ISSN 1684–8853

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

НАУЧНЫЙ ЖУРНАЛ

5(84)/2016

doi:10.15217/issn1684-8853.2016.5

ISSN 1684-8853

SCIENTIFIC JOURNAL

5(84)/2016

INFORMATSIONNO-UPRAVLIAIUSHCHIE SISTEMY
(INFORMATION AND CONTROL SYSTEMS)

REFEREED EDITION

Contact information
The Editorial and Publishing Center, SUAI
67, B. Morskaia, 190000, St. Petersburg, Russia
Website: http://i-us.ru/en, E-mail: ius.spb@gmail.com
Tel.: +7 - 812 494 70 02

The Journal was registered in the Ministry of Press,
Broadcasting and Mass Media of the Russian Federation.
Registration Certificate JD № 77-12412 from April, 19, 2002.
Re-registration in the Federal Service for Supervision in the Sphere of Telecom,
Information Technologies and Mass Communications (ROSKOMNADZOR)
due to change of the founder: «Information and Control Systems», Ltd.,
JD № FS77-49181 from March, 30, 2012.

Submitted for publication 05.09.16. Passed for printing 21.10.16. Format 60×84$_{1/8}$.
Offset paper. Phototype SchoolBookC. Digital printing.

Layout original is made at the Editorial and Publishing Center, SUAI.
67, B. Morskaia, 190000, St. Petersburg, Russia
Printed from slides at the Editorial and Publishing Center, SUAI.
67, B. Morskaia, 190000, St. Petersburg, Russia

The journal is distributed by subscription. Subscription can be made in the Editorial and publishing center, SUAI as well as in any post office based on «Rospechat» catalogue:
№ 48060 — annual subscript, № 15385 — semiannual subscript.

doi:10.15217/issn1684-8853.2016.5

ISSN 1684-8853

НАУЧНЫЙ ЖУРНАЛ

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

5(84)/2016

РЕЦЕНЗИРУЕМОЕ ИЗДАНИЕ

Учредитель
ООО «Информационно-управляющие системы»

Издатель
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Адрес редакции: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Тел.: (812) 494-70-02, e-mail: ius.spb@gmail.com, сайт: http://i-us.ru

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации ПИ № 77-12412 от 19 апреля 2002 г.
Перерегистрирован в Роскомнадзоре.
Свидетельство о регистрации ПИ № ФС77-49181 от 30 марта 2012 г.

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

Сдано в набор 05.09.16. Подписано в печать 21.10.16. Формат 60×84 1/8.
Бумага офсетная. Гарнитура SchoolBookC. Печать цифровая.
Усл. печ. л. 12,3. Уч.-изд. л. 16,9. Тираж 1000 экз (1-й завод 150 экз). Заказ 390.
Оригинал-макет изготовлен в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.
Отпечатано с готовых диапозитивов в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.

Журнал распространяется по подписке. Подписку можно оформить через редакцию, а также в любом отделении связи по каталогу «Роспечать»: № 48060 — годовой индекс, № 15385 — полугодовой индекс.

УДК 519.614
doi:10.15217/issn1684-8853.2016.5.2

МАТРИЦЫ МЕРСЕННА И АДАМАРА, ПРОИЗВЕДЕНИЯ

Н. А. Балонин[a]***,*** *доктор техн. наук, профессор*
М. Б. Сергеев[a]***,*** *доктор техн. наук, профессор*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Цель исследования: *показать возможность обобщения кронекерова произведения с последующей коррекцией элементов на малоуровневые квазиортогональные матрицы локального максимума детерминанта для получения матриц того же качества (малоуровневых) высокой размерности, в частности матриц Адамара и Мерсенна.* ***Результаты:*** *показано, что сложность формул коррекции произведения Кронекера малоуровневых квазиортогональных матриц (критских матриц) зависит от типа симметрии сомножителей, порядка их следования и близости размеров сомножителей между собой. Описаны типы возможных сомножителей: виды их симметрии, зависимость симметрии от размера матрицы и ее положения в цепочке критских матриц возрастающих порядков. Приведены таблицы симметрированных матриц. Обобщено произведение Скарпи матрицы Адамара на ее ядро или округленную матрицу Мерсенна; показано, что перестановка симметрированных сомножителей позволяет умножать матрицы Адамара как простых, так и составных порядков. Техника кронекерова произведения расширена на сомножители, разница порядков которых (дистанция) не превышает 4. Показано, что произведение матриц Мерсенна порядков $4t + 1$ и Зейделя порядков $4t - 1$ порождает регулярные матрицы Адамара с равными друг другу суммами столбцов. Разнесение порядков сомножителей ведет к блочным структурам, в которых отличные от 1 и –1 элементы встречаются только на диагонали.* ***Практическая значимость:*** *алгоритмы нахождения критских матриц использованы при построении исследовательского программного комплекса. Субоптимальные по детерминанту матрицы составляют основу фильтров Мерсенна и Ферма, применяемых для сжатия и маскирования изображений.*

Ключевые слова *— кронекерово произведение, ортогональные матрицы, критские матрицы, матрицы Адамара, конференц-матрицы, матрицы Мерсенна, матрицы Ферма, обобщенный метод Скарпи, циклические матрицы.*

Введение

В статье [1] подводится итог работы с квазиортогональными матрицами локального максимума детерминанта. Основной вывод этого исследования состоит в том, что между числами и экстремальными по детерминанту матрицами существует взаимно однозначное соответствие.

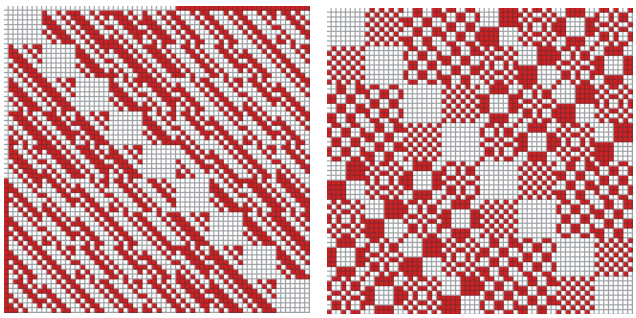
Например, субоптимальные по детерминанту циклические матрицы Зейделя **S** порядков (с некоторыми пропусками) $n = 4t + 1$ и циклические матрицы Мерсенна **M** порядков $n = 4t - 1$ (без пропусков), t — целое число, строго симметричны или асимметричны соответственно, если n — простое число. Аналогичные матрицы составных порядков состоят из циклических блоков, что отвечает мультипликативному разложению чисел на составные части. Большая часть элементов субоптимальных матриц равна 1, остальные отрицательные элементы меньше по модулю 1. Причем с ростом порядка n значения элементов обоих типов матриц стремятся к 1 и –1 соответственно, но никогда не достигают предельных значений.

Поэтому интересно, что при взаимном вложении матриц **S** по месту элементов **M** (или наоборот), с учетом знаков, элементы итоговой расширенной квазиортогональной матрицы, называемой *витражом*, могут приблизиться к 1 и –1, а при определенных условиях и стать равными им, когда витраж переходит в недостижимое для оригиналов новое качество. Условия эти отвечают представлению о связи чисел и матриц, так как витраж с элементами 1 и –1 порождают максимально близкие по порядкам матрицы **S** и **M** (дополнительное требование такого построения состоит в коррекции структуры диагональных блоков и добавлении каймы). Перед нами матричное обобщение свойств близких пар целых чисел.

Порядок витража размера $(4t + 1)(4t - 1)$, наращиваемого каймой, равен четному числу $n = 4u^2$, u — целое число, это характерный порядок так называемых *регулярных* матриц Адамара **H** с элементами 1 и –1, все суммы ортогональных между собой строк и столбцов равны между собой. Если в построении витража используются блоки строго симметричные и асимметричные, то добиться равенства сумм элементов несложно, перед нами, по сути, теория построения регулярных матриц Адамара.

Для четных значений u регулярную матрицу можно построить вложением матрицы Адамара **H** порядка $\sqrt{n}$ в саму себя *без каймы*. Она отличается от матрицы с каймой, состоящей из циклических блоков, наличием блоков разной частоты, оцениваемой по количеству смен знаков элементов в столбце (рис. 1).

Необходимое условие существования матриц Зейделя — разложимость порядка в сумму квадратов, регулярные матрицы с ними имеют пропуски. Например, число $n = 4t + 1 = 21$ не раскла-



■ *Рис. 1.* Блочные регулярные матрицы Адамара с каймой и без каймы

дывается в сумму квадратов, регулярной матрицы размера $n = (4t + 1)(4t - 1) + 1 = 21 \times 19 = 400$ с каймой нет, но $400 = 4u^2 = 20 \times 20$, для четного $u = 10$, соответственно, есть регулярная матрица без каймы.

Выделяют еще, например, матрицы Буша на основе латинских квадратов, без каймы, сегодня известно всего три такие матрицы порядков 36, 100 и 324. Матрица Буша порядка 196 не известна, но она, в свою очередь, легко строится с помощью матриц Мерсенна и Зейделя. К сожалению, для порядка $n = 21 \times 23 = 484$ нет версий отмеченных матриц, а регулярная структура, предположительно, существует.

Хотя все такие матрицы смотрятся как дополняющие друг друга, мы предлагаем не путать их между собой, поскольку они отражают разные по содержанию разложения целых чисел n.

Настоящая статья ставит целью более полно отразить тему матричных вложений *критских* матриц (квазиортогональных матриц с относительно небольшим числом элементов) как обобщений кронекерова произведения для них.

Кронекерово произведение и его обобщения

В теории ортогональных матриц кронекерову произведению $\mathbf{A} \otimes \mathbf{B}$ отведена роль генератора ортогональных матриц повышенной размерности. Его можно описать как вставку матрицы $\mathbf{B}$ по месту элементов матрицы $\mathbf{A}$ с умножением на эти элементы:

$$\mathbf{A} \otimes \mathbf{B} = \begin{pmatrix} a_{11}\mathbf{B} & a_{12}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ a_{21}\mathbf{B} & a_{22}\mathbf{B} & \cdots & a_{2n}\mathbf{B} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}\mathbf{B} & a_{n2}\mathbf{B} & \ldots & a_{nn}\mathbf{B} \end{pmatrix}.$$

Ортогональность — инвариант этого произведения по отношению к возможной замене сомножителей: какие бы ортогональные по столбцам (строкам) матрицы мы ни брали, результатом будет матрица с тем же качеством.

К сожалению, если матрицы-сомножители $\mathbf{A}$ и $\mathbf{B}$ имеют значения элементов (уровни), отличные от 1 и –1, кронекерово произведение заметно увеличивает их количество. Рост числа уровней нежелателен в том случае, когда матрицы разбиваются на классы эквивалентности в соответствии с количеством и значениями их элементов.

Это касается обобщения матриц Адамара на дополнительные четные и нечетные порядки [1, 2], называемые *критскими матрицами* [3].

Для бинарных критских матриц кронекерово произведение описывает структуру, которую несложно свести снова к бинарной матрице коррекцией ее элементов. Вскоре после первой публикации матриц Адамара [4] на это обратил внимание Скарпи [5], взяв в качестве сомножителей матрицы близких четного и нечетного порядков.

Упрощая метод Скарпи, Пэли [6] исключил из рассмотрения матрицы нечетных порядков. Он воспользовался тем, что трехуровневые конференц-матрицы Белевича [7] четных порядков либо кососимметричны, либо симметричны, что сокращает формулу поправки. Кронекерово произведение матриц Адамара не создает таких проблем, поскольку их элементы имеют значения 1 и –1.

Две конструкции Пэли сводятся к следующему.

Кососимметричная матрица Белевича $\mathbf{C}$ порядка $n = 4t$, t — целое число, дает матрицу Адамара коррекцией нулевой диагонали $\mathbf{H} = \mathbf{C} + \mathbf{I}$, где $\mathbf{I}$ — единичная матрица. Ортогональность столбцов — инвариант, не зависящий от значений элемента диагонали.

Результат кронекерова произведения матрицы $\mathbf{C}$ четного порядка $n = 4t - 2$ на матрицу Адамара $\mathbf{H}_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ порядка $m = 2$ есть матрица Адамара удвоенного порядка $2n$ после аналогичной поправки нулевых элементов первого сомножителя непосредственно в формуле кронекерова произведения $\mathbf{H} = \begin{pmatrix} \mathbf{C}+\mathbf{I} & \mathbf{C}-\mathbf{I} \\ \mathbf{C}-\mathbf{I} & -\mathbf{C}-\mathbf{I} \end{pmatrix}$.

При обратной вставке с учетом знаков элементов в матрицу $\mathbf{C}$ матрицы $\mathbf{H} = \begin{pmatrix} \mathbf{H}_{11} & \mathbf{H}_{12} \\ \mathbf{H}_{21} & \mathbf{H}_{22} \end{pmatrix}$ поправки касаются, что характерно для реверсных вставок, только диагонали — по месту нулей в $\mathbf{C}$ размещается $\bar{\mathbf{H}} = \begin{pmatrix} \mathbf{H}_{21} & \mathbf{H}_{22} \\ -\mathbf{H}_{11} & -\mathbf{H}_{12} \end{pmatrix}$.

Отметим, что поправки к кронекерову произведению критских матриц [3] также упрощаются, если брать их в симметричной или антисимметричной форме и использовать реверсную вставку.

Критские матрицы

Критские матрицы — квадратные, ортогональные по столбцам (строкам) матрицы, содержащие небольшое количество различных по зна-

чению элементов — уровней. Бинарные критские матрицы имеют всего два уровня $a = 1$ и $-b$, $b \le 1$. Значение b зависит от размера матрицы, эта зависимость называется *функцией уровня*.

На четных порядках $4t - 2$ критские матрицы — бициклические матрицы вида $\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix}$. Оба блока **A** и **B** зависят от значений двух элементов $a = 1$ и $-b$.

Порядки $4t - 3$ (или $4t + 1$) сложнее прочих тем, что ортогональность матриц достижима при введении дополнительного уровня d для элементов диагонали (матрицы Зейделя) или каймы s (матрицы Ферма). Формулы для вычисления значения уровней основных семейств критских матриц приведены в табл. 1.

Договоримся обозначать округленные до целых значений критские матрицы Ферма (**F**) порядков $n = 4t + 1$, Адамара (**H**) порядков $n = 4t$, Мерсенна (**M**) порядков $n = 4t - 1$, Эйлера (**E**) порядков $n = 4t - 2$, Зейделя (**S**) порядков $n = 4t - 3$ буквами без подчеркивания. Будем обозначать $\underline{\mathbf{F}}$, $\underline{\mathbf{H}}$, $\underline{\mathbf{M}}$, $\underline{\mathbf{E}}$ и $\underline{\mathbf{S}}$, соответственно, матрицы, ортогонализованные выбором предписанных значений отрицательных элементов, элементов диагонали и каймы.

Матрицы Эйлера отличаются от других матриц разделяемых четных порядков тем, что это бициклические матрицы, существующие всегда. Они замещают симметричные матрицы Белевича в том случае, если последних нет, а необходимое условие их существования связано с известной в теории чисел теоремой Эйлера — Ферма [1].

Матрица $\underline{\mathbf{H}} = \mathbf{H}$. Матрица $\mathbf{S} = \mathrm{sign}(\underline{\mathbf{S}})$ совпадает с точностью до диагонали с целочисленной матрицей Зейделя (adjacency matrix) матричного описания графов: узлы нумеруются одинаково с номерами строк и столбцов матрицы, взаимно связанные узлы помечаются элементом 1, на диагонали (по договоренности) 0, прочие элементы равны –1. Критские матрицы Зейделя ортогональны по столбцам, они отличаются от целочисленной матрицы Зейделя значениями отрицательных элементов и наличием ненулевых элементов диагонали d.

Симметричные и кососимметричные матрицы

Симметричные и кососимметричные матрицы с нулем на диагонали и прочими элементами 1 и –1 начал исследовать Эрнст Якобсталь, ученик Фробениуса и Шура. В начале прошлого века в диссертации по квадратичным вычетам он выделил близкие к ортогональным целочисленные матрицы, удовлетворяющие матричному уравнению $\mathbf{Q}^{\mathrm{T}}\mathbf{Q} = n\mathbf{I} - \mathbf{J}$, где **I**, **J** — единичная матрица и матрица, состоящая полностью из единиц, причем $\mathbf{QJ} = \mathbf{JQ} = \mathbf{0}$.

Циклическая матрица Якобсталя **Q** построена на векторе символов Лежандра $\left(\frac{k}{n}\right)$, где $k = 0, \ldots, n - 1$. Она симметрична $\mathbf{Q}^{\mathrm{T}} = \mathbf{Q}$ для $n = 4t - 3$ или кососимметрична $\mathbf{Q}^{\mathrm{T}} = -\mathbf{Q}$ для $n = 4t - 1$, где n — простое число.

Симметричная матрица Якобсталя **Q** порядка $n = 4t - 3$ совпадает с матрицей Зейделя

■ ***Таблица 1***. Значения уровней семейств матриц

Символ	Порядок n	Матрица	Значения элементов
H	$4t$	Адамара	1, –1
C	$2t$, $4t$	Белевича	1, –1, 0
W	t, $2t$, $3t$, $4t$	Себерри (взвешенная)	1, –1, 0
M	$4t - 1$	Мерсенна	$1, -b$, где $b = \dfrac{t}{t + \sqrt{t}}$
E	$4t - 2$	Эйлера	$1, -b$, где $b = \dfrac{t}{t + \sqrt{2t}}$
S	$4t - 3$	Зейделя	$1, -b, d$, где $b = 1 - 2d$, $d = \dfrac{1}{1 + \sqrt{n}}$
F	$4t - 3$	Ферма	$1, -b, s$, где $q = n - 1 = 4u^2$, $p = q + \sqrt{q}$, $b = \dfrac{2n - p}{p} = 1 - \dfrac{2u - 1}{2u + 1}\dfrac{1}{u}$, $s = \dfrac{\sqrt{nq - 2\sqrt{q}}}{p} = \dfrac{\sqrt{nu - 1}}{2u + 1}\dfrac{1}{\sqrt{u}}$

теории графов. В теории критских матриц $\mathbf{S} = \mathrm{sign}(\underline{\mathbf{S}}) = \mathbf{Q} + \mathbf{I}$. Наращиванием каймы из единичных элементов матрица $\mathbf{Q}$ приводится к матрице Белевича $\mathbf{C}$.

Кососимметричная матрица Якобсталя $\mathbf{Q}$ порядка $n = 4t - 1$ порождает матрицу Мерсенна $\mathbf{M}$ в виде $\mathbf{M} = \mathbf{Q} + \mathbf{I}$. Обратное утверждение не верно. В самом деле, циклические матрицы $\mathbf{M}$ составных порядков [1], являющихся произведениями пар близких чисел $3 \cdot 5 = 15$, $5 \cdot 7 = 35$ и т. п., не имеют оси симметрии и адекватных им матриц $\mathbf{Q}$.

Матрица $\mathbf{M}$ не обязана быть кососимметричной, множество таких матриц шире, чем множество кососимметричных матриц $\mathbf{Q}$.

При построении матриц большое значение имеют цепочки критских матриц [2, 8].

Цепочки критских матриц

Кососимметричные матрицы $\mathbf{M}$ порядков $n = 4t - 1$ и симметричные матрицы $\mathbf{S}$ порядков $n = 4t - 3$ сходны вплоть до алгоритмов их построения замещением диагонали матриц $\mathbf{Q}$. Тем не менее эти матрицы существенно различаются. Бициклическая форма порождает матрицу Эйлера удвоенного порядка $\underline{\mathbf{E}} = \begin{pmatrix} \underline{\mathbf{M}} & \underline{\mathbf{M}} \\ \underline{\mathbf{M}}^{\mathrm{T}} & -\underline{\mathbf{M}}^{\mathrm{T}} \end{pmatrix}$, матрица Эйлера с каймой приводит к новой матрице $\mathbf{M}$ отличного на единицу порядка [2].

Возникают цепочки матриц вида **M–E–M–E–M–E...**, описывающие рост порядков матриц при их рекурсивном вычислении. Матрицы Зейделя не выстраиваются в рекурсии матриц нечетного порядка. Матрица Зейделя порождает только первую матрицу Эйлера. Цепочка имеет вид **(S)–E–M–E–M–E...** . Скобки означают, что матрица Зейделя не всегда существует. Если матрицы Зейделя нет (невозможно реверсное расщепление стартовой матрицы Эйлера с выделением матрицы Зейделя половинного размера), матрица Эйлера все равно существует. Аналогичные связи существуют между матрицами Адамара и Белевича — матрицы Белевича используются для построения матриц Адамара, если они есть. Отсутствие матриц Белевича не исключает существования матриц Адамара.

Цепочки говорят о том, что матрицы Адамара, Мерсенна, Эйлера можно ранжировать порядковым номером их нахождения в цепочке. У матриц Зейделя порядковый номер всегда начальный. Добавление каймы к матрице $\mathbf{S}$ дает матрицу $\mathbf{C}$. Добавление каймы к матрице $\mathbf{M}$ дает матрицу $\mathbf{H}$. Полная цепочка имеет вид

$$\begin{array}{ccccccc} \mathbf{(S)} & - & \mathbf{E} & - & \mathbf{M} & - & \mathbf{E} - \mathbf{M} - \ldots \\ | & & | & & | & & \\ \mathbf{(C)} & & \mathbf{H} & & \mathbf{H} & & -\ldots \end{array} .$$

Стартовые матрицы цепочек следует выделить особо, это матрицы упрощенной структуры, а их порядки связаны с простыми числами, близкими парами целых чисел, или степенями простых чисел.

