируемые логические интегральные схемы (ПЛИС - FPGA) нового поколения, которые предоставляют потенциальную возможность для существенного повышения эффективности аппаратной реализации блочных шифров, оцениваемую по показателю отношения производительности к используемым вычислительным ресурсам. Реализация этой возможности предполагает проектирование УППС, ориентированных на максимальное использование ресурсов типовых логических блоков, содержащихся в новых ПЛИС. Это делает актуальным вопрос о поиске новых типов операций, зависящих от преобразуемых данных (ОЗПД) и реализуемых с помощью УППС, построенных с использованием управляемых элементов (УЭ), более полно использующих объем памяти элементарных ячеек памяти в логических матрицах FPGA, по сравнению с ранее пользованными типами УЭ $F_{2/1}$ [1], $F_{2/2}$ [2].

Программируемые логические матрицы, широко распространенные в настоящее время (к примеру, Virtex-6), содержат типовые логические блоки, включающие два SLICE-узла, каждый из которых включает четыре логические ячейки LUT (LOOP UP TABLE), представляющие собой 64-битовые элементы памяти (ячейки). Каждая такая ячейка позволяет реализовать произвольную булеву функцию (БФ) от шести переменных. Это обеспечивает эффективную реализацию УЭ типов $F_{2/3}$ и $F_{2/4}$, задающих, соответственно, выполнение 8 и 16 подстановок размера 2×2 в зависимости от значения двоичного вектора на управляющем входе, что показано в работах [3–5].

Заметим, что эффективность ОЗПД связана с увеличением размера подблока преобразуемых данных, над которыми они задают некоторую подстановку. Если модификации данной ОЗПД задают преобразование n-битовых векторов и число этих модификаций M, то сама ОЗПД определяет преобразование над N-битовыми векторами, где $N=n+\log_2 M$. Из последнего соотношения видно, что для повышения эффективности ОЗПД необходимо увеличивать число модификаций (размерность управляющего вектора) и размер подблока преобразуемых данных. Таким образом, интерес представляет управляемый элемент $F_{4/2}$, который позволяет на 100% использовать ресурс ячейки памяти. При этом, в отличие от УЭ с двухбитовым входом данных (таким как $F_{2/4}$), для УЭ $F_{4/2}$ возможно построение УППС, обеспечивающих нелинейность преобразования данных при фиксировании управляющего подблока данных. Разумно предположить, что при соответствующем выборе УЭ типа $F_{4/2}$ можно обеспечить существенное повышение криптографических показателей синтезируемого операционного блока. Это позволит сократить число раундов преобразования при сохранении высокой стойкости алгоритмов.

В данной работе рассматривается задача разработки критериев выбора УЭ $F_{4/2}$ и их использования для синтеза УППС и скоростных блочных шифров, ориентированных на эффективную аппаратную реализацию с использованием ПЛИС.

2. Варианты представления, критерии построения и проектирование УЭ $F_{4/2}$. Управляемый элемент $F_{4/2}$ обладает 4-х битовым входом и выходом и 2-х битовым управляющим входом. Схемное представление УЭ $F_{4/2}$ представлено на рисунке 1.

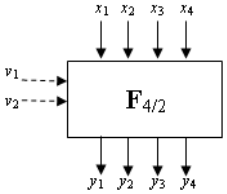


Рис. 1. Управляемый элемент $F_{4/2}$

В общем случае УЭ $F_{4/2}$ удобно представлять в следующих двух видах:

1) В виде четырех булевых функций от 6-ти переменных;

2) В виде упорядоченного набора из четырех подстановок размером 4×4, каждая из которых выполняется над входным 4-х битовым двоичным вектором $X=(x_1, x_2, x_3, x_4)$ при одном из четырех возможных значений управляющего вектора $V=(v_1, v_2)=(0,0), (0,1), (1,0), (1,1)$.

Для синтеза эффективных многослойных УППС требуется

сформулировать некоторые критерии выбора конкретных вариантов УЭ вида $F_{4/1}$. На основании вышеизложенного и результатов, полученных в работе [1], сформулируем следующие базовые критерии отбора и проектирования УЭ $F_{4/2}$:

1) Любой из четырех выходов блока $F_{4/2}$ должен представлять собой нелинейную БФ от шести переменных: $y_i=f_i(x_1, x_2, x_3, x_4, v_1, v_2)$, i=1, ..., 4, каждая из которых имеет значение нелинейности близкое к максимально возможному значению для сбалансированных БФ от шести переменных;

2) Каждая из четырех элементарных модификаций УЭ $F_{4/2}$, а именно $F^{(0)}$, $F^{(1)}$, $F^{(2)}$, $F^{(3)}$ должна осуществлять биективное преобразование $(x_1, x_2, x_3, x_4) \rightarrow (y_1, y_2, y_3, y_4)$;

3) Каждая из четырех модификаций УЭ $F_{4/2}$ должна быть инволюцией;

4) Все линейные комбинации БФ: $f_5= y_1 \oplus y_2$, $f_6= y_1 \oplus y_3$, $f_7= y_1 \oplus y_4$, $f_8= y_2 \oplus y_3$, $f_9= y_2 \oplus y_4$, $f_{10}= y_3 \oplus y_4$, $f_{11}= y_1 \oplus y_2 \oplus y_3$, $f_{12}= y_1 \oplus y_2 \oplus y_4$, $f_{13}= y_1 \oplus y_3 \oplus y_4$, $f_{14}= y_2 \oplus y_3 \oplus y_4$ *и* $f_{15}= y_1 \oplus y_2 \oplus y_3 \oplus y_4$ должны иметь значения нелинейности близкие к $NL(y_1)$, $NL(y_2)$, $NL(y_3)$, $NL(y_4)$.

Используя эти критерии и перебирая различные варианты УЭ $F_{4/2}$, можно найти множество конкретных элементов $F_{4/2}$, представляющих интерес для использования в проектировании блочных шифров. Для оценки возможности полного перебора всех возможных вариантов УЭ $F_{4/2}$ могут быть использованы два варианта поиска УЭ.

Первый состоит в переборе всех возможных четверок булевых функций $y_1=f_1(x_1,x_2,x_3,x_4,v_1,v_2)$, $y_2=f_2(x_1,x_2,x_3,x_4,v_1,v_2)$, $y_3=f_3(x_1,x_2,x_3,x_4,v_1,v_2)$, $y_4=f_4(x_1,x_2,x_3,x_4,v_1,v_2)$. Но объем вычислений, требующихся для реализации этого варианта, очень велик. В самом деле, существует 2^{64} различных булевых функций от 6 переменных, следовательно, необходимо перебрать $2^{64}\cdot(2^{64}-1)\cdot(2^{64}-2)\cdot(2^{64}-3)\approx \approx 11{,}5\cdot10^{76}$ различных четверок булевых функций. Мы можем существенно ограничить количество вариантов перебора, воспользовавшись следствием из второго критерия выбора БФ, а именно тем, что выход операции, реализующей биективное преобразование, описывается сбалансированной БФ. Количество сбалансированных БФ от n переменных равно числу сочетаний $C_{2^{n-1}}^{2^n}$, которое при n=6 приблизительно равняется $1{,}8\cdot10^{18}$, что также достаточно велико и не позволяет выполнить полный перебор.

Минимальное количество вариантов перебора достигается при втором подходе, так как в этом случае проектирование УЭ $F_{4/2}$ сводится к формальному выбору модификаций $F^{(0)}$, $F^{(1)}$, $F^{(2)}$, $F^{(3)}$, каждая из

которых является подстановкой размера 4×4. Количество подстановок размера 4×4 определяется по формуле $2^n!$, что при n=4 равняется $2{,}092 \cdot 10^{13}$. Причем существует $4{,}621 \cdot 10^7$ вариантов таких подстановок удовлетворяющих третьему критерию. Следовательно, проектирование сводится к выбору четверок подобных модификаций. Однако и в этом случае полный перебор является сложной вычислительной задачей.

Рассмотрим возможность сокращения числа рассматриваемых подстановок. Итак, наименьшее число вариантов подстановок обеспечивает требование номер три. Построение всего множества подстановок 4×4 являющихся инволюциями представляется вычислимой задачей. Каждую инволюцию можно представить в виде векторной булевой функции - совокупности БФ, каждая из которых будет описывать по одному выходу УЭ $F_{4/2}$. Для обеспечения максимальной нелинейности преобразования, при фиксированных битах управляющего вектора следует отфильтровывать только те инволюции, в векторную БФ которых входят БФ с максимально возможным значением нелинейности. Хотя максимальное значение нелинейности для БФ от 4-х переменных и равняется 6, для сбалансированных БФ (следствие 2-го критерия) этот показатель не превышает значения 4.

Существенным является влияние всех входных битов на каждый выходной бит, для этого БФ описывающая выход должна зависеть от каждого входного бита, иными словами ее алгебраическая нормальная форма должна иметь в своей записи столько различных переменных, сколько входов у УЭ. В нашем случае это 4.

Для противодействия попыткам проведения криптоанализа немаловажную роль играет также показатель корреляционной эффективности БФ.

В целях проведения исследования была разработана программа, позволяющая отсеивать инволюции по значению характеристик векторных БФ соответствующих конкретной инволюции. Она позволяет отсеивать инволюции по приведенным критериям и выводит результат в файл с некоторой сопутствующей информацией. С учетом вышеизложенных требований остается всего 32256 инволюций. Перебор всех четверок модификаций требует анализа $1{,}08 \cdot 10^{18}$ вариантов, что существенно меньше полученного ранее значения, но также велико.

Для практического применения УЭ $F_{4/2}$ достаточно найти сравнительно малое число таких элементов представляющих их основные подклассы, удовлетворяющие сформулированным критериям. Поэтому можно применить полный перебор по некоторой репрезентативной выборке УЭ $F_{4/2}$, генерируя варианты $F_{4/2}$ путем равновероятной случайной выборки модификаций $F^{(0)}$, $F^{(1)}$, $F^{(2)}$, $F^{(3)}$. В таблице 1 приведена небольшая выборка из множества инволюций,

удовлетворяющих описанным выше критериям. Каждая строчка этой таблицы задает инволюцию.

Таблица 1. Выборка из множества инволюций

№ п/п	f_1	f_2	f_3	f_4
1	$x_4 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1$	$x_3 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$
2	$x_4 \oplus x_3 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1x_3$	$x_3 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_2 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_3 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_3$
3	$x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$	$x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1 \oplus x_1x_3$	$x_3x_4 \oplus x_2 \oplus x_2x_4 \oplus x_1x_4$	$x_3x_4 \oplus x_2x_4 \oplus x_1 \oplus x_1x_4$
4	$x_4 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_3x_4 \oplus x_2 \oplus x_2x_4 \oplus x_1 \oplus x_1x_4$	$x_4 \oplus x_2 \oplus x_1x_3 \oplus x_1x_2$	$x_3 \oplus x_3x_4 \oplus x_2 \oplus x_2x_4 \oplus x_1x_4$
5	$x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_4 \oplus x_3x_4 \oplus x_2 \oplus x_2x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_4 \oplus x_2 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_3 \oplus x_2 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$
6	$x_4 \oplus x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$	$x_3x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$	$x_3 \oplus x_2 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$	$x_1x_2 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_3$
7	$x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1x_2$	$x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1 \oplus x_1x_4$	$x_3 \oplus x_3x_4 \oplus x_2 \oplus x_1 \oplus x_1x_4$	$x_4 \oplus x_3 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1x_4$
8	$x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1x_2$	$x_3x_4 \oplus x_2 \oplus x_1x_4 \oplus x_1x_3$	$x_4 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x_1x_2$	$x_4 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1$
9	$x_3 \oplus x_2x_4 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$	$x_4 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x \oplus x_1x_4 \oplus x_1x_3$	$x_4 \oplus x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x \oplus x_1x_4 \oplus x_1x_3$	$x_4 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$
10	$1 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x_1 \oplus x_1x_4$	$x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$	$x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$	$x_3x_4 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_3$
11	$1 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1 \oplus x_1x_4 \oplus x_1x_3$	$x_2 \oplus x_1 \oplus x_1x_4 \oplus x_1x_3$	$x_3x_4 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$	$x_3 \oplus x_2 \oplus x_1x_4 \oplus x_1x_3$
12	$1 \oplus x_4 \oplus x_3x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1x_3$	$x_3 \oplus x_3x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1x_3$	$x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_2$	$x_3 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_2$
13	$x_3x_4 \oplus x_2x_4 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2$	$1 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x \oplus x_1x_4 \oplus x_1x_3$	$x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$	$x_4 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_2$
14	$x_3x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_2$	$1 \oplus x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_2$	$x_4 \oplus x_2x_3 \oplus x_1x_2$	$x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1 \oplus x_1x_2$
15	$1 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$	$1 \oplus x_4 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_2$	$x_4 \oplus x_3 \oplus x_2 \oplus x_1 \oplus x_1x_2$	$x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1$
16	$1 \oplus x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_2$	$1 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$	$x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_4 \oplus x_3 \oplus x_2 \oplus x_1x_4 \oplus x_1x_3$
17	$1 \oplus x_4 \oplus x_2 \oplus x_1x_4 \oplus x_1x_3$	$1 \oplus x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_2$	$x_4 \oplus x_3 \oplus x_1x_2$	$x_4 \oplus x_3 \oplus x_2 \oplus x_1 \oplus x_1x_2$
18	$x_4 \oplus x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$	$x_3 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1$	$1 \oplus x_3 \oplus x_2 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$	$x_3 \oplus x_1x_4 \oplus x_1x_2$
19	$x_3x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_3$	$x_3 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2$	$1 \oplus x_3 \oplus x_3x_4 \oplus x_2 \oplus x_2x_4 \oplus x_1x_4$	$x_4 \oplus x_3 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$
20	$1 \oplus x_4 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$	$x_4 \oplus x_3x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1$	$1 \oplus x_4 \oplus x_3 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_3x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$

В целях проведения анализа свойств УЭ $F_{4/2}$ по заданным модификациями $F^{(0)}$, $F^{(1)}$, $F^{(2)}$, $F^{(3)}$ получим алгебраическую нормальную форму, реализующих его БФ f_1, f_2, f_3, f_4.

Пусть $\left\{f_1^1(x_1,x_2,x_3,x_4), f_2^1(x_1,x_2,x_3,x_4), f_3^1(x_1,x_2,x_3,x_4), f_4^1(x_1,x_2,x_3,x_4)\right\}$ – БФ, реализующая модификацию $F^{(0)}$ при значении V=(0,0), $\left\{f_1^2(x_1,x_2,x_3,x_4), f_2^2(x_1,x_2,x_3,x_4), f_3^2(x_1,x_2,x_3,x_4), f_4^2(x_1,x_2,x_3,x_4\right\}$, реализующие модификацию $F^{(1)}$ при значении V=(0,1), $\left\{f_1^3(x_1,x_2,x_3,x_4), f_2^3(x_1,x_2,x_3,x_4), f_3^3(x_1,x_2,x_3,x_4), f_4^3(x_1,x_2,x_3,x_4\right\}$, реализующие модификацию $F^{(2)}$ при значении V=(1,0), $\left\{f_1^4(x_1,x_2,x_3,x_4), f_2^4(x_1,x_2,x_3,x_4), f_3^4(x_1,x_2,x_3,x_4), f_4^4(x_1,x_2,x_3,x_4\right\}$, реализующие модификацию $F^{(3)}$ при значении V=(1,1).

Тогда конкретный вид четырех БФ, реализующих УЭ $F_{4/2}$, можно получить следующим образом:

$$y_1 = (v_1 \oplus 1)(v_2 \oplus 1) f_1^1(x_1,x_2,x_3,x_4) \oplus (v_1 \oplus 1)(v_2) f_1^2(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2 \oplus 1) f_1^3(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2) f_1^4(x_1,x_2,x_3,x_4);$$

$$y_2 = (v_1 \oplus 1)(v_2 \oplus 1) f_2^1(x_1,x_2,x_3,x_4) \oplus (v_1 \oplus 1)(v_2) f_2^2(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2 \oplus 1) f_2^3(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2) f_2^4(x_1,x_2,x_3,x_4);$$

$$y_3 = (v_1 \oplus 1)(v_2 \oplus 1) f_3^1(x_1,x_2,x_3,x_4) \oplus (v_1 \oplus 1)(v_2) f_3^2(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2 \oplus 1) f_3^3(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2) f_3^4(x_1,x_2,x_3,x_4);$$

$$y_4 = (v_1 \oplus 1)(v_2 \oplus 1) f_4^1(x_1,x_2,x_3,x_4) \oplus (v_1 \oplus 1)(v_2) f_4^2(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2 \oplus 1) f_4^3(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2) f_4^4(x_1,x_2,x_3,x_4).$$

3. Основные криптографические свойства. В таблице 2 представлены некоторые наборы модификаций, которые удовлетворяют критериям 1–4.

Таблица 2. Представительные наборы модификаций

№	Значение нелинейности БФ	Набор модификаций
1	16-20-24-20-24-20-16-16-16-16-16-20-20-20-16	3-4-5-7
2	20-16-20-20-20-16-24-20-20-16-24-20-20-16-20	5-6-9-15
3	16-20-24-16-24-16-16-16-16-16-16-20-20-16-24	9-14-17-18

3.1. Дифференциальные характеристики. Одними из важных характеристик криптографических примитивов являются дифференциальные, которые отражают подверженность дифференциальному криптоанализу в целом алгоритма шифрования,

построенного на этих примитивах [1, 2, 5]. Их также можно получить для самого УЭ. Рассмотрим дифференциальные характеристики типового конструктивного элемента $F_{4/2}$ которые определят для заданной топологии операционного блока дифференциальные характеристики последнего. На рисунке 2 представлены варианты весов Хэмминга всех возможных разностей, относящихся к УЭ $F_{4/2}$.

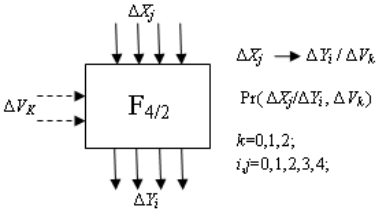


Рис. 2. Варианты разностей для УЭ $F_{4/2}$

Управляемые элементы $F_{4/2}$, удовлетворяющие заданным критериям отбора, обладают хорошими дифференциальными свойствами. Например, дифференциальные характеристики УЭ $F_{4/2}$ (см. вариант 2 в таблице 2) приведены в таблице 3.

Таблица 3. Дифференциальные характеристики

k	*i*	*j*	*Pr*	*k*	*i*	*j*	*Pr*	*k*	*i*	*j*	*Pr*
0	0	0	0.016	1	0	0	0.004	2	0	0	0.003
0	0	1	0.004	1	0	1	0.012	2	0	1	0.008
0	0	2	0.006	1	0	2	0.023	2	0	2	0.01
0	0	3	0.006	1	0	3	0.019	2	0	3	0.007
0	0	4	0	1	0	4	0.004	2	0	4	0.002
0	1	0	0	1	1	0	0.011	2	1	0	0.007
0	1	1	0.024	1	1	1	0.043	2	1	1	0.023
0	1	2	0.04	1	1	2	0.071	2	1	2	0.036
0	1	3	0.024	1	1	3	0.05	2	1	3	0.024
0	1	4	0.005	1	1	4	0.012	2	1	4	0.004
0	2	0	0	1	2	0	0.012	2	2	0	0.003
0	2	1	0.025	1	2	1	0.05	2	2	1	0.023
0	2	2	0.039	1	2	2	0.071	2	2	2	0.037
0	2	3	0.027	1	2	3	0.043	2	2	3	0.024
0	2	4	0.002	1	2	4	0.011	2	2	4	0.007
0	3	0	0	1	3	0	0.004	2	3	0	0.002
0	3	1	0.009	1	3	1	0.019	2	3	1	0.008
0	3	2	0.009	1	3	2	0.023	2	3	2	0.011
0	3	3	0.005	1	3	3	0.012	2	3	3	0.007
0	3	4	0.009	1	3	4	0.004	2	3	4	0.002
0	4	0	0	1	4	0	0	2	4	0	0
0	4	1	0	1	4	1	0	2	4	1	0
0	4	2	0	1	4	2	0	2	4	2	0
0	4	3	0	1	4	3	0	2	4	3	0
0	4	4	0	1	4	4	0	2	4	4	0

3.2 Линейные свойства УЭ $F_{4/2}$. Также важными характеристиками криптографических примитивов являются линейные, которые отражают подверженность линейному криптоанализу [1, 2, 5].

Чтобы вычислить смещение для линейных характеристик УЭ вида $F_{4/2}$, используем следующую формулу:

$$P(a,b,c)=|Pr(\mathrm{XOR}(X\bullet a,F_{4/2}(X,c)\bullet b)=0)-1/20|,$$

где $0 \le a,b \le 15$ и $0 \le c \le 3$. По этой форме, просто вычислять смещения, результаты вычисления смещения для набора модификаций номер 2 в таблице 2, представлены в таблице 4.

Таблица 4. Фрагмент таблицы линейных характеристик для УЭ $F_{4/2}$

a	*b*	*c*	*P*	*a*	*b*	*c*	*P*	*a*	*b*	*c*	*P*	*a*	*b*	*c*	*P*
0	0	0	0.5	0	0		0.5	0	0	2	0.5	0	0	3	0.5
0	1	0	0	0	1	1	0	0	1	2	0	0	1	3	0
0	2	0	0	0	2	1	0	0	2	2	0	0	2	3	0
0	3	0	0.25	0	3	1	0.25	0	3	2	0.25	0	3	3	0.25
0	4	0	0	0	4	1	0	0	4	2	0	0	4	3	0
0	5	0	0.25	0	5	1	0.25	0	5	2	0.25	0	5	3	0.25
1	0	0	0	1	0	1	0	1	0	2	0	1	0	3	0
1	1	0	0.25	1	1	1	0	1	1	2	0	1	1	3	0
1	2	0	0.25	1	2	1	0.25	1	2	2	0.25	1	2	3	0.125
1	3	0	0.125	1	3	1	0.125	1	3	2	0.25	1	3	3	0.25
1	4	0	0.25	1	4	1	0.25	1	4	2	0.25	1	4	3	0.25
1	5	0	0.125	1	5	1	0.25	1	5	2	0.375	1	5	3	0.25
2	0	0	0	2	0	1	0	2	0	2	0	2	0	3	0
2	1	0	0.25	2	1	1	0.25	2	1	2	0.25	2	1	3	0.125
2	2	0	0.25	2	2	1	0.25	2	2	2	0.25	2	2	3	0.25
2	4	0	0.125	2	4	1	0.25	2	4	2	0.25	2	4	3	0.25
3	0	0	0.25	3	0	1	0.25	3	0	2	0.25	3	0	3	0.25
3	1	0	0.125	3	1	1	0.125	3	1	2	0.25	3	1	3	0.25
3	3	0	0.25	3	3	1	0	3	3	2	0	3	3	3	0.25
4	1	0	0.25	4	1	1	0.25	4	1	2	0.25	4	1	3	0.25
4	2	0	0.125	4	2	1	0.25	4	2	2	0.25	4	2	3	0.25
4	4	0	0	4	4	1	0	4	4	2	0	4	4	3	0.25
4	5	0	0.125	4	5	1	0.25	4	5	2	0.25	4	5	3	0.375
5	0	0	0.25	5	0	1	0.25	5	0	2	0.25	5	0	3	0.25
5	1	0	0.125	5	1	1	0.25	5	1	2	0.375	5	1	3	0.25
5	3	0	0.25	5	3	1	0.3125	5	3	2	0.4375	5	3	3	0.3125

5	4	0	0.125	5	4	1	0.25	5	4	2	0.25	5	4	3	0.375
5	5	0	0	5	5	1	0	5	5	2	0.25	5	5	3	0.25
6	6	0	0.25	6	6	1	0	6	6	2	0.25	6	6	3	0.25
7	7	0	0.25	7	7	1	0	7	7	2	0.25	7	7	3	0.25
8	8	0	0	8	8	1	0.25	8	8	2	0.25	8	8	3	0.25
8	9	0	0.375	8	9	1	0.375	8	9	2	0.125	8	9	3	0.375
8	10	0	0.25	8	10	1	0.375	8	10	2	0.125	8	10	3	0.375
9	8	0	0.375	9	8	1	0.375	9	8	2	0.125	9	8	3	0.375
9	9	0	0	9	9	1	0.25	9	9	2	0.25	9	9	3	0.25
10	12	0	0.312	10	12	1	0.4375	10	12	2	0.25	10	12	3	0.4375
10	14	0	0.375	10	14	1	0.375	10	14	2	0.25	10	14	3	0.375
11	11	0	0.25	11	11	1	0.25	11	11	2	0.25	11	11	3	0.25
11	13	0	0.312	11	13	1	0.4375	11	13	2	0.4375	11	13	3	0.4375
11	15	0	0.375	11	15	1	0.375	11	15	2	0.375	11	15	3	0.375
12	12	0	0.25	12	12	1	0.25	12	12	2	0.25	12	12	3	0.25
13	11	0	0.312	13	11	1	0.4375	13	11	2	0.4375	13	11	3	0.4375
13	12	0	0.375	13	12	1	0.375	13	12	2	0.375	13	12	3	0.375
13	13	0	0.25	13	13	1	0.25	13	13	2	0.5	13	13	3	0.25
13	15	0	0.375	13	15	1	0.375	13	15	2	0.5	13	15	3	0.375
14	12	0	0.375	14	12	1	0.375	14	12	2	0.375	14	12	3	0.375
14	14	0	0.25	14	14	1	0.25	14	14	2	0.5	14	14	3	0.25
14	15	0	0.375	14	15	1	0.375	14	15	2	0.5	14	15	3	0.375
15	14	0	0.375	15	14	1	0.375	15	14	2	0.5	15	14	3	0.375
15	15	0	0.25	15	15	1	0.25	15	15	2	0.5	15	15	3	0.25

4. Блочный шифр на основе управляемых операций. Покажем пример использования УЭ $F_{4/2}$ при разработке блочного шифра на основе управляемых операций.

Необходимо определить критерии построения:

1) Блочный шифр должен быть итеративным, обеспечивающим высокую скорость преобразования данных при относительно недорогой аппаратной реализации. Блок данных определим в 128 бит;

2) Для выполнения процедур зашифрования и расшифрования должен использоваться один и тот же алгоритм, а смена режима преобразования должна обеспечиваться сменой расписания

использования ключей;

3) В целях сохранения высокой производительности шифра в приложениях, требующих частой сменой ключа, будем использовать простое расписание ключа.

Схема итеративного шифрования представлена на рисунке 3, где $\mathrm{Crypt}^{(e)}$ – раундовое преобразование, а значение $e \in GF(2)$ определяет режим преобразования.

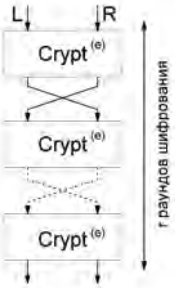


Рис. 3. Схема итеративного шифрования

На рисунке 4 приведен вариант реализации раундового преобразования $\mathrm{Crypt}^{(e)}$.

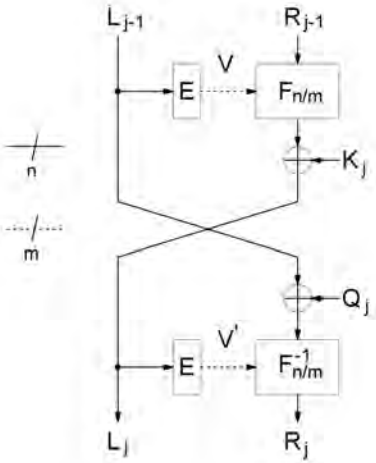


Рис. 4. Вариант раундового преобразования $\mathrm{Crypt}^{(e)}$ в общем виде

Преобразование Crypt можно представить в виде функции:

$$(L_j, R_j)=\text{Crypt}(L_{j-1},R_{j-1}, K_j, Q_j),$$

или в виде

$$L_j \leftarrow F_{n/m}(R_{j-1}, E(L_{j-1})) \text{ XOR } K_j$$

$$R_j \leftarrow F^{-1}{}_{n/m}(L_{j-1} \text{ XOR } Q_j, E(F_{n/m}(R_{j-1}, E(L_{j-1})) \text{ XOR } K_j)),$$

здесь (L_{j-1}, R_{j-1}) и (L_j, R_j) входной и преобразованные блоки данных, представленные в виде конкатенации подблоков одного размера. (K_j, Q_j) – j раундовый ключ, состоящий из двух раундовых подключей одного размера и равных по размеру подблокам L_j и R_j. E – блок расширения, необходимый для формирования управляющего вектора V и представляющий собой простое разветвление проводов, что практически не вносит временную задержку.

Данное раундовое преобразование обращается простой перестановкой раундовых подключей:

$$\text{Crypt}(L, R, K, Q) = (L', R');$$

$$\text{Crypt}(L', R', Q, K) = (L, R).$$

Таким образом, при использовании простого расписания ключей для которого $(K_j, Q_j)=(Q_{r-j+1}, K_{r-j+1})'$, где штрихом обозначен $(r-j+1)$ раундовый ключ процедуры расшифрования, шифрование является корректным, т.е. процедура расшифрования обратна процедуре шифрования.

Дальнейшее проектирование шифра сводится к выбору конкретной реализации блока расширения, выбору числа раундов R, формированию расписания ключа, и разработке конкретной пары управляемых операций F и F^{-1}.

Блок $F_{n/m}$ построенный на основе УЭ $F_{4/2}$ представляет несколько слоев параллельно расположенных и не пересекающихся между собой УЭ $F_{4/2}$. Между соседними слоями используются фиксированные коммутаторы π, основной принцип коммутации – обеспечение влияния каждого входного бита на каждый выходной бит. Общий вид блока $F_{n/m}$ представлен на рисунке 5.

Мы определили размер блока данных в 128 бит, отсюда следует, что n для нашего блока равно 64. Один слой нашего блока будет состоять из 16 УЭ $F_{4/2}$. Для того чтобы каждый входной бит влиял на все выходные потребуется $\log_4 16+1=3$ слоя. Соответственно размер управляющего вектора равен $3 \cdot 16 \cdot 2=96$ бит, а размер управляющего подблока данных всего 64, поэтому необходимо использовать блок расширения E. Реализация $F_{64/92}$ представлена на рисунке 6.

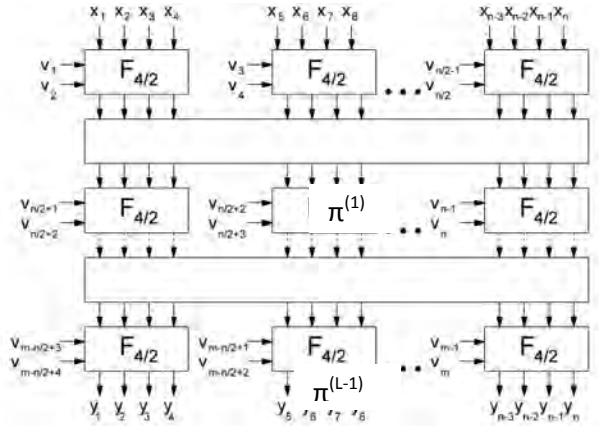


Рис.5. Общий вид блока $F_{n/m}$ на основе $F_{4/2}$ с послойной структурой

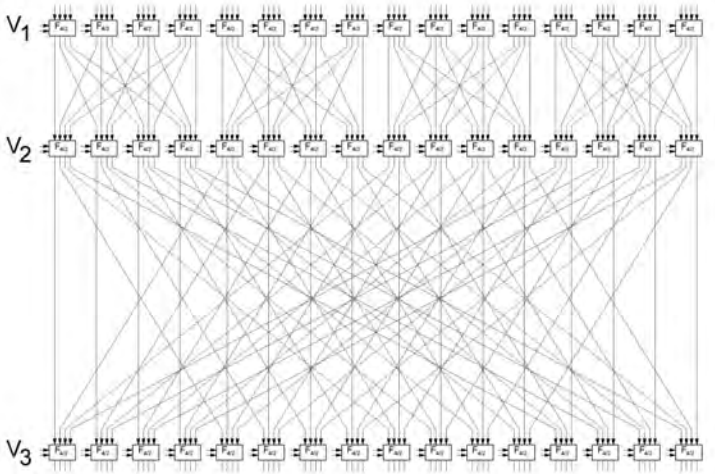


Рис. 6. Структура блока $F_{64/92}$

Для построения обратного преобразования F^{-1} достаточно в блоке F поменять местами вход и выход а управляющий вектор, представленный в виде конкатенации векторов размера *m*/*l*, записать в обратном порядке.

Вероятность прохождения разницы минимального веса через один раунд шифрования равняется $2^{-13,6}$. Таким образом, 10 раундов будет достаточно для успешного противодействия дифференциальному криптоанализу.

Результаты сравнительного анализа сложности аппаратной

реализации [6] и скорости преобразования современных блочных алгоритмов шифрования приведены в таблице 5.

Таблица 5. Сравнение аппаратной реализации различных блочных шифров ПЛИС Xilinx Virtex-6

Шифр	#CLB	Скорость Mbps	Эффективность Mbps / #CLB
AES	2358	259	0,11
IDEA	2878	600	0,21
DES	722	181	0,25
Шифр на основе $F_{4/2}$	*96*	*1119*	*11,65*

4. Заключение. На настоящий момент использование управляемых операций прошло достаточную практическую апробацию на примере блочных шифров DES, RC5, RC6 и MARS и др.. Исследования показывают, что применение управляемых операций позволяет эффективно противостоять дифференциальному и линейному криптоанализу. Использование управляемых операций позволяет строить стойкие и высокоскоростные блочные шифры. В настоящей работе приведено описание УЭ $F_{4/2}$, сформулированы основные требования к проектированию УЭ, показаны основные методы построения таких элементов, и приведены дифференциальные и линейные характеристики для конкретного примера реализации УЭ.

Результаты могут быть использованы при проектировании скоростных блочных шифров на основе управляемых операций, предназначенных для защиты информации, циркулирующей в ИТКС.

Литература

1. *Молдовян А.А., Еремеев М.А., Молдовян Н.А., Морозова Е.В.* Полная классификация и свойства нелинейных управляемых элементов минимального размера и синтез криптографических примитивов // Вопросы защиты информации. 2003. №3. С.15–27.
2. *Еремеев М.А., Молдовян А.А., Молдовян Н.А.* Шифры на основе управляемых операций: комбинирование сетей различного типа // Вопросы защиты информации. 2004. №3. С.17–23.
3. *Хо Н.З.* Разработка и исследование нового класса управляемых элементов $F_{2/3}$ // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. СПб.: ВАС. 2010. С. 419–424.
4. *Хо Н.З., Молдовян А.А.* Разработка управляемых подстановочно-перестановочных сетей на основе управляемых элементов $F_{2/3}$ для синтеза скоростных блочных шифров // Известия СПбГЭТУ ‹‹ЛЭТИ››. 2011. №6. С. 25–30.
5. *Еремеев М.А., Молдовян А.А., Молдовян Н.А.* Разработка и исследование подстановочно-перестановочных сетей для блочных алгоритмов шифрования на основе одного класса управляемых элементов $F_{2/2}$ // Вопросы защиты информации. 2003. №4. С.14–22.
6. *Еремеев М.А., Коркишко Т.А., Мельник А.А., Молдовян А.А., Молдовяну П.А.* Аппаратная поддержка программных шифров // Вопросы защиты информации. 2002. №2. С.26–34.

References

1. Moldovjan A.A., Eremeev M.A., Moldovjan N.A., Morozova E.V. [Complete classification and properties of nonlinear control elements of the minimum size and synthesis of cryptographic primitives]. *Voprosy zashhity informacii – Information security questions*. Moscow: Federal Informational and Analytical Center of the Defense Industry (VIMI). 2003. vol. 3. pp. 15–27. (In Russ).
2. Eremeev M.A., Moldovjan A.A., Moldovjan N.A. [Ciphers based on controlled operations: combining different types of networks]. *Voprosy zashhity informacii - Information security questions*. Moscow: Federal Informational and Analytical Center of the Defense Industry (VIMI). 2004. vol. 3. pp. 17–23. (In Russ).
3. Ho N.Z. [Development and research of a new class of managed elements $F_{2/3}$]. *Innovacionnaja dejatel'nost' v Vooruzhennyh silah Rossijskoj Federacii: Trudy vsearmejskoj nauchno-prakticheskoj konferencii* [Innovative activity in the Armed Forces of the Russian Federation: Proceedings of the All-Army scientific and practical conference]. SPB: Military Academy of Telecommunications. 2010. pp. 419–424. (In Russ).
4. Ho N.Z., Moldovjan A.A. [Development of controlled substitution-permutation network based on managed elements $F_{2/3}$ for the synthesis of high-speed block ciphers]. *Izvestija SPbGJeTU «LJeTI» – News of the SPbGJeTU «LJeTI»*. SPB: Saint Petersburg Electrotechnical University "LETI". 2011. vol. 6. pp. 25–30. (In Russ).
5. Eremeev M.A., Moldovjan A.A., Moldovjan N.A. [Development and research of controlled substitution-permutation network for block encryption algorithms based on a class of controlled elements $F_{2/2}$]. *Voprosy zashhity informacii – Information security questions*. Moscow: Federal Informational and Analytical Center of the Defense Industry (VIMI). 2003. vol. 4. pp. 14–22. (In Russ).
6. Eremeev M.A., Korkishko T.A., Mel'nik A.A., Moldovjan A.A., Moldovjanu P.A. [Hardware support for software ciphers]. *Voprosy zashhity informacii – Information security questions*. Moscow: Federal Informational and Analytical Center of the Defense Industry (VIMI). 2002. vol. 2. pp. 26–34. (In Russ).

Еремеев Михаил Алексеевич — д-р техн. наук, профессор, начальник кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: информационная безопасность, криптография, моделирование конфликтующих систем, автоматизированные системы сбора и обработки информации. Число научных публикаций — 200. mae1@rambler.ru; ул. Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812) 237-19-60.

Eremeev Mikhail Alekseevich — Ph.D., Dr. Sci., professor, head of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: information security, cryptography, modeling of the conflicting systems. The number of publications — 200. mae1@rambler.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

Горбачев Игорь Евгеньевич — к-т техн. наук, доцент, докторант кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: исследование операций, информационная безопасность, искусственный интеллект, информационные конфликты в инфотелекоммуникационном пространстве. Число научных публикаций — 60. gie1976@mail.ru; ул. Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812) 347-96-87.

Gorbachev Igor' Evgen'evich — Ph.D., associate professor, doctoral student of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: research of operations, artificial intelligence, information security, the information conflicts in infotelekommunikatsionny space. The number of publications — 60. gie1976@mail.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 347-96-87.

РЕФЕРАТ

Еремеев М.А., Горбачев И.Е. **Свойства управляемых подстановочно-перестановочных сетей для блочных алгоритмов шифрования на основе одного класса подстановок.**

Постоянно увеличивающийся объем конфиденциальной информации, циркулирующей в информационно-телекоммуникационных сетях, предъявляет повышенные требования к современным шифрам. Характерным является повышение требований одновременно по стойкости, скорости и простоте реализации.

Статья посвящена исследованию управляемых подстановочно-перестановочных сетей на основе управляемых элементов $F_{4/2}$ в качестве примитива блочных алгоритмов шифрования. Показано, что применение управляемых операций позволяет эффективно противостоять дифференциальному и линейному криптоанализу, а также строить стойкие и высокоскоростные блочные шифры. В работе рассматривается задача разработки критериев выбора управляемых элементов $F_{4/2}$ и их использования для синтеза управляемых подстановочно-перестановочных сетей и скоростных блочных шифров, ориентированных на эффективную аппаратную реализацию с использованием программируемых логических интегральных схем.

Результаты могут быть использованы при проектировании скоростных блочных шифров на основе управляемых операций, предназначенных для защиты информации, циркулирующей в критической инфраструктуре.

SUMMARY

Eremeev M.A., Gorbachev I.E. **Properties of the Controlled Substitution-Permutation Network for Block Encryption Algorithm Based on One Class of Permutations.**

An ever-increasing amount of confidential information circulating in the information and telecommunications networks, has high requirements for modern ciphers. Characteristic is the increasing demands concurrently for durability, speed and ease of implementation.

Article is devoted to investigation of the controlled substitution-permutation network based on managed elements $F_{4/2}$ as a primitive block encryption algorithms. It is shown that the use of controlled operations allows to effectively resist differential and linear cryptanalysis, as well as build resistant and high-speed block ciphers. The paper examines the problem of the development of criteria for the selection of managed elements $F_{4/2}$ and their use for the synthesis of controlled substitution-permutation networks and block ciphers, focused on efficient hardware implementation using programmable logic integrated circuits.

The results can be used in the design of high-speed block ciphers based on managed operations designed to protect the information circulating in the critical infrastructure.

УДК 629.7.054

В.И. Миронов, И.В. Фоминов, А.Н. Малетин

МЕТОД АВТОНОМНОЙ КОСВЕННОЙ ИДЕНТИФИКАЦИИ КОЭФФИЦИЕНТА ПРЕОБРАЗОВАНИЯ МАЯТНИКОВОГО КОМПЕНСАЦИОННОГО АКСЕЛЕРОМЕТРА В УСЛОВИЯХ ОРБИТАЛЬНОГО ПОЛЕТА КОСМИЧЕСКОГО АППАРАТА

Миронов В.И., Фоминов И.В., Малетин А.Н. **Метод автономной косвенной идентификации коэффициента преобразования маятникового компенсационного акселерометра в условиях орбитального полета космического аппарата.**

Аннотация. Рассматривается метод автономной косвенной идентификации коэффициента преобразования маятникового компенсационного акселерометра, позволяющий с высокой точностью определить указанный коэффициент в условиях орбитального полета встроенными аппаратно-программными средствами данного измерителя и, таким образом, снизить погрешность определения приращения кажущейся скорости при выполнении маневра космическим аппаратом.

Ключевые слова: маятниковый компенсационный акселерометр, коэффициент преобразования, графоаналитический метод, колебательная система, апериодическая система, переходная характеристика, производная.

Mironov V.I., Fominov I.V., Maletin A.N. **Method of the Autonomous Indirect Identification of the Conversion Factor of Pendulum Compensating Accelerometer Under the Conditions for the Orbital Flight of Automatic Spacecraft.**

Abstract. The paper examines the method of the autonomous indirect identification of the conversion factor of pendulum compensating accelerometer, which makes it possible with the high accuracy to determine the coefficient under the conditions for orbital flight indicated by the built-in firmware means of this gauge and to, thus, decrease an error in the determination of the apparent velocity increment with the accomplishment of maneuver by automatic spacecraft.

Keywords: pendulum compensating accelerometer, conversion factor, graphical analysis, oscillatory system, aperiodic system, transient response, derivative.

1. Введение. Одной из приоритетных задач развития космической деятельности Российской Федерации до 2030 года является создание космических аппаратов (КА), способных выполнять свои функции 10–15 лет. При этом одной из проблем, стоящих перед достижением этой цели, является необходимость обеспечения стабильности метрологических характеристик измерительных устройств систем управления КА в течение длительного орбитального полета. Деградация измерительных средств под воздействием различных факторов космического пространства приводит к отклонению их параметров от номинальных (паспортизированных) значений [1, 2], что в результате может привести к метрологическому отказу измерительного средства.

В этой связи возникает актуальная задача контроля метрологических характеристик измерительных средств в процессе орбитального полета КА, что позволит обеспечить необходимый уровень точности и надежности систем управления КА.

В настоящее время активно ведутся разработки встроенных средств контроля и диагностирования в измерительные устройства систем навигации и определения ориентации КА, то есть разработка так называемых «интеллектуальных» датчиков [3, 4], в том числе и маятниковых акселерометров (МА).

Изменение параметров МА приводит к отклонению его коэффициента преобразования (КП), который является одним из основных метрологических характеристик акселерометров. Это вызывает рост погрешности измерения кажущегося ускорения, а, следовательно, и определения приращения кажущейся скорости КА в режиме маневра.

Определение КП акселерометров, как правило, осуществляют в лабораторных условиях на специализированных стендах. В условиях же орбитального полета такая задача является сложной как с научной, так и технической стороны.

Необходимо отметить, что задача идентификации параметров различных технических устройств в процессе их функционирования приобретает в настоящее время широкий интерес. Так, например, в работе [5] рассматривается метод самодиагностики интеллектуальных датчиков вибрации. Допущением предложенного метода на основе применения эталонной модели является предположение о гармоническом характере измеряемой величины. Вследствие этого помеха в полезном сигнале существенно оказывает влияние на точность оценивания параметров вибрационного акселерометра.

Широкое распространение приобрел аппарат искусственных нейронных сетей в задачах параметрической идентификации. В работах [6, 7] предлагаются варианты решения задачи оценивания параметров технических устройств авиакосмических систем. Основным недостатком применения искусственных нейронных сетей, на наш взгляд, является сложность формирования обучающей выборки, адекватной реальным процессам, протекающим в космическом пространстве. Несмотря на это, авторы придерживаются мнения о целесообразности такого подхода к задачам идентификации.

