DOI 10.17587/issn.1684-6400

ISSN 1684-6400

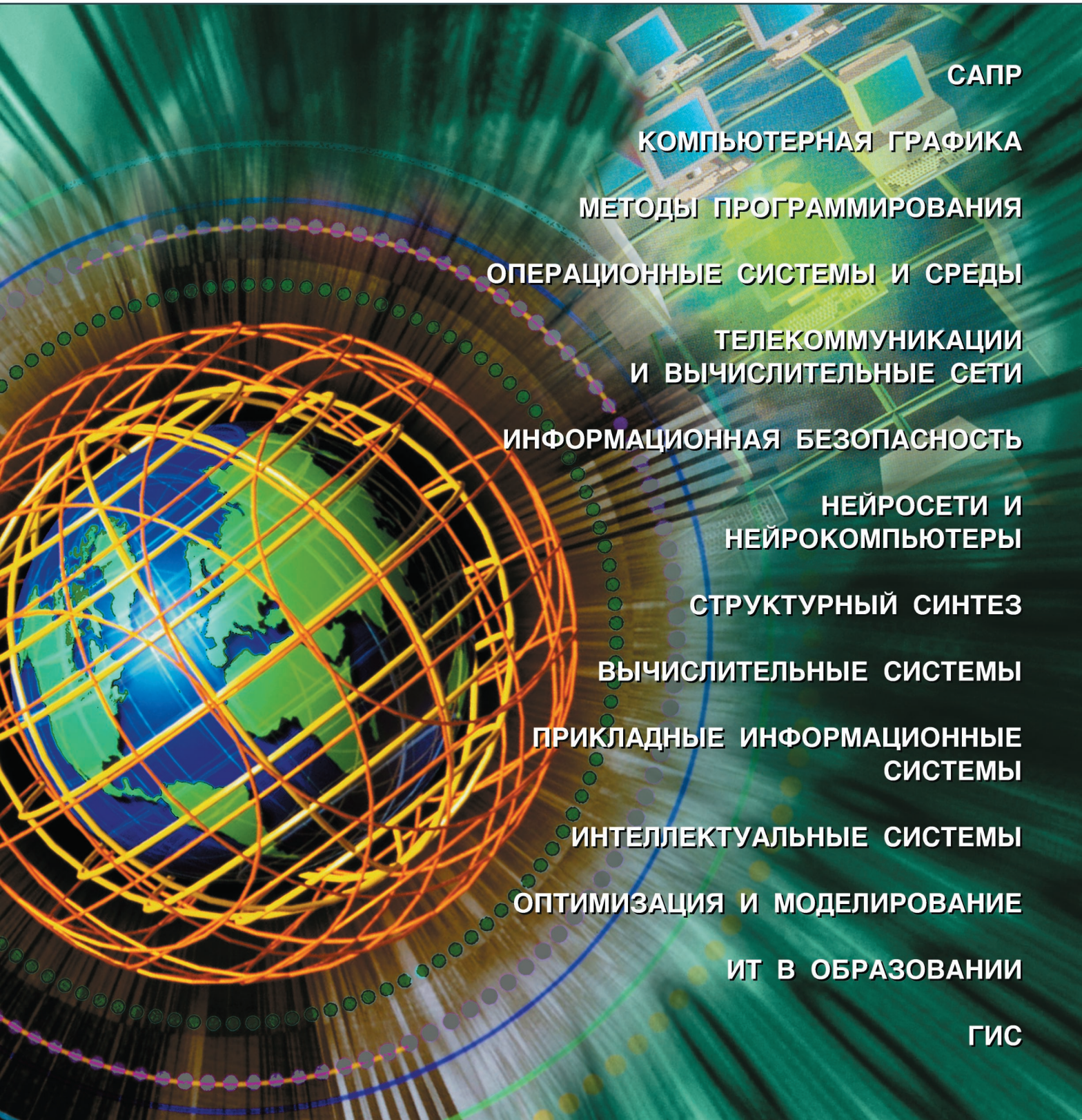
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Том 27

2021

№ 2

ТЕОРЕТИЧЕСКИЙ И ПРИКЛАДНОЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ



САПР

КОМПЬЮТЕРНАЯ ГРАФИКА

МЕТОДЫ ПРОГРАММИРОВАНИЯ

ОПЕРАЦИОННЫЕ СИСТЕМЫ И СРЕДЫ

ТЕЛЕКОММУНИКАЦИИ И ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

НЕЙРОСЕТИ И НЕЙРОКОМПЬЮТЕРЫ

СТРУКТУРНЫЙ СИНТЕЗ

ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ

ПРИКЛАДНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ

ОПТИМИЗАЦИЯ И МОДЕЛИРОВАНИЕ

ИТ В ОБРАЗОВАНИИ

ГИС

Рисунки к статье А. Б. Терентьева, И. В. Штурца

«УСТРАНЕНИЕ АЛИАСИНГА В ДОППЛЕРОВСКОЙ ЭХОКАРДИОГРАФИИ С ПОМОЩЬЮ ФИЛЬТРАЦИИ СУБМАКСИМАЛЬНЫХ КОМПОНЕНТ СКОРОСТЕЙ»

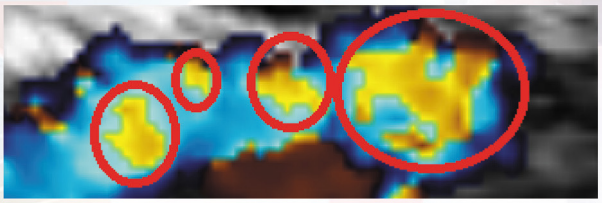
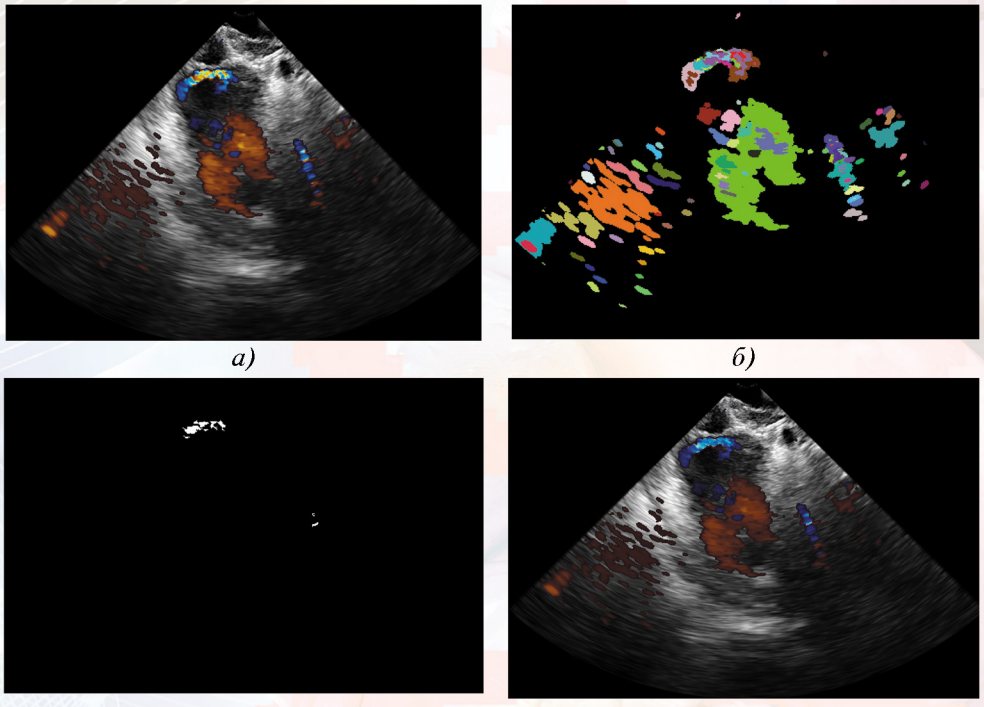


Рис. 1. Пример алиасинга. Кровоток от датчика с наиболее высокими скоростями отображается как обратный



а) *б)* *в)* *г)*

Рис. 2. Оригинальный кадр (*а*) последовательности набора данных, разбиение его данных кровотока на компоненты, каждая окрашена своим цветом (*б*), маска пикселов с алиасингом (*в*) и итоговое изображение (*г*)

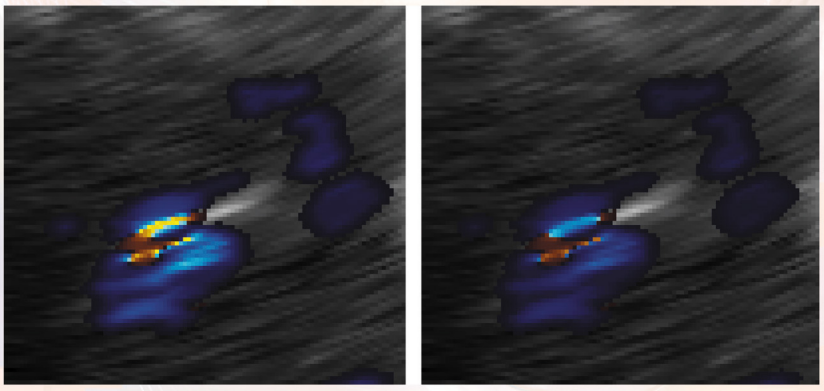


Рис. 3. Пример неполного устранения алиасинга на фрагменте кадра

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Том 27
2021
№ 2

ТЕОРЕТИЧЕСКИЙ И ПРИКЛАДНОЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

Издается с ноября 1995 г. DOI 10.17587/issn.1684-6400

УЧРЕДИТЕЛЬ
Издательство "Новые технологии"

СОДЕРЖАНИЕ

Информация о журнале доступна по сети Internet по адресу **http://novtex.ru/IT.**
Журнал включен в систему Российского индекса научного цитирования и базу данных RSCI на платформе Web of Science.
Журнал входит в Перечень научных журналов, в которых по рекомендации ВАК РФ должны быть опубликованы научные результаты диссертаций на соискание ученой степени доктора и кандидата наук.

INFORMATION TECHNOLOGIES
INFORMACIONNYE TEHNOLOGII

Vol. 27
2021
No. 2

THEORETICAL AND APPLIED SCIENTIFIC AND TECHNICAL JOURNAL

Published since November 1995

DOI 10.17587/issn.1684-6400

ISSN 1684-6400

CONTENTS

Complete Internet version of the journal at site: **http://novtex.ru/IT.**
According to the decision of the Higher Certifying Commission of the Ministry of Education of Russian Federation, the journal is inscribed in "The List of the Leading Scientific Journals and Editions wherein Main Scientific Results of Theses for Doctor's or Candidate's Degrees Should Be Published"

УДК 004.942 DOI: 10.17587/it.27.59-64

Д. А. Абрамешин, аспирант, вед. инженер, e-mail: Dabrameshin@hse.ru,
Е. Д. Пожидаев, д-р техн. наук, проф., e-mail: EPozhidaev@hse.ru,
С. Р. Тумковский, д-р техн. наук, проф., e-mail: STumkovskiy@hse.ru,
Национальный исследовательский университет "Высшая школа экономики", Москва

Моделирование радиационного заряжения корпусов микроэлектронной аппаратуры космического применения

Разработана модель и методика математического моделирования радиационного заряжения полимерных корпусов микроэлектронной аппаратуры, обладающих повышенной проводимостью, в основе которых лежит применение аппроксимационной функции экспериментальной зависимости проводимости корпуса от времени облучения, полученной с использованием методов параметрической идентификации. Результаты исследований направлены на разработку композитных полимерных материалов для корпусов микроэлектронной аппаратуры с проводимостью, обеспечивающей отсутствие электростатических разрядов, что, в свою очередь, позволяет существенно увеличить сроки активного существования космических аппаратов.

Ключевые слова: *математическое и компьютерное моделирование, радиационная заряжение, радиационная проводимость, электростатические разряды, космические аппараты, микроэлектронная аппаратура*

Введение

В настоящее время корпусирование в полимерные композиционные материалы является перспективным направлением герметизации микросхем, применяющихся в космической технике, что дает ряд преимуществ, а именно: уменьшение массогабаритных характеристик интегральных микросхем в 2,5...3 раза по сравнению со схемами, корпусированными в металлокерамику; обеспечение корпусом хорошего теплоотвода; высокую технологичность производства интегральных схем; снижение себестоимости интегральных схем в пластиковых корпусах.

В то же время полимерные корпуса микроэлектронной аппаратуры космических аппаратов (КА), функционирующих на околоземных орбитах, подвержены интенсивному воздействию электронов и ионов космической плазмы [1, 2]. В результате в них накапливается электрический заряд и, таким образом, происходит радиационное заряжение. Последующие электростатические разряды (ЭСР) могут приводить к отказам в работе микроэлектронной аппаратуры и, тем самым, влияют на надежность функционирования КА [3—5].

К настоящему времени разработан ряд методов защиты микроэлектронной аппаратуры (МЭА) от воздействия ЭСР [6, 7]. Для микроэлектроники, находящейся внутри КА, было предложено использовать композитные полимерные материалы корпусов с повышенной проводимостью [8, 9], получаемые добавлением в полимер корпуса МЭА определенного количества проводящего материала (нанотрубок, графитированной сажи, металлического порошка и т.д.). Тем самым увеличивается темновая проводимость полимера, возникает растекание и выравнивание накапливаемого заряда, и разряды не происходят.

По данным НАСА [10] при радиационном заряжении диэлектриков, находящихся под воздействием космической плазмы, электростатические разряды возникают, когда напряженность электрического поля в них достигает критического значения, равного $2 \cdot 10^7$ В$\cdot$м$^{-1}$. С учетом этого фактора моделирование кинетики заряжения позволит установить минимально допустимую проводимость полимерного корпуса микроэлектронной аппаратуры, обеспечивающую отсутствие электростатических разрядов. Однако, если для чистых диэлектриков с удельной объемной проводимо-

стью порядка $10^{-16}...10^{-18}$ Ом$^{-1}\cdot$м$^{-1}$ имеется целый ряд работ по кинетике накопления заряда и соответствующие физико-математические модели заряжения [11, 12], то для полимерных композитов такие работы за исключением нескольких [13, 14] практически отсутствуют.

В работе [13] на простой модели, учитывающей только темновую проводимость диэлектрика, показано, что его удельная объемная проводимость 10^{-10} Ом$^{-1}\cdot$м$^{-1}$обеспечивает отсутствие ЭСР. Однако эта модель не рассматривает наличие радиационной проводимости, хотя последняя в процессе облучения может существенно уменьшать сопротивление диэлектрика. Первая попытка учета радиационной проводимости полимера была сделана в работе [14]. Настоящее исследование является дальнейшим развитием работ в данном направлении.

Для описания временной зависимости радиационной проводимости можно использовать систему уравнений модели Роуза—Фаулера—Вайсберга [15]. Однако при этом возникает необходимость решения сложной системы интегрально-дифференциальных уравнений, что не всегда оправдано, поэтому для построения модели мы использовали аналитическую функцию кинетики заряжения, полученную путем аппроксимации экспериментальной кривой зависимости радиационной проводимости конкретного полимерного материала от времени.

Модель радиационного заряжения полимерного корпуса

Для нас представляет интерес не столько зависимость от времени количества накапливаемого в полимере корпуса заряда, сколько рост со временем облучения значения напряженности электрического поля, создаваемого этим зарядом. Для ЭСР, возникающих при воздействии космической плазмы, как мы уже отмечали, обычно принимается, что они появляются при достижении напряженностью электрического поля в диэлектрике критического значения, составляющего $2\cdot10^7$ В$\cdot$м$^{-1}$ [10]. По указанной причине при моделировании мы будем использовать дифференциальное уравнение зависимости напряженности электрического поля от времени воздействия электронов плазмы на полимер (времени радиационного облучения):

$$\frac{dE}{dt} = \frac{h-R}{h\varepsilon_0\varepsilon}\{i_0 - [E(t)(\gamma_D + \gamma_R)]\}, \qquad (1)$$

где E — напряженность электрического поля в облучаемой части полимера, В$\cdot$м$^{-1}$; t — время обучения, с; i_0 — плотность потока электронов, падающих на поверхность пленки, А$\cdot$м$^{-2}$; $\varepsilon_0 = 8{,}85\cdot10^{-12}$ Ф$\cdot$м$^{-1}$ — электрическая постоянная; ε — относительная диэлектрическая постоянная полимерного электрика; γ_D — темновая проводимость полимера корпуса; $\gamma_R(t)$ — радиационная проводимость полимера (в облучаемой ее части); R — максимальный пробег электрона; h — толщина корпуса.

Схема радиационного заряжения полимерного корпуса по предложенной нами модели приведена на рис. 1. Электроны с плотностью потока i_0 из магнитосферной плазмы падают на поверхность полимерного корпуса и проникают в него вплоть до длины пробега R.

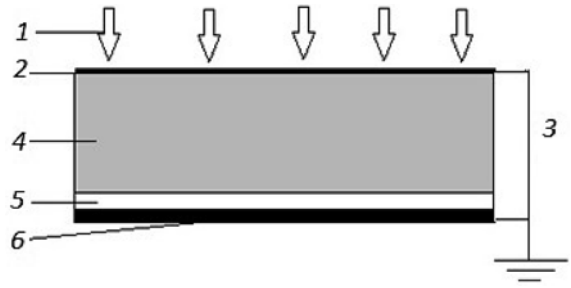


Рис. 1. Схема радиационного заряжения полимерного корпуса при его облучении электронами:

1 — электроны из космической плазмы; *2* — верхний тонкий проводящий электрод из оксида индия; *3* — заземление; *4* — облучаемый слой корпуса; *5* — не облучаемый слой корпуса; *6* — нижний металлический электрод

В верхней части полимерного корпуса выход заряда на электрод осуществляется как за счет темновой, так и за счет радиационной проводимости. В нижней части корпуса, куда не проникают падающие электроны, выход заряда на электрод осуществляется только за счет темновой проводимости.

Методика моделирования зависимости радиационной проводимости полимерного корпуса от времени облучения

Для моделирования зависимости накопленного заряда в полимерном корпусе от времени нужно знать, как меняется во времени его радиационная проводимость (РП) $\gamma_R(t)$. В качестве аппроксимационной функции нами была предложена следующая:

$$\gamma_R = c_1 + c_2\exp(-t/c_3) + c_4\exp(-t/c_5), \qquad (2)$$

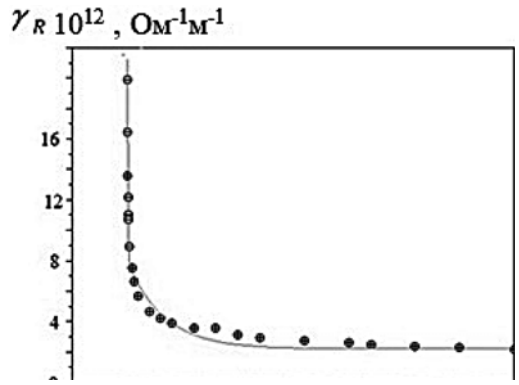


Рис. 2. Экспериментальная и расчетная зависимости радиационной проводимости от времени облучения:
⊕ — экспериментальная; —— — расчетная

где c_1, c_2, c_3, c_4, c_5 — параметры, постоянные для конкретного полимера, из которого состоит корпус.

При корпусировании МЭА применяются сложные полимерные композитные материалы. Однако механизм радиационного заряжения различных полимеров один и тот же, поэтому для построения аппроксимирующей функции в качестве модельного материала полимерного корпуса мы будем использовать полистирол (ПС).

На рис. 2 приведены экспериментальная и расчетная зависимости радиационной проводимости от времени облучения образца ПС с толщиной 20 мкм, полученные для энергии электронного пучка 50 кэВ и плотности потока электронного облучения $i_0 = 3{,}18 \cdot 10^{-4}$ А·м$^{-2}$.

Эксперимент проводился на установке, имитирующей радиационное заряжение полимерных образцов под воздействием потока электронов из космической плазмы при комнатной температуре в вакууме $2 \cdot 10^{-5}$ мм рт. ст. Блок-схема установки и методика измерений подробно описана в работе [16].

```
clear;
function [zr]=G(c,z)
   zr=z(2)- c(1) - c(2)*exp(-z(1)/c(3))-c(4)*exp(-z(1)/c(5));
endfunction
//Исходные данные
x=[1 2 3 6 4 12 16 20 24 28 32 36 40 44 48 52 56 60 64 68 72 76 80];
y=[12.74 11.82 11.54 11.33 9.34 7.78 6.94 6.23 5.52 5.03 4.74 4.32 4.18 3.96 3.82
3.61 3.47 3.33 3.26 3.17 3.11 3.04 3.02];
//Построение графика экспериментальных данных

plot2d(x',y',[-3],"011"," ",[0,0,x(length(x)),14]);
//Вектор начальных приближений
c=[2.8;15;10;1;400];
//Формирование матрицы исходных данных
z=[x;y];
//Решение задачи
[c,err]=datafit(G,z,c);

// Построение графика подобранной функции
xnew = 0:10:x(length(x));
ycalc=c(1)+c(2)*exp(-xnew/c(3))+c(4)*exp(-xnew/c(5));
plot2d(xnew',ycalc',[3],"000");
printf("\nc(1)=%3.3g c(2)=%3.3g c(3)=%3.3g c(4)=%3.3g
c(5)=%3.3g\n",c(1),c(2),c(3),c(4),c(5));
```

Рис. 3. Программа идентификации коэффициентов аппроксимирующей функции для системы SciLab

В качестве аппроксимационной функции для ПС была выбрана следующая функция:

$$\gamma_R = 0{,}475 \cdot 10^{-11} + 7 \cdot 10^{-11} \exp(-t/5) + \\ + 0{,}9 \cdot 10^{-11} \exp(-t/470). \qquad (3)$$

При этом коэффициенты c_1, c_2, c_3, c_4, c_5 были получены методом идентификации, основанном на квазиньютоновском методе оптимизации. Программа идентификации параметров с применением системы SciLab приведена на рис. 3.

Как видно из рис. 2, предложенная аппроксимирующая функция дает хорошее совпадение с экспериментальными данными.

Экспериментальные данные по РП были получены для плотности потока электронного облучения $i_0 = 3{,}18 \cdot 10^{-4}$ А·м$^{-2}$, однако спокойной геомагнитной обстановке соответствует $i_0 = 10^{-7}$ А·м$^{-2}$, а суббуре — 10^{-5} А·м$^{-2}$. Для получения общего выражения зависимости радиационной проводимости от времени облучения при переменной плотности электронного потока нами был использован подход, изложенный в работе [12], где РП описывается выражением

$$\gamma_R = A_m (R_0)^{\Delta} f(t).$$

Здесь R_0 — мощность дозы облучения; Δ — постоянный параметр, определяемый природой полимера, для ПС $\Delta = 0{,}75$; $f(t)$ — временная функция РП; A_m — постоянная.

Мощность дозы R_0 связана с плотностью потока электронов i_0 выражением

$$R_0 = i_0 \frac{dE/dx}{q_e},$$

где $q_e = 1{,}602 \cdot 10^{-19}$ Кл — заряд электрона; $\frac{dE}{dx}$ — тормозная способность электронов, эВ·м$^{-1}$.

Принимая это во внимание, мы будем вместо (3) использовать выражение

$$\gamma_R = A(i_0)^{\Delta} f(t), \qquad (4)$$

где A — соответствующая постоянная.

Тогда, сопоставляя выражения (2) и (4), получаем для РП ПС от времени облучения следующее выражение:

$$\gamma_R = A(i_0)^{\Delta} f(t) = 2 \cdot 10^{-9} (i_0)^{0,75} \times \\ \times [1 + 14,7 \exp(-t/5) + 1,89 \exp(-t/470)]. \quad (5)$$

Полученное выражение (5) позволяет рассчитывать изменение РП ПС во времени для разных плотностей потока электронов. Это представляется существенным при анализе заряжения ПС в условиях протекании суббури, когда плотность потока электронов из космической плазмы может существенно возрастать по сравнению со спокойной геомагнитной обстановкой.

Моделирование радиационного заряжения ПС

Полученную функцию (5) подставим в дифференциальное уравнение (1), численно проинтегрируем методом Рунге—Кутты четвертого порядка с использованием системы SciLab. Решение уравнения позволяет моделировать заряжение полимерных композитных корпусов при различных значениях проводимости.

В качестве примера для $R = 0,5h$ на рис. 4 приведены результаты компьютерного моделирования кинетики заряжения ПС, имеющего удельную объемную темновую проводимость $\gamma_D = 10^{-15}$ Ом$^{-1}$·м$^{-1}$. Плотность потока электронов составляет 10^{-7} А·м$^{-2}$, что соответствует спокойной геомагнитной обстановке.

Кривая *1* показывает, как изменяется напряженность электрического поля со временем облучения в отсутствии радиационной проводимости. Штриховой линией на рис. 4 показан уровень критической напряженности поля, при которой должен иметь место разряд. Видно, что при учете только темновой проводимости должен происходить электростатический разряд, и это обусловлено ее незначительным значением. Но наличие радиационной проводимости приводит к резкому снижению напряженности электрического поля (кривая *2*), и ЭСР возникать не будет. Таким образом, РП ПС в спокойной геомагнитной обстановке обеспечивает отсутствие разрядов в тонком слое ПС.

В то же время в условиях суббури, когда плотность потока электронов возрастает до 10^{-5} А·м$^{-2}$, как показывает рис. 5, радиационная проводимость ПС с $\gamma_D = 10^{-15}$ Ом$^{-1}$·м$^{-1}$ уже не будет в достаточной мере снижать напряженность поля, и это приводит к возникновению ЭСР. Для того чтобы в этих условиях исключить ЭСР, как показывает рис. 6, необходимо создавать композитный корпус ПС с проводящим наполнителем, имеющий удельную объемную темновую проводимость по крайней мере $\gamma_D = 10^{-12}$ Ом$^{-1}$·м$^{-1}$.

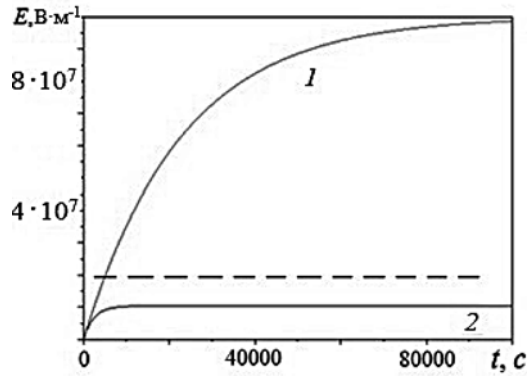


Рис. 4. Изменение напряженности электрического поля ПС с $\gamma_D = 10^{-15}$ Ом$^{-1}$·м$^{-1}$ от времени облучения электронами с плотностью потока 10^{-7} А·м$^{-2}$ пленки:

1 — без учета РП; *2* — с учетом РП. Штриховая линия показывает уровень критической напряженности поля, при которой возникает ЭСР

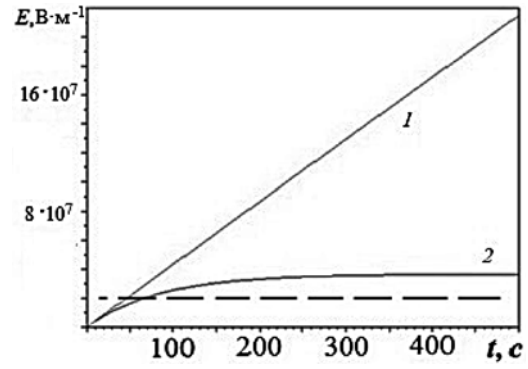


Рис. 5. Изменение напряженности электрического поля ПС с $\gamma_D = 10^{-15}$ Ом$^{-1}$·м$^{-1}$ от времени облучения электронами с плотностью потока 10^{-5} А·м$^{-2}$:

1 — без учета РП; *2* — с учетом РП. Штриховая линия показывает уровень критической напряженности поля, при которой возникает ЭСР

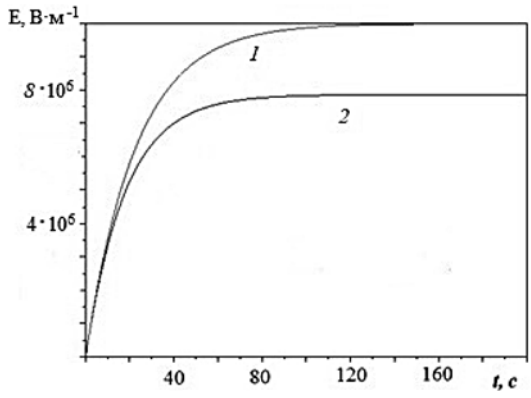


Рис. 6. Изменение напряженности электрического поля ПС с $\gamma_D = 10^{-12}$ Ом$^{-1}$·м$^{-1}$ от времени облучения электронами с плотностью потока 10^{-5} А·м$^{-2}$:

1 — без учета РП; *2* — с учетом РП

Заключение

Предложена модель радиационного заряжения полимерных корпусов микроэлектронной аппаратуры, учитывающая как темновую, так и радиационную проводимость, возникающие в процессе облучения. Модель адекватно описывает радиационное заряжение полимерных композитных корпусов с повышенной проводимостью, в которые добавлен в строго определенной степени проводящий наполнитель и которые в результате растекания заряда обеспечивают отсутствие электростатических разрядов.

С использованием указанной модели разработана методика моделирования зависимости РП полимерного корпуса от времени облучения, в основе которой лежит обработка экспериментальных данных с использованием метода идентификации коэффициентов аппроксимации.

Разработанные модель и методика направлены на исследование радиационного заряжения полимерных композитных корпусов при воздействии на них космической плазмы. На примере пленок ПС проведено моделирование их радиационного заряжения и показано, что в условиях спокойной геомагнитной обстановки радиационная проводимость обеспечивает отсутствие ЭСР, а в условиях геомагнитной суббури, когда плотность потока электронов возрастает на два порядка, радиационная проводимость не обеспечивает достаточный сток заряда, возникают ЭСР, и для их устранения необходимо в ПС вводить проводящий наполнитель, создающий удельную объемную темновую проводимость не ниже, чем $\gamma_D = 10^{-12}$ Ом$^{-1}$·м$^{-1}$.

Список литературы

1. **DeForest S. E.** Spacecraft charging at synchronous orbit // J. Geophys. Res. 1972. Vol. 77, N. 4. P. 651—659.

2. **Frederickson A. R.** Radiation Induced Electrical Current and Voltage in Dielectric Structures, 1974. 41 p.

3. **Frederickson A.** Electric Discharge Pulses in Irradiated Solid Dielectrics in Space // IEEE Transactions on Electrical Insulation. 1983. Vol. EI-18, N. 3. P. 337—349.

4. **Акишин А. И.** Электроразрядные сбои в космических аппаратах в зоне космических излучений // Перспективные материалы. 2010. № 2. С. 27—32.

5. **Catani J.-P., Payan D.** Electrostatic behavior of materials in a charging space environment // Proc. 9th Int. Symp. On Materials in a Space Environment. Noordwijk: ESA Publ. Division, 2003. P. 3—16.

6. **Pike C. P., Bunn M. H.** A Correlation Study Relating Spacecraft Anomalies to Environmental Data // Spacecraft Charging by Magnetospheric Plasmas. American Institute of Aeronautics and Astronautics, 1976. P. 45—60.

7. **Purvis C. K., Garrett H. B., Whittlesey A. C., Stevens N. J.** Design Guidelines for Assessing and Controlling Spacecraft Charging Effects // NASA Technical Paper 2361, National Aeronautics and Space Administration. September 1984.

8. **Saenko V., Tyutnev A., Abrameshin A., Belik G.** Computer Simulations and Experimental Verification of the Nanoconductivity Concept for the Spacecraft Electronics // 14th Spacecraft Charging Technology Conference, 04-08 April 2016, ESA-ESTEC, Noordwijk.

9. **Пожидаев Е. Д. Саенко В. С., Смирнов И. А., Бабкин Г. В., Тютнев А. П.** Повышение стойкости космических аппаратов к воздействию поражающих факторов электризации // Космонавтика и ракетостроение. 2003. № 1 (30). С. 32—35.

10. **NASA — HDBK — 4002A.** Mitigating In-Space Charging Effects-A. Guideline: NASA, 2011.

11. **Садовничий Д. Н., Тютнев А. П., Хатипов С. А., Саенко В. С., Пожидаев Е. Д.** Накопление объемных зарядов при облучении эпоксидного компаунда электронами в вакууме // Высокомолекулярные соединения. Серия А. 2003. Т. 45, № 2. С. 230—236.

12. **Boev S. O., Paderin V. A., Tyutnev A. P.** Reversal of the current in irradiated dielectrics // Journal of Electrostatics. 1995. Vol. 34. P. 27—35.

13. **Абрамешин А. Е., Азаров М. Д., Пожидаева А. Е.** Компьютерное моделирование радиационного заряжения слабопроводящих диэлектриков // Системный администратор. 2015. № 4. С. 91—95.

14. **Korkinets V., Abrameshin A. E., Pozhidaev E. D.** Model of radiation electrization of low-pressure polyethylene films with controlled conductivity // 2018 Moscow Workshop on Electronic and Networking Technologies (MWENT). Proceedings. M.: IEEE, 2018. Ch. 7. P. 1—5.

15. **Tyutnev A. P., Ikhsanov R. Sh., Saenko V. S., Pozhidaev E. D.** Theoretical Analysis of the Rose—Fowler—Vaisberg Model // Polymer Sci. Series A. 2006. Vol. 48. P. 2015—2022.

16. **Tyutnev A. P., Belik G. A., Abrameshin A. E., Saenko V. S.** Laboratory Simulation of Charging of Polymers by Beams of Low-Energy Electrons /// Inorganic Materials: Applied Research. 2013. Vol. 4, N. 2. P. 98—102.

D. A. Abrameshin, PhD Student, Principal Engineer, e-mail: dabrameshin@hse.ru,
E. D. Pozhidaev, Dr. Sc., Tech., Professor, e-mail: EPozhidaev@hse.ru,
Tumkovskiy S. R., Dr. Sc., Tech., Professor, e-mail: STumkovskiy@hse.ru,
National Research University "Higher School of Economics", Moscow, 101000, Russian Federation

Simulation of Radiation Charging of Microelectronic Equipment Cases for Space Applications

A model and a method for mathematical modeling of radiation charging of polymer microelectronic equipment housings with increased conductivity are developed, which are based on the application of the approximation function of the experimental dependence of the housing conductivity on the irradiation time obtained using parametric identification methods. The research results are aimed at developing composite polymer materials for microelectronic equipment housings with a conductivity that ensures the absence of electrostatic discharges and significantly increases the active life of spacecraft.