Цепочки критских матриц с заданной симметрией

Для получения новых ортогональных матриц с нужными свойствами, если циклическая матрица уже не может быть ортогональной, используются бициклические формы с каймой на порядках, соответствующих аддитивному разложению $n = 2q + 1$, когда

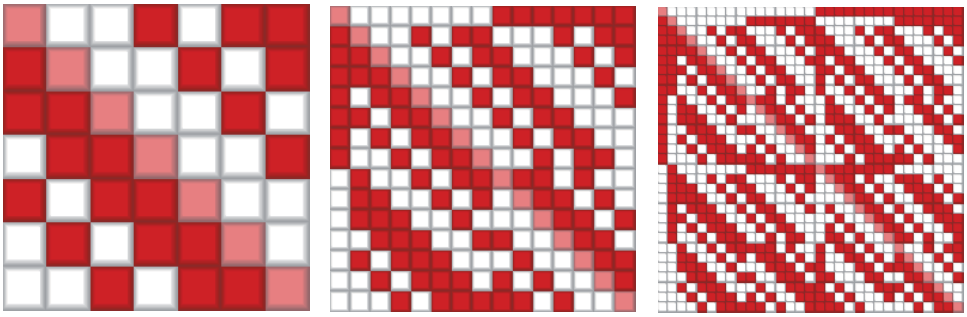
$$\mathbf{S} = \begin{pmatrix} \mathbf{1} & -\mathbf{e}^{\mathrm{T}} & \mathbf{e}^{\mathrm{T}} \\ -\mathbf{e} & \mathbf{A} & \mathbf{B} \\ \mathbf{e} & \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix}; \quad \mathbf{M} = \begin{pmatrix} \mathbf{1} & \mathbf{e}^{\mathrm{T}} & -\mathbf{e}^{\mathrm{T}} \\ -\mathbf{e} & \mathbf{A} & \mathbf{B} \\ \mathbf{e} & -\mathbf{B}^{\mathrm{T}} & \mathbf{A}^{\mathrm{T}} \end{pmatrix}.$$

Симметричная матрица Зейделя строится на основе блоков $\mathbf{A}$ и $\mathbf{B}$ четного порядка, являющихся предикторами разложения симметричной структуры, тогда как составными частями матрицы Мерсенна могут быть как матрицы Мерсенна, так и Зейделя меньшего порядка. Для $q = 4t - 3$, являющегося числом Мерсенна или простым числом, осуществляется переход от кососимметричной циклической матрицы Мерсенна $\mathbf{A} = \mathbf{M}_q$, $\mathbf{B} = \mathbf{M}_q$ порядка q к бициклической матрице Эйлера порядка $2q$ и далее к следующей матрице $\mathbf{M}_n$ порядка $n = 2q + 1$. Для $q = 4t - 1$, являющегося простым числом, циклическая матрица Зейделя $\mathbf{B} = \mathbf{S}_q$ симметрична и дает половину нужного результата. Комплементарная ей кососимметричная матрица $\mathbf{A}$ ищется отдельно.

Циклические матрицы $\mathbf{M}$ принадлежат к трем семействам [1] порядков, вложенных в последовательность нечетных чисел $n = 4t - 1$. Это числа Мерсенна вида $2^k - 1$, где k — натуральное число, простые числа и произведения пар простых чисел.

Кососимметричные матрицы соответствуют только первым двум семействам, что повышает их роль в качестве потенциальных сомножителей. Здесь сказывается различие матриц $\mathbf{M}$, служащих для построения связанных с ними матриц $\mathbf{H}$ на единицу большего порядка (или матриц $\mathbf{H}$ более высоких порядков через рекурсию $n = 2q + 1$, где q — предыдущий порядок), и кососимметричных матриц $\mathbf{M}$, соответствующих матрицам $\mathbf{Q}$. Вторые пригодны в качестве сомножителей корректируемого кронекерова произведения для построения матриц $\mathbf{H}$ дополнительных порядков. Для других цепочек матрицы должны быть более тщательно отобраны.

Портреты кососимметричных матриц $\mathbf{Q}$ порядков 7, 15, 31, входящих в критскую цепочку, приведены на рис. 2.



■ ***Рис. 2.*** Цепочка матриц Якобсталя **Q** порядков 7, 15, 31

Порядок 15 — непростое число, являющееся произведением пар близких чисел $3 \cdot 5 = 15$. Это означает, что существует некососимметрическая циклическая матрица $\mathbf{M}_{15}$, пригодная для построения матрицы $\mathbf{H}_{16}$, но не пригодная как сомножитель корректируемого кронекерова произведения. Вместо нее следует использовать вторую кососимметрическую матрицу приведенной выше критской цепочки.

В связи с разнообразием структур критских матриц возникает необходимость их систематизации по виду симметрии: циклические (Ц) и бициклические (Б) (табл. 2).

Матриц Якобсталя порядков $n = 4t - 3$ нет, если n — не квадрат суммы квадратов двух целых чисел. Эти пропуски невосполнимы — их положение в таблице отличается упорядоченностью: начиная с $n = 21$, сложные порядки следуют с шагом 12.

Следующие с шагом 20 порядки 5, 25, 45, 65 и 85 известны тем, что первая пара 5 и 25 допускает бициклическое решение, промежуточный порядок 45 встречается в теории графов и разрешим в конструкции Матона [9]. Вторая пара 65 и 85 хорошо известна в теории матриц Белевича: это первые неразрешенные порядки. Они требуют уникальной структуры, если она вообще есть.

Максимальная сложность матриц Мерсенна — бицикл с каймой [1], это всего лишь вторая позиция в цепочках критских матриц. Для их поиска применимы методы теории конечных полей Галуа [1]. Матрицы Зейделя входят в состав некоторых бициклических форм матриц Мерсенна, такая симметричная основа вызывает противоречие при поиске кососимметричного варианта решения. Как правило, порядки, связанные с матрицами Зейделя прямо или опосредованно, неразрешимы. Произведение критских матриц требует только кососимметричных структур, поэтому в таблице возникают пропуски.

Кососимметричные матрицы Мерсенна составных порядков существуют, если они являются матрицам критских цепочек, начинающихся от матриц порядков чисел Мерсенна или простых порядков $n = 4t - 1$. Матрицы Зейделя являются

■ ***Таблица 2.*** Циклические и бициклические матрицы Якобсталя

n	Тип	Ц	Б	n	Тип	Ц	Б	n	Тип	Ц	Б	n	Тип	Ц	Б
1	**S**	+	–	25	**S**	–	+	49	**S**	–	+	73	**S**	+	+
3	**M**	+	+	27	**M**	–	+	51	**M**	–	–	75	**M**	–	+
5	**S**	+	+	29	**S**	+	+	53	**S**	+	+	77	**S**	Нет	Нет
7	**M**	+	+	31	**M**	+	+	55	**M**	–	–	79	**M**	+	+
9	**S**	–	+	33	**S**	Нет	Нет	57	**S**	Нет	Нет	81	**S**	–	+
11	**M**	+	+	35	**M**	–	–	59	**M**	+	+	83	**M**	+	+
13	**S**	+	+	37	**S**	+	+	61	**S**	+	+	85	**S**	–	–
15	**M**	–	+	39	**M**	–	+	63	**M**	+	+	87	**M**	–	+
17	**S**	+	+	41	**S**	+	+	65	**S**	–	–	89	**S**	+	+
19	**M**	+	+	43	**M**	+	+	67	**M**	+	+	91	**M**	–	–
21	**S**	Нет	Нет	45	**S**	–	–	69	**S**	Нет	Нет	93	**S**	Нет	Нет
23	**M**	+	+	47	**M**	+	+	71	**M**	+	+	95	**M**	–	+

предикторами цепочек — это матрицы без предыстории. Соответственно, два последних столбца таблицы составлены на основании оптимистических предположений о матрицах Зейделя высоких порядков и нуждаются в проверке.

Первый критический порядок, на котором нет ни циклической, ни бициклической кососимметричных матриц, — 35. Такие числа возникают во многих задачах теории ортогональных матриц, это первый критический порядок для матриц Вильямсона. Порядки 9, 25, 27, 81 — степени простых чисел 3 и 5, для которых существуют блочные матрицы Якобсталя, находимые по рекурсивным формулам Белевича: $\mathbf{Q} \otimes \mathbf{Q} + \mathbf{I} \otimes \mathbf{J} - \mathbf{J} \otimes \mathbf{I}$ соответствует квадрату порядка, $\mathbf{Q} \otimes \mathbf{Q} \otimes \mathbf{Q} + \mathbf{Q} \otimes \mathbf{I} \otimes \mathbf{J} + \mathbf{I} \otimes \mathbf{J} \otimes \mathbf{Q} + \mathbf{J} \otimes \mathbf{Q} \otimes \mathbf{I}$ — кубу порядка. С ними связаны порядки $51 = 2 \cdot 25 + 1$, $55 = 2 \cdot 27 + 1$, для которых нет циклической и бициклической структур, но есть промежуточные структуры.

Гипотеза о кососимметрии всех матриц Мерсенна

Отсутствие циклической структуры не означает, что матрицы нет вообще. Кососимметрические матрицы Мерсенна есть для любых выделенных им порядков. Это не доказанное предположение, но оно следует из связи матриц Мерсенна с кососимметричными матрицами Адамара [1].

Порядки, равные числам Мерсенна, выделены тем, что существование решения в виде кососимметричной циклической матрицы не зависит от их простоты.

К ним примыкают матрицы, построенные для простых чисел $n = 4t - 1$. Остальные кососимметричные матрицы должны быть блочными, каковыми являются матрицы критских цепочек. Параметры элементов первых строк **a**, **b** циклических блоков **A** и **B** матриц Якобсталя приведены в табл. 3.

■ ***Таблица 3.*** Первые строки бициклических матриц Якобсталя

n	q	Тип	Первая строка **a** блока **A**	Первая строка **b** блока **B**
3	1	**M**	[0]	[1]
5	2	**S**	[0,1]	[–1,1]
7	3	**M**	[0,1,–1]	[1,1,–1]
9	4	**S**	[0,1,–1,1]	[1,1,–1,–1]
11	5	**M**	[0,1,–1,1,–1]	[1,1,–1,–1,1]
13	6	**S**	[0,–1,1,1,1,–1]	[–1,–1,1,1,–1,1]
15	7	**M**	[0,1,1,–1,1,–1,–1]	[1,1,1,–1,1,–1,–1]
17	8	**S**	[0,–1,1,1,–1,1,1,–1]	[1,1,1,–1,–1,–1,1,–1]
19	9	**M**	[0,–1,–1,–1,1,–1,1,1,1]	[–1,1,1,–1,1,–1,1,1,–1]
21	10	**S**	Нет	Нет
23	11	**M**	[0,1,–1,1,1,1,–1,–1,–1,1,–1]	[1,1,–1,1,1,1,–1,–1,–1,1,–1]
25	12	**S**	[0,1,–1,–1,1,1,–1,1,1,–1,–1,1]	[1,–1,1,1,1,1,–1,–1,–1,–1,1,–1]
27	13	**M**	[0,–1,1,–1,1,1,1,–1,–1,–1,1,–1,1]	[1,1,–1,1,1,–1,–1,–1,–1,1,1,–1,1]
29	14	**S**	[0,1,–1,1,–1,–1,1,1,1,–1,–1,1,–1,1]	[1,–1,–1,1,1,–1,1,1,1,1,–1,–1,–1,–1]
31	15	**M**	[0,1,–1,–1,–1,–1,1,1,–1,1,–1,1,1,1,1,1,–1]	[1,–1,1,1,1,–1,–1,–1,1,1,–1,1,1,–1,–1]
33	16	**S**	Нет	Нет
35	17	**M**	$\mathbf{Q}_{35} = \mathrm{core}(\mathbf{H}_{36})$	
37	18	**S**	[0,–1,1,–1,–1,1,–1,1,1,1,1,1,1,–1,1,–1,–1,1,–1]	[1,1,–1,1,1,1,–1,–1,–1,1,1,1,–1,–1,–1,1,–1,–1]
39	19	**M**	[0,1,–1,–1,1,1,1,1,1,–1,1,–1,1,–1,–1,–1,–1,1,1,1,–1]	[1,1,–1,–1,1,1,1,1,1,–1,1,–1,1,–1,–1,–1,–1,1,1,1,–1]
41	20	**S**	[0,1,1,1,–1,–1,1,–1,1,1,–1,–1,–1,1,1,–1,1,1,–1,–1,1,1,1,1]	[1,1,1,1,–1,1,1,–1,–1,1,1,1,–1,1,1,1,–1,1,1,–1,–1,–1,–1,–1]
43	21	**M**	[0,1,1,1,1,1,1,–1,–1,1,1,–1,1,1,–1,–1,1,1,1,–1,–1,–1,–1,–1]	[–1,1,1,1,1,–1,1,1,–1,1,1,–1,1,1,–1,1,1,–1,1,1,1,1,1,–1]
45	22	**S**	$\mathbf{Q}_{45}$ имеет структуру Матона [9]	
47	23	**M**	[0,1,1,1,1,–1,1,–1,1,1,1,–1,–1,1,1,1,–1,–1,1,1,–1,1,1,–1,–1, –1,–1]	[1,1,1,1,1,–1,1,1,–1,1,1,1,–1,–1,1,1,1,–1,–1,1,1,–1,1,1,–1,–1, –1,–1]

■ *Окончание табл. 3*

n	q	Тип	Первая строка **a** блока **A**	Первая строка **b** блока **B**
49	24	**S**	[0,1,1,1,–1,–1,–1,1,–1,1,1,–1,–1,–1,1,1,–1,1,–1,–1, –1,1,1,1]	[1,–1,–1,1,1,–1,1,1,1,1,–1,1,–1,1,–1,–1,–1,–1,1,–1, –1,1,1,–1]
51	25	**M**	$\mathbf{Q}_{25} = \mathbf{Q}_5 \otimes \mathbf{Q}_5 + \mathbf{I} \otimes \mathbf{J} - \mathbf{J} \otimes \mathbf{I}$	
53	26	**S**	[–1,1,–1,–1,1,–1,–1,1,1,1,1,–1,–1,1,1,–1,–1,–1,–1, 1,1,–1,1,1,–1,1]	[0,1,–1,–1,–1,–1,1,–1,1,1,1,–1,1,1,1,–1,1,1,1,–1,1,1,–1, –1,–1,–1,1]
55	27	**M**	$\mathbf{Q}_{27} = \mathbf{Q}_3 \otimes \mathbf{Q}_3 \otimes \mathbf{Q}_3 + \mathbf{Q}_3 \otimes \mathbf{I} \otimes \mathbf{J} + \mathbf{I} \otimes \mathbf{J} \otimes \mathbf{Q}_3 + + \mathbf{J} \otimes \mathbf{Q}_3 \otimes \mathbf{I}$	
57	28	**S**	Нет	Нет
59	29	**M**	[0,1,–1,–1,–1,–1,–1,1,1,–1,1,–1,1,–1,–1,1,1,–1,1,–1, 1,–1,–1,1,1,1,1,1,–1]	[1,1,–1,–1,1,1,1,1,–1,1,–1,–1,–1,1,–1,–1,1,–1,–1,–1, 1,–1,1,1,1,1,–1,–1,1]
61	30	**S**	[0,1,–1,–1,1,1,–1,–1,1,–1,1,1,1,–1,–1,–1,–1,–1,1,1,1, –1,1,–1,–1,1,1,–1,–1,1]	[1,–1,1,1,–1,1,–1,–1,–1,–1,–1,1,–1,–1,–1,1,1,1,–1,1, 1,1,1,1,–1,1,–1,–1,1,–1]
63	31	**M**	[0,1,1,–1,1,1,–1,1,1,1,1,1,–1,–1,–1,1,1,–1,1,–1,1,1,1,–1, –1,–1,–1,1,–1,–1,1,–1,–1]	[1,1,1,–1,1,1,–1,1,1,1,1,1,–1,–1,–1,1,1,–1,1,–1,–1,1,1,1,–1, –1,–1,–1,1,–1,–1,1,–1,–1]

Из гипотезы о кососимметрии следует, что трудности в поиске сомножителей корректируемого кронекерова произведения есть, но они преодолимы. Для матрицы $\mathbf{S}_{17}$ нет комплементарной кососимметрической матрицы, в этом случае матрица $\mathbf{M}_{35}$ строится, например, широко используемым усечением кососимметричного массива Вильямсона — Себерри [12], состоящего из четырех циклических блоков. Цепочки критских матриц интересны тем, что дают заметно более простые формы.

Произведение Скарпи

Около ста лет назад итальянский математик Умберто Скарпи вставил матрицу Адамара порядка $4t$ в ее собственный блок без каймы порядка $4t - 1$. В нашей классификации — в матрицу Мерсенна. Оказалось, что ортогонализация столбцов (и строк) такого вложения возможна при циклическом смещении блока матрицы Адамара пропорционально мере расстояния (в виде произведения индексов) замещаемого элемента от левого верхнего угла матрицы.

Опишем этот метод в нашей редакции заметно короче, чем в оригинале [5], — одной формулой кронекерова произведения с коррекцией (произведение Скарпи $\times$) в виде описанного Скарпи смещения, используя понятие нормальной формы матрицы Адамара и ее основы (core).

$$\mathbf{M} \times \mathbf{H} = \begin{pmatrix} \begin{pmatrix} -1 & m_{11}\mathbf{e}^{\mathrm{T}} \\ m_{11}\mathbf{e} & \mathbf{M} \end{pmatrix} & \begin{pmatrix} -1 & m_{12}\mathbf{e}^{\mathrm{T}} \\ m_{12}\mathbf{e} & \mathbf{M} \end{pmatrix} & \cdots & \begin{pmatrix} -1 & m_{1(n-1)}\mathbf{e}^{\mathrm{T}} \\ m_{1(n-1)}\mathbf{e} & \mathbf{M} \end{pmatrix} \\ \begin{pmatrix} -1 & m_{21}\mathbf{e}^{\mathrm{T}} \\ m_{21}\mathbf{e} & \mathbf{M} \end{pmatrix} & \begin{pmatrix} -1 & m_{22}\mathbf{e}^{\mathrm{T}} \\ m_{22}\mathbf{e} & \mathbf{TM} \end{pmatrix} & \cdots & \begin{pmatrix} -1 & m_{2(n-1)}\mathbf{e}^{\mathrm{T}} \\ m_{2(n-1)}\mathbf{e} & \mathbf{T}^{n-2}\mathbf{M} \end{pmatrix} \\ \cdots & \cdots & \ddots & \cdots \\ \begin{pmatrix} -1 & m_{(n-1)1}\mathbf{e}^{\mathrm{T}} \\ m_{(n-1)1}\mathbf{e} & \mathbf{M} \end{pmatrix} & \begin{pmatrix} -1 & m_{(n-1)2}\mathbf{e}^{\mathrm{T}} \\ m_{(n-1)2}\mathbf{e} & \mathbf{T}^{n-2}\mathbf{M} \end{pmatrix} & \cdots & \begin{pmatrix} -1 & m_{(n-1)(n-1)}\mathbf{e}^{\mathrm{T}} \\ m_{(n-1)(n-1)}\mathbf{e} & \mathbf{T}^{(n-2)(n-2)}\mathbf{M} \end{pmatrix} \end{pmatrix},$$

где $\mathbf{H} = \begin{pmatrix} -1 & \mathbf{e}^{\mathrm{T}} \\ \mathbf{e} & \mathbf{M} \end{pmatrix}$ — матрица Адамара; $\mathbf{M} = -\mathrm{core}(\mathbf{H})$ — округленная до целых значений элементов матрица Мерсенна; $\mathbf{e}$ — вектор единичных элементов каймы; $\mathbf{T}$ — матрица циклического смещения. Каждый блок смещается на величину произведения $(i - 1)(j - 1)$, при этом смещать можно как строки, так и столбцы — процедура симметрична. Знак замещаемого элемента переносится только на элементы каймы.

С помощью алгоритма Скарпи нашел новую матрицу Адамара высокого составного порядка $7 \cdot 8 = 56$ [5]. Метод не зависит от вида матрицы Мерсенна (она может быть любой, не кососимметрической), но подходит только для простых порядков $4t - 1$. В общем случае метод дает ошибку — требует более громоздкой коррекции.

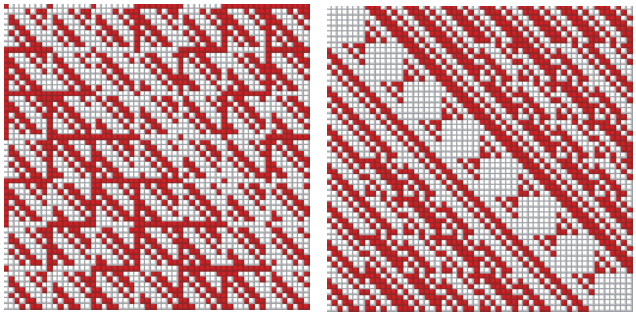
Однако нами замечено, что произведение Кронекера с коррекцией можно использовать для любых порядков, а не только простых. Это не отмечалось ранее, поскольку такими произведениями мало кто занимался. Так как оригинальный алгоритм работал только для простых порядков, естественны попытки обобщить такой алгоритм на степени простого числа, но более серьезное обобщение исключает требование простоты как несущественный фактор.

Решение проблемы состоит в том, что при обратном следовании асимметричных сомножителей смещения не нужны: в таком случае коррекция сводится к смене знака отрицательных элементов диагональных матриц **M**. Таким образом, при округлении до целых на диагонали возникает **J** — матрица из единичных элементов порядка матрицы **M**. Как и в разобранном Пэли умножении матриц Белевича, простота коррекции зависит в первую очередь от типа симметрии сомножителей.

Обобщенное произведение Скарпи (generalized Scarpis method) имеет вид $[\mathbf{H} \otimes \mathbf{M}] = \mathbf{I} \otimes \mathbf{J} + (\mathbf{H} - \mathbf{I}) \otimes \mathbf{M}$, $\mathbf{M} = -\mathrm{core}(\mathbf{H})$, где **I** — единичная матрица, аннулирующая диагональные элементы асимметричной матрицы Адамара $\mathbf{H} = \begin{pmatrix} 1 & -\mathbf{e}^{\mathrm{T}} \\ \mathbf{e} & -\mathbf{M} \end{pmatrix}$.