В работе [8] предложен поисковой метод динамической идентификации параметров двигателя постоянного тока на основе применения генетических алгоритмов. Применение генетических алгоритмов к задаче идентификации параметров интеллектуальных датчиков представляется, на наш взгляд, ограниченным из-за сравнительно большого интервала времени, требуемого на оценивание параметров.

В предлагаемой статье рассматривается косвенный метод автономной идентификации КП МА на основе известных графоаналитических методов идентификации параметров систем второго порядка, из-

ложенных в работе [9], а также методов диагностики, базирующихся на создании в цепи обратной связи априорных диагностических тестовых сигналов $U_{\text{тест}}$.

Эти методы основаны на применении ступенчатого воздействия на систему и анализа переходных процессов выходного сигнала. Учитывая, что математическая модель МА может быть приближенно описана системой второго порядка, то можно сделать вывод о принципиальной возможности идентификации некоторых параметров встроенными аппаратно-программными средствами данного измерителя, в том числе, об идентификации КП.

2. Постановка задачи. В качестве исходных данных примем математическую модель МА с емкостным датчиком перемещения (ДП) и магнитоэлектрическим датчиком момента (ДМ) (рисунок 1) [10].

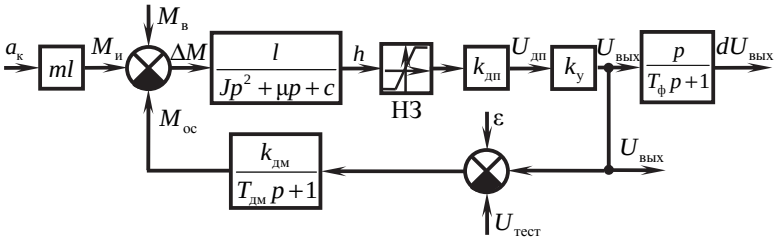


Рис. 1. Структурная схема МА с магнитоэлектрической обратной связью

На рисунке 1 обозначено: $a_к$ — измеряемое кажущееся ускорение; ml — маятниковость чувствительного элемента (ЧЭ) МА; $M_и$ — момент силы инерции; $M_в$ — сумма неучтенных внешних возмущающих воздействий; l — длина ЧЭ (маятника); J — момент инерции ЧЭ МА; μ — коэффициент демпфирования ЧЭ; c — коэффициент жесткости ЧЭ; h — линейное перемещение ЧЭ; НЗ — нелинейное звено типа ограничение по перемещению ЧЭ; $k_{дп}$ — коэффициент передачи ДП; $U_{дп}$ — сигнал ДП; $k_у$ — коэффициент передачи усилителя; $T_ф$ — постоянная времени фильтра; $U_{вых}$ — выходное напряжение усилителя; ε — внутренний шум МА, выраженный через среднеквадратическое отклонение, с нулевым математическим ожиданием; $U_{тест}$ — тестовый сигнал; $k_{дм}$ — коэффициент передачи ДМ; $T_{дм}$ — постоянная времени ДМ; $M_{ос}$ — момент обратной связи; p — символ дифференцирования.

Передаточная функция МА по выходному сигналу имеет следующий вид:

$$W(p)=\frac{U_{\text{вых}}(p)}{a_{\text{к}}(p)}=\frac{ml^2k_{\text{дп}}k_{\text{у}}(T_{\text{дм}}p+1)}{(Jp^2+\mu p+c)(T_{\text{дм}}p+1)+k_{\text{дм}}lk_{\text{дп}}k_{\text{у}}}. \quad (1)$$

Тогда КП МА определяется следующим выражением:

$$K_a=\frac{ml^2k_{\text{дп}}k_{\text{у}}}{c+k_{\text{дм}}lk_{\text{дп}}k_{\text{у}}}. \quad (2)$$

Требуется найти оценку коэффициента преобразования $\hat{K}_a(U_{\text{тест}},P,h_{\max},t)$, где $P=\{m,l,J,\mu,c,k_{\text{дп}},k_{\text{дм}},k_{\text{у}}\}$ — множество параметров МА, подверженных различным возмущающим воздействиям, $h_{\max}$ — предельное значение отклонения маятника (подвижной пластины) акселерометра.

3. Содержание метода идентификации коэффициента преобразования.

3.1 Аппроксимация маятникового акселерометра моделью, описывающей колебательную систему второго порядка.

В соответствие с поставленной задачей для идентификации КП МА, функционирующего в режиме орбитального полета, целесообразно использовать известные графоаналитические методы идентификации параметров систем второго порядка, изложенные в работе [9], и основанные на оценке параметров разомкнутой системы по виду выходной переходной характеристики (ПХ). А также косвенные методы диагностики, базирующиеся на создании в цепи обратной связи априорных тестовых сигналов $U_{\text{тест}}$.

Учитывая, что математическая модель МА может быть приближенно представлена апериодической или колебательной системой второго порядка, то можно сделать вывод о принципиальной возможности идентификации некоторых параметров встроенными аппаратно-программными средствами данного измерителя, в том числе, определения КП.

В качестве допущений примем, что постоянная времени $T_{\text{дм}}$ равна нулю, а тестовое воздействие стабильно $U_{\text{тест}}(t)=const$.

Тогда в соответствие с графоаналитическим методом идентификации разомкнутых колебательных систем второго порядка запишем

передаточную функцию МА по тестовому воздействию $W_{U_{\text{тест}}}^{U_{\text{вых}}}(p)$ в виде:

$$W_{U_{\text{тест}}}^{U_{\text{вых}}}(p) = \frac{K_{\text{тест}}}{T^2 p^2 + 2\xi T p + 1}, \tag{3}$$

где:

$$T = \sqrt{\frac{J}{c + k_{\text{дм}} l k_{\text{дп}} k_{\text{у}}}}; \tag{4}$$

$$\xi = \frac{\mu}{2}\sqrt{\frac{1}{J(c + k_{\text{дм}} l k_{\text{дп}} k_{\text{у}})}}; \tag{5}$$

$$K_{\text{тест}} = \frac{k_{\text{дм}} l k_{\text{дп}} k_{\text{у}}}{c + k_{\text{дм}} l k_{\text{дп}} k_{\text{у}}}, \tag{6}$$

а T, ξ, $K_{\text{тест}}$ — постоянная времени, коэффициенты относительного демпфирования ($\xi < 1$) и преобразования замкнутой системы МА по тестовому воздействию $U_{\text{тест}}$, соответственно.

Возведем в квадрат выражение (4) и его знаменатель подставим в формулу (2). В результате получим приближенную формулу для определения КП МА через постоянную времени T:

$$\hat{K}_a \approx \gamma T^2 k_{\text{дп}} k_{\text{у}}, \tag{7}$$

где γ — коэффициент, характеризующий конструктивные характеристики маятника (форму, массу и габариты). Для модели (1) $\gamma = 3/4$.

Из формулы (7) видно, что для идентификации КП $\hat{K}_a$ достаточно экспериментально определить значения постоянной времени T, а также произведение коэффициентов $k_{\text{дп}} k_{\text{у}}$. Для этого необходимо произвести следующие операции.

1. Для определения значения постоянной времени T из формулы (7) необходимо получить экспериментальную ПХ МА путем создания тестового воздействия в виде постоянного напряжения $U_{\text{тест}}$ на входе дополнительной обмотки ДМ МА.

2. По полученной экспериментальной ПХ МА $U_{\text{вых}}(t)$ определяются моменты времени t_1 и t_2 перехода через линию установившегося значения выходного сигнала $\bar{U}_{\text{уст}}$ (см. рисунок 2). Далее в соот-

ветствие с формулой (8) вычисляется частота собственных колебаний ЧЭ:

$$\omega = \frac{2\pi}{t_2 - t_1}. \qquad (8)$$

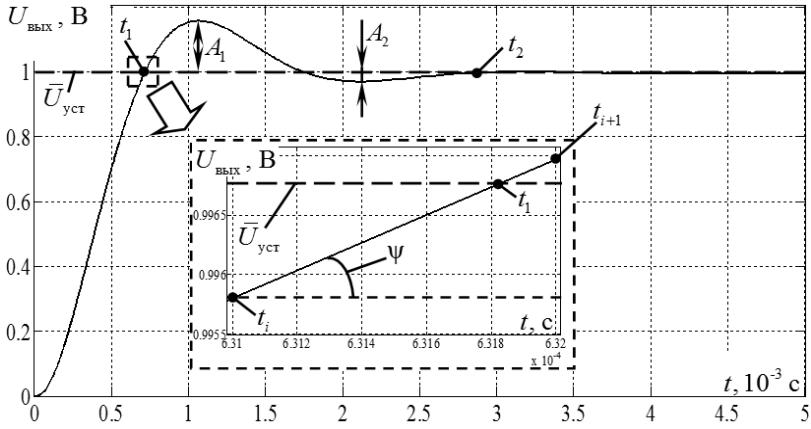


Рис. 2. Переходная колебательная характеристика МА

3. Далее определяются значения амплитуд A_1 и A_2 на интервале времени ПХ от t_1 до t_2 и вычисляется относительный коэффициент демпфирования [11]:

$$\xi = \frac{1}{\sqrt{1 + \dfrac{\pi^2}{\ln^2(A_1 / A_2)}}}. \qquad (9)$$

4. Постоянная времени вычисляется в соответствии с известной формулой для колебательной системы второго порядка [9]:

$$T = \frac{\sqrt{1-\xi^2}}{\omega}. \qquad (10)$$

5. Для определения произведения значений параметров $k_{дп}k_{у}$ необходимо подать тестовые сигналы $\pm U_{тест}$ в цепь обратной связи МА таких величин, при которых угловое положение ЧЭ достигает со-

ответствующих предельных значений $h^{+}_{\max}$ и $h^{-}_{\max}$. В этом случае произведение значений параметров $k_{\text{дп}}k_{\text{у}}$ определяется формулой:

$$k_{\text{дп}}k_{\text{у}} = \frac{1}{2}\left(\frac{U^{+}_{\text{тест}}}{h^{+}_{\max}} - \frac{U^{-}_{\text{тест}}}{h^{-}_{\max}}\right). \qquad (11)$$

Для подтверждения эффективности изложенного метода было проведено математическое моделирование процесса функционирования МА в режиме идентификации КП. В качестве исходных данных для моделирования были выбраны следующие значения параметров МА [10]:

$$m = 2{,}9\cdot10^{-4}\ \text{кг};\ l = 4{,}28\cdot10^{-3}\ \text{м};\ J = 7{,}09\cdot10^{-9}\ \text{кг}\cdot\text{м}^2;$$

$$\mu = 2{,}54\cdot10^{-5}\ \text{Н}\cdot\text{м}\cdot\text{с};\ c = 3{,}02\cdot10^{-4}\ \text{Н}\cdot\text{м};\ h_{\max} = 1{,}9\cdot10^{-6}\ \text{м};$$

$$k_{\text{дп}} = 2{,}5\cdot10^{5}\ \text{В/м};\ k_{\text{у}} = 8{,}5;\ k_{\text{дм}} = 9{,}23\cdot10^{-6}\ \text{Н}\cdot\text{м/В};\ T_{\text{дм}} = 10^{-5}\ \text{с};$$

$$\varepsilon = 10^{-5}\ \text{В};\ T_{\text{ф}} = 10^{-5}\ \text{с};\ U_{\text{тест}} = 1;\pm5\ \text{В}.$$

Моделирование было проведено при допущении постоянства момента неучтенных сил $M_{\text{в}} = 1\cdot10^{-6}\ \text{Н}\cdot\text{м}$, действующих на ЧЭ, а также при условии отсутствия кажущегося ускорения $a_{\text{к}} = 0$.

Такие условия могут быть обеспечены при движении КА в пассивном орбитальном полете, где для высоты 300 км кажущееся ускорение, воздействующее на ЧЭ МА, не превышает значений порядка $10^{-6}\ g$.

Результаты моделирования подтвердили принципиальную возможность идентификации КП. При вышеприведенных исходных данных относительная погрешность оценивания КП составила:

$$\delta K_a = \frac{\hat{K}_a - K_a}{\hat{K}_a}\cdot100\%,\ \delta K_a = 0{,}141\%.$$

Проведенные исследования показывают, что погрешность определения фактического КП в соответствии с предложенным методом зависит от:

– величины относительного коэффициента демпфирования, определяющего возможность представления физической модели МА колебательным звеном второго порядка;

– случайной погрешности измерения, обусловленной внутренними шумами блока электроники МА;

– допущения о равенстве нулю постоянных времени инерционных звеньев МА (усилителя, ДМ и ДП);

– допущения о постоянстве момента внешних сил в процессе идентификации.

Для оценки влияния первых трёх причин на точность оценки КП МА было проведено математическое моделирование и получены результаты, отображенные на рисунке 3.

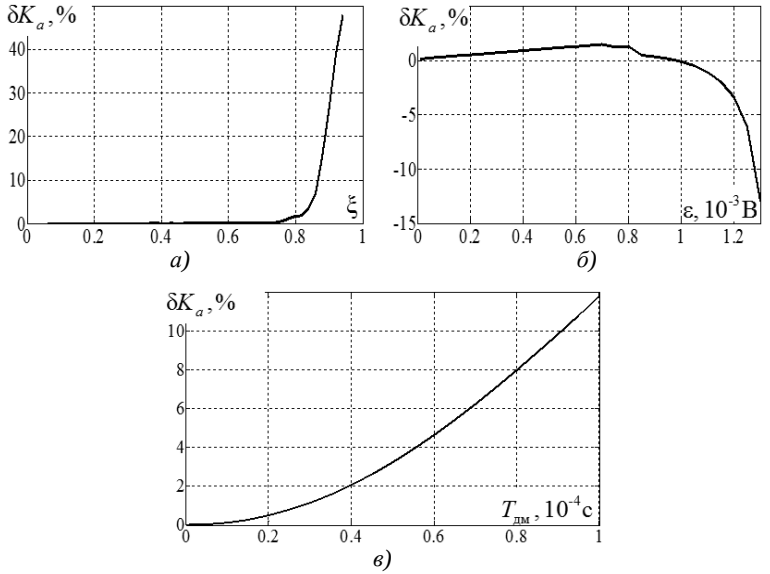


Рис. 3. Зависимости относительной погрешности оценивания КП МА: *а*) от относительного коэффициента демпфирования МА; *б*) среднеквадратического отклонения внутреннего шума МА; *в*) и постоянной времени датчика момента МА

Из рисунка 3*а* видно, что относительная погрешность определения КП существенно увеличивается при стремлении относительного коэффициента демпфирования ξ к единице. Это связано с тем, при малых значениях ξ кривая переходного процесса пересекает линию установившегося значения под большим углом ψ (рисунок 2), что позволяет повысить отношение сигнал/шум при вычислении моментов времени t_1 и t_2.

Результаты исследования влияния помехи на точность определения КП подтверждают предшествующий тезис (рисунок 3*б*). С увеличением уровня помехи значительно сложнее оценить характер переходного процесса, что влияет на качественную оценку КП МА.

При увеличении постоянной времени ДМ погрешность определения КП растёт (рисунок 3*в*) в связи с увеличением расходимости модели МА второго и третьего порядка.

3.2 Аппроксимация МА моделью, описывающей апериодическую систему второго порядка. В соответствие с графоаналитическим методом идентификации разомкнутых апериодических систем второго порядка запишем передаточную функцию МА по тестовому воздействию $W_{U_{\text{тест}}}^{U_{\text{вых}}}(p)$ в виде:

$$W_{U_{\text{тест}}}^{U_{\text{вых}}}(p) = \frac{K_{\text{тест}}}{T_2^2 p^2 + T_1 p + 1}, \tag{12}$$

где:

$$T_1 = \frac{\mu}{c + k_{\text{дм}}\, l\, k_{\text{дп}} k_{\text{у}}}, \tag{13}$$

T_1, T_2 — постоянные времени замкнутой системы МА по тестовому воздействию $U_{\text{тест}}$, соответственно, причем $T_1 > 2T_2$.

Апериодическое звено второго порядка (12) представим в следующем виде [9]:

$$W_{U_{\text{тест}}}^{U_{\text{вых}}}(p) = \frac{K_{\text{тест}}}{(T_3 p + 1)(T_4 p + 1)},$$

где:

$$T_1 = T_3 + T_4; \tag{14}$$

$$T_2 = \sqrt{T_3 T_4}\ . \tag{15}$$

Для идентификации КП $\hat{K}_a$ по формуле (7) необходимо произвести следующие операции.

1. Для определения значения постоянной времени T_2 необходимо получить экспериментальную ПХ МА $U_{\text{вых}}(t)$ и её производную $\dot{U}_{\text{вых}}(t)$ (рисунок 4) путем создания тестового воздействия $U_{\text{тест}}$ на входе датчика момента МА.

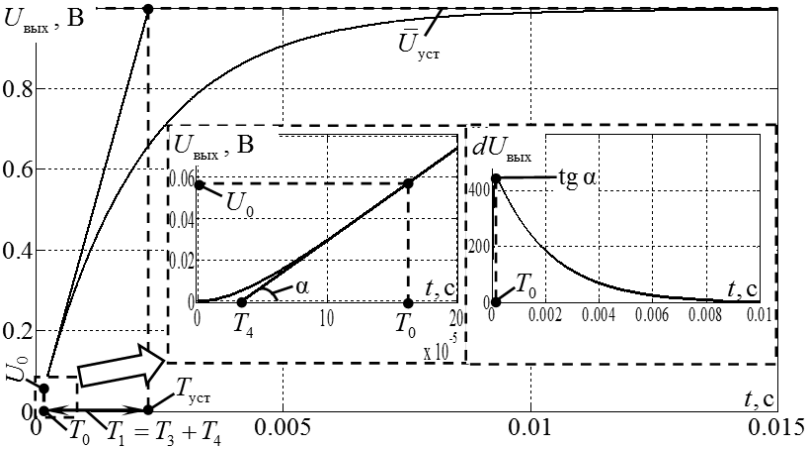


Рис. 4. Переходная апериодическая характеристика МА

2. Находится максимум производной выходного сигнала $\dot{U}_{вых}(t)$ МА $\dot{U}_{вых}^{max} = \operatorname{tg}\alpha$ (рисунок 4) и соответствующий ему момент времени T_0:

$$T_0 = T_0^{изм} - T_ф - T_{дм}, \qquad (16)$$

где $T_ф$ — постоянная времени фильтра (см. рисунок 1).

3. Определяется момент времени, соответствующий пересечению касательной к переходной характеристике в точке T_0 линии, характеризующей установившееся значение:

$$T_{уст} = \frac{\bar{U}_{уст} + \operatorname{tg}\alpha\ T_0 - U_0}{\operatorname{tg}\alpha}.$$

4. Определяется приближённое значение момента времени пересечения касательной к переходной характеристике оси абсцисс:

$$T_4 = \frac{\operatorname{tg}\alpha\ T_0 - U_0}{\operatorname{tg}\alpha}.$$

5. Определяется постоянная времени T_1:

$$T_1 = T_{уст} - T_0.$$

6. Из формулы (14) определяется приближённое значение постоянной времени T_3:

$$T_3 = T_1 - T_4 .$$

7. По формуле (15) определяется приближённое значение постоянной времени T_2.

8. Определяется величина T_2, которая может быть найдена в результате решения рекуррентного соотношения [9]:

$$T_0\,(k+1) = \frac{T_2^2(k)}{2\sqrt{\frac{T_1^2}{4} - T_2^2(k)}} \ln \frac{T_2^2(k)}{\left(\frac{T_1}{2} - \sqrt{\frac{T_1^2}{4} - T_2^2(k)}\right)^2},$$

количество итераций k, в котором определяется условием:

$$\min(T_0(k+1) - T_0) .$$

Начальные значения постоянной времени T_2 и T_0 определяются соответственно по формулам (15) и (16).

9. Для определения произведения значений параметров $k_{\text{дп}} k_{\text{у}}$ необходимо подать тестовые сигналы $\pm U_{\text{тест}}$ в цепь обратной связи МА таких величин, при которых угловое положение ЧЭ достигает соответствующих предельных значений $h_{\max}^{+}$ и $h_{\max}^{-}$. Произведение значений параметров $k_{\text{дп}} k_{\text{у}}$ определяется по формуле (11).

10. По уточнённому значению $T = T_{2\text{у}}$ по формуле (7) также определяется КП МА. В случае если $T_1 = 2T_2$ (ξ =1), то $T_2 = T_0$.

Для подтверждения эффективности изложенного метода было проведено математическое моделирование процесса функционирования МА в режиме идентификации КП. Моделирование проводилось при аналогичных исходных данный, представленных для колебательной системы МА, за исключением значения коэффициента демпфирования, величина которого равна:

$$\mu = 1,01 \cdot 10^{-4}\ \text{Н} \cdot \text{м} \cdot \text{с} .$$

При вышеприведенных исходных данных и отсутствии постоянных возмущений относительная погрешность оценивания КП составила:

$$\delta K_a = 0,682\,\% .$$

Для оценки влияния постоянных времени T_1, T_2, внутреннего шума МА и постоянной времени ДМ на точность оценки КП МА было проведено математическое моделирование, и получены результаты, отображенные на рисунке 5.

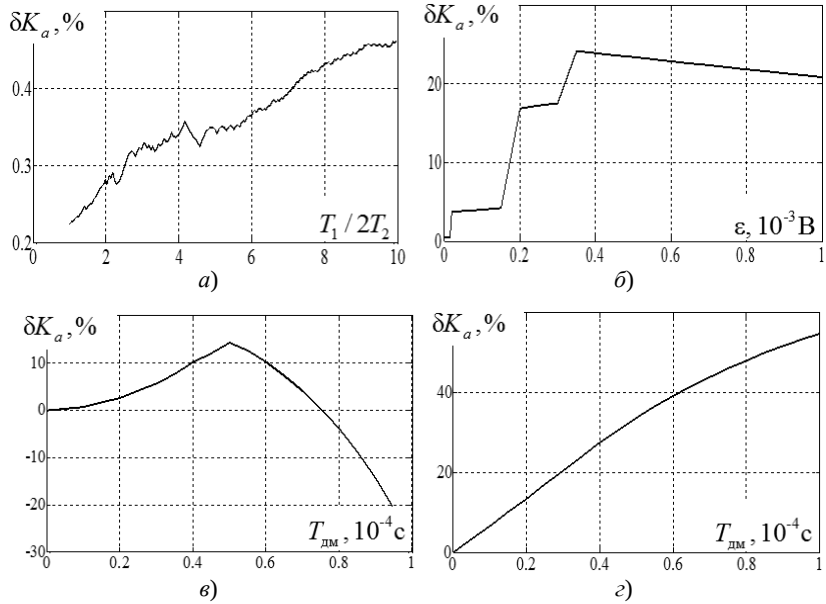


Рис. 5. Зависимости относительной погрешности оценивания КП МА: *а*) от отношения постоянных времени $T_1 / 2T_2$; *б*) среднеквадратического отклонения внутреннего шума МА; *в*) постоянной времени датчика момента с её алгоритмической компенсацией; *г*) без таковой

Из рисунка 5*а* видно, что относительная погрешность определения КП незначительно увеличивается при увеличении отношения $T_1 / 2T_2$.

Из сравнения рисунков 3*б* и 5*б* можно сделать вывод о том, что внутренние шумы МА оказывают большее влияние на точность идентификации КП в случае аппроксимации физического прибора апериодической системой по сравнению с теми же условиями, но при аппроксимации МА колебательной системой. Исследования, проведенные авторами, показывают, что нелинейность зависимости (рисунок 5*б*) обусловлена влиянием фильтрующих свойств МА (постоянные времени T_1, T_2, $T_{\text{дм}}$, $T_{\text{ф}}$).

Из сравнения рисунков 5*в*, *г* следует, что алгоритмическая компенсация постоянной времени датчика момента по формуле (16) способствует снижению относительной погрешности определения КП. Данная компенсация приводит к удовлетворительному результату только в том случае, если значение $T_{\text{дм}}$ известно и постоянно.

4. Выводы. Разработанный метод автономной косвенной идентификации коэффициента преобразования может быть использован для проведения текущей диагностики работоспособности маятниковых акселерометров в процессе полёта КА. Это способствует учёту деградации метрологических характеристик и повышению точности измерения приращения кажущейся скорости КА в режиме выполнения маневров.

Предложенный метод может быть применен как к апериодическим, так и к колебательным системам второго порядка. Проведенные исследования показали, что применение разработанного метода более эффективно с точки зрения точности оценки коэффициента преобразования маятникового акселерометра, физическая модель которого близка к колебательной системе.

Литература

1. *Фоминов И.В.* Обобщенная структура адаптивного информационно-измерительного комплекса подвижного объекта // Известия вузов. Приборостроение. 2013. № 7. С. 5–9.
2. *Фоминов И.В., Голяков А.Д.* Анализ влияния надежности и стойкости адаптивных информационно-измерительных навигационных систем на эффективность их использования // Навигация и гидрография. 2013. № 36. С. 9–16.
3. ГОСТ Р 8.734-2011. Датчики интеллектуальные и системы измерительные интеллектуальные. Методы метрологического самоконтроля // М.: Стандартинформ. 2012.
4. *Пронин А.Н., Сапожникова К.В., Тайманов Р.Е.* Интеллектуализация средств измерений как фактор увеличения надежности систем управления // Управление в морских и аэрокосмических системах (УМАС-2014): Сб. научн. тр. конф. СПб.: ЦНИИ «Электроприбор. 2014. С. 23–28.
5. *Лачин В.И., Плотников Д.А.* Реализация функций самодиагностики интеллектуальных датчиков вибрации // Известия ЮФУ. Технические науки. 2012. № 3. С. 241–251.
6. *Никишов А.Н., Зайцев А.В., Канушкин С.В., Семенов А.В.* Подход к тестированию и диагностике авиакосмических систем с использованием нейросетевого идентификатора // Электронный журнал «Труды МАИ». 2011. № 47. 10 с. URL: www.mai.ru/science/trudy.
7. *Никишов А.Н., Зимарин А.М.* Оптимальное управление сложными техническими системами с использованием обобщённого квадратичного показателя качества // Приборы и системы. Управление, контроль, диагностика. 2011. № 6. С. 5–8.
8. *Гаргаев А.Н., Каширских В.Г.* Идентификация параметров двигателей постоянного тока с помощью поисковых методов // Вестник Кузбасского ГТУ. 2013. № 1. С. 131–134.

9. *Дмитриев А.К., Юсупов Р.М.* Идентификация и техническая диагностика // М.: МО СССР. 1987. 521 с.
10. *Распопов В.Я.* Микромеханические приборы // М.: Машиностроение. 2007. 400 с.
11. *Дилигенская А.Н.* Идентификация объектов управления // Самара: СГТУ. 2009. 136 с.

References

1. Fominov I.V. [Generalized structure of the adaptive data-measuring complex of mobile object]. *Izv. vyssh. uchebn. zavedenij: Priborostroenie – Proceedings of the higher educational institutions: Instrumentation*. 2013. vol. 7. pp. 5–9. (In Russ.).
2. Fominov I.V., Golyakov A.D. [Analysis of the influence of reliability and durability of adaptive data-measuring navigation systems on the effectiveness of their use]. *Navigacija i gidrografija – Navigation and hydrography*. 2013. vol. 36. pp. 9–16. (In Russ.).
3. GOST R 8.734-2011. [Smart sensors and system measuring intellectual. Methods of metrological self-control]. M.: STANDARTINFORM. 2012. (In Russ.).
4. Pronin A.N., Sapozhnikova K.V., Taymanov R.E. [Intellectualization of the means of measurements as the factor of an increase in the reliability of control systems]. *Upravlenie v morskih i ajerokosmicheskih sistemah (UMAS-2014): Sb. nauchn. tr. konf.* [Administration in the sea and aerospace systems]. SPb.: CNII «Jelektropribor». 2014. pp. 23–28. (In Russ.).
5. Lachin V.I., Plotnikov D.A. [Analysis of the self-testing functions implementation for intelligent vibration sensors]. *Izvestija JuFU. Tehnicheskie nauki – Proceedings YuFU. The technical sciences*. 2012. vol. 3. pp. 241–251. (In Russ.).
6. Nikishov A.N., Zajcev A.V., Kanushkin S.V., Semenov A.V. [Approach to testing and diagnostics of aerospace systems with the use of neuron network identifier]. *Jelektronnyj zhurnal «Trudy MAI» – Electronic journal «Transactions of the MAI»*. 2011. vol. 47. 10 p. Available at: www.mai.ru/science/trudy. (In Russ.).
7. Nikishov A.N., Zimarin A.M. [Optimal control of complex technical systems with the use of the generalized quadratic qualitative index]. *Pribory i sistemy. Upravlenie, kontrol', diagnostika – Instruments and system. Control, control, diagnostics.* 2011. vol. 6. pp. 5–8. (In Russ.).
8. Gargaev A.N., Kashirskih V.G. [Identification of the parameters of direct-current motors with the aid of the search methods]. *Vestnik Kuzbasskogo GTU – Herald of Kuzbas GTU*. 2013. vol. 1. pp. 131–134. (In Russ.).
9. Dmitriev A.K., Jusupov R.M. *Identifikacija i tehnicheskaja diagnostika* [Identification and technical diagnostics]. M. 1987. 521 p. (In Russ.).
10. Raspopov V.Ja. *Mikromehanicheskie pribory* [Micromechanical instruments]. M.: Mashinostroenie. 2007. 400 p. (In Russ.).
11. Diligenskaja A.N. *Identifikacija objektov upravlenija* [Identification of the objects of control]. Samara: SGTU. 2009. 136 p. (In Russ.).

Миронов Вячеслав Иванович — д-р техн. наук, профессор, ведущий научный сотрудник, Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), профессор кафедры автономных систем управления, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: функциональные и прикладные исследования теории комплексного моделирования, теории оптимального наблюдения и управления динамическими процессами, вычислительной математики, баллистических космических полётов, статистического анализа характеристик сложных технических систем. Число научных публикаций — более 400. mironuv@mail.ru; 14-я линия В.О., д. 39, Санкт-Петербург, 199178; р.т.: +7(812)328-4450.

Mironov Vyacheslav Ivanovich — Ph.D., Dr. Sci., professor, leading researcher, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS), professor of the autonomous systems of the control department, Mozhaisky Military Space Academy. Research interests: functional theory and applied research of integrated modeling, theory of optimal control and monitoring dynamic processes, computational mathematics, ballistic space flight, a statistical analysis of the characteristics of complex technical systems. The number of publications — is more than 400. mironuv@mail.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-4450.

Фоминов Иван Вячеславович — к-т техн. наук, докторант кафедры автономных систем управления, Военно-космическая академия им. А.Ф. Можайского. Область научных интересов: системы навигации и управления движением космических аппаратов. Число научных публикаций — 23. i.v.fominov@gmail.com; Ждановская улица, д. 13, Санкт-Петербург, 197198; р.т.: +7(812)347-9521.

Fominov Ivan Vyacheslavovich — Ph.D., doctoral student of the autonomous control systems department, Mozhaisky Military Space Academy. Research interests: navigation and control systems of spacecrafts. The number of publications — 23. i.v.fominov@gmail.com; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812)347-9521.

Малетин Андрей Николаевич — к-т техн. наук, начальник лаборатории — старший научный сотрудник военного института (научно-исследовательского), Военно-космическая академия им. А.Ф. Можайского. Область научных интересов: повышение точности инерциальных измерителей параметров движения. Число научных публикаций — 11. maletin@bk.ru; ул. Ждановская 13, 197198, Санкт-Петербург; р.т.: +7(906) 242-75-61.

Maletin Andrey Nikolayevich — Ph.D., head of laboratory — senior researcher of the military institute (of scientific research), Mozhaisky Military Space Academy. Research interests: increase in the accuracy of the inertial gauges of the parameters of motion. The number of publications — 11. maletin@bk.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(906) 242-75-61.

РЕФЕРАТ

Миронов В.И., Фоминов И.В., Малетин А.Н. **Метод автономной косвенной идентификации коэффициента преобразования маятникового компенсационного акселерометра в условиях орбитального полета космического аппарата.**

В настоящее время активно ведутся разработки встроенных средств контроля и диагностирования в измерительные устройства систем навигации и определения ориентации космических аппаратов, то есть разработка так называемых «интеллектуальных» датчиков, в том числе и маятниковых акселерометров.

Изменение параметров маятниковых акселерометров приводит к отклонению его коэффициента преобразования, который является одним из основных метрологических характеристик акселерометров. Это вызывает рост погрешности измерения кажущегося ускорения, а, следовательно, и определения приращения кажущейся скорости космического аппарата в режиме маневра.

Определение коэффициента преобразования акселерометров, как правило, осуществляют в лабораторных условиях на специализированных стендах. В условиях же орбитального полета такая задача является сложной как с научной, так и технической стороны.

В статье предлагается косвенный метод автономной идентификации коэффициента преобразования маятникового акселерометра на основе известных графоаналитических методов идентификации параметров систем второго порядка, изложенных в работе, а также методов диагностики, базирующихся на создании в цепи обратной связи априорных диагностических тестовых сигналов.

Эти методы основаны на применении ступенчатого воздействия на систему и анализа переходных процессов выходного сигнала. Учитывая, что математическая модель маятникового акселерометра может быть приближенно описана системой второго порядка, то можно сделать вывод о принципиальной возможности идентификации некоторых параметров встроенными аппаратно-программными средствами данного измерителя, в том числе, об идентификации коэффициента преобразования.

Разработанный метод автономной косвенной идентификации коэффициента преобразования может быть использован для проведения текущей диагностики работоспособности маятниковых акселерометров в процессе полёта космического аппарата. Это способствует учёту деградации метрологических характеристик и повышению точности определения приращения кажущейся скорости космического аппарата в режиме выполнения маневров.

Предложенный метод может быть применен как к апериодическим, так и к колебательным системам второго порядка. Проведенные исследования показали, что применение разработанного метода более эффективно с точки зрения точности оценки коэффициента преобразования маятникового акселерометра, физическая модель которого близка к колебательной системе.

SUMMARY

Mironov V.I., Fominov I.V., Maletin A.N. **Method of the Autonomous Indirect Identification of the Conversion Factor of Pendulum Compensating Accelerometer Under the Conditions for the Orbital Flight of Automatic Spacecraft.**

At present the developments of the built-in means of control and diagnosis into the measuring devices of the systems of navigation and determination of the orientation of automatic spacecraft are actively conducted, i.e., development of the so-called smart sensors, including pendulum accelerometers.

A change in the parameters of pendulum accelerometers leads to deviation of its conversion factor, which is one of the fundamental metrological characteristics of accelerometers. This produces an increase in the error of measurement of the apparent acceleration, and, therefore, determination of the automatic spacecraft's apparent velocity increment in the regime of maneuver.

The determination of the conversion factor of accelerometers is, as a rule, accomplished under laboratory conditions on the specialized stands. However, under the conditions for orbital flight this task is complex both from the scientific and technical side.

The article proposes the indirect method of the autonomous identification of the conversion factor of pendulum accelerometer on the basis of the known graphical analyses of the identification of the parameters of the systems of the second order, presented in work, and also the methods of diagnostics, based on creation in the feedback loop of a priori diagnostic test signals.

These methods are based on the application of step input on the system and the analysis of the transient processes of output signal. Taking into account that the mathematical model of pendulum accelerometer can be approximately described by the system of the second order, it is possible to make a conclusion about the possibility in principle of the identification of some parameters by the built-in firmware means of this gauge, as well as about the identification of conversion factor.

The developed method of the autonomous indirect identification of conversion factor can be used for conducting current diagnostics of the fitness for work of pendulum accelerometers in the process of the flight of automatic spacecraft. This contributes to the calculation of the degradation of metrological characteristics and to an increase in the accuracy of determination of the automatic spacecraft's apparent velocity increment in the regime of the accomplishment of maneuvers.

The proposed method can be applied both to the aperiodic and to the oscillatory systems of the second order. The conducted investigations have shown that the application of the developed method is more effective in respect to the accuracy of estimate of the conversion factor of the pendulum accelerometer, whose physical model is close to the oscillatory system.

УДК 004.7

Р.Р. Фаткиева, Д.К. Левоневский

ПРИМЕНЕНИЕ БИНАРНЫХ ДЕРЕВЬЕВ ДЛЯ АГРЕГАЦИИ СОБЫТИЙ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Фаткиева Р.Р., Левоневский Д.К. **Применение бинарных деревьев для агрегации событий систем обнаружения вторжений.**
Аннотация. В статье рассматривается проблема выбора алгоритмов и структур данных для эффективной обработки событий, производимых системами обнаружения вторжений. Предложен подход к выполнению операций добавления и поиска записей с использованием сбалансированных бинарных деревьев. Приведено теоретическое и экспериментальное подтверждение эффективности разработанного подхода.
Ключевые слова: информационная безопасность, структуры данных, системы обнаружения вторжений, сетевой трафик, сетевые аномалии.

Fatkieva R.R., Levonevskiy D.K. **Application of Binary Trees for the IDS Events Aggregation Task.**
Abstract. This paper considers the problem of a choice of algorithms and data structures to achieve the effective processing of events generated by intrusion detection systems. The proposed approach is based on balanced binary trees and speeds up the operations of adding and searching records in the structure. The paper provides the theoretical and experimental confirmation of the efficiency of the developed approach.
Keywords: information security, data structures, intrusion detection systems, network traffic, network anomalies.

1. Введение. Использование крупными предприятиями межсетевых экранов, систем обнаружения атак, антивирусных средств не всегда приводит к полному пониманию процессов, происходящих в сетевой инфраструктуре. Проблема обеспечения безопасности в крупных системах имеет свои особенности. В частности, следует учитывать требования безопасности, связанные с использованием виртуализации (гипервизоров), регулировкой трафика между узлами комплекса, управлением правами доступа, определением периметра сети и его защитой. Конкретные технологии и решения для защиты распределенных систем ориентированы на узкий спектр решаемых задач. Поэтому для решения проблем безопасности в распределенных информационных системах применяют метод системной интеграции, использование которого значительно снижает количество инцидентов безопасности [1, 2]. Несмотря на это, остаются проблемы, которые требуют тщательного анализа и проработанного решения. В частности, сигнатурный и поведенческий анализ, реализованный в системах обнаружения вторжений, не всегда достаточен для детектирования новых видов угроз в автоматическом режиме. В этой ситуации, помимо применения средств активного обнаружения угроз, необходимо вести непрерывный мониторинг сетевой инфраструктуры на предмет ее нештатного функ-

ционирования, также называемого аномальной активностью. Критерии аномальной активности размыты, и ее выявление требует участия специалиста по информационной безопасности, которому должна быть предоставлена статистическая информация о сетевой активности в виде, удобном для оценки [4].

Проблема усугубляется тем, что исследуемые системы в силу своей масштабируемости содержат значительное число активно обменивающихся данными узлов, а применяемые средства анализа сетевой активности генерируют чрезмерное количество событий. К примеру, это относится к распространенным системам мониторинга и обнаружения вторжений Snort [3], Bro IDS, OSSEC HIDS, Ganglia и др. Все это приводит к возможности потери или недооценке важности отдельных событий. Для упорядочивания множества событий, протекающих в компьютерных системах, с целью их дальнейшего анализа необходимо рассмотреть существующие методы агрегации. Проблема заключается в ограниченности методов и средств анализа и визуализации приведенных выше данных о системных и сетевых событиях с точки зрения информационной безопасности.

2. Анализ релевантных работ. На практике обработка событий, происходящих в информационных системах, основана на решении двух типов задач: *классификации событий и эффективного хранения и поиска событий*.

Для классификации событий используются различные методы. Основные из них:

— классификация с помощью деревьев решений;
— байесовская (наивная) классификация;
— классификация при помощи искусственных нейронных сетей;
— классификация методом опорных векторов;
— статистические методы, в частности, линейная регрессия;
— классификация при помощи метода ближайшего соседа;
— классификация CBR-методом;
— классификация при помощи генетических алгоритмов.

В работе [4] рассмотрены методы классификации на основе статистической модели поведения протокола прикладного уровня, а также на основе использования наивных байесовских моделей, идентификации приложений на основе изучения распределения размеров пакетов для сетевых пакетов, на основе профилей приложений. Интерес работы вызывает сравнение классификации по скорости, эффективности и стабильности. Показано, что на качество классификации влияют такие факторы, как важность выбора набора непротиворечивых и не-

избыточных атрибутов, чувствительность к выбору предполагаемых параметров распределения значений атрибутов внутри классов.

В работе [5] рассмотрены динамические байесовские модели, модели ближайших k-соседей, методы опорных векторов, проведен анализ существующих методов машинного обучения сетевых угроз, применимых для решения задачи обнаружения сетевых атак. Интерес представляет сравнение количества обнаружения и процессов ложных срабатываний для указанных моделей. Рассмотрен метод опорных векторов, при этом для минимизации размерности и повышения скорости обучения в качестве предобработки предложен метод главных компонент, который позволяет снизить время работы алгоритма.

Вызывает интерес подход, представленный в работе [6], как возможность агрегации и классификации событий, происходящих в сети. Решение задачи обнаружения вторжений основано на применении алгоритма AntMiner+. Конечный результат обнаружения может быть представлен в виде набора составных частей определенного вида, что позволяет в том числе определить сигнатуру атаки. С каждым набором составных частей ассоциируется вершина графа. Это позволяет при оценке характеристик нормальных событий в компьютерной системе вершины (узлы) рассматриваемого графа исключать их из рассмотрения за счет наложения ограничений (равенство значения характеристики фиксированному значению, принадлежность некоторому интервалу значений). Такой подход позволяет построить ограничения, выделяющие из непрерывного потока смешанных данных элементы, принадлежащие только целевому множеству, решая тем самым задачу обнаружения той или иной аномалии. Однако метод имеет ограничения применения к системам, требующим оперативного реагирования и в задачах, требующих высокой точности результатов в связи с низкой скоростью обработки информации. Как утверждают авторы, модификация алгоритма путем оптимизации расчета эвристики, вероятностей и качества решений позволит получить более точные результаты. Применение данного метода также возможно в системах отложенного аудита.

В работах [7, 8] исследовано применение нейронных сетей для обнаружения вторжений. Использование бинарной классификации сетевых пакетов с разделением на классы на классы «норма» / «атака» показали возможность использования сетей прямого распространения функций в многоклассовом случае.

Для решения задачи упорядочивания событий применяются алгоритмы хранения и обработки множеств однотипных и логически связанных данных, которые основаны на структурах данных. Тради-

ционно к таким структурам данных относятся: массивы, списки (связные списки, очереди, стеки), деревья, которые являются простыми в исполнении. Однако при выборе алгоритма скорость добавления и поиска является критической. Использование массивов требует поддержки массива в отсортированном состоянии для ускорения поиска. Сложность поиска становится в таком случае логарифмической, а скорость вставки остается линейной. Ввиду большого количества событий использование отсортированных массивов для решения поставленной задачи по этой причине неприемлемо. При использовании связанных списков операция вставки имеет константную сложность, но операция поиска становится линейной.

Оптимальным с точки зрения скорости является применение сбалансированных бинарных деревьев, так как это позволяет осуществить операции вставки и поиска элемента в бинарном дереве по ключу и имеет логарифмическую сложность.

3. Оценка использования структур данных для алгоритма агрегации событий. Реализация алгоритма с использованием обычных массивов приводит к тому, что сложность алгоритма в среднем случае будет $O(N^3)$, где N - количество записей в файле. Действительно, для каждой записи будет производиться линейный поиск в массиве групп, при обнаружении необходимой группы для каждого из наборов будет производиться линейный поиск требуемого элемента.

Два последовательных линейных списка поиска для одной записи дают сложность $O(X)\,O(Y)$, где X - количество групп, а Y - среднее количество элементов в каждом наборе адресов/портов. Но так как вся совокупность событий (N) разделяется на объединение непересекающихся множеств (групп), то X можно выразить через N:

$$X = x \cdot N,$$

где x - константа, обратная среднему количеству элементов в группе. Аналогично, Y тоже находится в линейной зависимости от N. В итоге, для одной записи получаем сложность обработки $O(N^2)$, для всех записей – $O(N^3)$.

Выделим следующие основные признаки применительно к оценке событий происходящих при передаче информационных потоков:

— номер правила, по которому сгенерировано событие – signature id;

— адрес источника события— ip source и source port;

— адрес цели события — ip destination и destination port;

— дата происхождения события.

Используя тот или иной признак за основу, можно объединять события в группы. Например, если взять за основной признак адрес источника события, то в одной группе окажутся все события с одинаковым адресом источника события, а вся совокупность событий разобьется на объединение непересекающихся групп событий (рисунок 1).