Keywords: *mathematical and computer modeling, radiation contamination, radiation conductivity, electrostatic discharges, spacecraft, microelectronic equipment*

DOI: 10.17587/it.27.59-64

References

1. **DeForest S. E.** Spacecraft charging at synchronous orbit, *J. Geophys. Res.,* 1972, vol. 77, no. 4, pp. 651—659.
2. **Frederickson A. R.** Radiation Induced Electrical Current and Voltage in Dielectric Structures, 1974. 41 p.
3. **Frederickson A.** Electric Discharge Pulses in Irradiated Solid Dielectrics in Space, *IEEE Transactions on Electrical Insulation*, 1983, vol. EI-18, no. 3, pp. 337—349.
4. **Akishin A. I.** Spacecraft electrical discharge failures in in the space radiation zone, *Perspektivnye Materialy*, 2010, no. 2, pp. 27—32 (in Russian).
5. **Catani J.-P., Payan D.** Electrostatic behavior of materials in a charging space environment, *Proc. 9th Int. Symp. On Materials in a Space Environment*, Noordwijk,ESA Publ. Division, 2003, pp. 3—16.
6. **Pike C. P., Bunn M. H.** A Correlation Study Relating Spacecraft Anomalies to Environmental Data, *Spacecraft Charging by Magnetospheric Plasmas*, American Institute of Aeronautics and Astronautics, 1976, pp. 45—60.
7. **Purvis C. K., Garrett H. B., Whittlesey A. C., Stevens N. J.** Design Guidelines for Assessing and Controlling Spacecraft Charging Effects, NASA Technical Paper 2361, National Aeronautics and Space Administration, September 1984.
8. **Saenko V., Tyutnev A., Abrameshin A., Belik G.** Computer Simulations and Experimental Verification of the Nanoconductivity Concept for the Spacecraft Electronics, *14th Spacecraft Charging Technology Conference*, 04—08 April 2016, ESA-ESTEC, Noordwijk.
9. **Pozhidaev E. D., Saenko V. S., Smirnov I. A., Babkin G. V., Tyutnev A. P.** Improving the stability of the spacecraft to the impact of factors affecting the electrification, *Kosmonavtika i Raketostroenie*, 2003, no. 1 (30), pp. 32—35 (in Russian).
10. **NASA — HDBK — 4002A.** Mitigating In-Space Charging Effects-A, Guideline, NASA, 2011.
11. **Sadovnichij D. N., Tyutnev A. P., Khatipov S. A., Saenko V. S., Pozhidaev E. D.** Accumulation of bulk charges during irradiation of epoxy compound with electrons in vacuum, *Vysokomolekulyarnye soedineniya. Seriya A*, 2003, vol. 45, no. 2, pp. 230—236 (in Russian).
12. **Boev S. O., Paderin V. A., Tyutnev A. P.** Reversal of the current in irradiated dielectrics, *Journal of Electrostatics*, 1995, vol. 34, pp. 27—35.
13. **Abrameshin A. E., Azarov M. D.** Computer simulation of radiation charging of low-conducting dielectrics, *Sistemnii Administrator*, 2015, no. 4, pp. 91—95 (in Russian).
14. **Korkinets V., Abrameshin A. E., Pozhidaev E. D.** Model of radiation electrization of low-pressure polyethylene films with controlled conductivity, *2018 Moscow Workshop on Electronic and Networking Technologies (MWENT). Proceedings*, Moscow, IEEE, 2018, Ch. 7, pp. 1—5.
15. **Tyutnev A. P., Ikhsanov R. Sh., Saenko V. S., Pozhidaev E. D.** Theoretical Analysis of the Rose—Fowler—Vaisberg Model, Polymer Sci. Series A, 2006. Vol. 48. P. 2015—2022.
16. **Tyutnev A. P., Belik G. A., Abrameshin A. E., Saenko V. S.** Laboratory Simulation of Charging of Polymers by Beams of Low-Energy Electrons, *Inorganic Materials: Applied Research*, 2013, vol. 4, no. 2, pp. 98—102.

УДК 519.873

DOI: 10.17587/it.27.64-71

С. М. Сидоров, ст. преп., e-mail: xaevec@mail.ru,
Севастопольский государственный университет, г. Севастополь

Скрытая марковская модель двухкомпонентной системы с групповым мгновенно пополняемым резервом времени[1]

Обсуждается решение задачи оценки согласованности модели с полученными данными (сигналами), уточнения модели и ее параметров на основе теории скрытых марковских моделей. На основе полумарковской модели с общим фазовым пространством состояний двухкомпонентной системы с групповым мгновенно пополняемым резервом времени построена скрытая марковская модель двухкомпонентной системы с групповым мгновенно пополняемым резервом времени. Чтобы перейти от полумарковской модели системы к ее скрытой марковской модели, предлагается сначала укрупнить полумарковскую модель, используя алгоритм стационарного фазового укрупнения. Построенная модель используется для оценки характеристик и прогнозирования состояний рассматриваемой системы на основе полученного вектора сигналов. Показано влияние резерва времени на вероятность появления полученного вектора сигналов.

Ключевые слова: *полумарковская модель, резерв времени, скрытая марковская модель, алгоритм фазового укрупнения, вектор сигналов, оценка характеристик, прогнозирование состояний*

Введение

Для моделирования систем различного назначения широко используются полумарковские процессы [1—4, 7, 12]. Временное резервирование [5—7, 11] представляет собой один из методов повышения надежности и эффективности систем. В монографии [13] указывается, что временное резервирование является недостаточно изученным. Важной составной частью полумарковского процесса является вло-

[1]Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований № 18-01-00392а.

женная цепь Маркова (ВЦМ), которая отвечает за переходы между состояниями системы. Фазовое пространство состояний ВЦМ совпадает с фазовым пространством состояний полумарковского процесса. Однако во время функционирования систем, для которых построена полумарковская модель, не всегда удается при изменениях ее состояний полностью получить информацию, содержащуюся в кодировке состояний, а есть только возможность получить некоторый сигнал (информацию), связанный с состояниями ВЦМ (полумарковского процесса). Например, в фазовом состоянии полумарковского процесса для каждого элемента системы указано, находится ли он в рабочем состоянии или на восстановлении, а при использовании системы можно получить сигнал только о числе работоспособных элементов. При использовании систем бывает сложно или невозможно получить значения дополнительных непрерывных компонент. В этих случаях состояния ВЦМ можно считать скрытыми (ненаблюдаемыми). Следовательно, необходимо оценить, насколько построенная модель согласуется с полученными результатами функционирования системы, уточнить модель и параметры модели на основе полученного вектора сигналов. Одним из подходов к решению этих задач является использование теории скрытых марковских моделей [8—11].

В данной работе рассматривается методика построения скрытой марковской модели (СММ) на примере полумарковской модели с общим фазовым пространством состояний системы с групповым мгновенно пополняемым резервом времени, приведенной в работе [7]. Сначала строится укрупненная полумарковская модель этой системы (для случая $N = 2$), используя алгоритм стационарного фазового укрупнения [1, 2]. На основе укрупненной модели строится СММ двухкомпонентной системы с групповым мгновенно пополняемым резервом времени. Построенная СММ используется для оценки характеристик и прогнозирования состояний укрупненной модели на основе полученного вектора сигналов.

1. Построение укрупненной полумарковской модели

Опишем, следуя работе [7], полумарковскую модель системы с групповым мгновенно пополняемым резервом времени. Рассмотрим систему S (случай $N = 2$), состоящую из элементов K_i, времена безотказной работы которых — случайные величины (СВ) α_i с функциями распределения (ФР) $F_i(t)$, а времена восстановления элементов — СВ β_i с ФР $G_i(t)$, $i = 1, 2$. СВ α_i, β_i, предполагаются независимыми в совокупности, имеющими конечные математические ожидания; ФР $F_i(t)$ и $G_i(t)$ предполагаются имеющими конечные плотности $f_i(t)$ и $g_i(t)$. Система становится неисправной, если отказали $p = 2 = N$ элементов системы (параллельное соединение). Отказ системы S наступает тогда, когда неисправность длится время, большее чем $h > 0$ (h — групповой мгновенно пополняемый резерв времени), и продолжается до восстановления одного из отказавших элементов; при этом резерв времени становится равным h.

Для построения полумарковской модели системы S в монографии [7] используется полумарковский процесс $\xi(t)$ с дискретно-непрерывным фазовым пространством состояний E [1, 2, 4, 7]:

$$E = \{1110x_2,\ 211x_10,\ 1010x_2,\ 201x_10,\ 1100x_2,$$
$$210x_10,\ 1000x_2,\ 200x_10,\ 1\overline{0}\overline{0}0x_2,\ 2\overline{0}\overline{0}x_10\},$$

где x_k указывает время до очередного отказа или восстановления элемента с номером k.

Рассмотрим содержательный смысл кодов состояний:

- $1110x_2$ — элемент K_1 восстановился, K_2 продолжает работу, $x_2 > 0$ — время до отказа элемента K_2;
- $211x_10$ — элемент K_2 восстановился, K_1 продолжает работу, $x_1 > 0$ — время до отказа элемента K_1;
- $1010x_2$ — элемент K_1 отказал, K_2 продолжает работу, $x_2 > 0$ — время до отказа элемента K_2;
- $201x_10$ — элемент K_2 восстановился и начал работать, K_1 продолжает восстановление, $x_1 > 0$ — время до восстановления элемента K_1;
- $1100x_2$ — элемент K_1 восстановился и начал работать, K_2 продолжает восстановление, $x_2 > 0$ — время до восстановления элемента K_2;
- $210x_10$ — элемент K_2 отказал, K_1 продолжает работу, $x_1 > 0$ — время до отказа элемента K_1;
- $1000x_2$ — элемент K_1 отказал, K_2 восстанавливается, система функционирует за счет резерва времени, $x_2 > 0$ — время до восстановления элемента K_2;
- $200x_10$ — элемент K_2 отказал, K_1 восстанавливается, система функционирует за счет резерва времени, $x_1 > 0$ — время до восстановления элемента K_1;
- $1\overline{0}\overline{0}0x_2$ — время восстановления элементов K_1 и K_2 превысило значение резерва време-

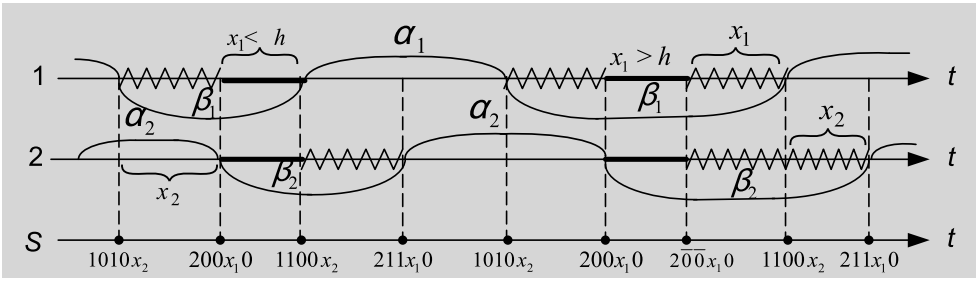


Рис. 1. Временная диаграмма функционирования системы

ни h, система в отказе, $x_2 > 0$ — время до восстановления элемента K_2;

- $2\overline{00}x_10$ — время восстановления элементов K_1 и K_2 превысило значение резерва времени h, система в отказе, $x_1 > 0$ — время до восстановления элемента K_1.

Временная диаграмма функционирования системы S изображена на рис. 1. На временной диаграмме ломаной линией показан отказ элементов, а жирной линией — функционирование элементов системы за счет резерва времени.

В монографии [7] показано, что стационарное распределение ВЦМ полумарковского процесса $\xi(t)$ имеет следующий вид:

$$\begin{aligned}
\rho(1110x_2) &= \rho(1010x_2) = \rho_0\bar{F}_2(x_2),\\
\rho(211x_10) &= \rho(210x_10) = \rho_0\bar{F}_1(x_1),\\
\rho(1100x_2) &= \rho(1000x_2) = \rho_0\bar{G}_2(x_2),\\
\rho(201x_10) &= \rho(200x_10) = \rho_0\bar{G}_1(x_1),\\
\rho(1\overline{00}0x_2) &= \rho_0\bar{G}_1(h)\bar{G}_2(x_2),\\
\rho(2\overline{00}x_10) &= \rho_0\bar{G}_2(h)\bar{G}_1(x_1),
\end{aligned} \qquad (1)$$

где постоянная ρ_0 находится из условия нормировки. Здесь и далее $\bar{F}(x) = 1 - F(x)$.

В целях упрощения модели системы S построим укрупненную полумарковскую модель системы, используя алгоритм стационарного фазового укрупнения, предложенный в работах [1, 2]. Для построения укрупненной полумарковской модели необходимо [2]: определить укрупненное фазовое пространство состояний $\widehat{E}$ в соответствии с исходным; вычислить вероятности перехода между состояниями, входящими в $\widehat{E}$, и средние времена пребывания в этих состояниях.

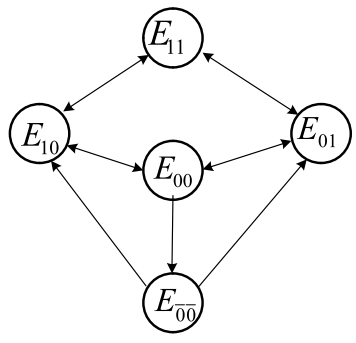


Рис. 2. Граф переходов укрупненной системы

Отметим, что укрупненная полумарковская модель приближенно описывает поведение исходной системы в установившемся режиме. Для систем с быстрым восстановлением (время безотказной работы значительно (в 10 и более раз) больше времени восстановления элементов) потеря точности составляет менее 2...3 %.

Разобьем фазовое пространство состояний E исходной модели на $N = 5$ классов:

$$\begin{aligned}
E_{11} &= \{1110x_2, 211x_10\},\\
E_{10} &= \{1100x_2, 210x_10\},\ E_{01} = \{1010x_2, 201x_10\},\\
E_{00} &= \{1000x_2, 200x_10\},\ E_{\overline{00}} = \{1\overline{00}0x_2, 2\overline{00}x_10\},
\end{aligned} \qquad (2)$$

каждый из которых "склеивается" в одно состояние укрупненной модели. Фазовое пространство состояний $\widehat{E}$ укрупненной модели имеет вид

$$\widehat{E} = \{11, 10, 01, 00, \overline{00}\}. \qquad (4)$$

Физический смысл состояний укрупненной модели следующий:

- 11 — оба элемента функционируют;
- 01 — элемент K_1 восстанавливается, K_2 функционирует;
- 10 — элемент K_1 функционирует, K_2 восстанавливается;
- 00 — оба элемента восстанавливаются;
- $\overline{00}$ — отказ системы.

Граф переходов укрупненной системы представлен на рис. 2.

Отметим, что фазовое пространство полумарковских состояний получается добавлением к кодам физических состояний совокупности непрерывных компонент, фиксирующих остаточные времена действия факторов, изменяющих состояния системы. Эти непрерывные компоненты и желательно укрупнять, оставляя только дискретное множество физических состояний. Разбивать фазовое пространство состояний E исходной модели на классы можно

различными способами, используя основную идею: в классы объединяются однотипные состояния по определенному признаку, общему для них всех.

Определим вероятности перехода $\hat{p}_k^r$ ВЦМ и средние времена пребывания в состояниях $\hat{m}_k$ укрупненной модели, которые согласно работам [1, 2] находятся по формулам

$$\hat{p}_k^r = \int\limits_{E_к} \rho(de)P(e, E_r)/\rho(E_к),\ k, r = \overline{1, N};$$
$$\hat{m}_k = M\hat{\theta}_k = \int\limits_{E_к} \rho(de)m(e)/\rho(E_к),\ k = \overline{1, N}, \quad (5)$$

где $\rho(d_e)$ — стационарное распределение ВЦМ, определяемое формулами (1); $m(e)$ — средние времена пребывания в состояниях исходной модели; $P(e, E_r)$ — вероятности перехода ВЦМ.

Используя формулы (5), (1) и полумарковскую модель системы S, приведенную в работе [7], найдем вероятности перехода ВЦМ укрупненной модели, которые будут использованы при построении скрытой марковской модели:

$$\hat{p}_{11}^{10} = \frac{M\alpha_1}{M\alpha_1 + M\alpha_2},\ \hat{p}_{11}^{01} = \frac{M\alpha_2}{M\alpha_1 + M\alpha_2},$$
$$\hat{p}_{10}^{11} = \frac{M\alpha_1}{M\alpha_1 + M\beta_2},\ \hat{p}_{10}^{00} = \frac{M\beta_2}{M\alpha_1 + M\beta_2},$$
$$\hat{p}_{01}^{11} = \frac{M\alpha_2}{M\alpha_2 + M\beta_1},\ \hat{p}_{01}^{00} = \frac{M\beta_1}{M\alpha_2 + M\beta_1},$$
$$\hat{p}_{\overline{00}}^{10} = \frac{\int\limits_0^\infty \bar{G}_2(y)dy\int\limits_0^y g_1(h+t)dt + \int\limits_0^\infty \bar{G}_1(y)dy\int\limits_y^\infty g_2(h+t)dt}{\bar{G}_1(h)M\beta_2 + \bar{G}_2(h)M\beta_1},$$
$$\hat{p}_{\overline{00}}^{01} = \frac{\int\limits_0^\infty \bar{G}_2(y)dy\int\limits_y^\infty g_1(h+t)dt + \int\limits_0^\infty \bar{G}_1(y)dy\int\limits_0^y g_2(h+t)dt}{\bar{G}_1(h)M\beta_2 + \bar{G}_2(h)M\beta_1}, \quad (6)$$
$$\hat{p}_{00}^{\overline{00}} = \frac{\bar{G}_1(h)\int\limits_h^\infty \bar{G}_2(t)dt + \bar{G}_2(h)\int\limits_h^\infty \bar{G}_1(t)dt}{M\beta_1 + M\beta_2},$$
$$\hat{p}_{00}^{01} = \frac{\bar{G}_1(h)\int\limits_0^h \bar{G}_2(t)dt + G_2(h)\int\limits_0^\infty \bar{G}_1(t)dt}{M\beta_1 + M\beta_2},$$
$$\hat{p}_{00}^{10} = \frac{G_1(h)\int\limits_0^\infty \bar{G}_2(t)dt + \bar{G}_2(h)\int\limits_0^h \bar{G}_1(t)dt}{M\beta_1 + M\beta_2},$$

остальные $\hat{p}_k^r = 0$.

Используя формулы (5), (1) и полумарковскую модель системы S, приведенную в работе [7], найдем средние времена пребывания в состояниях укрупненной модели:

$$\hat{m}_{11} = \frac{M\alpha_1 M\alpha_2}{M\alpha_1 + M\alpha_2},\ \hat{m}_{10} = \frac{M\alpha_1 M\beta_2}{M\alpha_1 + M\beta_2},$$
$$\hat{m}_{01} = \frac{M\alpha_2 M\beta_1}{M\alpha_2 + M\beta_1},\ \hat{m}_{00} = \frac{M\beta_1 M\beta_2}{M\beta_1 + M\beta_2},$$
$$\hat{m}_{00} = \frac{\bar{G}_2(h)M\beta_1\bar{G}_1(h)M\beta_2}{\bar{G}_2(h)M\beta_1 + \bar{G}_1(h)M\beta_2}.$$

Зная $\hat{E}, \hat{p}_k^r, \hat{m}$, можно построить укрупненную модель. Отметим, что укрупненная модель также является полумарковской. Средние времена пребывания в состояниях укрупненной модели не будут учитываться в дальнейшем для построения СММ.

2. Скрытая марковская модель на основе укрупненной полумарковской модели

Для полного описания СММ [9, 10] необходимо определить:

1. Множество состояний модели.

В нашем случае множество состояний модели соответствует множеству (4) состояний укрупненной модели.

2. Алфавит наблюдаемой последовательности (множество сигналов).

Предположим, что при функционировании системы S состояния ВЦМ укрупненной модели не наблюдаются (скрытые состояния), а наблюдаются только число работоспособных элементов во время смены состояний ВЦМ. Введем следующее множество сигналов:

$$J = \{0, 1, 2\}, \quad (7)$$

где

- 0 — оба элемента восстанавливаются;
- 1 — работоспособен один элемент;
- 2 — оба элемента работоспособны.

Множество сигналов можно выбирать поразному. Множество сигналов J (7) выбрано в таком виде, так как "точную" информацию о числе работоспособных элементов можно получить практически для любой системы. Оно соответствует физическому описанию состояний модели с учетом числа работоспособных элементов системы.

3. Матрицу переходных вероятностей между состояниями системы.

Пусть $\{X_n, n = 1, 2, ...\}$ — ВЦМ укрупненной модели, вероятности переходов которой опре-

деляются формулами (6). Для нашей модели матрица переходных вероятностей состоит из переходных вероятностей (6) укрупненной полумарковской модели.

4. Связь состояний модели с сигналами.

Рассмотрим связь между состояниями ВЦМ укрупненной модели и сигналами (7), т.е. определим функцию связи $R(s \mid \boldsymbol{x})$ [8, 9]:

$$R(s \mid \boldsymbol{x}) = P(S_n = s \mid X_n = \boldsymbol{x}),$$
$$\boldsymbol{x} \in E,\ s \in J,\ \sum_{s \in J} R(s \mid \boldsymbol{x}) = 1, \tag{8}$$

где S_n — n-й сигнал.

Функция $R(s \mid \boldsymbol{x})$ связи состояний ВЦМ укрупненной модели с сигналами представлена в табл. 1.

Таблица 1

Функция связи $R(s \mid x)$ состояний ВЦМ укрупненной модели с сигналами

Состояние $\boldsymbol{x}$	Сигнал s		
	$s = 0$	$s = 1$	$s = 2$
11	0	0	1
10	0	1	0
01	0	1	0
00	1	0	0
$\overline{00}$	1	0	0

5. Начальное распределение вероятностей модели.

Будем считать, что в начальный момент времени укрупненная модель находится в состоянии 11. Следовательно, СММ в начальный момент времени с вероятностью 1 находится в состоянии 11, с нулевой вероятностью — в остальных состояниях.

СММ на основе укрупненной полумарковской модели построена.

3. Анализ характеристик и прогнозирование состояний укрупненной полумарковской модели

Следуя работам [8, 9], перейдем к анализу характеристик укрупненной полумарковской модели, используя построенную СММ.

Пусть $\overline{S}^n = (S_1, S_2, \ldots, S_n)$ — случайный вектор первых n сигналов. Для полученного вектора сигналов $\overline{s}_n = (s_1, s_2, \ldots, s_n)$ пусть $\overline{s}_k = (s_1, s_2, \ldots, s_k)$, $k \leqslant n$. Требуется оценить характеристики ВЦМ укрупненной (скрытой) модели на основе полученного вектора сигналов $\overline{s}_n$. Предполагается, что в начальный момент времени модель находится в состоянии 11.

Введем функции $F_k(i)$ (прямые переменные) [8, 9]:

$$F_k(i) = P(\overline{S}^k = \overline{s}_k, X_k = i),\ k = 1, 2, \ldots, n. \tag{9}$$

Для этих функций справедлива следующая рекуррентная формула [8, 9]:

$$F_k(i) = R(s_k \mid i) \sum_j F_{k-1}(j) P_j^i;$$
$$F_1(i) = R(s_1 \mid i) p_i, \tag{10}$$

где P_j^i — вероятности перехода ВЦМ укрупненной модели, определенные формулами (6); (p_i) — распределение начального состояния ВЦМ.

Рассмотрим также функции $B_k(i)$ (обратные переменные) [8, 9]:

$$B_k(i) = P(S_{k=1} = s_{k=1}, \ldots, S_n = s_n \mid X_k = i),$$
$$k = \overline{1, n-1},$$

для которых справедлива рекуррентная формула [8, 9]:

$$B_k(i) = \sum_j R(s_{k+1} \mid j) B_{k+1}(j) P_i^j,$$
$$B_{n-1}(i) = \sum_j P_i^j R(s_n \mid j).$$

Функции $F_k(i)$, $B_k(i)$ играют важную роль при использовании скрытых марковских моделей для анализа функционирования систем.

Перейдем к анализу динамики укрупненной полумарковской модели на основе построенной СММ.

В качестве примера рассмотрим систему S, для которой перед началом ее функционирования принято, что СВ α_1, α_2, β_1, β_2 имеют распределение Эрланга IV порядка и $M\alpha_1 = 28{,}57$ ч, $M\alpha_2 = 25$ ч, $M\beta_1 = 2$ ч, $M\beta_2 = 1{,}6$ ч. Групповой мгновенно пополняемый резерв времени $h = 1{,}5$ ч.

Предположим, что в результате функционирования системы S получен следующий вектор сигналов:

$$\overline{s}_7 = (2, 1, 0, 1, 2, 1, 0),\ n = 7.$$

4. Задачи по оценке характеристик скрытой марковской модели

Рассмотрим задачи по оценке характеристик СММ с учетом введенных параметров.

1. Определим вероятности состояний скрытой модели в момент испускания седьмого сигнала. Воспользуемся формулой [8, 9]

$$P(X_n = i \mid \overline{S}^n = \overline{s}_n) = \frac{F_n(i)}{\sum\limits_j F_n(j)}. \qquad (11)$$

В результате получаем, что на седьмом шаге укрупненная модель с вероятностью 1 находилась в состоянии 00. Для состояний 11, 10, 01, $\overline{00}$ эта вероятность равна нулю.

2. Найдем вероятности, с которыми скрытая модель осуществит переход в состояния на следующем восьмом шаге. Для этого используем формулу [8, 9]

$$P(X_{n+1} = j \mid \overline{s}_n) = \sum_i P(X_n = i \mid \overline{s}_n) P_i^j, \qquad (12)$$

Получаем следующие вероятности перехода скрытой модели на восьмом шаге: в состояние 10 — с вероятностью 0,3369, 01 — 0,5100, $\overline{00}$ — 0,1531; во все остальные — с нулевой вероятностью.

3. Определим вероятности появления сигналов на следующем восьмом шаге, применив формулу [4, 5]

$$P(S_{n+1} = s_{n+1} \mid \overline{s}_n) = \\ = \sum_i P(X_{n+1} = i \mid \overline{s}_n) R(s_{n+1} \mid i), \qquad (13)$$

при этом используется формула (12).

Получаем следующие вероятности появления сигналов на восьмом шаге: сигнал 1 с вероятностью 0,8469, 0 — 0,1531, 2 — 0.

4. Найдем вероятность появления (испускания) полученного вектора сигналов $\overline{s}_7$.

Для этого можно использовать формулы [8, 9]

$$P(\overline{S}^n = \overline{s}_n) = \sum_i F_n(i) = \sum_i R(s_1 \mid i) B_1(i) p_i, \qquad (14)$$

а также

$$P(\overline{S}^n = \overline{s}_n) = \sum_i F_k(i) B_k(i), \qquad (15)$$

при любом фиксированном k.

Таким образом, вероятность появления полученного вектора сигналов $\overline{s}_7$, вычисленная по формулам (14), (15), равна 0,0031.

5. Прогнозирование состояний скрытой модели по полученному вектору сигналов.

Таблица 2

Наиболее вероятные состояния скрытой модели на переходах

Номер перехода	1	2	3	4	5	6	7
Наиболее вероятное состояние	11	01	00	01	11	01	00
Вероятность состояния	1,000	0,550	1,000	0,597	1,000	0,550	1,000

Таблица 3

Вероятность появления $\overline{s}_7$ при различных значениях резерва времени

Вероятность	Резерв времени h, ч			
	1,5	1,1	0,7	0,3
$P(\overline{S}^n = \overline{s}_n)$	0,0031	0,0025	0,0016	0,0006

На основании полученного вектора сигналов $\overline{s}_7$ необходимо найти наиболее вероятные состояния скрытой модели на переходах. Для решения этой задачи используется формула [8, 9]

$$P(X_k = i \mid \overline{S}^k = \overline{s}_k) = \frac{F_k(i) B_k(i)}{\sum\limits_j F_k(j) B_k(j)}. \qquad (16)$$

Таким образом, необходимо найти i, которое максимизирует выражение $F_k(i)B_k(i)$.

В табл. 2 указаны наиболее вероятные состояния скрытой модели на указанных в ней переходах и вероятности этих состояний.

Покажем влияние значения группового мгновенно пополняемого резерва времени на вероятность появления полученного вектора сигналов $\overline{s}_7 = (2,1,0,1,2,1,0)$. Результаты представлены в табл. 3.

Из табл. 3 видно, что при уменьшении резерва времени вероятность появления вектора сигналов $\overline{s}_7$ уменьшается. Это объясняется тем, что при уменьшении резерва времени увеличивается вероятность отказа системы, а поскольку полученный вектор сигналов не содержит отказа (двух последовательных нулей), то, следовательно, вероятность такой цепочки уменьшается.

Используя алгоритм Баума—Велша [8, 9], можно уточнить начальные параметры модели, чтоб они наиболее точно согласовывались с полученным вектором сигналов.

Применяя этот алгоритм, получаем уточненную матрицу переходных вероятностей для рассматриваемой системы:

$$P_i^j = \begin{pmatrix} 0 & 0,5333 & 0,4667 & 0 & 0 \\ 0,9470 & 0 & 0 & 0,0530 & 0 \\ 0,9260 & 0 & 0 & 0,0740 & 0 \\ 0 & 0,3369 & 0,5100 & 0 & 0,1531 \\ 0 & 0,4221 & 0,5779 & 0 & 0 \end{pmatrix} —$$

исходная матрица переходных вероятностей P_i^j;

$$\overline{P}_i^j = \begin{pmatrix} 0 & 0,4500 & 0,5500 & 0 & 0 \\ 0,3094 & 0 & 0 & 0,6906 & 0 \\ 0,3517 & 0 & 0 & 0,6483 & 0 \\ 0 & 0,4032 & 0,5968 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} —$$

уточненная матрица переходных вероятностей $\overline{P}_i^j$.

Применяя алгоритм Витерби [8, 9] к уточненной модели, определяем наиболее вероятную цепочку состояний для полученного вектора сигналов: 11, 10, 00, 01, 11, 10, 00.

Заключение

На основе укрупненной полумарковской модели двухкомпонентной системы с групповым мгновенно пополняемым резервом времени построена СММ двухкомпонентной системы с групповым мгновенно пополняемым резервом времени. Полученная СММ используется для оценки характеристик рассматриваемой системы и прогнозирования ее состояний на основе полученного вектора сигналов. Проведен анализ влияния значения группового мгновенно пополняемого резерва времени на вероятность испускания полученного вектора сигналов.

В дальнейшем предполагается использование рассмотренного в работе подхода к анализу функционирования многокомпонентных систем с различными стратегиями использования и видами резерва времени.

Список литературы

1. **Королюк В. С., Турбин А. Ф.** Процессы марковского восстановления в задачах надежности систем. Киев: Наук. Думка, 1982, 236 с.
2. **Korolyuk V. S., Korolyuk V. V.** Stochastic Models of Systems. Dordrecht: Springer Science + Business Media, 1999, 185 p.
3. **Grabski F.** Semi-Markov Processes: Applications in System Reliability and Maintenance. Amsterdam: Elsevier Science, 2014, 270 p.
4. **Obzherin Yu. E., Boyko E. G.** Semi-Markov Models: Control of Restorable Systems with Latent Failures. London: Elsevier Academic Press, 2015, 214 p.
5. **Черкесов Г. Н.** Надежность технических систем с временной избыточностью. Москва: Сов. Радио, 1974, 296 с.
6. **Креденцер Б. П.** Прогнозирование надежности систем с временной избыточностью. Киев: Наук. Думка, 1978, 240 с.
7. **Копп В. Я., Обжерин Ю. Е., Песчанский А. И.** Стохастические модели автоматизированных производственных систем с временным резервированием. Севастополь: Изд-во СевГТУ, 2000, 284 с.
8. **Ross S. M.** Introduction to Probability Models, 9th ed. Elsevier Academic Press, USA, 2006. 800 p.
9. **Rabiner L. R.** A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition // PROC. IEEE. 1989. Vol. 77, N. 2. P. 257—286.
10. **Kobayashi H., Mark B., Turin W.** Probability, Random Processes, and Statistical Analysis: Applications to Communications, Signal Processing, Queueing Theory and Mathematical Finance. Cambridge: Cambridge University Press, 2011. 812 p.
11. **Obzherin Y. E., Sidorov S. M., Nikitin M. M.** Hidden Markov Model of Information System with Component-Wise Storage Devices // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11965 LNCS (2019). P. 354—364.
12. **Obzherin Y. E., Sidorov S. M.** Semi-markov model and phase-merging scheme of a multi-component system with the group instantly replenished time reserve // International Journal of Reliability, Quality and Safety Engineering. 2019. Vol. 26, N. 3. Art, no. 1950014.
13. **Ushakov I. A.** Probabilistic Reliability Models. San Diego, California: Wiley-Blackwell, 2012. 248 p.

S. M. Sidorov, Senior Lecturer, e-mail: xaevec@mail.ru,
Sevastopol State University, Higher Mathematics Department, Sevastopol, 299053, Russian Federation

Hidden Markov Model of Two-Component System with Group Instantly Replenished Time Reserve

Most systems allow the construction of a semi-Markov model. However, during the operation of the system, full information contained in the state encoding is not always available, but it is possible to obtain some signal (information). Tasks arise to assess the consistency of the model with the received data (signals), to refine the model and its parameters. Such parameters can be characteristics of random values characterizing system operation, time reserve value, etc. The theory of hidden Markov models allows solving these problems. In order to move from a semi-Markov model of the system to its hidden Markov model, it is proposed to first the semi-Markov model merge using a stationary phase merging algorithm. In this paper, on the basis of the semi-Markov model with a common phase state space of a two-component system with a group instantly replenished time

reserve, we construct a hidden Markov model of a two-component system with a group instantly replenished time reserve. It is used to evaluate the characteristics and predict the states of the system in question based on the received vector of signals. The influence of the time reserve value on the probability of occurrence of the obtained vector of signals is shown.

Keywords: *semi-Markov model, time reserve, hidden Markov model, phase merging algorithm, vector of signals, characteristic estimation, state prediction*

DOI: 10.17587/it.27.64-71

References

1. **Korolyuk V. S., Turbin A. F.** Markovian restoration processes in the problems of system reliability, Kiev, Nauk. Dumka, 1982, 236 p. (in Russian).

2. **Korolyuk V. S., Korolyuk V. V.** Stochastic Models of Systems, Dordrecht, Springer Science + Business Media, 1999, 185 p.

3. **Grabski F.** Semi-Markov Processes: Applications in System Reliability and Maintenance, Amsterdam, Elsevier Science, 2014, 270 p.

4. **Obzherin Yu. E., Boyko E. G.** Semi-Markov Models: Control of Restorable Systems with Latent Failures, London, Elsevier Academic Press, 2015, 214 p.

5. **Cherkesov G. N.** Reliability of technical systems with time redundancy, Moscow, Sovietskoe Radio, 1974, 296 p. (in Russian).

6. **Kredentser B. P.** Prediction of reliability of systems with time redundancy, Kiev, Nauk. Dumka, 1978, 240 p. (in Russian).

7. **Kopp V. Y., Obzherin Yu. E., Peschanskiy A. I.** Stochastic models of automized system with time reservation, Sevastopol, Publishing house of SevGTU, 2000, 284 p. (in Russian).

8. **Ross S. M.** Introduction to Probability Models, 9th ed., Elsevier Academic Press, USA, 2006, 800 p.

9. **Rabiner L. R.** A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition, *PROC. IEEE*, 1989, vol. 77, no. 2, pp. 257—286.

10. **Kobayashi H., Mark B., Turin W.** Probability, Random Processes, and Statistical Analysis: Applications to Communications, Signal Processing, Queueing Theory and Mathematical Finance, Cambridge, Cambridge University Press, 2011, 812 p.

11. **Obzherin Y. E., Sidorov S. M., Nikitin M. M.** Hidden Markov model of information system with component-wise storage devices, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019, vol. 11965, pp. 354—364.

12. **Obzherin Y. E., Sidorov S. M.** Semi-Markov model and phase-merging scheme of a multi-component system with the group instantly replenished time reserve, *International Journal of Reliability, Quality and Safety Engineering*, 2019, vol. 26, no. 3, art. no. 1950014.

13. **Ushakov I. A.** Probabilistic Reliability Models, San Diego, California, Wiley-Blackwell, 2012, 248 p.

УДК 004.021 DOI: 10.17587/it.27.72-77

М. Е. Сухопаров, канд. техн. наук, ст. науч. сотр., e-mail: mikhailsukhoparov@yandex.ru,
НПК "ТРИСТАН",
И. С. Лебедев, д-р техн. наук, гл. науч. сотр., e-mail: lebedev@iias.spb.su,
К. И. Салахутдинова, мл. науч. сотр., e-mail: kainagr@mail.ru,
Санкт-Петербургский институт информатики и автоматизации РАН

Метод идентификации состояния информационной безопасности устройств интернета вещей

Описан подход к анализу состояния информационной безопасности устройств промышленного интернета и интернета вещей за счет применения внешних контролирующих систем, использующих побочные каналы и позволяющих уйти от потребления вычислительных ресурсов функционирующих устройств. Предлагаемое решение позволяет в оперативном режиме отслеживать состояние устройства с минимальными затратами на использование вычислительных ресурсов в ходе эксплуатации.