Матрицы Адамара, полученные методом Скарпи для двух описанных выше реализаций, представлены на рис. 3.

Вторая более общая формула произведения Скарпи справедлива для порядков матриц Мерсенна в виде простых чисел 3, 7, 11, произведений близких целых $3 \cdot 5 = 15$ и $7 \cdot 5 = 35$, степени простого числа $3^3 = 3 \cdot 3 \cdot 3 = 27$ и прочих составных порядков. Из матрицы Мерсенна порядка 27 получим матрицу Адамара порядка 756 (оригинальным методом это сделать невозможно). После публикации работы Пэли [6] метод Скарпи со смещениями был почти забыт, комментарии к нему редки. Его обобщение, не зависящее от блочного вида асимметричной матрицы **M**, мы привели впервые в работе [1].



■ ***Рис. 3.*** Матрицы Адамара порядка 56, полученные двумя методами Скарпи

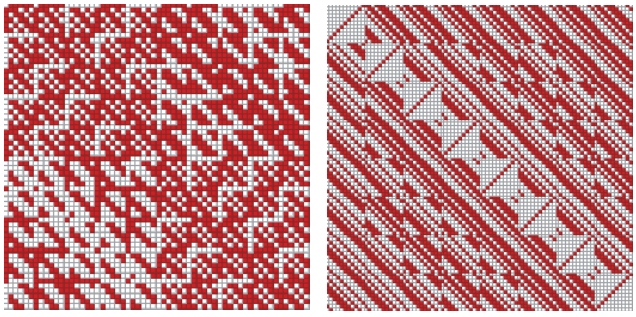
Обратный метод Скарпи

В прямом методе Скарпи к матрице **M** добавляется кайма. С ее помощью строится матрица Адамара, вставляемая в матрицу Мерсенна с циклическим смещением внутреннего блока. Кайма, являясь компенсатором, может как добавляться, так и удаляться. Произведем удаление каймы, назвав новый метод *обратным* методом Скарпи. Он является таким же общим, как и прямой метод Скарпи, но позволяет вычислять матрицы Адамара иных порядков.

Возьмем матрицу **M** в форме бицикла с каймой $\mathbf{M} = \begin{pmatrix} 1 & \mathbf{e}^{\mathrm{T}} & -\mathbf{e}^{\mathrm{T}} \\ -\mathbf{e} & \mathbf{A} & \mathbf{B} \\ \mathbf{e} & -\mathbf{B}^{\mathrm{T}} & \mathbf{A}^{\mathrm{T}} \end{pmatrix}$ порядка $2q + 1$, удалим кайму как компенсатор, ставший ненужным. Бициклическая основа матрицы **M** имеет четный порядок $2q$. Разделим ее по строкам и столбцам, выделив два блока нечетного порядка **A** и **B**, и построим их формальные расширения $[\mathbf{A}] = \begin{pmatrix} -1 & \mathbf{e}^{\mathrm{T}} \\ \mathbf{e} & \mathbf{A} \end{pmatrix}$, $[\mathbf{B}] = \begin{pmatrix} -1 & \mathbf{e}^{\mathrm{T}} \\ \mathbf{e} & \mathbf{B} \end{pmatrix}$. Блоки квадрируем × по Скарпи (применяем описанный выше одной формулой алгоритм к блокам **A** и **B**), получаем расширенную матрицу Адамара $\mathbf{H} = \begin{pmatrix} \mathbf{A} \times [\mathbf{A}] & \mathbf{B} \times [\mathbf{B}] \\ -(\mathbf{B} \times [\mathbf{B}])^{\mathrm{T}} & (\mathbf{A} \times [\mathbf{A}])^{\mathrm{T}} \end{pmatrix}$ порядка $2q(q + 1)$.

Прямой метод Скарпи применим только к матрицам Мерсенна и исключает матрицы Зейделя, поскольку последние (как и матрица Белевича), будучи началом самостоятельной цепочки матриц, не выражаются через матрицы более низких порядков. В обратном методе, напротив, симметричный блок **B** кососимметричной матрицы Мерсенна **M** порядка 11 может быть матрицей Зейделя порядка $q = 5$, например. Получаемая из таких блоков матрица **H** порядка $2q(q + 1) = 60$ приведена на рис. 4.

Такие продолжения не единственны. Во втором нашем независимом продолжении прямого метода Скарпи матрица Адамара умножается



■ ***Рис. 4.*** Матрицы Адамара порядков 60 и 88

на матрицу Мерсенна $[\mathbf{H} \otimes \mathbf{M}]$ не ниже, а выше нее по порядку. Чтобы при разнице 3 между порядками сомножителей не усложнять блоки на диагонали, для вставки следует выбирать циклическую матрицу Мерсенна — компенсатором служит матрица с –1 на антидиагонали. Для матриц $\mathbf{H}$ порядка $11 - 3 = 8$ и $\mathbf{M}$ порядка 11 кронекеровым умножением получим матрицу Адамара порядка 88 (см. рис. 4).

Произведение матриц Мерсенна и Зейделя

Перемножение парных матриц Мерсенна и Зейделя с коррекцией дистанции 2 между их порядками (рис. 5) — обобщение произведения пар близких целых чисел на произведение матриц.

Основу нового метода составляет тот факт, что формула Белевича квадрирования порядка матрицы Якобсталя $\mathbf{Q} \otimes \mathbf{Q} + \mathbf{I} \otimes \mathbf{J} - \mathbf{J} \otimes \mathbf{I}$ может быть обобщена двумя возможными способами.

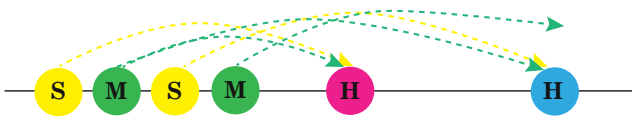
Формула $\mathbf{Q} = \mathbf{Q}_S \otimes \mathbf{Q}_M + \mathbf{I} \otimes \mathbf{J} - \mathbf{J} \otimes \mathbf{I}$ описывает вставку кососимметричной матрицы Якобсталя $\mathbf{Q}_M = \mathbf{M} - \mathbf{I}$ в симметричную матрицу Якобсталя $\mathbf{Q}_S = \mathbf{S} - \mathbf{I}$.

Обратная вставка $\mathbf{Q} = \mathbf{Q}_M \otimes \mathbf{Q}_S + \mathbf{I} \otimes \mathbf{J} - \mathbf{J} \otimes \mathbf{I}$ также возможна. Размеры единичной $\mathbf{I}$ и $\mathbf{J}$ согласованы с порядками сомножителей.

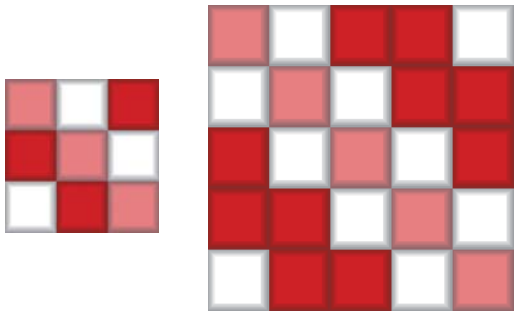
Для получения матрицы Адамара необходима еще кайма, коррекцию произведения Кронекера обозначим квадратными скобками. При вычислении $\mathbf{H} = [\mathbf{S} \otimes \mathbf{M}]$ парные матрицы $\mathbf{A} = \mathbf{Q}_M - \mathbf{I}$ и $\mathbf{B} = -(\mathbf{Q}_M + \mathbf{I})$ замещают положительный и отрицательный элементы первого сомножителя, осевые блоки состоят из $\mathbf{J}$, построение завершается каймой из 1.

При вычислении $\mathbf{H} = [\mathbf{M} \otimes \mathbf{S}]$ парные матрицы $\mathbf{A} = \mathbf{Q}_S - \mathbf{I}$ и $\mathbf{B} = -(\mathbf{Q}_S + \mathbf{I})$ замещают положительный и отрицательный элементы первого сомножителя, осевые блоки состоят из $\mathbf{J} - 2\mathbf{I}$, построение завершается каймой из 1, исключая начальный элемент –1.

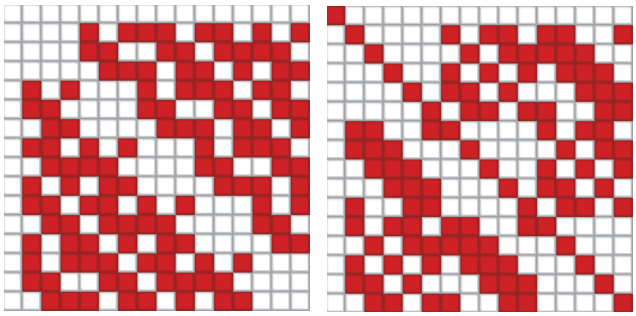
В примерах взаимных произведений возьмем матрицы Якобсталя $\mathbf{Q}_M$ порядка 3 и $\mathbf{Q}_S$ порядка 5 (рис. 6). Кососимметричная матрица дает матрицу $\mathbf{M}$, симметричная матрица дает матрицу $\mathbf{S}$. Брать их можно как в циклической, так и бициклической форме, поскольку бициклическая имеет ту же ось симметрии.



■ *Рис. 5.* Расчет матриц Адамара парными матрицами



■ *Рис. 6.* Циклические матрицы Якобсталя порядков 3 и 5



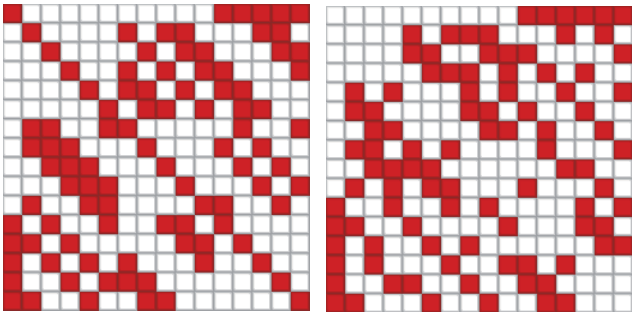
■ *Рис. 7.* Прямая и обратная матрицы-витражи порядка 16

Вставку будем называть *матрицей-витражом*. Пусть $n = 3 \cdot 5 + 1 = 16$. Матрица $\mathbf{M}_3$ образует витраж $\mathbf{H}_{16} = [\mathbf{S}_5 \otimes \mathbf{M}_3]$ с матрицей $\mathbf{S}_5$. Матрица $\mathbf{S}_5$ образует витраж $\mathbf{H}_{16} = [\mathbf{M}_3 \otimes \mathbf{S}_5]$ с матрицей $\mathbf{M}_3$. Матрицы-витражи, отличающиеся диагональными блоками и начальным элементом каймы, приведены на рис. 7.

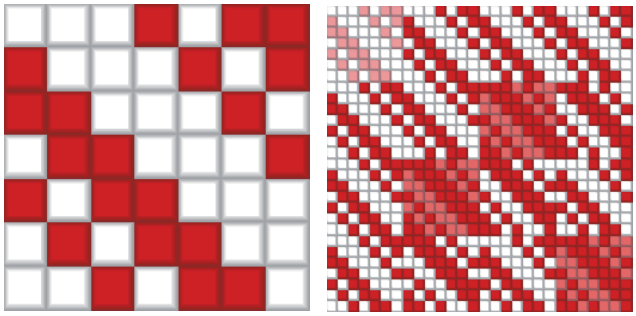
Вычисление регулярных матриц Адамара

Теперь мы подошли к задаче вычисления матриц с равными суммами строк и столбцов (регулярных матриц), поставленной во введении. Для выравнивания сумм строк и столбцов прямую и обратную матрицы-витражи нужно *нормализовать* инверсией знаков строк и столбцов, захватывая неуравновешенную вторую половину блоков. Без учета первого блока количество блоков является нечетным числом. В примере выше это дает регулярные матрицы Адамара порядка 16 (рис. 8).

Инверсия строк и столбцов — операция легко выполнимая, поэтому переход к регулярным матрицам оказывается простым и не требует сколь-нибудь подробных комментариев. Матрицы Мерсенна и Зейделя пар близких порядков находятся на расстоянии 2. Оно привлекательно тем, что их произведение с каймой дает порядки $4u^2 = n(n + 2) + 1$ вида 4, 16, 36, 100, 144, 196, 256, 324 и т. п., не найденная в форме Буша матрица



■ ***Рис. 8.*** Регулярные матрицы Адамара порядка 16



■ ***Рис. 9.*** Матрица Мерсенна и Пропус $\mathbf{H}_{28}$

196-го порядка приведена нами в работе [10]. Для простых порядков имеем: $1 \cdot 3 + 1 = 4, 3 \cdot 5 + 1 = 16$, $5 \cdot 7 + 1 = 36$, $11 \cdot 13 + 1 = 144$, $17 \cdot 19 + 1 = 324$, $29 \cdot 31 + 1 = 900, 41 \cdot 43 + 1 = 1764$. Добавим к ним матрицы, находимые с помощью бициклов с каймой: $13 \cdot 15 + 1 = 196$, $37 \cdot 39 + 1 = 1444$. Матрицы Якобсталя степеней простых порядков могут быть найдены при помощи формул Белевича, они дают порядки $7 \cdot 9 + 1 = 64$, $9 \cdot 11 + 1 = 100$, $25 \cdot 27 + 1 = 676$, $49 \cdot 51 + 1 = 2500$, $53 \cdot 55 + 1 = 2916$. Матрица Якобсталя порядка 45 конструкции Матона [9] дает порядок $45 \cdot 47 + 1 = 2116$. Для вычисления матриц порядков $\mathbf{21} \cdot 23 + 1 = 484$, $\mathbf{33} \cdot 35 + 1 = 1156$ и т. п. нет соответствующих им матриц Зейделя, — пробел, связанный с принципиальными особенностями числовой системы.

Вычисление матриц Ферма

Матрицы Ферма — производные от регулярных матриц Адамара критские матрицы нечетных порядков $n = 4t + 1$, отличающиеся от них уровнем отрицательного элемента и каймой со значениями s. Матрицы Ферма рассмотрены нами в работе [11]. Показанная ниже структура охватывает все перечисленные в табл. 1 критские матрицы, исключая лишь взвешенные:

$$\begin{array}{ccccccccc} \mathbf{(S)} & - & \mathbf{E} & - & \mathbf{M} & - & \mathbf{E} & - & \mathbf{M} & -\ldots \\ | & & & & | & & & & | & \\ \mathbf{(C)} & & & & \mathbf{H} & & & & \mathbf{H} & \\ & & & & | & & & & & \\ & & & & \mathbf{F} & & & & & \end{array}$$

Возможность существования матриц Ферма обусловлена регулярностью матриц Адамара порядков, равных произведениям пар целых чисел. Порядок, на котором заканчивается ответвление одной цепочки, служит началом другой.

Блочные критские матрицы (Проклы и Пропусы)

При разнесении порядков сомножителей (матриц Зейделя или Мерсенна) описанная выше структура витража не меняется. Более того, внедиагональные блоки по-прежнему можно считать блоками с элементами, равными 1 и –1. В данном случае отсутствует компенсатор, тем самым витраж является примером составной критской матрицы с настраиваемыми элементами диагональных блоков.

Свобода выбора структуры диагональных клеток велика.

На диагонали может стоять клетка Зейделя или Мерсенна, назовем такую структуру *гофр*, одиночная *складка* типа матрицы $\mathbf{J} - 2\mathbf{I}$ и, наконец, блок вида $\mathbf{J}$, но не с единичными элементами (масштабируемый монотонный блок). Так как количество диагональных блоков невелико, оно равно порядку сомножителя (а не порядку всей матрицы), такие произведения аппроксимируют матрицы Адамара с малой погрешностью.

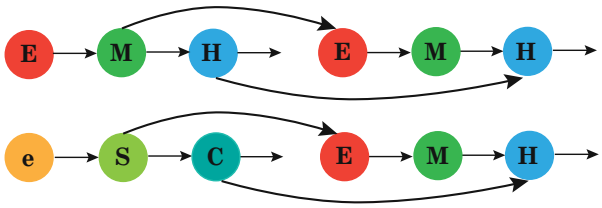
Например, каждая вторая матрица Эйлера порядков $n = 4t - 2$, построенная на паре матриц Мерсенна в виде $\underline{\mathbf{E}} = \begin{pmatrix} \underline{\mathbf{M}} & \underline{\mathbf{M}} \\ \underline{\mathbf{M}}^{\mathrm{T}} & -\underline{\mathbf{M}}^{\mathrm{T}} \end{pmatrix}$, может быть упрощена приравниванием элементов внедиагональных блоков 1 и –1. Эта параметрическая разновидность названа матрицами Прокла ввиду выраженного диагональю стремления к некоторой золотой середине.

Рекурсия с матрицей Прокла дает, в свою очередь, Пропусы [2] — четырехблочные массивы с попарно совпадающими блоками. К сходному (после перестановки центральных блоков) результату приводит вставка матрицы Мерсенна в симметричный массив Вильямсона (рис. 9).

При таком осреднении количество элементов, отличных от 1 и –1, убывает, при этом элементы диагональных блоков равны 1 и $-b$ при $-b$, стремящемся к –1.

Связь критских матриц

Связь критских матриц между собой отражает структурная формула, *меандр* (рис. 10), обладающий, как и таблица Менделеева (таблица химических элементов кратна 4), предсказывающей силой.



■ ***Рис. 10***. Меандр критских матриц

В самом деле, меандр подводит к выводу, например, о том, что матрицы Зейделя, как и матрицы Мерсенна, разлагаются на квазиортогональные матрицы, предикторы **e**, сходные с матрицами Эйлера **E**. Предсказанные матрицы, обозначенные малым символом **e**, действительно обнаружены и названы *теневыми*: необычность предикторов матриц Зейделя **S** состоит в том, что они существуют на порядках матриц Адамара, но связаны, опосредованно, с симметричными матрицами Белевича **C** (тени матриц Белевича). Это форма существования симметричных бициклов порядков $4t$, тогда как матрицы Адамара конструкции Пэли асимметричны.

Тема симметрии давно привлекает к себе внимание многих ученых. Компьютерное исследование матриц Адамара начинается в 1962 году находкой матрицы порядка 92, недостижимой методами Скарпи и Пэли. Кососимметричная матрица Адамара того же размера — рекорд 1971 года [13]. Кососимметричные (с точностью до элементов диагонали) матрицы Адамара конструкции Вильямсона — Себерри рассматриваются в диссертации профессора Дж. Себерри [12]. В 1992 г. компьютерные методы вставки (plug into) матриц друг в друга систематизируются в обзоре Дж. Себерри и Миеко Ямады [14], это одна из самых широко цитируемых работ этих авторов.

Многие асимметричные матрицы Адамара (skew-type) составных порядков найдены компьютерным поиском профессором Др. Джоковичем [16, 17]. Индексы симметрии и кососимметрии матриц Адамара исследованы в работе [18]; первый порядок-исключение 35 симметричной матрицы Вильямсона обсуждается в работах [19, 20]. Благодаря симметрии массива Балонина — Себерри [21] (особенности Пропус-конструкции [2, 22] критских матриц см. на рис. 8) удалось доказать существование симметричных матриц Адамара порядков 116 и 172 [23].

Меандры (специфические формулы связей критских матриц) обеспечивают целостное восприятие такого обширного материала, как ортогональные базисы четных и нечетных порядков. На каждом порядке сосуществуют как простые, так и сложные матрицы, порождения идущих снизу цепочек. Этим обстоятельством можно пользоваться для кодирования, поскольку глубина вложения цепочки (порядковый номер матрицы в цепочке) — скрываемый перестановками строк и столбцов код.

Теория критских матриц иллюстрирует основные теоремы и факты теории чисел [1], заостряет внимание на сопоставлении четным и нечетным числам матричных портретов малоуровневых экстремальных (локально оптимальных по детерминанту) матриц [2]. На критских матрицах базируются ныне фильтры Мерсенна и Ферма [24], применяемые в процедурах помехозащитного кодирования и сжатия видеоизображений. Квазиортогональные матрицы с иррациональными элементами, связанные с золотым сечением, дают матричные модели квазикристаллов [25, 26].

Заключение

Работа Пэли завершила начатое Адамаром построение теории квазиортогональных матриц с элементами 1 и –1 предложением методов генерации матриц (алгоритмами, работающими в арифметике конечных полей) и поправок кронекерова произведения для расширения полученных алгоритмами результатов.

Настоящая статья дополняет наш обзор критских матриц с базовыми элементами 1 и $-b$, $b \le 1$ порядков, определенных на всей числовой оси, рассмотрением наших поправок к произведению Кронекера, позволяющих вычислить как матрицы Адамара, так и связанные с ними критские матрицы Мерсенна, Ферма, Эйлера и прочие.

Блочные критские матрицы четных порядков обобщают матрицы Белевича в том, что отличные от 1 и –1 элементы расположены только на (блочной) диагонали. Мы отмечаем их постольку, поскольку Пропусы существуют на четных порядках 668, 716, 892, на которых матрицы Адамара пока не найдены.

Например, Пропус 668 строится на основе матрицы $\mathbf{M}_{167}$. Число 167 — простое, циклическая матрица имеет конструкцию, как и матрица $\mathbf{M}_{28}$.