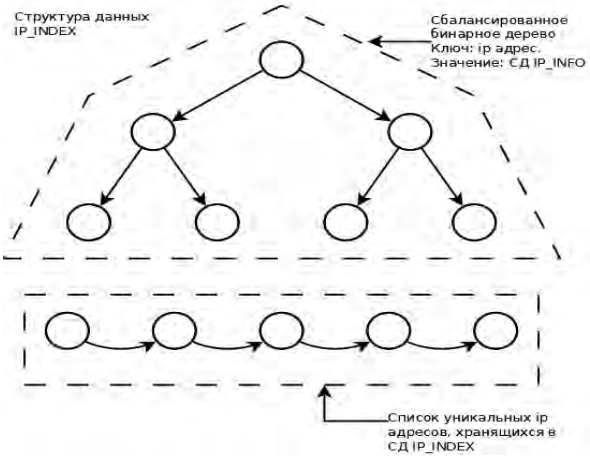


Рис. 1. Бинарное дерево с IP-адресом в качестве ключа

Однако стоит заметить, что если брать за основной признак адреса узлов сети или дату происхождения событий, то можно получить внушительное количество групп: количество узлов сети, адресуемое протоколом IPv4, равно нескольким миллиардам. В связи с этим целесообразно рассматривать как основной признак значение signature id — каждая группа будет соответствовать одному конкретному типу события, например, одному из видов сканирования портов. Бинарное дерево строится так, что в левом поддереве каждого элемента располагаются записи с меньшим значением signature id, в правом поддереве – с большим. Расположение элементов в бинарном дереве никак не связано с классификацией событий и их связью друг с другом.

Такой подход позволяет хранить все события, которые относятся к группам, каждая из которых будет соответствовать ровно одному типу событий. Если в каждой группе также произвести разбиение по другим признакам, то получим двухуровневую структуру. В качестве примера — на верхнем уровне события делятся на группы по типу события; на нижнем уровне в каждой группе два набора адресов и два набора портов делятся на группы по признаку адреса или порта, хранящие в себе количество событий с этими адресами/портами, а также временной интервал, в течение которого происходили события данно-

го типа. Такое структурирование позволяет быстро и эффективно проанализировать все сгенерированные сообщения о событиях.

4. Тестирование. Для оценки возможности использования сбалансированного бинарного дерева была разработана программная реализация метода. При тестировании применены материалы крупнейшей в мире конференции DEFCON, на официальном сайте которой доступны дампы сетевого трафика [9]. Результаты тестирования производительности программы на компьютерах с процессорами разной производительности представлены в таблицах 1 и 2. В таблицах приводится время построения бинарного дерева для исходного множества событий, т. е. время агрегации событий.

Таблица 1. Тестирование программы на реальных данных, процессор: Intel Core 2 Duo

Количество событий в файле (в миллионах)	Время работы программы (ms)
0.2	250
0.3	380
0.4	550
0.5	680
0.6	800
1.0	1260
1.8	2220
3.654978	4490
10.456365	14220
14.619912	17710
18.375484	24060

Файл для тестирования содержит 36 миллионов записей и имеет размер больше двух гигабайт. В качестве примера приведем, что для генерации такого файла из исходных 800 Гб дампов сетевого трафика системе обнаружения Snort потребовалось около 10 часов.

Таблица 2. Тестирование программы на реальных данных, процессор: Intel Core i3

Количество событий в файле (в миллионах)	Время работы программы (ms)
0.279322	232
0.609163	340
1.827489	1067
3.654987	2109
7.309956	4139
10.456365	6286
14.619912	8276
18.375484	10994

Зависимости времени работы от количества событий на разных процессорах и разных наборах данных приведены на рисунке 2.

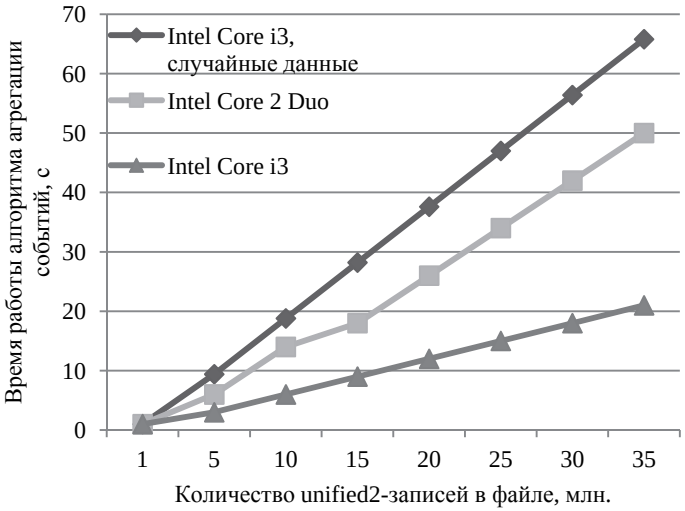


Рис. 2. Зависимость времени работы программы от процессора и исходных данных

Ранее при выборе структуры данных для эффективной реализации разработанного метода агрегации событий упоминалась возможность использования таких структур данных, как отсортированные массивы и линейные списки. Рассмотрим реализации алгоритма, использующего отсортированные массивы или линейные списки как структуру данных. Тестирование на производительность этих двух реализаций производилось на тестах, соответствующих худшему случаю (т. е. случайной выборке данных). В таблицах 3 и 4 представлены результаты этого тестирования.

Таблица 3. Тестирование производительности реализации алгоритма с использованием отсортированных массивов

Количество событий в файле (в миллионах)	Время работы программы (ms)
0.099855	2990
0.199808	8628
0.299754	16319
0.399423	25183
0.499848	35500
0.599848	47299
0.699730	59513
0.799235	74199
0.899650	88374
0.999000	103493

Последняя строка таблицы 3 показывает, что 1 миллион записей был обработан за 103,5 секунды, что в 50 раз медленнее аналогичного времени обработки записей на бинарных деревьях.

Таблица 4. Тестирование производительности алгоритма на основе линейных списков

Количество событий в лог файле (в миллионах)	Время работы программы (ms)
0.099855	1056
0.199808	2969
0.299754	5637
0.399423	8530
0.499848	11977
0.599848	16941
0.699730	20489
0.799235	25605
0.899650	34682
0.999000	35333
10.999170	1558871 (примерно 26 минут)

Для наглядного сравнения различных реализаций приведем графики времени обработки записей в зависимости от их количества (рисунок 3) при использовании различных алгоритмов обработки.

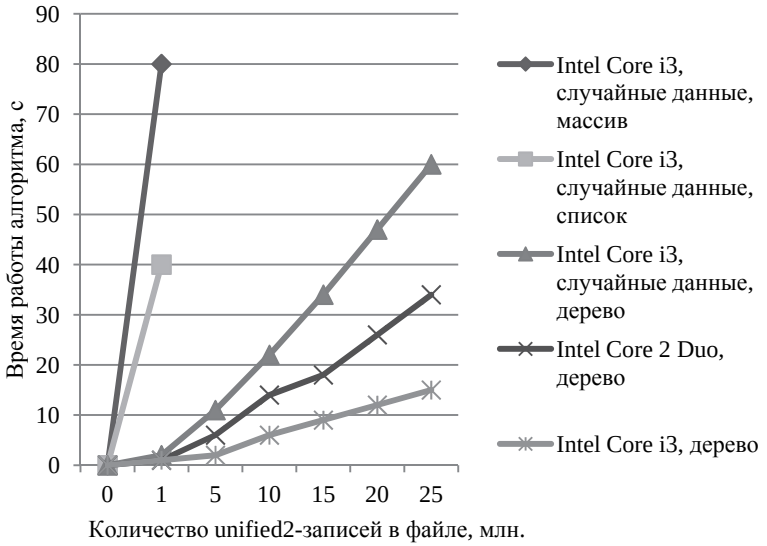


Рис. 3. Скорость обработки событий для различных алгоритмов

5. Заключение. Для организации эффективной обработки и быстрого доступа к базам событий критически важно найти такие структуры данных и алгоритмы, которые обеспечивают максимальную скорость добавления и поиска записей. Исследование показало, что этому условию соответствуют алгоритмы, основанные на бинарных деревьях, которые позволяют сделать сложность вышеприведенных операций логарифмической, что обеспечивает меньшее время работы по сравнению с аналогами.

Недостатком предлагаемого подхода является повышенное использование оперативной памяти. Этот недостаток может быть устранен путем использования баз данных на основе технологии NoSQL [10], которые позволяют организовывать базы данных с древовидной структурой.

Литература

1. *Котенко И. В., Юсупов Р. М.* Текущее состояние и тенденции развития в области построения безопасных компьютерных систем // Часть 5-й Российской мультиконференции по проблемам управления (МКПУ-2012) – конференция "Информационные технологии в управлении" (ИТУ-2012). Материалы конференции. СПб. 2012. С. 671–675.
2. *Левоневский Д.К., Фаткиева Р.Р.* Разработка системы обнаружения аномалий сетевого трафика // Научный вестник Новосибирского государственного технического университета. 2014. № 3(56). С. 108–114.
3. *Szmit M., Węży k R., Skowroński M., Szmit A.* Traffic Anomaly Detection with Snort // Information Systems Architecture and Technology. Information Systems and Computer Communication Networks. Wrocław: Wydawnictwo Politechniki Wrocławskiej. 2007. pp. 181–187.
4. *Щербакова Н.Г.* Анализ IP-трафика методами Data Mining. Проблема классификации // Вычислительные и сетевые ресурсы. URL: http://problem-info.sscc.ru/2012-4/5.pdf (дата обращения: 17.02.2015).
5. *Носков А.Н., Чечулин А.А, Тарасова Д.А.* Исследование эвристических подходов к обнаружению атак на телекоммуникационные сети на базе методов интеллектуального анализа данных // Труды СПИИРАН. 2014. Вып. 37. С. 208–224.
6. *Таран А.А.* Приложения алгоритма Antminer+ к задаче классификации событий при анализе сетевого трафика // Известия ЮФУ. Технические науки. 2012. № 12(137). С. 60–67. URL: http://cyberleninka.ru/article/n/prilozheniya-algoritma-antminer-k-zadache-klassifikatsii-sobytiy-pri-analize-setevogo-trafika (дата обращения: 17.02.2015).
7. *Swimmer M.* Using the danger model of immune systems for distributed defense in modern data networks // Computer Networks. 2007. vol. 51. pp. 1315–1333.
8. *Клионский Д.М., Большев А.К., Геппенер В.В.* Применение искусственных нейронных сетей в сетевых технологиях // Нейроинформатика. 2011.
9. DEF CON Hacking Conference. URL: https://www.defcon.org/ (дата обращения: 17.02.2015).

10. *Ohene-Kwofie D., Otoo E.J., Nimako G.* O2-Tree: A Fast Memory Resident Index for NoSQL Data-Store // Proceedings of the 2012 IEEE 15th International Conference on Computational Science and Engineering (CSE). 2012. pp. 50–57.

References

1. Kotenko I. V., Yusupov R. M. [Current situation and trends of secure computer system development]. *Chast' 5-j Rossijskoj mul'tikonferencii po problemam upravlenija (MKPU-2012) – konferencija "Informacionnye tehnologii v upravlenii" (ITU-2012)* [5th part of Russian multiconference on management problems (MKPU-2012) – conference "Information Technologies in Management" (ITU-2012)]. Saint-Petersburg. 2012. pp. 671–675. (In Russ.).
2. Levonevskiy D.K., Fatkieva R.R. [Development of network anomaly detection system architecture]. *Nauchnyj vestnik Novosibirskogo gosudarstvennogo tehnicheskogo universiteta – Bulletin of Novosibirsk State Technical University*. 2014. vol. 3(56). pp. 108–114. (In Russ.).
3. Szmit M., Wężyk R., Skowroński M., Szmit A. Traffic Anomaly Detection with Snort. *Information Systems Architecture and Technology. Information Systems and Computer Communication Networks*. Wrocław: Wydawnictwo Politechniki Wrocławskiej. 2007 pp. 181–187.
4. Shcherbakova N.G. [IP traffic analysis by means of Data Mining. Classification problem]. *Vychislitel'nye i setevye resursy – Computational and network resources*. Available at: http://problem-info.sscc.ru/2012-4/5.pdf (accessed: 17.02.2015). (In Russ.).
5. Noskov A.N., Chechulin A.A, Tarasova D.A. [Research of heuristic approaches to the network attack detections on the basis of intellectual data analysis]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2014. vol. 37. pp. 208–224. (In Russ.).
6. Taran A.A. [Applications of Antminer+ algorithm to the task of network events classification]. *Izvestija JuFU. Tehnicheskie nauki – UFU Proceedings. Technical science*. 2012. vol. 12(137). pp. 60–67. Available at: http://cyberleninka.ru/article/n/prilozheniya-algoritma-antminer-k-zadache-klassifikatsii-sobytiy-pri-analize-setevogo-trafika (accessed: 17.02.2015). (In Russ.).
7. Swimmer M. Using the danger model of immune systems for distributed defense in modern data networks. *Computer Networks*. 2007. vol. 51. pp. 1315–1333.
8. Klionskiy D.M., Bolshev A.K., Geppener V.V. Primenenie iskusstvennykh nejronnykh setej v setevykh tekhnologiyakh [Application of artificial neural networks in ICT]. *Nejroinformatika - Neuroinformatics*, 2011. (In Russ.).
9. DEF CON Hacking Conference. Available at: https://www.defcon.org/ (accessed: 17.02.2015).
10. Ohene-Kwofie D, Otoo E.J., Nimako G. O2-Tree: A Fast Memory Resident Index for NoSQL Data-Store. Proceedings of the 2012 IEEE 15th International Conference on Computational Science and Engineering (CSE). 2012. pp. 50–57.

Фаткиева Роза Равильевна — к-т техн. наук, доцент, старший научный сотрудник лаборатории информационно-вычислительных систем и технологии программирования, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: моделирование информационных систем. Число научных публикаций — 50. rrf@iias.spb.su; 14-я линия В.О., д. 39, Санкт-Петербург, 199178; р.т.: +7-812-328-43-69, Факс: +7 (812)350-1113.

Fatkieva Roza Ravilievna — Ph.D., associate professor, senior researcher of computer and information systems and software engineering laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: modeling of information systems. The number of publications — 50. rrf@iias.spb.su; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7-812-328-43-69, Fax: +7 (812)3501113.

Левоневский Дмитрий Константинович — младший научный сотрудник лаборатории информационно-вычислительных систем и технологии программирования, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: исследование сетевых атак, статистический анализ и моделирование трафика локальных сетей. Число научных публикаций — 10. DLewonewski.8781@gmail.com; 14-я линия В.О., д. 39, Санкт-Петербург, 199178; р.т.: +7-812-328-43-69, Факс: +7 (812)350-1113.

Levonevskiy Dmitriy Konstantinovich — junior researcher of computer and information systems and software engineering laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: network attacks research, statistical analysis and modeling of the network traffic. The number of publications — 10. DLewonewski.8781@gmail.com; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7-812-328-43-69, Fax: +7 (812)350-1113.

РЕФЕРАТ

Фаткиева Р.Р., Левоневский Д.К. **Применение бинарных деревьев для агрегации событий систем обнаружения вторжений.**

Методы, реализованные в системах обнаружения вторжений, не всегда достаточны для обнаружения новых видов угроз в автоматическом режиме. В этой ситуации, помимо применения средств активного обнаружения угроз, необходимо вести мониторинг сетевой инфраструктуры на предмет фактов подозрительной активности. Ее выявление требует участия специалиста по информационной безопасности, которому должна быть предоставлена статистическая информация о сетевой активности в виде, удобном для оценки.

Для упорядочивания множества событий IDS с целью их дальнейшего анализа рассматриваются различные структуры данных: массивы, списки, деревья. При выборе структуры данных критическим параметром является скорость алгоритма добавления и поиска.

Оптимальным с точки зрения скорости является применение сбалансированных бинарных деревьев, так как это позволяет осуществить операции вставки и поиска элемента в бинарном дереве по ключу и имеет логарифмическую сложность. Программная реализация подтверждает эффективность разработанного подхода по сравнению с аналогами.

Недостатком предлагаемого подхода является повышенное использование оперативной памяти. Этот недостаток может быть устранен путем использования баз данных на основе технологии NoSQL, которые позволяют организовывать базы данных с древовидной структурой.

SUMMARY

Fatkieva R.R., Levonevskiy D.K. **Application of Binary Trees for the IDS Events Aggregation Task.**

The methods implemented in intrusion detection systems are often not sufficient to detect new types of threats in the automatic mode. Therefore, one should, besides using intrusion detection and prevention systems, monitor the network infrastructure for any suspicious traffic. This activity needs the participation of an information security specialist who should be provided with the network statistics in a convenient form.

This paper considers various data structures (arrays, linked lists, binary trees) to put the variety of IDS events in order for their further analysis. When choosing data structure the critical parameter is the speed of the algorithm for adding and search.

The usage of balanced binary trees is optimal regarding the speed criterion because it enables performing the tasks of adding and searching in a tree using a key and guarantees the logarithmical complexity of these operations. The implementation of the algorithm proves the efficiency of this approach in comparison with other data structures.

The disadvantage of the proposed approach is the high use of the random access memory. This disadvantage can be eliminated by using the NoSQL technology that enables organizing tree-type databases.

УДК 004.056

А.В. Иванов, В.А. Трушин, В.Е. Хиценко

О ВЫБОРЕ МОДЕЛИ ТЕСТОВОГО СИГНАЛА ПРИ ОЦЕНКЕ ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Иванов А.В., Трушин В.А., Хиценко В.Е. **О выборе модели тестового сигнала при оценке защищенности речевой информации от утечки по техническим каналам.**
Аннотация. Производится переоценка базовых зависимостей, лежащих в основе методики оценки защищенности речевой информации от утечки по техническим каналам. Описывается постановка и результаты эксперимента по определению формантного распределения для случаев обычной и форсированной речи. Используя данные распределения возможно определить вклады частотных полос в суммарную разборчивость речи. Получена зависимость словесной разборчивости от формантной для случая форсированной речи. Проведен эксперимент по определению амплитудного состава речи, по результатам которого сделаны выводы о достаточных уровнях тестового сигнала при проведении оценки защищенности речевой информации.
Ключевые слова: разборчивость речи, тестовый сигнал, амплитудный состав речи, формантное распределение.

Ivanov A.V., Trushin V.A., Khitcenko V.E. **Choice of Model of Test Signal at an Assessment of Security of Speech Information from Leakage through Technical Channels.**
Abstract. Revaluation of the basic dependences which are used in the method of an assessment of security of speech information from leakage through technical channels is made. The statement and results of experiment for definition of formant distribution for cases of the usual and forced speech are described. Using these distributions it is possible to define contributions of frequency bands to total legibility of speech. Dependence of word legibility on formant legibility for a case of forced speech is received. The paper presents an experiment to determine amplitude structure of the speech by results of which conclusions of sufficient levels of a test signal are drawn for an assessment of security of speech information.
Keywords: legibility of the speech, test signal, amplitude structure of the speech, formant distribution.

1. Введение. В помещениях, предназначенных для проведения переговоров, возможна утечка речевой информации по техническим каналам (акустический, вибрационный, акустоэлектрический). Оценку защищенности речевой информации принято производить по методике [1], основанной на формантном подходе [2]. Количественным критерием защищенности в данной методике является словесная разборчивость. В последнее время в ряде работ обсуждается возможность усовершенствования данной методики с учетом специфики задач защиты информации (ЗИ) [3, 4, 5]. При этом, в качестве тестового сигнала, имитирующего диктора, принято использовать широкополосный сигнал (белый шум) с огибающей спектра соответствующей речевому сигналу и интегральным уровнем равным 70дБ (спокойная речь). Вме-

сте с тем, в процессе дискуссии часто бывают ситуации, когда возникает эффект форсирования речи (например, когда говорящие пытаются перекричать друг друга).

Еще одним важным фактором является выбор уровня тестового сигнала. Данный уровень возможно определить по известной функции распределения амплитудного состава речи [2, с. 115 (рисунок 5.6), с. 152 (рисунок 6.17)]. Так в работе [5], на основе анализа данной функции, делается вывод о целесообразности задания определенной вероятности обеспечения требуемого уровня защищенности с последующим нахождением соответствующего этой вероятности интегрального уровня речи. Так, для вероятности 0,95 обеспечения заданного показателя защищенности W необходим интегральный уровень тестового сигнала в 85 дБ. Однако, необходимо отметить, что используемые зависимости были получены Покровским Н.Б. для условий, существенно отличающихся от задач ЗИ: так, расстояние от источника звука до микрофона принималось равным 8 см (в обсуждаемой методике требуется 1 м), за средний уровень речи принято 82 дБ (а не 70 дБ), амплитудное распределение форсированной речи не исследовалось вообще.

Таким образом, для корректировки методики [1] как для случая спокойной (нормальной) речи, так и при возникновении эффекта форсирования, необходимо определить амплитудный состав речи, по которому можно будет сделать вывод о выборе достаточного уровня тестового сигнала. Также для случая форсирования необходимо определение зависимости разборчивости формант от частоты, что позволяет пересчитать весовые коэффициенты вклада в суммарную разборчивость частотных полос и влечет за собой изменение зависимости словесной разборчивости от формантной.

2. Формантное распределение. Экспериментальное определение формантного распределения (зависимость разборчивости формант от частоты) производится аналогично экспериментам Покровского [2, с. 146], но с использованием связных текстов, а не слоговых таблиц, как для спокойной речи, так и в случае форсирования. Пересмотр данного распределения также влечет за собой изменение зависимости словесной разборчивости от формантной. Эффекта форсирования добивались путем воздействия на диктора шумом через наушники (для исключения влияния этого шума на запись). Подробно данная часть эксперимента изложена в работе [6].

Эксперимент заключается в следующем:

– для каждой записи речи диктора при прослушивании аудитором с применением НЧ и ВЧ фильтров определяется такая частота сре-

за фильтров f_0, чтобы полученные после фильтрации две записи, включающие частоты от 90 Гц до f_0 и от f_0 до10 кГц, обладали одинаковой словесной разборчивостью речи;

– полагается, что, поскольку формантная разборчивость (R) обладает свойством аддитивности, каждая из полученных записей будет обладать формантной разборчивостью $R = 0.5$;

– параллельно с этим определяется и словесная разборчивость (W) полученных записей;

– далее каждая из полученных записей подвергается повторно подобному анализу, только теперь каждая из «четвертинок» будет обладать формантной разборчивостью $R = 0.25$ и т.д.

Следует отметить, что под словесной разборчивостью понимается количество правильно принятых слов при использовании связных текстов, тогда как у Покровского данный термин обозначал количество правильно принятых слов при использовании некоррелированных таблиц слов.

Работа в частотной области анализируемых записей речи производилась с использованием ПО Adobe Audition. В исследовании использовались 8 записей речи дикторов (4 мужских и 4 женских, как для спокойной, так и для форсированной речи), каждую из которых проанализировали 4 аудитора. Результаты эксперимента представлены на рисунке 1. Для сравнения приводится функция распределения, используемая в методике.

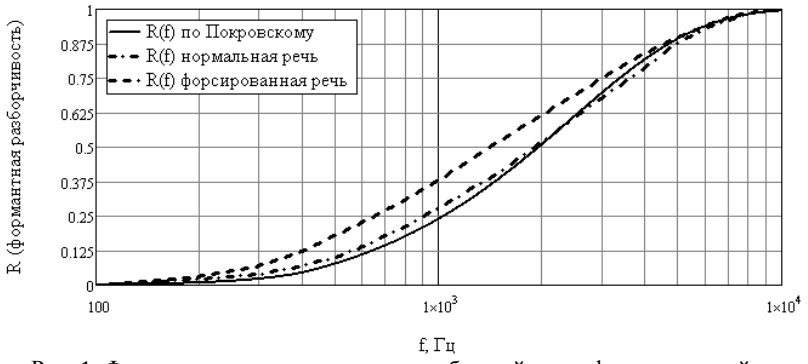


Рис. 1. Формантное распределение для обычной речи, форсированной и используемое в общепринятой методике

Полученная зависимость для обычной речи практически совпала с результатами Покровского Н.Б., а для форсированной существенно отличается, что требует пересчета значений весовых коэффициентов вклада в суммарную разборчивость частотных полос.

3. Зависимость словесной разборчивости от формантной. Вторым результатом данного эксперимента являются приведенные на рисунке 2 зависимости словесной разборчивости от формантной *W(R)*.

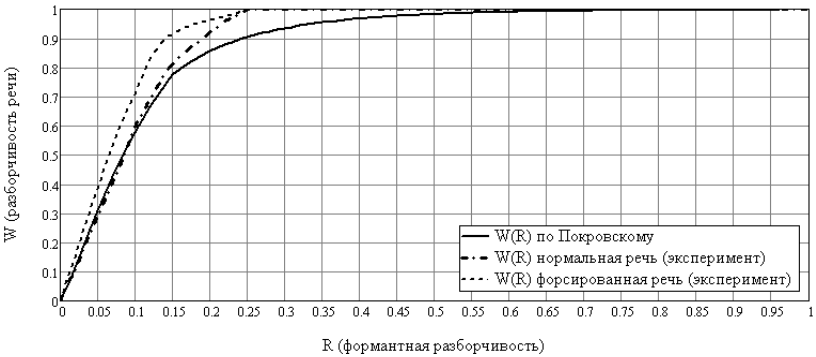


Рис. 2. Зависимости словесной разборчивости от формантной для обычной речи, форсированной и используемая в общепринятой методике

При проведении работ по оценке защищенности речевой информации, диапазон значений разборчивости речи, представляющий интерес для задач защиты информации, составляет от 0,1 до 0,6. По результатам опубликованных исследований [7], можно сделать вывод о том, что при словесной разборчивости выше 0,6 возможно составить подробную справку о содержании переговоров, при разборчивости же меньше 0,1 чаще всего уже невозможно даже установить сам предмет разговора. Исходя из этого, предлагается ограничить зависимости $W(R)$ и линеаризовать их (рисунок 3).

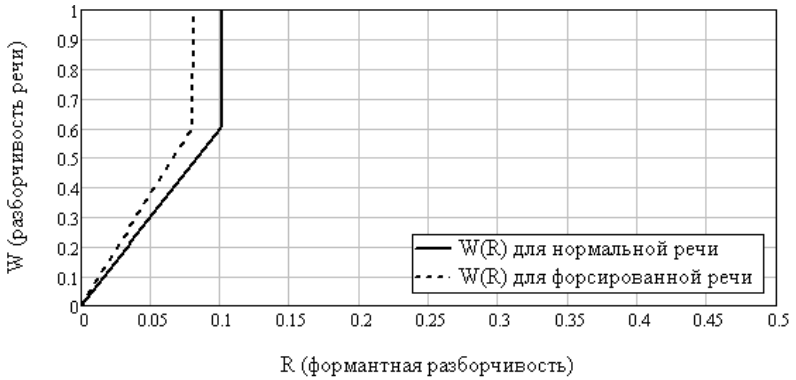


Рис. 3. Зависимости словесной разборчивости речи от формантной для обычной и форсированной речи

В аналитической форме зависимость для обычной речи выражается следующим образом:

$$W(R) = \begin{cases} 6 \cdot R, если\ R \le 0{,}1; \\ 1, если\ R > 0{,}1. \end{cases}, \quad (1)$$

для форсированной:

$$W(R) = \begin{cases} 7{,}5 \cdot R, если\ R \le 0{,}08; \\ 1, если\ R > 0{,}08. \end{cases}. \quad (2)$$

4. Амплитудный состав речи. Амплитудный состав речи анализировался аналогично эксперименту, приведенному у Покровского Н.Б. [2, с. 148]. Для исследования были созданы записи 8 дикторов (4 мужчины и 4 женщины) с обычной и форсированной речью. Запись производилась с использованием шумомера ZET 110 и микрофона BC501 с частотой дискретизации 50 кГц. Длительность каждой из записей составляла 600 с. Из-за большого количества отсчетов обработка производилась частями по 100 с.

Эксперимент заключается в следующем:

– по полученным отсчетам находятся среднеквадратичные значения на интервалах времени по 0,125 с;

– динамический диапазон полученных значений разбивается на коридоры шириной по 1дБ (относительно порога слышимости 20 мкПа);

– рассчитывается количество попаданий среднеквадратичных значений в каждый из коридоров;

– строятся гистограммы (рисунки 4, 5) и функции распределения (рисунок 8).

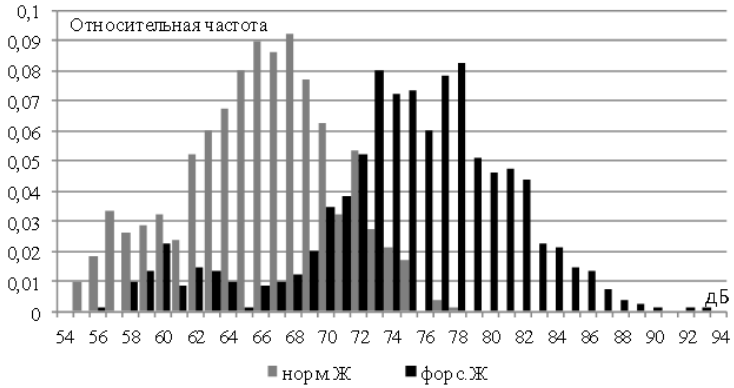


Рис. 4. Гистограммы распределения нормальной и форсированной речи дикторов женщин

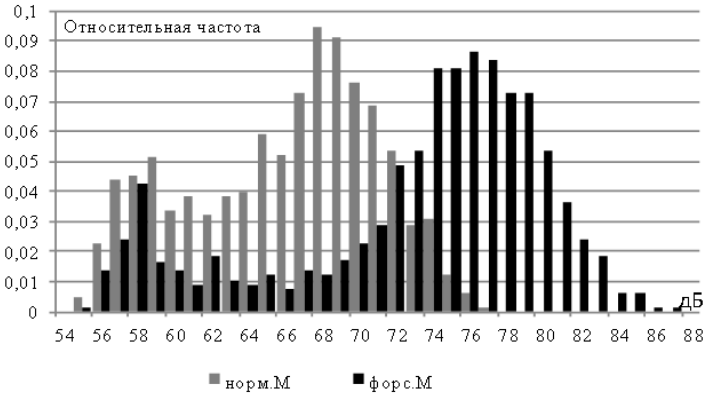


Рис. 5. Гистограммы распределения нормальной и форсированной речи дикторов мужчин

Внешний вид гистограмм позволяет предположить модель амплитудного состава речи на фоне естественного шума в виде смеси двух близких к гауссовским законов распределения.

Механизм, порождающий такую смесь, по-видимому, выглядит так. В некоторых интервалах усреднения ($\Delta t = 0{,}125c$) речь диктора не звучала, и долю таких пауз, где слышен только шумовой фон, обозначим α. Остальная доля измерений $(1-a)$ это аддитивная сумма речевого и шумового сигналов

Таким образом, имеем гипотезу: плотность состава речи равна:

$$f(x, m_1, m_2, \sigma_1, \sigma_2, \alpha) = (1-\alpha)\varphi(x, m_1, \sigma_1) + \alpha\varphi(x, m_2, \sigma_2), \qquad (3)$$

где φ - гауссовская плотность, (m_1, σ_1) и (m_2, σ_2) – параметры закона речи и шума соответственно, α - доля шумовой составляющей.

На рисунке 6 показаны гистограмма амплитудного состава нормальной речи и аппроксимирующая ее плотность вида (3), где параметры $m_2 = 57{,}70$ дБ и $\sigma_2 = 1{,}28$ дБ были предварительно оценены по выборке шумовой составляющей. Параметры $m_1 = 67{,}02$ дБ, $\sigma_1 = 4{,}10$ дБ и $\alpha = 0{,}1$ подбирались по минимуму критерию χ^2 до достижения значимости, превышающей 0,05 и не позволяющей отклонить гипотезу (3). Таким образом, паузы в этом речевом сигнале составляют примерно 10%.

В литературе [8, 9] описаны различные методы оценивания параметров смеси распределений применительно к задачам классификации. В основном это модификации метода моментов и метода максимального правдоподобия. Наиболее эффективным представляется так называемый EM-алгоритм.

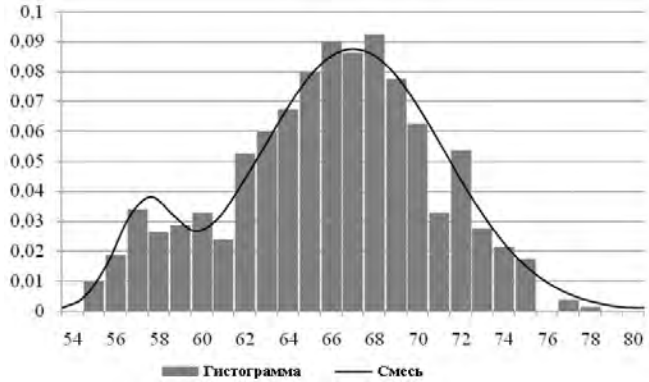


Рис. 6. Гистограмма и теоретическая плотность (смесь) нормальной речи

Оценка математического ожидания уровня смеси определяется по:

$$m = (1-\alpha)m_1 + \alpha m_2, \qquad (4)$$

и для нормальной речи составляет приблизительно *66,09дБ*.

Однако эти вопросы выходят за рамки настоящей работы. Для задачи выбора уровней тестовых сигналов достаточно сопоставить эмпирическую функцию распределения и теоретическую, найденную по:

$$f(x, m_1, m_2, \sigma_1, \sigma_2, \alpha) = (1-\alpha)\Phi(x, m_1, \sigma_1) + \alpha\Phi(x, m_2, \sigma_2), \qquad (5)$$

где Φ – функция Лапласа. Варьируя параметрами α, m_1, σ_1, добиваемся практического совпадения эмпирической и теоретической квантилей уровня 0,95. На рисунке 7 хорошо видно данное совпадение.

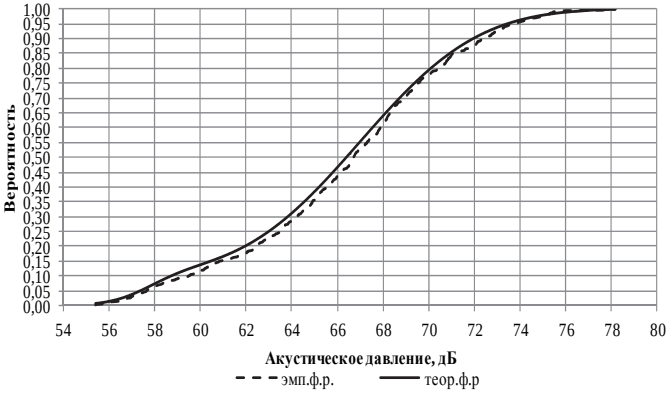


Рис.7. Эмпирическая и теоретическая функции распределения нормальной речи

Для рассмотренных четырех видов речевых сигналов (мужской спокойный, женский спокойный, мужской форсированный, женский форсированный) на рисунке 8 сведены результаты экспериментов в виде зависимостей вероятности превышения тестового сигнала от его уровня.

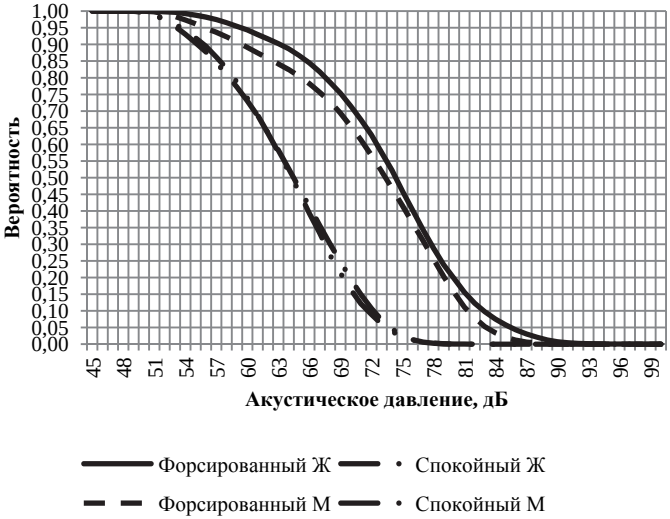


Рис. 8. Амплитудные составы спокойной и форсированной речи дикторов (мужчин и женщин)

Исходя из результатов эксперимента можно сделать выводы о том, что для обеспечения доверительной вероятности 0,95 необходимо выбирать уровни тестового акустического сигнала 74 дБ для обычной речи и 85 дБ для форсированной.

4. Заключение. Проведен пересмотр зависимостей, лежащих в основе методики оценки защищенности речевой информации [1, 2], с учетом возникновения эффекта форсирования.

Экспериментально получена функция распределения формант, существенно отличающаяся от общепринятой в случае форсирования, что указывает на то, что весовые коэффициенты (вклады частотных полос в суммарную разборчивость) при форсировании речи будут другими (увеличивается вклад низких и средних частот).

Также, по результатам данного эксперимента, получена зависимость словесной разборчивости от формантной при форсировании, существенно отличающаяся от случая спокойной речи.

Показано, что распределение уровня речевого сигнала в реальных условиях шумов может быть представлено смесью двух гауссовских законов.

Произведена экспериментальная оценка амплитудного состава как обычной, так и форсированной речи, по результатам которой были определены достаточные уровни тестовых акустических сигналов. Для обычной (спокойной) речи – 74 дБ, для форсированной – 85 дБ.

Полученные результаты и зависимости позволяют скорректировать методику оценки защищенности речевой информации с учетом уровней тестового сигнала и эффекта форсирования.

Литература

1. *Железняк В.К., Макаров Ю.К., Хорев А.А.* Некоторые методические подходы к оценке эффективности защиты речевой информации // М. Специальная техника. 2000. № 4. С. 39–45.
2. *Покровский Н.Б.* Расчет и измерение разборчивости речи // М.: Связьиздат. 1962. 390 с.
3. *Трушин В.А., Рева И.Л., Иванов А.В.* Усовершенствование методики оценки разборчивости речи в задачах защиты информации // Барнаул. Ползуновский вестник. 2012. №3/2. С. 238–241.
4. *Иванов А.В., Рева И.Л., Трушин В.А., Тудэвдагва У.* Корректировка методики оценки защищенности речевой информации от утечки по техническим каналам в условиях форсирования речи // Научный вестник Новосибирского государственного технического университета. 2014. № 2(55). С. 183–189.
5. *Авдеев В.Б.* О некоторых направлениях совершенствования методических подходов, применяемых при оценке эффективности технической защиты информации // Специальная техника. М. 2013. №2. С. 1–10.
6. *Иванов А.В., Трушин В.А., Береснева А.В., Маркелова Г.В.* Экспериментальные исследования защищенности речевой информации от утечки по техническим каналам с учетом эффекта форсирования речи // Актуальные проблемы электронного приборостроения (АПЭП-2014). Новосибирск. Изд-во НГТУ. 2014. Т. 3. С. 164–170.
7. *Хореев А.А., Макаров Ю.К.* Оценка эффективности систем виброакустической маскировки // Вопросы защиты информации. 2001. № 1. С. 21–28.
8. *Айвазян С.А. Бухштабер В.М., Енюков И.С., Мешалкин Л.Д.* Прикладная статистика. Классификация и снижение размерности // М.: Финансы и статистика. 1989. 607 с.
9. *Королев В.Ю.* ЕМ-алгоритм, его модификации и их применение к задаче разделения смесей вероятностных распределений. Теоретический обзор // М.: ИПИ РАН. 2007. 102 с.

References

1. Zheleznjak V.K., Makarov Ju.K., Horev A.A. [Some methodical approaches to an assessment of efficiency of protection of speech information]. *Special'naja tehnika – Special equipment*. 2000. vol. 4. pp. 39–45. (In Russ).
2. Pokrovskij N.B. *Raschet i izmerenie razborchivosti rechi* [Calculation and measurement of legibility of the speech]. Moscow: Svyazyizdat. 1962. 390 p. (In Russ).
3. Trushin V.A., Reva I.L., Ivanov A.V. [Improvement of a technique of an assessment of legibility of the speech in problems of information security]. *Polzunovskij vestnik – Polzunovsky messenger*. 2012. vol. 3/2. pp. 238–241. (In Russ).

4. Ivanov A.V., Reva I.L., Trushin V.A., Tudevdagva U. [Corrected methods for the assessment of audio information security against leakage through engineering channels for forced speech]. *Nauchnyj vestnik Novosibirskogo gosudarstvennogo tehnicheskogo universiteta – Science bulletin of the Novosibirsk state technical university*. 2014. vol. 2(55). pp. 183–189. (In Russ).
5. Avdeev V.B. [About some directions of improvement of the methodical approaches applied at an assessment of efficiency of technical information security]. *Special'naja tehnika – Special equipment*. 2013. vol. 2. pp. 1–10. (In Russ).
6. Ivanov A.V., Trushin V.A., Beresneva A.V., Markelova G.V. [The experimental research of security of speech information of leakage from technical channels with account of forcing speech effect] *Aktual'nye problemy jelektronnogo priborostroenija (APJeP-2014)* [Actual problems of electronic instrument engineering (APEIE–2014)]. Novosibirsk. Izd-vo NGTU. 2014. Issue 3. pp. 164–170. (In Russ).
7. Horeev A.A., Makarov Ju.K. [Assessment of efficiency of systems of vibroacoustic masking]. *Voprosy zashhity informacii – Questions of information security*. 2001. vol. 1. pp. 21–28. (In Russ).
8. Ajvazjan S.A. Buhshtaber V.M., Enjukov I.S., Meshalkin L.D. *Prikladnaja statistika. Klassifikacija i snizhenie razmernosti* [Applied statistics. Classification and decrease in dimension]. Moscow: Finansy i statistika, 1989. 607 p. (In Russ).
9. Koroljov V.Ju. *EM-algoritm, ego modifikacii i ih primenenie k zadache razdelenija smesej verojatnostnyh raspredelenij. Teoreticheskij obzor.* [EM-algorithm, its modifications and their application to a problem of division of mixes of probabilistic distributions. Theoretical review.]. Moscow: IPI RAN. 2007. 102 p. (In Russ).

Иванов Андрей Валерьевич — старший преподаватель кафедры защиты информации, Новосибирский государственный технический университет. Область научных интересов: защита информации. Число научных публикаций — 15. andrej.ivanov@corp.nstu.ru; пр. К. Маркса, 20, корпус 7, Новосибирск, 630073; р.т.: +7 383 346 0853.

Ivanov Andrey Valer'evich — senior lecturer of information security department, Novosibirsk State Technical University. Research interests: information security. The number of publications — 15. andrej.ivanov@corp.nstu.ru; 20, Prospekt K. Marksa, housing 7, Novosibirsk, 630073, Russia; office phone: +7 383 346 0853.

Трушин Виктор Александрович — к-т техн. наук, заведующий кафедрой защиты информации, Новосибирский государственный технический университет. Область научных интересов: защита информации, информационно-измерительные системы. Число научных публикаций — 70. rastr89@mail.ru; пр. К. Маркса, 20, корпус 7, Новосибирск, 630073; р.т.: +7 383 346 0853.

Trushin Viktor Aleksandrovich — Ph.D., head of information security department, Novosibirsk State Technical University. Research interests: information security, information-measuring systems. The number of publications — 70. rastr89@mail.ru; 20, Prospekt K. Marksa, housing 7, Novosibirsk, 630073, Russia; office phone: +7 383 346 0853.

Хиценко Владимир Евгеньевич — к-т техн. наук, доцент, доцент кафедры защиты информации, Новосибирский государственный технический университет. Область научных интересов: социальная самоорганизация, прикладная статистика. Число научных публикаций — 60. khits@is.cs.nstu.ru; пр. К. Маркса, 20, корпус 7, Новосибирск, 630073; р.т.: +7 383 346 0853.

Khitcenko Vladimir Evgen'evich — Ph.D., associate professor, associate professor of information security department, Novosibirsk State Technical University. Research interests: social self-organization, applied statistics. The number of publications — 60. khits@is.cs.nstu.ru; 20, Prospekt K. Marksa, housing 7, Novosibirsk, 630073, Russia; office phone: +7 383 346 0853.

РЕФЕРАТ

Иванов А.В., Трушин В.А., Хищенко В.Е. **О выборе модели тестового сигнала при оценке защищенности речевой информации от утечки по техническим каналам.**

В работе рассматривается методика оценки разборчивости речи Н.Б. Покровского. Данная методика разрабатывалась для задач, условия которых существенно отличаются от условий защиты информации. Также в данном подходе не учитывается возможность возникновения эффекта форсирования речи. Все это приводит к необходимости переоценки базовых зависимостей, лежащих в основе данной методики.

В процессе оценки защищенности речевой информации используется система формирования тестового сигнала. Вопрос выбора достаточного уровня данного сигнала тоже является актуальным. А в случае форсирования речи, отсутствуют даже экспериментальные данные, на основе которых можно сделать вывод об уровне тест-сигнала.