Ключевые слова: *интернет вещей, киберфизические системы, идентификация состояния, информационная безопасность, побочные каналы*

Введение

Современная парадигма интернета вещей (Internet of Things, IoT) определяет концепцию развития общедоступных сетей информационных, телекоммуникационных и киберфизических систем. Происходит стремительный рост числа устройств, датчиков, сенсоров, подключаемых к сетевой инфраструктуре. Используемые подходы и методы интернета вещей связаны с интеллектуализацией процессов функционирования, передачи информации, сбора и обработки разнородных данных. Это достигается благодаря развитию технологий идентификации и мягкой настройки устройств и узлов, передачи, обработки данных, которые обеспечивают увеличение скорости, устранение избыточности передаваемых сообщений. Используемые в IoT оконечные устройства и датчики, в основном, не обладают большими вычислительными мощностями, поэтому эффект быстродействия обеспечивается упрощением ряда технологических процессов, в том числе обеспечивающих информационную безопасность узлов и элементов интернета вещей.

В связи с этим возникает определенное противоречие, поскольку, с одной стороны, возникает потребность в реализации высокоэффективного встраиваемого программного обеспечения, реализующего методы искусственного интеллекта, машинного обучения, обработки разнородных данных, а с другой, имеются условия ограничений вычислительных ресурсов и необходимость реализации процессов обеспечения информационной безопасности критически важных узлов инфраструктуры.

Существующие подходы

Унифицированные решения интернета вещей можно найти как в обычных бытовых приборах, так и в промышленных системах управления и мониторинга сетей промышленных объектов, производств, государственных учреждений [1].

Доступность, относительно небольшая стоимость, широкое применение встраиваемых элементов устройств делает возможным использование различных методов реверс-инжиниринга в целях модификации программной и аппаратной частей, встраивания "функционала", необходимого для реализации различных деструктивных воздействий, что может приводить к утечкам конфиденциальной информации, к катастрофическим системным сбоям [2—5]. Имеется достаточное число примеров, когда для осуществления распределенных атак

типа "отказ в обслуживании" (DDoS), организации ботнетов использовались обычные роутеры, веб-камеры и принтеры [5—7]. Произошедшие инциденты определили значительный интерес к разработке и реализации решений по обеспечению безопасности встроенных устройств интернета вещей, среди которых можно выделить несколько направлений.

Один из основных подходов связан с мониторингом состояния информационной безопасности устройств, узлов и сегментов информационно-телекоммуникационных сетей на основе статистических параметров функционирования. Обнаружение атаки во время выполнения рассматривается как задача обнаружения аномального состояния, для чего применяется хорошо зарекомендовавший себя научно-методический аппарат марковских моделей, нейронных сетей, опорных векторов [8, 10].

Однако анализ состояния на основе статистической информации доступной в процессе функционирования, ориентирован на внешние признаки и не позволяет обнаружить аномальные ситуации, возникающие на программном уровне, например, переполнение буфера [7]. Для этого используются решения, связанные с реализацией мониторов, отслеживающих информацию о выполнении сегментов кода [7, 10]. Применение таких средств может негативно влиять на производительность устройств, распределение вычислительных ресурсов и стоимость. При осуществлении атаки злоумышленник пытается в первую очередь отключить систему защиты.

Вместе с тем, существуют побочные каналы, которые могут использоваться как для атаки на устройство, так и для построения систем мониторинга информационной безопасности [9]. Подобные подходы используют временные ряды, полученные от регистрирующих устройств, фиксирующих в процессе функционирования электромагнитное излучение, изменения потребляемой мощности, напряжения, загрузки вычислительных ресурсов и т.д. для мониторинга аномальных состояний [11].

Таким образом, дальнейшее развитие методов анализа состояния информационной безопасности предполагает использование большого спектра различных информационных каналов.

Предлагаемый подход

В целях идентификации состояния информационной безопасности возникает необходимость анализа ряда процессов по временным рядам, регистрируемым различными датчиками. Современные устройства промышленного интернета и интернета вещей имеют ограниченный функционал и вычислительные ресурсы, производительность которых обеспечивает выполнение возложенных на них функциональных задач. Внедрение мониторов состояния и дополнительных защитных функций не всегда возможно. Поэтому одним из направлений решения поставленных проблемных вопросов является применение внешних контролирующих систем, использующих сторонние (побочные) каналы, не потребляющих вычислительные ресурсы функционирующих устройств.

В процессе функционирования сети происходит множество процессов, связанных с приемом, передачей, обработкой сообщений, реализацией вычислительных и других алгоритмов. Это вызывает одновременную смену множества параметров. Путем регистрации их значений и синхронизации по времени полученных значений от различных мониторов, датчиков и сенсоров можно определить временные ряды, связанные с процессом, поступающие от регистрирующих устройств.

Идентификация состояния IoT-устройства происходит на основе значений, определяемых в дискретные моменты времени t_0, t_1, ..., t_n. В целях повышения качества анализируемых данных предполагается, что временной ряд должен имеет постоянную длину [12]. В результате по каждому состоянию получаем описания, выраженные m-мерными векторами признаков $X = (X_1, X_2, ..., X_m)$.

Множество рассматриваемых состояний C определяется заранее, что позволяет разметить обучающую выборку векторов X и определить два множества опасного и безопасного состояний $\{C_1, C_2\} \in C$

По очередным поступающим значениям вектора признаков $X = (X_1, X_2, ..., X_m)$ проводится идентификация класса C_i, $i = 1, 2$. Строится решающее правило для алгоритма $\rho(x)$, которое ставит в соответствие наблюдению одно из множеств C_1 или C_2. Оно определяется функцией $\varphi(x)$, порождающей разбиение пространства на две непересекающиеся области:

$$\rho(x) = \begin{cases} C_1, \text{ при } \varphi(x) \geqslant \varepsilon; \\ C_2, \text{ при } \varphi(x) < \varepsilon, \end{cases} \quad (1)$$

где ε — пороговое значение.

Экспериментальная оценка

При проведении экспериментальной оценки рассматривали работу двух программ, потребляющих вычислительные ресурсы.

Целью проведения эксперимента было выявление состояния вычислительного узла, определяемого алгоритмом обработки данных, на основе оцифрованных показателей загрузки вычислительных ресурсов [13—16]. В качестве временных рядов, описывающих состояния, использовались синхронизированные по времени процентные показатели монитора системной загрузки.

В качестве основного метода оценки рассматривается один из наиболее популярных алгоритмов кластеризации k-means. Он включает ряд шагов:

1) первоначально определяется число рассматриваемых состояний. Определяется размер анализируемых временных рядов, поступающих от монитора загрузки. Подготавливается обучающая выборка, где заданные состояния заранее размечаются;

2) анализируемые состояния разделяются на два подмножества: безопасные, где выполняются заранее предопределенные процессы, и опасные — где имеются отклонения от параметров в заданных режимах работы;

3) на основе обучающей выборки по мере поступления различных временных рядов определяются начальные центры их кластера:

$$\arg\min_S \sum_{i=1}^{k} \sum_{x \in S_i} \rho(x, \mu_i)^2, \qquad (2)$$

где μ_i — центры кластеров, $i = 1, ..., k$; $\rho(x, \mu_i)$ — функция расстояния между x и μ_i;

4) по мере поступления дополнительных значений временных рядов определяется ближайший центр кластера, вычисляются центроида и смещение центра кластера;

5) дальнейший анализ происходит на основе сравнений полученных текущих значений устройства с эталонными значениями центров кластеров и классов, вычисленными в условиях формировании обучающей выборки.

Рассмотрим четыре состояния:

S_0 — состояние, где работают фоновые процессы — устройство не выполняет полезные вычислительные действия;

S_1 — функционирует только алгоритм 1;

S_2 — функционирует только алгоритм 2;

S_3 — запущены обе программы, реализующие алгоритм 1 и алгоритм 2.

Каждое состояние определяется временным рядом, показывающим загрузку центрального процессора и памяти. Вид временного ряда для различных состояний представлен на рис. 1, *а—г*.

При проведении эксперимента была получена выборка временных рядов для рассматриваемых состояний. Выборка была разделена на обучающую и тестовую. Идентификацию состояния выполняли на основе метода кластеризации k-means [17, 18]. На обучающей выборке были размечены состояния, что позволило определить центры кластеров μ_i $i = 1, 2, ..., 4$, а поступающие значения тестовой выборки оценивали исходя из метрики расстояния и соотносили с соответствующим кластером.

В качестве меры близости использовано евклидово расстояние:

$$\rho(x, \mu_i) = \sqrt{\sum_{r=1}^{n} (x_r - \mu_i)^2}, \qquad (3)$$

где R — пространство наблюдений; $x, \mu_i \in R^n$.

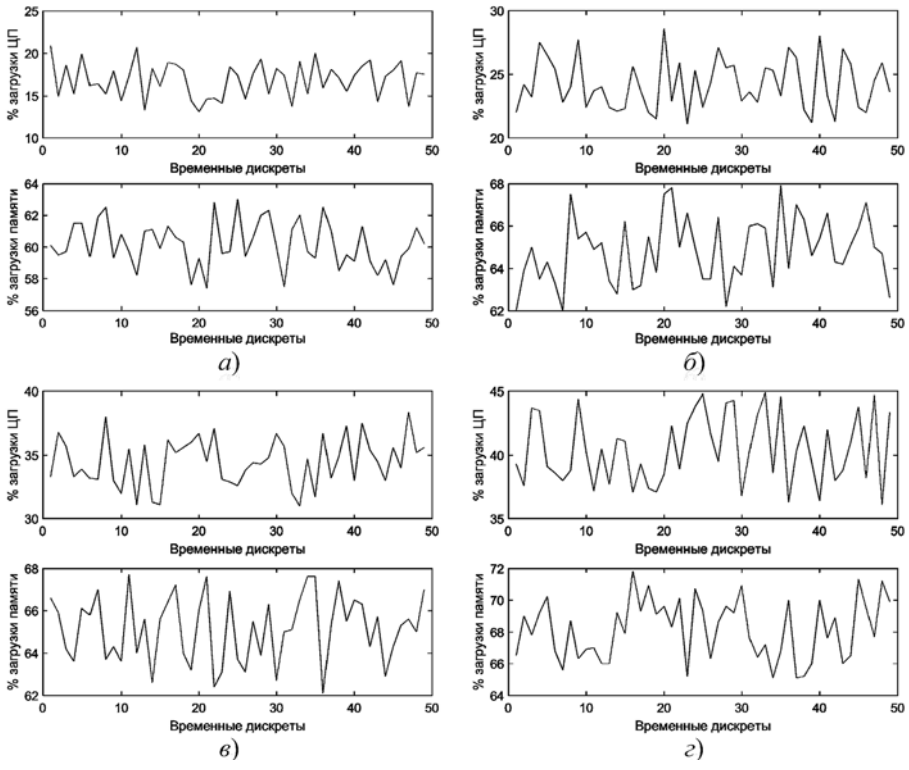


Рис. 1. Загрузка процессора и памяти для состояния:
а — S_0; *б* — S_1; *в* — S_2; *г* — S_3

Рассматривая двумерные значения загрузки процессора и памяти как обучающую выборку, для состояний S_0, ..., S_4 получаем кластеры, представленные на рис. 2.

Измерив расстояние до центроидов, выбираем из них минимальное значение, на основе которого принимаем решение о принадлежности к кластеру, идентифицирующему состояние:

$$Sh(x^{(j)}) = \frac{b(x^{(j)}) - a(x^{(j)})}{\max(a(x^{(j)}), b(x^{(j)}))}, \qquad (4)$$

где $a(x^{(j)})$ — среднее значение от точки $x^{(j)}$ до других точек кластера; $b(x^{(j)})$ — минимум (по другим кластерам) средних значений расстояний от точки $x^{(j)}$ до точек другого кластера.

Визуализация оценки полученных кластеров приведена на рис. 3.

Временные ряды от центрального процессора и ресурсов памяти для различных состояний позволяют формировать достаточно хорошо отличимые друг от друга кластеры.

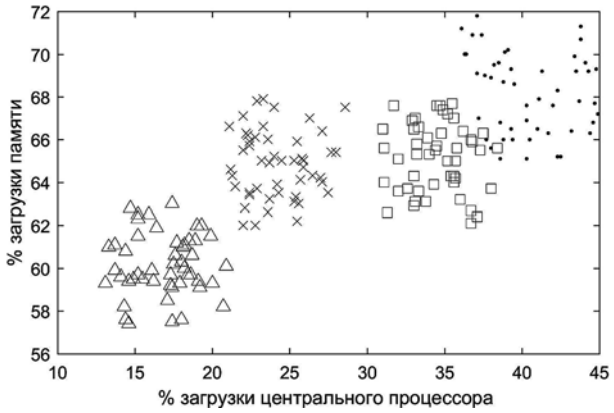


Рис. 2. Результаты кластеризации на основе метода кластеризации k-means

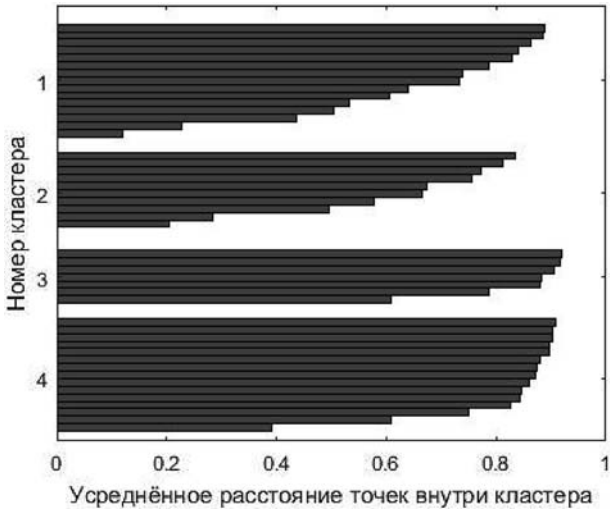


Рис. 3. Визуализация оценки полученных кластеров

Заключение

В настоящее время в связи с развитием интернета вещей возникает проблема оценки состояния информационной безопасности огромного числа устройств, находящихся вне контролируемой зоны. В качестве одного из методов был выбран и рассмотрен метод идентификации состояния на основе метода кластеризации k-means, обрабатывающего временные ряды от регистрирующих устройств. Новизна состоит в том, что представленный метод идентификации состояния информационной безопасности устройства, базирующийся на анализе временных рядов, позволяет в оперативном режиме отслеживать состояние устройства с минимальными затратами на использование вычислительных ресурсов в ходе эксплуатации.

Характерными особенностями представленного решения являются его простота реализации и модификации.

Применение метода существенно зависит от обрабатываемых данных. Скорость и точность обработки связаны с выбором центройдов кластеров, размером поступающего на вход временного ряда, отсутствием "выбросов" данных. Основной вопрос состоит в том, чтобы найти такие центры, для которых сформированные кластеры были бы компактны, что позволит достигать заданных показателей точности.

Список литературы

1. **Han Y., Etigowni S., Liu H., Zonouz S., Petropulu A.** Watch me, but don't touch me! Contactless control flow monitoring via electromagnetic emanations // Proc. 2017 ACM SIGSAC Conf. Computer and Communications Security. P. 1095—1108.

2. **Garcia L., Brasser F., Cintuglu M. H., Sadeghi A.-R., Mohammed O., Zonouz S. A.** Hey, my malware knows physics! Attacking PLCs with physical model aware rootkit // Proc. Network and Distributed System Security Symp. San Diego, CA. 2017. P. 26—28.

3. **Slay J., Miller M.** Lessons learned from the Maroochy water breach // Proc. Int. Conf. Critical Infrastructure Protection. 2007. P. 73—82.

4. **Falliere N., Murchu L. O., Chien E.** "W32. Stuxnet dossier // Symantect Security Response. 2011. Vol. 5, N. 6. P. 29.

5. **Bertino E., Islam N.** Botnets and Internet of Things security // Computer. 2017. Vol. 50, N. 2. P. 76—79.

6. **McLaughlin S. E., Zonouz S. A., Pohly D. J., McDaniel P. D.** A trusted safety verifier for process controller code // Presented at the Network and Distributed System Security Symp., San Diego, CA. Feb. 23—26. 2014.

7. **Qiao Y., Xin X., Bin Y., Ge S.** Anomaly intrusion detection method based on HMM // Electron. Lett. 2002. Vol. 38, N. 13. P. 663—664.

8. **Ryan J., Lin M.-J., Miikkulainen R.** Intrusion detection with neural networks // Advances Neural Inform. Process. Syst. 1998. P. 943—949.

9. **Etigowni S., Tian D. J., Hernandez G., Zonouz S., Butler K.** CPAC: Securing critical infrastructure with cyber-physical

access control // Proc. 32nd Annu. Conf. Computer Security Applications. 2016. P. 139—152.

10. **Farwell J. P., Rohozinski R.** Stuxnet and the Future of Cyber War // Survival. 2011. Vol. 53:1. P. 23—40.

11. **Yeung D.-Y., Ding Y.** Host-based intrusion detection using dynamic and static behavioral models // Pattern recognition. 2003. Vol. 36, N. 1. P. 229—243.

12. **Igure V., Laughter S., Williams R.** Security issues in SCADA networks // Computers & Security. 2006. Vol. 25, 7. P. 498—506.

13. **Зикратов И. А., Зикратова Т. В., Лебедев И. С.** Доверительная модель информационной безопасности мультиагентных робототехнических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 2 (90). С. 47—52.

14. **Gao D., Reiter M., Song D.** Beyond output voting: Detecting compromised replicas using HMM-based behavioral distance // IEEE Transactions on Dependable and Secure Computing. 2009. Vol. 6, N. 2. P. 96—110.

15. **Bevir M. K., O'Sullivan V. T., Wyatt D. G.** Computation of electromagnetic flowmeter characteristics from magnetic field data // Journal of Physics D Applied Physics. 1981. Vol. 14(3). P. 373—388.

16. **Semenov V. V., Lebedev I. S., Sukhoparov M. E., Salakhutdinova K. I.** Application of an Autonomous Object Behavior Model to Classify the Cybersecurity State // Internet of Things, Smart Spaces, and Next Generation Networks and Systems. 2019. P. 104—112.

17. **Семенов В. В., Лебедев И. С., Сухопаров М. Е.** Подход к классификации состояния информационной безопасности элементов киберфизических систем с использованием побочного электромагнитного излучения // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18, № 1. С. 98—105.

18. **Сухопаров М. Е., Семенов В. В., Салахутдинова К. И., Лебедев И. С.** Выявление аномального функционирования устройств индустрии 4.0 на основе поведенческих паттернов // Проблемы информационной безопасности. Компьютерные системы. 2020. № 1 (41). С. 96—102.

19. **Бендат Д., Пирсол А.** Применение корреляционного и спектрального анализа. М.: Мир, 1983. 312 с.

20. **Засов В. А., Тарабардин М. А., Никоноров Е. Н.** Алгоритмы и устройства для идентификации входных сигналов в задачах контроля и диагностики динамических объектов // Вестник Самарского государственного аэрокосмического университета. 2009. № 2. С. 115—123.

21. **Lockhart D. J.** et al. Expression monitoring by hybridization to high-density oligonucleotide arrays // Nat. Biotechnol. 1996. Vol. 14. P. 1675—1680.

22. **Golub T. R.** Molecular classification of cancer: class discovery and class prediction by gene expression monitoring // Science. 1999. Vol. 286 (5439). P. 531—537.

23. **Anderberg M. R.** Cluster Analysis for Applications. New York: Academic Press, 1976. 376 p.

24. **Dembele D., Kastner P.** C-means method for clustering microarray data // Bioinformatics. 2003. Vol. 19 (8). P. 973—980.

25. **Rousseeuw J. P.** Silhouettes: a graphical aid to the interpretation and validation of cluster analysis // J. Comp. Appl. Math. 1987. Vol. 20. P. 53—65.

26. **Whitfield M. L.** et al. Identification of Genes Periodically Expressed in the Human Cell Cycle and Their Expression in Tumors // Mol. Biol. Cell. 2002. Vol. 13. P. 1977—2000.

M. E. Sukhoparov, Ph.D. of Engineering Sciences, e-mail: mikhailsukhoparov@yandex.ru,
NPK "TRISTAN", St. Petersburg, 195256, Russian Federation,
I. S. Lebedev, Advanced Doctor in Engineering Sciences, e-mail: lebedev@iias.spb.su,
K. I. Salakhutdinova, Research Assistant, e-mail: kainagr@mail.ru,
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
St. Petersburg, 199178, Russian Federation

Method for Identifying the Information Security Status of Internet of Things Devices

An approach to analyzing the state of information security of industrial Internet devices and the Internet of things is described. External control systems that use side channels and allow to avoiding the consumption of computing resources of functioning devices are used. The proposed solution allows one to monitor the state of the device on-line with minimal costs for using computing resources during operation.

Keywords: *Internet of things, cyber-physical systems, state identification, information security, side channels*

DOI: 10.17587/it.27.72-77

References

1. **Han Y., Etigowni S., Liu H., Zonouz S., Petropulu A.** Watch me, but don't touch me! Contactless control flow monitoring via electromagnetic emanations, *Proc. 2017 ACM SIGSAC Conf. Computer and Communications Security*, pp. 1095—1108.

2. **Garcia L., Brasser F., Cintuglu M. H., Sadeghi A.-R., Mohammed O., Zonouz S. A.** Hey, my malware knows physics! Attacking PLCs with physical model aware rootkit, *Proc. Network and Distributed System Security Symp.*, San Diego, CA, 2017, pp. 26—28.

3. **Slay J., Miller M.** Lessons learned from the Maroochy water breach, *Proc. Int. Conf. Critical Infrastructure Protection*, 2007, pp. 73—82.

4. **Falliere N., Murchu L. O., Chien E.** W32. Stuxnet dossier, *Symantecm Security Response*, 2011, vol. 5, no. 6, p. 29.

5. **Bertino E., Islam N.** Botnets and Internet of Things security, *Computer*, 2017, vol. 50, no. 2, pp. 76—79.

6. **McLaughlin S. E., Zonouz S. A., Pohly D. J., McDaniel P. D.** A trusted safety verifier for process controller code, *presented at the Network and Distributed System Security Symp.*, San Diego, CA, 2014, Feb. 23—26.

7. **Qiao Y., Xin X., Bin Y., Ge S.** Anomaly intrusion detection method based on HMM, *Electron. Lett.*, 2002, vol. 38, no. 13, P. 663—664.

8. **Ryan J., Lin M.-J., Miikkulainen R.** Intrusion detection with neural networks, *Advances Neural Inform. Process. Syst.*, 1998, pp. 943—949.

9. **Etigowni S., Tian D. J., Hernandez G., Zonouz S., Butler K.** CPAC: Securing critical infrastructure with cyber-physical access control, *Proc. 32nd Annu. Conf. Computer Security Applications*, 2016, pp. 139—152.

10. **Farwell J. P., Rohozinski R.** Stuxnet and the Future of Cyber War, *Survival*, 2011, vol. 53:1, pp. 23—40.

11. **Yeung D.-Y., Ding Y.** Host-based intrusion detection using dynamic and static behavioral models, *Pattern recognition*, 2003, vol. 36, no. 1, pp. 229—243.

12. **Igure V., Laughter S., Williams R.** Security issues in SCADA networks, *Computers & Security,* 2006, vol. 25, no. 7, pp. 498—506.

13. **Zikratov I. A., Zikratova T. V., Lebedev I. S.** Trust model for information security of multi-agent robotic systems with a decentralized management, *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014, vol. 2 (90), pp. 47—52 (in Russian).

14. **Gao D., Reiter M., Song D.** Beyond output voting: Detecting compromised replicas using HMM-based behavioral distance, *IEEE Transactions on Dependable and Secure Computing*, 2009, vol. 6, no. 2, pp. 96—110.

15. **Bevir M. K., O'Sullivan V. T., Wyatt D. G.** Computation of electromagnetic flowmeter characteristics from magnetic field data, *Journal of Physics D Applied Physics*, 1981, vol. 14(3), pp. 373—388.

16. **Semenov V. V., Lebedev I. S., Sukhoparov M. E., Salakhutdinova K. I.** Application of an Autonomous Object Behavior Model to Classify the Cybersecurity State, *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, 2019, pp. 104—112.

17. **Semenov V. V., Lebedev I. S., Sukhoparov M. E.** Approach to classification of the information security state of elements for cyberphysical systems by applying side electromagnetic radiation, *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*., 2018, vol. 18, no. 1, pp. 98—105 (in Russian)..

18. **Sukhoparov M. E., Semenov V. V., Salakhutdinova K. I., Lebedev I. S.** Identification of anomalous functioning of industry 4.0 devices based on behavioral patterns, *Information Security Problems. Computer Systems,* 2020, no. 1 (41), pp. 96—102 (in Russian).

19. **Julius S. Bendat, Allan G. Piersol.** Engineering Applications of Correlation and Spectral Analysis, Moscow, Mir, 1983, 312 p. (in Russian).

20. **Zasov V. A., Tarabardin M. A., Nikonorov Y. N.** Algorithms and devices for input signal identification in problems of dynamic object control and diagnostics, *Vestnik of samara university. Aerospace and mechanical engineering*, 2009, no. 2, pp. 115—123 (in Russian).

21. **Lockhart D. J.** et al. Expression monitoring by hybridization to high-density oligonucleotide arrays, *Nat. Biotechnol.*, 1996, vol. 14, pp. 1675—1680.

22. **Golub T. R.** Molecular classification of cancer: class discovery and class prediction by gene expression monitoring, *Science*, 1999, vol. 286 (5439), pp. 531—537.

23. **Anderberg M. R.** Cluster Analysis for Applications, *Academic Press*, New York, 1976, 376 p.

24. **Dembele D., Kastner P.** C-means method for clustering microarray data, *Bioinformatics*, 2003, vol. 19 (8), pp. 973—980.

25. **Rousseeuw J. P.** Silhouettes: a graphical aid to the interpretation and validation of cluster analysis, *J. Comp. Appl. Math.*, 1987, vol. 20, pp. 53—65.

26. **Whitfield M. L.** et al. Identification of Genes Periodically Expressed in the Human Cell Cycle and Their Expression in Tumors, *Mol. Biol. Cell.*, 2002, vol. 13, pp. 1977—2000.

УДК 004.9, 004.94, 004.56 DOI: 10.17587/it.27.77-88

А. А. Коляда, д-р физ.-мат. наук, доц., e-mail: razan@tut.by,
П. В. Кучинский, д-р физ.-мат. наук, доц., e-mail: niipfp@bsu.by,
С. Ю. Протасеня, мл. науч. сотр., estellita@mail.ru,
Научно-исследовательское учреждение "Институт прикладных физических проблем имени А. Н. Севченко" Белорусского государственного университета, Минск

Метод и алгоритм выполнения декодирующей операции в пороговом криптомодуле разделения секрета с использованием минимально избыточной модулярной системы счисления

Представлена новая разработка метода и алгоритма выполнения в пороговом криптомодуле разделения секрета с маскирующим преобразованием декодирующей операции. Для решения рассматриваемой задачи применены рекурсивная схема деления на двоичную экспоненту и вычислительная технология на диапазонах больших чисел таблично-сумматорного типа, основанная на минимально избыточной модулярной арифметике (МИМА). Отличительной особенностью развиваемого подхода является использование в качестве области принадлежности секрета-оригинала конечных колец вычетов по модулям, имеющим вид степеней числа 2. Это существенно уменьшает сложность результирующей декодирующей МИМА-процедуры. Осуществляемая в рамках базовой технологии декомпозиция масштабируемых вычетов по большим модулям позволяет эффективно отображать реализуемый вычислительный процесс на наборы легко реализуемых операций извлечения данных из табличной памяти и их суммирования, обеспечивая высокий уровень производительности, однородности и унификации базовых структур. По быстродействию синтезированный декодирующий МИМА-алгоритм превосходит неизбыточные аналоги как минимум в $\frac{l(19l-3)}{22l-6}$ *раз (l — число абонентов, восстанавливающий секрет-оригинал). При l = 7...40 достигается (6,15...34,65)-кратное увеличение производительности.*

Ключевые слова: *пороговое разделение секрета, криптосхемы разделения секрета, маскирующее преобразование, декодирующая операция, модулярный код, модулярные системы счисления, минимально избыточная модулярная арифметика*

Введение

Важнейшей актуальной задачей современного процесса развития распределенных компьютерных и инфокоммуникационных систем является надежное обеспечение необходимого уровня безопасности при хранении, обработке и передаче данных [1, 2]. При решении обозначенной задачи особую роль выполняет применяемая технология управления криптографическими ключами. В настоящее время к наиболее перспективным технологиям такого рода относят технологию активной безопасности [1—3], которая базируется на периодическом обновлении ключей, одноразовых паролях и пространственном разделении секрета. На практике разделение секретной информации обычно осуществляется в рамках пороговых схем [1—12].

Реализуемое (t, n)-пороговой системой решающее правило обеспечивает разделение секрета n абонентами с возможностью его восстановления по компонентам, принадлежащим любым l участникам сеанса связи ($2 \leqslant t \leqslant l \leqslant n$; t — пороговое число абонентов). При этом группы абонентов числом $k < t$ реконструировать секрет-оригинал по соответствующим компонентам не могут. Криптографический ключ фактически представляет собой главный секрет во всем процессе шифрования. Механизм ключей предполагает использование специальной операционной базы, обеспечивающей генерирование и надежное хранение ключей, декомпозицию ключей на компоненты в целях распределения их между абонентами системы, а также восстановление ключей-оригиналов по их составным частям. Исходный и долевые секреты представляют собой большие целые числа (ЦЧ), поэтому эффективность выполняемых в пороговых криптосистемах преобразований определяется реализационными свойствами используемой технологии перевода осуществляемых вычислений из диапазонов больших чисел в диапазоны ЦЧ стандартной разрядности. В свете сказанного в качестве компьютерно-арифметической основы для криптографических приложений рассматриваемого класса целесообразно принять модулярную арифметику — арифметику модулярных систем счисления (МСС). Модулярное кодирование служит простым средством декомпозиции (разделения) секрета на составные части и позволяет минимизировать затраты при оперировании в диапазонах больших чисел. Фундаментальные преимущества МСС наиболее полно удается реализовать в рамках так называемого минимально избыточного кодирования [2, 12—14].

Наиболее трудоемкой операцией в пороговых криптосистемах модулярной арифметики разделения секретной информации является реконструкция секрета-оригинала по модулярным кодам маскирующего аналога. Это обусловлено главным образом использованием в операциях данного класса вычислительных технологий, ориентированных на диапазоны больших чисел, а также соответствующих конфигураций интегрально-характеристической базы системы счисления в остатках [1, 2, 12—15]. Настоящая статья посвящена разработке метода и алгоритма выполнения декодирующей операции в пороговом криптомодуле разделения секрета, базирующемся на минимально избыточной модулярной арифметике (МИМА) [2, 12—14]. Применение вычислительной МИМА-технологии на диапазонах больших чисел для решения рассматриваемой задачи позволяет в значительной мере минимизировать необходимые временные и аппаратурные затраты.

1. Постановка задачи и методы ее решения

Введем обозначения:

$\lfloor a \rfloor$ и $\lceil a \rceil$ — наибольшее и наименьшее ЦЧ, соответственно не большее и не меньшее вещественной величины a;

НОД (A, B) — наибольший общий делитель целых чисел A и B;

$\mathbf{Z}_m = \{0, 1, ..., m-1\}$ и $\mathbf{Z}_m^- = \left\{-\frac{m}{2}, -\frac{m}{2}+1, \ldots, \frac{m}{2}-1\right\}$ — множества наименьших неотрицательных и абсолютно наименьших вычетов (остатков) по натуральному модулю $m > 1$;

$A \equiv B \pmod{m}$ — условная запись равноостаточности по модулю m целых чисел A и B;

$\chi = |A/B|_m = (A/B) \pmod{m}$ и $\chi^- = |A/B|_m^-$ — элементы соответственно множеств $\mathbf{Z}_m$ и $\mathbf{Z}_m^-$, удовлетворяющие сравнениям $B\chi \equiv A \pmod{m}$ и $B\chi^- \equiv A \pmod{m}$ ($B \neq 0$, НОД (B, m) = 1);

$\mathbf{M}\_l = \{m_1, m_2, \ldots, m_l\}$ — базис МСС, состоящий из $l > 1$ попарно простых модулей (оснований);

$(|X|_{m_1}, |X|_{m_2}, \ldots, |X|_{m_l})$ — представление ЦЧ X (модулярный код) в МСС с базисом $\mathbf{M}\_l$.

Пусть $p_1, p_2, ..., p_n$ — упорядоченные по возрастанию попарно простые большие натуральные числа ($n > 1$); $P_i = \prod_{s=1}^{i} p_s$; $\_P_j = \prod_{s=1}^{j} p_{n-s+1} = /P_{n-j}$ ($i, j = \overline{1,n}$); $\mathbf{P} = \{p_1, ..., p_2, ..., p_n\}$; $\mathbf{I}\_l = \{\forall(i_1, i_2, ..., i_l) | 1 \leqslant i_1 < i_2 < ... < i_l \leqslant n;\ 2 \leqslant t \leqslant l \leqslant n\}$

(t — фиксированное натуральное число); $I\_l = (i_1, i_2, ..., i_l)$ — произвольный элемент множества $\mathbf{I}\_l$; $\mathbf{P}_{I\_l} = \{p_{i_1}, p_{i_2}, \ldots, p_{i_l}\}$; $P_{I\_l} = \prod_{j=1}^{l} p_{i_j}$.

Концептуальную основу (t, n)-пороговой схемы разделения секрета с модулярным базисом $\mathbf{P} = \mathbf{P}\_n = \{p_1, p_2, ..., p_n\}$, которая рассчитана на полное число n и пороговое число t абонентов распределенной системы, составляют нижеследующие определяющие положения.

А. Исходный секрет (секрет-оригинал) представляет собой ЦЧ $S \in \mathbf{Z}_p$ (p — большой модуль, взаимно простой с $p_1, p_2, ..., p_n$).

Б. Над S в МСС с базисом $\mathbf{P}$ выполняется маскирующее преобразование вида

$$\tilde{S} = S + Cp, \tag{1}$$

где C — псевдослучайный целочисленный параметр.

Цифры $\tilde{\sigma}_i = |\tilde{S}|_{p_i} = |\sigma_i + |Cp|_{p_i}|_{p_i}$ ($\sigma_i = |S|_{p_i}$; $i = \overline{1, n}$) получаемого кода $(\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_n)$ рассматриваются как долевые (частичные) секреты, принадлежащие одноименным абонентам.

В. Любые l абонентов ($t \leqslant l \leqslant n$) могут восстановить секрет-оригинал S по принадлежащим им долевым (маскирующим) секретам. Но никакая группа абонентов, число которых $k < t$, сделать этого не может.

Построение теоретико-методологической, алгоритмической и инструментальной базы, обеспечивающей оптимальную реализацию перечисленных основополагающих принципов порогового разделения секретной информации в распределенных системах обработки данных является важнейшим направлением развития технологии активной безопасности [1—3].

Представляемые исследования нацелены на решение задачи восстановления секрета-оригинала S по кодам $(\tilde{\sigma}_{i_1}, \tilde{\sigma}_{i_2}, \ldots, \tilde{\sigma}_{i_l})$ МСС с базисами $\mathbf{P}_{I\_l}$ ($I\_l \in \mathbf{I}\_l$) маскирующего аналога (1) (см. пункт **А**) с обеспечением минимизации временных затрат на выполнение результирующей декодирующей процедуры при сохранении максимального уровня криптостойкости, присущего классическим пороговым схемам, таким, в частности, как схемы Шамира, Блэкли и другие [3—11]. При этом для синтеза искомого декодирующего алгоритма (алгоритма восстановления секрета-оригинала) используются метод деления на двоичную экспоненту, а также вычислительная МИМА-технология [2]. Применяемый методологический и реализационный инструментарий адаптирован к решаемой проблеме.