Литература

1. **Балонин Н. А., Сергеев М. Б.** Матрицы Мерсенна и Адамара // Информационно-управляющие системы. 2016. № 1(80). С. 2–15. doi:10.15217/issn1684-8853.2016.1.2
2. **Балонин Н. А., Сергеев М. Б.** Матрицы локального максимума детерминанта // Информационно-управляющие системы. 2014. № 1(68). С. 2–15.
3. **Balonin N. A., Seberry Jennifer.** Remarks on Extremal and Maximum Determinant Matrices with Real

Entries ≤ 1 // Информационно-управляющие системы. 2014. № 5(71). С. 2–4.
4. **Hadamard J.** Résolution d'une Question Relative aux Déterminants// Bulletin des Sciences Mathématiques. 1893. Vol. 17. P. 240–246.
5. **Scarpis U.** Sui Determinanti di Valore Massimo // Rendiconti Della R. Istituto Lombardo di Scienze e Lettere. 1898. Vol. 31. P. 1441–1446.
6. **Paley R. E. A. C.** On Orthogonal Matrices // Journal of Mathematics and Physics. 1933. Vol. 12. P. 311–320.
7. **Belevitch V.** Theorem of 2n-terminal Networks with Application to Conference Telephony // Electr. Commun. 1950. Vol. 26. P. 231–244.
8. **Балонин Н. А., Сергеев М. Б., Востриков А. А.** О двух предикторах вычисляемых цепочек квазиортогональных матриц // Автоматика и вычислительная техника. 2015. № 3. С. 42–48. doi:10.3103/S0146411615030025
9. **Balonin N. A., Seberry Jennifer.** A Review and New Symmetric Conference Matrices // Информационно-управляющие системы. 2014. № 4(71). P. 2–7.
10. **Balonin N. A., Sergeev M. B.** Regular Hadamard Matrix of Order 196 and Similar Matrices // Информационно-управляющие системы. 2015. № 1(73). P. 2–3. doi:10.15217/issn1684-8853.2015.1.2
11. **Balonin N. A., Seberry Jennifer, Sergeev M. B.** Three Level Cretan Matrices of Order 37//Информационно-управляющие системы. 2015. № 2(74). P. 2–3. doi:10.15217/issn1684-8853.2015.2.2
12. **Awyzio Gene and Seberry Jennifer.** On Good Matrices and Skew Hadamard Matrices. http://www.uow.edu.au/~jennie/WEB/WEB15/2015_11_Good_matrices.pdf (дата обращения: 15 ноября 2014).
13. **Baumert Leonard, Golomb S. W. and Hall Marshall.** Discovery of an Hadamard Matrix of Order 92 // Bull. Amer. Math. Soc. California Institute of Technology. 1962. Vol. 68. P. 237–238.
14. **Seberry Wallis Jennifer.** A skew-Hadamard Matrix of Order 92 // Bulletin of the Australian Mathematical Society. 1971. Vol. 5. P. 203–204.
15. **Seberry Jennifer and Yamada Mieko.** Hadamard Matrices, Sequences, and Block Designs // Contemporary Design Theory. A Collection of Surveys. J. H. Dinitz and D. R. Stinson eds. — John Wiley and Sons, 1992. P. 431–560.
16. **Djokovic D. Z.** Ten New Orders for Hadamard Matrices of Skew Type // Univ. Beograd Pull. Electrotehn. Fak. Ser. Math. 1992. N 3. P. 47–59.
17. **Balonin N. A., Djokovic D. Z.** Negaperiodic Golay Pairs and Hadamard Matrices // Информационно-управляющие системы. 2015. № 5(78). С. 2–17. doi:10.15217/issn1684-8853.2015.5.2
18. **Balonin N. A., Djokovic D. Z.** Symmetry of Two Circulant Hadamard Matrices and Periodic Golay Pairs // Информационно-управляющие системы. 2015. №3(76). С. 2–16. doi:10.15217/issn1684-8853.2015.3.16
19. **Djokovic D. Z.** Williamson Matrices of Order 4*n* for *n* = 33;35;39 // Discrete Math. 1993. Vol. 115. P. 267–271.
20. **Holzmann W. H., Kharaghani H., Tayfeh-Rezaie B.** Williamson Matrices up to Order 59 // Designs, Codes and Cryptography. 2008. Vol. 46. Iss. 3. P. 343–352.
21. **Balonin N. A., Seberry Jennifer.** The Propus Construction for Symmetric Hadamard Matrices. 2015. http://arxiv.org/abs/1512.01732 (дата обращения: 5 сентября 2015).
22. **Balonin N. A., Seberry Jennifer.** Two-level Cretan Matrices Constructed Using SBIBD // Special Matrices. 2015. Vol. 3.1. P. 186–192.
23. **Di Matteo O., Djokovic D. Z., Kotsireas I. S.** Symmetric Hadamard Matrices of Order 116 and 172 Exist // Special Matrices. 2015. Vol. 3.1. P. 227–234.
24. **Балонин Н. А., Сергеев М. Б.** О расширении ортогонального базиса в задачах сжатия видеоизображений // Вестник компьютерных и информационных технологий (ВКИТ). 2014. № 2. С. 11–15. doi: 10.14489/vkit.2014.02.pp.011-015
25. **Балонин Н. А., Сергеев М. Б.** М-матрицы и кристаллические структуры // Вестник Магнитогорского государственного технического университета им. Г. И. Носова. 2013. № 3. С. 58–62.
26. **Балонин Н. А., Сергеев М. Б.** Матрица золотого сечения G10 // Информационно-управляющие системы. 2013. № 6. С. 2–5.

UDC 519.614
doi:10.15217/issn1684-8853.2016.5.2

Mersenne and Hadamard Matrices, Products

Balonin N. A.[a], Dr. Sc., Tech., Professor, korbendfs@mail.ru
Sergeev M. B.[a], Dr. Sc., Tech., Professor, mbse@mail.ru
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Purpose: The goal is to demonstrate that a Kronecker product with subsequent correction of its elements can be generalized for quasiorthogonal local maximum determinant matrices with a low number of levels in order to obtain high-dimension matrices of the same quality (with a low number of levels), in particular, Hadamard and Mersenne matrices. **Results:** It has been shown that the complexity of the correction formulas for the Kronecker product of quasiorthogonal matrices with a low number of levels (Cretan matrices) depends on the type of symmetry of the factor matrices, their order in the product, and distance between the sizes of the matrix factors.

We have described the types of possible matrix factors by the types of their symmetry, dependence of the symmetry on the matrix size and the position of a matrix in the chain of Cretan matrices with increasing orders. Tables of symmetrized matrices are provided. We have generalized Scarpis product for Hadamard matrix by its core or a rounded Mersenne matrix, and demonstrated that the permutation of symmetrized factors allows you to multiply Hadamard matrix of both prime and composite orders. The Kronecker product technique is expanded into matrix factors whose sizes have a difference (distance) not exceeding 4. The product of Mersenne matrices of order 4t+1 and Seidel matrices of order 4t−1 generates regular Hadamard matrices with sums of columns equal to each other. The diversity of sizes of the matrix factors leads to block structures in which elements different from 1 or −1 are placed only inside the diagonal blocks. **Practical relevance:** Algorithms of calculating Cretan matrices were used in the construction of research software. Matrices which are suboptimal by determinant are the basis of Mersenne and Fermat filters used in image compression and masking.

Keywords — Kronecker Product, Orthogonal Matrix, Cretan Matrix, Hadamard Matrix, Conference Matrix, Mersenne Matrix, Fermat Matrix, Generalized Scarpis Method, Circulant Matrix.

References

1. Balonin N. A., Sergeev M. B. Mersenne and Hadamard Matrices. *Informatsionno-upravliaiushchie systemy* [Information and Control Systems], 2016, no. 1(80), pp. 2–15 (In Russian). doi:10.15217/issn1684-8853.2016.1.2
2. Balonin N. A., Sergeev M. B. Local Maximum Determinant Matrices. *Informatsionno-upravliaiushchie systemy* [Information and Control Systems], 2014, no. 1(68), pp. 2–15 (In Russian).
3. Balonin N. A., Seberry Jennifer. Remarks on Extremal and Maximum Determinant Matrices with Real Entries ≤ 1. *Informatsionno-upravliaiushchie systemy* [Information and Control Systems], 2014, no. 5(71), pp. 2–4.
4. Hadamard J. Resolution D'une Question Relative aux Determinants. *Bulletin des Sciences Mathematiques*, 1893, vol. 17, pp. 240–246 (In French).
5. Scarpis U. Sui Determinanti di Valore Massimo. *Rendiconti della R. Istituto Lombardo di Scienze e Lettere*, 1898, vol. 31, pp. 1441–1446 (In Italian).
6. Paley R. E. A. C. On Orthogonal Matrices. *Journal of Mathematics and Physics*, 1933, vol. 12, pp. 311–320.
7. Belevitch V. Theorem of 2n-terminal Networks with Application to Conference Telephony. *Electr. Commun.*, 1950, vol. 26, pp. 231–244.
8. Balonin N. A., Sergeev M. B., Vostrikov A. A. On Two Predictors of Calculable Chains of Quasi-Orthogonal Matrices. *Avtomatika i vychislitel'naia tekhnika*, 2015, vol. 49, no. 3, pp. 153–158 (In Russian). doi:10.3103/S0146411615030025
9. Balonin N. A., Seberry Jennifer. A Review and New Symmetric Conference Matrices. *Informatsionno-upravliaiushchie systemy* [Information and Control Systems], 2014, no. 4(71), pp. 2–7.
10. Balonin N. A., Sergeev M. B. Regular Hadamard Matrix of Order 196 and Similar Matrices. *Informatsionno-upravliaiushchie systemy* [Information and Control Systems], 2015, no. 1(73), pp. 2–3. doi:10.15217/issn1684-8853.2015.1.2
11. Balonin N. A., Seberry Jennifer, Sergeev M. B. Three Level Cretan Matrices of Order 37. *Informatsionno-upravliaiushchie systemy* [Information and Control Systems], 2015, no. 2(74), pp. 2–3. doi:10.15217/issn1684-8853.2015.2.2
12. Awyzio Gene and Seberry Jennifer. On Good Matrices and Skew Hadamard Matrices. Available at: http://www.uow.edu.au/~jennie/WEB/WEB15/2015_11_Good_matrices.pdf (accessed 5 November 2014).
13. Baumert Leonard, Golomb S. W. and Hall Marshall. Discovery of an Hadamard Matrix of Order 92. *Bull. Amer. Math. Soc.*, California Institute of Technology, 1962, no. 68, pp. 237–238.
14. Seberry Wallis Jennifer. A Skew-Hadamard Matrix of Order 92. *Bulletin of the Australian Mathematical Society*, 1971, no. 5, pp. 203–204.
15. Seberry Jennifer and Yamada Mieko. Hadamard Matrices, Sequences, and Block Designs. In: *Contemporary Design Theory*: A *Collection of Surveys*. J. H. Dinitz and D. R. Stinson eds., John Wiley and Sons, 1992, pp. 431–560.
16. Djokovic D. Z. Ten New Orders for Hadamard Matrices of Skew Type. *Univ. Beograd Publ., Electrotehn. Fak. Ser. Math.*, 1992, no. 3, pp. 47–59.
17. Balonin N. A., Djokovic D. Z. Negaperiodic Golay Pairs and Hadamard Matrices. *Informatsionno-upravliaiushchie systemy* [Information and Control Systems], 2015, no. 5(78), pp. 2–17. doi:10.15217/issn1684-8853.2015.5.2
18. Balonin N. A., Djokovic D. Z. Symmetry of Two Circulant Hadamard Matrices and Periodic Golay Pairs. *Informatsionno-upravliaiushchie systemy* [Information and Control Systems], 2015, no. 3(76), pp. 2–16. doi:10.15217/issn1684-8853.2015.3.16
19. Djokovic D. Z. Williamson Matrices of Order 4*n* for *n* = 33;35;39. *Discrete Math.*, 1993, no. 115, pp. 267–271.
20. Holzmann W. H., Kharaghani H., Tayfeh-Rezaie B. Williamson Matrices up to Order 59. *Designs, Codes and Cryptography*, 2008, vol. 46, iss. 3, pp. 343–352.
21. Balonin N. A., Seberry Jennifer. The Propus Construction for Symmetric Hadamard Matrices. 2015. Available at: http://arxiv.org/abs/1512.01732 (accessed 15 September 2015).
22. Balonin N. A., Seberry Jennifer. Two-level Cretan Matrices Constructed Using SBIBD. *Special Matrice*, 2015, vol. 3.1, pp. 186–192.
23. Di Matteo O., Djokovic D. Z., Kotsireas I. S. Symmetric Hadamard Matrices of Order 116 and 172 Exist. *Special Matrices*, 2015, vol. 3.1, pp. 227–234.
24. Balonin N. A., Sergeev M. B. Expansion of the Orthogonal Basis in Video Compression. *Vestnik komp'iuternykh i informatsionnykh tekhnologii* [Herald of Computer and Information Technologies], 2014, no. 2, pp. 11–15 (In Russian). doi:10.14489/vkit.2014.02.pp.011-015
25. Balonin N. A., Sergeev M. B. M-matrices and Crystal Structures. *Vestnik Magnitogorskogo gosudarstvennogo tekhnicheskogo universiteta im. G. I. Nosova*, 2013, no. 3, pp. 58–62 (In Russian).
26. Balonin N. A., Sergeev M. B. Matrix of Golden Ratio G10. *Informatsionno-upravliaiushchie systemy* [Information and Control Systems], 2013, no. 6, pp. 2–5 (In Russian).

УДК 004.932
doi:10.15217/issn1684-8853.2016.5.15

ПРИМЕНЕНИЕ НЕЧЕТКОГО ЭВОЛЮЦИОННОГО КЛАССИФИКАТОРА ТАКАГИ — СУГЕНО ДЛЯ ЗАДАЧ ОБНАРУЖЕНИЯ И СОПРОВОЖДЕНИЯ ОБЪЕКТОВ НА ВИДЕОПОСЛЕДОВАТЕЛЬНОСТИ

В. В. Буряченко[a], *канд. техн. наук, старший преподаватель*
М. Н. Фаворская[a], *доктор техн. наук, профессор*
А. И. Томилина[a], *аспирант*
[a]*Сибирский государственный аэрокосмический университет им. академика М. Ф. Решетнёва, Красноярск, РФ*

Постановка проблемы: *обнаружение и сопровождение объектов на видеопоследовательности является неотъемлемой функцией систем видеонаблюдения. Несмотря на то, что объекты интереса, как правило, известны заранее, их вариативность относительно форм, местоположений, характера движения и взаимодействия с другими объектами сцены является значительной, что не позволяет применять жесткие классификационные схемы. В последнее время все большее распространение получают интеллектуальные методы, в частности, методы, основанные на нечеткой логике.* ***Цель:*** *построение эволюционного классификатора на основе нечеткой модели Такаги — Сугено для обнаружения и сопровождения объектов интереса в сложных условиях видеонаблюдения.* ***Результаты:*** *разработан нечеткий эволюционный классификатор, разделяющий блоки пикселов на фон и объекты интереса (объекты переднего плана) и предсказывающий положение движущихся объектов интереса. Эволюционный классификатор на основе нечеткой модели Такаги — Сугено применен для анализа сцен со стационарной и перемещающейся видеокамерой при наличии артефактов съемки, вызывающих нестабильность получаемых видеоматериалов. Алгоритм протестирован с использованием общедоступных данных SVW (Sports Videos for Wild), которые содержат большое число видеопоследовательностей, отснятых движущейся видеокамерой.* ***Практическая значимость:*** *применение нечеткой модели позволяет достичь высокой точности 80–95 % обнаружения и сопровождения объектов в сложных условиях видеонаблюдения.*

Ключевые слова *— нечеткий эволюционный классификатор, нечеткая логика, модель Такаги — Сугено, детектирование фона, компенсация движения.*

Введение

В настоящее время задачи видеонаблюдения и видеоаналитики тесно связаны с проблемами обнаружения людей и других объектов и могут применяться как для создания коммерческих систем, например для поиска постоянных клиентов в магазинах или на автозаправках, так и в городских системах безопасности для обнаружения аварий, оставленных предметов и детектирования сложных ситуаций на дорогах. В большинстве таких задач необходимо выполнять детектирование значимых объектов переднего плана, их сопровождение и анализ видов движения. При этом в непростых условиях видеонаблюдения, таких как изменение освещения, смещение положения камеры, перекрытие значимого объекта различными элементами переднего плана, сложно применять обычные методы детектирования и отслеживания объектов [1, 2].

В последнее время исследования, направленные на разработку методов обнаружения и сопровождения объектов, проводятся с использованием предсказательных алгоритмов. Одним из наиболее известных способов обнаружения объектов на видеопоследовательностях является метод вычитания фона. При этом детектирование объектов переднего плана осуществляется по значительным отличиям их цветояркостных характеристик от построенной на основе большого количества кадров модели фона [3, 4]. Главным его недостатком является необходимость наличия статической сцены, так как используются несколько десятков кадров для построения стабильной модели фона. При этом некоторые изменения в освещенности или незначительные изменения, такие как листва деревьев, вода в реке, могут существенно ухудшить точность обнаружения объектов. Другим недостатком подобных методов является необходимость обработки большого количества кадров при определении положения объекта интереса в сцене.

Анализ методов обнаружения объектов

Метод детектирования и сопровождения объектов с применением фильтра Калмана [5] предсказывает положение объектов, опираясь на гауссово распределение, и предполагает линейную модель движения, которая не всегда применима в реальных условиях.

Широко известен метод, основанный на построении модели фона путем оценки плотности

ядра (Kernel Density Estimation — KDE [3]) по линейной зависимости

$$p\left(z(i,j)_t\right)=\frac{1}{N}\sum_{r=1}^{N}\prod_{l=1}^{n}K_\sigma\left(z(i,j)_{tl}-z(i,j)_{rl}\right), \quad (1)$$

где $z(i, j)$ — набор особенностей, например цветовых характеристик (H, S, V; R, G, B — оттенок, насыщенность, яркость; красный, зеленый, синий); K_σ — функция ядра с пропускной способностью σ; n — количество характеристик; N — количество кадров; i, j — координаты пиксела; r и t — индексы предыдущего и текущего кадров соответственно.

При использовании гауссова распределения модель принадлежности пиксела фону определяется функцией

$$p\left(z(i,j)_t\right)=\frac{1}{N\sqrt{2\pi\sigma^2}}\sum_{r=1}^{N}e^{-\sum_{l=1}^{n}\left(z(i,j)_{tl}-z(i,j)_{rl}\right)^2}. \quad (2)$$

Пусть имеется видеопоток, содержащий информацию о статичной сцене. Тогда можно оценить плотность ядра $p(z(\cdot))$ для каждого пиксела, после чего на основе заданного порога определить, является ли этот пиксел фоном или принадлежит некоторому новому объекту переднего плана [3, 4]. Данный метод считается точным, но дорогостоящим подходом с точки зрения вычислительных затрат. К тому же необходимо подбирать пороговое значение экспериментально [4, 6]. Решение о принадлежности пиксела фону или объектам переднего плана принимается на основе следующего правила:

$$\begin{aligned}&\text{R: ЕСЛИ}\left(p(z(i,j)_t)<\text{Порог}\right)\\&\text{ТО}\left(p\left(z(i,j)_t\right)\text{Область Интереса}\right)\\&\text{ИНАЧЕ}\left(p\left(z(i,j)_t\right)\text{Фон}\right).\end{aligned} \quad (3)$$

В данной работе предложен алгоритм, позволяющий совместить способ оценки ядра с предсказательными способностями эволюционных алгоритмов и нечетких моделей. Нечеткие системы успешно применяются к большому набору задач, таких как принятие решений, распознавание образов и интеллектуальная обработка изображений [7–9]. В дальнейшем развитие алгоритмов и нечетких классификаторов, основанных на искусственных нейронных сетях, стало эффективным решением для построения универсальных классификаторов, в том числе в задачах аппроксимации [10, 11]. Также стоит отметить, что результаты классификации систем, основанных на нечеткой логике, проще интерпретировать и обосновывать, чем результаты работы нейронных и эволюционных алгоритмов.

Эволюционная модель нечеткого классификатора имеет ряд достоинств по сравнению с обычными моделями. Для такой модели следует задавать только вид правил, основанных на экспертных знаниях. Параметры же нечетких правил и их количество классификатор подстраивает в зависимости от ситуации. Это улучшает точность классификации, при этом влияние пользовательских оценок снижается [12].

Эволюционная нечеткая модель Такаги — Сугено (эТС) рассматривалась в работах для решения задач обнаружения объектов [13] и является одной из быстро работающих систем с возможностью предсказания и интерактивной подстройки правил и параметров модели. Предложенный в работе алгоритм позволяет производить оценку положения и траектории объекта в интерактивном режиме однопроходным способом, так как вычисления выполняются с использованием рекурсивных расчетов. К тому же алгоритм не использует пороги, подобранные вручную, что исключает влияние пользовательских оценок на результат работы.