Проставлен и проведен эксперимент по определению формантного распределения, используя которое возможно оценить вклад каждой частотной полосы в суммарную разборчивость речи. Для спокойной речи данный эксперимент проводился Н.Б. Покровским (результаты совпали), для форсированной подобная оценка была проведена впервые. Также произведена экспериментальная переоценка зависимости словесной разборчивости от формантной. В случае форсирования речи данная зависимость существенно отличается.

Проведена экспериментальная оценка амплитудного состава как обычной (спокойной) речи, так и форсированной. Опираясь на данные зависимости можно с заданной долей вероятности, например 0.95, определить достаточный уровень тестового акустического сигнала. Так, для обычной речи достаточный уровень 74дБ, для форсированной – 85дБ.

Полученные результаты позволяют существенно скорректировать методику оценки разборчивости речи, а также сформулировать методику, учитывающую эффект форсирования.

SUMMARY

Ivanov A.V., Trushin V.A., Khitcenko V.E. **Choice of Model of Test Signal at an Assessment of Security of Speech Information from Leakage through Technical Channels.**

In this work the method of an assessment of legibility of the speech by N.B. Pokrovsky is considered. This method was developed for tasks conditions of which significantly differ from information security conditions. In addition, in this approach possibility of effect of forcing of the speech is not considered. All this leads to the need for revaluation of the basic dependences which are the cornerstone of this method.

In process of an assessment of security of speech information the system of formation of a test signal is used. The question of a choice of sufficient level of this signal is actual. And in case of forcing of speech, there are even no experimental data on the basis of which it is possible to draw a conclusion of test signal level.

Experiment to determine formant distribution is put down and made, using which it is possible to estimate a contribution of each frequency band to total legibility of speech. For normal speech this experiment was made by N.B. Pokrovsky (results coincided), for forced speech a similar assessment was carried out for the first time. Experimental revaluation of dependence of word legibility on formant legibility is also made. In case of forcing of speech this dependence significantly differs.

The experimental assessment of amplitude structure of both normal (quiet) and forced speech is carried out. Relying on these dependences it is possible with a given probability, for example 0.95, to determine the sufficient level of a test acoustic signal. So for normal speech the sufficient level is 74dB and for forced speech is 85dB.

The received results allow to correct significantly a method of an assessment of legibility of speech, as well as formulate the method considering forcing effect.

УДК 004.942

Г.Ю. Потерпеев

МЕТОД ПРОГНОЗИРОВАНИЯ ДЕЙСТВИЙ ЗЛОУМЫШЛЕННИКА ПРИ ВЫБОРЕ ОПТИМАЛЬНОГО СКРЫТНОГО ВОЗДЕЙСТВИЯ НА ОПЕРАЦИОННУЮ СИСТЕМУ МОБИЛЬНОГО ПЕРСОНАЛЬНОГО УСТРОЙСТВА

Потерпеев Г.Ю. **Метод прогнозирования действий злоумышленника при выборе оптимального скрытного воздействия на операционную систему мобильного персонального устройства.**
Аннотация. В статье реализован один из подходов количественной оценки скрытности вредоносных воздействий, приведён способ формирования множества потенциально реализуемых воздействий, раскрыто понятие демаскирующих признаков воздействий, проведено количественное сравнение отрицательного и положительного эффектов при выборе конкретного механизма воздействия.
Ключевые слова: операционная система, мобильное персональное устройство, ранжирование, расстановка коэффициентов.

Poterpeev G.Y. **Method of Forecasting Maleficent Actions when Choosing the Optimal Covert Action on the Operating System of Mobile Personal Device.**
Abstract. The article contains one of the approaches to quantitative maleficent actions secrecy evaluation. The paper shows a method to form a multitude of potentially implemented maleficent actions. The article also explains the term «sign of action» and includes measurement of positive and negative effects when choosing the specific action mechanism.
Keywords: operation system, mobile personal device, ranking, coefficients factoring.

1. Введение. Современные вирусы для мобильных платформ на сегодняшний день стали вполне осязаемой и реальной угрозой. Так же как и в случае атак на операционную систему персонального компьютера (ОС ПК), зачастую целью становится персональные данные пользователя – владельца МПУ, идентификационные данные устройства, сведения об особенностях работы операционной системы и т.д.

Можно выделить несколько основных направлений развития мобильных угроз:

– кража конфиденциальных и персональных данных;

– скрытная отправка платных SMS-сообщений или выполнение звонков на «партнерский номер» без ведома владельца;

– мошеннические транзакции с использованием систем интернет-банкинга;

– осуществление скрытного копирования пользовательских данных;

– нарушение работоспособности мобильного персонального устройства.

Среди особенностей мобильного устройства можно выделить следующие:

– возможность физическоо доступа к МПУ значительно выше, чем к ПК;

– для передачи данных в основном используется беспроводная среда;

– существует возможность получения доступа к ОС без её запуска;

– в конкретном устройстве содержатся персональные данные конкретного пользователя, что позволяет персонифицировать владельца МПУ

– практически отсутствует разграничение к ресурсам со стороны пользователя (принцип: «один пользователь – одно МПУ»).

2. Исходные данные. Будем считать, что злоумышленник располагает активной компьютерной системой S_A. «Активность» S_A заключается в том, что S_A может оказывать влияние на качество функционирования «пассивной» мобильной операционной системы S_P, которая активно не влияет на S_A.

Предполагается, что активные воздействия системой S_A производятся при наличии уязвимостей. К таковым относятся: открытые порты приёма у системы S_P, возможность прямого доступа приложений к памяти S_P, возможность запуска фоновых процессов, наличие «слабых» паролей или открытого административного доступа к операционной системе S_P, отсутствие шифрования персональной информации или хранение ключей шифрования в открытом виде, возможность не замечаемых системой S_P самопроизвольных запусков различных приложений и т.п. Перечень уязвимостей может быть получен из готовой базы данных уязвимостей (NVD, CVE и др.) либо сформирован самостоятельно.

Полагаем, что злоумышленник (далее система S_A) для каждой уязвимости системы S_P располагает некоторым множеством механизмов их реализации. В то же время считаем, что реализации уязвимостей могут обнаруживать себя множеством выявляемых (демаскирующих) признаков (например, изменение содержимого доступных для просмотра системных файлов, некорректная работа служб, невозможность авторизации легального пользователя и т.п.).

В этом случае для системы S_A множеством выявляемых (демаскирующих) признаков является множество отрицательных результатов воздействий на систему S_P. К множеству положительных результатов воздействий на S_P злоумышленник относит получение доступа к ОС, возможность считывания и/или

изменения системной информации, дестабилизацию функционирования системы S_P и т.п.

Требуется разработать инструментарий прогнозирования действий злоумышленника при выборе оптимального скрытного деструктивного воздействия на систему S_P, используя которое система S_A достигает наибольший результирующий эффект. Создание такого инструментария позволяет в дальнейшем определять необходимые меры (способы) и/или требования к разработке средств эффективной защиты системы S_P от подобного рода воздействий.

3. Модель угроз информационной безопасности системы. Для осуществления несанкционированного воздействия на систему необходимо изначально просканировать её на предмет наличия уязвимостей, включая сбор информации об ОС, используемых протоколах, сведениях о сетевом устройстве и т.д.

В результате получаем множество возможных уязвимостей объекта воздействия $R = \{r_1, r_2, \ldots, r_n\}$. Элементами данного множества являются открытые порты приема данных, прямой доступ приложений к памяти устройства, возможность запуска фоновых процессов, слабые пароли либо открытый административный доступ к ОС, отсутствие шифрования персональной информации либо хранение ключей шифрования в открытом виде, возможность скрытного самопроизвольного запуска приложений без ведома пользователя и т.п.

Для каждой уязвимости существует множество $M = \{m_1, m_2, \ldots, m_k\}$ – множество известных способов реализаций уязвимостей для каждого r в момент времени t. При этом время, затрачиваемое на реализацию, не должно превышать некоторого значения t_{max} .

Для объекта существует множество выявляемых признаков воздействий $P = \{p_1, p_2, ..., p_l\}$. К таковым относятся: изменение содержимого системных файлов, некорректная работа служб, невозможность авторизации легального пользователя и т.д.

Для каждого элемента множества M существует результат воздействия, принадлежащий множеству $I = \{i_1, i_2, ..., i_l\}$. Таковым результатом воздействия может быть, например, получение доступа к ОС, возможность считывания и/или изменения персональной и системной информации, дестабилизация работы системы.

Таким образом, при соответствии операционной системы мобильного персонального устройства (МПУ) некоторому состоянию r_i

и существующей возможности использования механизма реализации уязвимости, строится матрица возможных воздействий:

$R\backslash M$	m_1	m_2	…	…	m_k
r_1	$r_1\, m_1$	$r_1\, m_2$	…	…	$r_1\, m_k$
r_2	$r_2\, m_1$	$r_2\, m_2$	…	…	$r_2\, m_k$
…	…	…	…	…	…
…	…	…	…	…	…
r_n	$r_n\, m_1$	$r_n\, m_2$	…	…	$r_n\, m_k$

При этом если данный механизм реализации уязвимости m не может быть реализован по отношению к r в момент времени t то соответствующее поле принимает значение 0.

В процессе заполнения матрицы получаем набор возможных результатов реализаций имеющихся уязвимостей объекта. При этом ненулевой результат реализаций относится к множеству I, каждое i имеет фиксированное ненулевое значение, то есть предположительно приводит к определенному результату воздействия. К накладываемым ограничениям относятся:

1) Время, затрачиваемое на реализацию.

2) Обнаруживаемые признаки воздействия.

Таким образом, результатом будет являться множество:

$$I = R \times M$$

Математическая модель функционирования МПУ в условиях преднамеренного воздействия будет проиллюстрирована с помощью следующих выражений:

$$\Phi = \{\Phi_1 = \{\{\Phi_{11}\}, \{\Phi_{12}\}, ..., \{\Phi_{1n_1}\}\}, ..., \Phi_k = \{\{\Phi_{k1}\}, \{\Phi_{k2}\}, ..., \{\Phi_{kn_k}\}\}\},$$

$$W_1 = \begin{cases} \{w_{11}\} = <\{a_{11} * w_1'\}, \{C_{11} * w_1, C_{12} * w_2, ..., C_{1r} * w_r\}> \\ \{w_{1n_1}\} = <\{a_{1n_1} * w_{n_1}'\}, \{C_{1n_1} * w_1, C_{1n_1+1} * w_2, ..., C_{1n_1+r} * w_r\}> \end{cases},$$

$$W_k = \begin{cases} \{w_{k1}\} = <\{a_{k1} * w_{k1}'\}, \{C_{k1} * w_1, C_{k2} * w_2, ..., C_{kp} * w_r\}> \\ \{w_{kn_k}\} = <\{a_{kn_k} * w_{kn_k}'\}, \{C_{kn_k} * w_1, C_{kn_k+1} * w_2, ..., C_{kn_k+r} * w_r\}> \end{cases},$$

где: Ф – множество механизмов воздействий (при этом Φ_1 – множество механизмов воздействий на уязвимость U_1, а Φ_2 – множество механизмов воздействий на уязвимость U_2 и т.д.). Наборы демаскирующих признаков для каждого механизма воздействия формируются на

основании существующей базы знаний и проверяются экспериментально. При этом весовые коэффициенты расставляются на основании метода экспертной оценки, а при наличии временных ограничений - методом попарного сравнения.

В приведенном выше выражении: $W = \{W_1, \ldots, W_k\}$ – множество результатов воздействий на ОС, $\{w'_{11}, \ldots, w'_{k1}\}$ – множество целевых «положительных» результатов воздействий на U_1 уязвимость, $\{w_1, \ldots, w_r\}$ – множество «побочных» результатов воздействий, то есть так называемых демаскирующих факторов.

Таким образом, результат вредоносного воздействия можно представить в виде:

$$\Phi_i = \{\Phi_{i1}, \Phi_{i2}, ..., \Phi_{in_i}\} \to U_i \Rightarrow (F_i) \Rightarrow W_i \to \{w_{i1}, w_{i2}, ..., w_{in_i}\},$$

$$\{w_{i1}, w_{i2}, ..., w_{in_i}\} = \{a_i \otimes w_i^*\}\{C_{i1}^{(1)} * w_1, C_{i2}^{(2)} * w_2, ..., C_{ir}^{(*)} * w_r\}.$$

С практической точки зрения, к возможным уязвимостям следует относить:

– возможность НСД к персональной информации;

– утечка персональных данных;

– несанкционированная модификация персональных данных;

– угрозы дестабилизации работы устройства;

– воздействия на уровне ОС (к примеру, СМС сообщение с определенным текстом, приводящее к недекларированному поведению системы);

– воздействия на периферийные устройства (к примеру, вывод из строя GSM-модуля);

– угроза доступа к операционной системе мобильного передающего устройства с получением определенных прав.

Предложенная модель позволяет осуществить параметризацию имеющихся в целевой операционной системе уязвимостей и механизмов воздействия на них для последующей оценки полезности положительного эффекта и степени проявления демаскирующих признаков, проявляющихся в ходе применения того или иного механизма воздействия.

4. Метод выбора механизма воздействия на операционную систему. Сущность метода состоит в ранжировании выделенных уязвимостей и суммарной оценке механизмов реализации с учетом полезного эффекта и степени проявления демаскирующих признаков.

Структура метода представлена на рисунке 1.

Рис. 1. Структура метода выбора механизма воздействия

Метод состоит из следующей последовательности шагов:

1. Формирование множества уязвимостей системы S_P, где:

$$U = \{u_1, u_2, ..., u_k\}.$$

2. Для каждой уязвимости u_i из множества U определяется множество допустимых механизмов воздействий. Все допустимые механизмы воздействий на все уязвимости образуют множество Φ, где:

$$\Phi = \{\Phi_1, \Phi_2, ..., \Phi_n\}.$$

3. Для каждой пары $< U_i, \Phi_j >$, где U_i – i-я уязвимость u_i, Φ_j – j-й механизм воздействия, определяется при наличии положительного результата w^+_l ($l = 1(1)p$) и отрицательных результатов w^-_d ($d = 1(1)r$).

4. Для каждой вышеописанной пары $< U_i, \Phi_j >$ определяется весовой коэффициент положительного эффекта.

5. Для каждой вышеописанной пары $< U_i, \Phi_j >$ определяются весовые коэффициенты демаскирующих признаков.

6. Задаётся ограничение на суммарный эффект положительного результата (результативность) – не менее заданного положительного значения R^+:

$$c^+_{ijl} * w^+_l \geq R^+.$$

7. Задаётся ограничение на суммарный эффект отрицательных (демаскирующих) признаков (скрытность) – не более заданного положительного значения R^-:

$$\sum_{i=1}^{k} \sum_{j=1}^{n} \sum_{l=1}^{r} c^-_{ijl} * w^-_d \leq R^-.$$

8. Вычисляется результирующий эффект как разность положительного эффекта и суммы демаскирующих признаков с учетом весовых коэффициентов для каждого механизма воздействия:

$$(c^+_{ijl} * w^+_l - \sum_{i=1}^{k} \sum_{j=1}^{n} \sum_{l=1}^{r} c^-_{ijl} * w^-_d) \rightarrow \max.$$

9. Осуществляется выбор уязвимости и её механизма реализации, обладающих максимальным результирующим эффектом.

Заметим, что выше рассматривался подход, при котором значения w^+_l и w^-_d были заданы в абсолютной шкале измерений.

Однако, если величины w^+_l и w^-_d задаются в порядковой шкале,

алгоритм действий был бы другим. Изменяется данный алгоритм и в том случае, когда эти величины определяются не как числовые, а как лингвистические или нечёткие переменные.

Существенное влияние на изменение алгоритма оказывает учёт продолжительностей проявления отрицательных и положительных результатов воздействий на уязвимости, а также типы шкал, в которых изменяют упомянутые выше продолжительности проявлений.

5. Заключение. Таким образом, предложенный подход позволяет выявить наиболее результативные и наименее заметные возможные воздействия на МПУ, что позволяет прогнозировать наиболее вероятные вредоносные воздействия и пути их реализации.

Также результатом применения подхода является ранжирование угроз, на основании чего можно выработать рекомендации по предотвращению наиболее вредоносных воздействий на МПУ.

Литература

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных ФСТЭК // М. 2008. 231 с.
2. *Девянин П.Н.* Модели безопасности компьютерных систем // М.: 2011 128 с.
3. *Потерпеев Г.Ю.* Модель угроз информационной безопасности мобильных персональных устройств. Методы обеспечения информационной безопасности // 2013.
4. *Лукацкий А.В.* Обнаружение атак // Санкт-Петербург: БХВ. 2001. 624 с.
5. *Климов А.В.* Программирование для мобильных устройств // Санкт-Петербург: Питер. 2007. 321 с.
6. *Б. Харди, Б. Филлипс*. Программирование под Android:практическое руководство // Санкт-Петербург: Питер. 2014. 592 с.
7. *Еремеев М.А., Ломако А.Г., Новиков В.А.* Метод выявления дефектов и недокументированных возможностей программ // Информационное противодействие угрозам терроризма. 2010. №14. С. 46–49.
8. *Еремеев М.А., Пономарев Ю.А., Потерпеев Г.Ю.* Модель и методы дистанционного контроля мобильных персональных устройств: сборник трудов 23 научно-технической конференции СПБГПУ // Санкт-Петербург. 2014. 382 с.

References

1. [Basic model of personal data security during it's processing in personal data proceeding systems, FSTEC]. M. 2008. 231 p. (In Russ.).
2. Devianin P.N. *Modeli bezopasnosti komp'juternyh sistem* [Computer system security models]. M. 2011.128 p. (In Russ.).
3. Poterpeev G.Y. *Model' ugroz informacionnoj bezopasnosti mobil'nyh personal'nyh ustrojstv. Metody obespechenija informacionnoj bezopasnosti* [Model of information security vulnerabilities of mobile personal devices]. Spb. 2013. (In Russ.).
4. Lukatskiy A.V. *Obnaruzhenie atak* [Attack detection]. SPb. 2001. 624 p. (In Russ.).
5. Klimov A.V. *Programmirovanie dlja mobil'nyh ustrojstv* [Mobile device programming]. SPb. 2007. 321 p. (In Russ.).
6. B.Hardie, B. Fillips. *Programmirovanie pod Android:prakticheskoe rukovodstvo* [Android programming: a practical guide]. Spb. 2014. 592 p. (In Russ.).
7. Eremeeev M.A., Novikov V.A., Lomako A.G. [Method of program vulnerabilities detection]. *Informacionnoe protivodejstvie ugrozam terrorizma – Information*

counteraction to threats of terrorism. M. 2010. no. 14. pp. 46-79. (In Russ.).
8. Eremeev M.A., Ponomarev Y.A., Poterpeev G.Y. [Model and methods of personal mobile devices remote control] *Trydy 23-oi naychno-tehnicheskoi konferencii SPBGPU* [Proceedings of the 23-th Scientific and Technical Conference on SPbPU]. SPb. p. 382. (In Russ.).

Потерпеев Герман Юрьевич — старший научный сотрудник - начальник научно-исследовательской лаборатории экспериментального моделирования защищенного применения средств сбора, обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: защищенное представление и обработка данных, системы защиты информации, информационная безопасность, мобильные персональные устройства. Число научных публикаций — 14. gypo@mail.ru; ул. Ждановская 13, Санкт-Петербург, 197198; р.т.: +7(812)230-28-15.

Poterpeev German Yurievich — senior researcher - head of the experimental modeling of data proceeding system secure using laboratory, Mozhaisky Military Space Academy. Research interests: secure data proceeding, system of information protection, information security, mobile personal devices. The number of publications — 14. gypo@mail.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812)230-28-15.

РЕФЕРАТ

Потерпеев Г.Ю. **Метод прогнозирования действий злоумышленника при выборе оптимального скрытного воздействия на операционную систему мобильного персонального устройства.**

Статья посвящена рассмотрению подхода к выявлению, классификации и ранжированию угроз защищенности мобильных персональных устройств. Реализован подход количественной оценки скрытности вредоносных воздействий, предполагающий расстановку коэффициентов для каждого потенциально возможного механизма воздействия.

В основе предлагаемого подхода лежит ранжирование альтернатив на основе метода анализа иерархий. Каждый элемент множества потенциально реализуемых механизмов воздействий оценивается с точки зрения скрытности и результативности, после чего проводится количественное сравнение положительного и отрицательных эффектов или демаскирующих признаков (ДП).

SUMMARY

Poterpeev G.Y. **Method of Forecasting Maleficent Actions when Choosing the Optimal Covert Action on the Operating System of Mobile Personal Device.**

The article considers the approach to the identification, classification and ranking of threats to the security of mobile personal devices. Implemented approach quantifies covert harmful interference, involving the alignment of coefficients for each possible mechanism of action.

The proposed approach is based on the ranking of alternatives based on the analytic hierarchy process. Each element of the set of potentially implemented action mechanisms is assessed in the view of its secrecy and efficiency, followed by a quantitative comparison of the positive and negative effects or telltale signs (TS).

УДК 511; 519.6

А.Е.Ваулин

СВЕДЕНИЕ ЗАДАЧИ ФАКТОРИЗАЦИИ НАТУРАЛЬНОГО ЧИСЛА К ЗАДАЧЕ РАЗБИЕНИЯ ЧИСЛА НА ЧАСТИ. ЧАСТЬ 2

Ваулин А.Е. **Сведение задачи факторизации натурального числа к задаче разбиения числа на части. Часть 2.**

Аннотация. В настоящей работе рассматриваются и описываются вопросы разработки алгоритмов факторизации составных натуральных чисел. Автором предлагается иной подход, основанный на изучении внутренней структуры натурального ряда чисел и использовании свойств чисел, не зависящих от их разрядности (по типу признаков делимости). Такой подход обеспечивает преобразование задачи разложения числа на множители в задачу поиска специального разбиения новой характеристики числа, названной ф-инвариантом, что следует признать менее сложной задачей.

Ключевые слова: натуральный ряд, нечетное число, ф-инвариант числа, разбиения числа, контур натурального ряда чисел.

Vaulin A.E. **Conversion of Integer Factorization to a Problem of Decomposition of a Number. Part 2.**

Abstract. The development of factorization mechanisms of composite integer numbers is examined in this work. The author proposes a different approach, based on the study of the internal structure of the positive integers and the use of the properties of numbers which do not depend on their digits (the criterion for divisibility). That kind of approach provides a conversion from integer factorization task to a retrieval task of the special partition of the new characteristic of a number, so-called f-invariant, which turns out to be less complex problem. – Bibl. 22 items.

Keywords: natural number, odd number, f-invariant of a numbers, partitions of a number, the contour of the natural numbers.

1. Введение. Разработка новых методов решения задачи факторизации больших чисел (ЗФБЧ) за приемлемые для практических нужд временные интервалы становится необходимостью настоящего времени. Известные характеристики лучших компьютеров настоящего времени не обеспечивают требуемых параметров решения ЗФБЧ. Самые мощные компьютеры мира (Tianhe-2, его производительность 33,86 петафлопс) в Китае; на втором месте – американский Titan (17,59 петафлопс); суперкомпьютер России «Ломоносов» из МГУ (0.9 петафлопс) – на 42 месте, фактически не изменяют ситуацию к лучшему.

Сложность вычислений в ЗФБЧ, как правило, связывают с зависимостью количества операций, необходимых для вычисления рассматриваемой функции, от разрядности аргумента функции. По нарастанию различают полиномиальную, субэкспоненциальную и экспоненциальную сложности.

Зависимость свойств чисел от разрядности, на которых базируются современные алгоритмы факторизации, не позволяет создать при

их использовании быстродействующие алгоритмы [4–16]. Проблема факторизации числа имеет непосредственное отношение к теории чисел, так как среди арифметических операций этой теории отсутствует операция факторизации натурального числа [11-16], которая удовлетворяла бы запросам науки и общественной практики.

Метод дискретного логарифмирования Копперсмита сегодня является лучшим по скорости, но его применимость ограничена, для группы точек эллиптической кривой он не применим.

В предлагаемой работе вводятся новые модель натурального ряда чисел (НРЧ) и характеристика нечетного числа ф-инвариант. Эта числовая характеристика, определяется для нечетного натурального числа N, имеющего произвольную разрядность и представляется разбиениями специального вида. Разбиения соответствуют разным интервалам для числа N и отображаются в контурную структуру модели НРЧ. Соответствующие числу N интервалы имеют полные квадраты на своих границах. Это свойство числа не зависит от его разрядности.

Формула, описывающая интервал длиной N, расстоянием между граничными точками интервала (между квадратами), обеспечивает время реализации решения ЗФБЧ N весьма слабо зависящим от разрядности факторизуемого числа.

В этой (II) части работы показывается путь преобразования ЗФБЧ в задачу о разбиениях числа на основе новой его характеристики ф-инварианта с обоснованием преимуществ такого сведения.

2. Ф-инвариант числа. Инвариантом объекта (числа) называется количественная характеристика, которая остается без изменений при преобразованиях (изменениях), выполняемых с объектом. Так, например, аффинная и проективная геометрии отличаются инвариантами: в аффинной – это простое отношение, а в проективной – двойное отношение.

Ф-инвариантом числа N называется меньшее число, обозначаемое $k_п(N)/2$ и равное половине номера предельного контура числа N. Ф-инвариант существует для чисел произвольной разрядности. Получаемые различные представления (разными интервалами в НРЧ) числа N сохраняют значение ф-инварианта.

Пример 1. Рассмотрим введенные понятия на числовом примере. Пусть задано нечетное составное число $N = 3 \cdot 5 \cdot 7 = 105$. Это наименьшее из нечетных чисел с тремя различными простыми нетривиальными делителями. Число 105 является составным правым нечетным числом, так как $N_п = 105 \equiv 1 (\mathrm{mod} 4)$. Определим для $N_п = 105$ номер предельного контура через его длину $k_п = L_п(N) /8 = (103 + 105)/8 = 26$.

Так как число $N_{п} = 105$ в составе контура лишь правая «половина» (полуконтур), то ему соответствует лишь половина номера, то есть $k_{п}\ (N=105)/2 = 26/2 = 13$. Это значение $k_{п}\ (N)/2 = 13$ для N называется (является) ф-инвариантом.

Для числа $N_{п} = 105$ альтернативными предельному полуконтуру интервалами, определяемыми их границами, являются еще три интервала, характеристики которых приведены ниже в таблице 1.

Можно показать, что, если число N является нечетным левым и составным, то рассмотренные зависимости имеют место и в этом случае. Изменится только положение крайнего полуконтура в соответствующих интервалах, он станет равным половине меньшего, а большего контура в сумме. На сумму номеров контуров это изменение положения полуконтура влияния не окажет: она останется равной половине номера предельного контура.

Анализ данных таблицы показывает, что все альтернативные интервалы образованы совокупностями контуров и полуконтура такими, что их номера следуют непрерывно один за другим. В сумме эти номера задают специальные разбиения числа 13 равного половине номера предельного контура $k_{п}\ (105)/2 = 13.$

Таблица 1. Характеристики альтернативных интервалов (моделей) числа $N_{п} = 105$

Альтернативные интервалы их границы и длина для заданного числа $N_{п} = 105$	Суммы номеров контуров и длин полуконтуров, образующие интервалы, и их длины для числа $N_{п} = 105$
$\Gamma_{п1} = 11^2$, $\Gamma_{л1} = 4^2$, $\Gamma_{п1} - \Gamma_{л1} = 121 - 16 = 105$	$2/2 + 3 + 4 + 5 = 13;$ спецразбиение $9+11+13+15+17+19+21=105$
$\Gamma_{п2} = 13^2$, $\Gamma_{л2} = 8^2$, $\Gamma_{п2} - \Gamma_{л2} = 169 - 64 = 105$	$4/2 + 5 + 6 = 13;$ спецразбиение $17+19+21+23+25 = 105$
$\Gamma_{п3} = 19^2$, $\Gamma_{л3} = 16^2$, $\Gamma_{п3} - \Gamma_{л3} = 361 - 256 = 105$	$8/2 + 9 = 13;$ спецразбиение $33+35+37 = 105$

Обратим внимание на то, что в суммах номеров контуров и полуконтура, вычисляемых для альтернативных интервалов, все слагаемые являются следующими подряд натуральными числами. Исключение составляет одно из крайних слагаемых, но и в этом случае контур, из номера которого берется в сумму лишь половина, имеет номер, примыкающий к основной последовательности номеров.

Это наблюдение дает основание для рассмотрения в качестве подмодели факторизуемого числа N суммы элементов разбиений специального вида для числа, равного половине номера предельного контура этого факторизуемого числа. А также рассматривается в качестве части алгоритма решения задачи факторизации числа N алгоритм ге-

нерации разбиений специального вида для ф-инварианта (половины номера предельного контура числа ***N***). Следующий пример служит для прояснения сказанного.

Пример 2. В средней колонке таблицы 2 в части I работы [3] приводится точечная диаграмма Феррера [13] для разбиений чисел. Блокам разбиения соответствуют строки диаграммы с возрастающим на единицу числом точек при движении вверх. Каждая строка точек интерпретируется как номер контура в интервальной модели натурального числа ***N***. Части всех разбиений (в строках) образованы монотонно возрастающими на единицу натуральными числами (точками строк). Разбиваемые числа (комбинаторные сочетания из ***k*** по два) C_k^2 описываются непрерывными совокупностями строк, начиная с нижней строки. Крайние блоки специальных разбиений – номера полуконтуров обозначены ***p*** и ***n, p > n***.

Таблица 2. Сочетания для числового примера $C_k^2 = C_6^2$

Сочетания по 2 из 6 цифровых элементов $P = \{1,2,3,4,5,6\}$, $\lvert P\rvert = 6$		
1. 1 2	6. 2 3	11. 3 5
2. 1 3	7. 2 4	12. 3 6
3. 1 4	8. 2 5	13. 4 5
4. 1 5	9. 2 6	14. 4 6
5. 1 6	10. 3 4	15. 5 6

Например, строки (см. таблицу 2, [3]) с первой снизу по пятую строку включительно содержат количества точек: ***1+2+3+4+(p=5)=15***, что соответствует числу комбинаторных сочетаний C_k^2, где значение ***k*** на единицу больше последнего элемента в сумме, т.е. ***k = p +1 = 5 +1 = = 6*** и $C_6^2 = 15$. В этом легко убедиться, построив все такие сочетания и подсчитав суммы (см. таблицу 2, [3]).

Таким образом, интерес в задаче факторизации числа ***N*** представляют не все возможные разбиения половины номера $k_п(105)/2 = 26/2 = 13$ предельного контура для ***N = 105***, а только разбиения специального типа. Примеры таких специальных разбиений приведены в табл.***1.*** Они ниже в табл. ***3*** выделены заливкой. В этой таблице приводится список всех лексикографически упорядоченных разбиений числа ***13*** на все части для числового примера с $N_n = 105$. Список сформирован в таблице 3 программой-генератором разбиений чисел.

Среди множества всех лексикографически упорядоченных разбиений числа $k_n/2 = 13$ (таблица 3, см. пример 4) диаграмме Феррера (см. таблицу 2, [3]) удовлетворяют лишь четыре специальных разбиения, а именно, разбиения с лексикографическими номерами:
№53 → 2/2 + 3 + 4 + 5; №70 → 4/2+ 5+ 6; №94 →8/2 + 9 и ***№101→13.***

Эти разбиения выделены заливкой в таблице 3. Последнее ***101***-е разбиение образовано одной частью (одной строкой), равной самому числу ***13***. Особенность этих разбиений состоит в том, что меньший блок разбиения в каждом из них равен лишь половине числа, которое начинает список блоков каждого разбиения. В ***53***-м разбиении это число ***2***, за которым следуют ***3, 4*** и ***5***, но от двойки в сумму берется лишь половина, т.е. единица. В ***70***-м разбиении меньший номер контура – это число ***4***, за которым следуют ***5*** и ***6***, но от четверки в сумму берется лишь половина, т.е. двойка. В ***94***-м разбиении это число ***8***, за которым следует единственное число ***9***, но от восьмерки в сумму берется лишь половина, т.е. четверка. Последнее разбиение ***№101*** соответствует половине номера ***26/2*** предельного контура для правого числа ***N = 105***, т.е. $k_n/2 = 26/2 = 13$.

Таблица 3. Полный список упорядоченных разбиений числа $k_n(105)/2 = 13$ на все части

Лексикографически упорядоченные разбиения числа 13 на все части с указанием их номеров				
1. 1 1 1 1 1 1 1 1 1 1 1 1 1	21. 3 3 3 3 1	41. 5 2 1 1 1 1 1 1	61. 6 2 2 2 1	81. 7 5 1
2. 2 1 1 1 1 1 1 1 1 1 1 1	22. 4 1 1 1 1 1 1 1 1 1	42. 5 2 2 1 1 1 1	62. 6 3 1 1 1 1	82. 7 6
3. 2 2 1 1 1 1 1 1 1 1 1	23. 4 2 1 1 1 1 1 1 1	43. 5 2 2 2 1 1	63. 6 3 2 1 1	83. 8 1 1 1 1
4. 2 2 2 1 1 1 1 1 1 1	24. 4 2 2 1 1 1 1 1	44. 5 2 2 2 2	64. 6 3 2 2	84. 8 2 1 1 1
5. 2 2 2 2 1 1 1 1 1	25. 4 2 2 2 1 1 1	45. 5 3 1 1 1 1 1	65. 6 3 3 1	85. 8 2 2 1
6. 2 2 2 2 2 1 1 1	26. 4 2 2 2 2 1	46. 5 3 2 1 1 1	66. 6 4 1 1 1	86. 8 3 1 1
7. 2 2 2 2 2 2 1	27. 4 3 1 1 1 1 1 1	47. 5 3 2 2 1	67. 6 4 2 1	87. 8 3 2
8. 3 1 1 1 1 1 1 1 1 1 1	28. 4 3 2 1 1 1 1	48. 5 3 3 1 1	68. 6 4 3	88. 8 4 1
9. 3 2 1 1 1 1 1 1 1 1	29. 4 3 2 2 1 1	49. 5 3 3 2	69. 6 5 1 1	89. 8 5
10. 3 2 2 1 1 1 1 1 1	30. 4 3 2 2 2	50. 5 4 1 1 1 1	*70. 6 5 2*	90. 9 1 1 1 1
11. 3 2 2 2 1 1 1 1	31. 4 3 3 1 1 1	51. 5 4 2 1 1	71. 6 6 1	91. 9 2 1 1
12. 3 2 2 2 2 1 1	32. 4 3 3 2 1	52. 5 4 2 2	72. 7 1 1 1 1 1	92. 9 2 2
13. 3 2 2 2 2 2	33. 4 3 3 3	*53. 5 4 3 1*	73. 7 2 1 1 1 1	93. 9 3 1
14. 3 3 1 1 1 1 1 1 1	34. 4 4 1 1 1 1 1	54. 5 4 4	74. 7 2 2 1 1	*94. 9 4*
15. 3 3 2 1 1 1 1 1	35. 4 4 2 1 1 1	55. 5 5 1 1 1	75. 7 2 2 2	95. 10 1 1 1
16. 3 3 2 2 1 1 1	36. 4 4 2 2 1	56. 5 5 2 1	76. 7 3 1 1 1	96. 10 2 1
17. 3 3 2 2 2 1	37. 4 4 3 1 1	57. 5 5 3	77. 7 3 2 1	97. 10 3
18. 3 3 3 1 1 1 1	38. 4 4 3 2	58. 6 1 1 1 1 1 1 1	78. 7 3 3	98. 11 1 1
19. 3 3 3 2 1 1	39. 4 4 4 1	59. 6 2 1 1 1 1 1	79. 7 4 1 1	99. 11 2
20. 3 3 3 2 2	40. 5 1 1 1 1 1 1 1 1	60. 6 2 2 1 1 1	80. 7 4 2	100. 12 1
				101. 13

Задача представления ф-инварианта, необходимого для факторизации, таким образом, может быть сведена к разработке алгоритма и построению генератора разбиений такого специального вида. Анали-

тическое исследование возможностей получения таких разбиений может быть выстроено и иначе. Легко получается сумма элементов (точек) строк от первой до некоторой заданной с номером $k - 1$ – это расчет числа сочетаний по формуле $C_k^2 = k(k - 1)/2$. Например, при $k = 7$ имеем $C_k^2 = k(k - 1)/2 = 7 \cdot 6/2 = 21$. К сожалению, приведенная формула не учитывает «половинки» номеров крайних контуров, что при расчетах вызывает неудобства.

Выход из положения состоит в том, чтобы каким-то образом такие половинки учесть. Оказывается это вполне реализуемая задача. Так, например, имеем сумму ряда чисел в общем виде, где последнее слагаемое (верхняя строка диаграммы Феррера (см. табл. **2,** [3])) делится пополам, тогда $1 + 2 + 3 + \ldots + n - 1 + n/2 = n^2/2$. В случае конкретных чисел $1 + 2 + 3 + 4/2 = 4^2/2 = 8$, как видим, сумма такого ряда вычисляется также достаточно просто.

Обозначим символом $\Delta(N)$ разность суммы C_k^2 номеров строк диаграммы Феррера (см. табл. **2,** [3]) до верхней выделенной строки с номером $k - 1 = 6$ и суммы $n^2/2$ номеров строк, учитывающей половину точек верхней строки с заданным номером $n = 4$ этой диаграммы, где, если $n < k$, как $\Delta(N) = C_k^2 - n^2/2$, а если $k < n$, то наоборот $\Delta(N) = n^2/2 - C_k^2$.

Очевидно, для решения задачи факторизации в обоих случаях разность должна быть равна ф-инварианту, т.е. половине номера $k_n(N)/2$ предельного контура числа N.

Другими словами, путем выбора значений k и n при вычислении $\Delta(N) = |C_k^2 - n^2/2| = k_n(N)/2$ необходимо обеспечить выполнение записанного равенства при заданном N. При этом состав и номера строк диаграммы, привлекаемых для вычислений сохраняются. Понятно, что определив одну из величин k или n, другая определяется как функция от первой. Например, при заданном значении k значение n определяется (берется арифметическое значение корня) как $n = \sqrt{2C_k^2 - k_n(N)}$.

Пример 3. (*Формирование специального разбиения: число* $N = 105$ *– это правый полуконтур в предельном контуре*).

Факторизовать правое число $N = 105$ с использованием специальных разбиений.

Для $N = 105$ ранее был определен ф-инвариант (номер предельного полуконтура) $k_n(105)/2 = 26/2 = 13$. Необходимо выбрать в точечной диаграмме (см. табл. **2,** [3]) трапецию, определяемую ее основаниями, с суммарным значением точек равным $k_n(105)/2 = 13$. Уже пятая строка ($k = 5$) диаграммы таблицы **2** соответствует **15** точкам, следовательно, значение k может быть только большим, чем **5**. Вычисления для $k = 7$ дают значение $C_k^2 = 21$. Необходимо для выполнения

равенства $\Delta(105) = |C_k^2 - n^2/2| = k_n(105)/2 = 13$ определить значение переменной n (номер нижнего основания трапеции). Очевидно, n должно быть таким, чтобы выполнялось равенство $C_k^2 - 13 = n^2/2$.

Тогда $21 - 13 = 8 = n^2/2$ и $n = \sqrt{2 \cdot 8} = 4$. Действительно, при $k = 7$, $p = k - 1 = 6$ и $n = 4$ разность $\Delta(105) = 13$ и факторизация числа $N = 105$ может быть успешно выполнена. В примере найдены значения крайних блоков (номеров контуров в НРЧ): $p = 6$ и $n = 4$, специального разбиения, формирующего представляющий число N интервал.

Ранее суммированием элементов было показано и получено значение $4/2 + 5 + 6 = 13$, которое интерпретируется с одной стороны как сумма блоков специального разбиения числа 13, а с другой – как сумма номеров контуров НРЧ, образующих интервал для факторизуемого числа N. Преобразование номеров контуров (аддитивная форма числа) в их длину и суммирование этих длин дает следующий результат:

$$6 \cdot 8 + 5 \cdot 8 + (4 \cdot 8 + 2)/2 = 48 + 40 + 17 = 105 = N.$$

В последнем слагаемом левой части вычисляется длина крайнего (правого) полуконтура контура с номером $k = 4$. Суммарный интервал из длин контуров равняется как раз факторизуемому числу. Представляющий N интервал найден правильно. Но этого недостаточно, чтобы выполнить факторизацию N. Необходимо перейти к мультипликативной форме представления числа для чего определяются значения границ найденного интервала $\Gamma_п(105)$; $\Gamma_п(105)$ или значения крайних точек представляющего число $N = 105$ интервала. Разумеется, они должны быть квадратами натуральных чисел. Определим эти границы.

Меньшая, левая граница совпадает с центральной границей меньшего контура, имеющего номер 4, т.е.:

$$\Gamma_л(105) = \Gamma_ц(4) = (2 \cdot 4)^2 = 8^2 = 64.$$

Большая, правая граница совпадает с правой границей большего контура с номером $k = 6$, т.е. $\Gamma_п(105) = \Gamma_п(6) = (2 \cdot 6 + 1)^2 = 13^2 = 169$.

После этих вычислений, используя основное соотношение мультипликативной модели составного натурального числа:

$$N = x_1^2 - x_o^2 = (x_1 - x_o)(x_1 + x_o),$$

находятся факторы числа, а именно,

$$N = \Gamma_п - \Gamma_л = 13^2 - 8^2 = (13 - 8)(13 + 8) = 5 \cdot 21 = 105.$$

Пример 4. (*Формирование специального разбиения – число* $N=1\ 1\ 1$ *это левый полуконтур в предельном контуре*).

Факторизовать левое число N с использованием специальных разбиений. Рассмотрим натуральное левое нечетное число $N = 1\ 1\ 1$, $N_л = 1\ 1\ 1 \equiv 3(\mathbf{mod}4)$. Предельный контур заданного числа имеет текущий номер $k_п(1\ 1\ 1) = (N+1)/4 = 28$, и полуконтуру соответствует число $k_п(1\ 1\ 1)/2 = 28/2 = 14$.

В полном списке разбиений числа 14 (табл.4) единственное специальное разбиение с номером $№123 \rightarrow 9+10/2 = 14$ соответствует нумерационной модели этого натурального составного числа $N = 1\ 1\ 1$. Суммарная длина представляющего интервала равна:

$$8 \cdot 9 + (8 \cdot 10 - 2)/2 = 72 + 39 = 1\ 1\ 1.$$

Таблица 4. Полный список упорядоченных разбиений числа $k_п(1\ 1\ 1)/2 = 14$ на все части

Лексикографически упорядоченные разбиения числа 14 на все части с указанием их номеров				
1. 11111111111111	28. 42221111	55. 532211	82. 64211	109. 8222
2. 2111111111111	29. 4222211	56. 53222	83. 6422	110. 83111
3. 221111111111	30. 422222	57. 533111	84. 6431	111. 8321
4. 22211111111	31. 431111111	58. 53321	85. 644	112. 833
5. 2222111111	32. 43211111	59. 5333	86. 65111	113. 8411
6. 222221111	33. 4322111	60. 5411111	87. 6521	114. 842
7. 22222211	34. 432221	61. 542111	88. 653	115. 851
8. 2222222	35. 4331111	62. 54221	89. 6611	116. 86
9. 311111111111	36. 433211	63. 54311	90. 662	117. 911111
10. 32111111111	37. 43322	64. 5432	91. 71111111	118. 92111
11. 3221111111	38. 43331	65. 5441	92. 7211111	119. 9221
12. 322211111	39. 44111111	66. 551111	93. 722111	120. 9311
13. 32222111	40. 4421111	67. 55211	94. 72221	121. 932
14. 3222221	41. 442211	68. 5522	95. 731111	122. 941
15. 3311111111	42. 44222	69. 5531	96. 73211	123. 95
16. 332111111	43. 443111	70. 554	97. 7322	124. 101111
17. 33221111	44. 44321	71. 611111111	98. 7331	125. 10211
18. 3322211	45. 4433	72. 62111111	99. 74111	126. 1022
19. 332222	46. 44411	73. 6221111	100. 7421	127. 1031
20. 33311111	47. 4442	74. 622211	101. 743	128. 104
21. 3332111	48. 5111111111	75. 62222	102. 7511	129. 11111
22. 333221	49. 521111111	76. 6311111	103. 752	130. 1121
23. 333311	50. 52211111	77. 632111	104. 761	131. 113
24. 33332	51. 5222111	78. 63221	105. 77	132. 1211
25. 41111111111	52. 522221	79. 63311	106. 8111111	133. 122
26. 4211111111	53. 53111111	80. 6332	107. 821111	134. 131
27. 422111111	54. 5321111	81. 641111	108. 82211	135. 14

Границами представляющего интервала служат левая граница девятого ($k = 9$) контура и центральная граница – правого ($k = 10$):

$$\Gamma_л(1\,1\,1) = \Gamma_л(9) = (2\cdot 9 - 1)^2 = 17^2 = 289; \text{ и } \Gamma_п(1\,1\,1) = \Gamma_ц(10) = (2\cdot 10)^2 = 20^2 = 400.$$

Использование этих границ обеспечивает решение задачи факторизации числа $N = 1\,1\,1$ на основе основного соотношения модели:

$$N = \Gamma_п - \Gamma_л = 20^2 - 17^2 = (20 - 17)(20 + 17) = 3\cdot 37 = 1\,1\,1.$$

Рассмотрим теперь вопрос о связи характеристик интервальной и нумерационной моделей числа N более подробно.