Основополагающая идея предлагаемой алгоритмизации преобразования $\tilde{S} \to S$ состоит в использовании для кодирования секрета-маски $\tilde{S}$ семейства минимально избыточных МСС (МИМСС), определяемых базисами $\mathbf{P}_{I\_l}$, которые в соответствии с пунктом **В** отвечают группам абонентов числом l. Без нарушения общности изложение дальнейшего материала в целях упрощения употребляемых обозначений преимущественно проводится на примере группы абонентов, за которыми закрепляются основания $p_1, p_2, ..., p_l$ набора $\mathbf{P}\_l$ — представителя множества $\mathbf{P}_{\mathbf{I}\_l}$ с $I\_l = (1, 2, ..., l) \in \mathbf{I}\_l$. Долевые секреты, принадлежащие абонентам указанной группы, являются цифрами кода $(\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ МСС с модулями $p_1, p_2, ..., p_l$ секрета-маски $\tilde{S}$.

В компьютерных алгоритмах МИМА фундаментальную роль выполняет интервально-модулярная форма чисел. В случае ЦЧ $\tilde{S} = (\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ она имеет вид

$$\tilde{S} = \sum_{i=1}^{l-1} P_{i,l-1}\tilde{\sigma}_{i,l-1} + P_{l-1}I_l(\tilde{S}), \tag{2}$$

где $P_{i,l-1} = \dfrac{P_{l-1}}{p_i}$, $P_{l-1} = \prod_{s=1}^{l-1} p_s$;

$$\tilde{\sigma}_{i,l-1} = \left|P_{i,l-1}^{-1}\tilde{\sigma}_i\right|_{p_i}; \tag{3}$$

$I_l(\tilde{S})$ — интервальный индекс числа $\tilde{S}$ по базису $\mathbf{P}\_l$. Принцип минимально избыточного модулярного кодирования раскрывает нижеследующая теорема [2, 13, 14].

Теорема 1. Для того, чтобы в МСС с базисом $\mathbf{P}\_l$ интервальный индекс $I_l(\tilde{S})$ каждого элемента $\tilde{S}$ диапазона $\mathbf{Z}_P = \{0, 1, ..., P - 1\}$ ($P = p_0P_{l-1}$; p_0 — вспомогательный модуль) полностью определялся вычетом $\hat{I}_l(\tilde{S}) = \left|I_l(\tilde{S})\right|_{p_l}$, необходимо и достаточно выполнения условия

$$p_l \geqslant 2p_0 + l - 2 \ (p_0 \geqslant l - 2). \tag{4}$$

При этом для $I_l(\tilde{S})$ верны расчетные соотношения:

$$I_l(\tilde{S}) = \begin{cases} \hat{I}_l(\tilde{S}), & \text{если } \hat{I}_l(\tilde{S}) < p_0, \\ \hat{I}_l(\tilde{S}) - p_l, & \text{если } \hat{I}_l(\tilde{S}) \geqslant p_0; \end{cases} \tag{5}$$

$$\hat{I}_l(\tilde{S}) = \left| \sum_{i=1}^{l} R_{i,l}(\tilde{\sigma}_i) \right|_{p_l}; \tag{6}$$

$$\begin{aligned} R_{i,l}(\tilde{\sigma}_i) &= \left| -p_i^{-1} \left| P_{i,l-1}^{-1}\tilde{\sigma}_i \right|_{p_i} \right|_{p_l} \ (i \neq l), \\ R_{l,l}(\tilde{\sigma}_l) &= \left| \frac{\tilde{\sigma}_l}{P_{l-1}} \right|_{p_l}. \end{aligned} \tag{7}$$

Главное преимущество МИМСС с базисами $\mathbf{P}_{\_l}$ ($I\_l \in \mathbf{I}\_l$) над неизбыточными аналогами обусловлено l-кратным сокращением реализационных затрат на вычисление интервального индекса, осуществляемое по формулам вида (5)—(7) [2, 13, 14].

Корректное согласование порогового принципа разделения секрета и минимально избыточного модулярного кодирования с обеспечением необходимого уровня криптостойкости результирующей МИМА-схемы дает нижеследующая теорема [12].

Теорема 2. Пусть $p_1, p_2, ..., p_n$ — упорядоченные по возрастанию попарно простые натуральные числа, составляющие базис $\mathbf{P} = \mathbf{P}\_n$ модулярной схемы разделения секрета, p — взаимно простой с $p_1, p_2, ..., p_n$ модуль кольца $\mathbf{Z}_p$ принадлежности секрета-оригинала S, который разделяется между n абонентами путем наделения их долевыми секретами $\tilde{\sigma}_i = |\tilde{S}|_{p_i}$ $(i = \overline{1,n})$, получаемыми в результате декомпозиции применяемой функции маскирования: $\tilde{S} = S + Cp$ (C — псевдослучайный целочисленный параметр). Для того чтобы любые l абонентов ($2 \leqslant t \leqslant l \leqslant n$; t — фиксированное ЦЧ) могли восстановить S по соответствующему коду МСС маскирующего секрета $\tilde{S}$, удовлетворяющей условию вида (4) минимальной избыточности (см. теорему 1), но никакая группа абонентов числом $k < t$ не имела такой возможности, достаточно выполнения системы условий:

$$\begin{cases} \tilde{S} \in \tilde{\mathbf{S}} = \{\tilde{S}_{\text{нп}}, \tilde{S}_{\text{нп}} + 1, \ldots, \tilde{S}_{\text{вп}}\} \subseteq \\ \subseteq \{\_P_{t-1}, \_P_{t-1} + 1, \ldots, p_0 P_{t-1} - 1\}, \\ C \in \tilde{\mathbf{C}} = (\mathbf{C} \backslash \mathbf{C}_p), \end{cases}$$

где $\tilde{S}_{\text{нп}}$ и $\tilde{S}_{\text{вп}}$ — используемые нижнее и верхнее пороговые значения секрета-маски $\tilde{S}$; p_0 — вспомогательный модуль, удовлетворяющий ограничению $p_0 \leqslant p_t - t + 2$;

$$\mathbf{C} = \{C_{\text{нп}}, C_{\text{нп}} + 1, \ldots, C_{\text{вп}}\}$$

$$(C_{\text{нп}} = \left\lfloor \tilde{S}_{\text{нп}}/p \right\rfloor; \quad C_{\text{вп}} = \left\lfloor \tilde{S}_{\text{вп}}/p \right\rfloor);$$

$$\mathbf{C}_p = \{\forall\, C \in \mathbf{C} \mid S + Cp \in (\tilde{S}_{\text{нп}}; \tilde{S}_{\text{вп}});$$

$$Q(\tilde{S}; j_1, j_2, \ldots, j_k) = \left\lfloor \frac{\tilde{s}}{\prod_{i=1}^{k} p_{j_i}} \right\rfloor$$

$(1 \leqslant j_1 < j_2 \ldots < j_k \leqslant n;\ 2 \leqslant k < t)\}$, p — делитель ЦЧ Q.

Использование в качестве допустимой области значений для псевдослучайного параметра C множества $\tilde{\mathbf{C}}$, как того требует условие $C \in \tilde{\mathbf{C}}$ теоремы 2, обеспечивает результирующей МИМА-криптосхеме максимальный уровень криптостойкости, свойственный схемам рассматриваемого класса.

Из соотношения (1) вытекает равенство $S = |\tilde{S}|_p$, указывающее на то, что для получения S по $\tilde{S}$ в принципе достаточно ЦЧ $\tilde{S}$ привести к остатку по модулю p. Но так как p — большое число, то в общем случае данная операция весьма трудоемка. Поэтому для ее выполнения целесообразно воспользоваться процедурами, в которых применяются модули p частного вида.

В статье рассматривается случай, когда p представляет собой двоичную экспоненту разрядностью b_p бит, т. е. имеет вид $p = 2^{b\_p}$, и пусть $r = 2^{b\_r}$, $b\_r \leqslant b\_p$, $\nu = \lceil b\_p/b\_r \rceil$, $(\tilde{s}_{\nu-1}\ \tilde{s}_{\nu-2} \ldots \tilde{s}_0)_r$ ($\tilde{s}_j \in \mathbf{Z}_r$; $j = \overline{0, \nu-1}$) — код числа $|\tilde{S}|_{r^\nu}$ в позиционной системе счисления (ПСС) с основанием r разрядностью ν цифр. Тогда основой для восстановления секрета-оригинала S по маскирующему секрету $\tilde{S}$ может служить формула

$$S = |\tilde{S}|_p = |\tilde{S}|_{2^{b\_p}} = (s_{\nu-1}\ s_{\nu-2} \ldots s_0)_r, \qquad (8)$$

где

$$s_j = \begin{cases} \tilde{s}_j \text{ при } j = \overline{0, \nu-2}, \\ \tilde{s}_{\nu-1}(\mathrm{mod}(\exp_2(b_p - (\nu-1)b\_r))) \\ \text{при } j = \nu - 1. \end{cases} \qquad (9)$$

Из соотношений (8), (9) следует, что в случае $p = 2^{b\_p}$ решение поставленной задачи для группы пользователей, отвечающей рассматриваемому набору оснований $\mathbf{P}\_l = \{p_1, p_2, ..., p_l\}$, сводится к преобразованию минимально избыточного модулярного кода (МИМК) $(\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ в позиционный r-ичный код $(\tilde{s}_{\nu-1}\ \tilde{s}_{\nu-2} \ldots \tilde{s}_0)_r$. Это преобразование может быть осуществлено по методу деления на двоичную экспоненту [2]: маскирующего секрета $\tilde{S} = (\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ на $r = 2^{b\_r}$, причем по упрощенному МИМА-алгоритму.

2. Метод деления на двоичную экспоненту с применением МИМСС

Преобразование минимально избыточного модулярного кода $(\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ в позиционный r-ичный код $(\tilde{s}_{\nu-1}\ \tilde{s}_{\nu-2} \ldots \tilde{s}_0)_r$ числа $\tilde{S}$ методом деления на двоичную экспоненту $r = 2^{b\_r}$ базируется на операционном кортеже рекурсивного типа:

$$\left\langle \tilde{S}_0 = \tilde{S},\ \tilde{s}_0 = |\tilde{S}_0|_r;\ \tilde{S}_1 = \lfloor \tilde{S}_0/r \rfloor,\ \tilde{s}_1 = |\tilde{S}_1|_r; \right.$$
$$\tilde{S}_2 = \lfloor \tilde{S}_1/r \rfloor,\ \tilde{s}_2 = |\tilde{S}_2|_r;\ \ldots; \qquad (10)$$
$$\left. \tilde{S}_{\nu-1} = \tilde{S}_{\nu-2}/r,\ \tilde{s}_{\nu-1} = |\tilde{S}_{\nu-1}|_r \right\rangle.$$

На j-й итерации процесса реализации (10) сначала формируется минимально избыточный модулярной код $(\tilde{\sigma}_1^{(j)}, \tilde{\sigma}_2^{(j)}, \ldots, \tilde{\sigma}_l^{(j)})$ ЦЧ $\tilde{S}_j$, а затем находится цифра $\tilde{s}_j$ его r-ичного позиционного кода путем расширения полученного минимально избыточного модулярного кода на модуль $r = 2^{b\_r}$ согласно правилу

$$\tilde{s}_j = |\tilde{S}_j|_r = \left| \sum_{i=1}^{l-1} \left| P_{i,l-1} \tilde{\sigma}_{i,l-1}^{(j)} \right|_r + |P_{l-1} I_l(\tilde{S}_j)|_r \right|_r$$
$$(j = \overline{0, \nu-1}), \qquad (11)$$

где

$$\tilde{\sigma}_{i,l-1}^{(j)} = \left| P_{i,l-1}^{-1} \tilde{\sigma}_i^{(j)} \right|_{p_i}; \qquad (12)$$

интервально-индексная характеристика $I_l(\tilde{S}_j)$ числа $\tilde{S}_j$ определяется по расчетным соотношениям (5)—(7) при $\tilde{S} = \tilde{S}_j$ и $\tilde{\sigma}_i = \tilde{\sigma}_i^{(j)}$ $(i = \overline{1, l})$.

Что касается числа $\tilde{S}_j$, то в соответствии с (10) для цифр его минимально избыточного модулярного кода верна формула

$$\tilde{\sigma}_i^{(j)} = \left\| \frac{\tilde{S}_{j-1}}{r} \right\|_{p_i} =$$
$$= \begin{cases} \tilde{\sigma}_i \text{ при } j = 0, \\ \left| \left| \tilde{\sigma}_i^{(j-1)} - \tilde{s}_{j-1} \right|_{p_i} |r^{-1}|_{p_i} \right|_{p_i} \text{ при } j = \overline{1, \nu-1} \end{cases} \qquad (13)$$
$$(i = \overline{1, l}).$$

Конкретный выбор способа компьютерной реализации базовых расчетных соотношений (10)—(13) рассматриваемого метода модулярно-позиционного кодового преобразования в первую очередь определяется необходимостью оперирования в диапазонах больших чисел — в конечных кольцах по большим модулям $p_1, p_2, \ldots, p_n$. В частности, это относится к нормированным остаткам (12), вычетам (7) и (13).

Наряду с отмеченным фактором важной особенностью предлагаемой конфигурации метода деления на двоичную экспоненту $r = 2^{b\_r}$ является использование значений параметра *b_r,* допускающих применение так называемой таблично-сумматорной вычислительной технологии [2] в процедурах расширения минимально избыточного модулярного кода и получения неполных частных на итерациях рекурсивного процесса (10) (см. (11), (13)).

Пусть $m \in \mathbf{P}$, X — элемент множества $\mathbf{Z}_m$, C — произвольный целочисленный масштаб. Тогда представляя X в позиционной системе счисления с основанием $u = 2^{b\_u}$ (b_u — натуральное число), т. е. в виде $X = \sum_{h=0}^{v-1} x_h u^h$ ($x_h \in \mathbf{Z}_u$; $v = \lceil b\_mod/b\_u \rceil$; $b\_mod = \lceil \log_2 m \rceil$ — разрядность модуля m), будем иметь:

$$\chi = |CX|_m = \left| \sum_{h=0}^{v-1} \left| C x_h u^h \right|_m^- \right|_m. \qquad (14)$$

Для компьютерной реализации выражений типа (14) воспользуемся таблицами аддитивных компонент масштабируемой позиционной формы ЦЧ CX, представляемых симметрическими остатками по модулю m. В соответствии с (14) необходимые таблицы формируются по правилу

$$TACMPF\_h[x] = |Cxu^h|_m^-$$
$$\left(x = \overline{0, u-1}; h = \overline{0, v-1}\right). \qquad (15)$$

Слагаемые модульные суммы (14) могут быть как положительными, так и отрицательными, поэтому в таблицах (15) их следует хранить в двоичном дополнительном коде.

Применяемый способ вычисления вычетов χ по выражению (14) является двухшаговым. На первом шаге с помощью таблиц (15) находится сумма

$$\Sigma = \sum_{h=0}^{v-1} TACMPF\_h[x_h], \qquad (16)$$

а на втором Σ приводится к остатку по модулю m. Определим максимальную разрядность b_Σ (в битах) суммы Σ. Из соотношений (15), (16) следует, что для нижнего и верхнего пороговых значений Σ верны оценки: $\Sigma_{НП} = -v\lfloor m/2 \rfloor$ и $\Sigma_{ВП} = v(\lceil m/2 \rceil - 1)$. Таким образом,

$$b\_\Sigma = \lceil \log_2 (\Sigma_{ВП} - \Sigma_{НП}) \rceil \leqslant b\_mod + b\_v \qquad (17)$$

($b\_v = \lceil \log_2 v \rceil$ — разрядность величины v).

Как показывает (17), суммирование вычетов (15) согласно (16) должно проводиться на двоичном сумматоре, разрядность b_Σ которого превышает разрядность b_mod сумматора по модулю m на b_v бит.

Обозначая $(x_{b\_\Sigma-1}^{(\Sigma)} x_{b\_\Sigma-2}^{(\Sigma)} \ldots x_0^{(\Sigma)})_2$ дополнительный двоичный код суммы Σ разрядностью b_Σ бит, разобьем его на две части — младшую $(x_{b\_mod-2}^{(\Sigma)} x_{b\_mod-3}^{(\Sigma)} \ldots x_0^{(\Sigma)})_2$ и старшую $(x_{b\_\Sigma-1}^{(\Sigma)} x_{b\_\Sigma-2}^{(\Sigma)} \ldots x_{b\_mod-1}^{(\Sigma)})_2$, которые имеют соответственно разрядности $b\_mod - 1$ и $b\_v + 1$ бит, принимая во внимание равенство $\Sigma = \sum_{h=0}^{b\_\Sigma-2} x_h^{(\Sigma)} 2^h - x_{b\_\Sigma-1}^{(\Sigma)} 2^{b\_\Sigma-1}$.

Заключаем, что для выполнения преобразования $\Sigma \to |\Sigma|_m$ может быть применена формула

$$\chi = |\Sigma|_m = |\Sigma_0 + \Sigma_1|_m, \qquad (18)$$

где

$$\Sigma_0 = \sum_{h=0}^{b\_mod-2} x_h^{(\Sigma)} 2^h; \qquad (19)$$

$$\Sigma_1 = \left| \sum_{h=b\_mod-1}^{b\_\Sigma-2} x_h^{(\Sigma)} 2^h - x_{b\_\Sigma-1}^{(\Sigma)} 2^{b\_\Sigma-1} \right|_m. \qquad (20)$$

Значения $b\_$-битового вычета Σ_1 по модулю m рассчитываются согласно (20) предварительно и записываются в табличную память — в таблицу TRes_MP по правилу

$$TRes\_MP[(x_{b\_\Sigma-1}^{(\Sigma)} x_{b\_\Sigma-2}^{(\Sigma)} \dots x_{b\_mod-1}^{(\Sigma)})_2] = \Sigma_1. \qquad (21)$$

Емкость таблицы (21) составляет 2^{b_v} слов разрядностью b_mod бит.

Описанный метод тривиальным образом распространяется и на случай принадлежности входного ЦЧ X и выходного вычета χ конечным кольцам по разным модулям. В частности, это относится к вычетам $R_{i,l}(\tilde{\sigma}_{i,l-1}^{(j)}) = \left| -p_i^{-1} \sigma_{i,\,l-1}^{(j)} \right|_{p_l}$ $(\sigma_{i,l-1}^{(j)} \in \mathbf{Z}_{p_i})$, т. е. к вычетам второго каскада операции формирования слагаемых $R_{i,l}(\tilde{\sigma}_i^{(j)})$ модульной суммы вида (6) (см. (7), (12)).

Остановимся теперь на особенностях предлагаемой компьютерной реализации расчетных соотношений (8) и (12) операции расширения минимально избыточного модулярного кода $(\tilde{\sigma}_1^{(j)}, \tilde{\sigma}_2^{(j)}, \dots, \tilde{\sigma}_l^{(j)})$ числа $\tilde{S}_j$ на модуль $r = 2^{b\_r}$. Отметим, что исходными данными j-й итерации рекурсивного процесса (7) деления секрета-маски $\tilde{S}$ на r служат минимально избыточный модулярный код $(\tilde{\sigma}_1^{(j-1)}, \tilde{\sigma}_2^{(j-1)}, \dots, \tilde{\sigma}_l^{(j-1)})$ ЦЧ $\tilde{S}_{j-1}$ и цифра $\tilde{s}_{j-1}$ его r-ичного кода $(\tilde{s}_{v-1}\, \tilde{s}_{v-2} \dots \tilde{s}_0)_r$. Следуя лемме Эвклида из теории делимости, представим i-ю цифру $\tilde{\sigma}_i^{(j-1)}$ минимально избыточного модулярного кода числа $\tilde{S}_{j-1}$ в виде

$$\tilde{\sigma}_i^{(j-1)} = |\tilde{\sigma}_i^{(j-1)}|_r + \left\lfloor \frac{\tilde{\sigma}_i^{(j-1)}}{r} \right\rfloor r. \qquad (22)$$

С учетом выражения (22) для всех $j = \overline{1, \eta - 1}$ из (12) получаем:

$$\tilde{\sigma}_i^{(j)} = \left| \left\| \frac{\tilde{\sigma}_i^{(j-1)}}{r} \right\|_{p_i} + \left| \frac{|\tilde{\sigma}_i^{(j-1)}|_r - \tilde{s}_{j-1}}{r} \right|_{p_i} \right|_{p_i}. \qquad (23)$$

Для компьютерной реализации выражение (23) более удобно, чем (12). Числитель $d_i^{(j-1)} = |\tilde{\sigma}_i^{(j-1)}|_r - \tilde{s}_{j-1}$ дроби $f_i^{(j-1)} = \dfrac{d_i^{(j-1)}}{r}$ из (23) удовлетворяет неравенству $-(r-1) \leqslant d_i^{(j-1)} \leqslant r - 1$, поэтому разность $d_i^{(j-1)}$ полностью определяется своим дополнительным $(b\_r + 1)$-битовым кодом или симметрическим остатком $\delta_i^{(j-1)} = |d_i^{(j-1)}|_{2^{b\_r+1}}^{-} = |d_i^{(j-1)}|_{2r}^{-}$ по модулю $2r$. Благодаря небольшой разрядности r, а значит и $\delta_i^{(j-1)}$, величина $\varphi_i^{(j-1)} = \left| \dfrac{\delta_i^{(j-1)}}{r} \right|_{p_i}$ может быть получена табличным способом. Необходимая таблица генерируется по правилу

$$TRes\_f\_i[\delta] = \left| \frac{\delta}{r} \right|_{p_i} \quad (\delta = \overline{-r, r-1}). \qquad (24)$$

Таким образом, вычисление i-й цифры МИМК числа $\tilde{S}_j$ по формуле (23) с использованием таблицы (24) сводится к выделению из двоичного кода цифры $\sigma_i^{(j-1)}$ ЦЧ $\tilde{S}_{j-1}$ старшей $((b\_mod\_i)\text{-}r)$-битовой части $\left\lfloor \tilde{\sigma}_i^{(j-1)} / r \right\rfloor$ числа $\tilde{S}_{j-1}$, извлечению из таблицы $TRes\_f\_i$ по получаемому симметрическому остатку $\delta_i^{(j-1)} = |d_i^{(j-1)}|_{2r}^{-}$ величины $\varphi_i^{(j-1)} = TRes\_f\_i[\delta_i^{(j-1)}]$ и выполнению операции сложения по модулю p_i над вычетами $\left\| \dfrac{\tilde{\sigma}_i^{(j-1)}}{r} \right\|_{p_i}$ и $\varphi_i^{(j-1)}$. Отметим, что емкость таблицы $TRes\_f\_i$ составляет $r + 1$ слов разрядностью $b\_mod\_i = \lceil \log_2 p_i \rceil$ бит.

Что касается базового расчетного соотношения (8) операций расширения МИМК $(\tilde{\sigma}_1^{(j)}, \tilde{\sigma}_2^{(j)}, \dots, \tilde{\sigma}_l^{(j)})$ чисел $\tilde{S}_j$, то для его реализации также применима таблично-сумматорная вычислительная технология. Это обеспечивается выбором приемлемого по величине модуля r. Основой представляемого подхода к выполнению операций расширения минимально избыточного модулярного кода служат таблицы остатков по модулю r слагаемых интервально-модулярной формы ЦЧ. Элементы этих таблиц определяются по формулам

$$TRes\_AIMFi[\sigma] = \\ = \| P_{i,l-1} |_r \sigma |_r \ (\sigma = \overline{0, r-1};\ i = \overline{1, l}), \qquad (25)$$

$$TRes_{AIMFl[I]} = \| P_{l-1} |_r I |_r \ (I = \overline{0, r-1}). \qquad (26)$$

Используя выражения (13), (9), а также (25), (26), запишем соотношение (8) в виде

$$\tilde{s}_j = \left| \sum_{i=1}^{l-1} TRes\_AIMFi[|\sigma_{i,l-1}^{(j)}|_r] + \right. \\ \left. + TRes\_AIMFi[|\hat{I}_l(\tilde{S}_j)|_r] + C\_II \right|_r, \qquad (27)$$

где *C_II* — поправка для интервального индекса числа $\tilde{S}_j$, которая в соответствии с (9) вычисляется по формуле

$$C\_II = (1 - sn(\hat{I}_l(\tilde{S}_j) - p_0)|-P_l|_r \quad (P_l = P_{l-1}p_l); \tag{28}$$

sn — знаковая функция вида

$$sn(a) = \begin{cases} 0, \text{ если } a \geqslant 0, \\ 1, \text{ если } a < 0. \end{cases}$$

Отметим, что вычеты $\tilde{\sigma}_{i,l-1}^{(j)}$ находятся в процессе вычисления интервально-индексной характеристики $\hat{I}_l(\tilde{S}_j)$. Так как *r* является двоичной экспонентой, то получение остатков $|\tilde{\sigma}_{i,l-1}^{(j)}|_r$ и $|\hat{I}_l(\tilde{S}_j)|_r$ как аргументов для таблиц *TRes_AIMFi* и *TRes_AIMFl* в (27), а также остатка $|-P_l|_r$ сводится к выделению из двоичных кодов соответствующих ЦЧ *b_r*-битовых младших частей. Что касается интервально-индексной поправки *C_II*, то согласно формуле (28) для ее формирования требуется определить знак разности $\hat{I}_l(\tilde{S}_j) - p_0$. Это может быть осуществлено с помощью (1 + *b_mod_l*)-битового сумматора. Важным фактором, способствующим упрощению декодирующей процедуры на основе метода деления на двоичную экспоненту, является простота вычисления модульной суммы (27). Компьютерная реализация (27) осуществляется на *b_r*-битовых сумматорах, причем без контроля переполнений.

3. Алгоритм выполнения декодирующей операции

Изложенное позволяет сформулировать нижеследующий алгоритм восстановления секрета-оригинала с применением метода деления на двоичную экспоненту.

Параметрическая база алгоритма:

— $\mathbf{P} = \{p_1, p_2, ..., p_n\}$ — базис (*t*,*n*)-порогового МИМА-криптомодуля разделения секрета, состоящий из $n > t$ упорядоченных по возрастанию попарно простых оснований (*t* — пороговое число абонентов);

— p_0 — вспомогательный модуль, удовлетворяющий ограничению $\_qp_t \leqslant p_0 \leqslant p_t - t + 2$ $(0 \leqslant \_q \leqslant 1)$;

— *p* — модуль кольца $\mathbf{Z}_p = \{0, 1, ..., p - 1\}$ принадлежности секрета-оригинала *S*, взаимно простой с $p_1, p_2, ..., p_n$ и имеющий разрядность *b_p* битов;

— $\tilde{\mathbf{S}} = \{\lceil \_P_{t-1}pq \rceil, \lceil \_P_{t-1}pq \rceil + 1, ..., \lfloor \_qP_t \rfloor - 1\}$ — рабочий диапазон криптомодуля по маскирующему секрету $\tilde{S} = S + Cp$ ($\_P_{t-1} = \prod_{s=1}^{t-1} p_{n-s+1}$; $q \geqslant p^{-1}$; $P_t = \prod_{s=1}^{t} p_s$; $S \in \mathbf{Z}_p$; $C \in \tilde{\boldsymbol{C}}$; $\tilde{\boldsymbol{C}}$ — множество допустимых значений для псевдослучайного параметра *C* (см. теорему 2));

— $\mathbf{P}\_l = \{\forall\{p_{i_1}, p_{i_2}, ..., p_{i_l}\} \mid 1 \leqslant i_1 < i_2 < ... < i_l \leqslant n; t \leqslant l \leqslant n\}$ — множество *l*-компонентных наборов оснований из $\mathbf{P}$, распределяемых между группами абонентов, которые могут восстановить секрет-оригинал *S* по кодам секрета-маски $\tilde{S}$;

— $\{p_1, p_2, ..., p_l\}$ — фиксируемый представитель множества $\mathbf{P}\_l$;

— $r = 2^{b\_r}$ — модуль разрядностью *b_r* бит ($b\_r \leqslant b\_p$), используемый в базовом методе деления на двоичную экспоненту *r*;

— $u = 2^{b\_u}$ — основание позиционной системы счисления разрядностью *b_u* битов, применяемой для декомпозиции вычетов в процессе их преобразования с масштабированием в элементы колец по большим модулям в рамках таблично-сумматорной вычислительной технологии.

Входные данные алгоритма: подлежащий декодированию модулярный код $(\tilde{\sigma}_1, \tilde{\sigma}_2, ..., \tilde{\sigma}_l)$ секрета-маски $\tilde{S}$ по заданному набору $\mathbf{P}_{I\_l}$ оснований ($\mathbf{P}_{I\_l} = \{p_1, p_2, ..., p_l\}$).

Выходные данные: позиционный код $(s_{\nu-1}s_{\nu-2}...s_0)_r$ секрета-оригинала *S*, эквивалентный его двоичному коду разрядностью $b\_p = \lceil \log_2 p \rceil$ битов.

Предварительно получаемые данные:

- системные константы

$$C_i = |P_{i,l-1}|_r, \ \mu_{i,l-1} = |P_{i,l-1}^{-1}|_{p_i} \ (i = \overline{1, l-1});$$

$$C_l = |P_{l-1}|_r; |-P_l|_r; |r^{-1}|_{p_i} \ (i = \overline{1, l});$$

$$m_{i,l} = |-p_i^{-1}|_{p_l} \ (i = \overline{1, l-1}); \ \mu_{l,l} = |P_{l-1}^{-1}|_{p_l};$$

- таблицы остатков по модулю *r* слагаемых интервально-модулярной формы ЦЧ, генерируемые по расчетным соотношениям:

$$TRes\_AIMFi[\sigma] = \| |P_{i,l-1}|_r \sigma|_r,$$

$$TRes\_AIMFl[I] = \| |P_{l-1}|_r I|_r$$

$$(\sigma, I = \overline{0, r-1}; i = \overline{1, l-1});$$

- таблицы формальных частных для поитерационных операций деления на *r* расширенных минимально избыточных модулярных кодов, рассчитываемые по формуле

$$TRes\_f_{i[\delta]} = \left|\frac{\delta}{r}\right|_{p_i} \quad (\delta = \overline{-r, r-1}; i = \overline{1, l})$$

- таблицы аддитивных компонент масштабируемой позиционной формы ЦЧ по основанию $u = 2^{b\_u}$, формируемые согласно формулам

$$TACMPF\_i\_h[x] = \left\| P_{i,l-1}^{-1} \right|_{p_i} xu^h \Big|_{p_i}^{-}$$
$$(x = \overline{0, u-1};\ h = \overline{0, \lceil b\_mod\_i / b\_u \rceil - 1};\ i = \overline{1, l-1}), \quad (29)$$

$$\_TACMPF\_i\_h[x] =$$
$$= \begin{cases} \left\| -P_i^{-1} \right|_{p_l} xu^h \Big|_{p_l}^{-} \ (x = \overline{0, u-1}; \\ h = \overline{0, \lceil b\_mod\_i / b\_u \rceil - 1}) \text{ при } i = \overline{1, l-1}, \\ \left\| P_{l-1}^{-1} \right|_{p_l} xu^h \Big|_{p_l}^{-} \\ (x = \overline{0, u-1};\ h = \overline{0, \left\lceil \frac{b\_mod\_l}{b\_u} \right\rceil - 1}) \text{ при } i = l; \end{cases} \quad (30)$$

- таблицы старшей L-битовой части по основаниям p_i ЦЧ А с $b\_$-разрядным дополнительным двоичным кодом ($a_{b\_A-1}\ a_{b\_A-2}$ ... $a_{b\_A-L} \dots a_0)_2$ $(a_s \in \{0,1\}\ (s = \overline{0, b\_A-1}))$, генерируемые по правилу

$$TRes\_MP\_i[(a_{b\_A-1} a_{b\_A-2} \dots a_{b\_A-L})_2] =$$
$$= \left| \sum_{s=b\_A-L}^{b\_A-2} a_s 2^s - a_{b\_A-1} 2^{b\_A-1} \right|_{p_i} \ (i = \overline{1, l}). \quad (31)$$

Тело алгоритма восстановления секрета-оригинала (ВСО) по методу деления на двоичную экспоненту:

ВСО_Д.1. Активировать (l + 1)-элементный массив MC_Q для модулярных кодов неполных частных ЦЧ и поместить в него код $(\tilde{\sigma}_1^{(0)}, \tilde{\sigma}_2^{(0)}, \dots, \tilde{\sigma}_l^{(0)}) = (\tilde{\sigma}_1, \tilde{\sigma}_2, \dots, \tilde{\sigma}_l)$ числа $\tilde{S}_0 = \tilde{S}$ согласно правилу $MC\_Q[i] = \tilde{\sigma}_i^{(0)}$ $(i = \overline{1, l})$.

ВСО_Д.2. Определить число v итераций реализуемого рекурсивного процесса деления на экспоненту $r = 2^{b\_r}$ как $v = \lceil b\_p / b\_r \rceil$, активировать элементный массив PC_S для цифр r-ичного кода $(s_{\nu-1} s_{\nu-2} \dots s_0)_r$ секрета-оригинала S, записываемых в PC_S в порядке возрастания индексов (от 0 до $\nu - 1$), и порядковому номеру текущей итерации осуществляемого процесса (а значит и очередной цифры формируемого r-ичного кода) присвоить начальное значение $j = 0$.

ВСО_Д.3. Положить $s = 0$.

Вычисление компьютерного интервального индекса $\hat{I}_l(\tilde{S}_j)$ ЦЧ $\tilde{S}_j$.

ВСО_Д.4. Переменным I и i присвоить значения $I = 0$ и $i = 1$.

ВСО_Д.5. Выполнить операции: $X = 0$, $\sigma = MC\_Q[i] = \tilde{\sigma}_i^{(j)}$, $h = 0$, $v = \lceil b\_mod\_i / b\_u \rceil$.

Получение нормированного остатка $\tilde{\sigma}_{i,l-1}^{(j)}$ (см. (13)).

ВСО_Д.6. Следуя (14)—(16), выполнить операцию накопления, аккумулятивную операцию $X = X +$ TACMPF_i_h[$\sigma \wedge (u-1)$].

ВСО_Д.7. Инкрементировать переменную h ($h = h + 1$).

ВСО_Д.8. Если $h \neq v$, то значение переменной σ логически сдвинуть на b_u бит вправо ($\sigma = \sigma \gg= b\_u$) и перейти к ВСО_Д.6.

ВСО_Д.9. Текущее значение X привести к остатку по модулю p_i, реализуя операционную последовательность:

ВСО_Д.9А. Из двоичного кода ЦЧ X выделить младшую ((b_mod_i)-1)-битовую часть $X_0 = X \wedge (2^{(b\_mod\_i)-1} - 1)$.

ВСО_Д.9Б. Выделить старшую часть ЦЧ X разрядностью $L = (b\_v) + 1$ бит ($b\_v = \lceil \log_2 v \rceil$ и с помощью таблицы TRes_MP_i получить остаток $X_1 = TRes\_MP\_i\ [X \gg= ((b\_mod\_i) - 1)]$ (см. (18)—(21), (31)).

ВСО_Д.9В. Определить нормированный остаток $\tilde{\sigma}_{i,l-1}^{(j)} = \sigma = |X_0 + X_i|_{p_i}$ по модулю p_i.

ВСО_Д.10. Используя таблицу TRes_AIMFi, выполнить аккумулятивную операцию $s = s +$ $+ TRes\_AIMFi\ [\sigma \wedge (r-1)]$.

Вычисление вычета $R_{i,l}(\tilde{\sigma}_{i,l-1}^{(j)})$ по модулю p_l, определяемого согласно (11).

ВСО_Д.11. Положить $R = 0$, $h = 0$.

ВСО_Д.12. С помощью таблицы _TACMPF (см. (30)) выполнить операцию накопления $R = R +$ _TACMPF_i_h[$\sigma \wedge (u-1)$].

ВСО_Д.13. Инкрементировать переменную h ($h = h + 1$).

ВСО_Д.14. Если $h \neq v$, то значение переменной σ сдвинуть на b_u битов вправо ($\sigma = \sigma \gg= b\_u$) и перейти к ВСО_Д.12.

ВСО_Д.15. Текущее значение переменной R привести к остатку по модулю p_l, реализуя последовательность действий:

ВСО_Д.15А. Из двоичного кода ЦЧ R выделить младшую ((b_mod_l)-1)-битовую часть $R_0 = R \wedge (2^{(b\_mod\_l)-1} - 1)$.