Описание работы эволюционного классификатора

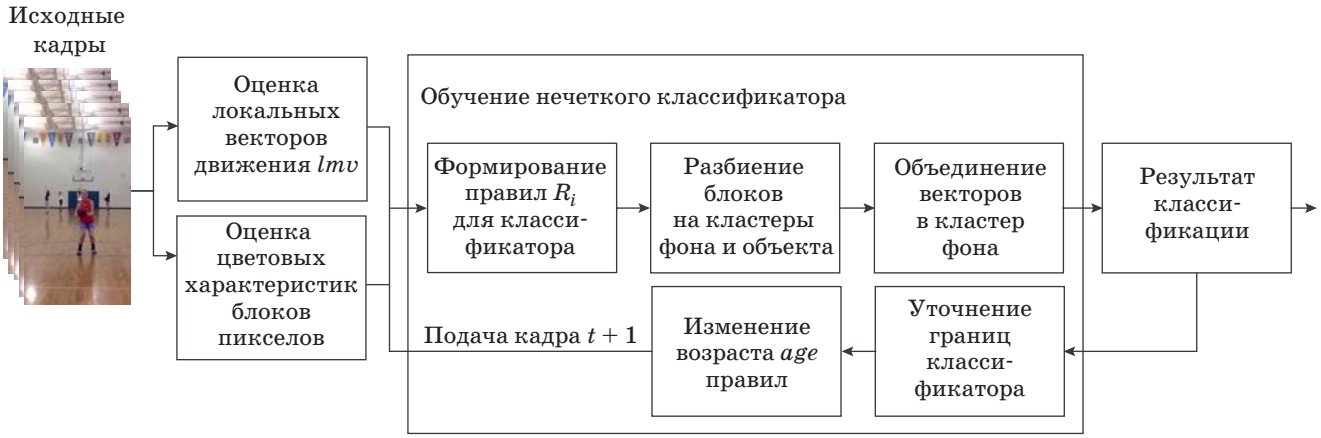
Эволюционная нечеткая модель Такаги — Сугено состоит из набора нечетких правил, количество и параметры которых не являются заранее заданными, а могут подстраиваться в процессе работы. Она является интерактивной самообучающейся версией широко известной нечеткой модели Такаги — Сугено [14], в которой комбинируются нечеткие правила, состоящие из частей ЕСЛИ (антецедент — условие, которое может иметь линейный и нелинейный вид), ТО (консеквент — заключение). Модель обучается на основе набора данных, которые подаются последовательно, и не требует экспертных знаний при создании системы. В данной работе под исходными данными понимается информация о движении и цветовых параметрах объектов, получаемая из кадров видеопотока. Классификация образцов в процессе работы системы состоит из двух этапов:

1) кластеризации данных — положение и характеристики пространства пикселов на текущем и предыдущих кадрах разделяются на локальные подмножества;

2) подстройки параметров нечетких правил в области заключений в соответствии с ранее поданными на вход модели образами и результатами кластеризации на предыдущих этапах.

Во время первого этапа работы значения классов неизвестны и должны быть предсказаны. На втором этапе выполняется обновление информации и подстройка параметров классификатора, в том числе количество нечетких правил (рис. 1).

Алгоритм кластеризации пикселов на принадлежность к фону или объектам переднего плана состоит из трех основных этапов: вычисления



■ ***Рис. 1.*** Схема работы алгоритма кластеризации пикселов на фон и объекты переднего плана при помощи нечеткого классификатора

значений входных параметров модели, формирования нечетких правил для классификатора и обучения классификатора, состоящего в уточнении параметров правил. При успешном обнаружении значимого объекта алгоритм выполняет предсказание его положения на следующем кадре.

Вычисление входных параметров для нечеткой модели

Оценка векторов движения $lmv_{i,j}$ для каждого блока изображения t выполняется на основе вычисления среднеквадратичного отклонения для блоков пикселов между кадрами $t-1$ и t [15]. Набор локальных векторов для всего кадра t позволяет вычислить вектор глобального движения кадра gmv_t в соответствии с аффинной моделью движения, который показывает смещение камеры между двумя соседними кадрами.

Вычисление значения оттенка и интенсивности HL для пиксела с координатами (i, j) производится по формуле

$$HL(i,j)_t = \sqrt{\left(H(i,j)_t\right)^2 - \left(L(i,j)_t\right)^2}. \qquad (4)$$

Показатель среднего значения для данного блока вычисляется на основе суммы квадратов разности H и L для текущего блока изображения размером $w/10$, $h/10$:

$$HL(b,m)_t = \sqrt{\left(\frac{H_t + H_{t-1}}{2}\right)^2 - \left(\frac{L_t + L_{t-1}}{2}\right)^2}, \qquad (5)$$

где b, m — номер блока изображения t, соответствующий текущему положению пикселов (i, j); w, h — ширина и высота изображения.

Формирование правил для классификатора

Эволюционная модель Такаги — Сугено используется для выполнения кластеризации пикселов на принадлежность фону изображения или области, которая может относиться к объектам переднего плана. Достоинством модели является автоматическая подстройка параметров в зависимости от изменяющихся условий на различных кадрах: освещенности, уровня движения, наличия или отсутствия движущихся объектов переднего плана. Также следует отметить, что в связи с реалистичной природой видеопоследовательностей, а именно нелинейным движением камеры, становится невозможным использовать классические методы детектирования фона и объектов в кадре [3, 4].

Эволюционная модель Такаги — Сугено представляется в виде набора правил, который формируется самостоятельно в процессе обучения модели при подаче новых образцов (кадров) в интерактивном режиме. При этом число правил может быть различным в зависимости от количества необходимых состояний модели.

Дополнительно вводится ограничение «возраста» каждого правила, которое позволяет выполнять постепенное обновление состояний модели с целью уменьшить влияние тех правил, которые не применялись за последние t кадров.

При формировании нового правила ему присваивается значение $age_r = 1$. Далее коэффициент возраста каждого правила изменяется при подаче нового образца в зависимости от общего числа правил, возраста правила и того, применялось ли данное правило r на последней итерации. Коэффициент возраста age правила r вычисляется по формуле

$$age_r = age_r + Used_r \left[\frac{age_r}{R}\frac{frame_r}{t(t-frame_r)}\right], \qquad (6)$$

где R — общее число активных правил в модели на данный момент; $frame_r$ — номер кадра, в котором было сформировано правило r; t — номер текущего кадра; $Used_r$ принимает значение 1 или –1 в зависимости от того, было ли использовано правило r на последней итерации.

Эволюционная модель Такаги — Сугено имеет еще одно достоинство: формируемые правила могут быть представлены в виде легкоинтерпретируемых лингвистических выражений следующего вида:

$$\begin{aligned}&\text{R: ЕСЛИ}\left(lmv(i,j)_t \text{ около } gmv_t\right)\\&\text{И}\left(HL(i,j)_t \text{ около } HL(b,m)_t\right)\\&\text{ТО}\left(p(i,j) \text{ Область Интереса}\right)\\&\text{ИНАЧЕ}\left(p(i,j) \text{ Фон}\right).\end{aligned} \quad (7)$$

Эволюционная нечеткая модель Такаги — Сугено также позволяет предсказать значения вычисляемых параметров на следующем кадре, что дает возможность задать границы параметров, отвечающих за выполнение кластеризации блоков пикселов изображения:

$$\begin{aligned}&\text{R: ЕСЛИ}\left(lmv(i,j)_t \text{ около } gmv_t\right)\\&\text{И}\left(HL(i,j)_t \text{ около } HL(b,m)_t\right)\\&\text{ТО}\begin{pmatrix}gmv_{t+1}=a_0+a_1lmv_t+a_2HL_t\\HL_{t+1}=b_0+b_1lmv_t+b_2HL_t\end{pmatrix},\end{aligned} \quad (8)$$

где a_0, a_1, a_2, b_0, b_1, b_2 — настраиваемые в процессе обучения коэффициенты модели Сугено.

Обучение классификатора

В процессе работы алгоритма выполняется интерактивная подача новых изображений видеопоследовательности, и классификатор эволюционной модели Такаги — Сугено постепенно обучается более точно выполнять разделение на объекты переднего плана и фон изображения. Для различных блоков пикселов подбираются разные показатели HL_t и lmv_t, так как цветовые характеристики изображения различны на разных участках. Поэтому формируются различные правила для участков изображения, характеризующих появление объектов переднего плана в соседних блоках пикселов изображения.

При подаче большего числа кадров увеличивается точность оценки принадлежности пиксела одному из классов. Для каждого блока пикселов обучение производится на правилах вида

$$\begin{aligned}&\text{R: ЕСЛИ}\left(x_1 \text{ около } x_1^{i*}\right)\\&\text{И}\ldots\text{И}\left(x_n \text{ около } x_n^{i*}\right)\text{ТО}\left(y_i=\mathbf{X}^{\mathrm{T}}\Theta\right),\end{aligned} \quad (9)$$

где $\mathbf{X}=\left[1, x_1, x_2, \ldots, x_n\right]^{\mathrm{T}}$ описывает $n+1$ расширенных векторов особенностей; y^i — выход модели. Значения вектора $\mathbf{X}$ формируются на основе входных данных HL_t и lmv_t, и этот вектор соответствует сумме квадратов нормализованных параметров для каждого блока:

$$x_i=\sqrt{\sum_{j=0}^{n}\sum_{j=0}^{m}\frac{gmv_{ij}{}^2}{gmv_{med}}+\frac{HL_{ij}{}^2}{HL_{med}}}. \quad (10)$$

Выходные значения каждого правила можно нормализовать таким образом, что сумма значений всех правил будет равна 1:

$$\mathbf{Y}_i=y_i\Big/\sum_{i=1}^{N}y_i. \quad (11)$$

Нормализованные значения y_i могут быть интерпретированы как вероятность принадлежности данного блока изображения к определенному классу: 0 как не относящегося к этому классу и 1 как принадлежащего данному классу. В этом отношении данный подход имеет сходство с так называемым матричным классификатором [16], который используется при наличии знаний обо всех доступных образцах. Подобная схема может применяться не только для разделения исходных данных на два класса, но и в более общих случаях.

Общий выход модели формируется как взвешенная сумма нормированных выходов каждого правила по методу центра тяжести:

$$y=\sum_{i=1}^{N}\left(\delta_i\Big/\sum_{j=1}^{N}\delta_j\right)\mathbf{Y}_i, \quad (12)$$

где δ_i — степень доверия i-го нечеткого правила, которое определяется как произведение (логическая операция И) значений функции принадлежности j-й особенности μ_j^i, $j=[1, n]$, нечеткого множества (x_j около x_j^{i*}):

$$\delta_i=\prod_{j=1}^{n}\delta_j^i(x_j),\ i=\left[1,n\right]. \quad (13)$$

Данная схема вывода соответствует известному правилу эволюционных алгоритмов «Победитель забирает все» [17].

Значение выхода y используется для определения принадлежности набора входных данных к одному из двух классов. Разделение на классы выполняется на основе порога, в этом случае все значения, которые находятся ниже порога, относятся к классу 1, а значения выше порога принадлежат к классу 2. Значение порога tr модифицируется в процессе обучения классификатором, на первом шаге оно задано как $tr = 0{,}5$. Подобная модель может быть применена для решения различных задач классификации входных данных, причем не только на два различных класса [6]:

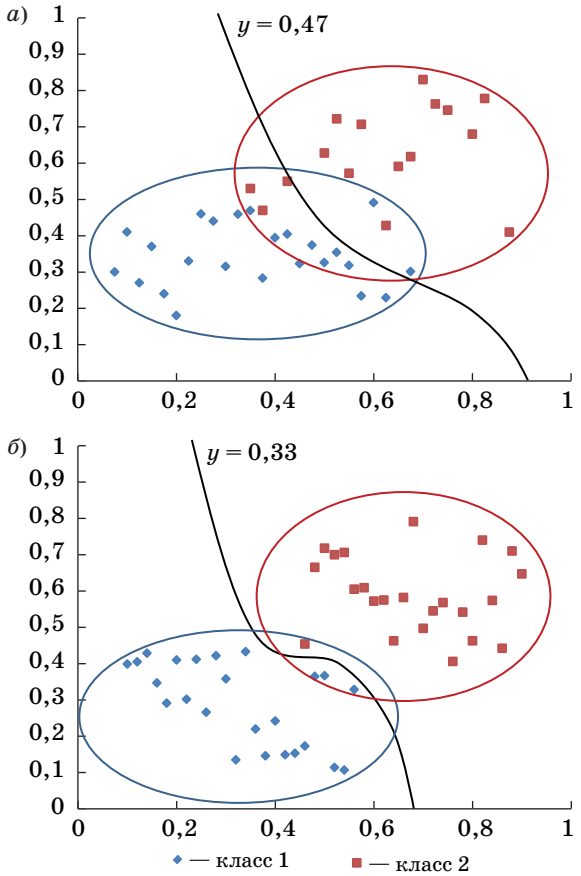
$$\begin{aligned}&\text{ЕСЛИ}\left(y>tr\right)\\&\text{ТО (Класс 1) ИНАЧЕ}\left(\text{Класс 2}\right).\end{aligned} \quad (14)$$

В данной работе выполняется классификация на принадлежность фону или значимым объектам переднего плана, которые, как правило, имеют отличные от фона параметры движения

и цветояркостные характеристики. Таким образом, все блоки пикселов, исходные значения которых находятся выше порога tr, принадлежат объектам переднего плана; пикселы, показатели которых ниже порога, принадлежат фону изображения.

Результаты классификации блоков изображения на два класса (фон и объекты переднего плана) после 100 и 200 образцов (кадров) представлены на рис. 2. Сформированы четыре нечетких правила, которые показаны на двумерном изображении для двух своих признаков. Нелинейная классификация поверхности выводится как значение y, которое равно 0,47 (рис. 2, *а*), и 0,33 (рис. 2, *б*). На рис. 2 показан процесс эволюции классификатора для различных кадров одной и той же видеопоследовательности, что свидетельствует о необходимости интерактивной классификации для решения данной и других задач.

В процессе обучения нечеткий классификатор выполняет подстройку своих параметров: число нечетких правил, изменение возраста правила, при котором влияние каждого из правил изменяется, подстройка порога классификации и другие



■ ***Рис. 2.*** Эволюция границ классификатора на 100-м кадре (*а*) и 200-м кадре (*б*); видеопоследовательность basketball1.mp4, база данных SVW [18]

■ ***Рис. 3.*** Оценка достоверности работы классификатора при обучении в зависимости от формирования правил, изменения их актуальности и изменения сцены видеопотока; видеопоследовательность gymnastic_5511.mp4, база данных SVW [18]

параметры. При этом достоверность классификации после подачи 50–100 образцов (кадров видеопоследовательности) доходит до высоких значений порядка 80–95 % (рис. 3).

Классификатор применялся для задач определения фона и значимых объектов переднего плана на видеопоследовательностях. Отметим, что в зависимости от частоты изменения сцены может потребоваться переобучение классификатора.

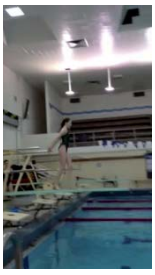
Результаты экспериментов

Эксперименты проводились с применением видеопоследовательностей, представленных в табл. 1. В общей сложности проанализировано 50 видеопоследовательностей из базы данных SVW (Sports Videos in the Wild) [18], включающей более 500 видеопоследовательностей, для которых известен ряд параметров, а именно: принадлежность к определенному виду спорта, наличие движения и дрожания камеры, определены границы движущихся объектов и разрешение видеопоследовательности.

Результаты тестирования набора данных SVW по скорости и достоверности работы предложенного классификатора по сравнению с другими известными алгоритмами эволюционного обучения и разделения изображения на фон и объекты переднего плана приведены в табл. 2.

Также были проведены эксперименты, позволяющие оценить возможность отслеживать движущиеся объекты на основе выделения значимых объектов переднего плана. Данная задача имеет свои особенности в зависимости от наличия движущейся камеры. Один из наиболее часто применяемых методов в задачах отслеживания объектов основан на методе вычитания фона [4]. Однако в случае движения оператора он становится неприменим. Алгоритм показал

■ ***Таблица 1.*** Описание исходных данных экспериментов

Название	Пример кадра	Разрешение, пикс	Количество кадров	Виды движения	Объекты переднего плана	Априорная информация о границах движения
basketball_ 10191.mp4 (SVW)		270×480	120	Статичная сцена, неравномерное движение объектов	Несколько объектов	Есть границы движения для каждого из кадров
gymnastic_ 5511.mp4 (SVW)		360×480	300	Нестабильная съемка, движение значимого объекта в кадре	Один объект интереса	То же
diving_4140 .mp4 (SVW)		270×480	180	Один движущийся объект, быстрое смещение камеры	Один объект интереса	–"–
volley_1010 0153.mp4 (SVW)		270×480	480	Несколько движущихся объектов, статичная сцена	Несколько объектов небольшого размера	–"–
diving_1104 .mp4 (SVW)		270×480	180	Один движущийся объект, быстрое смещение камеры	Один объект интереса	–"–
running_546 .mp4 (SVW)		270×480	210	Один движущийся объект, быстрое смещение камеры	Один объект интереса	–"–
sam_1.avi (Grundmann, [19])		630×360	330	Нестабильная съемка, неравномерное движение объекта в кадре	Один объект интереса	Маска движения для тестовых кадров

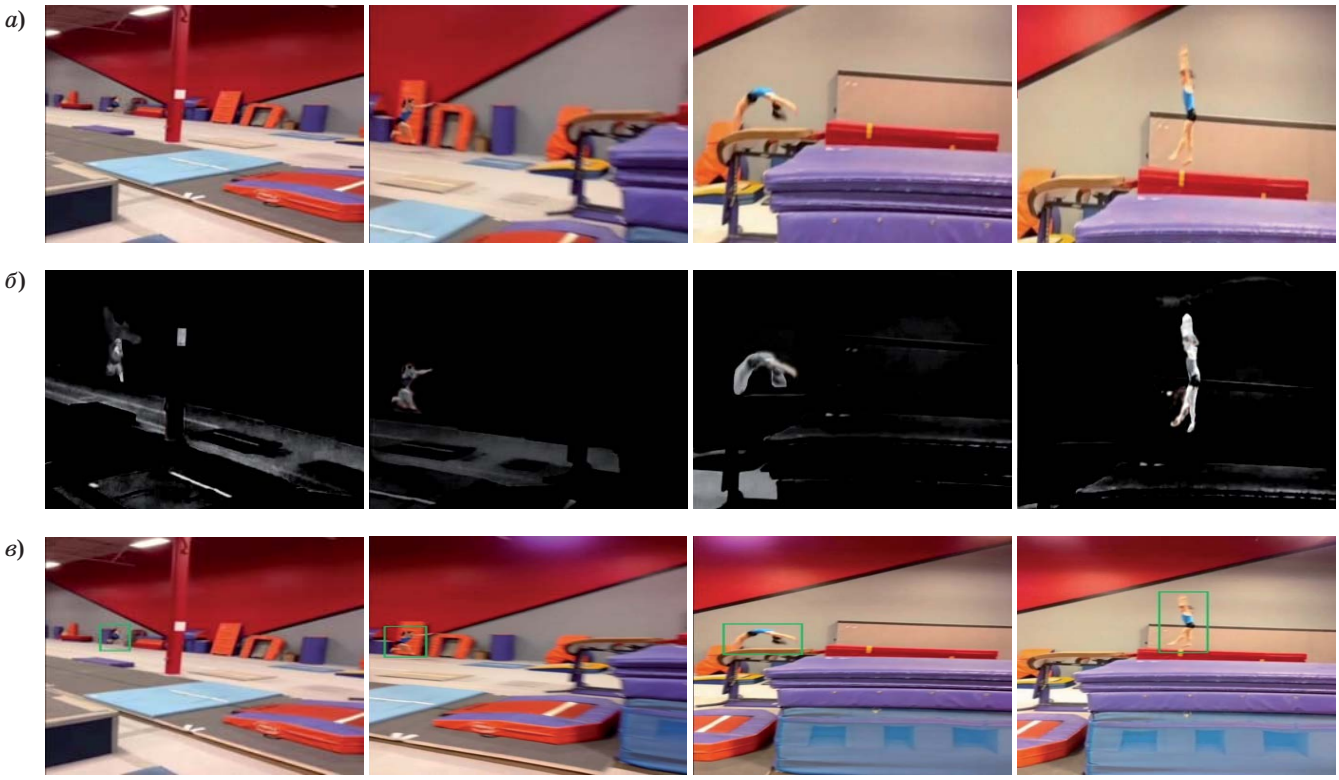
■ ***Таблица 2.*** Сравнение эффективности работы эТС-классификатора с другими алгоритмами

Название алгоритма	Время обработки одного кадра, мс	Время обработки 300 кадров (с учетом дополнительных операций), мс	Достоверность классификации, %	Вычислительные затраты
эТС-модель	2,11	452,16	82,0	0,315
KNN [12]	2,52	652,10	83,4	0,45
C45 [12]	8,39	2411,67	75,5	6,48
RDE [6]	1,27	271,32	75,1	0,41
eClass1 [12]	1,98	591,00	84,5	0,2480

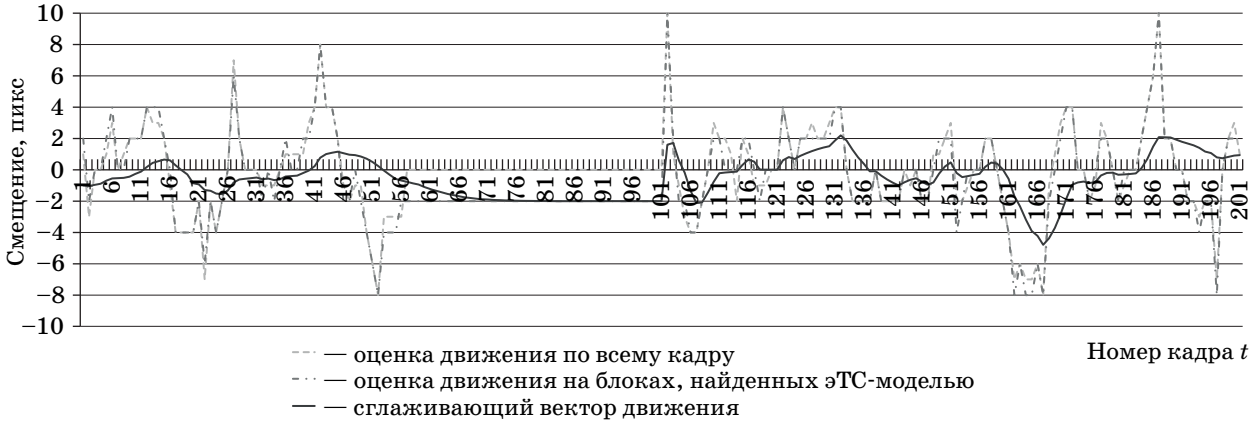
высокую надежность работы при отслеживании положения движущихся объектов (более 85 %), однако точность отслеживания объекта можно повысить, если от блочного способа выделения объекта перейти к цветояркостным компонентам (рис. 4).