3. Взаимосвязь характеристик интервальной и нумерационной моделей. *Пример 5. (Взаимосвязь характеристик интервальной и нумерационной моделей нечетного натурального числа* N*)*

Пусть $N = 231 = 1\,1\cdot 21 = 33\cdot 7 = 77\cdot 3 = 231\cdot 1$, $N = 231 \equiv 3 (\mathbf{mod} 4)$, число N левое. Интервальная модель числа N сформирована как последовательность примыкающих друг к другу полуконтуров. Полуконтур в интервальной модели самый большой из всех в сумме и размещен справа, а больший квадрат (правая граница интервала) четный. Длина предельного контура $L_п = 231 + 233 = 464$, его номер $k_п(231) = L/8 = 464/8 = 58$, границы предельного полуконтура: правая граница $\Gamma_п = \Gamma_ц = (2k_п)^2 = 1\,16^2$, левая граница $\Gamma_л = (2k_п - 1)^2 = 1\,15^2$.

Запишем интервальную модель N разностью границ интервала

$$N = \Gamma_п - \Gamma_л = x_{1i}^2 - x_{oi}^2 = (2\cdot 58)^2 - (58\cdot 2 - 1)^2 = 1\,16^2 - 1\,15^2 = 231\cdot 1.$$

Такое представление приводит к тривиальному разложению на множители числа N. Нетривиальные нумерационные модели числа 231 с ф-инвариантом $k_п(231)/2 = 58/2 = 29$ представлены тремя, $i = 1(1)3$, суммами номеров (тремя наборами слагаемых) последовательных номеров контуров с учетом лишь половины номера от большего контура Здесь таблицу со списком всех разбиений не приводим (она слишком велика), а укажем ниже только специальные разбиения из нее:

$$k_п(N)/2 = 29 = (3 + 4 + 5 + 6 + 7 + 8\ /2) = (7 + 8 + 9 + 10/2) = (19 + 20/2).$$

Через суммы номеров контуров (нумерационные модели) число $N = 231 = 4k - 1 = 58\cdot 4 - 1$ имеет три представления, где число 29 представляется разными суммами номеров, приведенными выше:

$$N = 231 = 29\cdot 8 - 1 = (3 + 4 + 5 + 6 + 7 + 8/2)8 - 1 =$$
$$= (7 + 8 + 9 + 10/2)8 - 1 = (19 + 20/2)8 - 1.$$

Эти три суммы в скобках представляют собой разбиения в полном лексикографическом списке разбиений числа 29 и имеют в этом

списке лексикографические номера: ***№1403→8/2 7 6 5 4 3=7 6 5 4 4 3; №2533 →10/2 9 8 7 = 9 8 7 5; №4468 →20/2 19 = 19 10.***

Можно увидеть, что в разбиении с номером ***№1403*** как бы не выполнено условие специальности разбиения, так как оно имеет два одинаковых подряд следующих блока (***4 4***). На самом деле одна из четверок это половина номера большего контура (***8/2 = 4***), следующего за седьмым контуром. В следующем разбиении блок ***5*** следует не за шестым, а за седьмым блоком. Это означает, что пятерка – это половина номера десятого контура, следующего в НРЧ за девятым контуром. Аналогично и в последнем разбиении ***10 = 20/2*** – это половина номера двадцатого контура, следующего за девятнадцатым. Дело в том, что совсем не тривиальная программа-генератор лексикографически упорядоченных разбиений числа представляет блоки разбиения именно в таком порядке. Особой необходимости переделывать программу не возникает, и здесь ограничиваемся просто краткими пояснениями.

Ниже выписаны представления числа ***N = 231*** границами интервалов (интервальная модель) и результаты факторизации числа:

$$N = \Gamma_п - \Gamma_л = x_{1i}^2 - x_{oi}^2,\ i = 1(1)4,$$

$$\Gamma_п\ (2\cdot 8) - \Gamma_л\ (3\cdot 2 - 1) = x_{1i}^2 - x_{oi}^2 = 256 - 25 = 231 = (16+5)(16-5) = 21\cdot 11;$$

$$\Gamma_п\ (2\cdot 10) - \Gamma_л\ (7\cdot 2 - 1) = x_{1i}^2 - x_{oi}^2 = 400 - 169 = 231 = (20+13)(20-13) = 33\cdot 7;$$

$$\Gamma_п\ (2\cdot 20) - \Gamma_л\ (19\cdot 2) = x_{1i}^2 - x_{oi}^2 = 600 - 1369 = 231 = (40+7)(40\ 37) = 77\cdot 3;$$

$$\Gamma_п(2\cdot 58) - \Gamma_л(58\cdot 2 - 1) = x_{1i}^2 - x_{oi}^2 = 1\ 16^2 - 1\ 15^2 = (1\ 16+1\ 15)(1\ 16 - 1\ 15) = 231\cdot 1.$$

Наличие различных представлений ф-инварианта $k_п(N)/2$ несколькими суммами свидетельствует о том, что ***N*** составное число и в его интервальной модели контурный состав формируется в разных областях НРЧ.

Так для ***N = 231*** в НРЧ существуют четыре интервала. Ближний к началу НРЧ интервал включает контуры с номерами от контура ***3*** до контура ***8***, от большего из которых в интервал включатся только левый полуконтур. Существует второй интервал, включающий контуры с номерами от контура ***7*** до контура ***10***, и еще один интервал от контура ***19*** до ***20*** и, наконец, предельный контур с номером ***58*** , левый полуконтур которого и есть число равное ***N = 231.*** Причем, от большего контура в каждом случае берется лишь его левый полуконтур.

Рассмотренный пример иллюстрирует все возможные решения задачи факторизации числа ***N = 231*** на два сомножителя (фактора). По основной теореме арифметики в разложениях ***N*** необходимо указывать все простые делители для числа ***N.*** Это выполняется несложно, применяя алгоритм к найденным факторам до тех пор, пока все факторы не станут простыми числами. Здесь приведено решение задачи, но не по-

казано, как оно получено. Ранее указывались отдельные возможные способы нахождения решений. Этот вопрос достаточно объемный и сложный и не рассматривается в работе детально.

Пример 6. (Взаимосвязь характеристик интервальной и нумерационной моделей числа кратного трем).

Для левого числа $N(x_1, x_o) = 183$ и правого числа $N(x_1, x_o) = 189$ выполнить факторизацию, определить значение предельного контура чисел $k_п\ (N_л) = k_п\ (183) = (183 + 185)/8 = 46$, и $k_п(N_п) = k_п(189) = (187 + 189)/8 = 47$. Далее составляется уравнение в общем виде для номера предельного полуконтура в нумерационной модели $k_п\ (183)/2 = (k + 1)/2 + k$, откуда $k_п = 3k + 1$ и $k = (k_п - 1)/3 = 45/3 = 15$. Большая граница интервала для $N = 183$ правая четная $Г_ц(16) = (2 \cdot 16)^2 = 32^2 = 1024$ и меньшая левая граница $Г_л(15) = (2 \cdot 15 - 1)^2 = 29^2 = 841$. Факторизация числа $N = 183 = 32^2 - 29^2 = (32 + 29)(32 - 29) = 61 \cdot 3$.

Связь правых чисел вида $N_п(x_1, x_o) = 3t$ (t - произвольное ННЧ) с суммой номеров контуров интервальной модели следующая: половина номера контура плюс номер следующего контура интервала равны половине номера предельного контура $k_п\ (N_п)/2$ исследуемого числа.

Для правого числа $N(x_1, x_o) = 189$ значение предельного полуконтура $k_п\ (189)/2 = (k - 1)/2 + k$, откуда:

$$k_п = 47 = 3k - 1 \text{ и } k = (k_п + 1)/3 = 48/3 = 16.$$

Меньшая граница интервала для $N = 189$ левая четная лежит в 15 контуре $Г_ц(15) = (2 \cdot 15)^2 = 30^2 = 900$ и $Г_п(16) = (2 \cdot 16 + 1)^2 = 33^2 = 1089$.

Факторизация числа:

$$N = Г_п(16) - Г_ц(15) = 1089 - 900 = (33 + 30)(33 - 30) = 63 \cdot 3$$

Аналогичные расчеты могут быть выполнены для чисел левых и правых кратных $5, 7, 9$ и т.д.

4. Специальные разбиения натурального числа кратного трем. Натуральные нечетные числа $N(x_1, x_o) = 3t$ (t – произвольное нечетное) кратные трем всегда формируются тремя смежными полуконтурами, два из которых – целый контур. Пусть номер целого контура обозначен как k. Для таких чисел нумерационная модель очень простая. Для левых нечетных натуральных чисел:

$k_п(N_л)/2 = k + (k + 1)/2 \rightarrow k_п(N_л) = 3k + 1$. Отсюда $k = (k_п(N_л) - 1)/3$.

Для правых нечетных натуральных чисел:

$k_п(N_п)/2 = (k - 1)/2 + k \rightarrow k_п(N_п) = 3k - 1$. Отсюда $k = (k_п(N_п) + 1)/3$.

Пример 7. (*Факторизация чисел кратных числу три*). Задано составное кратное трем нечетное число $N = 129 = 3 \cdot 43$. Это число правое, так как $129 \equiv 1 (\mathrm{mod} 4)$.

Предельный контур для этого числа имеет длину $127 + 129 = 256$. Номер $k_п(129)$ предельного контура числа равен $k_п(129) = 256/8 = 32$. Ф-инвариант для числа 129 равен $k_п(129)/2 = 32/2 = 16$. Подставляем в формулу для k найденные значения $k = (32 + 1)/3 = 1\ 1$. Это номер большего контура из двух полуконтуров $43 + 45 = 88 = 1 \cdot 18$. Для формирования интервала включаем в сумму правый (больший) полуконтур из предшествующего контура с номером $k_{пр} = 10 = 1\ 1 - 1$, длина которого $M = 4k_{пр} + 1 = 41$.

И окончательно, длина интервала позиций для числа $N = 129$ есть сумма трех полуконтуров $129 = 41 + 43 + 45$. Теперь можно найти значения границ этого интервала и факторизовать N.

– меньшая граница интервала $Г_л(129) = Г_ц(k = 10)$ – это левая граница для контура с номером 10, $Г_w(10) = (2 \cdot 10)^2 = 400 = 20^2$;

– большая граница интервала $Г_п(129) = Г_п(1\ 1)$ – это правая граница для правого контура с номером $1\ 1$, $Г_ц(1\ 1) = (2 \cdot 1\ 1 + 1)^2 = 529 = 23^2$;

Интервал числа $N = 129$ представляем разностью границ

$$Г_п(129) - Г_л(129) = Г_п(1\ 1) - Г_ц(10) = 23^2 - 20^2 = (23 - 20)(23 + 20)$$

и получаем разложение N на множители $3 \cdot 43 = 129$.

Пример 8. (*Разбиение правого числа, где половина номера предельного контура (не целое число) в сумму берется от меньшего контура).* Для правого числа $N(x_1, x_o) = 621$ выполнить факторизацию.

Будем формировать нумерационную модель числа. Определяем номер $k_п(N_п)$ по значению длины предельного контура числа 621, $k_п(N_п) = k_п(621) = (621 - 1)/4 = (619 + 621)/8 = 155$. Затем определяем его половину $k_п(621)/2 = 77{,}5$ и находим разность $C^2_{k+1} - k_п/2$, ближнюю к началу НРЧ. В столбце C^2_{k+1} (см. табл. *2* [3]) находим при $k = 12$ значение 78, превышающее $k_п(621)/2 = 77{,}5$. Тогда искомая разность $C^2_{k+1} - k_п/2 = 78 - 77{,}5 = 0{,}5$. Проверяем, совпадает ли найденная разность со значением $k^2/2$ при некотором значении k. Совпадение имеет место со значением $0{,}5$ в нижней строке таблицы. Отсюда определяется номер меньшего контура $k_п^2/2 = 0{,}5 \rightarrow k = 1$, формируемого интервала. Интервал, представляющий число $N = 621$, начинается средней точкой квадрата (четной) первого контура и доходит до 12-го контура включительно. Известно, что через границы длина интервала для числа N представляется выражением $N = Г_п - Г_л = x_{1i}^2 - x_{oi}^2$. Зная номера контуров на границах интервала, находим его граничные точки. Границами интервала будут:

для правого полуконтура первого контура левая граница $\Gamma_л = (2k)(2\cdot1)^2 = 4$, и правая граница контура при $k = 12$ есть $\Gamma_п = (2k+1)^2 = (2\cdot12+1)^2 = 625$.

Тогда $N = \Gamma_п - \Gamma_л = x_{1i}^2 - x_{oi}^2 = 625 - 4 = 621$. С другой стороны, при наличии границ легко выполняется факторизация числа:

$$N = x_{1i}^2 - x_{oi}^2 = (25 + 2)(25 - 2) = 27\cdot23.$$

Рассмотренная в примере схема решения задачи факторизации обеспечивает нахождение и других альтернативных пар границ. Поиск разности $C_{k+1}^2 - k_п/2$, совпадающей с $k^2/2$ приводит к получению такого совпадения при большем $k = 19$.

Имеем равенство $C_{k+1}^2 - k_п/2 = 190 - 77{,}5 = 1\ 12{,}5$ из которого находим меньшее $k = \sqrt{2\cdot112{,}5} = \sqrt{225} = 15$. Теперь можно приступить к поиску границ интервала и факторизации.

Границами интервала будут:
левая граница при $k = 15$, $\Gamma_л = (2k)^2 = (2\cdot15)^2 = 900$, и
правая граница при $k = 19$ есть $\Gamma_п = (2k + 1)^2 = (2\cdot19 + 1)^2 = 39^2 = 1521$, $N = \Gamma_п - \Gamma_л = x_{1i}^2 - x_{oi}^2 = 1521 - 900 = 621$ и $N = x_{1i}^2 - x_{oi}^2 = (39+30)(39-30) = 69\cdot9$.

Пример 9. (*Разбиение левого числа, где половина номера предельного контура (не целое число) в сумму берется от большего контура).* Пусть задано число $N = 235$, число $N = 235 \equiv 3 (\mathrm{mod}\, 4)$ левое. Для числа 235 длина предельного контура $L_п = 235 + 237 = 472$, его номер $k_п = L/8 = 472/8 = 59$, $k_п/2 = 29.5$, границы предельного контура: правая $\Gamma_п = (2k_п)^2 = 1\ 18^2$, левая $\Gamma_л = (2k_п - 1)^2 = 1\ 17^2$ им соответствует тривиальное разложение числа $N = 235\cdot1$.

Из нумерационной модели следует, что $k_п/2 = 29.5$. Для $N = 235$ (см. пример ранее) $k_п(235)/2 = 29.5$.

Ближайшее значение в столбце $n^2/2 = 40.5$ лежит в строке $n = 9$. Ему соответствует разность $n^2/2 - k_п/2 = 40.5 - 29.5 = 1\ 1$, которая отсутствует в столбце «сумма». Следующий допустимый уровень $n = 1\ 1$ и $n^2/2 = 60.5$, ему соответствует разность $n^2/2 - k_п/2 = 60.5 - 29.5 = 31$, которая также отсутствует в столбце «сумма». Следующий допустимый уровень $n = 13$ и $n^2/2 = 84.5$, ему соответствует разность $n^2/2 - k_п/2 = 84.5 - 29.5 = 55$, которая присутствует в столбце «сумма» в строке с номером 10.

Отсюда следует вывод о том, что все строки диаграммы Ферера, начиная с номера 10 и ниже, не включаются в сумму $k_п/2$. Следовательно, $k_п/2 = 29.5 = 1\ 1 + 12 + 13/2$.

Выполним факторизацию заданного числа. Найдены номера контуров, образующие нумерационную модель числа: $k = 1\ 1, 12$ и 13. От $k =$

13 в формулу входит лишь левая половина этого контура. Вычислим длины контуров ***L(1 1 =8·1 1 = 88; L(12) = 8·12 = 96; L(13) = 8·13 = 104;*** левая половина (полуконтур) ***13***-го контура ***m(13)=104/2–1=51***. Интервальная модель ***88 + 96 + 51 = 235***.

Определим границы интервальной модели:

$$\Gamma_п(13) = (2\cdot 13)^2 = 26^2 = 676;\ \Gamma_л(1\ 1) = (2\cdot 1\ 1 - 1)^2 = 21^2 = 441.$$

Теперь число $N = 235$ можно факторизовать:

$$N(x_1, x_o) = 235 = (x_1 + x_o)(x_1 - x_o) = (26 + 21)(26 - 21) = 47\cdot 5 = 235.$$

Пример 10. (*Разбиение правого числа, где половина номера предельного контура (не целое число) в сумму берется от меньшего контура).* Пусть $N = 357$. Это правое число $N = 357 \equiv 1 (\mathbf{mod}\, 4)$. Длина предельного контура $L_п = 357 + 355 = 712$, его номер $k_п = L/8 = 712/8 = 89$, $k_п/2 = 44.5$, границы предельного контура: левая $\Gamma_л = (2\ k_п - 1)^2 = 177^2$, средняя $\Gamma_ц = (2\ k_п) = 178^2$, правая $\Gamma_п = (2\ k_п + 1)^2 = 179^2$ им соответствует тривиальное разложение числа $N = 357\cdot 1$.

а) $x_1 = 19;\ x_o = 2;\ N = \Gamma_п(2\cdot 58) - \Gamma_л(58\cdot 2 - 1) = x_{1i}^2 - x_{oi}^2 = 19^2 - 2^2 = 361 - 4 = (19 + 2)\cdot(19 - 2) = 21\cdot 17 = 357,\ k_п/2 = ½ + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 44.5$

б) $x_1 = 61;\ x_o = 58;\ N = \Gamma_п(2\cdot 58) - \Gamma_л(58\cdot 2 - 1) = x_{1i}^2 - x_{oi}^2 = 61^2 - 58^2 = 3721 - 3364 = (61 + 58)\cdot(61 - 58) = 1\ 19\cdot 3 = 357;\ k_п/2 = 29/2 + 30 = 44.5.$

Длина произвольных контура и интервала натурального ряда чисел между нечетными квадратами кратна числу ***8***. Вычет нечетного квадрата по **mod** ***8*** равен ***1***. Разность квадратов нечетных простых чисел ≥ 5 кратна ***24*** ($7^2 - 5^2 = 24$). Это можно показать следующим образом. Рассмотрим квадраты двух нечетных простых чисел, а затем найдем их разность. Из трех смежных чисел $2n - 1,\ 2n,\ 2n + 1$ одно всегда кратно трем. В нашем случае – это число n, так как крайние числа простые по условию.

$$Нч_1^2 = (2n - 1)^2 = 4n^2 - 4n + 1 = 1 + 4n(n - 1) = 1 + 8\ C_n^2,$$

$$Нч_2^2 = (2n + 1)^2 = 4n^2 + 4n + 1 = 1 + 4n(n + 1) = 1 + 8\ C_{k+1}^2,$$

$$Нч_2^2 - Нч_1^2 = 8(C_{k+1}^2 - C_n^2) = 4n(n + 1 - n + 1) = 8n = 8\cdot 3t = 24t.$$

Если число N кратно 3, оно в интервальной модели образовано тремя полуконтурами, стоящими рядом. Другими словами, если число правое, то полуконтур от меньшего контура. Для $N = 357 = 1\ 19\cdot 3,\ k_п/2 = 44.5$. Значение номера полуконтура определяется формулой $(k_п/2 - 1)/3 = (44/5 - 1)/3 = 14.5$. Следовательно, номер меньшего контура $14.5\cdot 2 = 29$, а номер следующего 30. Действительно, $29/2 + 30 = 44.5$ =

$k_п/2$. Если число N кратно 5 (образовано пятью полуконтурами), то номер $(k_п/2 – 6)/5$.

Пример 11. (*Восстановление числа $N_п$, кратного трем по номеру меньшего контура*). Задан номер левого контура в интервальной модели числа $N_п$ кратного трем с номером $k = 40$. Тогда ф-инвариант:

$$k_п(N_п)/2 = 40/2 + 41 = 61,$$

а длина интервала, представляющего число в интервальной модели:

$$L = 20·8 + 1 + 41·8 = 161 + 328 =161 +163 + 165 = 489.$$

Это правое нечетное число, так как $489 \equiv 1 (\mathbf{mod} 4)$. Границы интервала в интервальной модели обрабатываемого числа: правая большая $Г_п(41) = (2·41 + 1)^2 = 83^2 = 6889$; левая меньшая – четное число

$$Г_л(40) = (2·40)^2 = 80^2 = 6400.$$

Представление числа разностью границ интервала $N_п(x_1, x_о) = Г_п – Г_л = 83^2 – 80^2 = 6889 – 6400 = 489$ и его факторизация имеет вид: $N_п(x_1, x_о) = N_п(83, 80) = (83 + 80)(83 – 80) = 163·3 = 489$.

Число 163 – простое и других разложений не существует.

Пример 12. Пусть задано число $N(x_1, x_о) = 663 = 3t$, кратное трем. Это левое число, так как $663 \equiv 3 (\mathbf{mod} 4)$. Границы интервала модели числа правая большая четная и левая меньшая нечетная. Сам интервал образован контуром с номером k и левым полуконтуром $(k + 1)$-го контура. Рассмотрим нумерационную модель числа. Половина номера предельного полуконтура заданного числа $k_п(N_л)/2 = k_п(663)/2 = (663 + 665)/16 = 83 = k + (k + 1)/2 = (3k + 1)/2$, откуда $k = (166 – 1)/3 = 55$.

Выполним переход к интервальной модели числа. Длина интервала $L(k + (k + 1)/2) = 8·55 + 8·56/2–1 = 440 + 223 = 663$.

Значения границ интервальной модели:

$$Г_п(56) = (2·56)^2 = 1\ 12^2 = 12544;\ Г_л(55) = (2·55 – 1)^2 = 109^2 = 1\ 1881.$$

Теперь число N можно факторизовать $N(x_1, x_о) = 663 =$
$= (x_1 + x_о)(x_1 – x_о) = (1\ 12 +109)(1\ 12 –109) = 221·3 = 3·13·17 = 663$.

Пример 13. (*Разбиение инварианта левого $N_л$ числа, где половина номера (целое число) контура, включаемого в сумму, берется от большего контура).*

Пусть $N = 207$, число левое $N =207 \equiv 3 (\mathbf{mod} 4)$. Длина предельного контура $L_п=207+209 =416$, его номер $k_п = L/8=416/8=52$, $k_п/2=26$. Границы предельного полуконтура: правая $Г_п = (2k_п)^2 =104^2$, левая $Г_л=(2k_п – 1)^2 = 103^2$. Этим границам соответствует тривиальное мультипликативное разложение числа $N = 207 = 207·1$.

Из нумерационной модели следует, что имеются три разбиения $k_п(N_л)/2 = k_п(207)/2 = 17 +18/2 = 26 =4 +5 +6 +7 +8/2 = 4 +5 + 6+7 + 4.$

Эти разбиения в полном списке ***2436*** разбиений числа ***26*** имеют лексикографические номера

№***927*** →***76544*** (разбиение содержит две одинаковые части (четверки)), №***2369*** → ***17+ 9***. Для $N = 231$ (см. пример ***1*** ранее) $k_п(231)/2 = 29$ или ***3 + 4 + 5 + 6 + 7 + 8/2 = 29*** в разбиении также присутствуют две четверки. Результат факторизации $207 = 23 \cdot 9 = 69 \cdot 3.$

5. Заключение. На основе нового подхода к описанию натурального ряда чисел, в котором главная роль отводится положению квадратов натуральных чисел и интервалов между ними, формируется конструктивная модель НРЧ. Нечетные числа распределены в *два класса*: левые и правые. Модель используется для синтеза операции обращения произведения чисел, т.е. решения задачи *факторизации* больших чисел. Многочисленные числовые примеры иллюстрируют сведение ЗФБЧ к задаче формирования специальных разбиений числа.

В модели НРЧ используются понятия *контура* – расстояния между квадратами последовательных нечетных чисел, *полуконтура* – расстояния между квадратами смежных чисел, положение которых естественным образом упорядочено в пределах НРЧ. Этот порядок в модели реализуется естественной (от первого контура между 3^2 и ***1*** с увеличением на единицу для последующих) *нумерацией* контуров и полуконтуров. Положение контуров в НРЧ постоянное. С каждым контуром связывается пара полуконтуров, им также соответствуют номера. Вводятся понятия *длины* L контуров (полуконтуров) и, что особенно важно, их *границы*, роль которых играют квадраты чисел.

Любое нечетное число $N = pq,\ p < q,$ в модели НРЧ представляется непрерывной последовательностью нечетного количества (равного p) полуконтуров (фрагментом арифметической прогрессии со средним членом равным q), которая названа *интервалом*. Интервалы могут перемещаться вдоль НРЧ, но их границы всегда квадраты чисел разной четности.

Такое свойство обусловливает возможность представления длины интервалов (равна значению $L = N$) разностью их правой и левой границ $N = Г_п - Г_л = x_{1i}^2 - x_{oi}^2$ из чего следует мультипликативная форма записи для числа $N = (x_{1i} - x_{oi})(x_{1i} + x_{oi})$, соответствующая его факторизации.

Наличие нескольких альтернативных интервалов для представления нечетного числа N обусловлено множеством его простых делителей. Для определения положения альтернативных интервалов в НРЧ вводится понятие *ф-инварианта* нечетного числа, значение которого

сохраняется независимо от рассматриваемого альтернативного интервала. Эта числовая характеристика $\boldsymbol{N}$ допускает ее представление комбинаторными *разбиениями специального вида*, в которых роль частей разбиения играют номера контуров, формирующих интервалы для $\boldsymbol{N}$.

Все сформулированные положения обеспечивают универсальность подхода и допускают алгоритмизацию. Создаваемые алгоритмы базируются на свойствах, практически не зависящих от разрядности чисел, на использовании границ интервалов для $\boldsymbol{N}$, являющихся квадратами, что позволяет предположить высокое быстродействие при практической реализации.

Литература

1. *Бронштейн И.Н., Семендяев К.А.* Справочник по математике для инженеров и учащихся ВТУЗов // М.: ГИТТЛ. 1954. 608 с.
2. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии // М.: МЦНМО. 2003. 328 с.
3. *Ваулин А.Е., Назаров М.С.* Сведение задачи факторизации натурального числа к задаче разбиения числа на части. Часть 1 // Труды СПИИРАН. 2015. Вып. 39. С. 157-176.
4. *Ваулин А.Е.* и др. Фундаментальные структуры натурального ряда чисел // Сб.тр. 7-го Международного симпозиума. М.: РУСАКИ. 2006. С. 384–387.
5. *Ваулин А.Е.* Новый метод факторизации больших чисел в задачах анализа и синтеза двухключевых криптографических алгоритмов. Ч.1. // Информация и космос. 2005. №3. С. 74–78.
6. *Ваулин А.Е.* Новый метод факторизации больших чисел в задачах анализа и синтеза двухключевых криптографических алгоритмов. Ч.2. // Информация и космос. 2005. №4. С. 104 –112с.
7. *Дэвенпорт Г.* Высшая арифметика // М.: Наука. 1966. 176 с.
8. *Евклид*. Начала. М–Л. 1948–1950. Т. 1–3.
9. RSA. URL: https://ru.wikipedia.org/wiki/RSA.
10. *Ноден П., Китте К.* Алгебраическая алгоритмика (с упражнениями и решениями) // М. Мир. 1999. 720 с.
11. *Пойа Д.* Математика и правдоподобные рассуждения // М.: ИЛ. 1957. 464 с.
12. *Ферма П.* Исследования по теории чисел и диофантову анализу // М.: Наука. 1992. 320 с.
13. *Эндрюс Г.* Теория разбиений // М.: Наука. 1982. 256 с.
14. *Дирихле П.Г.Л.* Лекции по теории чисел //М.: Книжный дом «ЛИБРОКОМ». 2014. 368с.
15. *Манин Ю.И., Панчишкин А.А.* Введение в современную теорию чисел // М.: МЦНМО. 2013. 552с.
16. *Шафаревич И.Р.* Основы алгебраической геометрии //М.:МЦНМО. 2007.589с.

References

1. Bronshtejn I.N., Semendyaev K.A. *Spravochnik po matematike dlja inzhenerov i uchashhihsja VTUZov* [Handbook of mathematics for engineers and students VTUZov]. M.: GITTL. 1954. 608 p. (In Russ.).
2. Vasilenko O.N. *Teoretiko-chislovye algoritmy v kriptografii* [Number-theoretic algorithms in the cryptography]. M.: MTsNMO. 2003. 328 p. (In Russ.).

3. Vaulin A.E., Nazarov M.S. [Reduction of the integer factorization problem to the partition number on the part. Part 1]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2015. vol. 39. pp. 157-176.
4. Vaulin A.E. et al. [The fundamental structure of the naturally row numbers]. *Sb.tr. 7-go Mezhdunarodnogo simpoziuma – Proceedings of the 7th International Symposium*. M.: RUSAL KI. 2006. pp. 384–387. (In Russ.).
5. Vaulin A.E. [A new method of factoring large numbers in the analysis and synthesis of two-key cryptographic algorithms. Part 1]. *Informacija i kosmos – Information and Space.* 2005. no. 3. pp. 74– 78. (In Russ.).
6. Vaulin A.E. [A new method of factoring large numbers in the analysis and synthesis of two-key cryptographic algoritmov. Part 2]. *Informacija i kosmos – Information and Space.*. 2005. no. 4. pp. 104–112. (In Russ.).
7. Davenport G. *Vysshaja arifmetika* [Higher Arithmetic]. M.: Nauka. 1966. 176 p.
8. Euclid. *Euclid's Elements*. M-L. 1948–1950. vol. 1–3. (In Russ.).
9. RSA. Available at: https://ru.wikipedia.org/wiki/RSA. (In Russ.).
10. Noden P., Kitte K. *Algebraicheskaja algoritmika (s uprazhnenijami i reshenijami)* [Algebraic algorithmics (with exercising and decisions)]. Moscow: Mir, 1999. 720 p. (In Russ.).
11. Pojja D. *Matematika i pravdopodobnye rassuzhdenija* [Mathematics and plausible reasoning]. M.: IL, 1957. 464 p. (In Russ.).
12. Ferma P. *Issledovanija po teorii chisel i diofantovu analizu* [Studies in number theory and diophantine analease]. M.: Nauka. 1992. 320 p. (In Russ.).
13. Andrews G. *Teorija razbienij* [The Theory of partitions]. M.: Nauka. 1982. 256 p. (In Russ.).
14. Dirichlet P.G.L. *Lekcii po teorii chisel* [Lectures on the theory of numbers]. M.: Knizhnyj dom «LIBROKOM». 2014. 368 p. (In Russ.).
15. Manin Y.I., Panchishkin A.A. *Vvedenie v sovremennuju teoriju chisel* [Introduction to the modern theory of numbers]. M.: MCNMO. 2013. 552 p. (In Russ.).
16. Shafarevich I.R. *Osnovy algebraicheskoj geometrii* [Foundations of algebraic geometrii]. M.:MCNMO. 2007.589 p. (In Russ.).

Ваулин Арис Ефимович — к-т техн. наук, доцент, доцент кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: криптоаналитиз, теория автоматов. Число научных публикаций — 200. mikl21@mail.ru; ул. Ждановская д.13, Санкт-Петербург, 197082; р.т.: +7(812)347-9687.

Vaulin Aris Efimovich — Ph.D., associate professor, associate professor of system for collecting and processing information department, Mozhaisky military space Academy. Research interests: information security in automated systems for special purposes, cryptanalyst. The number of publications — 200. mikl21@mail.ru; 13, Zhdanovskaya street, St. Petersburg, 197198, Russia; office phone: +7(812)347-9687.

РЕФЕРАТ

Ваулин А.Е. **Сведение задачи факторизации натурального числа к задаче разбиения числа на части. Часть 2.**

Новый подход к проблеме факторизации составных целых чисел рассматривается работе. Предполагается, что новый метод и алгоритм будет быстродействующим и эффективным при его реализации. Метод базируется на использовании свойств чисел, слабо зависящих от их разрядности, что как ожидается, обеспечит ему высокую степень универсальности.

Большую роль при разработке метода играет изучении внутреннего строения натурального ряда чисел и создание его модели, включающей ряд новых понятий. Применения таких понятий как контур, полуконтур, интервал, границы объектов модели и некоторых других понятий обеспечивают разработку моделей отдельных нечетных чисел. Введение понятия ф-инварианта нечетных чисел, для которых рассматриваются два класса: левые и правые, открывает возможность выполнить переход от традиционного подхода к решению задачи факторизации к сведению поиска разбиений числа специального вида. При этом ожидается, что проблема будет менее сложной.

SUMMARY

Vaulin A.E. **Conversion of Integer Factorization to a Problem of Decomposition of a Number. Part 2.**

A new approach to the problem of factoring integers is considered in this work. It is assumed that the new method and the algorithm are fast and efficient in its implementation. The method is based on the properties of numbers, slightly dependent on their digits, which is expected to provide it with a high degree of versatility.

Important role in the development of a method plays a study of the internal structure of the positive integers and the creation of their model, which includes a number of new concepts. Application of concepts such as contour, half contour, the interval boundaries of model objects and some other concepts ensure the development of individual models of odd numbers.

The introduction of the concept of f-invariant of odd numbers, for which two classes are considered: the left and right, opens the possibility to perform the transition from the traditional approach to solving the factorization problem to a retrieval task of partitions of a number of a special kind. It is expected that the problem would be less complicated.

УДК 004.93

Л.А. Станкевич, К.М. Сонькин, Ж.В. Нагорнова, Ю.Г. Хоменко, Н.В. Шемякина

КЛАССИФИКАЦИЯ ЭЛЕКТРОЭНЦЕФАЛОГРАФИЧЕСКИХ ПАТТЕРНОВ ВООБРАЖАЕМЫХ ДВИЖЕНИЙ ПАЛЬЦАМИ РУКИ ДЛЯ РАЗРАБОТКИ ИНТЕРФЕЙСА МОЗГ-КОМПЬЮТЕР

Станкевич Л.А., Сонькин К.М., Нагорнова Ж.В., Хоменко Ю.Г., Шемякина Н.В. **Классификация электроэнцефалографических паттернов воображаемых движений пальцами руки для разработки интерфейса мозг-компьютер.**

Аннотация. В работе приводятся результаты классификации электроэнцефалографических (ЭЭГ) паттернов кинестетического воображения движений пальцами и кистью одной руки в заданном ритме на основе метода опорных векторов и разработанного комитета искусственных нейронных сетей. Показано, что точность попарной классификации ЭЭГ-паттернов воображаемых движений с использованием комитета искусственных нейронных сетей в среднем была выше, чем при использовании классификатора на основе метода опорных векторов. Выявлена возможность увеличения точности распознавания воображаемых движений мелкой моторики при использовании индивидуального подхода к выбору параметров классификации паттерна ЭЭГ сигнала.

Ключевые слова: кинестетическое воображение, пальцы одной руки, электроэнцефалограмма, комитет искусственных нейронных сетей, метод опорных векторов на основе радиальной базисной функции, одиночные пробы, интерфейс мозг-компьютер.

Stankevich L.A., Sonkin K.M., Nagornova Zh.V., Khomenko Ju.G., Shemyakina N.V. **Classification of Electroencephalographic Patterns of Imaginary One-hand Finger Movements for Brain-Computer Interface Development.**

Abstract. The results of kinesthetic motor imagery EEG-pattern classification of one hand fingers and wrist movements executed in a given rhythm are presented in this study. The classifiers were based on the support vector machine method and on the developed neural network committee. It was shown that the accuracy of pairwise EEG-pattern classification of imaginary movements by means of the neural network committee was higher on average than the accuracy of the support vector machine classifier. The possibility of improving the accuracy of fine motor imaginary classification was revealed with the help of individual approach implementation for selection of EEG-pattern classification parameters.

Keywords: kinesthetic motor imagery, fingers of one hand, electroencephalography, neural network committee, support vector machine with radial basis function, single trial, brain-computer interface.

1. Введение. Задача распознавания электроэнцефалографических паттернов (ЭЭГ-паттернов) воображаемых движений является крайне актуальной для проблемы реабилитации пациентов с нарушениями центральной нервной системы и обездвиженных пациентов. Разработка эффективного неинвазивного интерфейса «мозг-компьютер» (ИМК) обеспечит возможность взаимодействия человека с окружающим миром путем управления внешними исполнительными устройствами, такими как протезы конечностей, экзоскелет, инвалидные кресла,

функциональные электростимуляторы мышц и др. [1-3]. Ключевой проблемой совершенствования ИМК, основанных на распознавании ЭЭГ-паттернов воображаемых движений, является задача увеличения степеней свободы, т.е. увеличения количества распознаваемых биоэлектрических сигналов, при их небольшом накоплении. Одним из методов увеличения степеней свободы является переход от различения воображаемых движений относительно крупных частей тела (ног, рук, предплечий, головы) к различению воображаемых движений мелкой моторики (пальцев и кисти одной руки). В литературе описаны исследования, подтверждающие принципиальную различимость сигналов ЭЭГ мелкой моторики [4-6]. Однако, вследствие локализации источников распознаваемых сигналов мелкой моторики одной руки в анатомически близких зонах коры головного мозга и вариативности сигналов у разных испытуемых, на математический аппарат классификации налагаются особые требования по точности и индивидуальной настройке. Важными и нерешенными остаются вопросы повышения точности распознавания воображаемых движений-команд, снижения времени формирования управляющей команды и поиска параметров индивидуальной настройки классификатора.

Цель исследования состояла в разработке методики и средств классификации ЭЭГ-паттернов воображаемых движений пальцев одной руки и сравнительной оценке их эффективности. Классификация ЭЭГ-паттернов воображаемых движений пальцев одной руки проводилось с использованием двух подходов: метода опорных векторов (support vector machine - SVM) и комитета искусственных нейронных сетей (artificial neural networks - ANN). Это позволило получить новые данные, свидетельствующие о преимуществе реализованного нейросетевого подхода при классификации ЭЭГ-сигналов без накопления.

2. Методика получения, исследования и анализа данных.

2.1. Испытуемые. В исследовании приняли участие пять здоровых праворуких испытуемых (трое мужчин, две женщины, средний возраст – 32.8±3.1 [SD]). Испытуемые принимали участие в исследовании добровольно, согласно правилам и этическим нормам проведения исследований с участием волонтеров (Хельсинкская декларация 1964 с последующими изменениями и дополнениями).

2.2. Задания. В отдельных блоках заданий испытуемым предлагалось выполнить поочередно пять типов воображаемых движений (каждый блок проб состоял из движений одного типа) – мизинцем, большим, указательным, средним пальцами правой руки.

Еще одним типом движения, выполняемого испытуемыми, было сжатие мяча кистью правой руки (имитация взятия кружки).

Испытуемые должны были сначала в задаваемом звуками ритме нажимать на кнопку компьютерной мыши обозначенным, согласно инструкции исследователя, пальцем или сжимать мяч, а затем продолжать воображать соответствующее движение, когда звук пропадал. Инструкция на воображение движений была ориентирована на инициацию кинестетических ощущений у испытуемого [7].

Внутри одного блока задания серии реальных и воображаемых движений повторялись многократно. В результате, испытуемый выполнял не менее ста реальных и ста воображаемых движений в заданном ритме внутри одного блока задания. Количество блоков задания соответствовало количеству типов выполняемых движений (реальных/воображаемых (нажатий/сжатий)). Схема фрагмента блока проб приведена на рисунке 1:

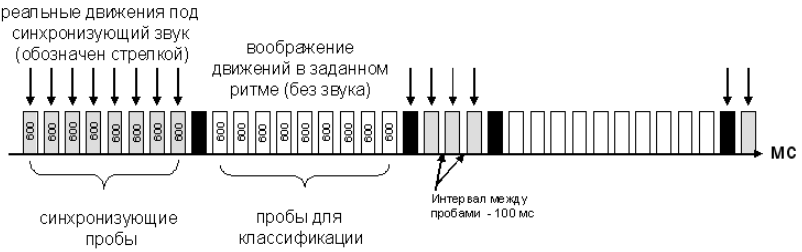


Рис. 1 Схема фрагмента блока проб с реальными движениями под синхронизующих звук и воображаемыми движениями в заданном звуками ритме (без звука)

На рисунке 1 черным цветом обозначены пробы, которые были исключены из рассмотрения, так как испытуемый мог в это время по инерции нажать на кнопку, когда синхронизующий звук пропадал или же наоборот – не успеть нажать на кнопку, когда он появлялся после проб на воображение.

Порядок выполнения блоков проб с разными типами движений был псевдорандомизирован между испытуемыми, чтобы избежать влияния эффекта утомления на выполнение заданий в одной и той же последовательности разными испытуемыми. Для контроля движений пальцев и кисти испытуемого во время выполнения реальных и воображаемых движений проводилась регистрация миограммы. Далее для анализа (классификации) использовали только пробы с воображаемыми движениями пальцами одной руки и сжатием мяча без миографических артефактов.

2.3. Процедура регистрация ЭЭГ. Регистрация ЭЭГ проводилась с помощью 32-х канального цифрового электроэнцефалографа «Мицар» (ООО «Мицар», С.-Петербург) посредством программного пакета WinEEG (Пономарев В.А., Кропотов Ю.Д., № государственной регистрации 2001610516 от 08.05.2001). Референт располагался на мочках обоих ушей, заземляющий электрод – в передне-центральном отведении на поверхности головы. ЭЭГ регистрировалась в полосе от 0.53 Гц – 30 Гц. Сопротивление электродов не превышало 5 кОМ, частота дискретизации на канал - 2000 Гц. Общая частота дискретизации составила 500 Гц. В ЭЭГ записях испытуемых помечались артефакты движения глаз, медленные волны (0-1 Гц с амплитудой больше 50 мкВ), быстрые волны (20-35 Гц с амплитудой выше 35 мкВ), фрагменты ЭЭГ с амплитудой сигнала больше 100 мкВ. Далее данные экспортировались в текстовый формат и пробы, содержащие артефакты, исключались из анализа данных.

Для анализа использовали записанную биоэлектрическую активность с сенсомоторных областей коры – отведения C3, Cz по системе 10-20 [8]. Временная область анализа соответствовала 600 мс от начала пробы. В это окно предположительно попадали последние этапы подготовки к воображаемому движению и само воображаемое движение, ранее задававшееся звуковыми стимулами на 300 мс от начала пробы.

2.4. Алгоритм вычисления характерных признаков сигналов ЭЭГ. Анализ сигналов ЭЭГ производился во временной области. *Первым шагом* алгоритма являлось выполнение операции накопления сигнала путем суммирования нескольких образцов сигналов (проб) одного типа воображаемых движений. Данный шаг направлен на увеличение соотношения сигнал-шум, т.е. на выделение слабого информативного сигнала. Подход основан на том факте, что сигнал, связанный с воображением определенного типа движения, повторяется в серии проб, а математическое ожидание сигнала фонового состояния стремится к нулю. С целью исследования влияния накопления сигнала на точность классификации в работе используется суммирование сигнала по 5, 10, 20 проб, а также подход без суммирования сигнала (по одной пробе).

Вторым шагом алгоритма являлось вычисление характерных признаков на основе предобработанных и накопленных сигналов. В данной работе реализован алгоритм совместного учета двух типов признаков – результатов интегрирования и вычисления длины кривой участка сигнала в скользящем окне. Важным для повышения точности

последующей классификации является выбор значения величины окна анализа. Ранее было показано, что подбор индивидуальных окон анализа может существенно повысить точность классификации воображаемых движений [6, 9, 10].

С целью реализации индивидуального подхода и выбора параметров, обеспечивающих наибольшую точность распознавания воображаемых движений у отдельных испытуемых, анализ сигналов ЭЭГ проводился во временных окнах, равных 30, 50, 70 отсчетам (один отсчет соответствует 2 мс). Сдвиг окна анализа составлял 50 процентов от рассматриваемой длины окна.

2.5. Статистический анализ данных проводился с использованием дисперсионного анализа ANOVA для больших сбалансированных планов, в качестве отдельных факторов рассматривались: комбинации пар воображаемых движений, тип классификатора, длина окна анализа, количество накоплений сигнала и испытуемые. Для каждой комбинации факторов было проведено 20 отдельных математических экспериментов с формированием непересекающихся наборов тестовых и обучающих выборок методом бутстрэпа [11]. В обучающую выборку входило 70% безартефактных проб, в тестовую – последующие 30% проб сформированной выборки.