ВСО_Д.15Б. Выделить старшую часть ЦЧ R разрядностью $L = (b\_v) + 1$ битов и с помощью таблицы TRes_MP_l получить остаток $R_1 = TRes\_MP\_l$ $[R \gg = ((b\_mod\_l) - 1)]$.

ВСО_Д.15В. Найти вычет $R_{i,l}(\tilde{\sigma}_{i,l-1}^{(j)}) =$ $= R = |R_0 + R_1|_{p_l}$.

ВСО_Д.16. Выполнить аккумулятивную операцию $I = I + R$.

ВСО_Д.17. Инкрементировать переменную i ($i = i + 1$).

ВСО_Д.18. При $i \neq l$ перейти к ВСО_Д.5.

Вычисление вычета $R_{l,l}(\tilde{\sigma}_l^{(j)})$ по модулю p_l, определяемого согласно (11).

ВСО_Д.19. Положить $R = 0$, $h = 0$, $v = \lceil b\_mod\_l / b\_u \rceil$, $\sigma = MC\_Q[l]$.

ВСО_Д.20. Выполнить аккумулятивную операцию $R = R +$ _TACMPF_$l_h[\sigma \wedge (u-1)]$ (см. (30).

ВСО_Д.21. Инкрементировать переменную h ($h = h + 1$).

ВСО_Д.22. При $h \neq v$ текущее значение переменной σ сдвинуть вправо на b_u битов ($\sigma = \sigma \gg = b\_u$) и перейти к ВСО_Д.20.

ВСО_Д.23. Текущее значение R привести к остатку по модулю p_l, реализуя последовательность:

ВСО_Д.23А. Выделить младшую ((b_mod_l)-1)-битовую часть $R_0 = R \wedge (2^{(b\_mod\_l)-1} - 1)$.

ВСО_Д.23Б. Выделить старшую часть ЦЧ R разрядностью $L = (b\_v) + 1$ бит и с помощью таблицы TRes_MP_l найти остаток $R_1 = TRes\_MP\_l$ $[R \gg = ((b\_mod\_l) - 1)]$.

ВСО_Д.23В. Получить вычет $R_{l,l}(\tilde{\sigma}_l^{(j)}) = R = \left|R_0 + R_1\right|_{p_l}$.

ВСО_Д.24. Выполнить операцию накопления $I = I + R$.

ВСО_Д.25. Полученное значение переменной I привести к остатку по модулю p_l, реализуя действия:

ВСО_Д.25А. Выделить младшую ((b_mod_l)-1)-битовую часть $I_0 = I \wedge (2^{(b\_mod\_l)-1} - 1)$ числа I.

ВСО_Д.25Б. Из двоичного кода ЦЧ I выделить старшую часть разрядностью $L = \lceil \log_2 l \rceil + 1$ бит и с помощью таблицы TRes_MP_l найти остаток $I_1 = TRes\_MP\_l$ $[I \gg = ((b\_mod\_l) - 1)]$.

ВСО_Д.25В. Вычислить компьютерный интервальный индекс ЦЧ $\tilde{S}_j$ по правилу $\hat{I}_l(\tilde{S}_j) = \left|I\right|_{p_l} = \left|I_0 + I_1\right|_{p_l}$.

ВСО_Д.26. Выполнить аккумулятивную операцию $s = s + TRes\_AIMFl$ $[I \wedge (r-1)]$ (см. (26)).

ВСО_Д.27. Если $I - p_0 \geqslant 0$, то в соответствии с (27) и (28) осуществить коррекцию переменной s по правилу $s = s + C\_II$ ($C\_II = |-P_l|_r$).

ВСО_Д.28. При $j \neq v - 1$ реализовать последовательность операций:

ВСО_Д.28А. В качестве j-й цифры позиционного r-ичного кода $(s_{v-1}\, s_{v-2} \ldots s_0)_r$ секрета-оригинала $S = \left|\tilde{S}\right|_p$ зафиксировать значение $s_j = |s|_r = s \wedge (r-1)$, поместив его в массив PC_S согласно правилу $PC\_S[j] = s_j$.

ВСО_Д.28Б. В соответствии с (23) сформировать минимально избыточный модулярный код $(\tilde{\sigma}_1^{(j+1)}, \tilde{\sigma}_2^{(j+1)}, \ldots, \tilde{\sigma}_l^{(j+1)})$ числа $\tilde{S}_{j+1}$ для следующей $(j+1)$-й итерации процесса деления на r, выполняя для всех $i = \overline{1,l}$ действия:

- получить симметрический остаток $\delta_i^{(j)} = \left|(r-1) \wedge MC\_Q[i] - s_j\right|_{2r}^{-}$ в дополнительном двоичном коде разрядностью $(b\_r) + 1$ битов;
- из таблицы $TRes\_f\_i$ извлечь вычет $\varphi_i^{(j)} = TRes\_f\_i\,[\delta] = \left|\delta_i^{(j)} / r\right|_{p_i}$;
- выделить из двоичного кода цифры $\tilde{\sigma}_i^{(j)} = MC\_Q[i]$ МИМК числа $\tilde{S}_j$ старшую $((b\_mod\_i) - b\_r)$-битовую часть $q_i^{(j)} = \left\lfloor \tilde{\sigma}_i^{(j)} / r \right\rfloor = \tilde{\sigma}_i^{(j)} \gg = b\_r$;
- завершить формирование i-й цифры минимально избыточного модулярного кода ЦЧ $\tilde{S}_{j+1}$, вычисляя модульную сумму $MC\_Q[i] = \tilde{\sigma}_i^{(j+1)} = \left|q_i^{(j)} + \varphi_i^{(j)}\right|_{p_i}$.

ВСО_Д.28В. Инкрементировать переменную j ($j = j + 1$) и перейти к ВСО_Д.4.

ВСО_Д.29. По достижении равенства $j = \nu - 1$ в качестве $(\nu - 1)$-й цифры позиционного r-ичного кода секрета-оригинала S зафиксировать значение $PC\_S[\nu - 1] = s_{\nu-1} = (s \wedge (r-1))$ $(\mathrm{mod}(\exp_2(b\_p - (\nu - 1)b\_r)))$ (см. (6)).

ВСО_Д.30. В качестве искомого r-ичного кода секрета-оригинала S зафиксировать $(s_{\nu-1}\, s_{\nu-2} \ldots s_0)_r = (PC\_S[\nu - 1]\ PC\_S[\nu - 2] \ldots PC\_S[0])_r$ и завершить работу алгоритма.

4. Оценка эффективности декодирующего МИМА-алгоритма

В (t, n)-пороговом МИМА-криптомодуле восстановление секрета-оригинала S по секрету-маске $\tilde{S}$ с помощью синтезированного алгоритма ВСО_Д.1 — ВСО_Д.30 деление на двоичную экспоненту осуществляется за время

$$t_{\text{ВСО}} = v(t_{\text{ИИ}} + t_{\text{р}} + t_{\text{МК}}), \tag{32}$$

где $v = \lceil b\_p / b\_r \rceil$ — число итераций процесса деления на r; $t_{\text{ИИ}}$ — время вычисления интервального индекса ЦЧ в l-модульной минимально избыточной МСС; t_p — время расширения кода на экспоненту $r = 2^{b\_r}$ (без учета затрат на получение интервального индекса); $t_{\text{МК}}$ — временные затраты на формирование модулярного кода неполного частного (для следующей итерации). Операционный анализ алгоритма ВСО_Д.1 — ВСО_Д.30 дает для $t_{\text{ИИ}}$, $t_{\text{р}}$, $t_{\text{МК}}$ оценочные выражения:

$$t_{\text{ИИ}} = ((2l-1)(\lceil b\_mod / b\_u \rceil + 1) + l + 3)t_{\text{сл},\,b\_mod}; \tag{33}$$

$$t_{\text{р}} = l t_{\text{сл}}; \tag{34}$$

$$t_{\text{МК}} = l(t_{\text{сл}} + 1 + t_{\text{сл},\,b\_mod}), \tag{35}$$

в которых $t_{\text{сл, }b\_\text{mod}}$ и $t_{\text{сл}}$ — длительности двух местных операций сложения в процессах суммирования *b_mod*-битовых вычетов и вычетов стандартной разрядности соответственно. С учетом (34), (35) оценку (32) можно записать в следующем развернутом виде:

$$t_{\text{ВСО}} = \left\lceil \frac{b\_p}{b\_r} \right\rceil \left(\left((2l-1)\left(\left\lceil \frac{b\_\text{mod}}{b\_u} \right\rceil + 1 \right) + \right. \right. \\ \left. \left. + 2l + 3 \right) t_{\text{сл},b\_mod} + 2lt_{\text{сл}} \right). \quad (36)$$

В случае применения в пороговом криптомодуле разделения секрета рассматриваемого класса вместо минимально избыточной МСС неизбыточного аналога оценка (32) суммарных временных затрат на выполнение декодирующей операции по алгоритму типа ВСО_Д.1 — ВСО_Д.30 принимает вид

$$t'_{\text{ВСО}} = \nu(t'_{\text{ИИ}} + t_{\text{р}} + t_{\text{МК}}), \quad (37)$$

где $t'_{\text{ИИ}}$ — время вычисления в неизбыточной l-модульной МСС интервально-индексной характеристики. Согласно представленному в работах [2, 14] алгоритму РИХ_ОА.1 — РИХ_ОА.8 расчет интервального индекса ЦЧ в l-модульной неизбыточной МСС требует примерно в l раз больше временных затрат, чем в минимально избыточных МСС с такими же основаниями, т. е. $t'_{\text{ИИ}} = lt_{\text{ИИ}}$. Таким образом, в виду (32)—(37) получаемый выигрыш по рассматриваемому показателю при использовании минимально избыточных МСС вместо неизбыточной МСС для построения порогового криптомодуля разделения секрета оценивается коэффициентом

$$V = \frac{lt_{\text{ИИ}} + t_{\text{р}} + t_{\text{МК}}}{t_{\text{ИИ}} + t_{\text{р}} + t_{\text{МК}}}. \quad (38)$$

Пусть

$$U = \frac{t_{\text{р}} + t_{\text{МК}}}{t_{\text{ИИ}}}, \quad (39)$$

тогда (38) можно записать в следующей эквивалентной форме:

$$V = \frac{l-1}{U+1} + 1. \quad (40)$$

Функциональная зависимость $V = V(U)$, описываемая соотношением (40), представляет собой участок гиперболы с асимптотами $U = -1$ и $V = 1$ (см. рисунок). Согласно (33)—(36) аргумент (39) функции (40) представим в виде

$$U = \frac{l(t_{\text{сл},b\_mod} + t_{\text{сл}})}{\left((2l-1)\left(\left\lceil \frac{b\_\text{mod}}{b\_u} \right\rceil + 1 \right) + l + 3 \right) t_{\text{сл},b\_mod}} = \\ = \frac{1 + \frac{t_{\text{сл}}}{t_{\text{сл},b\_mod}}}{\left(2 - \frac{1}{l} \right)\left(\left\lceil \frac{b\_mod}{b\_u} \right\rceil + 1 \right) + 1 + \frac{3}{l}}. \quad (41)$$

Так как $t_{\text{сл}} < t_{\text{сл},b\_mod}$, $l \geqslant 2$, а параметры *b_mod* и *b_u* на практике удовлетворяют ограничениям $b\_mod \geqslant 128$, $b\_u \leqslant 16$, то значения переменной U удовлетворяют неравенству $0 < U < 0 < U < \frac{3l}{19l-6}$ и, как нетрудно проверить, пороговый МИМА-криптомодуль разделения секрета по производительности превосходит аналог на основе традиционно используемых версий МА не менее чем в $\frac{l(19l-3)}{2(11l-3)}$ раз. При этом, однако, коэффициент (40) достигаемого

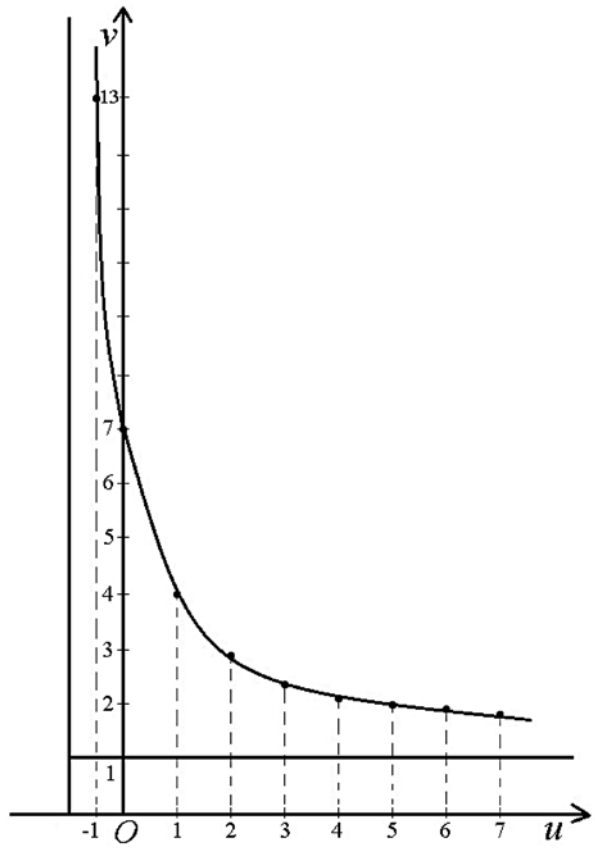


График коэффициента уменьшения времени выполнения декодирующей процедуры в пороговом МИМА-криптомодуле разделения секрета в сравнении с неизбыточным аналогом (для $l = 7$ абонентов)

Минимальные значения коэффициента V увеличения быстродействия декодирующей МИМА-процедуры на основе метода деления на двоичную экспоненту в сравнении с неизбыточными МА-аналогами

№ п/п	Число абонентов, восстанавливающих секрет l	Минимальное увеличение быстродействия декодирующей процедуры $V_{\text{мин}}(l)$
1	5	4,423
2	7	6,149
3	12	10,465
4	16	13,919
5	20	17,373
6	25	21,691
7	30	26,009
8	35	30,327
9	40	34,645

повышения быстродействия сверху ограничен порогом l. В таблице приведены значения указанного нижнего порога $\frac{l(19l-3)}{2(11l-3)} = V_{\text{мин}}(l)$ показателя V для некоторых l.

Заключение

Основные результаты представленной разработки по проблематике создания математического обеспечения модулярных пороговых криптосистем разделения секрета кратко можно охарактеризовать следующим образом.

1. Предложена МИМА-конфигурация метода деления на двоичную экспоненту для выполнения декодирующей операции в пороговом криптомодуле разделения секрета с маскирующим преобразованием. Главные отличительные особенности разработанного подхода к решению рассматриваемой задачи обусловлены использованием колец принадлежности секрета-оригинала по модулям, имеющим вид степеней числа 2, а также вычислительной МИМА-технологии, согласованной с пороговым принципом. Это приводит к существенному сокращению реализационных затрат на этапе реконструкции исходного секрета по кодам маскирующего аналога.

2. Для перевода трудоемких вычислений, приходящихся на декодирующее преобразование, из диапазонов больших чисел в диапазоны ЦЧ стандартной разрядности наряду с модулярной арифметикой применена таблично-сумматорная технология. Осуществляемая в рамках этой технологии поразрядная декомпозиция двоичных кодов масштабируемых вычетов по большим модулям служит эффективным инструментарием отображения выполняемых вычислительных процедур на наборы легкореализуемых операций извлечения данных из табличной памяти и их суммирования, обеспечивая при этом высокий уровень производительности, однородности и унификации базовых структур.

3. На основе метода деления на двоичную экспоненту и вычислительной МИМА-технологии таблично-сумматорного типа синтезирован эффективный алгоритм восстановления секрета-оригинала по кодам секрета-маски. Проведен сравнительный анализ эффективности предложенного алгоритма с неизбыточными аналогами. Показано, что по производительности декодирующий МИМА-алгоритм превосходит аналоги как минимум в $\frac{l(19l-3)}{2(11l-3)}$ раз (l — число абонентов, реконструирующих секрет-оригинал). В частности, при $l = 7...40$ достигается (6,15...34,65)-кратное повышение производительности.

Список литературы

1. **Червяков Н. И.** и др. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. М.: ФИЗМАТЛИТ, 2012. 280 с.

2. **Червяков Н. И., Коляда А. А., Ляхов П. А.** и др. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. М.: ФИЗМАТЛИТ, 2017. 400 с.

3. **Харин Ю. С.** и др. Криптология: учебник. Мн.: БГУ, 2013. 511 с.

4. **Shamir Adi.** How to share a secret // Communications of the ACM. 1979. Vol. 22, N. 11. P. 612—613.

5. **Blakley G. R.** Safe guarding cryptographic keys // Proc. Of the 1979 AFIPS national computer conference. Montvale: AFIPS press, 1979. P. 313—317.

6. **Mignotte M.** How to share a secret // Lecture notes in computer science. 1983. Vol. 149. P. 371—375.

7. **Asmuth C. A.**, **Bloom J.** A modular appoach to key safe guarding // IEEE Tras. On information theory. 1983. Vol. 29, N. 2. P. 208—210.

8. **Шнайер Б.** Алгоритмы разделения секрета. Схема интерполяционных полиномов Лагранжа // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Н.: Триумф, 2002. С. 588—589.

9. **Shiong Jian Shyu, Ying-Ru Chen.** Treshold secret image sharing by Chinese remainder theorem // IEEE Asia — Pacific Services Computing conference. Yilan, Taiwan, 9—12 dec., 2008. Vol. 1. P. 1332—1337.

10. **Bahramian Mojtaba, Khadijeh Eslami**. An efficient threshold verifiable multisecret sharing scheme using generalized Jacobean of elliptic curves // Journal of algebraic structures and their applications. 2017. Vol. 4, Iss. 2. P. 45—55.

11. **Jia Xingxing, Daoshun Wang, Daxin Nie, Xiangyang Luo, Jonathan Zheng Sun.** A new threshold changeable secret sharing scheme based on the Chinese remainder theorem // Information sciences. 2019. Vol. 473. P. 13—30.

12. **Коляда А. А., Кучинский П. В., Червяков Н. И.** Пороговый метод разделения секрета на базе избыточных модулярных вычислительных структур// Информационные технологии. Т. 25, № 9. М.: Новые технологии, 2019. С. 553—561.

13. **Коляда А. А., Пак И. Т.** Модулярные структуры конвейерной обработки цифровой информации. Мн.: Университетское, 1992. 256 с.

14. **Коляда А. А.** Обобщенная интегрально-характеристическая база модулярных систем счисления // Информационные технологии. 2017. Т.23, № 9. М.: Новые технологии, 2017. С. 641—649.

15. **Ananda Mohan P. V.** Residue number systems: Theory and applications. Basel: Birghauser, Mathematics, 2016. 351 p.

A. A. Kolyada, Doctor of Physical and Mathematical Sciences, Associate Professor, e-mail: razan@tut.by,
P. V. Kuchynski, Doctor of Physical and Mathematical Sciences, Associate Professor, e-mail: niipfp@bsu.by,
S. Yu. Protasenia, Junior Scientist, Laboratory of Specialized Computational Systems, e-mail: estellita@mail.ru,
Research establishment "Institute of Applied Physics Problems of A. N. Sevchenko"
Belarusian State University, Minsk

Method and Algorithm for Implementation of Decoding Operation in the Threshold Cryptomodule of Secret Separation Using a Minimally Redundant Modular Number System

The article presents a new development of method and algorithm for performing secret separation in a threshold cryptomodule with masking transformation of the decoding operation. To solve this problem a recursive binary exponent division scheme and computational technology on the ranges of large numbers of the table-adder type, based on minimally redundant modular arithmetic (MRMA) are applied. A distinctive feature of the developed approach is usage the secret-original domain of finite residue rings for modules that have the form of powers of the number 2. This significantly reduces the complexity of the resulting decoding MRMA-procedure. Decomposition of scalable residues into large modules allows you to efficiently map the computational process being implemented to sets of easily implemented data extraction operations from table memory and their summation, providing a high level of performance, uniformity, and unification of basic structures. In terms of speed, the created MIMA decoding algorithm surpasses non-redundant analogues by at least $\frac{l(19l-3)}{2(11l-3)}$ *times (l is the number of subscribers restoring the secret original). When l = 7...40 a (6.15...34.65) -fold increase in productivity is achieved.*

Keywords: *threshold secret sharing, secret sharing cryptographic schemes, masking conversion, decoding operation, modular code, modular number systems, minimally redundant modular arithmetic*

DOI: 10.17587/it.27.77-88

References

1. **Chervjakov N. I.** The use of artificial neural networks and the residual class system in cryptography, Moscow, FIZMATLIT Publ., 2012, 280 p. (in Russian).

2. **Chervjakov N. I., Koljada A. A., Ljahov P. A.** ets. Modular arithmetic and its applications in infocommunication technologies, Moscow, FIZMATLIT Publ., 2017, 400 p. (in Russian).

3. **Kharin Yu. S.** et al. Cryptology: a textbook, Minsk, BSU, 2013, 511 p. (in Russian).

4. **Shamir Adi.** How to share a secret, *Communications of the ACM*, 1979, vol. 22, no. 11, pp. 612—613.

5. **Blakley G. R.** Safe guarding cryptographic keys, *Proc. of the 1979 AFIPS National Computer Conference,* Montvale, AFIPS press, 1979, pp. 313—317.

6. **Mignotte M.** How to share a secret, *Lecture notes in computer science*, 1983, vol. 149, pp. 371—375.

7. **Asmuth C. A.**, **Bloom J.** A modular appoach to key safe guarding, *IEEE Tras. On Information Theory*, 1983, vol. 29, no. 2, pp. 208—210.

8. **Schneier B.** Secret Secretion Algorithms. Scheme of Lagrange interpolation polynomials, Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnyye teksty na yazyke Si, N., Triumf, 2002, pp. 588—589.

9. **Shiong Jian Shyu, Ying-Ru Chen.** Treshold secret image sharing by Chinese remainder theorem, *IEEE Asia — Pacific Services Computing Conference*, Yilan, Taiwan, 9—12 dec., 2008, vol. 1, pp. 1332—1337.

10. **Bahramian Mojtaba, Khadijeh Eslami**. An efficient threshold verifiable multisecret sharing scheme using generalized Jacobean of elliptic curves, *Journal of Algebraic Structures and their Applications*, 2017, vol. 4, iss. 2, pp. 45—55.

11. **Jia Xingxing, Daoshun Wang, Daxin Nie, Xiangyang Luo, Jonathan Zheng Sun.** A new threshold changeable secret sharing scheme based on the Chinese remainder theorem, *Information Sciences*, 2019, vol. 473, pp. 13—30.

12. **Kolyada A. A., Kuchinsky P. V., Chervyakov N. I.** The threshold secret sharing method based on redundant modular computing structures, *Informatsionnyye Tekhnologii*., 2019, vol. 25, no. 9, pp. 553—561 (in Russian).

13. **Koljada A. A., Pak I. T.** Modular structures of conveyor processing of digital information, *Minsk*, Universitetskoe, 1992, 256 p. (in Russian).

14. **Kolyada A. A.** Generalized integral-characteristic base of modular number systems, *Informatsionnyye Tekhnologii*. 2017, vol. 23, no. 9, pp. 641—649 (in Russian).

15. **Ananda Mohan P. V.** Residue number systems: Theory and applications. Basel, Birghauser, Mathematics, 2016, 351 p.

УДК 004.051 DOI: 10.17587/it.27.89-96

В. П. Кулагин, д-р техн. наук, проф., e-mail: kulagin@mirea.ru,
А. А. Логинов, аспирант, e-mail: loginov.a.a@edu.mirea.ru,
РТУ МИРЭА, Москва

Анализ программных средств для работы с сетями Петри

Представлен обзор существующего программного обеспечения для моделирования с использованием сетей Петри (СП). Приведены особенности аппарата СП и преимущества его использования. Обоснована актуальность разработки и использования инструментальных средств для работы с СП. Проведен сравнительный анализ возможностей программных средств, включающий сравнение функций анализа и синтеза, возможностей по созданию библиотек, поддержки кроссплатформенности и др. Сделаны выводы о сферах применения описанного ПО.

***Ключевые слова**: сети Петри, дискретно-событийное моделирование, программное обеспечение для сетей Петри, CPN Tools, AnyLogic, MATLAB, APT, APO, PIPE, TAPAAL, СП с синхронизированными дугами, раскрашенные СП, PNML*

Введение

Сети Петри (СП) впервые были описаны в 1962 г. немецким математиком Карлом Петри и к настоящему времени приобрели широкое применение во многих отраслях научных и практических исследований, связанных с анализом параллельно протекающих процессов и процедур использования разделяемых ресурсов. СП являются удобным математическим аппаратом для формализации, анализа и моделирования дискретно-событийных систем, они могут использоваться для эффективного моделирования различных технологических процессов [1, 6]. Анализ моделей вычислительных систем и устройств, выраженных в терминах СП (СП-моделей), позволяет на ранних этапах проектирования оценить корректность алгоритмов взаимодействия как отдельных устройств, так и работу всей системы в целом.

В связи с этим разработка и использование инструментальных средств, позволяющих наиболее полно и эффективно проводить анализ СП-моделей, не потеряло своей актуальности и в настоящий момент.

В данной работе проведен сравнительный анализ возможностей современных программных средств, моделирующих работу СП. В настоящее время существует ряд пакетов, исследующих свойства СП. В основном данные средства разработаны и поддерживаются университетскими командами, но есть и пакеты, которые созданы и поддерживаются другими разработчиками. К ним, например, можно отнести MATLAB и AnyLogic. Однако стоит заметить, что работа в этих средах с СП возможна только с помощью сторонних библиотек.

Рассмотрим основные функциональные возможности современных пакетов, моделирующих работу и проводящих анализ СП.

CPN Tools

CPN Tools — одна из самых известных программ для моделирования СП. Данное программное обеспечение (ПО) является открытым и свободным [19]. Его разработкой занимается рабочая группа Университета Орхуса из Дании. Оно работает с мощным классом сетей, называемых иерархическими временными раскрашенными СП.

CPN Tools используется в большом числе реальных проектов, особенно в области телекоммуникаций, для построения и анализа СП-моделей.

Основными функциями CPN Tools являются: создание СП-моделей, анализ их поведения с помощью имитации динамики СП, а также построение и анализ пространства состояний модели. Кроме того, продукт позволяет по-

лучить информацию о таких свойствах СП, как живость и ограниченность.

CPN Tools позволяет проводить пошаговую имитацию для поиска и устранения ошибок в разрабатываемой модели, а также автоматическое выполнение определенного числа шагов. Кроме того, в CPN Tools включен специальный язык программирования для описания атрибутов элементов сети [2, 3].

Стоит отметить, что в CPN Tools присутствует функционал, который позволяет создавать пользовательские расширения на Java. Данный продукт поддерживает экспорт в формат PNML (Petri Net Markup Language), что обеспечивает совместимость с другими программными продуктами [23]. PNML — гибкий, основанный на XML формат, являющийся стандартом ISO/IEC, поддерживается рядом программных продуктов и подходит для описания параллельных систем [9, 12].

К недостаткам CPN Tools можно отнести низкую скорость работы, а также своеобразный интерфейс, который может быть непривычен новичкам. Кроме того, последние версии CPN Tools поддерживают работу только с Windows. Работа на других операционных системах (ОС) возможна с помощью виртуальной машины или Wine — программного обеспечения, позволяющего запускать ПО для Windows на таких ОС, как macOS, Linux и др. [20, 28].

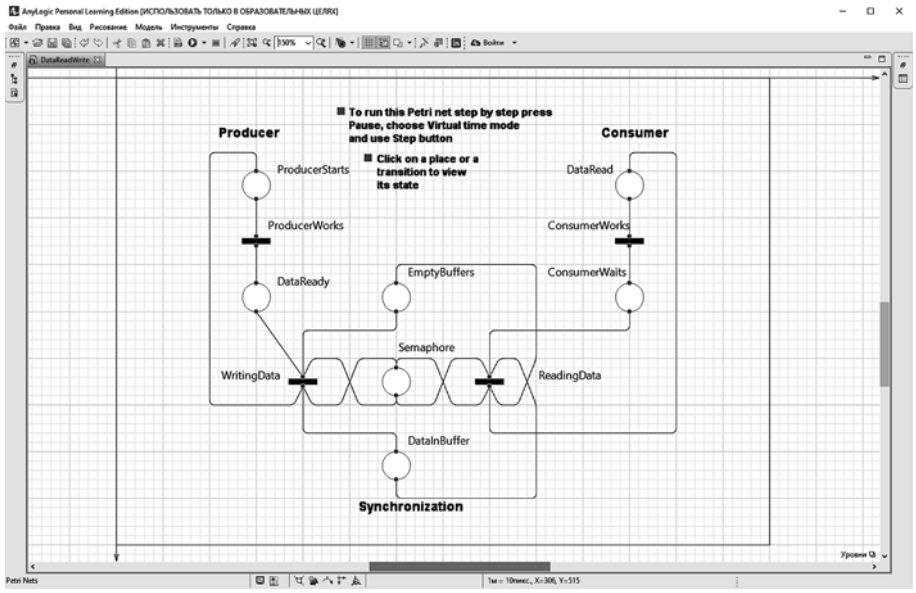


Рис. 1. Фрагмент сети Петри, построенной в AnyLogic

AnyLogic

AnyLogic — коммерческая среда для имитационного моделирования, которая обладает бесплатной версией для использования в образовательном процессе. Однако бесплатная версия обладает рядом ограничений, включая, например, невозможность динамического создания более 50 000 агентов [4, 8].

Разработкой данного ПО занимается многонациональная команда из России, Европы и США. AnyLogic объединяет в себе несколько методов моделирования и используется во множестве коммерческих организаций и учебных заведений по всему миру [7].

AnyLogic написан на Java в Eclipse и является кроссплатформенным программным обеспечением. ПО позволяет манипулировать моделью как с помощью графического интерфейса, так и с использованием языка программирования Java. AnyLogic располагает возможностью изменения параметров модели во время ее выполнения, что позволяет наглядно демонстрировать динамику моделируемой системы. Преимуществом данного продукта является наличие библиотеки объектов, которая позволяет создавать гибкие модели с наглядной визуализацией моделируемого процесса [5].

При создании AnyLogic не был нацелен на использование исключительно только СП, тем не менее, данный инструментарий предоставляет широкую базу для построения СП-моделей. В справке AnyLogic есть пример, позволяющий работать с СП, который используется в работе [18] для решения задачи об обедающих философах.

На рис. 1 представлен фрагмент СП, построенный в среде AnyLogic.

MATLAB Petri Net Toolbox

Petri Net Toolbox (PN Toolbox) представляет собой ПО, встроенное в окружение MATLAB. Согласно работе [21] поддерживается только одна платформа — Windows.

PN Toolbox разработан на кафедре автоматического управления и промышленной информатики Ясского технического университета им. Георге Асаки. Оно позволяет проводить моделирование и анализ СП-моделей.

ПО обладает графическим интерфейсом, и с его помощью возможно построить дерево до-

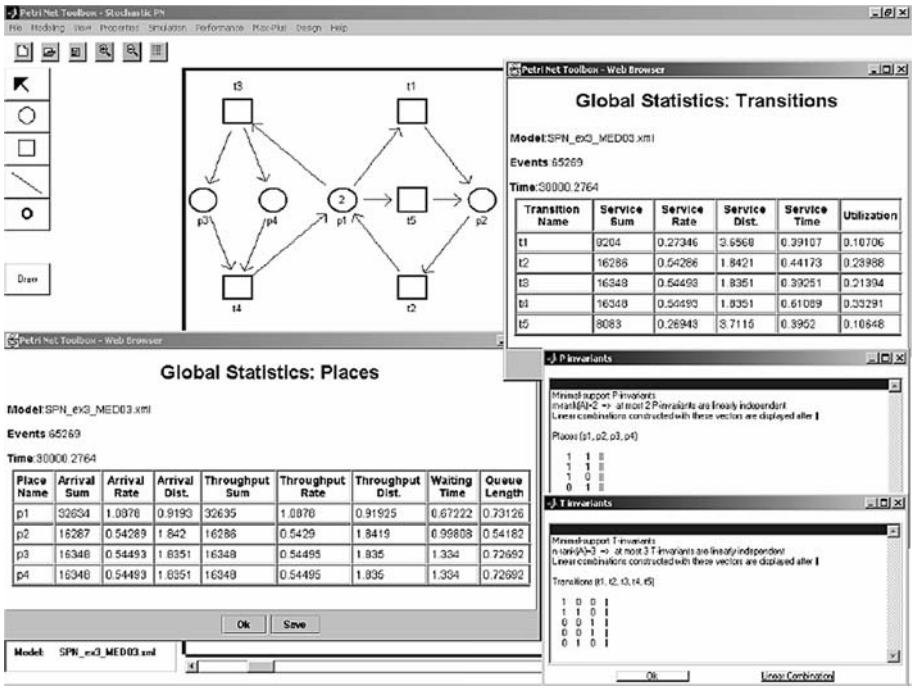


Рис. 2. Различная информация о СП, построенной в PN Toolbox

стижимых разметок (ДДР), которое может быть представлено как в виде списка, так и в виде графа; присутствует возможность отобразить СП в виде матриц инцидентности. Стоит отметить, что данный продукт позволяет определить свойства сети (ограниченность, живость и др.). Кроме того, PN Toolbox поддерживает расширения СП, включая стохастические и временные.

На рис. 2 представлена построенная в PN Toolbox СП и различная информация о ее функционировании [21, 22].

APT

APT является открытым и свободным программным обеспечением. Данный продукт, появившийся как проект студенческой группы университета Ольденбурга, написан на Java и может быть запущен на любой ОС, которая поддерживает JVM.

APT позволяет построить ДДР, отобразить матрицу инцидентности, а также определить такие свойства сети, как живость, ограниченность, наличие конфликтов и др.

APT поддерживает синтез СП из помеченного графа, однако данная функция имеет ряд ограничений при синтезе параллельных фрагментов СП. При необходимости пользователь может выбрать свойства, которым должна соответствовать создаваемая СП [14].

APT поддерживает работу с форматом PNML, а также обладает модульной структурой, что позволяет легко расширять его функционал [10, 14].

APT представляет собой консольную утилиту, однако существует проект APT-GUI, который позволяет работать с APT в графическом окружении (рис. 3) [15].

APO

APO представляет собой веб-интерфейс для APT, написанный на языке программирования CoffeeScript. Данный продукт позволяет проводить имитацию, анализ и синтез СП в браузере.

Среди функций анализа присутствуют построение ДДР (рис. 4) и оценка таких свойств сети, как ограниченность, однородность, безопасность, живость и др. [17]. APO имеет недостатки, аналогичные ПО APT.