Третий метод тестирования предназначался для оценки качества компенсации движения на видеопоследовательности [20]. В задачах стабилизации видеопоследовательности одним из этапов работы является оценка вектора глобального движения кадра [21], при этом на точность оценки может оказать негативное влияние наличие объектов переднего плана, движение которых отлично от движения камеры. Необходимо устранить непреднамеренное движение камеры, сохранив реальное движение, например панорамирование или поворот камеры. Поэтому целесообразно выполнять оценку сглаживающего вектора движения только на основе фона изображения.

Эволюционная модель Такаги — Сугено применялась для классификации кадров видеопоследовательности на фон и объекты переднего плана, после чего была проведена оценка сглаживающего вектора на основе всех имеющихся векторов движения и векторов [22], относящихся к фону изображения (рис. 5).



■ ***Рис. 4.*** Использование эТС-классификатора для отслеживания движущихся объектов в сложных условиях: *а* — оригинальные кадры видеопоследовательности; *б* — применение классификатора для обнаружения значимых объектов; *в* — выделение объекта при отслеживании движения; видеопоследовательность gymnastic_5511.mp4 [18]



■ ***Рис. 5.*** Использование эТС-классификатора для повышения качества оценки сглаживающего вектора движения для видеопоследовательности diving_4140.mp4 **[16]**

Результаты работы алгоритма показали увеличение достоверности оценки сглаживающего вектора на 10–20 %.

Заключение

В работе представлено описание эволюционного нечеткого классификатора на основе модели Такаги — Сугено, отличительной чертой которого является возможность изменять собственные правила и настраивать параметры модели. Для классификатора изначально задан вид правил и набор исходных данных. В процессе обучения подаются экземпляры данных — модуль и направление векторов движения и цвето-яркостные характеристики пикселов. В дальнейшем выполняется их сравнение с входными данными соседних блоков в целях кластеризации параметров на два класса: принадлежность к значимым объектам переднего плана или фону изображения. Эволюционный нечеткий классификатор показал высокую надежность при детектировании и сопровождении объектов переднего плана, сравнимую с другими известными алгоритмами. Следует отметить, что эффективность алгоритма при выделении объектов переднего плана значительно превосходит аналоги, в которых используются только пространственные характеристики, такие как яркость, контраст, цвет, но не учитывается движение самих объектов.

Производительность алгоритма была протестирована с использованием известных баз данных, содержащих большое количество видеопоследовательностей движущихся объектов при смещении и непреднамеренном движении камеры. Разработанный алгоритм эволюционного нечеткого классификатора Такаги — Сугено может быть использован в задачах сопровождения объектов, выделения нежелательных объектов на видеопоследовательности, а также в тех алгоритмах, для которых необходимо выполнять сглаживание движения, например для удаления глобального движения или стабилизации видеопоследовательностей в сложных сценах.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 16-07-00121 А.

Литература

1. **Foresti G.,** et al. Active Video-Based Surveillance System: the Low-Level Image and Video Processing Techniques Needed for Implementation/ G. Foresti, C. Micheloni, L. Snidaro, P. Remagnino, T. Elis // IEEE Signal Process Magazine. 2005. Vol. 22. N 2. P. 25–27.
2. **Pavlidis I.,** et al. Urban Surveillance Systems: from the Laboratory to the Commercial World/ I. Pavlidis, V. Morellas, P. Tsiamyrtzis, S. Harp // Proc. of the IEEE. 2001. Vol. 89. N 10. P. 1478–1497.
3. **Elgammal A.,** et al. Background and Foreground Modeling Using Non-Parametric Kernel Density Estimation for Visual Surveillance / A. Elgammal, R. Duraiswami, D. Harwood, L. Davis // Proc. of the IEEE. 2002. Vol. 90. N 7. P. 1151–1163.
4. **Cheung S.-C. S., Kamath C.** Robust Techniques for Background Subtraction in Urban Traffic Video // EURASIP Journal on Applied Signal Processing. 2005. Vol. 2005. P. 2330–2340.
5. **Kalman R. E.** A New Approach to Linear Filtering and Prediction Problem // Transactions of the ASME – Journal of Basic Engineering. 1960. Vol. 82 (Series D). P. 35–45.
6. **Angelov P., Sadeghi-Tehran P., Ramezani R.** An Approach to Automatic Real-Time Novelty Detection,

Object Identification, and Tracking in Video Streams Based on Recursive Density Estimation and Evolving Takagi–Sugeno Fuzzy Systems // Intern. Journal of Intelligent Systems. 2010. Vol. 26. N 3. P. 189–205.
7. **Cordon O.,** et al. Ten Years of Genetic Fuzzy Systems: Current Framework and New Trends/ O. Cordon, F. Gomide, F. Herrera, F. Hoffmann, L. Magdalena // Fuzzy Sets and Systems. 2004. Vol. 141. N 1. P. 5–31.
8. **Ishibuchi H., Nakashima T., Nii M.** Classification and Modeling with Linguistic Granules: Advanced Information Processing. — Berlin, Heidelberg: Springer-Verlag, 2004. — 304 p.
9. **Favorskaya M. N., Buryachenko V. V.** Video Stabilization of Static Scenes Based on Robust Detectors and Fuzzy Logic // Intelligent Interactive Multimedia Systems and Services: Proc. of the 6th Intern. Conf. on Intelligent Interactive Multimedia Systems and Services (IIMSS 2013); Frontiers in Artificial Intelligence and Applications/G. A. Tsihrintzis, M. Virvou, T. Watanabe, L. C. Jain, R. J. Howlett (Eds.). 2013. Vol. 254. P. 11–20.
10. **Wang L.-X.** Fuzzy Systems are Universal Approximators // Proc. of the IEEE Intern. Conf. on Fuzzy Systems, San Diego, CA, USA, 1992. P. 1163–1170.
11. **Hopner F., Klawonn F.** Obtaining Interpretable Fuzzy Models from Fuzzy Clustering and Fuzzy Regression // Proc. 4th Intern. Conf. on Knowledge-Based Intelligent Engineering Systems and Allied Technologies, Brighton, UK, 2000. Vol. 1. P. 162–165.
12. **Angelov P., Xiaowei Z.** Evolving Fuzzy-Rule-Based Classifiers from Data Streams // IEEE Transactions on Fuzzy Systems. 2008. Vol. 16. N 6. P. 1462–1475.
13. **Angelov P., Filev D.** An Approach to On-Line Identification of Takagi–Sugeno Fuzzy Models // IEEE Transactions on Systems, Man, and Cybernetics: Part B (Cybernetics). 2004. Vol. 34. N 1. P. 484–498.
14. **Sugeno M.** Industrial Applications of Fuzzy Control. — N. Y.: Elsevier Science Inc., 1985. — 278 p.
15. **Буряченко В. В., Ткачева А. А., Томилина А. И.** Разработка программного обеспечения стабилизации видеопоследовательностей в системах технического зрения // Региональные проблемы дистанционного зондирования Земли: материалы Междунар. науч. конф., Красноярск, 22–25 сентября 2015 г. Красноярск, 2015. С. 105–109.
16. **Hastie T., Tibshirani R., Friedman J.** The Elements of Statistical Learning: Data Mining, Inference and Prediction. 2nd ed. — Berlin, Heidelberg: Springer-Verlag, 2009. — 698 p.
17. **Klawonn F., Klement P. E.** Mathematical Analysis of Fuzzy Classifiers // Advances in Intelligent Data Analysis Reasoning about Data (IDA-97): Proc. of Second Intern. Symp., London, UK, Aug. 4–6, 1997/ X. Liu, P. Cohen, M. Berthold (Eds.). LNCS. 1997. Vol. 1280. P. 359–370.
18. **Safdarnejad S. M.,** et al. Sports Videos in the Wild (SVW): A Video Dataset for Sports Analysis, Automatic Face and Gesture Recognition/ S. M. Safdarnejad, L. Xiaoming, U. Lalita, A. Brooks, J. Wood, D. Craven // Proc. 11th IEEE Intern. Conf. and Workshops on Automatic Face and Gesture Recognition (FG), Ljubljana, Slovenia, 2015. Vol. 1. P. 1–7.
19. **Grundmann M., Kwatra V., Essa I.** Auto-Directed Video Stabilization with Robust L1 Optimal Camera Paths // Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), Providence, RI, USA, 2011. P. 225–232.
20. **Favorskaya M. N., Buryachenko V. V.** Fuzzy-Based Digital Video Stabilization in Static Scenes // Intelligent Interactive Multimedia Systems and Services in Practice / G. A. Tsihrintzis, M. Virvou, L. C. Jain, R. J. Howlett, T. Watanabe (Eds.). SIST. 2015. Vol. 36. P. 63–83.
21. **Favorskaya M. N., Jain L. C., Buryachenko V. V.** Digital Video Stabilization in Static and Dynamic Scenes // Computer Vision in Control Systems-1: Mathematical Theory / M. N. Favorskaya, L. C. Jain (Eds.). ISRL. 2015. Vol. 73. P. 261–310.
22. **Буряченко В. В., Томилина А. И.** Построение плавной 3D-траектории движения камеры на основе методов структуры по движению // Цифровая обработка сигналов и ее применение: материалы 18-й Междунар. конф., Москва, 30 марта — 1 апреля 2016 г. М., 2016. Т. 2. С. 876–881.

UDC 004.932
doi:10.15217/issn1684-8853.2016.5.15

Using Fuzzy Evolutionary Classifier for Detecting and Tracking Objects in Video Sequences

Buryachenko V. V.[a], PhD., Associate Professor, buryachenko@sibsau.ru
Favorskaya M. N.[a], Dr. Sc., Tech., Professor, favorskaya@sibsau.ru
Tomilina A. I.[a], Post-Graduate Student, nastomila@gmail.com
[a]Siberian State Aerospace University named after academician M. F. Reshetnev, 31, Krasnoyarsky Rabochy St., 660037, Krasnoyarsk, Russian Federation

Introduction: Detecting and tracking objects on video sequences is an essential function of surveillance systems. Even though the objects of interest are usually determined ahead, their variability in reference to shapes, locations, motion types and interaction with other objects is important, making rigid classification schemes inappropriate. Recently, intelligent methods, particularly those based

on fuzzy logic, are becoming more and more common. **Purpose:** On the base of Takagi–Sugeno fuzzy model, an evolutionary classifier has to be built, in order to detect and track objects of interest under difficult surveillance conditions. **Results:** A fuzzy evolutionary classifier is developed which separates pixel blocks into the background and objects of interest (foreground objects), predicting the location of the moving objects. This evolutionary classifier based on the fuzzy Takagi–Sugeno model is applied for the analysis of scenes with a stationary or moving video camera under shooting artifacts which make the video materials non-stationary. The algorithm was tested using a public data set "Sports Videos for Wild" (SVW) which contains a large number of video sequences obtained from a moving video camera. **Practical relevance:** The application of the fuzzy model provides a high accuracy (80–95 %) of detecting and tracking objects under difficult surveillance conditions.

Keywords — Fuzzy Evolutionary Classifier, Fuzzy Logic, Takagi–Sugeno Model, Background Detection, Motion Compensation.

References

1. Foresti G., Micheloni C., Snidaro L., Remagnino P., Elis T. Active Video-Based Surveillance System: the Low-Level Image and Video Processing Techniques Needed for Implementation. *IEEE Signal Process Magazine*, 2005, vol. 22, no. 2, pp. 25–27.
2. Pavlidis I., Morellas V., Tsiamyrtzis P., Harp S. Urban Surveillance Systems: from the Laboratory to the Commercial World. *Proc. of the IEEE*, 2001, vol. 89, no. 10, pp. 1478–1497.
3. Elgammal A., Duraiswami R., Harwood D., Davis L. Background and Foreground Modeling Using Non-Parametric Kernel Density Estimation for Visual Surveillance. *Proc. of the IEEE*, 2002, vol. 90, no. 7, pp. 1151–1163.
4. Cheung S.-C. S., Kamath C. Robust Techniques for Background Subtraction in Urban Traffic Video. *EURASIP Journal on Applied Signal Processing*, 2005, vol. 2005, pp. 2330–2340.
5. Kalman R. E. A New Approach to Linear Filtering and Prediction Problem. *Transactions of the ASME – Journal of Basic Engineering*, 1960, vol. 82 (Series D), pp. 35–45.
6. Angelov P., Sadeghi-Tehran P., Ramezani R. An Approach to Automatic Real-Time Novelty Detection, Object Identification, and Tracking in Video Streams Based on Recursive Density Estimation and Evolving Takagi–Sugeno Fuzzy Systems. *Intern. Journal of Intelligent Systems*, 2010, vol. 26, no. 3, pp. 189–205.
7. Cordon O., Gomide F., Herrera F., Hoffmann F., Magdalena L. Ten Years of Genetic Fuzzy Systems: Current Framework and New Trends. *Fuzzy Sets and Systems*, 2004, vol. 141, no. 1, pp. 5–31.
8. Ishibuchi H., Nakashima T., Nii M. *Classification and Modeling with Linguistic Granules: Advanced Information Processing*. Berlin, Heidelberg, Springer-Verlag, 2004. 304 p.
9. Favorskaya M. N., Buryachenko V. V. Video Stabilization of Static Scenes Based on Robust Detectors and Fuzzy Logic. *Proc. of the 6th Intern. Conf. on Intelligent Interactive Multimedia Systems and Services (IIMSS 2013) "Intelligent Interactive Multimedia Systems and Services"*, Tsihrintzis G. A., Virvou M., Watanabe T., Jain L. C., Howlett R. J. (Eds.), 2013, Frontiers in Artificial Intelligence and Applications, vol. 254, pp. 11–20.
10. Wang L.-X. Fuzzy Systems are Universal Approximators. *IEEE Intern. Conf. on Fuzzy Systems*, San Diego, CA, USA, 1992, pp. 1163–1170.
11. Hopner F., Klawonn F. Obtaining Interpretable Fuzzy Models from Fuzzy Clustering and Fuzzy Regression. *4th Intern. Conf. on Knowledge-Based Intelligent Engineering Systems and Allied Technologies*, Brighton, UK, 2000, vol. 1, pp. 162–165.
12. Angelov P., Xiaowei Z. Evolving Fuzzy-Rule-Based Classifiers from Data Streams. *IEEE Transactions on Fuzzy Systems*, 2008, vol. 16, no. 6, pp. 1462–1475.
13. Angelov P., Filev D. An Approach to On-Line Identification of Takagi–Sugeno Fuzzy Models. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 2004, vol. 34, no. 1, pp. 484–498.
14. Sugeno M. *Industrial Applications of Fuzzy Control*. New York, Elsevier Science Inc., 1985. 278 p.
15. Buryachenko V. V., Tkacheva A. A., Tomilina A. I. Development of Software Tool for Video Sequences Stabilization in Computer Vision Systems. *Materialy Mezhdunarodnoy nauchnoi konferentcii "Pegionalnyue problemy distantchionnogo zondirovania Zemli"* [Proc. Intern. Scientific Conf. "Regional Problems of Remote Sensing"]. Krasnoyarsk, September 22–25, 2015, pp. 105–109 (In Russian).
16. Hastie T., Tibshirani R., Friedman J. *The Elements of Statistical Learning: Data Mining, Inference and Prediction*. 2nd ed., Berlin, Heidelberg, Springer-Verlag, 2009. 698 p.
17. Klawonn F., Klement P. E. Mathematical Analysis of Fuzzy Classifiers. *Proc. of Second Intern. Symp. "Advances in Intelligent Data Analysis Reasoning about Data" (IDA-97)*, X. Liu, P. Cohen, M. Berthold (Eds.), 1997, LNCS, vol. 1280, pp. 359–370.
18. Safdarnejad S. M., Xiaoming L., Lalita U., Brooks A., Wood J., Craven D. Sports Videos in the Wild (SVW): A Video Dataset for Sports Analysis, Automatic Face and Gesture Recognition. *11th IEEE Intern. Conf. and Workshops on Automatic Face and Gesture Recognition (FG)*, Ljubljana, Slovenia, 2015, vol. 1, pp. 1–7.
19. Grundmann M., Kwatra V., Essa I. Auto-Directed Video Stabilization with Robust L1 Optimal Camera Paths. *IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, Providence, RI, USA, 2011, pp. 225–232.
20. Favorskaya M. N., Buryachenko V. V. Fuzzy-Based Digital Video Stabilization in Static Scenes. *Intelligent Interactive Multimedia Systems and Services in Practice*, G. A. Tsihrintzis, M. Virvou, L. C. Jain, R. J. Howlett, T. Watanabe (Eds.), 2015, SIST, vol. 36, pp. 63–83.
21. Favorskaya M. N., Jain L. C., Buryachenko V. V. Digital Video Stabilization in Static and Dynamic Scenes. *Computer Vision in Control Systems-1: Mathematical Theory*, Favorskaya M. N., Jain L. C. (Eds.), 2015, ISRL, vol. 73, pp. 261–310.
22. Buryachenko V. V., Tomilina A. I. Building of Smooth 3D Trajectory of Camera Motion Using Structure on Motion Methods. *Materialy 18 Mezdunarodnoy konferencii "Tsifrovaia obrabotka signalov i ee primenenie"* [Proc. 18 Intern. Conf. "Digital Signal Processing and its Applications"], Moscow, 30 March–1 April, 2016, vol. 2, pp. 876–881 (In Russian).

УДК 626
doi:10.15217/issn1684-8853.2016.5.25

К ВОПРОСУ О НАДЕЖНОСТИ АВТОНОМНОГО НЕОБИТАЕМОГО ПОДВОДНОГО АППАРАТА С МУЛЬТИАГЕНТНОЙ АРХИТЕКТУРОЙ СИСТЕМЫ УПРАВЛЕНИЯ

Л. А. Мартынова[a], *доктор техн. наук, ведущий научный сотрудник*
М. Б. Розенгауз[a], *канд. техн. наук, доцент, старший научный сотрудник*
[a]*АО «Концерн «ЦНИИ «Электроприбор», Санкт-Петербург, РФ*

Введение: *применение современных технологий при разработке систем управления автономных необитаемых подводных аппаратов, например мультиагентной технологии, несмотря на неоспоримые ее преимущества и обилие публикаций по этому вопросу, требовало оценки надежности функционирования автономных необитаемых подводных аппаратов с мультиагентной системой управления.* ***Цель:*** *проведение сравнительного анализа надежности автономных необитаемых подводных аппаратов с мультиагентной системой управления и с другими системами управления.* ***Методы:*** *сравнительный анализ осуществлялся на основе вероятности безотказной работы автономного необитаемого подводного аппарата, рассчитываемой по специально разработанной математической имитационной модели.* ***Результаты:*** *определены особенности мультиагентных систем управления, заключающиеся в возможности учета большего количества видов движения подводного аппарата при принятии решения в условиях возникновения нештатных и аварийных ситуаций. Немультиагентная система позволяет учитывать лишь два вида движения — по маршрутной траектории к точке и движение при преодолении препятствия, в отличие от мультиагентной системы, способной в дополнение учитывать движение еще в условиях боковых ограничений. Результаты моделирования показали, что при движении автономных необитаемых подводных аппаратов в условиях боковых ограничений превышение вероятности безотказной работы таких аппаратов с мультиагентной системой управления достигло 0,3 по сравнению с аппаратами с немультиагентной системой управления.* ***Практическая значимость:*** *приведенные в работе результаты свидетельствуют о повышении надежности автономного необитаемого подводного аппарата при переходе от немультиагентной системы управления к мультиагентной и целесообразности использования в дальнейшем мультиагентной системы управления.*

Ключевые слова *— автономный необитаемый подводный аппарат, система управления, мультиагентная технология, имитационная модель.*

Введение

Автономный необитаемый подводный аппарат (АНПА) является многофункциональным роботом морского базирования, предназначенным для перемещения из одного района в другой, доставки полезной нагрузки и выполнения миссии в удаленном районе [1].

По сравнению с использованием роботов наземного и воздушного базирования использование АНПА затруднено особенностями морской среды:

— отсутствием глобальной навигационной спутниковой системы;

— ограниченностью гидроакустической связи из-за быстрого затухания звука в воде;

— ограниченностью объема передаваемой информации по гидроакустической связи.

В последнее время в связи с совершенствованием оборудования на АНПА, прежде всего — аккумуляторных батарей, появилась возможность отправлять АНПА на несколько суток автономного плавания на сотни километров. При этом открывшаяся возможность повлекла за собой необходимость решать целый комплекс сопутствующих задач, направленных на прогнозирование ситуаций, в которых может оказаться АНПА при длительном переходе, в том числе нештатных и аварийных. В свою очередь это потребовало совершенствования всей системы, обеспечивающей функционирование АНПА, которой является система управления (СУ) АНПА. Поэтому в настоящий момент разработчики роботов переходят к современным технологиям, одной из которых является мультиагентная технология [2–4]. Переход к мультиагентной технологии, безусловно, способствует улучшению функционирования СУ АНПА, однако при этом возникает вопрос надежности функционирования АНПА. Дело в том, что формирование мультиагентной системы — процесс творческий, готовых шаблонов и алгоритмов нет, структура мультиагентной системы и взаимодействие агентов зависят от конкретного образца АНПА, его возможностей, задач, стоящих перед АНПА, и т. д. Кроме того, надежность АНПА, наряду с его архитектурой, определяется и особенностями программной реализации, которая также должна обеспечивать надежное функционирование программного обеспечения.

В связи с вышесказанным целью настоящей работы явилось проведение сравнительной оценки надежности АНПА при переходе от использования СУ, построенной на традиционных технологиях, к мультиагентной СУ.