3. Классификация ЭЭГ-паттернов. Точность классификации сложных временных рядов, таких как сигналы ЭЭГ, зависит от выбранных критериев распознавания, определяющих взаимное сочетание выделенных признаков сигналов и типов классификаторов. На основе сопоставительного анализа различных подходов в этой области были реализованы классификаторы, основанные на использовании метода опорных векторов и комитета искусственных нейронных сетей.

Работа классификаторов делилась на два этапа: обучение и тестирование. Предварительно данные разделялись на обучающую и тестовую выборки. На первом этапе на классификаторы подавалась обучающая выборка с присвоенными экспериментатором метками классов, и классификаторы строили модели, описывающие разделение выборки на заданные классы. На втором этапе происходила проверка адекватности построенной модели: на классификаторы подавалась тестовая выборка, не содержащая меток, для которой определяется принадлежность паттернов ЭЭГ к возможным классам. Далее определялась точность классификации (отношение проб, для которых были правильно определены классы, к общему количеству проб в тестовой выборке, выраженное в процентах), являющаяся мерой эффективности работы классификатора.

3.1. Классификатор на основе метода опорных векторов (SVM). Для распознавания паттернов ЭЭГ использовался классификатор на базе метода опорных векторов, предложенный В. Вапником и А. Червоненкисом [12]. Он относится к методам линейной классификации и заключается в разделении выборки на классы с помощью оптимальной разделяющей гиперплоскости, уравнение которой в общем случае имеет вид: $f(x) = (\omega,(x)) + b$, где $\omega = \sum_{i=1}^{N} \lambda_i y_i \ (x_i)$, коэффициенты λ_i зависят от y_i (векторов меток класса принадлежности) и от значения скалярных произведений $((x_i),(x_j))$. Таким образом, для нахождения решающей функции необходимо знать значения скалярных произведений. Преобразования данных определяются функцией-ядром: $K(x,y) = (\phi(x),\phi(y))$. В случае линейной классификации SVM ядро имеет вид: $K(x_i, x_j) = x_i^T x_j$.

На основании результатов исследований по выбору предпочтительного типа SVM [13,14,15] для классификации сигналов ЭЭГ в настоящей работе в качестве функции-ядра применена радиальная базисная функция Гаусса (radial basic function SVM - RBF SVM): $K\left(x_i, x_j\right) = \exp(-\gamma \left\| x_i - x_j \right\|^2)$, для $\gamma > 0$.

В данной работе для классификации использовалась библиотека LIBSVM [14] для MATLAB.

3.2. Классификатор на основе комитета искусственных нейронных сетей (ANN). Искусственные нейронные сети основаны на принципах нелинейной, распределенной, параллельной и локальной обработки данных и адаптации. Для совместного учета двух типов признаков был разработан комитет нейросетей, состоящий из двух нейросетей нижнего уровня и объединяющей их результаты нейросети верхнего уровня. Каждая из нейросетей нижнего уровня анализирует вектор признаков «своего» пространства признаков. Решения нейросетей нижнего уровня обрабатываются верхнеуровневой нейросетью, которая на их основе принимает окончательное решение о принадлежности данного ЭЭГ-сигнала некоторому классу из числа обученных.

В данном исследовании были использованы ANN типа многослойный персептрон с двумя скрытыми и одним выходным

слоями. Обучение сетей проводилось методом обратного распространения ошибки. В нейронах скрытых слоев была использована сигмоидная функция активации (гиперболический тангенс), а для нейронов выходного слоя – линейная функция. Процесс обучения сети продолжался до тех пор, пока не была достигнута назначенная пороговая точность классификации на всей обучающей выборке, или пока число итераций не превысит заданного значения.

Реализованный комитет ANN состоит из следующих элементов:

1) нейросеть нижнего уровня, классифицирующая вектора признаков, элементами которых являются площади под кривой ЭЭГ сигналов в скользящем окне;

2) нейросеть нижнего уровня, классифицирующая вектора признаков, элементами которых являются значения длины кривой ЭЭГ сигналов в скользящем окне;

3) нейросеть верхнего уровня, обобщающая результаты классификации сетей первого уровня и принимающая окончательное решение о принадлежности данного ЭЭГ-сигнала некоторому классу.

Алгоритм обучения комитета искусственных нейросетей включает в себя следующие шаги:

1) формирование векторов характерных признаков двух пространств (площадь под кривой и длина кривой ЭЭГ-сигнала в скользящем окне);

2) запуск нейросетей нижнего уровня со сформированными векторами признаков;

3) запуск нейросети верхнего уровня с результатами нейросетей нижнего уровня.

Алгоритм обучения нейросети верхнего уровня аналогичен алгоритму обучения сетей нижнего уровня.

Искусственная нейронная сеть второго уровня обучается на выборке, составленной путем автоматического накопления ответов искусственных нейронных сетей первого уровня. По результатам обучения нейросеть верхнего уровня определяет значимость решений каждой из нейросетей нижнего уровня и производит выбор оптимального решения. Кроме того, такой комитет ANN является масштабируемым, то есть при добавлении новых пространств признаков возможно расширение комитета путем добавления новых нейросетей нижнего уровня, принимающих решения на основе новых пространств признаков.

4. Результаты и обсуждение. В данной работе произведена оценка различительной способности классификаторов на основе комитета ANN и метода SVM при попарной классификации четырех

воображаемых движений пальцев и одного воображаемого движения кисти одной руки, выполнявшихся в заданном ритме**.**

4.1 Оценка различительной способности классификаторов. Результаты применения классификаторов с использованием двух методов приведены на рисунке 2, где 1, 5, 10, 20 по оси x – количество накопленных проб, по оси y – точность классификации (в процентах), усредненная по всем парам движений и всем испытуемым. I – классификация при помощи комитета нейросетей. II – классификация методом опорных векторов на основе радиальной базисной функции:

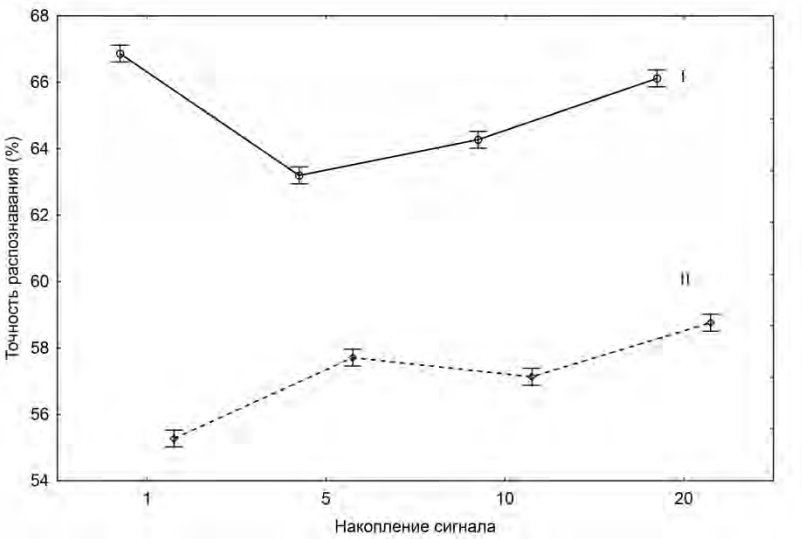


Рис. 2. Точность классификации ЭЭГ-паттернов воображаемых движений, выполняемых в заданном ритме, с использованием классификаторов на основе комитета искусственных нейронных сетей и метода опорных векторов

На рисунке 2 видно, что точность распознавания ЭЭГ-паттернов воображаемых движений при помощи комитета ANN была значимо выше, чем при помощи классификатора SVM, в среднем по всем парам воображаемых движений: $F_{(1,22800)}=7434.1$, $p<0.05$. Оценка успешности работы разных типов классификаторов с учетом количества накопленных проб выполнена с использованием дисперсионного анализа (ANOVA), который показал достоверный эффект влияния фактора «число накоплений (проб)» (4 градации) на процент верного распознаваний для обоих алгоритмов классификации (комитета ANN и SVM): $F_{(3,22800)}=202.1$, $p<0.05$. Зависимость точности классификации ЭЭГ-паттернов различных классификаторов от количества накоплений

проб, приведенная на рис.2, демонстрирует различную динамику: так, точность распознавания методом опорных векторов возрастает при увеличении количества накопленных проб, тогда как точность распознавания при помощи комитета искусственных нейронных сетей носит U-образный характер. Процент распознавания комитетом ANN в среднем по всем парам движений достигает максимальных значений при классификации единичных проб и с использованием наибольшего числа накопленных проб (по 20 проб).

Необходимо отметить, что качество работы интерфейса «мозг-компьютер» могут определять две характеристики: скорость и точность работы, а при накоплении 20, даже весьма коротких, проб длительностью 600 мс, задержка исполнения моторной команды составит не менее 12 секунд. В этих условиях для реализации интерфейса мозг-компьютер предпочтительным будет являться использование комитета искусственных нейронных сетей с единичными пробами сигнала, так как в данном случае он обладает наилучшей комбинацией факторов скорости и точности работы. Дополнительно точность классификации единичных проб, предположительно, может быть повышена с помощью сессий тренировки испытуемых.

4.2. Формирование индивидуального «языка команд». Проведенный выше анализ дает общую оценку точности классификации используемого пула воображаемых движений. Для оценки и выбора наилучшим образом распознаваемых воображаемых движений был проведен статистический анализ с рассмотрением взаимодействия факторов: «комбинация пар воображаемых движений», «тип классификатора», «испытуемый». Было выявлено достоверное взаимодействие указанных факторов для точности классификации ($F_{(36,22800)}=291.5$, $p<0.05$). Полученный эффект предполагает необходимость подбора классификаторов и пар воображаемых движений для дальнейших тренировок и формирования индивидуального «языка команд» для каждого испытуемого. Индивидуальный учет этих факторов позволит сократить время тренировок испытуемого и выбрать наилучшим образом различаемые воображаемые движения для успешной работы интерфейса «мозг-компьютер» с определенным человеком. На рисунке 3 приводятся результаты классификации отдельных пар воображаемых движений индивидуально для каждого испытуемого.

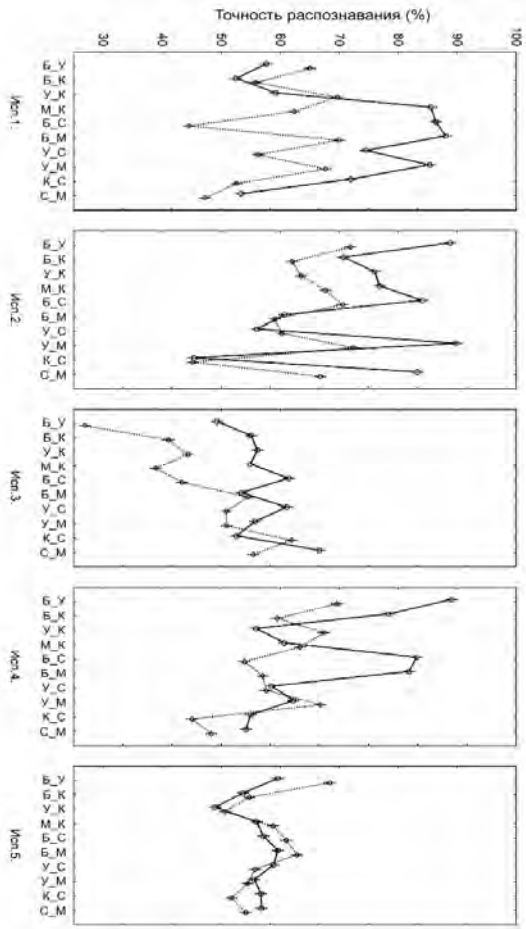


Рис. 3. Точность классификации отдельных пар воображаемых движений методом опорных векторов и при помощи комитета нейросетей

На рисунке 3 приведены индивидуальные данные для участников исследования: исп.1., исп.2., исп.3., исп.4., исп.5. – испытуемые. Сплошная линия – классификация при помощи комитета нейросетей. Пунктирная линия – классификация методом опорных векторов на основе радиальной базисной функции. По оси x – комбинации пар воображаемых движений: Б – воображаемое движение большим пальцем правой руки; У – воображаемое движение указательным пальцем правой руки; С – воображаемое движение средним пальцем; М – воображаемое движение мизинцем; К –

воображаемое движение кистью правой руки; По оси y – индивидуальная средняя точность классификации, без учета количества накоплений сигнала и величины временного окна анализа.

Результаты классификации, приведенные на рисунке 3, демонстрируют, что среди выполненных испытуемыми воображаемых движений более высокой точностью распознавания характеризовались следующие пары воображаемых движений: большим и указательным пальцами; большим пальцем и мизинцем; большим и средним пальцами; указательным пальцем и мизинцем.

Приведенные результаты для каждого испытуемого в отдельности позволяют сформировать индивидуальный «язык команд». С целью дальнейшего повышения точности классификации ЭЭГ-паттернов выбранных воображаемых предлагается применение индивидуальной настройки параметров классификации посредством определения оптимальных значений длины окна анализа и количества накоплений сигнала.

4.3. Индивидуальная настройка параметров классификации. Индивидуальная настройка параметров классификации направлена на решение задачи повышения точности распознавания разных информационных сигналов с помощью варьирования временных параметров генерации признаков (в частности, длины окна анализа), количества накопленных проб сигнала и методов классификации. Актуальность индивидуальной настройки параметров распознавания воображаемых движений для интерфейса мозг-компьютер обуславливается индивидуальной вариативностью ЭЭГ-сигнала. Параметры лучших индивидуальных результатов могут быть положены в основу тренировки для «закрепления» воспроизводимости результатов моторного воображения испытуемым, и использованы: для выбора для данного испытуемого: классификатора, длины окна анализа, величины сдвига окна анализа, количества накоплений сигнала и др.; для прогноза успешности обучения и применения интерфейса мозг-компьютер.

Актуальность задачи *индивидуального выбора классификатора* связана с тем, что, несмотря на большую точность распознавания ЭЭГ-паттернов воображаемых движений при помощи комитета нейросетей в среднем по испытуемым, по сравнению с классификатором на основе метода опорных векторов, для некоторых испытуемых (например, исп. №5, таблица.1) может наблюдаться обратный результат. Перспективой дальнейших исследований является разработка и применение масштабируемого комитета классификаторов, объединяющего искусственные нейронные сети и классификаторы на основе метода опорных векторов с автоматическим обобщением результатов локальных классификаторов нейрологическим классификатором второго уровня. При этом для повышения точности классификации будут использоваться преимущества обоих классификаторов.

Индивидуальная настройка параметров классификации воображаемых движений позволяет выбрать оптимальные параметры при генерации признаков. В данной работе было выявлено влияние факторов «длина окна анализа» и количества накопленных проб на точность распознавания ЭЭГ-паттернов воображаемых движения пальцев и кисти правой руки при попарном сравнении ($F[24,22800]=11.9$; $p<0.05$). При этом влияние данных факторов было индивидуальным, т.е. для каждого испытуемого могут быть определены временные параметры генерации признаков, в среднем повышающие процент распознавания воображаемых движений. На рисунке 4 приведен пример индивидуального влияния длины окна анализа и количества накоплений проб на процент успешной классификации воображаемых движений.

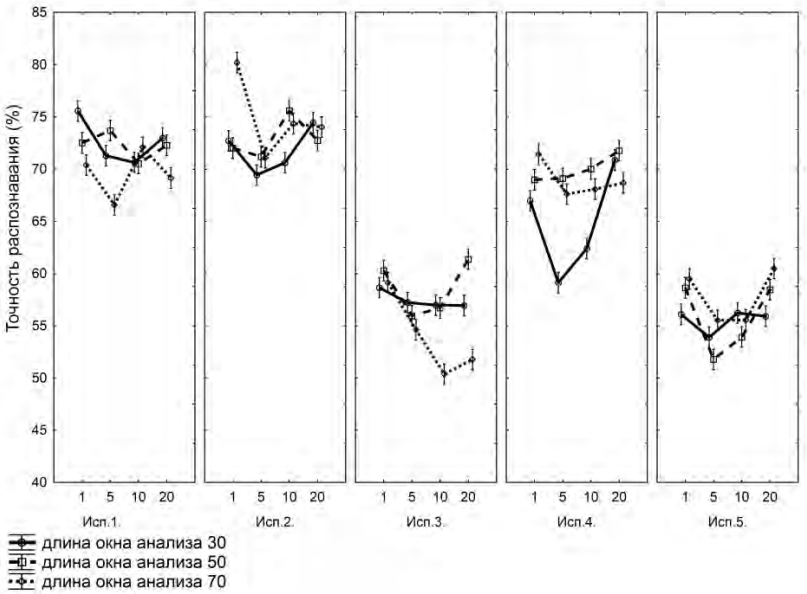


Рис. 4. Влияние параметров генерации признаков (длины окна анализа и количества накопленных проб сигнала) на среднюю индивидуальную точность классификации на основе комитета искусственных нейронных сетей

На рисунке 4 приведены индивидуальные данные для участников исследования: исп.1., исп.2., исп.3., исп.4., исп.5. – испытуемые. 1, 5, 10, 20 по оси x – количество накопленных проб. По оси y – индивидуальная средняя точность классификации для всех пар движений. Графики отображают точность классификации при различных длинах окна анализа (длина окна анализа в отсчетах: 1 отсчет = 2 мс.).

Следует отметить, что приводятся усредненные данные для точности классификации всех возможных сочетаний пар воображаемых движений.

Как видно из приведенных данных у некоторых испытуемых средняя точность распознавания воображаемых движений при изменении длины окна анализа изменяется незначительно – в пределах 2-5% (испытуемый 5), в то время, как у других – вариативность выше, и точность распознавания изменяется в среднем на 8-10% между показателями максимальной и минимальной средней точности (испытуемые 2, 3, 4).

Точность классификации в зависимости от параметров генерации признаков изменяется также при индивидуальном рассмотрении комбинаций пар движений. Таким образом, можно определить пары движений, для которых (а) изменение длины окна анализа может быть несущественным – и предоставлять широкий диапазон выбора параметров для настройки классификатора, и те, для которых (б) определение оптимальных параметров критично и является ограничивающим фактором для настройки классификатора.

При индивидуальной настройке длины окна анализа возможно повысить точность классификации для отдельных пар движений и выбрать индивидуальный набор команд с заданным минимальным порогом распознавания (таблица 1).

Таблица 1. Результаты классификации попарно сравниваемых воображаемых движений с учетом длины окна анализа

Пары воображаемых движений	Точность классификации (%), окно (отсчеты)									
	Комитет ANN					RBF SVM				
	Исп.1	Исп.2	Исп.3	Исп.4	Исп.5	Исп.1	Исп.2	Исп.3	Исп.4	Исп.5
Б-У	65%, 50	*100%* *50*	65%, 30	*93%*, *30*	75%, 70	77%, 50	78%, 30	47%, 50	*80%*, *30*	*91%*, *70*
Б-К	60%, 30	*84%*, *70*	64%, 70	*89%*, *70*	63%, 70	*82%*, *30*	*81%*, *30*	61%, 30	70%, 70	62%, 30
Б-С	*94%*, *30*	*96%*, *70*	69%, 30	*93%*, *70*	71%, 70	65%, 30	*81%*, *50*	62%, 30	67%, 50	78%, 30
Б-М	*97%*, *50*	66%, 50	66%, 70	*93%*, *70*	78%, 70	75%, 30	69%, 50	77%, 30	70%, 70	*84%*, *30*
У-К	75%, 30	*84%*, *50*	64%, 50	63%, 50	77%, 50	74%, 50	73%, 70	59%, 70	*85%*, *50*	63%, 50
У-С	*95%*, *70*	62%, 30	70%, 70	74%, 50	69%, 30	65%, 50	70%, 50	59%, 70	67%, 50	68%, 50
У-М	*94%*, *70*	*99%*, *50*	69%, 50	72%, 50	66%, 70	58%, 70	*80%*, *30*	63%, 50	*79%*, *50*	66%, 50
К-С	*91%*, *50,70*	62%, 30	78%, 70	63%, 30	65%, 50	77%, 30	67%, 50	75%, 50	54%, 30	60%, 30
К-М	*93%*, *70*	*89%*, *70*	66%, 50	72%, 50	76%, 50	74%, 70	76%, 50	54%, 50	*84%*, *50*	77%, 30
С-М	68%, 30	*95%*, *50*	71%, 70	62%, 70	68%, 50	58%, 30	75%, 50	66%, 70	60%, 30	62%, 50

В каждой ячейке таблицы 1 указаны – максимальная точность классификации в процентах и соответствующая длина окна анализа в отсчетах (1 отсчет = 2 мс) для попарных классификаций. Сдвиг окна анализа составлял 50% длины окна. Типы воображаемых движений: Б – воображаемое движение большим пальцем; У – воображаемое движение указательным пальцем; К – воображаемое движение кистью правой руки; С – воображаемое движение средним пальцем; М – воображаемое движение мизинцем.

5. Заключение. В результате проведенной работы, поставленная цель по разработке методики и средств классификации ЭЭГ-паттернов ритмических воображаемых движений пальцами одной руки - выполнена. Для классификации ЭЭГ-паттернов использовался классификатор на основе метода опорных векторов и двухуровневый классификатор на основе искусственных нейронных сетей. Проведенное исследование показало, что:

1. точность распознавания ЭЭГ-паттернов воображаемых движений пальцев и кисти одной руки с использованием комитета искусственных нейронных сетей, в среднем, была выше, чем при использовании классификатора на основе метода опорных векторов на основе радиальной базисной функции. Однако у некоторых испытуемых наблюдался и обратный результат. Таким образом, на практике следует применять классификатор, индивидуально настроенный на испытуемого;

2. точность распознавания ЭЭГ-паттернов воображаемых движений комитетом искусственных нейронных сетей имела U-образную форму – и достигала наибольших значений при единичных пробах и накоплении 20 проб при реализации воображаемых движений в заданном ритме;

3. использование индивидуального подхода к выбору параметров для генерации признаков – длины окна анализа, количества накоплений сигнала – может повышать точность распознавания ЭЭГ-паттернов воображаемых движений;

4. комитет искусственных нейронных сетей может быть расширен за счет дополнительного подключения классификаторов на основе метода опорных векторов с автоматическим объединением результатов классификации и выбором оптимальных решений. При этом для повышения точности классификации могут использоваться преимущества обоих типов классификаторов;

5. методы и подходы классификации, учитывающие несколько пространств признаков, могут быть применены для распознавания ЭЭГ–паттернов кинестетического воображения движений мелкой

моторики с целью дальнейшей разработки неинвазивного интерфейса “мозг-компьютер”.

Литература

1. *Ганин И. П., Каплан А. Я.* Интерфейс мозг компьютер на основе волны p300: предъявление комплексных стимулов “подсветка + движение” // Журнал высшей нервной деятельности. 2014. Т.64. № 1. С. 32–40.
2. *Фролов А.А., Рощин В.Ю.* Интерфейс мозг-компьютер. Реальность и перспективы // Научная конференция по нейроинформатике МИФИ 2008. Лекции по нейроинформатике. 2008. URL: http://neurolectures.narod.ru/2008/Frolov-2008.pdf (дата обращения 19.02.2014).
3. *Lotte F., Congedo M., Lecuyer A. et al.* Review of classification algorithms for EEG-based brain-computer interfaces // Journal of Neural Engineering. 2007. vol. 4. pp. 1–24.
4. *Xiao R., Ding L.* Evaluation of EEG features in decoding individual finger movements from one hand // Computational and Mathematical Methods in Medicine. 2013. vol. 2013. 10 p. URL: http://www.hindawi.com/journals/cmmm/2013/243257 (дата обращения 20.04.2014)
5. *Quandt F., Reichert C., Hinrichs H., Heinze H.J., Knight R.T., Rieger J.W.* Single trial discrimination of individual finger movements on one hand: A combined MEG and EEG study // NeuroImage. 2012. vol. 59. pp. 3316–3324.
6. *Sonkin KM, Stankevich LA, Khomenko JG, Nagornova ZV, Shemyakina NV.* Development of electroencephalographic pattern classifiers for real and imaginary thumb and index finger movements of one hand // Artificial intelligence in medicine. 2014. vol. 63. Issue 2. pp. 107–117.
7. *Neuper C, Scherer R, Reiner M, Pfurtscheller G.* Imagery of motor actions: differential effects of kinesthetic and visual-motor mode of imagery in single- trial EEG // Cognitive Brain Research. 2005. vol. 25. pp 668–677.
8. *Jasper H.* The ten-twenty electrode system of the International Federation // Electroencephalogr Clin Neurophysiol. 1958. no. 10. pp. 371–377.
9. *Wang L, Wu X.-P.* Classification of four-class motor imagery EEG data using spatial filtering // Bioinformatics and Biomedical Engineering (ICBBE 2008). The 2nd International Conference on IEEE eXpress Conference Publishing. Piscataway. NJ. USA. 2008. pp. 2153–2156.
10. *Ge S, Wang R, Yu D.* Classification of four-class motor imagery employing single-channel electroencephalography // PLoS One. 2014. vol. 9(6). pp. e98019
11. *Efron B.* Bootstrap Methods: Another Look at the Jackknife // Annals of Statistics. 1979. vol. 7. no. 1. pp. 1–26.
12. *Cortes C, Vapnik V.N.* Support-Vector Networks // Machine Learning. 1995. vol. 20(3). pp. 273–297.
13. *Shawe-Taylor J., Cristianini N.* Kernell methods for pattern analysis. Cambridge University Press. 2004. URL: http://www.kernel-methods.net/ (дата обращения 19.02.2014).
14. *Chang C.-C., Lin C.-J.* LIBSVM: a library for support vector machines //ACM Transactions on Intelligent Systems and Technology. 2011. vol. 2(27). pp. 1–27. URL: http://www.csie.ntu.edu.tw/~cjlin/libsvm (дата обращения 12.02.2014).
15. *Сонькин К.М., Станкевич Л.А., Хоменко Ю.Г., Нагорнова Ж.В., Шемякина Н.В.* Классификация электроэнцефалографических паттернов воображаемых и реальных движений пальцев одной руки методом опорных векторов // Тихоокеанский медицинский журнал. 2014. Т. 2. С. 30–35.

References

1. Ganin I. P., Kaplan A. Ya. [The P300- Based Brain-Computer Interface: Presentation of the Complex “Flash + Movement” Stimuli. I.P. Pavlov]. *Zhurnal vysshej nervnoj dejatel'nosti – Journal of Higher Nervous Activity*. 2014. vol. 64. no. 1. pp. 32–40. (In Russ.).
2. Frolov A.A., Roschin V. Yu. [Brain-computer Interface. Reality and Future]. *Nauchnaja konferencija po nejroinformatike (MIFI 2008). Lekcii po nejroinformatike* [Scientific Conference on Neuroinformatics (MEPhI 2008). Lectures on Neuroinformatics] MIFI 2008. Available at: http://neurolectures.narod.ru/2008/Frolov-2008.pdf (accessed 19.02.2014). (In Russ.).
3. Lotte F., Congedo M., Lecuyer A. et al. Review of classification algorithms for EEG-based brain-computer interfaces. *Journal of Neural Engineering*. 2007. vol. 4. pp. 1–24.
4. Xiao R., Ding L. Evaluation of EEG features in decoding individual finger movements from one hand. *Computational and Mathematical Methods in Medicine*. 2013. vol. 2013. 10 p. Available at: http://www.hindawi.com/journals/cmmm/2013/243257 (accessed: 20.04.2014).
5. Quandt F., Reichert C., Hinrichs H., Heinze H.J., Knight R.T., Rieger J.W. Single trial discrimination of individual finger movements on one hand: A combined MEG and EEG study. *NeuroImage*. 2012. vol. 59. pp. 3316–3324.
6. Sonkin KM, Stankevich LA, Khomenko JG, Nagornova ZV, Shemyakina NV. Development of electroencephalographic pattern classifiers for real and imaginary thumb and index finger movements of one hand. *Artificial intelligence in medicine*. 2014. vol. 63. Issue 2. pp. 107–117.
7. Neuper C, Scherer R, Reiner M, Pfurtscheller G. Imagery of motor actions: differential effects of kinesthetic and visual-motor mode of imagery in single- trial EEG. *Cognitive Brain Research*. 2005. vol. 25. pp 668–677.
8. Jasper H. The ten-twenty electrode system of the International Federation. *Electroencephalogr Clin Neurophysiol*. 1958. no. 10. pp. 371–377.
9. Wang L, Wu X.-P. Classification of four-class motor imagery EEG data using spatial filtering. Bioinformatics and Biomedical Engineering (ICBBE 2008). The 2nd International Conference on IEEE eXpress Conference Publishing. Piscataway. NJ. USA. 2008. pp. 2153–2156.
10. Ge S, Wang R, Yu D. Classification of four-class motor imagery employing single-channel electroencephalography. *PLoS One*. 2014. vol. 9(6). pp. e98019
11. Efron B. Bootstrap Methods: Another Look at the Jackknife. *Annals of Statistics*. 1979. vol. 7. no. 1. pp. 1–26.
12. Cortes C, Vapnik V.N. Support-Vector Networks. *Machine Learning*. 1995. vol. 20(3). pp. 273–297.
13. Shawe-Taylor J., Cristianini N. Kernell methods for pattern analysis. Cambridge University Press. 2004. Available at: http://www.kernel-methods.net/ (accessed: 19.02.2014).
14. Chang C.-C., Lin C.-J. LIBSVM: a library for support vector machines // *ACM Transactions on Intelligent Systems and Technology*. 2011. vol. 2(27). pp. 1–27. Available at: http://www.csie.ntu.edu.tw/~cjlin/libsvm (accessed:12.02.2014).
15. Sonkin K.M., Stankevich L.A., Khomenko Yu.G., Nagornova Zh.V., Shemyakina N.V. [Classification of electroencephalographic patterns of imagined and real movements by one hand fingers using the support vectors method]. *Tihookeanskij medicinskij zhurnal – Pacific Medical Journal*. 2014. vol. 2. pp. 30–35 (In Russ.).

Станкевич Лев Александрович — к-т техн. наук, доцент, профессор кафедры системного анализа и управления, Институт информационных технологий и управления Санкт-Петербургского государственного политехнического университета. Область научных интересов: искусственный интеллект, искусственные когнитивные системы, интеллектуальные роботы, нейроинтерфейсы. Число научных публикаций — 215. stankevich_lev@inbox.ru; ул. Политехническая, д. 21, Санкт-Петербург, 195251; р.т.: +7(812) 29742-14, Факс: + 7(812)29767-80.

Stankevich Lev Alexandrovich — Ph.D., associate professor, professor of system analysis and control department, Institute of Computing and Control of St. Petersburg State Polytechnic University. Research interests: artificial intelligence, artificial cognitive systems, intellectual robots, brain-computer interfaces. The number of publications — 215. stankevich_lev@inbox.ru; 21, Polytechnicheskaya st., St. Petersburg, 195251, Russia; office phone: +7(812) 29742-14, Fax: + 7(812)29767-80.

Сонькин Константин Михайлович — аспирант кафедры информационно-измерительных систем, Институт информационных технологий и управления Санкт-Петербургского государственного политехнического университета. Область научных интересов: искусственный интеллект, распознавание образов, анализ биоэлектрических сигналов, нейроинтерфейсы. Число научных публикаций — 7. sonkinkonst@mail.ru; ул. Политехническая, д. 21, Санкт-Петербург, 19525129; р.т.: +7(812)927-2715, Факс: +7(812)552-6080.

Sonkin Konstantin Mikhailovich — Ph. D. student of measuring information technologies department, Institute of Computing and Control of St. Petersburg State Polytechnic University. Research interests: artificial intelligence, pattern recognition, EEG signal analysis, brain-computer interfaces. The number of publications — 7. sonkinkonst@mail.ru; 21, Polytechnicheskaya st., St. Petersburg, 195251, Russia; office phone: +7(812)927-2715, Fax: +7(812)552-6080.

Нагорнова Жанна Владимировна — к-т биол. наук, научный сотрудник лаборатории сравнительных эколого-физиологических исследований, Институт эволюционной физиологии и биохимии им. И.М.Сеченова Российской академии наук (ИЭФБ РАН). Область научных интересов: воображение, возрастная физиология, анализ ЭЭГ сигнала, интерфейс мозг-компьютер. Число научных публикаций — 11. nagornova_n@mail.ru; пр. Тореза, 44, Санкт-Петербург, 194233; р.т.: +7(960)224-88293, Факс: +7(812)552-3012.

Nagornova Zhanna Vladimirovna — Ph.D., researcher of comparative ecologo-physiological researches laboratory, Sechenov Institute of Evolutionary Physiology and Biochemistry of the Russian Academy of Sciences (IEPhB RAS). Research interests: imagination, age physiology, the analysis of EEG signal, brain computer interface. The number of publications — 11. nagornova_n@mail.ru; 44, Thorez. pr., St. Petersburg, 194233, Russia; office phone: +7(960)224-88293, Fax: +7(812)552-3012.

Хоменко Юлия Геннадьевна — к-т психол. наук, научный сотрудник лаборатории нейровизуализации, Институт мозга человека им. Н.П.Бехтеревой Российской академии наук. Область научных интересов: интерфейс "мозг-компьютер", магнитно-резонансная томография, позитронно-эмиссионная томография. Число научных публикаций — 42. julkhom@rambler.ru; ул. Академика Павлова, д. 9, Санкт-Петербург, 197369; р.т.: +7(812) 234-1390.

Khomenko Julia Gennadievna — Ph.D., researcher of neuroimaging laboratory, N.P. Bechtereva Institute of the Human brain of the Russian Academy of Sciences. Research interests: brain-computer interface, magnetic resonance spectroscopy, positron emission tomography. The number of publications — 42. julkhom@rambler.ru; 9, Akademica Pavlova st., Saint-Petersburg, 197369, Russia; office phone: +7(812) 234-1390.

Шемякина Наталья Вячеславовна — к-т биол. наук, научный сотрудник лаборатории сравнительных эколого-физиологических исследований, Институт эволюционной физиологии и биохимии им. И.М.Сеченова Российской академии наук (ИЭФБ РАН). Область научных интересов: методы анализа биоэлектрического сигнала, возрастная физиология, творческая деятельность и ассоциативное мышление, воображаемые движения, интерфейс мозг-компьютер. Число научных публикаций — 17. shemyakina_n@mail.ru; пр. Тореза, 44, Санкт-Петербург, 194233; р.т.: +7(911)266-7304, Факс: +7(812)552-3012.

Shemyakina Natalia Vjacheslavovna — Ph.D., researcher of comparative ecologo-physiological researches laboratory, Sechenov Institute of Evolutionary Physiology and Biochemistry of the Russian Academy of Sciences (IEPhB RAS). Research interests: imagination, age physiology, the analysis of EEG signal, motor imaginary, brain computer interface. The number of publications — 17. shemyakina_n@mail.ru; 44, Thorez. pr., St. Petersburg, 194233, Russia; office phone: +7(911)266-7304, Fax: +7(812)552-3012.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (грант РФФИ-офи-м №13-01-12059).

Acknowledgements. This research is supported by RFBR (grants RFBR-ofi-m No.13-01-12059).

РЕФЕРАТ

Станкевич Л.А., Сонькин К.М., Нагорнова Ж.В., Хоменко Ю.Г., Шемякина Н.В. **Классификация электроэнцефалографических паттернов воображаемых движений пальцами руки для разработки интерфейса мозг-компьютер.**

В работе рассмотрены несколько подходов к классификации ЭЭГ паттернов при кинестетическом воображении движений пальцев и кисти одной руки в заданном ритме с целью дальнейшей реализации в разработке неинвазивного интерфейса мозг-компьютер. Для классификации ЭЭГ-паттернов воображаемых движений использовался метод опорных векторов на основе радиальной базисной функции и комитет искусственных нейронных сетей, использующий два пространства признаков (площадь под кривой и длина кривой). Показано, что точность попарной классификации ЭЭГ-паттернов воображаемых движений с использованием комитета нейронных сетей в среднем была выше, чем при использовании классификатора на основе метода опорных векторов. Выявлена возможность достижения точности распознавания некоторых пар воображаемых движений мелкой моторики у отдельных испытуемых до 90% и более при использовании индивидуального подхода к выбору параметров настройки классификаторов (величины окна анализа и количества накопленных проб). Разработанный классификатор на основе комитета нейронных сетей продемонстрировал более высокую точность классификации сигнала при использовании отдельных проб без накопления, чем классификатор на основе метода опорных векторов, что является перспективой для его дальнейшего использования в интерфейсе «мозг-компьютер» реального времени, например, для управления пятипалой искусственной кистью руки.

SUMMARY

Stankevich L.A., Sonkin K.M., Nagornova Zh.V., Khomenko Ju.G., Shemyakina N.V. **Classification of Electroencephalographic Patterns of Imaginary One-hand Finger Movements for Brain-Computer Interface Development.**

Several approaches to kinesthetic motor imagery EEG-pattern classification of one hand fingers and wrist movements executed in a given rhythm are examined in this study for the purpose of further implementation in Brain-Computer Interface development. Classification of motor imagery EEG-patterns was realized by means of support vector machine method with radial basis function and by artificial neural network committee based on two feature spaces (the area under the curve of the signals, curve length). It was shown that the accuracy of pairwise EEG-pattern classification of imaginary movements by means of the neural network committee was higher on average than the accuracy of the support vector machine classifier. The possibility of improving the accuracy of fine motor imaginary classification up to 90% and higher was revealed with the help of individual approach implementation for selection of EEG-pattern classification parameters (time window length, number of accumulated trials). Developed classifier based on the neural network committee demonstrated higher accuracy in case of single trial classification in comparison with the support vector machine classifier. This fact provides an opportunity for its further implementation in real-time BCI for artificial five-finger hand control.

УДК 004.932

М.В. Харинов, И.Г. Ханыков

ОПТИМИЗАЦИЯ КУСОЧНО-ПОСТОЯННОГО ПРИБЛИЖЕНИЯ СЕГМЕНТИРОВАННОГО ИЗОБРАЖЕНИЯ

Харинов М.В., Ханыков И.Г. **Оптимизация кусочно-постоянного приближения сегментированного изображения.**

Аннотация. В статье анализируется проблема сегментации цветового изображения, аппроксимируемого кусочно-постоянными приближениями. Качество сегментации оценивается по классическому среднеквадратичному отклонению (СКО) пикселей приближения от пикселей изображения. Обсуждаются современные версии классических методов кластеризации пикселей изображения посредством минимизации СКО или суммарной квадратичной ошибки. Описываются четыре основные операции с кластерами пикселей и критерии их выполнения для построения оптимизированных приближений. Предлагаются варианты алгоритма преобразования приближения изображения, которые при неизменном числе сегментов обеспечивают оптимизацию приближения как по СКО, так и по зрительному восприятию.

Ключевые слова: кластеры пикселей, сегменты изображения, кусочно-постоянное приближение, оценка качества, оптимизация, среднеквадратическое отклонение.

Khariniv M.V., Khanykov I.G. **Optimization of Piecewise Constant Approximation for Segmented Image.**

Abstract. In this paper a problem of segmentation of the color image, approached by piecewise constant approximations, is analyzed. The quality of the optimization is estimated by the classical standard deviation of image pixels from the pixels of approximations. The modern versions of the classical methods of image simulating by piecewise constant approximations characterized by minimal values of standard deviation or total squared error are detailed. Four main operations over pixel clusters and appropriate working criterions for the optimized approximation generating are discussed. The algorithmic versions of approximation transformation, providing the enhancement of approximation by standard deviation and also by visual perception for the given number of segments are proposed.

Keywords: pixel clusters, image segments, piecewise constant approximation, quality estimation, optimization, standard deviation.

1. Введение. Работа относится к области применения классических методов кластерного анализа [1, 2] для предварительной обработки цифрового изображения на стадии *сегментации*, которая состоит в разбиении исходного изображения на вложенные изображения «объектов» с целью дальнейшего автоматического или автоматизированного анализа признаков и распознавания. Заполнение каждого вложенного изображения одинаковыми пикселями с усредненным значением яркости преобразует исходное изображение в свое *приближение*. Качество разбиения и соответствующего приближения изображения из N пикселей оценивается по величине среднеквадратичного отклонения σ пикселей приближения от пикселей изображения или суммарной квадратичной ошибки $E = 3N\sigma^2$, где коэффициент 3 учитывает

число цветовых компонент в изображении. При *сегментации* требуется, чтобы пиксели каждого вложенного изображения составляли единственный связный сегмент, тогда как при *кластеризации* пикселей допускается, что вложенное изображение может состоять из нескольких или многих несмежных сегментов исходного изображения. Разбиение и приближение при данном числе кластеров пикселей, в частности сегментов изображения, считается *оптимальным*, если отвечает минимально возможному значению суммарной квадратичной ошибки E или среднеквадратичного отклонения σ. Тогда *объекты* определяются как кластеры, или сегменты оптимального приближения изображения.

Сформулированное определение объектов подходит для изображений произвольного содержания и не ограничивает алгоритмов генерации оптимальных приближений, что позволяет разрабатывать и верифицировать унифицированные методы кластеризации пикселей и сегментации, которые особенно актуальны для современной обработки изображений. Препятствием является то, что точное получение оптимальных приближений при кластеризации пикселей и, тем более, сегментации цветовых или многоспектральных изображений является задачей, в которой вычислительная сложность экспоненциально возрастает с ростом числа пикселей и рассматриваемых значений числа кластеров от 1 до N. При этом в практике сегментации изображений возникает задача аппроксимации оптимальных приближений *квазиоптимальными* приближениями, которые с достаточной скоростью генерируются в агломеративных и дивизимных алгоритмах минимизации ошибки E или среднеквадратичного отклонения σ [1, 2].

Основной целью статьи является анализ особенностей этих алгоритмов в приложении к цифровым изображениям. Сопутствующей темой является обсуждение адекватности применения E или σ для оценки различия приближения от изображения по зрительному восприятию, тем более что в настоящее время нетрудно встретить обратные утверждения, опирающиеся на работы [3, 4] и др. по эвристическому пересмотру традиционных оценок. В качестве конструктивного контраргумента по эффективному применению в задачах сегментации именно E или σ, в статье предлагается алгоритм адекватного улучшения качества приближения изображения.

2. Кусочно-постоянные приближения изображения. Под кусочно-постоянным приближением (или просто *приближением*) заданного изображения понимается изображение, значения пикселей кото-

рого совпадают со значениями пикселей, усредненными по кластерам, в частности, сегментам некоторого разбиения заданного изображения.

Суммарная квадратичная ошибка E для трехкомпонентных значений x_i пикселей изображения и значений y_i пикселей приближения определяется суммированием квадратов евклидовых расстояний $\|x_i - y_i\|^2$:

$$E = \sum_{i=0}^{N-1} \|x_i - y_i\|^2 , \qquad (1)$$

где суммирование выполняется по координатам i. В отличие от x_i с целочисленными значениями компонент, величины y_i образуются тройками вещественных, точнее, рациональных чисел. В [3, 4] суммарная квадратичная ошибка E вычисляется по формуле (1), но под y_i понимаются значения пикселей изображения, которое получается при том или ином искажении исходного изображения в пределах ограниченной ошибки E и не обязательно является его приближением. Причем, авторы [4], развивая идеи [3], приходят к необходимости предварительной сегментации для адекватного сопоставления различных изображений, которая выполняется посредством оптимизации определенного функционала качества.

Таким образом, в [3, 4] рассматривается общая задача сопоставления изображений, решение которой зависит от решения проблемы сегментации. При сегментации трудно обойтись без тщательного исследования возможностей оценки качества посредством классических методов минимизации E или σ, которые служат традиционной основой для сравнения.

Во избежание накопления ошибок округления формулу (1) практически не используют в расчетах по минимизации E. При этом суммарную квадратичную ошибку E_g вычисляют суммированием ошибок E_i по кластерам разбиения множества пикселей изображения:

$$E_g = \sum_{i=1}^{g} E_i , \qquad (2)$$

где g — число кластеров или сегментов, $g = 1, 2, ..., N$.

Для вычисления E_i пользуются выражением:

$$E_i = \sum_{j=0}^{n-1} \left\| x_j \right\|^2 - \frac{\left\| \sum_{j=0}^{n-1} x_j \right\|^2}{n}, \qquad (3)$$

где $n \equiv n_i$ — число пикселей в кластере или сегменте. Следует обратить внимание, что в (2), (3) исключена явная зависимость от пикселей, отличных от пикселей изображения, которая используется в [3, 4].