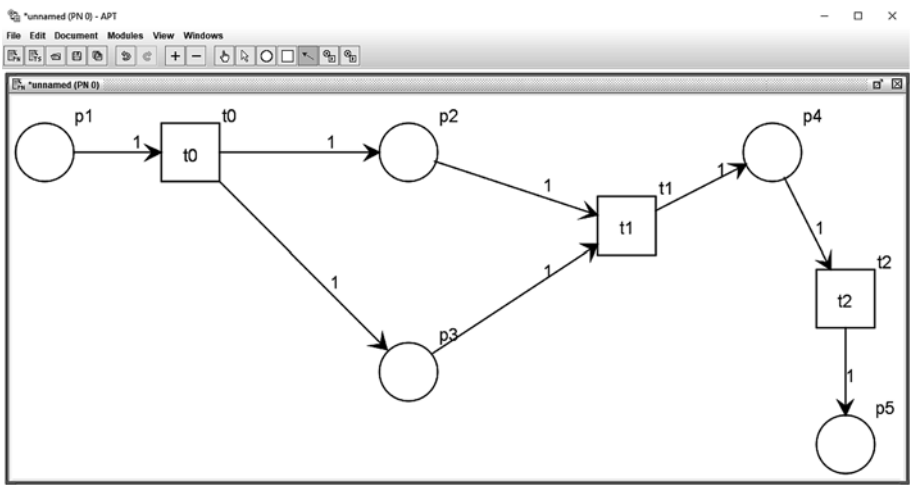


Рис. 3. Графический интерфейс APT-GUI

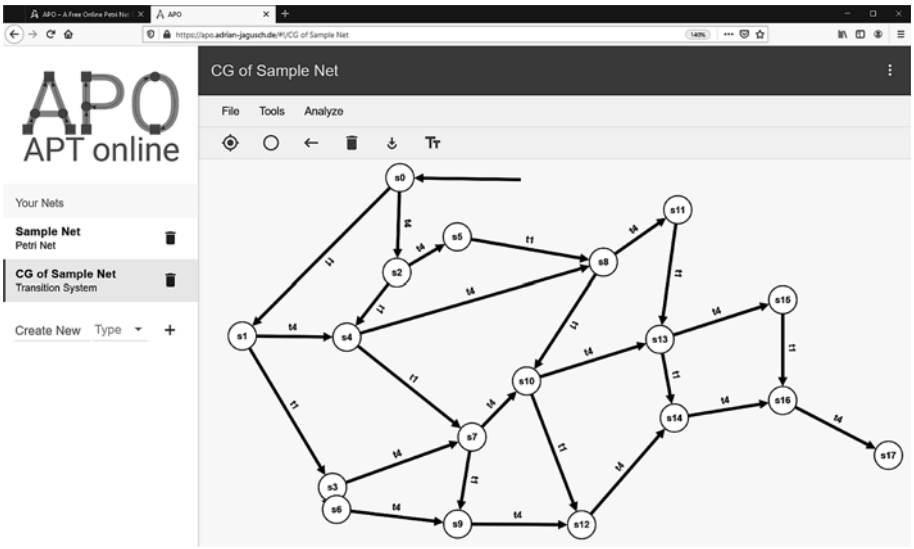


Рис. 4. ДДР сети Петри, построенной в APO

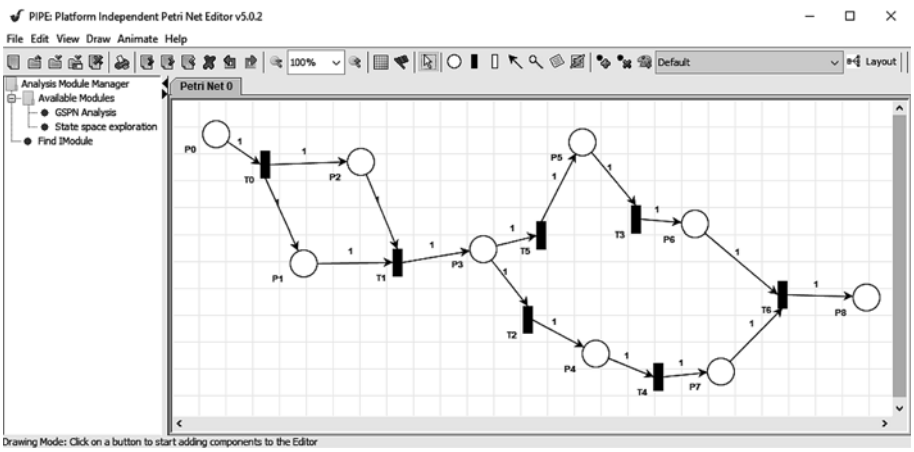


Рис. 5. Фрагмент программы, отображающий сеть Петри

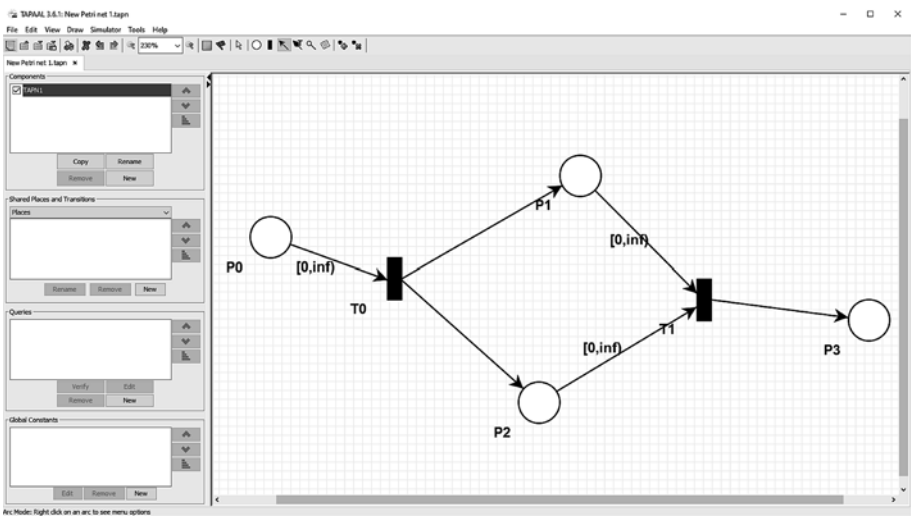


Рис. 6. Отображение графовой модели в TAPAAL

PIPE

PIPE — кроссплатформенное программное обеспечение с открытым исходным кодом для разработки и анализа СП. ПО поддерживает работу с обобщенными стохастическими СП. Оно написано на языке программирования Java, а его разработка ведется с 2002—2003 г. на кафедре вычислительной техники Имперского колледжа Лондона [16, 24].

PIPE обладает графическим интерфейсом (рис. 5) и располагает механизмом для интеграции новых функций через подключаемые модули, что выгодно отличает его от других инструментов, функционал которых не может быть расширен пользователем.

PIPE поддерживает режим имитации работы СП, а также имеет модули, позволяющие отобразить матрицы инцидентности, строить ДДР. Кроме того, ПО позволяет определить свойства СП, включая живость и ограниченность, а также провести анализ ее производительности.

Следует отметить, что PIPE поддерживает работу с форматом PNML [24].

TAPAAL

TAPAAL представляет собой программное обеспечение с открытым исходным кодом, разработка которого ведется в университете Ольборга. Данный продукт является кроссплатформенным и написан с использованием языков C++ и Java [13, 25].

Функции для анализа СП включают имитацию работы, анализ достижимости разметки и верификацию СП [9, 13].

ПО обладает графическим интерфейсом, который основан на наработках проекта PIPE (рис. 6) [26].

TAPAAL поддерживает работу СП с синхронизированными дугами. Этот тип СП является временным расширением классических СП. В нем каждая метка имеет свой возраст, а дуги, идущие к переходам, помечены временными интервалами, пропускающими метки с возрастом именно из этого диапазона (интервала) [13, 27].

ПО позволяет использовать ингибиторные дуги. Кроме того, поддерживается импорт и экспорт СП в PNML [9, 26].

Сравнительный анализ программных средств моделирования сетей Петри

Результаты анализа возможностей программных пакетов для моделирования СП сведены в представленную ниже таблицу.

Программные пакеты сравнивались по девяти критериям:

1. Возможность запуска на нескольких операционных системах (*Кроссплатформенное ПО*).
2. Язык программирования, на котором написано ПО (*язык программирования*).

Характеристики	CPN Tools	MATLAB Petri Net Toolbox	AnyLogic	APT	TAPAAL	PIPE	APO
Кроссплатформенное ПО	Нет	Да					Да[1]
Язык программирования	BETA/Standart ML/Java	Н/Д	Java	Java	Java/C++	Java	CoffeeScript
Графический интерфейс	Да			Да[2]	Да		
Поддержка сторонних библиотек	Да	Н/Д		Да	Н/Д	Да	Н/Д
Тип лицензии	Свободная	Коммерческая[3]	Коммерческая[4]	Свободная			
PNML	Да	Н/Д		Да	Да	Да	Н/Д
Синтез СП	Н/Д	Н/Д	Н/Д	Синтез из графа переходов	Н/Д	Н/Д	Синтез из графа переходов
Анализ СП	Оценка свойств сети	ДДР	Имитация работы	ДДР	Имитация работы	ДДР[5]	ДДР
		Оценка свойств сети					
	Имитация работы	Матричное представление		Матричное представление		Матричное представление[5]	Оценка свойств сетей
		Имитация работы		Оценка свойств сетей	Анализ достижимости	Имитация работы[5]	Имитация работы
				Имитация работы[6]	Верификация СП	Оценка свойств сетей[5]	
Расширения СП	Иерархические временные раскрашенные СП	Временные СП	Н/Д	Н/Д	СП с синхронизированными дугами	Обобщенные стохастические СП	Н/Д
		Стохастические СП					
		Обобщенные стохастические СП					

[1]Открывается в браузере, т. е. может быть запущено через браузер на различных ОС.
[2]Проект apt-gui позволяет работать с apt в графическом окружении.
[3]Для работы необходим MATLAB.
[4]Присутствует бесплатная версия для использования в образовательном процессе.
[5]Согласно [16] часть функций для анализа отсутствует в PIPE 5.
[6]Имитация возможна при использовании apt-gui.

3. Наличие в ПО графического интерфейса (*графический интерфейс*).

4. Возможность добавления новых функций в ПО путем создания пользовательских модулей (*поддержка сторонних библиотек*).

5. Тип лицензии, под которой распространяется ПО (*тип лицензии*).

6. Поддержка формата PNML (*PNML*).

7. Возможность построения (синтеза) СП на основе каких-либо входных данных.

7.1. *Синтез СП из графа переходов* — возможность синтеза из графа переходов СП, соответствующей выбранным пользователем свойствам (таким как безопасность, живость и т. д.).

8. Возможность анализа СП (*ДДР*).

8.1. *Оценка свойств сетей* — возможность анализа СП на ограниченность, однородность и т. д.

8.2. *ДДР* — возможность построения дерева достижимых разметок для СП.

8.3. *Матричное представление* — возможность представления СП в матричном виде.

8.4. *Имитация работы* — возможность пошаговой имитации работы СП.

8.5. *Верификация* — возможность верификации СП.

9. Возможность работы с расширениями СП *(расширения СП).*

Заключение

В статье проведен сравнительный анализ некоторых используемых в настоящее время средств для работы с сетями Петри. По результатам проведенного анализа можно сделать следующие выводы.

CPN Tools используется в большом числе реальных проектов и, пожалуй, является наиболее известным ПО для работы с СП [2, 3]. В силу своих возможностей данное ПО может быть использовано для проектирования систем со сложным взаимодействием между компонентами. Ввиду того, что этот продукт не является кроссплатформенным, он может быть запущен только на Windows [20]. Также стоит заметить, что ПО обладает своеобразным интерфейсом, который бывает непривычен новичкам.

AnyLogic и MATLAB обладают широким функционалом, позволяющим исследовать не только СП. Благодаря этому данные продукты дают специалисту большие возможности при условии приобретения коммерческой лицензии [8]. Стоит заметить, что для работы в этих средах с СП необходима установка дополнительных расширений [18, 21, 22].

APT является достаточно функциональным и (что немаловажно) кроссплатформенным продуктом [14]. Однако данное ПО не обладает графическим интерфейсом (доступна только командная строка). Таким образом, чтобы воспользоваться его функционалом через графический интерфейс, пользователю придется воспользоваться проектом APT-GUI [14, 15]. APT может быть использован, во-первых, как ПО для проектирования дискретно-событийных систем и, во-вторых, как библиотека в разрабатываемых проектах [11, 14].

APO отличается тем, что обладает простым интерфейсом и запускается прямо в браузере [17]. Данный продукт подойдет для использования в образовательном процессе в целях обучения основам аппарата СП.

PIPE обладает графическим интерфейсом, широким функционалом и может быть запущен на различных платформах [16, 24]. Кроме того, пользователь дополнительно может расширить функционал PIPE с помощью подключаемых модулей [24]. Данный программный продукт может быть использован при проектировании сложных систем, анализ которых подразумевает вероятностные и временные оценки.

TAPAAL является кроссплатформенным ПО, обладающим графическим интерфейсом, основанным на наработках проекта PIPE [13, 26]. Данный программный продукт может быть использован, если есть необходимость работать с СП с синхронизированными дугами, в которых метки могут быть связаны с функциями времени [13, 27].

В заключение можно отметить, что аппарат СП в настоящее время остается актуальным средством формализации, анализа и моделирования дискретно-событийных систем разного уровня сложности, и для работы с ним существует набор постоянно развивающихся функционально ориентированных программных модулей.

Список литературы

1. **Булавский П. Е., Ваисов О. К.** Формализация процессов электронного документооборота технической документации с помощью сетей Петри // Автоматика на транспорте. 2018. № 4. URL: https://cyberleninka.ru/article/n/formalizatsiya-protsessov-elektronnogo-dokumentooborota-tehnicheskoy-dokumentatsii-s-pomoschyu-setey-petri (дата обращения: 02.04.2020).

2. **Дмитриев В. Н., Тушнов А. С., Сергеева Е. В.** Имитационное моделирование системы мониторинга многозвенной сети передачи данных // Вестник АГТУ. Серия: Управление,

вычислительная техника и информатика. 2013. № 2. URL: https://cyberleninka.ru/article/n/imitatsionnoe-modelirovanie-sistemy-monitoringa-mnogozvennoy-seti-peredachi-dannyh (дата обращения: 02.04.2020).

3. **Зайцев Д. А., Шмелева Т. Р.** Моделирование телекоммуникационных систем в CPN Tools: Учеб. пособ. по курсу "Математическое моделирование информационных систем" для подготовки магистров в отрасли связи. Одесса: ОНАТ, 2006. 60 с.

4. **Калугин А. И.** Оптимизационный эксперимент в среде AnyLogic // Наука и школа. 2015. № 4. URL: https://cyberleninka.ru/article/n/optimizatsionnyy-eksperiment-v-srede-anylogic (дата обращения: 02.04.2020).

5. **Маликов Р. Ф.** Практикум по имитационному моделированию сложных систем в среде AnyLogic 6 / Учеб. пособ. Уфа: Изд-во БГПУ, 2013. 296 с.

6. **Питерсон Дж.** Теория сетей Петри и моделирование систем. М.: Мир, 1984. 264 с.

7. О **компании** — инструмент имитационного моделирования AnyLogic // AnyLogic: имитационное моделирование для бизнеса. URL: https://www.anylogic.ru/company/about-us/ (дата обращения: 03.10.2020).

8. **Скачать** — инструмент имитационного моделирования AnyLogic // AnyLogic: имитационное моделирование для бизнеса. URL https://www.anylogic.ru/downloads/ (дата обращения: 03.10.2020).

9. **Amparore E., Berthomieu B., Ciardo G., Dal Zilio S., Gall F., Hillah L. M., Hulin-Hubard F., Jensen P. G., Jezequel L., Kordon F., Le Botlan D., Liebke T., Meijer J., Miner A.,Paviot-Adet E., Srba J., Thierry-Mieg Y., van Dijk T., Wolf K.** Presentation of the 9th Edition of the Model Checking Contest // TACAS 2019: Tools and Algorithms for the Construction and Analysis of Systems. Lecture Notes in Computer Science. 2019. Vol. 11429. P. 50—68. doi:10.1007/978-3-030-17502-3_4.

10. **apt/extending.md** at master · CvO-Theory/apt · GitHub. URL: https://github.com/CvO-Theory/apt/blob/master/doc/extending.md (дата обращения: 28.09.2020).

11. **apt/obtaining.md** at master · CvO-Theory/apt · GitHub. URL: https://github.com/CvO-Theory/apt/blob/master/doc/obtaining.md (дата обращения: 13.09.2020).

12. **Billington J., Christensen S., van Hee K., Kindler E., Kummer O., Petrucci L., Post R., Stehno C., Weber M.** The Petri Net Markup Language: Concepts, Technology, and Tools // ICATPN 2003: Applications and Theory of Petri Nets 2003. Lecture Notes in Computer Science. 2003. Vol. 2679. P. 483—505. doi:10.1007/3-540-44919-1_31.

13. **David A., Jacobsen L., Jacobsen M., Jørgensen K. Y., Møller M. H., Srba J.** (2012) TAPAAL 2.0: integrated development environment for timed-arc Petri nets // TACAS 2012: Tools and Algorithms for the Construction and Analysis of Systems. Lecture Notes in Computer Science. 2012. Vol. 7214. P. 492—497. doi:10.1007/978-3-642-28756-5_36.

14. **Best E., Schlachter U.** Analysis of Petri Nets and Transition System // ICE 2015: 8th Interaction and Concurrency Experience, EPTCS 189. P. 53—67. doi:10.4204/EPTCS.189.6.

15. **GitHub** — CvO-Theory/apt-gui. URL: https://github.com/CvO-Theory/apt-gui (дата обращения: 20.04.2020).

16. **GitHub** — sarahtattersall/PIPE: PIPE — Platform Independent Petri Net Editor. URL: https://github.com/sarahtattersall/PIPE (дата обращения: 20.07.2020).

17. **GitHub** — stromhalm/apo: An Application for online Petri net design and analysis. URL: https://github.com/stromhalm/apo (дата обращения: 20.07.2020).

18. **Leskovar R., Tanzler J., Bicher M.** Petri Net Modelling and Simulation in AnyLogic and MATLAB for ARGESIM Benchmark C4 "Dining Philosophers" // SNE Educational Note. 2014. Vol. 24, N. 1. P. 55—58.

19. **Licenses** — CPN Tools. URL: http://cpntools.org/category/licenses/ (дата обращения: 02.04.2020).

20. **Linux/Mac OS X** — CPN Tools. URL: http://cpntools.org/2018/01/15/linux-mac-os-x/ (дата обращения: 02.04.2020).

21. **MATLAB** Petri Net Toolbox — File Exchange — MATLAB Central. URL: https://www.mathworks.com/products/connections/product_detail/petri-net-toolbox.html (дата обращения: 02.04.2020).

22. **Matcovschi M. H., Mahulea C., Pastravanu O.** Petri Net Toolbox for MATLAB // Proceedings of the 11th IEEE Mediterranean Conference on Control and Automation MED'03. URL: https://www.researchgate.net/publication/242388510_Petri_Net_Toolbox_for_MATLAB (дата обращения 11.06.2020).

23. **Westergaard M.** CPN Tools 4: Multi-formalism and Extensibility // Application and Theory of Petri Nets and Concurrency, vol. 7927 pp. 400—409. Berlin, Heidelberg: Springer. doi:10.1007/978-3-642-38697-8_22.

24. **Dingle N. J., Knottenbelt W. J., Suto T.** PIPE2: A Tool for the Performance Evaluation of Generalised Stochastic Petri Nets (PDF format). ACM SIGMETRICS Performance Evaluation Review (Special Issue on Tools for Computer Performance Modelling and Reliability Analysis). March 2009. Vol. 36(4). P. 34—39.

25. **tapaal.net**: Download. URL: http://www.tapaal.net/download/ (дата обращения: 27.07.2020).

26. **tapaal.net:** Features. URL: http://www.tapaal.net/features/ (дата обращения: 21.07.2020).

27. **tapaal.net:** Introduction. URL: http://www.tapaal.net/ (дата обращения: 18.09.2020).

28. **WineHQ** — Run Windows applications on Linux, BSD, Solaris and macOS. URL: https://www.winehq.org/ (дата обращения: 03.10.2020).

V. P. Kulagin, D. Tech. Sc., Professor, e-mail: kulagin@mirea.ru,
A. A. Loginov, Postgraduate Student, e-mail: loginov.a.a@edu.mirea.ru,
RTU MIREA, Moscow, 107996, Russian Federation

Analysis of Software Tools for Working with Petri Nets

There is provides an overview of the existing software for modeling using Petri nets. The features of the Petri nets and the advantages of its use are presented. The relevance of the development and use of tools for working with Petri nets is reasonable. A comparative analysis of the capabilities of software tools, including a comparison of the analysis and synthesis functions, the capabilities of creating libraries, cross-platform support, etc. Conclusions are drawn about the spheres of application of the described software.

Keywords*: petri nets, discrete-event simulation, petri net modeling software, CPN Tools, AnyLogic, MATLAB, APT, APO, PIPE, TAPAAL, Timed-Arc Petri net, Coloured Petri net*

DOI: 10.17587/it.27.89-96

References

1. **Bulavskii P. E., Vaisov O. K.** Formalization of electronic document management processes for technical documentation using Petri nets, *Avtomatika na Transporte,* 2018, no. 4, available at: https://cyberleninka.ru/article/n/formalizatsiya-protsessov-elektronnogo-dokumentooborota-tehnicheskoy-dokumentatsii-s-pomoschyu-setey-petri (date of access: 02.04.2020, in Russian).

2. **Dmitriev V. N., Tushnov A. S., Sergeeva E. V.** Simulation modeling of a multi-link data transmission network monitoring system, *Vestnik AGTU, Seriya: Upravlenie, vychislitel'naya tekhnika i informatika*, no. 2, 2013, available at: https://cyberleninka.ru/article/n/imitatsionnoe-modelirovanie-sistemy-monitoringa-mnogozvennoy-seti-peredachi-dannyh (date of access: 02.04.2020, in Russian).

3. **Zaitsev D. A., Shmeleva T. R.** Simulating of telecommunication systems with CPN Tools, Odessa, ONAT, 2006, 60 p. (in Russian).

4. **Kalugin A. I.** Optimization experiment in the AnyLogic environment (Optimizatsionnyi ehksperiment v srede AnyLogic), *Nauka i shkola*, no. 4, 2015, available at: https://cyberleninka.ru/article/n/optimizatsionnyy-eksperiment-v-srede-anylogic (date of access: 02.04.2020, in Russian).

5. **Malikov R. F.** Workshop on simulation of complex systems in the AnyLogic 6 environment, Ufa, BGPU, 2013, 296 p. (in Russian).

6. **Peterson J.** Petri net theory and system modeling, Moscow, Mir, 1984, 264 p. (in Russian).

7. **About us** — AnyLogic Simulation Software, available at: https://www.anylogic.ru/company/about-us/ (date of access: 03.10.2020)

8. **Downloads** — AnyLogic Simulation Software, available at: https://www.anylogic.ru/downloads/ (date of access: 03.10.2020).

9. **Amparore E., Berthomieu B., Ciardo G., Dal Zilio S., Gall F., Hillah L. M., Hulin-Hubard F., Jensen P. G., Jezequel L., Kordon F., Le Botlan D., Liebke T., Meijer J., Miner A.,Paviot-Adet E., Srba J., Thierry-Mieg Y., van Dijk T., Wolf K.** Presentation of the 9th Edition of the Model Checking Contest, *TACAS 2019: Tools and Algorithms for the Construction and Analysis of Systems, Lecture Notes in Computer Science*, *2019,* vol. 11429, pp. 50—68, Cham, Springer, doi:10.1007/978-3-030-17502-3_4.

10. **apt/extending.md** at master · CvO-Theory/apt · GitHub, available at: https://github.com/CvO-Theory/apt/blob/master/doc/extending.md (date of access: 28.09.2020).

11. **apt/obtaining.md** at master · CvO-Theory/apt · GitHub, available at: https://github.com/CvO-Theory/apt/blob/master/doc/obtaining.md (date of access: 13.09.2020).

12. **Billington J., Christensen S., van Hee K., Kindler E., Kummer O., Petrucci L., Post R., Stehno C., Weber M.** The Petri Net Markup Language: Concepts, Technology, and Tools, *ICATPN 2003: Applications and Theory of Petri Nets 2003, Lecture Notes in Computer Science*, 2003, vol. 2679, pp. 483—505, Berlin, Heidelberg, Springer, doi:10.1007/3-540-44919-1_31.

13. **David A., Jacobsen L., Jacobsen M., Jørgensen K. Y., Møller M. H., Srba J**. (2012) TAPAAL 2.0: integrated development environment for timed-arc Petri nets, *TACAS 2012: Tools and Algorithms for the Construction and Analysis of Systems, Lecture Notes in Computer Science*, 2012, vol. 7214, pp. 492—497, Berlin, Heidelberg, Springer, doi:10.1007/978-3-642-28756-5_36.

14. **Best E., Schlachter U.** Analysis of Petri Nets and Transition System, *ICE 2015: 8th Interaction and Concurrency Experience*, *EPTCS* 189, pp. 53—67, doi:10.4204/EPTCS.189.6.

15. **GitHub** — CvO-Theory/apt-gui, available at: https://github.com/CvO-Theory/apt-gui (date of access: 20.04.2020).

16. **GitHub** — sarahtattersall/PIPE: PIPE — Platform Independent Petri Net Editor, available at: https://github.com/sarahtattersall/PIPE (date of access: 20.07.2020).

17. **GitHub** — stromhalm/apo: An Application for online Petri net design and analysis, available at: https://github.com/stromhalm/apo (date of access: 20.07.2020).

18. **Leskovar R., Tanzler J., Bicher M.** Petri Net Modelling and Simulation in AnyLogic and MATLAB for ARGESIM Benchmark C4 "Dining Philosophers", *SNE Educational Note*, 2014, vol. 24, N. 1. P. 55—58.

19. **Licenses** — CPN Tools, available at: http://cpntools.org/category/licenses/ (date of access: 02.04.2020).

20. **Linux/Mac OS X** — CPN Tools, available at: http://cpntools.org/2018/01/15/linux-mac-os-x/ (date of access: 02.04.2020).

21. **MATLAB** Petri Net Toolbox — File Exchange — MATLAB Central, available at: https://www.mathworks.com/products/connections/product_detail/petri-net-toolbox.html (date of access: 02.04.2020).

22. **Matcovschi M. H., Mahulea C., Pastravanu O.** Petri Net Toolbox for MATLAB, *Proceedings of the 11th IEEE Mediterranean Conference on Control and Automation MED'03*, available at: https://www.researchgate.net/publication/242388510_Petri_Net_Toolbox_for_MATLAB (date of access 11.06.2020).

23. **Westergaard M.** CPN Tools 4: Multi-formalism and Extensibility, *Application and Theory of Petri Nets and Concurrency*, vol. 7927, pp. 400—409, Berlin, Heidelberg, Springer, doi:10.1007/978-3-642-38697-8_22.

24. **Dingle N. J., Knottenbelt W. J., Suto T.** PIPE2: A Tool for the Performance Evaluation of Generalised Stochastic Petri Nets (PDF format), *ACM SIGMETRICS Performance Evaluation Review (Special Issue on Tools for Computer Performance Modelling and Reliability Analysis),* March 2009, vol. 36(4), pp. 34—39.

25. **tapaal.net**: Download, available at: http://www.tapaal.net/download/ (date of access: 27.07.2020).

26. **tapaal.net**: Features, available at: http://www.tapaal.net/features/ (date of access: 21.07.2020).

27. **tapaal.net**: Introduction, available at: http://www.tapaal.net/ (date of access: 18.09.2020).

28. **WineHQ** — Run Windows applications on Linux, BSD, Solaris and macOS, available at: https://www.winehq.org/ (date of access: 03.10.2020).

УДК 004.021 + 519.688 DOI: 10.17587/it.27.97-101

А. Б. Терентьев, аспирант, e-mail: alexey.terentjev@gmail.com,
И. В. Штурц, ст. науч. сотр., канд. техн. наук, email: ishturts@gmail.com,
Санкт-Петербургский политехнический университет Петра Великого

Устранение алиасинга в допплеровской эхокардиографии с помощью фильтрации субмаксимальных компонент скоростей

Рассматривается задача устранения алиасинга в допплерографии. Все существующие алгоритмы являются приближенными, самые точные требуют значительного времени для обработки. Предлагается метод, устраняющий алиасинг лишь в областях, где вероятность его появления высока, а также поддерживающий возможность обработки в реальном времени. Эксперименты на реальных данных кровотока в сердцах животных подтвердили высокую точность определения областей алиасинга и показали возможность включения алгоритма в обработку в реальном времени.

Ключевые слова: *допплеровская эхокардиография, алиасинг, лес непересекающихся множеств, связные компоненты*

Введение

Двухмерная допплеровская эхокардиография является одним из основных и наиболее распространенных методов диагностики сердечно-сосудистых заболеваний. Основными его достоинствами по сравнению с аналогами являются: относительно низкая цена оборудования, его компактность, а также неинвазивность ультразвукового исследования. Одним из основных артефактов допплерографии является алиасинг (алайзинг, англ. *aliasing*), заключающийся в том, что кровоток со скоростями, превышающими лимит, обусловленный параметрами съемки, отображается как обратный (рис. 1, см. вторую сторону обложки).

Несмотря на достаточно серьезное влияние алиасинга на диагностику некоторое число ранних исследований, посвященных изучению кровотока с помощью допплерографии, либо предлагали достаточно ненадежные или ручные методы [1—3] или вовсе игнорировали данную проблему [4—6]. В трехмерной эхокардиографии предлагался подход, основанный на нечеткой логике [7]. В то же время в метеорологии, где данные с радаров также подвержены алиасингу, имелся ряд работ, предлагающих достаточно эффективные решения [8—11]. Часть из них основывалась на том, чтобы рассчитывать скорость в ячейке с учетом значений в соседних ячейках. Данный подход вдохновил исследователей на работу [12], в которой было реализовано автоматическое устранение шумов и алиасинга. Тем не менее, данный подход имел достаточно серьезные ограничения в применении в случае наличия хаотичного кровотока, который часто может возникать при различных патологиях клапанов сердца. В работе [13] используется схожий подход, в котором корректировка происходит с помощью графа, построенного по областям с одинаковыми скоростями. Однако в дальнейшем данный метод был признан проигрышным (незначительно) по сравнению с регуляризацией [15], в работе [14] показана неэффективность использования информации с соседних кадров. Кроме этого, существует набор подходов, использующих оператора для определения региона алиасинга [16].

Проблема подхода, рассмотренного в работе [13], заключается в том, что могут случаться ложные срабатывания в случае турбулентного потока, а также в силу того, что потоки, отделенные тонкими тканями, считаются алгоритмом смежными. Подход, представленный в работе [15], немного лучше устраняет алиасинг, но порождает искусственные скорости, пытаясь воссоздать связный поток. Кроме того, время обработки в данном методе значительно увеличилось.

Ложные срабатывания при поиске алиасинга могут оказать крайне негативное значение на диагностику. Нередко может оказаться более полезным не изменять исходную картину, оставляя решение вопроса радиологу. Кроме того, параметры съемки обычно подбираются

так, что многократный алиасинг крайне маловероятен. Таким образом, существует необходимость в реализации метода устранения алиасинга, который устранял бы алиасинг только в областях с высокими скоростями обратных направлений, смежных друг с другом.

В данной статье предлагается такой метод, который, ко всему прочему, может быть включен в комплексы программ для обработки допплерографических данных в реальном времени.

Описание алгоритма

Работа алгоритма основана на предположении, что параметры съемки выбраны так, что большая часть кровотока не подвержена алиасингу. Общая идея алгоритма заключается в том, что на границе областей с алиасингом находятся ячейки с большой разницей в скоростях противоположных направлений — критические границы скоростей. Кроме того, будем предполагать, что алиасинг не имеет слишком больших амплитуд и содержится только в областях субмаксимальных, приближенных к максимальным, скоростей. Кроме того, алгоритм предполагает предварительное отделение данных кровотока или их исходное наличие в результатах съемки.

◊ *Схема алгоритма*

Общая схема работы алгоритма выглядит следующим образом:

1. Составление маски алиасинга. Для каждого кадра выполняется:

1) разбиение данных кровотока на связные компоненты. Используются 5 групп — фон (отсутствие скорости или ткань), а также субмаксимальные и не субмаксимальные скорости в обоих направлениях;

2) поиск критических компонент (областей), а также составление критических регионов — наборов компонент, смежных с критическими;

3) обработка критических регионов. Поиск доминирующего направления в регионе. Запись внутренних компонент не доминирующего направления в маску.

2. Обработка кадров по маскам. Определение нового регистрируемого диапазона скоростей с помощью масок. Устранение алиасинга на каждом кадре с помощью маски и нового диапазона.

◊ *Входные данные*

Входными данными алгоритма устранения алиасинга являются: набор матриц $\{\mathbf{F}_i\}_{i=1}^{n}$ где $\mathbf{F}_i$ — данные кровотока i-го кадра, изображения размером $h_f \times w_f$, n — число кадров; граница модуля субмаксимальной скорости u; критическая разница скоростей алиасинга v_c — минимальная разница между скоростями на границе противоположных направлений; c_d — минимальная разница весов противоположных направлений для изменения скоростей в критическом регионе.

◊ *Выходные данные*

Результатом работы алгоритма являются пересчитанные значения интенсивностей пикселов в данных кровотока $\{\mathbf{F}'_i\}_{i=1}^{n}$.

◊ *Разбиение изображения на связные компоненты*

В предложенном алгоритме идет разбиение всех пикселей кровотока на смежные области (компоненты) по категориям. Для пиксела $p(x, y)$, скорость кровотока в котором v, категории выглядят следующим образом:

- фон, нулевые данные кровотока $v = 0$ или ткани;
- области субмаксимального кровотока в сторону датчика, $v > 0$, $|v| \geqslant u$;
- области субмаксимального кровотока в сторону от датчика $v < 0$, $|v| \geqslant u$;
- области не субмаксимального кровотока в сторону датчика, $v > 0$, $|v| < u$;
- области не субмаксимального кровотока в сторону от датчика, $v < 0$, $|v| < u$.

В алгоритме предложено использование двух типов смежности (связности):

- *4-смежность*. Пиксел $p(x, y)$ смежен с пикселами $(x - 1, y)$, $(x + 1, y)$, $(x, y - 1)$, $(x, y + 1)$ в случае существования таковых. Будем обозначать множество таких пикселей $N_4(p)$;
- *8-смежность*. Пиксел $p(x, y)$ смежен с пикселами $(x - 1, y - 1)$, $(x, y - 1)$, $(x + 1, y - 1)$, $(x - 1, y)$, $(x + 1, y)$, $(x - 1, y + 1)$, $(x, y + 1)$, $(x + 1, y + 1)$ в случае существования таковых. Будем обозначать множество таких пикселей $N_8(p)$.

Работа с компонентами происходит с помощью *леса непересекающихся множеств* — структуры для непересекающихся множеств [17, стр. 285]. Структура для конечного множества S поддерживает его разбиение на непересекающиеся подмножества $S = X_0 \cup X_1 \cup X_2 \cup ... \cup X_k$: $X_l \cap X_q = \varnothing \ \forall l, q \in \{0, 1, ..., k\}, l \neq q$. Каждому подмножеству X_l назначается представитель $r_l \in X_l$. Структура поддерживает операции:

- *MakeSet*(x). Создает для x новое подмножество, назначая x его представителем;
- *Find*(x). Определяет для x его подмножество, возвращая представителя.
- *Union*(r, s). Объединяет множества с представителями r, s, назначая r представителем итогового множества.

С помощью системы непересекающихся множеств для кадра i получается матрица $\mathbf{C}_i$

размера $h_f \times w_f$ целых чисел, значения которых соответствуют номеру компоненты или равны 0 для фона. Число компонент будем обозначать m, таким образом $0 \leqslant \mathbf{C}_i[y,x] \leqslant m$. Множество всех компонент обозначим S_i. После разбиения для каждой компоненты c_j также подсчитывается параллельный осям ограничивающий прямоугольник B_j и его площадь A_j.

◊ *Поиск критических областей*

Как уже говорилось в описании идеи алгоритма, алиасинг характерен тем, что на границе областей, ему подверженных, смежные пикселы соответствуют скоростям, противоположным по направлению, с амплитудами, близкими к максимальным. Будем называть такие границы и области, которым они принадлежат, критическими. Параллельно составляются критические регионы — списки областей, либо непосредственно смежных с критическими, либо смежных с субмаксимальными областями в списке.

Для поиска таких областей выполняется обход всех компонент. Для каждой компоненты, отмеченной как субмаксимальная, осуществляется обход граничных пикселей p_b. Если в $N(p_b)$ находится пиксел с обратным направлением кровотока: $\exists p'_b \in N(p_b) : |\mathbf{F}[p_b] - \mathbf{F}[p'_b]| \geqslant v_c$, такая область помечается как критическая.

Набор критических регионов составляется с помощью все той же системы непересекающихся множеств, но уже основанной на списках [17, стр. 584].