Особенности мультиагентных систем

Функционирование АНПА, его поведение определяется алгоритмами, заложенными в СУ АНПА. В зависимости от текущего состояния АНПА, а также от поступивших в СУ АНПА сообщений вырабатываются решения, которые передаются затем на соответствующие устройства АНПА. Первоначально, при выполнении несложных миссий, формирование архитектуры СУ АНПА основывалось на объектно-ориентированном подходе, при котором в СУ АНПА все переходы из одного состояния в другое были жестко заданы и заранее прописаны. Например, при рассмотрении перемещения АНПА из точки в точку разработчики ограничивались лишь двумя вариантами: движением к точке и обходом препятствия. В программной реализации такого алгоритма достаточно было всю логику представить единым файлом, а различные состояния АНПА программировать операторами условного перехода. Однако при возникновении сбоя в программном обеспечении процесс функционирования АНПА автоматически останавливался.

С увеличением автономности АНПА часть задач, выполняемых ранее оператором, перекладывается на АНПА для выполнения в автоматическом режиме. Это означает, что теперь уже в отсутствие возможности управления через оператора необходимо предусмотреть гораздо большее количество состояний, а каждое из них характеризуется гораздо большим количеством параметров. Жесткое прописывание всех возможных вариантов сочетания параметров становится практически неэффективным, поскольку, с одной стороны, существенно возросло количество ситуаций, в том числе нештатных и аварийных, а с другой стороны, при принятии решения в автоматическом режиме необходим полный перебор всех вариантов. Указанные обстоятельства приводят к значительным перегрузкам вычислительной системы АНПА и к снижению его надежности, поскольку при возникновении непредусмотренных заранее вариантов АНПА не будет знать, что делать, а это, в свою очередь, может привести к совершенно непредсказуемым последствиям.

Вследствие этого с течением времени разработчики АНПА стали переходить к компонентно-ориентированным системам [4], в которых каждой отдельной подсистеме СУ соответствовала своя программа, именуемая компонентом. Эти программы были условно разнесены по иерархическим слоям, а общение между программами-компонентами происходило по локальной сети. Такой подход, безусловно, повышал надежность всей системы АНПА, поскольку выход из строя одной какой-то программы в этом случае теперь уже не приводил к всеобщему сбою в программном обеспечении АНПА. Программы функционировали параллельно, что существенно увеличивало быстродействие и скорость вычислений.

Однако условное разбиение СУ на слои ограничивало возможности каждого из компонентов, поскольку компоненты верхнего слоя не могли общаться напрямую с компонентами нижнего слоя. Вместе с тем такой важный показатель, как текущий расход энергии и остаток энергоресурса (компоненты нижнего слоя) необходимы при планировании или перепланировании миссии (компоненты верхнего слоя) в случае возникновения нештатных ситуаций. Или результаты навигационных определений АНПА (компоненты нижнего слоя) необходимы при соотнесении их с положением АНПА на маршрутной траектории (компоненты верхнего слоя).

В связи с этим разработчики АНПА перешли к использованию более прогрессивного подхода — агентного, отличительной особенностью которого является рассмотрение агентов как равноправных компонентов, без разнесения по слоям. Каждый отдельно взятый агент общается только с теми агентами, с которыми есть необходимость. Такой подход повышает надежность системы, поскольку каждый агент имеет неограниченный доступ к информации, вырабатываемой другими агентами. Один из таких подходов агентной системы со слоем «классной доски» реализован в АНПА «ZT-AUV» [5]. В СУ «ZT-AUV» агенты различных устройств АНПА обращаются к единому слою «классной доски», получая от него необходимую информацию и попутно обновляя ее.

Однако еще более перспективным вариантом агентных систем являются мультиагентные системы [2–4], которые были успешно использованы в наземных роботах [4], а затем авторами предложены для реализации в СУ АНПА [6–9].

Мультиагентные системы оперируют понятиями агентов, т. е. автономных программных объектов, способных управлять достижением поставленных целей в условиях неопределенности путем выработки и анализа вариантов принятия решений и согласованного взаимодействия с другими агентами.

Ключевыми свойствами агентов являются:

— автономность — способность действовать самостоятельно, контролируя свои действия и внутреннее состояние;

— активность — стремление достичь поставленных целей;

— реактивность — адаптивное поведение как реакция на внешние воздействия;

— социальное поведение — взаимодействие с другими агентами для достижения согласованных решений.

Указанные свойства определяют следующие преимущества использования мультиагентных систем:

— модульность без необходимости учета функционирования всего программного обеспечения;

— распределенные вычисления;

— повышенную скорость доставки сообщений;

— взаимозаменяемость программных блоков;

— повышенную надежность;

— повторное использование отдельных программных блоков;

— независимость вычислительных процессов;

— параллельную обработку больших массивов данных;

— оперативное выявление выхода из строя отдельного программного блока и перераспределение управления между оставшимися программными блоками;

— способность к самообучению и самосовершенствованию.

Алгоритм каждого агента основан на анализе сложившейся обстановки, выработке решения относительно формируемой информации (сообщения, команды, запроса) и определения агента-адресата, которому предполагается передать эту информацию.

Все сказанное позволяет утверждать, что переход к использованию мультиагентного подхода приводит к повышению надежности таких систем, поскольку в мультиагентных системах организация функционирования каждого агента построена таким образом, что в любой возникшей ситуации будет принято решение, пусть и не оптимальное с точки зрения АНПА в целом.

Агентами в СУ АНПА являются подсистемы СУ АНПА, такие как подсистема навигации, подсистема освещения обстановки, подсистема движения, подсистема энергетического обеспечения и т. д. Каждый из перечисленных агентов в свою очередь также может являться мультиагентной системой. Например, для АНПА возможно предусмотреть следующие варианты движения:

— перемещение из точки в точку;

— возврат на маршрутную траекторию по результатам показания бортовой инерциальной навигационной системы или обсервации по гидроакустическим навигационным станциям (ГАНС) или глобальной навигационной спутниковой системе;

— обход препятствия;

— плавание в условиях ограничений (узкости, буровые вышки, другие подвижные и неподвижные объекты).

Каждому из перечисленных вариантов движения соответствует агент, которому присваиваются конкретные полномочия, а функционирование агентов движения определяется алгоритмами, направленными на формирование параметров движения АНПА — курса и скорости, и передачу параметров движения агенту движительно-рулевой системы. Количество ситуаций может быть и больше: например, в работе [10] предусмотрено 13 (!) вариантов движения АНПА:

— для исключения столкновения с препятствием;

— для исключения препятствия, положение которого заранее известно;

— для уменьшения расстояния между АНПА и обнаруженным препятствием;

— для управления АНПА последовательно по заданным глубинам;

— при изменении положения маршрутной точки;

— для исключения пересечений и возврата на прежний маршрут;

— для безопасности при выходе АНПА за ограничения по пространству, времени и глубине;

— с периодическим изменением скорости АНПА для обеспечения акустической связи в условиях пониженного собственного шума;

— с периодическим изменением глубины и скорости АНПА при получении уточнений местоположения АНПА по GPS-определениям;

— с имитацией наблюдаемых курса и скорости другого АНПА;

— для удержания АНПА на заданных широте/долготе путем изменения скорости;

— для удержания АНПА в заданном диапазоне параметров других указанных АНПА (в составе группы);

— для перемещения АНПА с набором заданных путевых точек в *X-Y*-плоскости.

Очевидно, что при использовании объектно-ориентированного подхода предусмотрение всех перечисленных выше вариантов движения АНПА в сочетании с другими параметрами СУ привело бы к существенной перегрузке всей вычислительной системы АНПА и увеличению времени на обработку информации.

Таким образом, формирование мультиагентных систем — это, с одной стороны, формирование идеологии функционирования СУ в целом, которая включает в себя назначение агентов, алгоритмы функционирования каждого агента в отдельности и алгоритмы обмена данными между агентами. С другой стороны, агент — это самостоятельная программа (программный компонент), и такие агенты-программы работают параллельно, а при использовании нескольких компьютеров формируют распределенные вычисления, более эффективные и надежные по сравнению с последовательными.

Надежность мультиагентных систем

При рассмотрении надежности АНПА будем ориентироваться на то, что надежность АНПА — это свойство АНПА выполнять свои функции, сохраняя во времени показатели качества эксплуатации, соответствующие режимам их использования в условиях чрезвычайных ситуаций. Иными словами, надежность в технике обычно означает тот минимум требований, который обеспечивает основное функционирование технического устройства. Надежность характеризуется безотказностью работы рассматриваемого технического устройства. Перенеся сказанное на АНПА как сложное техническое устройство, можно сказать, что надежность АНПА характеризует его способность выполнять миссию от начала и до самого конца, включая посадку на донное причальное устройство. Параметром, характеризующим надежность АНПА, как любого технического устройства, является вероятность его безотказной работы.

Надежность АНПА определяется в первую очередь надежностью перемещения АНПА из одной точки в другую, в том числе и в условиях возникновения препятствий. Сказанное означает, что при возникновении препятствия движение АНПА должно быть так организовано, чтобы не допустить столкновения. Препятствие может появиться внезапно, например, айсберг на пути следования АНПА.

Неизбежность столкновения может возникнуть из-за слишком близкого расстояния при обнаружении препятствия, когда АНПА не в состоянии выполнить маневр для обхода препятствия. В целях безопасности вокруг АНПА формируются зоны, в пределах которых АНПА может двигаться с допустимой скоростью [4]. Безусловно, такой подход обеспечивает безопасность, однако, надо полагать, что отчасти, поскольку:

— невозможно резко сбросить скорость при внезапном появлении препятствия; при построении зон вокруг препятствия необходимо учитывать также и возможности системы обнаружения препятствия, которые должны быть согласованы с маневренными характеристиками АНПА;

— невозможно резко сменить курс для выхода из «проблемной» зоны в зону более комфортного нахождения АНПА.

Сказанное означает, что при определенных условиях столкновение АНПА с препятствием может оказаться неизбежным. В связи с этим можно считать, что та СУ хороша, которая позволяет избежать столкновения с препятствием.

Если рассмотреть немультиагентные подходы (объектно-ориентированный, компонентно-ориентированный), то в силу ограниченности ресурса наряду с движением от точки к точке рассматривается лишь вариант обхода препятствия. В то же время при мультиагентном подходе, как отмечалось ранее, возможно наряду с агентом обхода препятствия выделить специально отдельного агента движения АНПА в условиях ограничений: алгоритм движения определяет положение АНПА ровно посередине между ограничениями. В этом случае, если обнаружено гидролокаторами бокового обзора ограничение, которое может затем перерасти в препятствие, АНПА находится посередине между боковыми ограничениями, и в момент проявления одного из них как препятствия вероятность столкновения гораздо меньше. Следует ожидать, что это приведет к повышению вероятности безотказной работы и надежности АНПА.

Поэтому для проведения исследований по оценке надежности АНПА следует предполагать, что в отсутствие осложняющих миссию факторов безопасности АНПА ничто не угрожает, и в такой ситуации АНПА будет надежна при любом подходе к построению архитектуры СУ АНПА. Другое дело, если АНПА оказывается в ситуации возникновения препятствия, причем внезапного, да еще в условиях ограничения слева и справа по борту.

Методика оценки надежности

Безотказность работы АНПА зависит от технических характеристик и технических решений АНПА, алгоритма его поведения, гидроакустических условий, т. е. вероятность безотказной работы АНПА можно представить в виде целевой функции, зависящей от времени t, которую необходимо максимизировать:

$$P_{\text{б.р}}(t) = f(\text{А, С, О, СОО}, H, E, t) \to \max,$$

где А — параметры АНПА (ходовые, акустические, алгоритмы поведения); С — параметры среды (гидрология, глубина моря, тип грунта, уровень волнения моря); О — параметры препятствия (параметры положения и движения); СОО — параметры системы освещения обстановки, обеспечивающие обнаружение препятствия; H — параметры навигации АНПА; E — характеристика аккумуляторной батареи АНПА; t — текущий момент времени.

Для расчета вероятности безотказной работы предлагается использовать метод статистических испытаний (метод Монте-Карло) [11].

Для реализации метода статистических испытаний проводится серия испытаний, в каждом из которых происходит воспроизведение тактического эпизода (ТЭ) со случайными значениями положения и размера препятствия. После воспроизведения ТЭ N раз (формула расчета N приведена ниже) с различными стартовыми параметра-

ми препятствия и параметрами его движения, т. е. после проведения так называемой серии испытаний, определяется вероятность безотказной работы $P_{б.р}(t)$ как отношение результативных испытаний $N_0(t)$ к общему количеству проведенных испытаний N:

$$P_{б.р}(t) = N_0(t)/N. \quad (1)$$

Результативность испытания $N_0(t)$ на момент времени t определяется отсутствием столкновения с препятствием к этому моменту. Работа АНПА в испытании считается безотказной, если не произошло столкновения АНПА с препятствием. Испытание считается завершенным, если АНПА не встретило на пути следования препятствия или его, в случае возникновения, удалось обойти.

Количество испытаний N в серии определяется исходя из ожидаемого значения вероятности $P_{б.р}(t)$ выполнения миссии:

$$N = t_\alpha^2 (P_{б.р}(t)(1 - P_{б.р}(t))/\varepsilon^2, \quad (2)$$

где t_α — коэффициент Стьюдента; ε — допустимое значение относительной ошибки.

Для проведения серии испытаний формируется цикл по испытаниям, в каждом из которых осуществляется воспроизведение ТЭ; количество испытаний определяется формулой (2).

В ходе проведения испытания, т. е. воспроизведения ТЭ, определяется результат преодоления препятствия G_i: $G_i = 1$ — препятствие удалось преодолеть или оно не появилось перед АНПА; $G_i = 0$ — произошло столкновение АНПА с препятствием. В пределах цикла по испытаниям происходит накопление результатов воспроизведения ТЭ:

$$N_0 = \sum_{i=1}^{N} G_i.$$

После завершения серии испытаний рассчитывается вероятность выполнения миссии $P_{б.р}(t)$ по формуле (1).

В каждом испытании воспроизводятся:

— движение АНПА;

— поведение АНПА, определяемое СУ АНПА.

Движение АНПА в общем случае моделируется как перемещение материальной точки: в каждом такте имитации вычисляются координаты ($X_{АНПА}$, $Y_{АНПА}$, $H_{АНПА}$) АНПА по формулам:

$$X_{АНПА} = X_{АНПА} + V_{АНПА}\Delta t\cos(Q_{АНПА});$$

$$Y_{АНПА} = Y_{АНПА} + V_{АНПА}\Delta t\sin(Q_{АНПА});$$

$$H_{АНПА} = H_{АНПА} + V_{АНПА}\Delta t\sin(\theta_{АНПА}),$$

где $V_{АНПА}$, $Q_{АНПА}$, $\theta_{АНПА}$ — скорость, курс и дифферент АНПА соответственно; Δt — длительность такта имитации.

Предполагается, что глубина положения АНПА на всем протяжении численного эксперимента была постоянна, поэтому в дальнейших расчетах не учитывается.

В имитационной модели учитываются разгон/торможение АНПА, в результате чего текущая скорость АНПА определяется выражением

$$V_{АНПА} = V_0 + a_i\Delta t,$$

где a_i — ускорение АНПА в i-м такте имитации.

Препятствие моделируется в виде круга радиуса R_p, начальное положение препятствия задается координатами положения центра круга (X_p, Y_p). Значения координаты Y_p распределены равновероятно в диапазоне, определяемом ТЭ. Движение препятствия определяется параметрами — курсом Q_p и скоростью V_p, и моделируется следующими выражениями:

$$X_p = X_p + V_p\Delta t\cos(Q_p);\ Y_p = Y_p + V_p\Delta t\sin(Q_p).$$

Положение ограничений, образующих коридор, моделируется кругами заданного радиуса R_1 и R_2 соответственно и координатами положения их центров (X_1, Y_1) и (X_2, Y_2).

Моделирование АНПА с немультиагентной и мультиагентной СУ

Моделирование АНПА с немультиагентной СУ. Текущее положение АНПА характеризуется парой координат (X_{nm}, Y_{nm}).

Для АНПА наличие ограничений никак не сказывается на изменении параметров его движения, поэтому расчет положения точки встречи АНПА с препятствием определяется выражением

$$\alpha_{nm} = \frac{\pi}{2} + \arcsin\left(\frac{Y_p - Y_{nm}}{R_p}\right).$$

Факт столкновения АНПА с препятствием определялся из условия

$$\sqrt{(X_{nm} - X_p)^2 + (Y_{nm} - Y_p)^2} < R_p^2.$$

Средний угол отворота АНПА по результатам серии испытаний определяется исходя из количества вероятных столкновений N_{nm}:

$$\alpha_{mid_{nm}} = \frac{\sum_{i=1}^{NM} |\alpha_{nm}|}{N_{nm}}.$$

Моделирование АНПА с мультиагентной СУ. Текущее положение АНПА характеризуется парой координат (X_{ma}, Y_{ma}).

Для АНПА определение факта столкновения с препятствием происходит по следующему алгоритму.

Координаты Y_{okr1} и Y_{okr2} бокового препятствия по левому и правому бортам АНПА определяются соответственно выражениями

$$Y_{okr_1} = \sqrt{R_1^2 - (X_{okr_1} - X_1)^2} + Y_1;$$

$$Y_{okr_2} = Y_2 - \sqrt{R_2^2 - (X_{okr_2} - X_2)^2}.$$

Поскольку для АНПА наличие ограничений слева и справа по борту оказывает влияние на положение АНПА, то координата Y_{ma} положения АНПА определяется по формуле

$$Y_{ma} = Y_{okr_1} + \frac{Y_{okr_2} - Y_{okr_1}}{2}.$$

Координата $Y_{в.п}$ возможного столкновения АНПА с препятствием определяется выражениями:

$Y_{в.п} = Y_p - \sqrt{R_p^2 - (X_{okr_1} - X_p)^2}$, если положение препятствия правее генерального направления движения АНПА;

$Y_{в.п} = \sqrt{R_p^2 - (X_{okr_1} - X_p)^2} + Y_p$, если положение препятствия левее генерального направления движения АНПА.

Поскольку предполагалось, что, воспринимая «внезапное» препятствие как боковое, АНПА сначала совершает маневр, чтобы оказаться посередине между боковыми препятствиями, то угол отворота для исключения столкновения с препятствием определяется из выражения

$$\alpha_{ma} = \frac{\pi}{2} + \arcsin\left(\frac{Y_p - Y_{ma}}{R_p}\right).$$

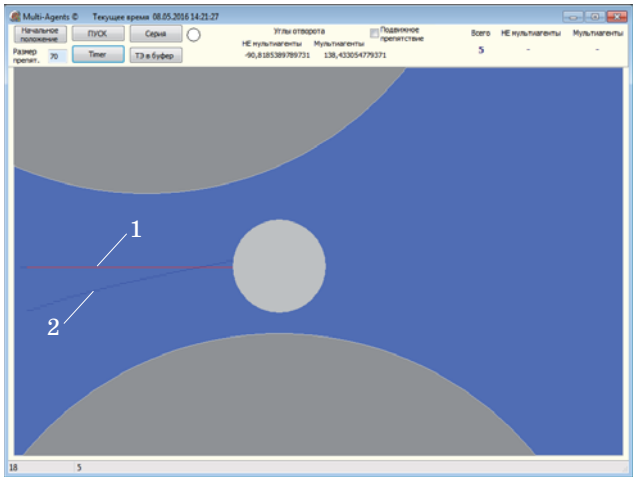
Признак столкновения АНПА с препятствием для мультиагентной СУ АНПА выражается условием

$$\sqrt{(X_{ma} - X_p)^2 + (Y_{ma} - Y_p)^2} < R_p^2,$$

где средний угол отворота АНПА по результатам серии испытаний определяется исходя из количества вероятных столкновений N_{ma}:

$$\alpha_{mid_{ma}} = \frac{\sum_{i=1}^{N_{ma}} |\alpha_{ma}|}{N_{ma}}.$$

Приведенные выражения легли в основу алгоритмов имитационной модели оценки надежности АНПА. Разработанная имитационная модель была программно реализована; вид окна программы Reliability (надежность) представлен на рис. 1. В верхней и нижней частях экрана отображаются положения боковых препятствий, образующие узкий «коридор». В «коридоре» находится «внезапно» появившееся препятствие, положение которого в каждом испытании разыгрывалось равновероятно. Линия *1* — траектория АНПА с немультиагентной СУ, не реагирующей на боковые ограничения; линия *2* — траектория перемещения АНПА с мультиагентной СУ, рассчитывающей положение АНПА посередине между препятствиями.



■ ***Рис. 1.*** Внешний вид окна программы Reliability

Тактический эпизод

Пусть АНПА совершает перемещение из точки старта в целевую точку, генеральное направление движения соответствует увеличению продольной координаты, т. е. слева направо. Маршрутная траектория АНПА проходит через коридор между двумя ограничениями, расположенными слева и справа по борту АНПА. Предполагается, что АНПА движется с максимально безопасной скоростью $V_{АНПА}$. Пусть в некоторый момент времени в коридоре между ограничениями внезапно появляется заранее непрогнозируемое препятствие произвольного размера и движется в произвольном направлении с произвольной скоростью.

Предполагается, что АНПА заранее неизвестны следующие параметры:

— размер препятствия;
— местоположение препятствия;
— плотность появления препятствий;
— частота появления препятствий;
— направление движения препятствия.

Размер и положение препятствия разыгрываются случайным образом равновероятно.

Обнаружение препятствия осуществляется СОО. Дальность обнаружения СОО зависит от скорости движения АНПА $V_{АНПА}$ и от характеристики окружающей среды. Успешность обхода препятствия без столкновения определяется положением АНПА в момент обнаружения препят-

ствия, его маневренными характеристиками и характеристиками самого препятствия.