Целевые оптимальные приближения, аппроксимируемые квазиоптимальными приближениями изображения, в задаче минимизации E или σ, обладают рядом свойств, которые полезно сохранять при построении квазиоптимальных приближений. Оптимальные приближения не меняются при линейном преобразовании изображения по яркости, коммутируют с преобразованием из позитива в негатив и с масштабированием изображения посредством дублирования пикселей. При возрастании числа кластеров g от 1 до N последовательность оптимальных приближений описывается монотонной последовательностью значений E_g, которые нестрого уменьшаются от максимального значения E_1 при единственном кластере до 0 при всех пикселях, отнесенных к различным кластерам. Нетривиальным свойством оптимальных приближений является *выпуклость* последовательности значений E_g:

$$E_g = \frac{E_{g-1} + E_{g+1}}{2}, \quad g = 2, 3, ..., N\text{-}1, \qquad (4)$$

при которой уменьшению ошибки E_g с ростом числа кластеров сопутствует нестрогое возрастание производной от E_g по g.

Нарушение выпуклости значений ошибки E_g для результатов агломеративных и дивизимных алгоритмов иерархической сегментации свидетельствует об отклонении получаемых разбиений от оптимальных. Поэтому детектирование точки перегиба на кривой E_g в зависимости от g часто используют в агломеративных алгоритмах в качестве правила останова слияния смежных сегментов [5].

3. Операции с кластерами и сегментами. Основой программно-алгоритмического инструментария модели иерархической сегмен-

тации цифрового изображения [6] являются четыре операции с кластерами пикселей, в частности, с сегментами изображения, которые применяются для минимизации суммарной квадратичной ошибки E или среднеквадратичного отклонения σ:

– операция «*merge*» слияния двух кластеров;

– операция «*divide*» разделения кластера надвое;

– операция «*split*» выделения части кластера в отдельный кластер;

– операция «correct» реклассификации пикселей посредством их исключения из одного кластера и отнесения к другому кластеру.

Первые две операции используются при построении и обработке модифицируемой или фиксированной иерархии кластеров. Пара остальных операций используется при построении и преобразованиях иерархии.

Посредством перечисленных операций, а также их комбинаций в модели [6] строится бинарная иерархия кластеров или сегментов, и формируется иерархическая последовательность квазиоптимальных разбиений изображения на последовательное число кластеров от 1 до N. При этом *иерархия* кластеров (сегментов) считается заданной, если для каждого кластера не менее, чем из одного пикселя, устанавливается пара кластеров, на которые разделяется данный кластер.

Приращение $\Delta E_{merge} = E(1 \cup 2) - E(1) - E(2)$ суммарной квадратичной ошибки E при слиянии кластеров 1 и 2 с числом пикселей n_1, n_2 выражается через квадрат евклидова расстояния $\|I_1 - I_2\|^2$ между трехкомпонентными средними яркостями I_1, I_2 в виде:

$$\Delta E_{merge} = \frac{n_1 n_2}{n_1 + n_2} \|I_1 - I_2\|^2, \qquad (5)$$

Именно выражение (5) используется для итеративного вычисления иерархической последовательности квазиоптимальных приближений изображения методом Уорда [7] по критерию:

$$\Delta E_{merge} = \min, \qquad (6)$$

согласно которому на каждом шаге построения выполняется слияние кластеров, сопровождающееся минимальным приращением суммарной квадратичной ошибки.

Характерным свойством иерархической последовательности приближений цветового изображения, получаемых методом Уорда,

является выпуклость (4) соответствующей последовательности значений суммарной квадратичной ошибки.

Метод Уорда обеспечивает минимизацию суммарной квадратичной ошибки E посредством перебора всех пар кластеров пикселей. Однако с ростом числа кластеров вычислительная сложность метода Уорда квадратично возрастает. Поэтому, в случае изображений, для эффективного применения метода необходимо предварительно существенно уменьшить начальное число кластеров по сравнению с числом пикселей N, например, в модели сегментации Мамфорда-Шаха [5, 6, 8–11].

Если в методе Уорда в качестве начального рассматривать разбиение изображения на отдельные пиксели, под кластерами понимать сегменты изображения и ограничиться слиянием пар смежных сегментов, то вычисления будут выполняться по модели сегментации Мамфорда–Шаха в версиях [6, 11] без учета границ между сегментами (в отличие от версий [5, 8–10], предусматривающих учет границ).

По сравнению с методом Уорда кластеризации пикселей изображения модель Мамфорда–Шаха сегментации изображения обеспечивает минимизацию суммарной квадратичной ошибки E посредством перебора ограниченного множества пар смежных сегментов, что влечет увеличение ошибки E аппроксимации изображения. Тем не менее, модель Мамфорда–Шаха снижает вычислительную сложность до линейной зависимости от числа N пикселей в изображении и обеспечивает аппроксимацию изображения любым числом связных сегментов от 1 до N.

Операция «*divide*» разделения кластера надвое вводится как обратная по отношению к операции «*merge*» для кластеров или сегментов, полученных в результате итеративного слияния, например, в модели Мамфорда-Шаха. При этом любому кластеру 1, содержащему более одного пикселя, сопоставляется приращение $\Delta E_{divide}(1)$ суммарной квадратичной ошибки E, которое описывает приращение суммарной квадратичной ошибки при разделении кластера 1 надвое и равно взятому с обратным знаком приращению $\Delta E_{merge}(1', 1'')$ ошибки E при формировании кластера 1 посредством слияния пары вложенных кластеров $1'$ и $1''$:

$$\Delta E_{divide}(1) \equiv -\Delta E_{merge}(1', 1'') \ , \qquad (7)$$

где $1 = 1' \cup 1''$.

В случае иерархии сегментов изображения сочетание операций «*merge*&*divide*» обеспечивает улучшение качества приближения изображения в методе сегментации «*SI*» (segmentation improvement) за счет разделения надвое одного из сегментов (под номером 1) и слияния несовпадающих с ним двух других (с номерами 2 и 3), которое выполняется итеративно по критерию [12]:

$$\Delta E_{divide}(1) + \Delta E_{merge}(2, 3) = \min < 0 . \qquad (8)$$

При этом на каждой итерации выбирается тройка сегментов, обеспечивающих максимальное падение суммарной квадратичной ошибки, и процесс комбинированного слияния/разделения смежных сегментов продолжается, пока обнаруживаются тройки сегментов, удовлетворяющие (8). В противном случае, обработка завершается.

Для приложений *SI*-метода важно, что число сегментов в результирующем приближении совпадает с числом сегментов исходного приближения.

Операция «*split*» является обобщением операции «*divide*», т.к. предусматривает выделение из n_1 пикселей кластера 1 в отдельный кластер любого подмножества из $k < n_1$ пикселей, в том числе, отличающегося от кластеров $1'$ и $1''$. Сопутствующее отрицательное или нулевое приращение ΔE_{split} суммарной квадратичной ошибки описывается формулой:

$$\Delta E_{split} = -\frac{kn_1}{n_1 - k}\left\|I - I_1\right\|^2 \le 0 , \qquad (9)$$

где I_1 и I – трехкомпонентные средние яркости обсуждаемых n_1 и k пикселей.

Операцию «*correct*» реклассификации подмножества пикселей из одного кластера в другой можно представить как комбинацию операций «*split*» и «*merge*», при которой $k < n_1$ пикселей исключают из кластера 1 с числом пикселей n_1 и относят к кластеру 2 с числом пикселей n_2. Приращение суммарной квадратичной ошибки описывается выражением:

$$\Delta E_{correct} = \frac{kn_2}{n_2 + k}\left\|I - I_2\right\|^2 - \frac{kn_1}{n_1 - k}\left\|I - I_1\right\|^2 , \qquad (10)$$

где I — среднее значение реклассифицируемых k пикселей, а I_1, I_2 — средние значения пикселей кластеров 1 и 2. Сравнивая послед-

нюю формулу с двумя предыдущими, можно заметить, что (10) является следствием формул (5) и (9).

При использовании операции «*correct*» для минимизации суммарной квадратичной ошибки критерием служит выражение:

$$\Delta E_{correct} = \min < 0 \qquad (11)$$

При этом рассматриваются множества пикселей из определенной иерархии, которые переносятся из кластера в кластер до тех пор пока это обеспечивает снижение суммарной квадратичной ошибки, как при использовании критерия (8) в *SI*-методе. В отличие от числа сегментов, число кластеров в процессе обработки не изменяется. Условие неизменного числа сегментов при реализации метода можно поддерживать программно, если допускать обмен множествами пикселей только между смежными сегментами и блокировать варианты реклассификации, сопровождающиеся разделением донорского сегмента на вложенные.

Обсуждаемый метод предложен в [6, 13]. В явном виде критерий (11) раскрывается в виде:

$$\sqrt{\frac{n_2}{n_2 + k}}\,\|I - I_2\| < \sqrt{\frac{n_1}{n_1 - k}}\,\|I - I_1\| \qquad (12)$$

Если в (12) опустить подкоренные выражения, то критерий (12) совпадает с критерием реклассификации пикселей в классическом методе *K-means* [1, 2, 14]. В отличие от *K-means*, в методе [6, 13] обходятся без самостоятельного вычисления средних по кластерам значений. Поэтому в [13] предложенный метод удачно назван «*K-meanless*». В отличие от версии [13], в нашей версии [6] кластеры при минимизации E могут обмениваться не только отдельными пикселями, но и подмножествами пикселей, которые рассчитываются при построении иерархии. При этом увеличивается эффективность минимизации E, но при условии точных вычислений по формуле (12), так при k, отличном от 1 пренебрегать коэффициентами в (12) становится не целесообразно. Использование явных выражений для приращений суммарной квадратичной ошибки в нашей версии [6] вместо вычислений самих значений функционала в версии [13] упрощает вычисления с массивами данных, т. к. позволяет обойтись без суммирования квадратов яркостей пикселей изображения.

Перечисленные операции с кластерами пикселей, в частности, с сегментами изображения, в различных комбинациях порождают множество методов и алгоритмов, которые подлежат экспериментальному исследованию для внедрения в практику обработки изображений. Судя по нашему опыту сегментации, в настоящее время для внедрения наиболее актуален *SI*–метод.

4. Экспериментальные результаты. Метод *SI* улучшения качества сегментации разработан для улучшения качества приближения изображения с достаточным числом сегментов произвольной формы и размеров. В результате обработки рассматриваемое приближение либо оптимизируется по суммарной квадратичной ошибке E и среднеквадратичному отклонению σ, либо не изменяется, как в методах типа *K-means* [1, 2, 6, 13, 14]. Наглядный эффект улучшения аппроксимации изображения проявляется тем сильнее, чем грубее входное приближение изображения (рисунок 1).

Рисунок 1 иллюстрирует *SI*–метод оптимизации приближения на примере стандартного цветового изображения «Лена» из 512×512 пикселей, показанном в левом верхнем углу. Рядом справа показано приближение изображения. В нижнем ряду демонстрируются результаты улучшения качества приближения в двух версиях *SI*–метода. Все приближения содержат по 1024 сегмента. Под приближениями выписаны соответствующие значения среднеквадратичного отклонения σ.

Рис. 1. Оптимизация приближения сегментированного изображения

Исходное приближение на рисунке 1 получено разбиением поля изображения на квадратные клетки размером 16×16 с последующим заполнением клеток средними значениями пикселей, что эквивалентно искажению изображения при сжатии в 256 раз.

На первом шаге обработки каждая из 1024 клеток обрабатывается как самостоятельное изображение, для которого вычисляется иерархическая сегментация по Мамфорду-Шаху [6, 11].

Далее, в одной из версий *SI*–метода, слияние смежных клеток продолжается до объединения в единственный сегмент. В результате рассчитывается полная бинарная иерархия сегментов изображения, которая фиксируется. В этом случае, операция *merge* при выполнении *SI*–метода ограничивается для каждого сегмента одним единственным вариантом, и получается приближение, показанное на рис.1 в левом нижнем углу.

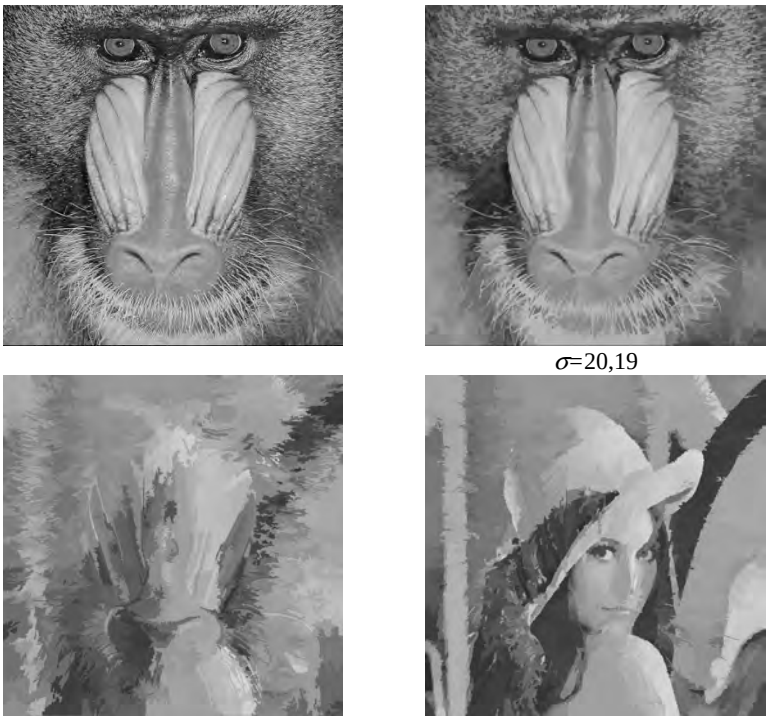
В другой версии *SI*–метода допускаются любые варианты слияния смежных сегментов, представленных в приближении на текущем шаге вычислений. В этом случае, благодаря модификации иерархии сегментов получается приближение с меньшим значением σ, которое показано на рисунке 1 в правом нижнем углу.

Версия *SI*–метода с фиксированной иерархией сегментов заметно проигрывает версии с модифицируемой иерархией, как по значению σ, так и по зрительному восприятию, но пока выигрывает по скорости обработки, которая выполняется со скоростью более миллиона пикселей в секунду. Для обеих версий предусмотрено ускорение вычислений и улучшение качества результирующего приближения, которые будут реализовываться в последующих версиях *SI*–метода.

В случае исходного разбиения, порождаемого не зависящей от содержания изображения регулярной решеткой рисунка 1, оптимизированное *SI*-методом приближение подобно результату «первичной сегментации», получаемой на основе пирамидального алгоритма [15]. В *SI*-методе используется более общая иерархия сегментов, чем в версиях [15, 16] пирамидального подхода, которая адаптируется к изображению и позволяет повысить качество сегментации, а также компенсировать дефекты неэффективной или ошибочной сегментации (рисунок 2).

Пара верхних картин на рис. 2, на примере стандартного цветового изображения «Mandrill» из 512×512 пикселей иллюстрирует *SI*–метод оптимизации приближения без искусственно внесенных искажений. Слева показано исходное изображение. Рядом справа показано его приближение 1024 сегментами, полученное в модели Мамфорда-Шаха [6, 11] и оптимизированное *SI*–методом в версии с модифици-

руемой иерархией сегментов. В нижнем ряду слева показано приближение стандартного изображения «Лена», для получения которого разбиение изображения «Mandrill» на 1024 сегмента заполнено средними значениями пикселей изображения «Лена», подсчитанными для тех же сегментов. В нижнем ряду справа на рис. 2 демонстрируется результат улучшения *SI*–методом «ошибочного» приближения изображения «Лена», вычисленного по разбиению изображения «Mandrill». Все приближения содержат по 1024 сегмента. Под приближениями выписаны соответствующие значения среднеквадратичного отклонения σ.



σ=20,19

σ=31,47

σ=14,88

Рис. 2. Исправление приближения сегментированного изображения

Пара верхних картин на рисунке 2, на примере стандартного цветового изображения «Mandrill» из 512×512 пикселей иллюстрирует *SI*–метод оптимизации приближения без искусственно внесенных искажений. Слева показано исходное изображение. Рядом справа показано его приближение 1024 сегментами, полученное в модели Мамфор-

да-Шаха [6, 11] и оптимизированное *SI*–методом в версии с модифицируемой иерархией сегментов. В нижнем ряду слева показано приближение стандартного изображения «Лена», для получения которого разбиение изображения «Mandrill» на 1024 сегмента заполнено средними значениями пикселей изображения «Лена», подсчитанными для тех же сегментов. В нижнем ряду справа на рис. 2 демонстрируется результат улучшения *SI*–методом «ошибочного» приближения изображения «Лена», вычисленного по разбиению изображения «Mandrill». Все приближения содержат по 1024 сегмента. Под приближениями выписаны соответствующие значения среднеквадратичного отклонения σ.

В верхнем ряду на рис. 2 левое изображение «Mandrill» и его приближение ограниченным числом сегментов справа визуально не просто отличить друг от друга благодаря минимизации среднеквадратичного отклонения σ, которая обеспечивается моделью Мамфорда-Шаха в сочетании с *SI*–методом.

В нижнем ряду на рис. 2 рассматриваемое в качестве исходного приближение изображения «Лена» слева, которое получено замещением значений пикселей приближения изображения «Mandrill» на средние значения пикселей изображения «Лена», искажено до неузнаваемости, отличается повышенным значением σ и не похоже ни на изображение «Лена», ни на изображение «Mandrill». Тем не менее, оцениваемое численно или визуально искажение приближения слева в значительной степени компенсируется в результате применения *SI*–метода, что иллюстрируется на рис. 2 оптимизированным приближением в правом нижнем углу.

Метод *SI* минимизации суммарной квадратичной ошибки E или среднеквадратичного отклонения σ при заданном числе сегментов относится к *глобальным* методам формирования однородных по яркости сегментов по всему полю изображения. Особенностью метода является, то, что он выводится из необходимых условий минимизации целевого функционала, а не посредством эвристической редакции функционала и критериев выполнения операций, как, например, в [10, 17]. В отличие от *SI*–метода, *сегментарная* версия метода *K-meanless* с модификацией только пар смежных сегментов и сохранением общего числа сегментов относится к методам *локальной* минимизации приближения по участкам изображения. Судя по опыту первичного экспериментального исследования, эффект минимизации E или σ методом *K-meanless* уступает результатам применения *SI*–метода. Однако, пока не исследована эффективность применения метода *K-meanless* в комбинации с *SI*–методом. По всей видимости, реальная

оптимизация приближения изображения относительно предельного значения, которое достижимо при данном числе сегментов, обеспечивается применением нескольких независимых алгоритмов, которые возможно разработать, опираясь на *SI*–метод, метод *K-meanless* и др.

Основное преимущество использования *SI*–метода может заключаться в том, что он позволяет оптимизировать сегментацию изображения, полученную по любым другим алгоритмам, например, скоростным алгоритмам «перцептивного хеширования» [18]. Вероятно, оптимизированная сегментация может оказаться полезной также в задаче сжатия изображений. В процессе пилотного экспериментального исследования по компрессии получаемых *SI*–методом *квазиоптимальных* приближений обнаружилось, что наиболее эффективно они сжимаются системными программами унифицированного сжатия ZIP (таблица 1).

Таблица 1. Результаты сжатия приближения изображения

Формат	JPEG	PNG	ZIP
Тип компрессии	Lossy	Lossless	Lossless
Коэффициент сжатия	24,8	24,6	*31,3*
	15,1	10,6	*16,5*

В таблице 1 приведены коэффициенты сжатия при упаковке приближений изображения в трех форматах: JPEG (с потерями), PNG и ZIP (без потерь). В первой и второй строках графы «Коэффициент сжатия» перечислены значения коэффициента при сжатии приближений, размещенных в правых нижних углах на рис. 1 и на рис. 2, соответственно.

Если задачу сжатия с потерями разделять на минимизацию потерь и последующее сжатие без потерь, то возникает проблема с выбором эффективного формата сжатия без потерь. Как отражено в таблице 1, при оценке искажений изображения по E или σ и минимизации потерь за счет применения *SI*–метода, для сжатия квазиоптимальных приближений наиболее перспективным представляется унифицированный способ сжатия произвольных данных, реализованный в формате ZIP, который выигрывает по сравнению со специальными форматами сжатия изображений (PNG и др.), и в ряде случаев превосходит даже формат JPEG сжатия с потерями.

5. Заключение. В статье мы постарались изложить аналитические основы модели сегментации цифрового изображения [6] в традиционной постановке задачи, в которой на выходе требуется получить единственное разбиение изображения на сегменты. На самом деле, проблема сегментации ставится и решается в общей постановке по-

строения иерархической последовательности всех квазиоптимальных (близких к оптимальным) разбиений изображения на сегменты или кластеры пикселей, что оказывается немногим сложнее [6]. Детальное аналитическое обоснование и интерпретация обсуждаемых в статье методов проиллюстрированы наглядными примерами, поясняющими актуальность их внедрения в практику современной сегментации изображений. Тем не менее, следует иметь в виду, что скоростная реализация описанных решений предполагает использование эффективной структуры данных, поддерживающей иерархическую организацию кластеров пикселей и сегментов изображения без чрезмерных затрат памяти.

Судя по результатам многолетних исследований [6], подходящей структурой данных является структура данных на основе динамических деревьев Слейтора-Тарьяна [19, 20]. В настоящее время динамические деревья активно внедряются в практику обработки изображений, в основном за рубежом [21]. Аппарат динамических деревьев интенсивно развивается за счет того, что они дополняются циклами, которые в совокупности с деревьями задают для многомерных данных некоторую сеть, подобно интеллектуальной нейронной сети [22]. Однако на языках высокого уровня, типа Java, динамические деревья реализуются пока с недостаточным набором операций, в числе которых не предусмотрена, например, операция *divide*, что повышает трудоемкость реализации скоростных обратимых вычислений [23]. Структура данных и операции с множеством пикселей в терминах динамических деревьев (рис. 1, 2) разрабатываются на языке C/C++. По завершению разработки имеет смысл включить операции и базовые алгоритмы в инструментальные среды типа MATLAB и пр.

Другой трудностью, которая возникает при внедрении методов автоматической сегментации, является проблема «локализации объектов» [24]. Проблема состоит в том, что компьютер детектирует на изображении иерархию объектов в виде однородных по яркости участков изображения, а инженеру-программисту для обеспечения дальнейшей обработки требуется анализировать сгруппированные из однородных участков изображения «визуальные объекты», которые он видит на экране компьютера при *адекватной* сегментации изображения. При этом не желательно принуждать инженера вникать в детали формализации вычислений в терминах динамических деревьев.

Для преодоления указанной трудности необходимо создать человеко-машинный интерфейс для перевода извлеченных компьютером визуальных данных в видеоданные, привычные для человека. Подобная задача, в гораздо более общей постановке, решается как проблема

искусственного интеллекта (ИИ) в проекте PPAML (Probabilistic Programming for Advancing Machine Learning) [25] авторитетного американского агентства DARPA (Defense Advanced Research Projects Agency). Проект PPAML начат в 2013 и закончится в 2017 г. В результате планируется разработать и разместить в открытом доступе программные средства, поддерживающие эффективное создание приложений ИИ силами рядовых инженеров-программистов.

Вполне вероятно, что при современных темпах развития компьютерного зрения сегментация цифровых изображений в ближайшие годы станет предметом разработки небольших групп профессиональных специалистов. Остальные будут пользоваться готовыми программами. Однако и в этом случае сохранит актуальность иллюстрированное аналитическое обоснование основных приемов первоначальной кластеризации пикселей и сегментации изображений, в частности, изложенных в настоящей статье.

Литература

1. *Айвазян С.А., Бухштабер В.М., Енюков И.С., Мешалкин Л.Д.* Прикладная статистика: Классификация и снижение размерности // М.: Финансы и статистика. 1989. 607 с.
2. *Мандель И.Д.* Кластерный анализ // М.: Финансы и статистика. 1988. 176 с.
3. *Wang Z., Bovik A. C., Sheikh H. R., Simoncelli E. P.* Image quality assessment: From error visibility to structural similarity // IEEE Transactions on Image Processing, Apr. 2004. vol. 13. no. 4. pp. 600–612.
4. *Blasch E., Li X., Chen G., Li W.* Image Quality Assessment for Performance Evaluation of Image Fusion // Int. IEEE Conf. on Information Fusion. 2008. pp. 583–588.
5. *Redding N.J., Crisp D.J., Tang D.H., Newsam G.N.* An efficient algorithm for Mumford–Shah segmentation and its application to SAR imagery // Proc. Conf. Digital Image Computing Techniques and Applications (DICTA'99). 1999. pp. 35–41.
6. *Харинов М.В.* Обобщение трех подходов к оптимальной сегментации цифрового изображения // Труды СПИИРАН. 2013. Вып. 2(25). С. 294–316.
7. *Ward J.H.*, Jr. Hierarchical grouping to optimize an objective function. // J. Am. Stat. Assoc. 1963. vol. 58. Issue 301. pp. 236–244.
8. *Mumford D., Shah J.* Boundary detection by minimizing functionals, I // Proc. IEEE Comput. Vision Patt. Recogn. Conf., San Francisco. 1985. pp. 22–26.
9. *Koepfler G., Lopez C., Morel J.* A Multiscale Algorithm for Image Segmentation by Variational Method // SIAM Journal on Numerical Analysis. 1994. vol. 31. no 1. pp. 282–299.
10. *Crisp D.J., Tao T.C.* Fast Region Merging Algorithms for Image Segmentation // The 5th Asian Conf. on Computer Vision (ACCV2002). Melbourne. Australia. 2002. pp. 1–6.
11. *Бугаев А.С., Хельвас А.В.* Поисковые исследования и разработка методов и средств анализа и автоматического распознавания потоковой информации в глобальных информационных системах. Шифр «Лацкан». Отчет по НИР // М.: МФТИ. 2001. Т. 1. 140 с.
12. *Харинов М.В.* Альтернатива иерархическому методу Оцу для цветового изображения // Вестник Бурятского государственного университета. Улан-Удэ: Изд-во Бурятского госуниверситета. 2014. №9. С. 64–72.

13. *Dvoenko S.D.* Meanless *k*-means as *k*-meanless clustering with the bi-partial approach // Pattern Recognition and Information Processing (PRIP'2014) // Proc. of the 12th Int. Conf. Minsk. 2014. pp. 50–54.
14. *Jain A.K.* Data Clustering: 50 Years Beyond K–Means // Pattern Recognition Letters, vol. 31. no. 8. 2010. pp. 651–666.
15. *Чочиа П.А.* Пирамидальный алгоритм сегментации изображения // Информационные процессы. 2010. Т. 10. № 1. С. 23–35.
16. *Александров В.В., Горский Н.Д.* Представление и обработка изображений. Рекурсивный подход // Л.: Наука. 1985. 190 с.
17. *Marfil R., Sandoval F.* Energy-Based Perceptual Segmentation Using an Irregular Pyramid // Bio-Inspired Systems: Computational and Ambient Intelligence. Springer–Verlag: Berlin/Heidelberg. 2009. LNCS 5517. pp. 424–431.
18. *Гнидко К.О., Ломако А.Г., Жолус Р.Б.* Обнаружение визуальных контаминантов на основе вычисления перцептивного хэша //Труды СПИИРАН. 2015. Т. 2. № 39. С. 193–211.
19. *Tarjan R.E.* Efficiency of a Good But Not Linear Set Union Algorithm // Journal of the ACM. 1975. vol. 22 (2). pp. 215–225.
20. *Sleator D.D., Tarjan R.E.* Self–Adjusting Binary Search Trees // Journal of the ACM. 1985. vol. 32 (3). pp. 652–686.
21. *Nock R., Nielsen F.* Statistical Region Merging // IEEE Trans. Pattern Anal. Mach. Intell. 2004. vol. 26(11). pp. 1452–1458.
22. *Осипов В.Ю.* Аналоговые ассоциативные интеллектуальные системы // Труды СПИИРАН. 2013. Т. 7. № 30. С. 141–155.
23. *Toffoli T.* Reversible computing // Springer Berlin Heidelberg. 1980. pp. 632–644.
24. *Визильтер Ю.В., Желтов С.Ю.* Проблемы технического зрения в современных авиационных системах // Механика, управление и информатика. 2011. №6. С. 11–44.
25. Probabilistic Programming for Advancing Machine Learning (PPALM). URL: http://www.darpa.mil/our_work/i2o/programs/probabilistic_programming_for_advanced_machine_learning_(ppaml).aspx (дата обращения: 2015-04-24).

References

1. Aivazian S.A., Bukhshtaber V.M., Eniukov I.S., Meshalkin L.D. *Prikladnaia statistika: Klassifikatsiia i snizhenie razmernosti* [Applied Statistics: Classification and dimension reduction]. M.: Finansy i statistika. 1989. 607 p. (In Russ.)
2. Mandel' I.D. *Klasternyi analiz* [Cluster analysis]. M.: Finansy i statistika. 1988. 176 p. (In Russ.)
3. Wang Z., Bovik A. C., Sheikh H. R., Simoncelli E. P. Image quality assessment: From error visibility to structural similarity. *IEEE Transactions on Image Processing*. 2004. vol. 13. no. 4. pp. 600–612.
4. Blasch E., Li X., Chen G., Li W. Image Quality Assessment for Performance Evaluation of Image Fusion. Int. IEEE Conf. on Information Fusion. 2008. pp. 583–588.
5. Redding N.J., Crisp D.J., Tang D.H., Newsam G.N. An efficient algorithm for Mumford–Shah segmentation and its application to SAR imagery. Proc. Conf. Digital Image Computing Techniques and Applications (DICTA'99). 1999. pp. 35–41.
6. Kharinov M.V. [A generalization of three approaches to an optimal segmentation of digital Image]. *Trudy SPIIRAN - SPIIRAS Proceedings*. 2013. vol. 25. no. 2. pp. 294–316. (In Russ.).
7. Ward J.H., Jr. Hierarchical grouping to optimize an objective function. *J. Am. Stat. Assoc.* 1963. vol. 58. Issue 301. pp. 236–244.

8. Mumford D., Shah J. Boundary detection by minimizing functionals. I. Proceedings of IEEE Computer. Vision Pattern. Recognition Conference. San Francisco. 1985. pp. 22–26.
9. Koepfler G., Lopez C., Morel J. A Multiscale Algorithm for Image Segmentation by Variational Method. *SIAM Journal on Numerical Analysis*. 1994. vol. 31. no. 1. pp. 282–299.
10. Crisp D.J., Tao T.C. Fast Region Merging Algorithms for Image Segmentation. The 5th Asian Conference on Computer Vision (ACCV2002). Melbourne. Australia. 2002. pp. 1–6.
11. Bugaev A.C., Khel'vas A.V. *Poiskovye issledovaniia i razrabotka metodov i sredstv analiza i avtomaticheskogo raspoznavaniia potokovoi informatsii v global'nykh informatsionnykh sistemakh. Shifr «Latskan». Otchet po NIR* [Exploratory research and development of methods and tools for analysis and automatic recognition of streaming media in global information systems. Code "Lapel". R&D Report]. Moscow: MIPT. 2001. vol. 1. 140 p. (In Russ.).
12. Kharinov M.V. [An alternative to hierarchical Otsu method for color image]. *Vestnik Buriatskogo gosudarstvennogo universiteta – Bulletin of the Buryat State University*. Ulan-Ude: 2014. no. 9, pp. 64–72. (In Russ.).
13. Dvoenko S.D. Meanless *k*-means as *k*-meanless clustering with the bi-partial approach. Proceedings of the 12th International Conference on Pattern Recognition and Information (PRIP'2014). Minsk. 2014. pp. 50–54.
14. Jain A.K. Data Clustering: 50 Years Beyond K–Means. *Pattern Recognition Letters*. 2010. vol. 31. no. 8. pp. 651–666.
15. Chochia P.A. [Pyramidal algorithm of image segmentation]. *Informacionnye processy – Informational processes*. 2010. vol. 10. no. 1. pp. 23–35. (In Russ.)
16. Aleksandrov V.V., Gorskii N.D. *Predstavlenie i obrabotka izobrazhenii. Rekursivnyi podkhod* [Representation and image processing. Recursive approach]. L.: Nauka. 1985. 190 p. (In Russ.).
17. Marfil R., Sandoval F. Energy-Based Perceptual Segmentation Using an Irregular Pyramid. *Bio-Inspired Systems: Computational and Ambient Intelligence*. Springer–Verlag: Berlin/Heidelberg. 2009. LNCS 5517. pp. 424–431.
18. Gnidko K.O., Lomako A.G., Zholus R.B. [Detection of Visual Contaminants on the Basis ofPerceptual Hash Calculation]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2015. vol. 2. no. 39. pp. 193–211. (In Russ.).
19. Tarjan R.E. Efficiency of a Good But Not Linear Set Union Algorithm. *Journal of the ACM*. 1975.vol. 22. no. 2. pp. 215–225.
20. Sleator D.D., Tarjan R.E. Self–Adjusting Binary Search Trees. *Journal of the ACM*. 1985. vol. 32 no. 3. pp. 652–686.
21. Nock R., Nielsen F. Statistical Region Merging. *IEEE Trans. Pattern Anal. Mach. Intell*. 2004. vol. 26 no. 11. pp. 1452–1458.
22. Osipov V.Iu. [Analog associative intelligent systems] *Trudy SPIIRAN – SPIIRAS Proceedings*. 2013. vol. 7. no. 30. pp. 141–155. (In Russ.).
23. Toffoli T. *Reversible computing*. Springer Berlin Heidelberg. 1980. pp. 632-644.
24. Vizil'ter Iu.V., Zheltov S.Iu. [Vision technical problems of modern aircraft systems]. *Mekhanika, upravlenie i informatika – Mechanics, control and informatics*. 2011. no. 6. pp. 11–44. (In Russ.)
25. Probabilistic Programming for Advancing Machine Learning (PPALM). Available at: http://www.darpa.mil/our_work/i2o/programs/probabilistic_programming_for_advanced_machine_learning_(ppaml).aspx (accessed 2015-04-24).

Харинов Михаил Вячеславович — к-т техн. наук, доцент, старший научный сотрудник лаборатории прикладной информатики и проблем информатизации общества,

Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: анализ цифровой информации, количественная оценка, система числового представления, иерархические структуры данных, сегментация и инвариантное представление изображений для распознавания, цветовое преобразование изображений. Число научных публикаций — 140. khar@iias.spb.su, http://www.machinelearning.ru/wiki/index.php?title=user:Khar; 14-я линия В.О., д. 39, Санкт-Петербург, 199178; р.т.: +7(812)328-1910, Факс: (812)328-4450.

Kharinov Mikhail Vyacheslavovich — Ph.D., associate professor, senior researcher of applied informatics and problems of society informatization laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: digital information analysis, information quantity estimation, numerical representation system, hierarchical data structures, image segmentation and invariant representation for recognition purposes, color transformations of images. The number of publications — 140. khar@iias.spb.su, http://www.machinelearning.ru/wiki/index.php?title=user:Khar; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-1910, Fax: (812)3284450.

Ханыков Игорь Георгиевич — аспирант лаборатории прикладной информатики и проблем информатизации общества, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: техническая диагностика, теория систем автоматического управления, компьютерное моделирование динамических систем, компьютерное зрение, задачи выделения объектов на изображении. Число научных публикаций — 8. igk@iias.spb.su; 14-я линия В.О., д. 39, Санкт-Петербург, 199178; р.т.: +7(812)328-1919, Факс: +7(812)328-4450.

Khanykov Igor Georgievich — Ph.D. student of applied informatics and problems of society informatization laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: technical diagnostics, automatic control systems theory, computer modeling of dynamic systems, computer vision, object isolation. The number of publications — 8. igk@iias.spb.su; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-1919, Fax: +7(812)328-4450.

РЕФЕРАТ

Харинов М.В., Ханыков И.Г. **Оптимизация кусочно-постоянного приближения сегментированного изображения.**

В статье рассматривается сегментация цифрового изображения, трактуемая как стадия автоматической обработки без использования управляющих параметров, которая обеспечивает предварительное обнаружение вложенных изображений объектов для последующего анализа признаков и распознавания. Под «объектами» понимаются вложенные изображения, на которые разбивается исходное изображение из условия минимизации суммарной квадратичной ошибки E или среднеквадратичного отклонения σ исходного изображения от своего кусочно-постоянного приближения с усредненными значениями пикселей. Объект могут образовывать как пиксели единственного связного сегмента, так и пиксели нескольких несмежных сегментов, которые, в этом случае именуются *кластером* пикселей. Термины «объект», «изображение» и «кластер пикселей», в частности, «сегмент изображения» не противопоставляются друг другу, а употребляются как своеобразные синонимы для обозначения определенных подмножеств многомерных пикселей цветового или спектрального изображения. Представление объекта как «изображения в изображении» предполагает иерархическую организацию объектов, которая рассчитывается посредством квартета перечисляемых в статье базовых операций: а) слияния пар кластеров или сегментов; б) обратного разделение кластера (сегмента) надвое; в) выделения подмножества пикселей в самостоятельный кластер; г) реклассификации подмножества пикселей из одного кластера или сегмента в другой. В качестве результата сегментации рассматривается иерархическая последовательность квазиоптимальных разбиений и соответствующих приближений изображения одним, двумя, ... , N кластерами или сегментами, где N — число пикселей в изображении. *Квазиоптимальными* считаются приближения, которые состоят из ограниченного числа сегментов, аппроксимируют, вообще говоря, неиерархическую последовательность оптимальных приближений изображения и строятся посредством базовых операций из условия минимизации E или σ либо при изменении на 1 числа кластеров, в частности, сегментов, либо при неизменном числе кластеров. Для практики наиболее актуальна традиционная задача оптимизации приближения изображения при заданном числе сегментов, решение которой детализируется в статье. Предлагается метод, который наряду с визуальным улучшением, обеспечивает улучшение приближения по E или σ, и применим для коррекции результатов других методов, в том числе для компенсации ошибочной сегментации.

В статье, во введении затрагивается тема адекватной оценки качества сегментации, в основной части дается аналитическое обоснование и интерпретация современных методов минимизации E или σ с позиций классического кластерного анализа, которая иллюстрируется примерами обработки. В заключении обсуждаются перспективы внедрения представленных методов.

SUMMARY

Khariniv M.V., Khanykov I.G. **Optimization of Piecewise Constant Approximation for Segmented Image.**

The paper addresses to digital image segmentation, interpreted as a stage of fully automatic processing without using any control parameters, which provides a pre-detection of sub-images of objects for subsequent feature analysis and image recognition. «Objects» are treated as nested images, obtained by dividing the original image into sub-images, from the condition of a minimization of the total squared error E or standard deviation σ of the original image from its piecewise constant approximation of the average pixel values. The object may contain a single connected segment or consist of several non-connected segments, which in this case are referred to as the clusters of pixels. The terms «object», «image» and «cluster of pixels», in particular, «image segments» are not opposed to each other, and are used as the synonyms to designate the certain subsets of multidimensional pixels of color or multispectral image. Representation of objects as «sub-images in the image» implies their hierarchical structure, which is generated by the quartet of basic operations presented in the paper, namely: a) merging of pairs of clusters or segments; b) reversive splitting of the cluster or segment into two ones; c) converting of a certain subset of pixels into a separate cluster; g) reclassification of subset of pixels from one cluster or segment into another. Target segmentation result is a quasi-optimal hierarchical sequence of image partitions and a sequence of corresponding approximations consisting of one, two, ..., N clusters or segments where N is total number of pixels in the image. The approximations are considered quasi-optimal, if they contain a limited number of segments and majorize in general case non-hierarchical sequence of optimal image approximations. These quasi-optimal approximations are obtained by minimizing of E or σ using basing operations that cause either the change in the cluster or segment number per unit either unchanged cluster or segment number. In practice, the conventional optimization problem for a given number of segments in source and also in enhanced approximations is most relevant. Solution of this problem is detailed in the paper. The proposed method provides the approximation improvement by the value of E or σ along with their visual improvement. It turns out, that our method is applicable not only to correct the results of other methods, but also to compensate of incorrect segmentation.

In the introduction to the paper the problem of adequate segmentation is revised. In it's main part the analytical justification and interpretation of modern methods for minimizing of the total squared error E or standard deviation σ are explained from the standpoint of classical cluster analysis followed by illustrative examples. In the conclusion the prospects for the implementation of presented methods are briefly outlined.

УДК 004.932.2

М.Н. Фаворская, А.В. Проскурин

КАТЕГОРИЗАЦИЯ СЦЕН НА ОСНОВЕ РАСШИРЕННЫХ ЦВЕТОВЫХ ДЕСКРИПТОРОВ

Фаворская М.Н., Проскурин А.В. **Категоризация сцен на основе расширенных цветовых дескрипторов.**

Аннотация. Категоризация сцен при автоматическом аннотировании изображений предполагает обязательный этап извлечения дескрипторов для построения гистограмм визуальных слов. Изучено семейство новых цветовых дескрипторов на основе точечных особенностей, инвариантных не только к геометрическим преобразованиям, но к изменениям освещенности. Особенностью дальнейшего алгоритма является предварительная цветовая и текстурная сегментация на основе алгоритма J-SEG с ранжированием полученных регионов по площади. Для построения визуальных слов и категоризации по методу опорных векторов используются расширенные цветовые дескрипторы, рассчитанные в 5–7 регионах с наибольшей площадью. Представлены сравнительные результаты экспериментальных оценок точности категоризации изображений из тестового набора 2688 изображений с применением расширенных цветовых дескрипторов.

Ключевые слова: автоматическое аннотирование изображений, категоризация сцен, метод опорных векторов, цветовые дескрипторы.

Favorskaya M.N., Proskurin A.V. **Scene Categorization Based on Extended Color Descriptors.**

Abstract. In automatic annotation systems, a scene categorization involves the compulsory stage of descriptor extraction in order to build a histogram of visual words. A family of new color descriptors based on point features, which are invariant not only to geometric transforms but also light changing, is investigated. In following, the algorithm executes a preliminary color and texture segmentation based on J-SEG algorithm. The received regions are ranked by areas. The extended color descriptors computing in 5–7 large area regions are applied for visual word construction. Then images are categorized by support vector machine. The comparative results of experimental estimators present the precision values of image categorization by use a test dataset containing 2,688 images.

Keywords: automatic image annotation, scene categorization, support vector machine, color descriptors.

1. Введение. Активное распространение цифровых устройств со встроенными видеокамерами привело к экспоненциальному увеличению количества изображений, доступных пользователям в сети Интернет. В связи с этим возникла проблема их эффективного поиска. Возможное решение заключается в автоматическом аннотировании изображений (ААИ) и последующем использовании хорошо известных методов текстового поиска. При этом под ААИ подразумевается автоматическая генерация текстового описания изображения на основе анализа его содержания [1]. Также активно предпринимаются попытки реализации систем ААИ на мобильных платформах, имеющих ограниченные вычислительные ресурсы [2]. Данная тенденция способствует

разработке быстрых алгоритмов ААИ. При этом наиболее рациональным представляется подход, когда вначале выполняется категоризация изображений по типу сцены (например, внутри / снаружи помещения и т. д.), после чего в каждой категории используется дерево решений для определения ключевых слов.

В общем случае системы категоризации сцен используют машинное обучение на основе признакового описания изображений. Однако в изображениях одной и той же категории возможны существенные различия в ракурсе съемки (рисунок 1, а), условиях освещения (рисунок 1, б) и наличии дополнительных объектов, не принадлежащих к категории (рисунок 1, в). Изображения, представленные на рисунке 1, взяты из тестового набора OT8 [3].

Рис. 1. Пример различий: (а) в ракурсе съемки, (б) условиях освещения, (в) наличии небольших объектов

Указанные артефакты приводят к снижению точности категоризации. Для решения этих проблем в данной статье предложено семейство локальных дескрипторов, инвариантных к повороту и масштабированию объектов, сдвигу и масштабированию цветовой интенсивности, а также метод категоризации сцен, использующий вычисление признаков только для наибольших по площади регионов изображения.

2. Локальные дескрипторы. В настоящее время известны различные дескрипторы, однако наиболее распространенными являются Scale-Invariant Feature Transform (SIFT) [4] и Speeded-Up Robust Features (SURF) [5]. В данной работе рассматривается дескриптор SURF и его модификации, т. к. экспериментально показано, что применение SURF дескрипторов требует на порядок меньших вычислительных ресурсов, обеспечивая примерно одинаковые результаты по сравнению с дескриптором SIFT [6, 7].

Базовый алгоритм SURF состоит из двух частей: обнаружение точек интереса и построение дескриптора. Обнаружение точек интереса осуществляется с помощью матрицы Гессе $\mathbf{H}(\mathbf{p},\sigma)$:

$$\mathbf{H}(\mathbf{p};\sigma)=\begin{bmatrix} L_{xx}(\mathbf{p},\sigma) & L_{xy}(\mathbf{p},\sigma) \\ L_{xy}(\mathbf{p},\sigma) & L_{yy}(\mathbf{p},\sigma) \end{bmatrix}, \quad (1)$$

где $\mathbf{p}(x,y)$ — точка в изображении I, σ — масштаб фильтра, $L_{xx}(\mathbf{p},\sigma)$ — свертка части изображения $I(\mathbf{p})$ в точке $\mathbf{p}$ со второй производной Гауссиана $g(\sigma)$:

$$L_{xx}(\mathbf{p},\sigma)=I(\mathbf{p})*\frac{\partial^2}{\partial x^2}g(\sigma). \quad (2)$$

Значения $L_{xy}(\mathbf{p},\sigma)$ и $L_{yy}(\mathbf{p},\sigma)$ вычисляются аналогично выражению (2). Определитель матрицы Гессе (гессиан) обладает инвариантностью относительно вращения, однако чувствителен к изменению масштаба. В связи с этим гессианы вычисляются для нескольких масштабов изображения, тем самым формируя пирамиду карт отклика. В качестве точек интереса выбираются локальные максимумы Гессианов, соответствующие локальным максимумам изменения градиента яркости (пятна, углы и края линий и т. п.).