◊ *Обработка критических регионов*

На данном шаге происходит уже непосредственное заполнение маски. Введем дополнительные понятия: R_{ik} — критический регион с индексом k кадра i; $V_{T_{ik}} = \sum_{\forall p \in S_{R_{ik}} : \mathbf{F}[p] > 0} \mathbf{F}[p]$ — сумма модулей скоростей в сторону датчика внутри региона k; $V_{B_{ik}} = \sum_{\forall p \in S_{R_{ik}} : \mathbf{F}[p] < 0} |\mathbf{F}[p]|$ — сумма модулей скоростей от датчика внутри региона; $A_{T_{ik}} = \sum_{j : c_j \in S_{R_{ik}},\ \mathbf{F}[c_j] > 0} A_j$ — сумма площадей областей региона со скоростями в сторону датчика; $A_{B_{ik}} = \sum_{j : c_j \in S_{R_{ik}},\ \mathbf{F}[c_j] < 0} A_j$ — сумма площадей областей региона со скоростями от датчика.

Тогда для каждого критического региона:

- вычисляются $O_{T_{ik}} = V_{T_{ik}} A_{T_{jk}}$ и $O_{B_{ik}} = V_{B_{ik}} A_{B_{ik}}$. Большее из этих значений будем обозначать O_{dk}, меньшее — O_{sk}, в данном сравнении выбирается доминирующее в регионе направление;
- если $\frac{O_{dk} - O_{sk}}{O_{dk}} < c_d$, обработка региона прекращается;
- далее происходит обход всех субмаксимальных областей критического региона. Если направление области не совпадает с доминирующим, она добавляется к маске путем применения побитового логического сложения.

◊ *Обработка кадров по маскам*

Далее с помощью вычисленных для каждого кадра масок подсчитывается новый максимальный модуль скорости путем полного перебора пикселов $\mathbf{F}_i$, пересекающихся с маской, и предварительного вычисления их итоговой скорости. После того как максимальный модуль найден, происходит пересчет всех данных кровотока по тому, как изменился диапазон отображения скоростей. Данные в процессе обработки алгоритмом одного кадра представлены на рис. 2 (см. вторую сторону обложки).

Методика проведения эксперимента

Для работы использовались 10 эпикардиальных наборов данных двухмерной допплеровской эхокардиографии больших животных (свиньи и овцы). Каждый набор имел примерно 400 кадров, продолжительность съемки составляла около 30 с, частота кадров — около 14 Гц. Наборы данных были сняты с помощью датчика X7-2 на аппарате Philips iE33 (Philips Healthcare, Андовер, Массачусетс). Протоколы экспериментов были одобрены научным комитетом бостонской детской больницы по уходу и обращению с животными. Все животные получили должный уход согласно Руководству по уходу и обращению с лабораторными животными 1996 г. [18]. Каждая последовательность предварительно обрабатывалась с помощью ретроспективного кадрирования для получения перестановленных кадров. Вычисления проводили на компьютере с процессором Intel Core i7-8700K. Обработку данных вели с помощью программы на языке C++ с использованием библиотеки OpenCV. Для разделенных данных кровотока и B-режима, а также данных об их относительном расположении, использовалась утилита, разработанная сотрудником Philips Healthcare.

Результаты

◊ *Параметры алгоритма*

Предлагаемый метод применялся со следующими параметрами:

- значение u было выбрано таким образом, чтобы порог субмаксимальных скоростей начинался примерно с 0,75 от максимума;

- значение v_c была подобрано так, чтобы разница между противоположными скоростями составляла как минимум 90 % диапазона;
- $c_d = 0{,}1$, т. е. если значения направлений отличались менее чем на 10 %, регион не рассматривался.

◊ *Тестирование на реальных данных*

Алгоритм был запущен на тестовых наборах и позволил успешно устранить алиасинг в большинстве кадров. Всего для тестовых наборов, насчитывающих порядка 4000 кадров, алиасингу была подвержена примерно треть кадров, были обнаружены ошибки устранения в примерно 10 кадрах (около 1 %). Проверка проводилась вручную.

◊ *Примеры неудачного устранения алиасинга*

Неполное устранение. Наиболее часто встречающейся проблемой алгоритма является неполное устранение алиасинга. Это связано с тем, что маска применяется лишь к субмаксимальным областям. На рис. 3 (см. вторую сторону обложки) показан пример неполного устранения на фрагменте кадра.

Параметр *и* был подобран таким образом, чтобы покрывать большое значение стандартных параметров съемки, так как радиологи обычно стараются подобрать адекватные параметры съемки. Тем не менее, в данных случаях параметр оказался выше требуемого. Одним из вероятных решений такой проблемы может стать более точный выбор порогового значения *и*. Например, можно давать возможность радиологу выбирать значение самостоятельно или же реализовать автоматический подбор значения, который дает наиболее равномерный кровоток, данная задача является предметом будущих исследований.

Смежность с «лишними» компонентами. Другой проблемой может стать плохая репрезентативность значения для поиска доминирующего направления. Она может приводить к тому, что смежность с компонентами, которые не должны были принадлежать критическому региону, дает неверное определение направления, как на рис. 4 (см. третью сторону обложки).

Частично эта проблема может усугубляться слишком широким критерием смежности при разбиении на компоненты (рис. 5, см. третью сторону обложки).

В данном случае такого эффекта можно избежать, применив не 8-смежность, а 4-смежность, разбиение на компоненты в таком случае изменится (рис. 6, см. третью сторону обложки). Таким образом, необходимо использовать 4-смежность для разбиения на компоненты.

Выбор 4-смежности в пользу 8-смежности не должен повлечь за собой проблем в нахождении смежных субмаксимальных областей — случай, когда такие области смежны только диагонально расположенными пикселами, крайне маловероятен.

Данный пример наглядно демонстрирует преимущества применения алгоритма только к областям с субмаксимальными скоростями. В противном случае все смежные области поменяли бы направление, что привело бы к непонятной радиологу картине. В данном же случае оператору будет виден артефакт исправления, и он сможет обратиться к исходным данным и разрешить этот вопрос.

◊ *Время работы*

Обработка одного кадра на персональном компьютере, использующая 4-смежность для определения критических границ, занимала в среднем около 5 мс, а для 8-смежности — 7 мс, что делает этот метод применимым для обработки кадров в реальном времени, а также говорит об осмысленности использования 8-смежности для поиска критических границ.

Заключение

В данной работе был предложен новый метод устранения алиасинга, который применяется только к областям с близкими к максимальным скоростями, что позволяет уменьшить область покрытия в случае некорректного определения и облегчить поиск ошибок определения. Алгоритм был протестирован на реальных двухмерных эхокардиографических данных и показал достаточно высокую точность определения (менее 1 % ошибок) и скорость работы, позволяющую включать его в комплексы для обработки допплерографических данных в реальном времени.

Список литературы

1. **Yotti R., Bermejo J., Antoranz, J C., Rojo-Álvarez J. L., Allue C., Silva J., Desco M M., Moreno M., Garci a-Fernández, M. A.** Noninvasive assessment of ejection intraventricular pressure gradients // J. Am Coll Cardiol. Journal of the American College of Cardiology. 2004. Vol. 43, N. 9. P. 1654—1662.

2. **Funamoto K., Hayase T., Saijo Y., Yambe T.** Detection and correction of aliasing in ultrasonic measurement of blood flows with Ultrasonic-Measurement-Integrated simulation // Technol Heal Care. IOS Press. 2005. Vol. 13, N. 4. P. 331—344.

3. **Plicht B., Kahlert P., Goldwasser R., Janosi R. A., Hunold P., Erbel R., Buck T.** Direct quantification of mitral regurgitant flow volume by real-time three-dimensional echocardiography using dealiasing of color Doppler flow at the vena contracta // J. Am Soc Echocardiogr. Elsevier, 2008. Vol. 21, N. 12. P. 1337—1346.

4. **Tonti G., Riccardi G., Denaro F. M., Trambaiolo P., Salustri A.** From digital image processing of colour Doppler M-mode maps to noninvasive evaluation of the left ventricular diastolic function: a dedicated software package // Ultrasound Med Biol. Elsevier, 2000. Vol. 26, N. 4. P. 603—611.

5. **Arigovindan M., Suhling M., Jansen C., Hunziker P., Unser M.** Full Motion and Flow Field Recovery from Echo Doppler Data // IEEE Transactions on Medical Imaging. 2006. Vol. 26, N.1. P. 31—45.

6. **Yakhot A., Anor T., Karniadakis G. E.** A reconstruction method for gappy and noisy arterial flow data // IEEE Trans Med Imaging. IEEE, 2007. Vol. 26, N. 12. P. 1681—1697.
7. **Shahin A., Ménard M., Eboueya M.** Cooperation of fuzzy segmentation operators for correction aliasing phenomenon in 3D color doppler imaging // Artif Intell Med. Elsevier, 2000. Vol. 19, N. 2. P. 121—154.
8. **James C. N., Houze Jr R. A.** A real-time four-dimensional Doppler dealiasing scheme // J. Atmos Ocean Technol. 2001. Vol. 18, N. 10. P. 1674—1683.
9. **Gao J., Droegemeier K. K.** A variational technique for dealiasing Doppler radial velocity data // J Appl Meteorol. 2004. Vol. 43, N. 6. P. 934—940.
10. **Xu Q., Nai K.** Mesocyclone-targeted Doppler velocity dealiasing // J. Atmos Ocean Technol. 2017. Vol. 34, N. 4. P. 841—853.
11. **Chang P.-L. Fang, W. T., Lin P. F., Yang M. J.** A Vortex-Based Doppler Velocity Dealiasing Algorithm for Tropical Cyclones // J Atmos Ocean Technol. 2019. Vol. 36, N. 8. P. 1521—1545.
12. **Muth S.,Dort S., Sebag I. A., Blais M. J., Garcia D.** Unsupervised dealiasing and denoising of color-Doppler data DeAN processed // Medical Image Analysis. 2011. Vol. 15. P. 577—588.
13. **Yatchenko A. M., Krylov A. S., Gavrilov A. V., Arkhipov I. V.** Graph-cut based antialiasing for Doppler ultrasound color flow medical imaging // Visual Communications and Image Processing (VCIP), 2011 IEEE. 2011. P. 1—4.
14. **Yatchenko A., Krylov A. S.** Cross-Frame Ultrasonic Color Doppler Flow Heart Image Unwrapping // Functional Imaging and Modeling of the Heart / ed. van Assen H., Bovendeerd P., Delhaas T. Springer International Publishing, 2015. Vol. 9126. P. 265—272.
15. **Yatchenko A. M., Krylov A. S., Sandrikov V. A., Kulagina T. Y.** Regularizing method for phase antialiasing in color doppler flow mapping // Neurocomputing. Elsevier. 2014. Vol. 139. P. 77—83.
16. **Oktamuliani S., Hasegawa K., Saijo Y.** Correction of Aliasing in Color Doppler Echocardiography Based on Image Processing Technique in Echodynamography // Proceedings of the 3rd International Conference on Biomedical Signal and Image Processing. 2018. P. 1—5.
17. **Кормен Т. Х., Лейзерсон Ч. И., Ривест Р. Л., Штайн К.** Алгоритмы: построение и анализ. М.: Вильямс. 2006. 1296 с.
18. **Council N. R.** Guide for the Care and Use of Laboratory Animals. Washington, DC: The National Academies Press, 1996.

A. B. Terentjev, PhD Student, e-mail: alexey.terentjev@gmail.com,
I. V. Shturts, Senior Research Fellow, e-mail: ishturts@gmail.com,
Peter the Great St.Petersburg Polytechnic University, St.Petersburg, Russian Federation

Two Dimensional Color Doppler Dealiasing Using Submaximal Velocity Components Filtering

Aliasing is one of the most common artifacts in 2D color Doppler echocardiography. Existing methods are approximate and the most precise of them require considerable amount of computations. In the proposed paper, we describe an algorithm that modifies only areas with submaximal velocities — areas most prone to aliasing, leaving other untouched in order to facilitate the process of analysis for the radiologist. Algorithm was tested on 10 in-vivo datasets of large animals and have shown the considerable precision and computation efficiency, which made it real-time compatible.

Keywords: *two-dimensional color Doppler, echocardiography, disjoint-set tree, connected components*

DOI: 10.17587/it.27.97-101

References

1. **Yotti R., Bermejo J., Antoranz J. C., Rojo-Álvarez J. L., Allue C., Silva J., Desco M. M., Moreno M., Garci a-Fernández M. A.** Noninvasive assessment of ejection intraventricular pressure gradients, *Journal of the American College of Cardiology*, 2004, vol. 43, no. 9, pp. 1654—1662.
2. **Funamoto K., Hayase T., Saijo Y., Yambe T.** Detection and correction of aliasing in ultrasonic measurement of blood flows with Ultrasonic-Measurement-Integrated simulation, *Technol Heal Care. IOS Press*, 2005, vol. 13, no. 4, pp. 331—344.
3. **Plicht B., Kahlert P., Goldwasser R., Janosi R. A., Hunold P., Erbel R., Buck T.** Direct quantification of mitral regurgitant flow volume by real-time three-dimensional echocardiography using dealiasing of color Doppler flow at the vena contracta, *J. Am. Soc. Echocardiogr,* Elsevier, 2008. vol. 21, no. 12, pp. 1337—1346.
4. **Tonti G., Riccardi G., Denaro F. M., Trambaiolo P., Salustri A.** From digital image processing of colour Doppler M-mode maps to noninvasive evaluation of the left ventricular diastolic function: a dedicated software package, *Ultrasound Med Biol.,* Elsevier, 2000, vol. 26, no. 4, pp. 603—611.
5. **Arigovindan M., Suhling M., Jansen C., Hunziker P., Unser M.** Full Motion and Flow Field Recovery from Echo Doppler Data, *IEEE Transactions on Medical Imaging*, 2006, vol. 26, no. 1, pp. 31—45.
6. **Yakhot A., Anor T., Karniadakis G. E.** A reconstruction method for gappy and noisy arterial flow data, *IEEE Trans Med Imaging*, IEEE, 2007, vol. 26, no. 12, pp. 1681—1697.
7. **Shahin A., Ménard M., Eboueya M.** Cooperation of fuzzy segmentation operators for correction aliasing phenomenon in 3D color doppler imaging, *Artif Intell Med.,* Elsevier, 2000, vol. 19, no. 2, pp. 121—154.
8. **James C. N., Houze Jr R. A.** A real-time four-dimensional Doppler dealiasing scheme, *J. Atmos. Ocean Technol.*, 2001, vol. 18, no. 10, pp. 1674—1683.
9. **Gao J., Droegemeier K. K.** A variational technique for dealiasing Doppler radial velocity data, *J. Appl. Meteorol.*, 2004, vol. 43, no. 6, pp. 934—940.
10. **Xu Q., Nai K.** Mesocyclone-targeted Doppler velocity dealiasing, *J. Atmos. Ocean Technol.,* 2017, vol. 34, no. 4, pp. 841—853.
11. **Chang P.-L. Fang, W. T., Lin P. F., Yang M. J**. A Vortex-Based Doppler Velocity Dealiasing Algorithm for Tropical Cyclones, *J. Atmos. Ocean Technol.*, 2019, vol. 36, no. 8, pp. 1521—1545.
12. **Muth S.,Dort S., Sebag I. A., Blais M. J., Garcia D.** Unsupervised dealiasing and denoising of color-Doppler data DeAN processed, *Medical Image Analysis,* 2011, vol. 15, pp. 577—588.
13. **Yatchenko A. M., Krylov A. S., Sandrikov V. A., Kulagina T. Y.** Graph-cut based antialiasing for Doppler ultrasound color flow medical imaging, *Visual Communications and Image Processing (VCIP)*, 2011 IEEE, 2011, pp. 1—4.
14. **Yatchenko A., Krylov A. S**. Cross-Frame Ultrasonic Color Doppler Flow Heart Image Unwrapping, *Functional Imaging and Modeling of the Heart* / ed. van Assen H., Bovendeerd P., Delhaas T. Springer International Publishing, 2015, vol. 9126, pp. 265—272.
15. **Yatchenko A. M., Krylov A. S., Sandrikov V. A., Kulagina T. Y.** Regularizing method for phase antialiasing in color doppler flow mapping, *Neurocomputing,* Elsevier, 2014, vol. 139, pp. 77—83.
16. **Oktamuliani S., Hasegawa K., Saijo Y.** Correction of Aliasing in Color Doppler Echocardiography Based on Image Processing Technique in Echodynamography, *Proceedings of the 3rd International Conference on Biomedical Signal and Image Processing*, 2018, pp. 1—5.
17. **Cormen T. H., Leiserson C. E., Rivest R., Stein C.** Introduction to algorithms, MIT press, 2005.
18. **Council N. R.** Guide for the Care and Use of Laboratory Animals, Washington, DC, The National Academies Press, 1996.

УДК 004.03 DOI: 10.17587/it.27.102-111

С. М. Авдошин, канд. техн. наук,
руководитель департамента программной инженерии, профессор, e-mail: savdoshin@hse.ru,
Е. Ю. Песоцкая, канд. экон. наук,
доц. департамента программной инженерии, e-mail: epesotskaya@hse.ru,
Д. М. Куруппуге, студент департамента программной инженерии, e-mail: dkuruppuge_1@edu.hse.ru,
Национальный исследовательский университет "Высшая школа экономики", Москва

Выбор MOOC для российских ИТ-специалистов при планировании карьеры

Цифровизация, о которой так много говорят в последнее время в России и во всем мире, способствует развитию многих отраслей, от образования до промышленности, но при этом диктует новые требования к кадрам и их компетенциям. Чтобы идти в ногу с появляющимися трендами и информационными технологиями и планировать будущую карьеру, специалисты в области информационно-коммуникационных технологий (ИКТ) должны постоянно обновлять набор навыков, осваивать передовые технологии и формировать новые компетенции. Лучший способ для специалиста в области ИКТ или студента бакалавриата ИТ-специальности — зарегистрироваться на платформе MOOC и пройти соответствующие курсы. Однако, учитывая большое разнообразие платформ и курсов, можно запутаться в том, что выбрать для будущего развития карьеры, какие курсы наиболее современны и отвечают потребностям работодателя. Авторы проводят исследование требований пользователей, существующих рекомендательных систем MOOC и их функций и предлагают рекомендательную систему, которая позволяет пользователям выбирать существующую платформу MOOC на основе заданий и навыков для планирования карьеры в области ИКТ. В статье предложен современный подход, который помогает ИТ-специалистам в России планировать свое дальнейшее развитие на основе рекомендаций MOOC, специфичных для рабочих мест и соответствующих их потребностям в развитии.

Ключевые слова: *MOOC, рекомендации, ИТ, карьера, навыки, ИКТ*

Введение

В России для развития цифрового общества и цифровой трансформации наиболее важными факторами являются достаточная зрелость цифровой культуры в обществе и на предприятиях, а также выбор правильных технологий и приоритетов [1].

Переход к цифровой экономике и проекты в области цифровой трансформации бизнеса создают повышенный спрос на высококвалифицированных специалистов в области информационно-коммуникационных технологий (ИКТ). Обязательным требованием современного рынка труда является новый набор базовых знаний и умений (цифровых, правовых, финансовых), необходимых для использования возможностей современной цивилизации [2].

Цифровизация, т. е. перевод всех видов информации в цифровую форму, проникает абсолютно во все сферы деятельности. Она меняет подход к управлению предприятиями, городами и даже собственной жизнью. Технологическая революция стремительно преображает общественный уклад. Многие задачи, выполняемые сейчас работниками в различных секторах экономики, будут автоматизированы или исчезнут в связи с изменением способа организации общества [3]. Для новой экономики потребуются специалисты нового типа.

Это подтверждает исследование HeadHunter [4], согласно которому спрос на высококвалифицированных ИТ-специалистов тоже динамично растет. Если в январе 2018 г. было опубликовано около 200 объявлений о работе, в названии которых присутствовали такие термины, как Data Science, Data analyst, Machine

Learning, Big Data, то в марте 2020 г. работодатели предлагают более 700 подобных вакансий.

Западными специалистами названы новые ИТ-профессии будущего [5], среди которых важнейшими могут стать Data Detective (детективы данных), Personal Data Broker (личный брокер данных), Cyber Attack Agent (агент по кибербезопасности), AI-Assisted Healthcare Technician (специалист по здравоохранению на основе искусственного интеллекта), Smart Home Design Manager (дизайнер умного дома) и другие.

При этом нынешние ИТ-специалисты стремятся найти новые способы обучения из-за страха остаться позади, если они не будут продолжать расти и развиваться. Так, по данным Metaari, за 2019 г. в глобальный рынок образования были инвестированы рекордные 18,66 млрд долларов, что примерно на 2 млрд долларов больше, чем в 2018 г. [6]. Усиленный приток капитала в эту область дает возможность создавать новые образовательные стартапы, расширять линейки образовательных продуктов и курсов, обеспечивать непрерывное повышение уровня знаний.

Процесс изучения новых навыков и знаний, который также известен как обучение в течение всей жизни, стимулируется глобализацией, экономикой, основанной на знаниях, и новыми технологиями [7]. Методы образования и способы получения знаний за последние несколько десятилетий были значительно развиты благодаря технологическому прогрессу. Сначала знания транслировались устно, затем — в письменной форме, позже на смену пришел цифровой формат обмена и приобретения информации. В настоящее время для получения образования достаточно щелчка мыши, подключения к интернету из любого удобного места. Формат обучения также может быть скорректирован под пожелания обучающегося.

Это стало возможным благодаря внедрению массовых открытых онлайн-курсов (MOOC), что стало результатом движения за открытость в образовании. С развитием MOOC появилась концепция платформ, также известных как провайдеры. В начале 2008 г. было 0 провайдеров, а в настоящее время их существует более 900 [8]. Провайдеры начали собирать курсы из разных университетов и предоставлять доступ к ним большому числу пользователей в одном месте через сеть Интернет. Такими провайдерами, появившимися на ранних этапах, являются Coursera с 40 млн [9], edX с 24 млн [10], Udacity с 11,5 млн [11] и FutureLearn с 10 млн [12] текущих пользователей.

Что касается наиболее популярных российских площадок в области ИТ, то по результатам исследования "Мой круг" [13] более половины респондентов слышали о таких школах, как Geekbrains (69 %), Coursera (68 %), Codecademy (64 %), HTML Academy (56 %). Udemy у российской аудитории оказалась на шестом месте (44 %), Udacity — на тринадцатом (об этой платформе слышали 32 % опрошенных).

Несмотря на то, что число поставщиков образования увеличивается с каждым днем, специалисты во всем мире все еще ощущают значительный разрыв между текущими навыками и потребностью в них в будущем. По данным Couseburg [14] 47 % респондентов идут на курсы, чтобы освоить новую профессию, 26 % опрошенных записываются на курсы для себя и общего развития, 17 % стремятся улучшить навыки и повысить квалификацию, 9 % важно получить сертификат, 1 % респондентов покупают курсы в качестве подарка.

Несоответствие между навыками и рабочими местами затрагивает профессии во многих сферах: социальной, экономической, политической, финансовой, в том числе в сфере ИТ. Также отмечается несоответствие навыков и ожиданий со стороны работодателей [15], в том числе:

1) отсутствие полного удовлетворения работодателей компетенциями кандидатов;

2) появление новых профессий и навыков, адаптирующихся к новым бизнес-задачам, для которых не существует готовых специалистов;

3) устаревание старых навыков в результате технологического прогресса, автоматизации и цифровизации общества;

4) недостаток практики у молодых специалистов и выпускников вузов, поскольку студенты часто получают теорию, но не знают, как использовать ее для работы в компании после трудоустройства [16].

Таким образом, можно сделать вывод, что современное образование не до конца закрывает потребность в освоении новых знаний и навыков, чтобы молодые выпускники могли чувствовать себя в профессиональной деятельности комфортно. Согласно исследованию НИУ ВШЭ, высшее и профессиональное образование на треть (а в ряде секторов на две трети) не соответствует запросам рынка труда. По окончании обучения по данным Росстата не по специальности трудоустраиваются 31,3 % выпускников вузов, 40,5 % выпускников организаций среднего профессионального образования [2].

Бизнес-среда постоянно трансформируется, возникают новые профессии и меняются требования к навыкам. И сложно гарантировать, что, приобретя определенные навыки, мы будем использовать их всю жизнь. Для работы в области ИКТ крайне важно иметь необходимые базовые навыки и постоянно изучать новые области знаний, приобретать дополнительные компетенции. Вот почему многие ИТ-специалисты в процессе учебы и далее в профессиональной деятельности занимаются дополнительным самообразованием — с помощью книг, видео, блогов. По данным исследования "Мой круг" [13] двое из трех ИТ-специалистов проходят курсы дополнительного профобразования, причем большинство платят за них; каждый второй посещает семинары, митапы, конференции.

В данной работе рассмотрена рекомендательная система, которая предоставляет пользователям ресурс, где они могут в одном месте получить информацию об актуальных рабочих профессиях, навыках и соответствующих курсах ИКТ для планирования своей карьеры и достижения карьерного роста. В статье описываются доступные инструменты для планирования карьеры и развития профессиональных навыков, проанализированы интересы потребителей и их ожидания от рекомендательной системы, а также возможности поставщиков МООС. В результате предлагаются функциональные возможности рекомендательной системы на основе требований пользователей и рассматриваются архитектура и возможные способы монетизации системы. Обсуждаются ограничения и дальнейшие шаги, которые относятся к этому исследованию.

1. Развитие ИТ и цифровых навыков в России

1.1. Потребность в ИТ и цифровых специалистах

На текущем российском рынке труда рабочие места в сфере ИТ стали наиболее привлекательными для трудоустройства. По оценкам аналитиков International Data Corporation (IDC) [31] российский рынок ИКТ в 2019 г. среди других стран Центральной и Восточной Европы достиг 47,05 млрд долларов. По их оценкам к концу года общие расходы составили 136,66 млрд долларов, что на 4 % превышает первоначальный бюджет, выделенный на год. Так, чуть более трети инвестиций пришло из России. В результате расширения российского ИТ-рынка возрастает спрос на квалифицированных ИТ-специалистов.

Несмотря на то что в целом Россия отстает от других стран по качеству и темпам цифровизации, в некоторых сегментах уже есть успешные примеры — в частности, цифровизация государственных услуг в России. Ярким примером является внедрение электронного правительства и предоставление полного спектра государственных и муниципальных услуг, доступных для граждан в цифровом формате. Кроме того, чтобы обеспечить доступ к цифровым порталам для всех, независимо от того, обладают ли они навыками или нет, услуги предоставляются всему населению через мобильные приложения или через службы коротких сообщений (SMS).

Еще один цифровой проект, который был запущен в пилотном режиме в Москве и Санкт-Петербурге в России с ноября 2019 г. по октябрь 2020 г., — это "Европротокол онлайн", который позволил гражданам в цифровом виде составлять уведомления об авариях и получать свой статус удаленно без участия ГАИ.

Помимо вышеупомянутых проектов развитие цифровых тенденций и платформ оказывает положительное влияние на рынок труда. Это сократит периоды поиска работы, повысит продуктивность сотрудников, облегчит возможности удаленной работы и обеспечит доступ к качественному образованию.

Согласно исследованию BCG (the Boston Consulting Group), The Network и HeadHunter.ru в 2019 г. [32] Россия заняла 25 место среди 180 стран по привлекательности для digital-специалистов как место работы. Это исследование также показало, что цифровые работники предпочитают работать в крупных компаниях в России, а не в стартапах. Последние 5 лет Тинькофф Банк в России хорошо известен тем, что открывает дорогу ИТ-специалистам, которые впоследствии уезжают в Европу и Кремниевую долину.

Россия занимает 45 место среди 176 других стран в глобальных рейтингах лидеров в области развития современных информационных и коммуникационных технологий [33]. ИТ — это самая быстрорастущая отрасль, которая гарантирует широкий спектр рабочих мест для специалистов в России, среди других стран мира. Не только специалисты, но и старшеклассники проявляют большой интерес к тому, чтобы стать ИТ-специалистами и предпринимателями в области новых технологий.

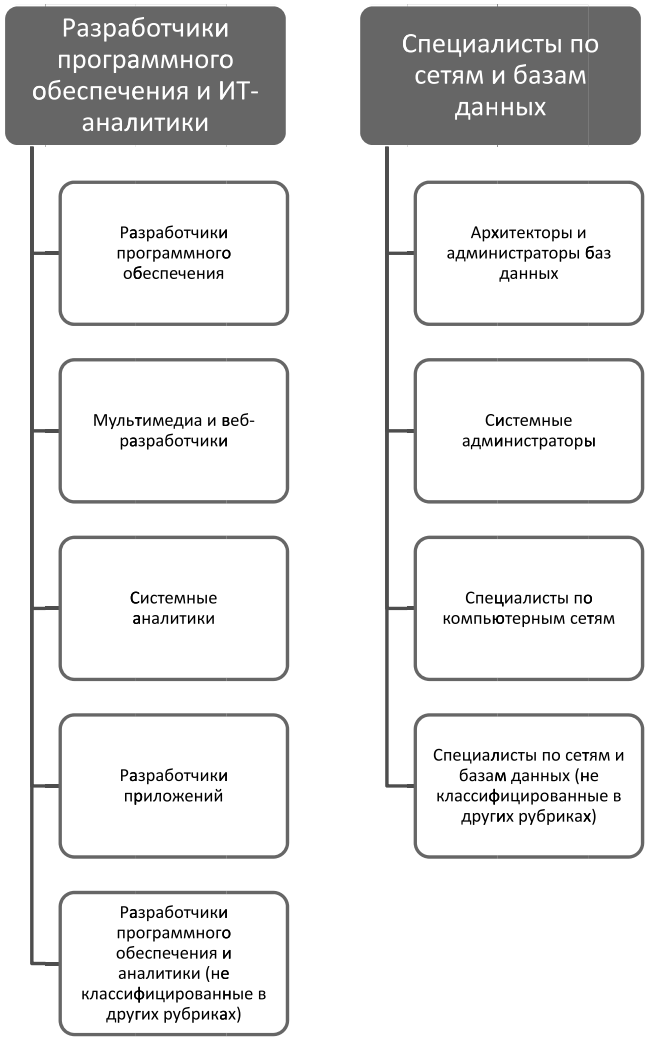


Рис 1. Классификация ESCO в части некоторых ICT профессий

Классификация некоторых основных профессий в области информационных и коммуникационных технологий на современном европейском рынке труда по данным ESCO представлена на рис. 1.

На основе совместного исследования старшеклассников и их родителей, проведенного GeekBrains и ReseachMe [34], 42 % учащихся и 24 % родителей среди участников выбрали ИТ-специалиста, а 39 % учащихся и 27 % родителей выбрали программистов в качестве будущей карьеры. Среди студентов, которые выбрали работу ИТ-специалиста как перспективную, 53 % процентов проявили интерес к искусственному интеллекту и большим данным.

Согласно этому исследованию 72 % студентов и 82 % родителей считают, что студентам необходимо овладеть дополнительными профессиональными навыками, которые не включены в учебную программу университетов. МООС и онлайн-обучение можно предложить в качестве решения проблемы отсутствия средств для приобретения навыков, и 73 % студентов и 60 % родителей согласились с этим.

1.2. Инструменты для развития карьеры ИТ специалиста в России

Для сегодняшнего развития карьеры специалист может совершенствовать свои компетенции и приобретать новые навыки как очно, офлайн, так и в интернете, т. е. онлайн. Последние тенденции и ситуация с коронавирусом привели к более динамичному развитию цифровых и онлайн-каналов в образовании. Обучение МООС, и прежде популярное среди молодежи [8, 17, 18], стало еще более доступным для более широкой аудитории.

Внедрение МООС привело к появлению большего числа поставщиков курсов, которые используют при разработке платформ схожие принципы [19]: являются открытыми для пользователей, содержат цифровые материалы, подразумевают самостоятельное обучение, но при этом поддерживают взаимодействие с экспертами в предметной области, предлагают комбинировать различные форматы приобретения знаний.

Чтобы определить, какие навыки необходимы в изменяющемся мире для увеличения шансов на получение доступа к карьере, надо заранее планировать карьерный путь. Наличие личного карьерного плана (ЛКП) поможет [20]:

- выявить сильные стороны и определить области для персонального роста;
- быть активнее в поиске и наиболее эффективном использовании возможностей развития;
- стремиться к более продвинутым навыкам, знаниям и методам для более качественного выполнения задач и поиска нестандартных решений;
- более успешно реализовывать карьерные устремления.

Существует множество современных инструментов и методологий для реализации ЛКП. Самооценка, исследование, фокусировка и поиск работы/план действий [20] являются шагами на этом пути:

- *самооценка.* Определение собственной ценности и навыков может сэкономить годы разочарований в несостоявшейся карьере, которая не соответствует ни навыкам, ни интересам. Сегодня доступно множество анкет и упражнений для самооценки. На-

пример, отдел по работе с персоналом Массачусетского технологического института (MIT) предлагает 20...30-минутное самооценочное упражнение для оценки достижений и самооценки личности [21];

- *исследование.* На этом этапе выясняется, чего именно ожидают работодатели от сотрудников и какие рабочие места у них соответствуют навыкам, признанным на этапе самооценки. Это касается изучения описания работы и должностных обязанностей, информации о рынке труда относительно средней заработной платы и перспектив работы. Одним из онлайн-инструментов, который можно использовать для изучения возможностей карьерного роста в научных областях для студентов и аспирантов, является myIDP (https://myidp.sciencecareers.org/);
- *фокусировка.* На этом этапе соискатели концентрируются на улучшении собственных навыков в соответствии с желаемой карьерой, что становится инвестицией в будущую профессию. Чтобы развить необходимые навыки, можно использовать МООС в качестве дополнительного инструмента, помимо университета;
- *поиск работы / план действий.* Наконец, можно воплощать в жизнь все собранные навыки и приступить к работе своей мечты. Для составления более конкретного плана подойдут инструменты планирования карьеры, предоставленные университетами или образовательными организациями для студентов, такие как CareerPlanner (https://www.careerplanner.com/), Prospects (https://www.prospects.ac.uk), EducationPlanner (http://www.educationplanner.org/). Эти инструменты, как правило, включают в себя тесты, которые позволят будущему сотруднику самостоятельно оценить уровень подготовки и наличие достаточных знаний для будущей карьеры в выбранной области.

Подводя итоги, можно сказать, что на каждом этапе планирования мы можем использовать онлайн-инструменты, от вопросников для самооценки до ресурсов по развитию карьеры, которые помогут принимать более четкие и обоснованные решения по выбору карьеры. Дополнительным фактором успеха будет наличие знаний о востребованных профессиях и специальностях, которые постоянно обновляются и корректируются в зависимости от изменений технологий, экономики и прочих факторов воздействия.

2. Рекомендательная система и ее характеристики

Рекомендательная система позволяет отталкиваться главным образом от актуальных на данный момент профессий и навыков, востребованных работодателями. Экосистема включает профессии, курсы МООС, конечных пользователей, поставщиков курсов, университеты и заинтересованные стороны (будущих работодателей).

Для разработки системы тщательно проанализированы интересы и потребности молодых специалистов, заинтересованных в развитии карьеры, и выделены ключевые особенности системы рекомендаций МООС для ИТ-специалистов.

2.1. Открытость и свободный доступ

Большая часть аудитории МООС определяется как пользователи из развивающихся стран [22], у которых ограниченные возможности путешествовать по миру и посещать престижные университеты, такие как MIT или Stanford. Большинство известных провайдеров, например Coursera, edX и Udacity, предлагают только частичный бесплатный доступ к своим материалам.

Рекомендательная система предоставляет пользователям доступ бесплатно с помощью простой регистрации или входа через социальные сети, что позволяет без ограничений просматривать навыки, определенные для каждой специальности или профессии, актуальной на текущий момент, и только после этого подбирать курсы внешних площадок (на условиях доступа провайдера). Навыки специалистов ИКТ базируются на Европейской классификации профессий и компетенций ESCO [23], списки профессий и компетенций постоянно обновляются согласно требованиям работодателей Европейского союза, коррелируя с международными трендами профессий и навыков будущего.

Классификация профессий ESCO представляет собой дерево специальностей от более общих к более частным. Таким образом, пользователь может выбрать либо широкую категорию, например разработчик ПО, либо более узкую — системный архитектор или UX/UI-дизайнер. Далее пользователю доступны наборы компетенций, присущих выбранной профессий.

2.2. Контент должен отражать потребности пользователей

Группа исследователей из Гарварда и Массачусетского технологического института [24] установила, что из всех участников первых МООС, предлагаемых edX, 74 % получивших сертификаты имеют степень бакалавра или более высокую квалификацию, 71 % из них были мужчинами, а средний возраст составлял 26 лет. Согласно отчетам о тенденциях и статистике МООС от Class Central [17], самый высокий процент потребителей МООС интересуются технологическими предметами (информатикой, программированием и наукой о данных), а почти 40 % — как бизнесом, так и технологическими дисциплинами.

Можно сделать вывод, что основная аудитория образованная, молодая и в основном заинтересована в технических предметах. Чтобы обеспечить потребности такой аудитории, предложенная система рекомендаций будет сфокусирована на курсах от самых престижных международных университетов в мире, таких как Гарвард, Массачусетский технологический институт, Стэнфорд, Беркли и Пекинский университет. Фокус системы будет на курсах и навыках, связанных с ИКТ и цифровыми специальностями, которые в настоящее время широко востребованы пользователями.

2.3. Наличие классификации навыков и персонализированный выбор

Выше были проанализированы подходы к реализации плана развития карьеры, чтобы получить четкое представление о том, чего ожидают будущие работодатели, и рассмотрены инструменты, которые представляют собой набор онлайн-тестов и оценок для определения возможностей сотрудников.

Однако эти инструменты не дают дальнейших решений проблемы развития навыков, скорее только идентифицируют и оценивают их. В качестве решения рассматриваемая рекомендательная система предоставляет набор навыков для каждой работы, чтобы пользователь мог видеть навыки в доступном виде и выбирать только те из них, в развитии которых он заинтересован в текущий момент. После выбора необходимых навыков для привлекающей пользователя профессии ему предлагаются курсы от различных поставщиков МООС, которые можно использовать для развития выбранных им навыков.

2.4. Агрегация МООС-провайдеров

Взаимосвязь данных стала обычной тенденцией в сети, и многие популярные компании, такие как Spotify, новости Google и AliExpress, воспользовались этой тенденцией, чтобы стать лидерами в своей отрасли. Пользователи ценят свое время, поэтому нахождение всей информации, связанной с темой, в одном месте, а не повторение процесса поискового клика является преимуществом подобных сервисов.

Внедрение аналогичного подхода к объединению МООС от различных поставщиков для облегчения поиска лучших курсов по заданным параметрам облегчит визуальное сравнение предложений различных поставщиков МООС и сэкономит время пользователя на принятие обоснованного решения.

Предлагаемая система рекомендаций представляет пользователю доступ к информации о МООС с полезной информацией о курсе и ссылкой на оригинальный сайт сразу от множества платформ. Выборка курсов происходит на основе заранее определенных пользователем профессий и навыков в соответствии с классификацией ESCO для специалистов в области ИКТ и цифровых технологий.

Помимо основных функций рекомендательная система поможет осуществить дополнительный поиск вакансий с использованием тегов и ключевых слов. В качестве дополнительных функций для удобства пользователей возможно создание закладок, добавление курсов в избранное, фильтрация курсов по поставщику МООС.

3. Архитектура рекомендательной системы и монетизация

3.1. Архитектура

Рекомендательная система может состоять из двух основных компонентов: бэкэнда и клиентской части (рис. 2). Бэкэнд включает в себя базу данных и файловую систему. Сервер приложения отвечает за реализацию пользовательских функций, таких как вход/регистрация, аутентификация, редактирование данных пользователя, и реализован в соответствии с архитектурой REST [25], что обеспечивает лучшую совместимость. Взаимодействие с пользователями происходит независимо от технологии, которую они используют.

Пользователь может выбрать набор компетенций и навыков, в которых он заинтересован, с помощью запроса к базе данных

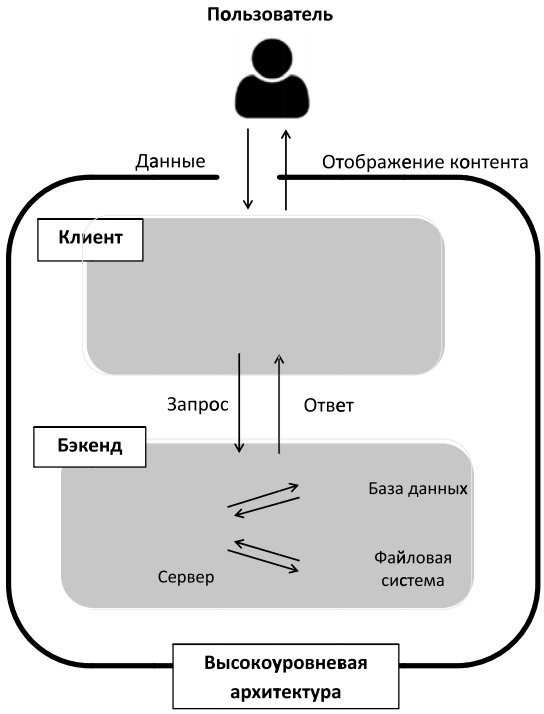


Рис. 2. Архитектура рекомендательной системы

через сервер и API-доступ к образовательной платформе внешних провайдеров, таких как Coursera, Udacity, edX и Udemy. База данных приложения используется для хранения базовой информации о MOOC, а также хранения учетных данных и настроек пользователя.

Для реализации сервера используется Node.js, который поддерживает язык программирования JavaScript и включает множество дополнительных необходимых библиотек, к которым легко получить доступ.

Для базы данных использована SQL с открытым исходным кодом для хранения больших файлов. При разработке клиентского компонента применены HTML, CSS и JavaScript с платформой React.js.

3.2. Монетизация

Основным источником монетизации являются партнерские программы провайдеров MOOC. Эти платформы предоставляют информацию о курсе через свои партнерские программы, где разработчики могут получить финансовую выгоду, в то время как создатели курсов сохраняют около 70 % доходов и интеллектуальные права. Например, Coursera предлагает более 4000 курсов и специализаций для продвижения и предоставляет разработчикам комиссионные в размере от 25 до 45 % в зависимости от числа кликов пользователей по квалифицированной ссылке [26].

Другими популярными поставщиками MOOC, которые предлагают такие партнерские программы, являются Udemy, Udacity и edX. Поставщики, за исключением edX, не взимают плату за активацию для разработчиков. Несмотря на то, что edX берет за активацию 5 долларов, они возвращаются после первого платежа [27]. Не нужно никаких других затрат, чтобы стать партнером. Это законный способ зарабатывания денег путем продвижения и рекомендации MOOC пользователям.

Можно сделать вывод, что реализация этой рекомендательной системы с использованием бесплатного программного обеспечения с открытым исходным кодом и платформ с помощью партнерских программ, предлагаемых платформами MOOC, может стать выгодным средством монетизации решения.

4. Ограничения и дальнейшее развитие

Настоящее исследование касается рекомендательных систем, MOOC, планов развития карьеры и классификации специальностей ИКТ в России.

Что касается алгоритма рекомендательных систем, авторами были проанализированы доступные варианты: контентно-ориентированная, совместная фильтрация и гибрид [28].

При контентно-ориентированном методе контент относится к функциям, которые интересуют пользователя. Концепция этого метода состоит в том, чтобы маркировать продукты с помощью явно определенных ключевых слов, понимать, что нравится пользователю, находить ключевые слова в базе данных и рекомендовать различные продукты с помощью этих особенностей.

Совместная фильтрация не зависит от заранее определенных функций или предпочтений. Основной фокус алгоритма составляют прошлые взаимодействия пользователей, исторические предпочтения по набору предметов и оценки пользователей.

Гибридный метод представляет собой комбинацию стратегий фильтрации на основе контента и совместной работы. Он делает прогнозы на основе средневзвешенного значения двух стратегий.

В качестве наиболее подходящего метода рекомендаций авторами выбран алгоритм, основанный на содержании, поскольку рекомендации MOOC базируются на заранее определенных рабочих навыках ESCO.

Следует отметить, что предлагаемая система не планирует карьеру без участия или вместо самого пользователя и представляет собой исключительно инструмент для получения доступа к необходимым курсам и источникам информации в области ИКТ при планировании своей карьеры. Разработка персонального карьерного пути, несомненно, требует более тщательного планирования, анализа личностных характеристик пользователя, доступных в географии пользователя вакансий и его карьерных амбиций.

Заключение

Средства получения образования и знаний эволюционируют, помогая студентам и специалистам следить за новыми технологиями и приобретать актуальные знания и опыт. Бумажные книги превратились в цифровые материалы, в то время как лекционные занятия в классе — в видео- или аудиоматериалы, что, безусловно, облегчает жизнь студентам. В настоящее время большое число образовательных платформ предоставляют открытые онлайн-курсы, и сложно определить, какие курсы, какую платформу выбрать, и какие из них помогут их будущей карьере.

Примерно 30 % работодателей во всем мире говорят, что у них возникают трудности с заполнением вакансий из-за отсутствия компетентных кандидатов [29]. Несоответствие между навыками и работой влияет на многие уровни, включая социальный, экономический и, прежде всего, бизнес и правительство. Одним из эффектов, вызванных несоответствием навыков и работы, является [30] отсутствие полной удовлетворенности работодателей компетенциями кандидатов. Возникают новые профессии и навыки, адаптированные к новым бизнес-задачам.

Предложенная система рекомендаций будет идеальным решением в таких ситуациях, поскольку она будет предлагать образовательные курсы, основанные на навыках и умениях, необходимых для конкретной профессии, исходя из предпочтений пользователя. Кроме того, пользователи смогут сравнивать курсы с разных образовательных платформ в одном месте и принимать обоснованные решения.

Авторы показали, как МООС развивались с течением времени и как они влияют на существующую образовательную экосистему, проанализировали, как планировать свой карьерный рост, и какие инструменты есть для такого планирования. В качестве помощи в планировании предложен инструмент, который рекомендует МООС на основе профессиональных интересов пользователей (учитывался интерес к профессиям в области ИКТ) и который ориентирован на навыки. Авторы объяснили ожидания пользователей от такого инструмента и подходящие функции приложения, которые могут их реализовать. Кроме того, предложена возможная архитектура для рекомендательной системы и информационные и технические ресурсы.

Для текущего исследования разработан прототип веб-приложения, который может быть доработан в виде мобильного приложения для более удобной работы пользователей. Также в планах дальнейшего развития возможно расширение системы за рамки профессий ИКТ. Кроме того, может быть разработано решение на основе искусственного интеллекта, которое поможет пользователю выбирать наиболее оптимальный персонализированный путь планирования карьеры и развития навыков в зависимости от его текущий знаний и навыков, способностей к освоению нового материала, карьерных амбиций и множества дополнительных личностных факторов.

Список литературы

1. **Udaltsova N. L.** Russian Digital Economy: State and Development Prospects // Proceedings of the international conference on Technology & entrepreneurship in digital society, Russia. 2019. P. 122—125.

2. **Кузьминов Я., Фрумин И., Овчарова Л.** Двенадцать решений для нового образования: доклад центра стратегических разработок и высшей школы экономики // Центр стратегических разработок совместно с НИУ ВШЭ, 2018. URL: https://www.hse.ru/data/2018/04/06/1164671180/Doklad_obrazovanie_Web.pdf (дата обращения: 15.07.2020).

3. **Лошкарева Е., Лукша П., Ниненко И., Смагин И., Судаков Д.** Навыки будущего. Что нужно знать и уметь в новом сложном мире // Доклад экспертов Global Education Futures и WorldSkills Russia. URL: https://futuref.org/futureskills_ru (дата обращения: 10.07.2020).

4. **Как стать** востребованным специалистом? Исследование HeadHunter. 2020. URL: https://hh.ru/article/26792?from=article_26787 (дата обращения: 29.06.2020).

5. **Teofilov T.** Careers of the Future: 42 Professions of Tomorrow. Medium. 2020 URL: https://medium.com/swlh/careers-of-the-future-42-new-professions-of-tomorrow-5d3905f8513 (дата обращения: 19.07.2020).

6. **Исследование** российского рынка онлайн-образования. Edmarket, 2020. URL: https://innoagency.ru/files/Issledovanie_rynka_rossiyskogo_online_obrazovania_2020.pdf (дата обращения: 10.07.2020).

7. **Laal M., Salamati P.** Lifelong learning; why do we need it? // Procedia — Social and Behavioral Sciences. 2012. Vol. 31. P. 399—403.

8. **Bozkurt, A., Stracke C.** Evolution of MOOC Designs, Providers and Learners and the Related MOOC Research and Publications from 2008 to 2018 // Proceedings of the International Open & Distance Learning Conference (IODL19). Anadolu University, Eskişehir, Turkey, 2019. P. 13—20.

9. **Coursera:** Build Skills with Online Courses from Top Institutions [Официальный сайт]. URL: https://www.coursera.org/ (дата обращения: 10.05.2020).

10. **EdX** [Официальный сайт]. URL: https://www.edx.org/ (дата обращения: 10.05.2020).

11. **Udacity:** Learn the Latest Tech Skills; Advance Your Career [Официальный сайт]. URL: https://www.udacity.com/ (дата обращения: 10.05.2020).

12. **FutureLearn**: Online Courses and Degrees from Top Universities [Официальный сайт]. URL: https://www.futurelearn.com/ (дата обращения: 10.05.2020).

13. **Рейтинг** площадок дополнительного образования в ИТ. "Мой круг", исследование-2020. [Официальный сайт]. URL: https://habr.com/ru/company/habr_career/blog/454906/ (дата обращения: 22.06.2020).

14. **Кострова А., Альхов А., Маньковская Н., Кеник П.** Как россияне выбирают курсы дополнительного образования. CourseBurg [Официальный сайт]. URL: https://courseburg.ru/analytics/Kak_rossiane_vybirayut_kursy_dopolnitelnogo_obrazovania.pdf (дата обращения: 02.08.2020).

15. **International** Labour Office: Skills and jobs mismatches in low- and middle-income countries [Официальный сайт]. URL: https://www.ilo.org/wcmsp5/groups/public/---ed_emp/documents/publication/wcms_726816.pdf (дата обращения: 02.08.2020).

16. **Avdoshin S., Pesotskaya E.** Development of P2P Educational Service in Russia // Proceedings of the Future Technologies Conference (FTC). 2019. Vol. 2 Switzerland: Springer, 2020. P. 833—847.

17. **Ubachs G., Konings L., Nijsten B.** (Eds.). The 2019 OpenupEd trend report on MOOCs. Maastricht, NL: EADTU, 2019.

18. **Shah D.** By the Numbers: MOOCs in 2019. Class Central [Официальный сайт]. URL: https://www.classcentral.com/report/mooc-stats-2019/ (дата обращения: 12.07.2020).

19. **Bonk C. J., Lee M. M., Reeves T. C.** MOOCs and Open Education around the World. Routledge, USA, 2015.

20. **European** Commission. Career Development Plan. Research: Publications Office of the European Union [Официальный сайт]. URL: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5bd4ed377&appId=PPGMS (дата обращения: 14.07.2020).

21. **MIT** Self-Assessment [Официальный сайт]. URL: https://capd.mit.edu/explore-careers/career-first-steps/self-assessment (дата обращения: 14.07.2020).

22. **Bates A. W.** Teaching in a Digital Age. Vancouver BC: Tony Bates Associates Ltd, 2015.

23. **ESCO-European** Skills/Competences, qualifications and Occupations [Официальный сайт]. URL: https://ec.europa.eu/esco/portal/ (дата обращения: 14.07.2020).

24. **Ho A. D., Reich J., Nesterko S., Seaton D. T., Mullaney T., Waldo J., Chuang I.** HarvardX and MITx: The first year of open online courses (HarvardX and MITx Working Paper No. 1). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2381263 (дата обращения: 23.07.2020).

25. **REST** API [Официальный сайт]. URL: https://restfulapi.net/ (дата обращения: 23.07.2020).

26. **Coursera:** Join our affiliate program [Официальный сайт]. URL: https://about.coursera.org/affiliates (дата обращения: 23.07.2020).

27. **edX:** Join the edX affiliate program [Официальный сайт]. URL: https://www.edx.org/affiliate-program (дата обращения: 23.07.2020).

28. **Rocca B.** Introduction to recommender systems. Towards Data Science. URL: https://towardsdatascience.com/introduction-to-recommender-systems-6c66cf15ada (дата обращения: 23.07.2020).

29. **International** Labour Office. (2015) Anticipating and matching skills and jobs. Geneva. [Официальный сайт]. URL: https://www.ilo.org/wcmsp5/groups/public/---ed_emp/---ifp_skills/documents/publication/wcms_534307.pdf (дата обращения: 24.07.2020)

30. **International** Labour Office. (2019) Skills and jobs mismatches in low- and middle-income countries. Geneva [Официальный сайт]. URL: https://www.ilo.org/wcmsp5/groups/public/---ed_emp/documents/publication/wcms_726816.pdf (дата обращения: 23.07.2020).

31. **Tadviser** [Официальный сайт]. URL: https://www.tadviser.ru/index.php/Статья:ИКТ_(мировой_рынок) (дата обращения: 23.07.2020)

32. **Petrova J., Podtserob M., Smertina P.** (2019) Russian IT-specialists less and less want to work abroad, Vedemosti (electronic journal). URL: https://www.vedomosti.ru/management/articles/2019/06/18/804488-rossiiskie-it-spetsialisti (дата обращения: 23.06.2020) (in Russian).

33. **Kolesnikov A.** (2020) World trends in the development of information and communicative technologies. Sciences of Europe, vol. 4, no 50, pp. 66—72.

34. **Mail.ru** group. (2019) GeekBrains study: three quarters of schoolchildren and students consider IT professions to be promising, mail.ru group (research). URL: https://corp.mail.ru/ru/press/infograph/10487/ (дата обращения: 24.06.2020) (in Russian).

S. M. Avdoshin, Ph.D., Professor, School Head,
School of Software Engineering / Faculty of Computer Science, e-mail: savdoshin@hse.ru,
E. Y. Pesotskaya, Ph.D., Associate Professor,
School of Software Engineering / Faculty of Computer Science, e-mail: epesotskaya@hse.ru,
D. M. Kuruppuge, Student,
School of Software Engineering / Faculty of Computer Science, e-mail: dkuruppuge_1@edu.hse.ru,
National Research University Higher School of Economics, Moscow, 101000, Russian Federation

The Selection of MOOCs While Planning a Career of an it Specialist in Russia

Digitalization, which has been so much talked about, contributes to the development of many industries in Russia and in the world, but at the same time dictates new requirements for digital personnel and their competencies. To keep pace with emerging trends and information technology and plan for future careers, information and communication technology (ICT) professionals should continually update their skill sets and develop new competencies with the help of the MOOC platforms that suggest appropriate courses. However, given the wide variety of platforms and courses, one can get confused about what to choose for the future development, which courses to take and what profession to follow. The authors conduct a research on user requirements, existing MOOC recommendation systems and their functions, and propose a recommendation system that allows users to select an existing MOOC platform based on assignments and skills for ICT career planning in Russia. The article proposes a modern approach that helps IT professionals plan their future development path based on MOOC recommendations corresponding to their development needs.

***Keywords**: MOOC, recommendations, IT, career, skills, ICT*

DOI: 10.17587/it.27.102-111

References

1. **Udaltsova N. L.** Russian Digital Economy: State and Development Prospects, Russia, 2019, *Proceedings of the international conference on Technology & entrepreneurship in digital society*, pp. 122—125.

2. **Kuzminov Y., Frumin I., Ovcharova L.** Twelve solutions for new education: report of the Center for Strategic Research and the Higher School of Economics, *Center for Strategic Research in cooperation with the Higher School of Economics*, 2018, available at: https://www.hse.ru /data/2018/04/06/1164671180/Doklad_obrazovanie_Web.pdf (in Russian).

3. **Loshkareva E., Luksha P., Ninenko I., Smagin I., Sudakov D.** Skills of the future. What you need to know and be able to do in a new complex world, *Report of experts from Global Education Futures and WorldSkills Russia*, available at: https://futuref.org/futureskills_ru (date accessed: 10 July 2020). (in Russian).

4. **How to** become a sought-after specialist? *HeadHunter Research*, 2020, available at: https://hh.ru/article/26792?from=article_26787 (date accessed: 29 June 2020) (in Russian).

5. **Teofilov T.** Careers of the Future: 42 Professions of Tomorrow, *Medium*, 2020, available at: https://medium.com/swlh/careers-of-the-future-42-new-professions-of-tomorrow-5d3905f8513 (date accessed: 19 July 2020).

6. **Research** of the Russian market of online education, *Edmarket*, 2020, available at: https://innoagency.ru/files/Issledovanie_rynka_rossiyskogo_online_obrazovania_2020.pdf (date accessed: 10 July 2020) (in Russian).

7. **Laal M., Salamati P.**, Lifelong learning; why do we need it?: *Procedia — Social and Behavioral Sciences*, 2012, vol. 31, pp. 399—403.

8. **Bozkurt A., Stracke C.** Evolution of MOOC Designs, Providers and Learners and the Related MOOC Research and Publications from 2008 to 2018. Proceedings of the *International Open & Distance Learning Conference (IODL19), Anadolu University, Eskişehir, Turkey,* 2019, pp. 13—20.

9. **Build** Skills with Online Courses from Top Institutions, *Coursera*, 2020, available at: https://www.coursera.org/ (date accessed: 08 May 2020).

10. ***EdX*,** 2020, available at: https://www.edx.org/ (date accessed: 10 May 2020).

11. **Learn** the Latest Tech Skills; Advance Your Career, *Udacity,* available at: https://www.udacity.com/ (date accessed: 10 May 2020).

12. **FutureLearn**: Online Courses and Degrees from Top Universities, *FutureLearn*, available at: https://www.futurelearn.com/ (date accessed: 05 May 2020).

13. **Rating** of sites for additional education in IT, *"My Circle", research-2020*, available at: https://habr.com/ru/company/habr_career/blog/454906/ (date accessed: 22 June 2020) (in Russian).

14. **Kostrova A., Alkhov A., Mankovskaya N., Kenik P.** How Russians choose additional education courses, *CourseBurg*, available at: https://courseburg.ru/analytics/Kak_rossiane_vybirayut_kursy_dopolnitelnogo_obrazovania.pdf (date accessed: 02 August 2020) (in Russian).

15. **Skills** and jobs mismatches in low- and middle-income countries, *International Labour Office*, 2019, Geneva, available at: https://www.ilo.org/wcmsp5/groups/public/---ed_emp/documents/publication/wcms_726816.pdf (date accessed: 02 August 2020).

16. **Avdoshin S., Pesotskaya E.** Development of P2P Educational Service in Russia, *Proceedings of the Future Technologies Conference (FTC)*, 2019, vol. 2 Switzerland: Springer, 2020. pp. 833—847.

17. **Ubachs G., Konings L., Nijsten B.** *The 2019 OpenupEd trend report on MOOCs*, 2019, Maastricht, NL, EADTU.

18. **Shah D.** By the Numbers: MOOCs in 2019, *Class Central*, 2019, available at: https://www.classcentral.com/report/mooc-stats-2019/ (date accessed: 12 July 2020).

19. **Bonk C. J., Lee M. M., Reeves T. C.** MOOCs and Open Education around the World, USA, Routledge, 2015.

20. **Career** Development Plan, European Commission, *Research: Publications Office of the European Union*, 2020, available at: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5bd4ed377&appId = PPGMS (date accessed: 14 July 2020).

21. **MIT** Self-Assessment, *MIT*, available at: https://capd.mit.edu/explore-careers/career-first-steps/self-assessment (date accessed: 07 July 2020).

22. **Bates A. W.,** Teaching in a Digital Age. Vancouver BC: Tony Bates Associates Ltd, 2015.

23. **ESCO-European** Skills/Competences, qualifications and Occupations, available at: https://ec.europa.eu/esco/portal/ (date accessed: 14 July 2020).

24. **Ho A. D., Reich J., Nesterko S., Seaton D. T., Mullaney T., Waldo J., Chuang I.,** HarvardX and MITx: The first year of open online courses (HarvardX and MITx Working Paper No. 1), 2014, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2381263 (date accessed: 23 July 2020).

25. **REST** API, available at: https://restfulapi.net/ (date accessed: 23 July 2020).

26. **Coursera**: Join our affiliate program, *Coursera*, available at: https://about.coursera.org/affiliates (date accessed: 23 July 2020).

27. **edX:** Join the edX affiliate program, *edX*, available at: https://www.edx.org/affiliate-program (date accessed: 23.07.2020).

28. **Rocca B.,** Introduction to recommender systems. Towards Data Science, 2019, available at: https://towardsdatascience.com/introduction-to-recommender-systems-6c66cf15ada (date accessed: 23 July 2020).

29. **Anticipating** and matching skills and jobs, *Labour Office*, Geneva, 2015, available at: https://www.ilo.org/wcmsp5/groups/public/---ed_emp/---ifp_skills/documents/publication/wcms_534307.pdf (date: 24 July 2020).

30. **Skills** and jobs mismatches in low- and middle-income countries, *International Labour Office*, Geneva, 2019, available at: https://www.ilo.org/wcmsp5/groups/public/---ed_emp/documents/publication/wcms_726816.pdf (date accessed: 23 July 2020).

31. ***Tadviser*,** available at: https://www.tadviser.ru/index.php/Статья:ИКТ_(мировой_рынок) (date accessed: 23 July 2020). (in Russian).

32. **Petrova J., Podtserob M., Smertina P.** Russian IT-specialists less and less want to work abroad, *Vedemosti*, 2019, available at: https://www.vedomosti.ru/management/articles/2019/06/18/804488-rossiiskie-it-spetsialisti (date accessed: 23 June 2020) (in Russian).

33. **Kolesnikov A.** World trends in the development of information and communicative technologies, *Sciences of Europe*, 2020, vol. 4, no 50, pp. 66—72.

34. **Mail.ru** group, GeekBrains study: three quarters of schoolchildren and students consider IT professions to be promising, *mail.ru group (research)*, 2019, available at: https://corp.mail.ru/ru/press/infograph/10487/ (date accessed: 24 June 2020) (in Russian).

31 мая – 4 июня 2021 г., ДГТУ, г. Ростов-на-Дону, Россия

Международная научная мультиконференция

"КИБЕР-ФИЗИЧЕСКИЕ СИСТЕМЫ: ПРОЕКТИРОВАНИЕ И МОДЕЛИРОВАНИЕ" "CYBER-PHYSICAL SYSTEMS DESIGN AND MODELLING" (CYBERPHY-2021) (SCOPUS, SPRINGER)

Секции

1. Cyber-Physical Systems: digital technologies and applications (Кибер-физические системы: цифровые технологии и приложения)
2. Cyber-physical systems: design and application for Industry 4.0 (Кибер-физические системы: проектирование и применение для Индустрии 4.0)
3. Cyber-Physical Systems: Modelling and Intelligent Control (Кибер-физические системы: моделирование и интеллектуальное управление)
4. Society 5.0: Cyberspace for advanced human-centered society (Общество 5.0: киберпространство для развитого общества, ориентированного на человека)

XXXIV Международная научная конференция

МАТЕМАТИЧЕСКИЕ МЕТОДЫ В ТЕХНИКЕ И ТЕХНОЛОГИЯХ - ММТТ-34 (РИНЦ, DOI)

Секции

1. Качественные и численные методы исследования дифференциальных и интегральных уравнений
2. Оптимизация, автоматизация и оптимальное управление технологическими процессами
3. Математическое моделирование технологических и социальных процессов
4. Математическое моделирование и оптимизация в задачах САПР, аддитивных технологий, цифрового производства
5. Математические методы в задачах радиотехники, радиоэлектроники и телекоммуникаций, геоинформатики, авионики и космонавтики
6. Математические методы и интеллектуальные системы в робототехнике и мехатронике
7. Математические методы в медицине, биотехнологии и экологии
8. Математические методы в экономике и гуманитарных науках
9. Информационные и интеллектуальные технологии в технике и образовании
10. Математические и инструментальные методы технологий Индустрии 4.0
11. Обсуждение квалификационных работ

Подача заявок на участие с 15 декабря 2020 г.

Подробная информация о конференции и условиях участия в ней размещается на сайте http://mmtt.sstu.ru/

Адрес редакции:

107076, Москва, Стромынский пер., 4

Телефон редакции журнала **(499) 269-5510**
E-mail: it@novtex.ru

Технический редактор *Е. В. Конова*.
Корректор *М. Ю. Безменова*.
Сдано в набор 07.12.2020. Подписано в печать 28.01.2021. Формат 60×88 1/8. Бумага офсетная.
Усл. печ. л. 8,86. Заказ IT221. Цена договорная.

Журнал зарегистрирован в Министерстве Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации ПИ № 77-15565 от 02 июня 2003 г.

Оригинал-макет ООО "Адвансед солюшнз". Отпечатано в ООО "Адвансед солюшнз".
119071, г. Москва, Ленинский пр-т, д. 19, стр. 1. Сайт: **www.aov.ru**

Рисунки к статье А. Б. Терентьева, И. В. Штурца

«УСТРАНЕНИЕ АЛИАСИНГА В ДОППЛЕРОВСКОЙ ЭХОКАРДИОГРАФИИ С ПОМОЩЬЮ ФИЛЬТРАЦИИ СУБМАКСИМАЛЬНЫХ КОМПОНЕНТ СКОРОСТЕЙ»

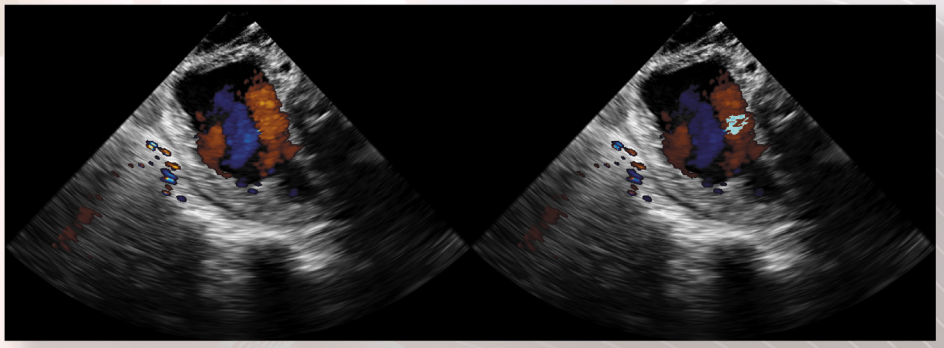


Рис. 4. Пример некорректного устранения алиасинга

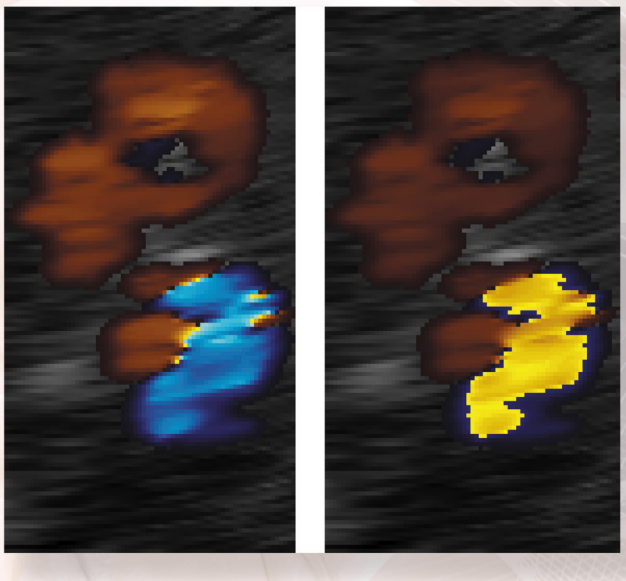
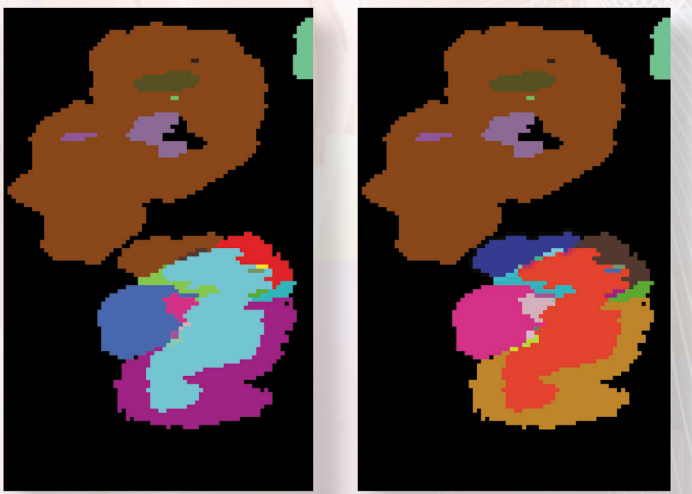


Рис. 5. Пример некорректного устранения алиасинга на фрагменте



а) *б)*

Рис. 6. Разбиение фрагмента кадра 22 из набора #4 на компоненты с помощью 8-смежности (*а*) и 4-смежности (*б*). В случае 4-смежности решена проблема смежности с большой областью над регионом неверно определённого алиасинга

Издательство «НОВЫЕ ТЕХНОЛОГИИ»

выпускает *научно-технические журналы*

Ежемесячный теоретический
и прикладной научно-технический журнал

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

В журнале освещаются современное состояние, тенденции и перспективы развития основных направлений в области разработки, производства и применения информационных технологий.

Подписной индекс по Объединенному каталогу
«Пресса России» – 72656

Подписной индекс по Объединенному каталогу
«Пресса России» – 79963

Научно-практический
и учебно-методический журнал

БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

В журнале освещаются достижения и перспективы в области исследований, обеспечения и совершенствования защиты человека от всех видов опасностей производственной и природной среды, их контроля, мониторинга, предотвращения, ликвидации последствий аварий и катастроф, образования в сфере безопасности жизнедеятельности.

Междисциплинарный
теоретический и прикладной
научно-технический журнал

НАНО- и МИКРОСИСТЕМНАЯ ТЕХНИКА

В журнале освещаются современное состояние, тенденции и перспективы развития нано- и микросистемной техники, рассматриваются вопрос разботки и внедрения нанои микросистем в различные области науки, технологии и производства.

Подписной индекс по Объединенному каталогу
«Пресса России» – 79493

Подписной индекс по Объединенному каталогу
«Пресса России» – 79492

Ежемесячный теоретический
и прикладной
научно-технический журнал

МЕХАТРОНИКА, АВТОМАТИЗАЦИЯ, УПРАВЛЕНИЕ

В журнале освещаются достижения в области мехатроники, интегрирующей механику, электронику, автоматику и информатику в целях совершенствования технологий производства и создания техники новых поколений. Рассматриваются актуальные проблемы теории и практики автомати ческого и автоматизированного управления техническими объектами и технологическими процессами в промышленности, энергетике и на транспорте.

Теоретический
и прикладной
научно-технический журнал

ПРОГРАММНАЯ ИНЖЕНЕРИЯ

В журнале освещаются состояние и тенденции развития основных направлений индустрии программного обеспечения, связанных с проектированием, конструированием, архитектурой, обеспечением качества и сопровождением жизненного цикла программного обеспечения, а также рассматриваются достижения в области создания и эксплуатации прикладных программно-информационных систем во всех областях челове ческой деятельности.

Подписной индекс по Объединенному каталогу
«Пресса России» – 22765

Адрес редакции журналов для авторов и подписчиков:
107076, Москва, Стромынский пер., 4. Издательство "НОВЫЕ ТЕХНОЛОГИИ".
Тел.: (499) 269-55-10, 269-53-97. Факс: (499) 269-55-10. E-mail: antonov@novtex.ru

ISSN 1684-6400. Информационные технологии. 2021. Том 27. № 2. 57–112. Индекс: 72656 (Объединенный каталог «Пресса России»)