Далее возле найденной точки интереса выбирается квадратный регион с размером сторон $20s$, где s – масштаб. Полученный регион интереса разбивается на квадратные блоки размером 4×4 элементов. В каждом блоке для 5×5 равномерно распределенных точек вычисля-

ются отклики вейвлета Хаара по горизонтальному L_x и вертикальному L_y направлениям. При этом полученные значения взвешиваются с помощью фильтра Гаусса, центрированного на точке интереса для подавления шумов. На следующем шаге для каждого блока формируется вектор $\mathbf{VD}_{SURF} = \left(\sum L_x, \sum L_y, \sum |L_x|, \sum |L_y|\right)$, образуя часть дескриптора. Конечный SURF дескриптор представляет собой объединение всех 16 векторов и, таким образом, имеет размерность 64.

SURF дескриптор инвариантен к повороту и масштабированию, однако в связи с использованием фильтра Гаусса происходит размытие краев и деталей изображения, что снижает точность описания. Для решения этой проблемы в работе [8] было предложено семейство дескрипторов Gauge SURF (G-SURF), основанных на использовании калибровочных координат. При построении этих дескрипторов в каждой точке интереса рассчитываются вектор градиента **w** и перпендикулярный к нему вектор **v**:

$$\mathbf{w} = \left(\frac{\partial L(\mathbf{p},\sigma)}{\partial x}, \frac{\partial L(\mathbf{p},\sigma)}{\partial y} \right) = \frac{1}{\sqrt{L_x^2(\mathbf{p},\sigma) + L_y^2(\mathbf{p},\sigma)}} \cdot \left(L_x(\mathbf{p},\sigma), L_y(\mathbf{p},\sigma) \right), \quad (3)$$

$$\begin{aligned} \mathbf{v} &= \left(\frac{\partial L(\mathbf{p},\sigma)}{\partial y}, -\frac{\partial L(\mathbf{p},\sigma)}{\partial x} \right) = \\ &= \frac{1}{\sqrt{L_x^2(\mathbf{p},\sigma) + L_y^2(\mathbf{p},\sigma)}} \cdot \left(L_y(\mathbf{p},\sigma), -L_x(\mathbf{p},\sigma) \right) \end{aligned}. \quad (4)$$

Наибольший интерес представляют производные второго порядка выражений (3), (4), использующие матрицы Гессе (выражение (1)) и обозначенные как $L_{ww}(\mathbf{p},\sigma)$ и $L_{vv}(\mathbf{p},\sigma)$:

$$\begin{aligned} L_{ww}(\mathbf{p},\sigma) = \frac{1}{L_x^2(\mathbf{p},\sigma) + L_y^2(\mathbf{p},\sigma)} \left(L_x(\mathbf{p},\sigma) \;\; L_y(\mathbf{p},\sigma) \right) \cdot \\ \cdot \begin{pmatrix} L_{xx}(\mathbf{p},\sigma) & L_{xy}(\mathbf{p},\sigma) \\ L_{yx}(\mathbf{p},\sigma) & L_{yy}(\mathbf{p},\sigma) \end{pmatrix} \begin{pmatrix} L_x(\mathbf{p},\sigma) \\ L_y(\mathbf{p},\sigma) \end{pmatrix} \end{aligned}, \quad (5)$$

$$\begin{aligned} L_{vv}(\mathbf{p},\sigma) = \frac{1}{L_x^2(\mathbf{p},\sigma) + L_y^2(\mathbf{p},\sigma)} \left(L_y(\mathbf{p},\sigma) \;\; -L_x(\mathbf{p},\sigma) \right) \cdot \\ \cdot \begin{pmatrix} L_{xx}(\mathbf{p},\sigma) & L_{xy}(\mathbf{p},\sigma) \\ L_{yx}(\mathbf{p},\sigma) & L_{yy}(\mathbf{p},\sigma) \end{pmatrix} \begin{pmatrix} L_y(\mathbf{p},\sigma) \\ -L_x(\mathbf{p},\sigma) \end{pmatrix} \end{aligned}. \quad (6)$$

Выражение (6) для расчета $L_{vv}(\mathbf{p},\sigma)$ часто используется как детектор «хребтов» («хребет» – это протяженный регион с приблизительно постоянной шириной и интенсивностью, точки которого являются локальными максимумами). Выражение (5), вычисляющее $L_{ww}(\mathbf{p},\sigma)$, содержит информацию об изменении градиента в направлении градиента. Тем самым, дескриптор G-SURF не размывает края на изображении, в то же время оказывает эффект размытия на текстуру, что является положительным фактором для снижения шумов.

В общем виде схема вычисления дескриптора G-SURF совпадает с базовым алгоритмом построения SURF дескриптора, однако для описания блоков региона интереса используется вектор $\mathbf{VD}_{G-SURF} = \left(\sum L_{ww}, \sum L_{vv}, \sum |L_{ww}|, \sum |L_{vv}|\right)$. При этом фильтр Гаусса не оказывает эффекта размытия всего изображения, что позволяет повысить точность описания. Дескриптор G-SURF также как и дескриптор SURF инвариантен к повороту и масштабированию объектов. Однако оба дескриптора SURF и G-SURF вычисляются только на изображениях в оттенках серого и не учитывают цветовую информацию, полезную при категоризации сцен.

3. Цветовые дескрипторы. Для описания цветовой информации были предложены дескрипторы, инвариантные к изменениям цветовой интенсивности, среди которых следует отметить следующие хорошо зарекомендовавшие себя дескрипторы:

- rg-гистограмма основана на нормализованной цветовой модели RGB, в которой хроматические компоненты r и g описывают цветовую информацию [9]. При этом компонент b является избыточным, поскольку $r+g+b=1$:

$$\begin{pmatrix} r \\ g \\ b \end{pmatrix} = \begin{pmatrix} \dfrac{R}{R+G+B} \\ \dfrac{G}{R+G+B} \\ \dfrac{B}{R+G+B} \end{pmatrix}. \qquad (7)$$

Благодаря нормализации компоненты r и g инвариантны к масштабированию интенсивности.

- Opponent-гистограмма вычисляется для изображений в цветовом пространстве Opponent, включающего два цветовых канала O_1, O_2 и компоненту интенсивности O_3 [10]:

$$\begin{pmatrix} O_1 \\ O_2 \\ O_3 \end{pmatrix} = \begin{pmatrix} \dfrac{R-G}{\sqrt{2}} \\ \dfrac{R+G-2B}{\sqrt{6}} \\ \dfrac{R+G+B}{\sqrt{3}} \end{pmatrix}. \quad (8)$$

Как отмечают авторы работы [10], цветовые компонент O_1 и O_2 инвариантны к сдвигу интенсивности, в то время как канал интенсивности O_3 не обладает такими инвариантными свойствами.

- Hue-гистограмма. Для перевода изображения из цветового пространства Opponent в цветовую модель HSI (Hue, Saturation, Intensity) используется следующее выражение:

$$\begin{pmatrix} h \\ s \\ i \end{pmatrix} = \begin{pmatrix} \operatorname{actan}\left(O_1/O_2\right) \\ \sqrt{O_1^2+O_2^2} \\ O_3 \end{pmatrix}. \quad (9)$$

При этом компонент h (оттенок) обладает нестабильностью вблизи серого цвета. В работе [10] было выяснено, что определенность оттенка обратно пропорциональна насыщенности (компонент s). Таким образом, hue-гистограмма становится более устойчивой при умножении каждого значения оттенка на соответствующее значение насыщенности. Hue-гистограмма инвариантна к сдвигу и масштабированию цветовой интенсивности.

- Нормализованная RGB-гистограмма. RGB-гистограмма не является инвариантной к изменениям в условиях освещения. Однако инвариантность к сдвигу и масштабированию интенсивности может быть достигнута нормализацией распределения значений пикселов [11]:

$$\begin{pmatrix} R' \\ G' \\ B' \end{pmatrix} = \begin{pmatrix} \dfrac{R-\mu_R}{\sigma_R} \\ \dfrac{G-\mu_G}{\sigma_G} \\ \dfrac{B-\mu_B}{\sigma_B} \end{pmatrix}, \quad (10)$$

где μ_i — среднее значение в i-ом канале, σ_i — среднеквадратичное отклонение в i-ом канале. Среднее значение μ_i и среднеквадратичное

отклонение σ_i вычисляются по выбранной области (блок или все изображение).

4. Семейство цветовых G-SURF дескрипторов. На основе G-SURF и приведенных выше цветовых дескрипторов (выражения (7) – (10)) разработано семейство дескрипторов, инвариантных к повороту и масштабированию объектов, сдвигу / масштабированию интенсивности:

- rgG-SURF. Для обеих компонент *r* и *g* вычисляются G-SURF дескрипторы, после чего они соединяются в один итоговый, размерностью 2×64. Такой дескриптор обладает инвариантностью к масштабированию интенсивности.
- OppG-SURF описывает все каналы цветового пространства Opponent с помощью G-SURF дескриптора. Благодаря компонентам O_1 и O_2 этот дескриптор инвариантен к сдвигу интенсивности.
- HueG-SURF. G-SURF вычисляется для взвешенного канала *hue* в цветовом пространстве HSI. Этот дескриптор обладает инвариантностью к сдвигу и масштабированию интенсивности. Следует отметить, что в работе [10] предложен дескриптор, в котором SIFT дескриптор, вычисленный на изображении в оттенках серого, объединен с *hue*-гистограммой. Подобным образом был создан дескриптор HHG-SURF, в котором вместо SIFT использовался G-SURF дескриптор. Проведенные эксперименты, не включенные в эту работу, показали, что HueG-SURF и HHG-SURF имеют близкие по значениям результаты категоризации, однако вычисление и последующая обработка HHG-SURF требует больших вычислительных затрат в связи с большей размерностью дескриптора (100 для HHG-SURF).
- RGBG-SURF вычисляется для всех нормализованных каналов цветового пространства RGB. Полученный дескриптор инвариантен к сдвигу и масштабированию интенсивности, а также к изменению интенсивности цветов в отдельных каналах.

5. Алгоритм категоризации сцен. Представим задачу категоризации сцен в следующем виде. Пусть $\mathbf{C}=\{c_1,c_2,\ldots,c_c\}$ — множество категорий сцен, полученных на этапе обучения, а $\mathbf{D}=\{\mathbf{d}_1,\mathbf{d}_2,\ldots,\mathbf{d}_k\}$ — множество глобальных дескрипторов изображений. Тогда категоризация изображения заключается в поиске отображения $f:\mathbf{d}_i\to c_j$, которое однозначно ассоциирует дескриптор *i*-го изображения $\mathbf{D}_i$ с категорией c_j. Таким образом, категоризация сцен требует два инструмента: метод извлечения глобальных дескрипторов и их классификатор.

Для описания изображения широко используется метод Bag-of-Visual-Words (BoVWs) [12], состоящий из трех этапов:

– извлечение из изображений локальных дескрипторов (в данном случае вычисление цветовых G-SURF дескрипторов, указанных в п. 4);

– кластеризация полученных дескрипторов и создание из центров кластеров словаря визуальных слов $\mathbf{V} = \{v_1, v_2 \ldots, v_n\}$;

– формирование на основе набора локальных дескрипторов изображения I глобального дескриптора $\mathbf{VD}_i$ как гистограммы визуальных слов.

Полученные глобальные дескрипторы вместе с метками категорий затем используются для обучения классификатора. Часто для этого применяется машина опорных векторов (Support Vector Machine – SVM) [13]. Рассмотрим данный метод подробнее.

Пусть имеется набор данных для двух категорий $S = \{(\mathbf{D}, \mathbf{L})\}$, где $\mathbf{D} = \{\mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_k\}$ — множество глобальных дескрипторов изображений, а $\mathbf{L} = \{l_1, l_2 \ldots, l_m\}$ — множество соответствующих изображениям меток категорий, принимающих значения ± 1. В случае линейной разделимости классов метод опорных векторов вычисляет гиперплоскость следующего вида:

$$f(\mathbf{D}) = \operatorname{sign}\left(\left\langle \mathbf{z}^{\mathrm{T}}, \mathbf{D} \right\rangle + b\right),$$

где $\mathbf{z}$ — вектор, перпендикулярный к гиперплоскости; b — параметр, характеризующий расстояние от начала координат до гиперплоскости.

Искомая гиперплоскость должна разделять пространство признаков таким образом, чтобы в одном полупространстве оставались объекты только одного класса. Если получено несколько таких гиперплоскостей, то выбирают гиперплоскость с максимальной шириной разделяющей полосы (расстоянием от гиперплоскости до объектов классов). Для этого решается следующая оптимизационная задача:

$$\begin{cases} \left\langle \mathbf{z}, \mathbf{z} \right\rangle \to \min \\ l_i\left(\left\langle \mathbf{z}^{\mathrm{T}}, \mathbf{D}_i \right\rangle + b\right) \geq 1, \quad i = 1, \ldots, k \end{cases}.$$

После вычисления необходимых параметров классификатор может быть использован для категоризации новых данных. Однако на практике данные редко разделяются линейно. Для решения этой проблемы используется два способа. Первый заключается в том, что алгоритму позволяется допускать ошибки на обучающей выборке. С этой целью вводятся дополнительные переменные $\xi_i \geq 0$, характеризующие

величину ошибки для объектов $\mathbf{D}_i$, $i = 1, \ldots, k$. В этом случае оптимизационная задача принимает следующий вид:

$$\begin{cases} \frac{1}{2}\langle \mathbf{z}, \mathbf{z} \rangle + \alpha \sum_{i=1}^{N} \xi_i \to \min \\ l_i \left(\langle \mathbf{z}^{\mathrm{T}}, \mathbf{D}_i \rangle + b \right) \geq 1, \quad i = 1, \ldots, k, \\ \xi_i \geq 0, \quad i = 1, \ldots, k \end{cases}$$

где α — параметр, позволяющий регулировать отношение между максимизацией ширины разделяющей полосы и минимизацией суммарной ошибки.

Другой способ решения проблемы линейной неразделимости классов основан на переходе от исходного пространства признаков $\mathbf{R}^z$ к новому пространству с более высокой размерностью $\mathbf{H}$ с помощью преобразования $\varphi : \mathbf{R}^z \to \mathbf{H}$. При этом отображение φ выбирается таким образом, чтобы в пространстве $\mathbf{H}$ данные были линейно разделимы. В полученном пространстве $\mathbf{H}$ построение SVM проводится точно также, как и ранее, однако скалярное произведение $\langle \mathbf{D}, \mathbf{D}' \rangle$ в пространстве $\mathbf{R}^z$ заменяется на ядро:

$$K(\mathbf{D}, \mathbf{D}') = \langle \varphi(\mathbf{D}), \varphi(\mathbf{D}') \rangle .$$

До сих пор не существует общих методов выбора ядра, поэтому на практике чаще всего используют следующие виды:

– полиномиальное ядро:

$$K(\mathbf{D}, \mathbf{D}') = \left(\gamma \langle \mathbf{D}, \mathbf{D}' \rangle + \alpha \right)^{\beta},$$

где γ, α, β — настраиваемые коэффициенты;

– радиальная базисная функция (РБФ):

$$K(\mathbf{D}, \mathbf{D}') = \exp\left(-\gamma \left\| \mathbf{D} - \mathbf{D}' \right\|^2 \right),$$

– сигмоид:

$$K(\mathbf{D}, \mathbf{D}') = \tanh\left(\gamma \langle \mathbf{D}, \mathbf{D}' \rangle + \alpha \right).$$

Следует отметить, что базовый алгоритм SVM разработан для классификации данных на два класса. Для решения задач классификации нескольких классов применяется метод «один против всех», в ре-

зультате которого обучается m SVM-классификаторов – по одному для каждой категории c_j.

Несмотря на простоту и эффективность метода опорных векторов, у него есть существенный недостаток – SVM неустойчив к шуму. Одним из способов решения этой проблемы является повышение эффективности описания изображений. Исходя из предположения, что изображения сцен состоят из наборов однородных регионов и небольших нетипичных объектов, в данной статье предлагается предварительно сегментировать изображения, после чего извлекать признаки только из 5–7 крупных регионов. Таким образом, алгоритм категоризации сцен имеет следующий вид:

– Шаг 1. Сегментация всех изображений (в работе применен алгоритм цвето-текстурной сегментации J-SEG [14]).

– Шаг 2. Выбор 5–7 наибольших регионов в каждом изображении.

– Шаг 3. Извлечение локальных дескрипторов из выбранных регионов.

– Шаг 4. Создание словаря визуальных слов (используется алгоритм k-средних).

– Шаг 5. Формирование BoVWs-дескрипторов изображений.

– Шаг 6. Обучение SVM-классификаторов.

В предлагаемом алгоритме существенное место занимают локальные дескрипторы, от которых требуется высокая устойчивость к различным изменениям.

6. Результаты экспериментальных исследований. Для экспериментов использовался набор из 8 категорий сцен (далее OT8) [3]. OT8 состоит из 2688 изображений, разделенных на 8 категорий: coast, mountain, forest, open country, street, inside city, tall buildings и highways. Размер каждого изображения 256×256 пикселов. Для обучения из каждой категории случайным образом выбиралось по 100 изображений, остальные использовались для тестирования. На рисунке 2 представлены примеры оригинальных изображений из набора OT8, их сегментированные прототипы (с применением J-SEG алгоритма) с закрашенными белым цветом небольшими регионами и изображения с найденными точками интереса.

Для формирования словаря визуальных слов из обучающей выборки случайным образом выбиралось 200 000 дескрипторов, которые кластеризовались с помощью алгоритма k-средних. В этой работе количество кластеров (визуальных слов) равно 400. С помощью словаря каждому изображению присваивалось BoVWs-описание. В качестве классификатора использовалась реализованная в библиотеке LibSVM [15] машина опорных векторов с ядром в виде радиальной

базисной функции. Все вычисления повторялись 5 раз, после чего точность усреднялась.

Для оценивания эффективности предложенных дескрипторов в тестовый набор были искусственно добавлены изменения: поворот изображений (значения углов: $\pm 2{,}5°, \pm 5{,}0°, \pm 7{,}5°, \pm 10°$), масштабирование интенсивности (значения множителей: $1{,}1^{\pm 1}, 1{,}25^{\pm 1}, 2{,}0^{\pm 1}$) и сдвиг интенсивности (значения: $\pm 5, \pm 10, \pm 15, \pm 20$). В таблицах 1, 2 и 3 представлены данные, полученные при категоризации измененных изображений.

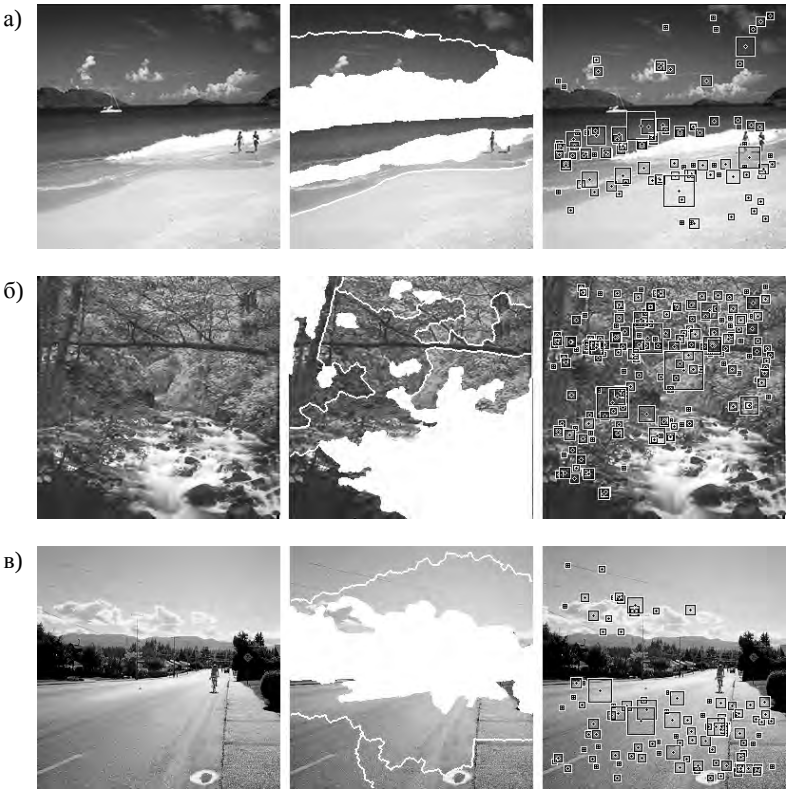


Рис. 2. Пример исходных изображений, их сегментированных прототипов и найденных точек интереса из набора изображений OT8: (а) coast_bea3; (б) forest_land810; (в) highway_urb471; (г) insidecity_hous50; (д) mountain_sharp48; (е) opencountry_open55; (ж) street_par203; (з) tallbuilding_urban1210

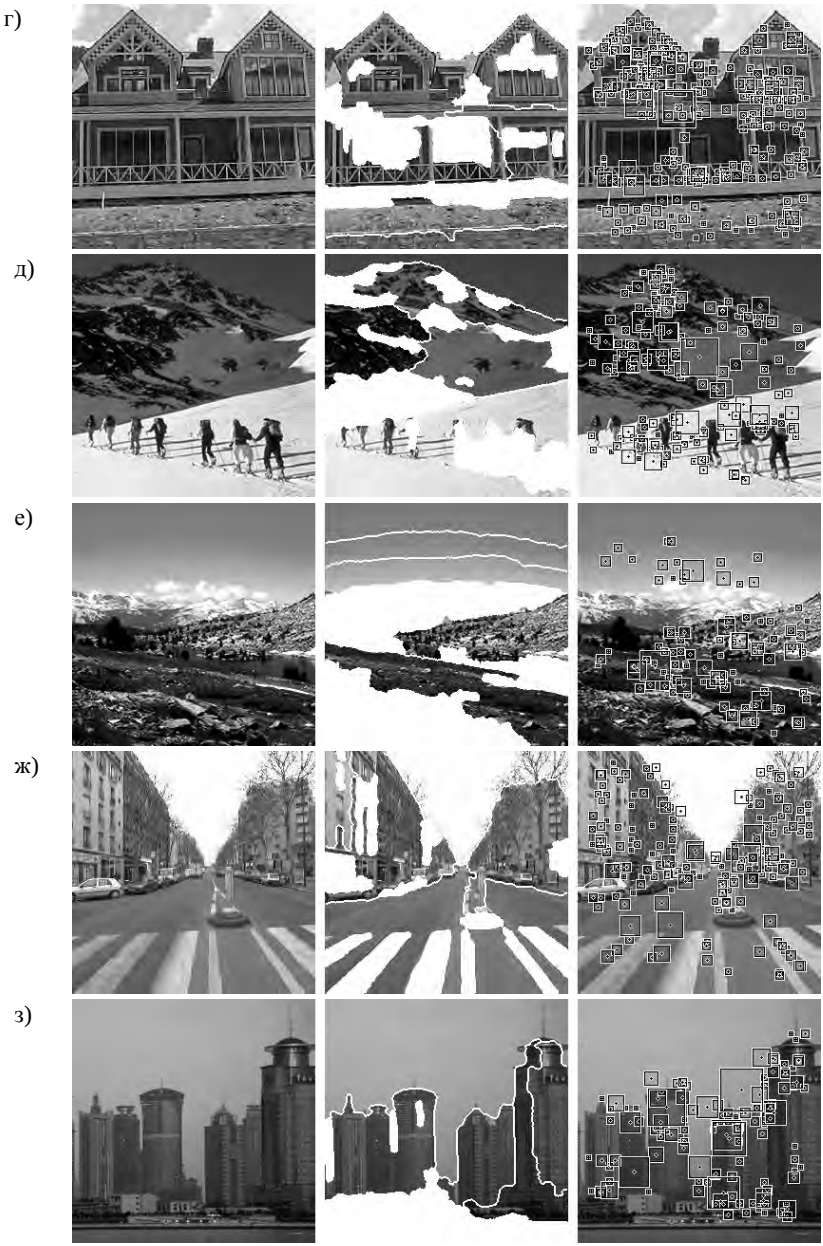


Рис. 2. (продолжение)

Таблица 1. Результаты точности категоризации набора OT8 при поворотах изображений (%)

Угол поворота, °	–10	–7,5	–5,0	–2,5	0,0	2,5	5,0	7,5	10
SURF	78,4	78,8	79,3	79,7	80,1	79,6	79,1	78,9	78,6
G-SURF	82,9	83,4	83,9	84,3	84,4	84,1	83,8	83,5	83,1

По результатам, представленным в таблицы 1, отметим, что устойчивость дескрипторов SURF и G-SURF к поворотам приблизительно одинаковая, однако точность категоризации с использованием дескриптора G-SURF на 4–5 % выше.

Таблица 2. Результаты точности категоризации набора OT8 при масштабировании интенсивности (%)

Множитель	2^{-1}	$1{,}5^{-1}$	$1{,}25^{-1}$	$1{,}1^{-1}$	1	1,1	1,25	1,5	2
G-SURF	82,4	83,7	84,4	85,1	85,4	83,6	80,6	74,3	59,9
rgG-SURF	76,6	76,8	77,0	77,4	77,6	76,9	76,9	74,6	68,7
OppG-SURF	84,2	84,4	84,7	84,9	85,3	84,5	83,3	79,7	70,1
HueG-SURF	66,8	70,0	70,1	71,3	71,6	71,5	70,4	67,9	62,7
RGBG-SURF	85,2	85,3	85,3	85,6	85,7	84,2	83,2	77,2	61,0

Из таблицы 2 видно, что дескриптор HueG-SURF не обладает устойчивостью к масштабированию интенсивности, а дескриптор G-SURF обладает лишь частичной устойчивостью. При этом применение дескрипторов rgG-SURF и HueG-SURF дает низкую точность категоризации. Резкое падение точности в двух последних столбцах (при значениях множителей 1,5 и 2) связано с тем, что значения большей части пикселов на изображениях превысили 255 и были обрезаны.

Таблица 3. Результаты точности категоризации набора OT8 при сдвиге интенсивности (%)

Сдвиг	–20	–15	–10	–5	0	5	10	15	20
G-SURF	82,2	83,4	83,9	84,7	85,4	84,9	84,2	83,4	82,6
rgG-SURF	76,4	76,7	77,2	77,5	77,6	77,6	77,4	77,4	77,1
OppG-SURF	85,3	85,6	85,8	85,5	85,3	85,2	85,1	84,6	84,3
HueG-SURF	70,6	70,8	70,9	71,6	71,6	71,2	71,0	70,9	70,9
RGBG-SURF	84,4	84,9	85,1	85,3	85,7	84,9	84,8	84,8	84,6

Как следует из таблицы 3, дескриптор G-SURF обладает частичной устойчивостью к сдвигу значений интенсивности цветов (имеется в виду сдвиг интенсивности относительно белого цвета). При этом все четыре предложенных дескриптора устойчивы к сдвигу, однако дескрипторы rgG-SURF и HueG-SURF по-прежнему показывают низкую точность категоризации.

Были проведены дополнительные эксперименты для оценки точности определения отдельных категорий изображений. Полученные результаты для набора OT8 представлены в таблице 4.

Как видно из таблицы 4, разные дескрипторы показывают хорошие результаты только для определенных категорий изображений. Таким образом, общую точность категоризации можно повысить, вычисляя дескрипторы на разных цветовых каналах с автоматическим определением весов для каждой категории.

Таблица 4. Результаты точности определения отдельных категорий изображений в наборе OT8 (%)

Категория	Coast	Forest	Highway	Inside city	Mountain	Open country	Street	Tall building
G-SURF	78,3	93,9	80,4	77,9	88,2	*77,8*	91,1	*95,9*
rgG-SURF	84,1	91,8	77,2	69,7	71,4	61,6	77,6	87,3
OppG-SURF	83,4	*96,4*	79,9	78,0	85,5	75,9	*91,5*	92,0
HueG-SURF	77,9	83,9	66,0	59,2	69,9	51,3	79,1	85,8
RGBG-SURF	78,3	95,7	82,9	79,4	*89,3*	*77,8*	88,5	93,9
Oliva A., Torralba A. [3]	79,0	91,0	*87,0*	*90,0*	81,0	71,0	89,0	82,0
Battiato S. и др. [16]	*85,0*	93,0	82,0	87,0	85,0	74,0	89,0	88,0
Gazolli K., Salles E. [17]	84,0	89,0	85,0	80,0	78,0	73,0	86,0	73,0

Следует отметить, что точность категоризации может быть повышена путем создания визуальных слов адаптивным алгоритмом кластеризации Enhanced Self-Organizing Incremental Neural Network [18]. Для формирования BoVWs-описания используя множественную ассоциацию (Multi-Assignment) [19] (ассоциация локального дескриптора не с одним визуальным словом, а с несколькими визуальными словами). Также метод сопоставления пространственных пирамид (Spatial Pyramid Matching) [20] позволит улучшить результаты категоризации.

7. Заключение. В статье представлен метод категоризации набора изображений, использующий расчет локальных дескрипторов только в больших по площади регионах изображений и выполняющий кластеризацию на основе машины опорных векторов. Разработано семейство новых цветовых дескрипторов, инвариантных к повороту и масштабированию объектов, а также к сдвигу и масштабированию цветовой интенсивности. Проведенные экспериментальные исследования показали, что точность категоризации достигает 78–96 % в зависимости от категории изображений, что на 4–5 % выше по сравнению

с применением известных дескрипторов. Приведены методы повышения точности категоризации, которые целесообразно рассмотреть в последующих исследованиях.

Литература

1. *Zhang D., Islam Md.M., Lu G.* A Review on Automatic Image Annotation Techniques // Pattern Recognition. 2012. vol. 45. no. 1. pp. 346–362.
2. *Qin C., Bao X., Choudhury R.R., Nelakuditi S.* TagSense: a Smartphone-based Approach to Automatic Image Tagging // Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services (MobiSys'11). 2011. pp. 1–14.
3. Modeling the Shape of the Scene: a Holistic Representation of the Spatial Envelope. URL: http://people.csail.mit.edu/torralba/code/spatialenvelope (дата обращения: 11.05.2015).
4. *Lowe D.G.* Distinctive Image Features from Scale-Invariant Keypoints // International Journal of Computer Vision. 2004. vol. 60. no. 2. pp. 91–110.
5. *Bay H., Ess A., Tuytelaars T., Gool L.V.* Speeded-Up Robust Features (SURF) // Computer Vision and Image Understanding. 2008. vol. 110. no. 3. pp. 346–359.
6. *Favorskaya M., Jain L.C., Buryachenko V.* Digital Video Stabilization in Static and Dynamic Scenes. Computer Vision in Control Systems-1 // ISRL. Springer Cham Heidelberg New York Dordrecht London: Springer International Publishing Switzerland. 2015. vol. 73. pp. 261–309.
7. *Jain L.C., Favorskaya M., Novikov D.* Panorama Construction from Multi-view Cameras in Outdoor Scenes. Computer Vision in Control Systems-2 // ISRL. Springer Cham Heidelberg New York Dordrecht London: Springer International Publishing Switzerland. 2015. vol. 75. pp. 71–108.
8. *Alcantarilla P.F., Bergasa L.M., Davison A.J.* Gauge-SURF Descriptors // Image and Vision Computing. 2013. vol. 31. no. 1. pp. 103–116.
9. *Gevers T., van de Weijer J., Stokman H.* Color Feature Detection: an Overview. Color Image Processing: Methods and Applications / edited by R. Lukac, K.N. Plataniotis. // University of Toronto. Ontario, Canada: CRC Press. 2006. pp. 203–226.
10. *Van de Weijer J., Gevers T., Bagdanov A.* Boosting Color Saliency in Image Feature Detection // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2006. vol. 28. no. 1. pp. 150–156.
11. *Van de Sande K.E.A., Gevers T., Snoek C.G.M.* Evaluating Color Descriptors for Object and Scene Recognition // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2009. vol. 32. no. 9. pp. 1582–1596.
12. *Csurka G., Dance C.R., Fan L., Willamowski J., Bray C.* Visual Categorization with Bags of Keypoints // Proceedings of Workshop on Statistical Learning in Computer Vision (ECCV'2004). 2004. pp. 1–22.
13. *Vapnik V.N.* Statistical Learning Theory // New York: Wiley. 1998. 768 p.
14. *Deng Y., Manjunath B. S.* Unsupervised Segmentation of Color-Texture Regions in Images and Videos // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2001. vol. 23. no. 8. pp. 800–810.
15. LIBSVM – a Library for Support Vector Machines. URL: http://www.csie.ntu.edu.tw/~cjlin/libsvm (дата обращения: 11.05.2015).
16. *Battiato S., Farinella G.M., Guarnera M., Ravi D., Tomaselli V.* Instant Scene Recognition on Mobile Platform // Computer Vision (ECCV 2012). Workshops and Demonstrations. Lecture Notes in Computer Science. 2012. vol. 7585. pp. 655–658.
17. *Gazolli K., Salles E.* A Contextual Image Descriptor for Scene Classification // Trends in Innovative Computing. 2012. pp. 66–71.

18. *Проскурин А. В.* Формирование визуальных слов для автоматического аннотирования изображений на основе самоорганизующейся нейронной сети // Цифровая обработка сигналов и ее применение (ДСПА'2014). Сб. научн. тр. 16-й Международной конференции. Москва: ИПУ РАН. 2014. Т. 2. С. 487–491.
19. *Jiang Y.G., Ngo C., Yang J.* Towards Optimal Bag-of-Features for Object Categorization and Semantic Video Retrieval // Proceedings of International Conference on Image and Video Retrieval (CIVR '2007). 2007. pp. 494–501.
20. *Lazebnik S., Schmid C., Ponce J.* Beyond Bags of Features: Spatial Pyramid Matching for Recognizing Natural Scene Categories // Proceedings of IEEE Conference on Computer Vision and Pattern Recognition. 2006. vol. 2. pp. 2169–2178.

References

1. Zhang D., Islam Md.M., Lu G. A Review on Automatic Image Annotation Techniques. *Pattern Recognition*. 2012. vol. 45. no. 1. pp. 346–362.
2. Qin C., Bao X., Choudhury R.R., Nelakuditi S. TagSense: a Smartphone-based Approach to Automatic Image Tagging. Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services (MobiSys'11). 2011. pp. 1–14.
3. Modeling the Shape of the Scene: a Holistic Representation of the Spatial Envelope. Available at: http://people.csail.mit.edu/torralba/code/spatialenvelope (accessed 11.05.2015).
4. Lowe D.G. Distinctive Image Features from Scale-Invariant Keypoints. *International Journal of Computer Vision*. 2004. vol. 60. no. 2. pp. 91–110.
5. Bay H., Ess A., Tuytelaars T., Gool L.V. Speeded-Up Robust Features (SURF). *Computer Vision and Image Understanding*. 2008. vol. 110. no. 3. pp. 346–359.
6. Favorskaya M., Jain L.C., Buryachenko V. Digital Video Stabilization in Static and Dynamic Scenes. Computer Vision in Control Systems-1. *ISRL*. Springer Cham Heidelberg New York Dordrecht London: Springer International Publishing Switzerland. 2015. vol. 73. pp. 261–309.
7. Jain L.C., Favorskaya M., Novikov D. Panorama Construction from Multi-view Cameras in Outdoor Scenes. Computer Vision in Control Systems-2. *ISRL*. Springer Cham Heidelberg New York Dordrecht London: Springer International Publishing Switzerland. 2015. vol. 75. pp. 71–108.
8. Alcantarilla P.F., Bergasa L.M., Davison A.J. Gauge-SURF Descriptors. *Image and Vision Computing*. 2013. vol. 31. no. 1. pp. 103–116.
9. Gevers T., van de Weijer J., Stokman H. Color Feature Detection: an Overview. Color Image Processing: Methods and Applications. Edited by R. Lukac, K.N. Plataniotis. University of Toronto. Ontario. Canada: CRC Press. 2006. pp. 203–226.
10. Van de Weijer J., Gevers T., Bagdanov *A.* Boosting Color Saliency in Image Feature Detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2006. vol. 28. no. 1. pp. 150–156.
11. Van de Sande K.E.A., Gevers T., Snoek C.G.M. Evaluating Color Descriptors for Object and Scene Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2009. vol. 32. no. 9. pp. 1582–1596.
12. Csurka G., Dance C.R., Fan L., Willamowski J., Bray C. Visual Categorization with Bags of Keypoints. Proceedings of Workshop on Statistical Learning in Computer Vision (ECCV'2004). 2004. pp. 1–22.
13. Vapnik V.N. Statistical Learning Theory. New York: Wiley. 1998. 768 p.
14. Deng Y., Manjunath B. S. Unsupervised Segmentation of Color-Texture Regions in Images and Videos. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2001. vol. 23. no. 8. pp. 800–810.
15. LIBSVM – a Library for Support Vector Machines. Available at: http://www.csie.ntu.edu.tw/~cjlin/libsvm (accessed 11.05.2015).

16. Battiato S., Farinella G.M., Guarnera M., Ravi D., Tomaselli V. Instant Scene Recognition on Mobile Platform. Computer Vision (ECCV 2012). Workshops and Demonstrations. Lecture Notes in Computer Science. 2012. vol. 7585. pp. 655–658.
17. Gazolli K., Salles E. A Contextual Image Descriptor for Scene Classification. *Trends in Innovative Computing*. 2012. pp. 66–71.
18. Proskurin A.V. [Creating Visual Words for Automatic Image Annotation Based on Self-Organizing Incremental Neural Network]. *Tsifrovaia obrabotka signalov I ee primenenie (DSPA-2014)*: *Sb. naychn. tr. 16-i Mezhdunarodnoi konferentsii* [Proceedings of the 16th International Conference “Digital Signal Processing and its Applications”]. Moscow: ISC RAS. 2014. vol. 2. pp. 487–491 (In Russ.).
19. Jiang Y.G., Ngo C., Yang J. Towards Optimal Bag-of-Features for Object Categorization and Semantic Video Retrieval. Proceedings of International Conference on Image and Video Retrieval (CIVR ‘2007). 2007. pp. 494–501.
20. Lazebnik S., Schmid C., Ponce J. Beyond Bags of Features: Spatial Pyramid Matching for Recognizing Natural Scene Categories. Proceedings of IEEE Conference on Computer Vision and Pattern Recognition. 2006. vol. 2. pp. 2169–2178.

Фаворская Маргарита Николаевна — д-р техн. наук, профессор, заведующий кафедрой информатики и вычислительной техники, Институт информатики и телекоммуникаций Сибирского государственного аэрокосмического университета имени академика М.Ф. Решетнева (СибГАУ). Область научных интересов: цифровая обработка изображений и видеопоследовательностей, распознавание образов, кластеризация, информационные технологии. Число научных публикаций — 170. favorskaya@sibsau.ru; пр. им. газ. "Красноярский рабочий", 31, Красноярск, 660014; р.т.: +7 391 291 9240, Факс: +7 391-291-91-47.

Favorskaya Margarita Nikolaevna — Ph.D., Dr. Sci., professor, head of informatics and computer techniques department, Institute of Informatics and Telecommunications of Siberian State Aerospace University named after academician M.F. Reshetnev (SibSAU). Research interests: digital image and videos processing, pattern recognition, fractal image processing, artificial intelligence, information technologies, remote sensing. The number of publications — 170. favorskaya@sibsau.ru; 31, Krasnoyarsky Rabochy av., Krasnoyarsk, 660014; office phone: +7 391 291 9240, Fax: +7 391 291 9147.

Проскурин Александр Викторович — аспирант кафедры информатики и вычислительной техники, Институт информатики и телекоммуникаций Сибирского государственного аэрокосмического университета имени академика М.Ф. Решетнева (СибГАУ). Область научных интересов: цифровая обработка изображений, распознавание образов. Число научных публикаций — 17. Proskurin.AV.WOF@gmail.com; пр. им. газ. "Красноярский рабочий", 31, Красноярск, 660014; р.т.: +7(391)291-9241, Факс: +7(391)291-9147.

Proskurin Alexander Viktorovich — Ph.D. student of informatics and computer science department, Institute of Informatics and Telecommunications, Siberian State Aerospace University named after academician M.F. Reshetnev (SibSAU). Research interests: digital image processing, pattern recognition. The number of publications — 17. Proskurin.AV.WOF@gmail.com; 31, Krasnoyarsky Rabochy av., Krasnoyarsk, 660014; office phone: +7(391)291-9241, Fax: +7(391)291-9147.

РЕФЕРАТ

Фаворская М.Н., Проскурин А.В. **Категоризация сцен на основе расширенных цветовых дескрипторов.**

Значительный рост количества изображений в сети Интернет и необходимость их поиска предполагает разработку систем автоматической категоризации изображений. Однако задача автоматической категоризации не является тривиальной, поскольку между изображениями часто наблюдаются существенные различия в ракурсе съемки, условиях освещения и наличии объектов, не принадлежащих категории. Для решения этих проблем предложен алгоритм категоризации сцен на основе описания изображений как гистограмм визуальных слов и машины опорных векторов. Разработано семейство новых цветовых дескрипторов на основе локального дескриптора Gauge Speeded-Up Robust Features, инвариантного к повороту и масштабированию. Предложенные дескрипторы дополнительно являются инвариантными к изменениям цветовой интенсивности. Они применяются для описания 5–7 больших по площади регионов изображения после предварительной цвето-текстурной сегментации нс основе J-SEG алгоритма. Проведенные экспериментальные исследования показали, что точность категоризации достигает 78–96 % в зависимости от категории изображений, что на 4–5 % выше по сравнению с применением известных дескрипторов. Приведены методы повышения точности категоризации, которые целесообразно рассмотреть в последующих исследованиях.

SUMMARY

Favorskaya M.N., Proskurin A.V. **Scene Categorization Based on Extended Color Descriptors.**

Huge volume of images in WWW and necessity of their retrieval assume the development of systems for automatic images categorization. However, the task of automatic image categorization is not trivial due to essential differences between images in viewpoint shooting, light intensities, and additional objects in images, which do not concern to some category. The algorithm of scene categorization based on image description as a histogram of visual words and support vector machine is designed in order to compensate such image artifacts. Family of novel color descriptors based on local Gauge Speeded-Up Robust Features, which is invariant to rotation and scaling, has been developed. Additionally, the proposed descriptors are invariant to light intensity. They are used for description of 5–7 large area regions in image after preliminary color and texture segmentation based on J-SEG algorithm. Experimental researches show that values of categorization precision achieve 78–96 % in dependence on image category. These values exceed results received by use of conventional descriptors on 4–5 %. The improved categorization methods are mentioned as future investigation.

РУКОВОДСТВО ДЛЯ АВТОРОВ

Взаимодействие автора с редакцией осуществляется через личный кабинет на сайте журнала «Труды СПИИРАН» http://www.proceedings.spiiras.nw.ru. При регистрации авторам рекомендуется заполнить все предложенные поля данных, так как это значительно ускорит процесс оформления метаданных к новым статьям.

Подготовка статьи ведется с помощью текстовых редакторов MS Word 2007 и выше. При подаче материала в редакцию сначала отправляется только статья в формате *.docx. Для обеспечения требований слепого рецензирования при представлении статьи в журнал авторам необходимо удалить персональные данные, содержащиеся в тексте файла и его свойствах.

Объем основного текста – от 5 до 20 страниц включительно. Формат страницы документа – A5 (148 мм ширина, 210 мм высота); ориентация – портретная; все поля – 20 мм. Верхний и нижний колонтитулы страницы – пустые. Основной шрифт документа – Times New Roman, основной кегль (размер) шрифта – 10 pt. Переносы разрешены. Абзацный отступ устанавливается размером в 10 мм. Межстрочный интервал – одинарный. Номера страниц не проставляются.

Не допускается использования цветных шрифтов, цветовых выделений и цветных рисунков. Статьи должны быть полностью готовы к черно-белой печати.

Основная часть текста статьи разбивается на разделы, среди которых являются обязательными: введение, хотя бы один «содержательный» раздел и заключение. Допускается также мотивированное содержанием и структурой материала выделение подразделов.

В основную часть допускается помещать рисунки, таблицы, листинги и формулы. Правила их оформления подробно рассмотрены на нашем сайте в разделе «Руководство для авторов».

ISSN 2078-9181

Вып. 3(40)

ТРУДЫ СПИИРАН
proceedings.spiiras.nw.ru

С-Пб
2015