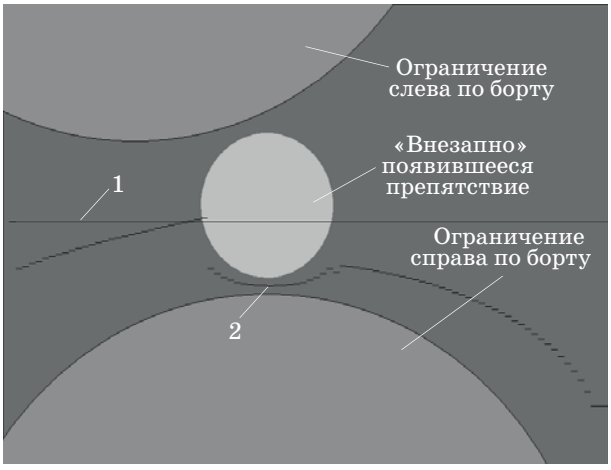
При формировании ТЭ рассматриваются различные варианты положения препятствия и его размеров. При возникновении перед АНПА препятствия происходит оценка угла отворота на текущей скорости, и если он не обеспечивается, то считается, что произошло столкновение АНПА с препятствием.

В ходе проведения численного эксперимента рассматривалось две тактики поведения АНПА в зависимости от организации его СУ (рис. 2):

— при немультиагентном подходе предполагалось, что в СУ АНПА предусмотрено только два вида движения: из точки в точку и обход препятствия, — в связи с чем АНПА не меняет параметров своего движения при появлении боковых ограничений, образующих коридор, если только эти ограничения не становятся препятствием, затрудняющим движение АНПА текущим курсом;

— в случае обнаружения боковых препятствий мультиагентной СУ АНПА держится постоянно посередине между ограничениями (рис. 2). В ходе эксперимента производился расчет углов отворота при обнаружении перед АНПА «внезапного» препятствия, и полученные значения сопоставлялись с допустимыми значениями для данной скорости движения. По результатам сравнительного анализа выявилось: если угол поворота не попадает в ограничение, то столкновение считается неизбежным; если попадет, АНПА сможет отвернуть и избежать столкновения.

Кроме того, принималось, что если препятствие слева от АНПА, то АНПА обходит его справа. Соответственно, если препятствие справа от АНПА, то АНПА обходит его слева. Учитывалось, что чем выше скорость, тем больше радиус циркуляции, с которым АНПА способен выполнить маневр отворота для исключения столкновения, и тем меньше угол, на который АНПА способен выполнить уклонение.



■ ***Рис. 2.*** Траектории перемещения АНПА с немультиагентной и мультиагентной СУ

Результаты численного эксперимента

При проведении численного эксперимента были использованы следующие исходные данные:

— положение «внезапного» препятствия разыгрывалось равновероятно из диапазона 150÷400 м по ширине между боковыми препятствиями. Положение «внезапного» препятствия по продольной оси между ограничениями принималось постоянным;

— размер «внезапного» препятствия изменялся путем перебора от 10 до 250 м;

— в каждой серии проводилось 1000 испытаний.

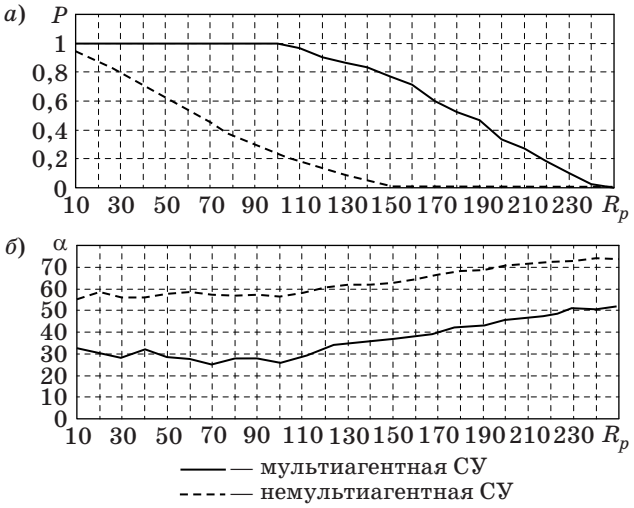
Обнаружение и положения боковых ограничений определялись только гидролокаторами бокового обзора.

В процессе проведения численного эксперимента при обнаружении «внезапного» препятствия по направлению движения АНПА регистрировался вариант возможного столкновения с ним. На рис. 2 линиями показаны траектории движения АНПА с немультиагентной (линия *1* проходит «сквозь» препятствие, что означает столкновение с ним) и мультиагентной СУ (линия *2*, огибающая препятствие). Кроме того, определялся угол, на который АНПА необходимо отвернуть, чтобы обогнуть препятствие и тем самым избежать столкновения с ним. В результате были получены предельные значения углов отворота для исключения столкновения. При этом о факте исключения столкновения можно говорить лишь с учетом скоростного режима движения АНПА.

При моделировании был рассмотрен случай равных исходных позиций «встречи» с препятствием АНПА с немультиагентной и мультиагентной СУ, когда к моменту встречи с препятствием положения обоих АНПА совпадали (см. рис. 1).

Рассмотрим результаты моделирования. На рис. 3, *а* приведены вероятности безотказной работы АНПА с немультиагентной и с мультиагентной СУ в зависимости от размера «внезапного» препятствия. На рис. 3, *б* приведены средние абсолютных значений углов отворота АНПА левого и правого борта для обеспечения обхода препятствия — также в зависимости от размера «внезапного» препятствия.

Значения вероятности безотказной работы АНПА с немультиагентной СУ определялись



■ ***Рис. 3.*** Результаты моделирования: зависимость вероятности безотказной работы (*а*) и необходимого угла поворота (*б*) от размера препятствия

в предположении, что АНПА не успевает отвернуть от препятствия, а для АНПА с мультиагентной СУ — в отсутствии ограничений на угол отворота. Поэтому для корректировки вероятности безотказной работы необходим учет ограничений на углы отворота в зависимости от скоростного режима АНПА. Если необходимый угол отворота для текущей скорости оказывается в заданных пределах, то принимается, что АНПА удалось избежать столкновения. Например, из рис. 3, *б* видно, что если отклонение не должно превышать 60°, то АНПА с мультиагентной СУ всегда успевает обогнуть препятствие, и вероятность безотказной работы нет необходимости корректировать. В то же время АНПА с немультиагентной СУ успевает отвернуть, но только от препятствий размером до 110 м. В этом случае вероятность безотказной работы АНПА при обходе препятствий до 110 м повышается до 1,0. Если ограничение на угол отворота составляет 30°, то АНПА с немультиагентной СУ не успеет отвернуть и столкнется с препятствием, поэтому вероятность безотказной работы АНПА не корректируется. В то же время АНПА с мультиагентной СУ сможет обогнуть препятствия, но размером только до 100 м, поэтому вероятность безотказной работы АНПА при обходе препятствий размером до 100 м не корректируется, а препятствий размером свыше 100 м — снижается.

Из рис. 3, *а* видно, что при движении АНПА посередине между ограничениями вероятность безотказной работы в среднем на 0,3 выше по сравнению с движением АНПА неизменным курсом. Различие по вероятности безотказной работы доходит иногда до 0,4. Это означает, что АНПА с мультиагентной СУ более надежен по сравнению с АНПА с немультиагентной СУ. Причина столь значительного преимущества заключается в том, что АНПА мгновенно повернуть не может, однако тактика нахождения АНПА между боковыми ограничениями способствует более благоприятному положению АНПА, в результате чего угол отворота оказывается меньше.

Приведенные на рис. 3 результаты не учитывают скоростного режима АНПА, в связи с чем нуждаются в корректировке в зависимости от скорости движения АНПА в момент обнаружения препятствия.

Результаты, приведенные на рис. 3, *б*, показывают преимущество надежности АНПА с мультиагентной СУ. При этом, как было отмечено выше, ТЭ был сформирован таким образом, что к моменту встречи с препятствием положение АНПА с немультиагентной СУ и с мультиагентной СУ совпадало. Очевидно, что во всех других случаях преимущество АНПА с мультиагентной СУ будет еще больше.

Заключение

Разработанные математическая модель и методика оценки надежности АНПА позволили провести количественную оценку надежности АНПА с мультиагентной СУ. Результаты исследований показали, что использование мультиагентного подхода к проектированию СУ повышает надежность АНПА по сравнению с «немультиагентным» подходом: вероятность безотказной работы АНПА повысилась в среднем на 0,3. Преимущество вызвано особенностями формирования мультиагентной системы, позволяющими, по сути, учитывать при принятии решения неограниченное количество различных вариантов отдельных процессов, в данном случае — вариантов движения. Любой немультиагентный подход допускает лишь ограниченное рассмотрение возможных вариантов, что приводит к учету лишь ограниченного количества факторов. В то же время мультиагентный подход позволяет учесть более тонкие особенности отдельно взятого процесса АНПА, что приводит к выработке более взвешенного и всестороннего решения. А это, в свою очередь, в условиях критических, нештатных и даже аварийных ситуаций позволяет выработать наиболее рациональное решение с учетом всех обстоятельств.

С точки зрения программной реализации мультиагентный подход также приводит к повышению надежности функционирования АНПА, поскольку выход из строя программы отдельно взятого агента-компонента не приведет к сбою всего программного обеспечения. При грамотной реализации мультиагентного подхода произой-

дет просто перераспределение функций между оставшимися агентами, что слабо скажется на надежности всей системы в целом. Кроме того, при мультиагентном подходе вместо отладки единой программы достаточно отладить по отдельности программы-агенты и наладить их взаимосвязи с другими агентами. Это удобно и в том случае, когда программное обеспечение разрабатывается разными независимыми разработчиками.

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект № 14-08-01006-а).

Литература

1. Автономные подводные роботы. Системы и технологии / под ред. М. Д. Агеева. — М.: Наука, 2005. — 398 с.
2. **Городецкий В. И., Грушинский М. С., Хабалов А. В.** Многоагентные системы (обзор) // Новости искусственного интеллекта. 1998. № 2. С. 64–116.
3. **Ржевский Г. А., Скобелев П. О.** Как управлять сложными системами? Мультиагентные технологии для создания интеллектуальных систем управления предприятиями. — Самара: Офорт, 2015. — 290 с.
4. **Innocenti B.** A Multi-Agent Architecture with Distributed Coordination for an Autonomous Robot. PhD. dissertation. — Universitat de Girona, 2009. — 146 p.
5. **Lei Zhang,** et al. An AUV for Ocean Exploring and its Motion Control System Architecture/ Lei Zhang, Dapeng Jiang, Jin-xin Zhao, Shan Ma // The Open Mechanical Engineering Journal. 2013. N 7. P. 40–47.
6. **Мартынова Л. А., Машошин А. И.** Построение системы управления автономных необитаемых подводных аппаратов на базе мультиагентной технологии // Известия ЮФУ. Технические науки. 2016. № 2. С. 38–48.
7. **Мартынова Л. А., Машошин А. И., Пашкевич И. В., Соколов А. И.** Система управления — наиболее сложная часть автономных необитаемых подводных аппаратов // Морская радиоэлектроника. 2015. № 4(54). С. 23–32.
8. **Мартынова Л. А., Машошин А. И., Пашкевич И. В., Соколов А. И.** Интегрированная система управления автономного необитаемого подводного аппарата // 8-я Всерос. мультиконференция по проблемам управления, Дивноморское, 28 сентября – 3 октября 2015 г. Т. 3. С. 191–193.
9. **Мартынова Л. А., Машошин А. И., Пашкевич И. В., Соколов А. И.** Алгоритмы, реализуемые интегрированной системой управления АНПА // Известия ЮФУ. Технические науки. 2015. № 1(162). С. 50–58.
10. **Benjamin M. R.** Interval Programming: A Multi-Objective Optimization Model for Autonomous Vehicle Control: Doctoral Dissertation. — Brown University Providence, RI, USA, 2002. — 130 p.
11. **Jackel P.** Monte Carlo Methods in Finance. — Willy, 2002. — 304 p.

UDC 626
doi:10.15217/issn1684-8853.2016.5.25

Reliability of an Autonomous Underwater Vehicle with a Multiagent Control System

Martynova L. A.[a], Dr. Sc., Tech., Senior Researcher, martynowa999@bk.ru
Rozengauz M. B.[a], PhD, Tech., Senior Researcher, rozengauz_mb@mail.ru
[a]State Research Center of the Russian Federation Concern CSRI Elektropribor, JSC, 30, Malaya Posadskaya St., 197046, Saint-Petersburg, Russian Federation

Introduction: Developing control systems for autonomous underwater vehicles often involves modern technologies, for example, the multiagent technology. Even though it has undeniable advantages and a lot of publications were devoted to it, the reliability of autonomous underwater vehicles with multiagent control system still needs to be evaluated. **Purpose:** We conduct a comparative analysis of the reliability of autonomous underwater vehicles with a multiagent control system and with other control systems. **Methods:** Our comparative analysis was focused on the probability of trouble-free operation of an autonomous underwater vehicle, calculated using a specially developed mathematical simulation model. **Results:** We have identified the specific features of multiagent control systems which involve taking into account a large number of factors when you have to make a decision in a contingency or emergency situation. A non-multiagent system allows you to consider only two types of movement: along the route path to the destination point, and around an obstacle. A multiagent system additionally considers movement under lateral restrictions. The simulation results have shown that when an autonomous underwater vehicle is moving under lateral restrictions, its trouble-free operation probability is 0.3 times higher compared to the vehicles with a non-multiagent control system.**Practical relevance:** The results of this study demonstrate that the reliability of an autonomous underwater vehicle is higher when you replace a non-multiagent control system by a multiagent control system. In the future, using the latter one is preferable.

Keywords — Autonomous Underwater Vehicle, Control System, Multiagent Technology, Simulation Model.

References

1. *Avtonomnye podvodnye roboty. Sistemy i tekhnologii* [The Autonomous Underwater Robots. Systems and Technology]. Ed. M. D. Ageev. Moscow, Nauka Publ., 2005. 398 p. (In Russian).
2. Gorodetskiy V. I., Grushinskiy M. S., Khabalov A. V. Multi-Agent Systems (review). *Novosti iskusstvennogo intellekta* [News of Artificial Intelligence], 1998, no. 2, pp. 64–116 (In Russian).
3. Rzhevskiy G. A., Skobelev P. O. *Kak upravliat' slozhnymi sistemami? Mul'tiagentnye tekhnologii dlia sozdaniia intellektual'nykh sistem upravleniia predpriiatiiami* [How to Manage Complex Systems? Multi-Agent Technology to Create Intelligent Business Management Systems]. Samara, Ofort Publ., 2015. 290 p. (In Russian).
4. Innocenti B. *A Multi-Agent Architecture with Distributed Coordination for an Autonomous Robot*. PhD Dissertation. Universitat de Girona, 2009. 146 p.
5. Lei Zhang, Da-peng Jiang, Jin-xin Zhao, Shan Ma. An AUV for Ocean Exploring and its Motion Control System Architecture. *The Open Mechanical Engineering Journal*, 2013, no. 7, pp. 40–47.
6. Martynova L. A., Mashoshin A. I. Formation of AUV Control System Based on Multi-Agent Technology. *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2016, no. 2 (175), pp. 38–48 (In Russian).
7. Martynova L. A., Mashoshin A. I., Pashkevich I. V., Sokolov A. I. Control System — the Most Difficult Part of the Autonomous Underwater Vehicle. *Morskaya radioelektronika* [Marine Electronics], 2015, no. 4 (54), pp. 23–32 (In Russian).
8. Martynova L. A., Mashoshin A. I., Pashkevich I. V., Sokolov A. I. Integrated Management System Autonomous Underwater Vehicle. *8-ia Vseros. mul'tikonferentsiia po problemam upravleniia* [Materials of the 8th All-Russian Multiconference Management]. Divnomorskoe, 2015, vol. 3, pp. 191–193 (In Russian).
9. Martynova L. A., Mashoshin A. I., Pashkevich I. V., Sokolov A. I. Algorithms Realized the Integrated Control System of AUV. *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, no. 1 (162), pp. 50–58 (In Russian).
10. Benjamin M. R. *Interval Programming: A Multi-Objective Optimization Model for Autonomous Vehicle Control*. Doctoral Dissertation. Brown University Providence, RI, USA, 2002. 130 p.
11. Jackel P. Monte Carlo Methods in Finance. Willy, 2002. 304 p.

Научный журнал
«ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ»
выходит каждые два месяца.

Стоимость годовой подписки (6 номеров) для подписчиков России — 4800 рублей,
для подписчиков стран СНГ — 5400 рублей, включая НДС 18%, таможенные и почтовые расходы.

Подписку на печатную версию журнала можно оформить в любом отделении связи по каталогу:
«Роспечать»: № 48060 — годовой индекс, № 15385 — полугодовой индекс,
а также через посредство подписных агентств:
«Северо-Западное агентство „Прессинформ“»
Санкт-Петербург, тел.: (812) 335-97-51, 337-23-05,
эл. почта: press@crp.spb.ru, zajavka@crp.spb.ru,
сайт: http://www.pinform.spb.ru
«МК-Периодика» (РФ + 90 стран)
Москва, тел.: (495) 681-91-37, 681-87-47,
эл. почта: export@periodicals.ru, сайт: http://www.periodicals.ru
«Информнаука» (РФ + ближнее и дальнее зарубежье)
Москва, тел.: (495) 787-38-73, эл. почта: informnauka3@yandex.ru,
сайт: http://www.informnauka.com
«Деловая пресса»
Москва, тел.: (495) 962-11-11, эл. почта: podpiska@delpress.ru,
сайт: http://delpress.ru/contacts.html
«Коммерсант-Курьер»
Казань, тел.: (843) 291-09-99, 291-09-47, эл. почта: kazan@komcur.ru,
сайт: http://www.komcur.ru/contacts/kazan/
«Урал-Пресс» (филиалы в 40 городах РФ)
Сайт: http://www.ural-press.ru
«Идея» (Украина)
Сайт: http://idea.com.ua
«BTL» (Узбекистан)
Сайт: http://btl.sk.uz/ru/cat17.html и др.

На электронную версию нашего журнала (все выпуски, годовая подписка, один выпуск, одна статья) вы можете подписаться на сайтах НЭБ: http://elibrary.ru;
РУКОНТ: http://www.rucont.ru; ИВИС: http://www.ivis.ru/

Полнотекстовые версии журнала за 2002–2015 гг.
в свободном доступе на сайте журнала (http://www.i-us.ru),
НЭБ (http://www.elibrary.ru)
и Киберленинки (http://cyberleninka.ru/
journal/n/informatsionno-upravlyayuschiesistemy).

УДК 681.518.3
doi:10.15217/issn1684-8853.2016.5.35

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТРУКТУРНО-ЛОГИЧЕСКОГО ПОДХОДА К МОДЕЛИРОВАНИЮ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ ФУНКЦИОНИРОВАНИЯ РАКЕТНО-КОСМИЧЕСКОЙ ТЕХНИКИ

В. В. Шмелев[а], *канд. техн. наук*
М. Ю. Охтилев[б], *доктор техн. наук, профессор*
[а]*Военно-космическая академия им. А. Ф. Можайского, Санкт-Петербург, РФ*
[б]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Введение: *качество управляющего алгоритма технологического процесса в предметной области функционирования ракетно-космической техники и обработки и анализа измерительной информации определяется не только результатами тестирования алгоритма, но и способом описания алгоритма. Простая и в то же время полностью адекватная предметной области модель технологического процесса является инструментом описания управляющего алгоритма, в значительной степени повышающим его качество. Одним из перспективных направлений в моделировании технологических процессов является применение структурно-логического подхода.* ***Цель:*** *классифицировать известные подходы к моделированию технологических процессов с учетом особенностей предметной области, выявить их достоинства и недостатки на примере практических внедрений.* ***Результаты:*** *с позиции классического определения динамической системы технологический процесс в предметной области в общем случае является нестационарным конечномерным нелинейным процессом с дискретным временем. На основе этого представлена классификация известных подходов к моделированию процессов по четырем группам: функциональной, алгебраической, темпоральной и структурной. Интерпретация подходов сопровождается показательными примерами их прикладной реализации в космической отрасли Российской Федерации с указанием достоинств и недостатков. Рекомендуется этапность выбора (создания) модели технологического процесса. Структурно-логический подход классифицирован как симбиоз комплексного, логико-алгебраического и логического подходов.* ***Практическая значимость:*** *полученные результаты целесообразно применять для повышения качества квалиметрии разрабатываемого читателями подхода к моделированию технологических процессов, для обоснования выбора среди известных подходов к моделированию технологических процессов, для определения актуальности и перспективности теоретических и практических исследований в области разработки и совершенствования специального программного обеспечения мониторинга технологических процессов в предметной области.*

Ключевые слова *— ракетно-космическая техника, моделирование технологических процессов, квалиметрия моделей, структурно-логический подход.*

Введение

При создании и эксплуатации современной ракетно-космической техники (РКТ) широко применяется вычислительная техника. Наиболее сложной и недостаточно формализованной является проблема автоматического (автоматизированного) управления технологическими процессами различного назначения: подготовкой и пуском ракеты-носителя в автоматизированном режиме, функционированием систем ракеты-носителя на активном участке траектории в автоматическом режиме, работой систем космического аппарата в автоматическом и автоматизированном режимах, обработкой и анализом измерительной информации по результатам испытаний и применения РКТ.

С позиций системного анализа управление можно рассматривать как совокупность циклических операций измерения, обработки и анализа результатов измерений, формирования и выдачи управляющих воздействий. Особенностью работы именно космической техники является тот факт, что зачастую управляющее воздействие не является одноактным действием. Автоматической (автоматизированной) системой управления формируется целый комплекс операций, направленный на достижение требуемого эффекта. Поэтому управляющее воздействие в данной предметной области можно назвать технологическим процессом, осуществляемым по управляющему алгоритму [1]. Управляющий алгоритм — это строгая последовательно-параллельная совокупность действий по переводу технического процесса из начального в конечное состояние с требуемым показателем качества. Практической реализацией алгоритма является программа — специальное программное обеспечение.

Сегодня проблема создания управляющих алгоритмов надлежащего качества в требуемые сроки перешла из плоскости сложности аппаратной реализации на борту в плоскость сложности программно-алгоритмической реализации. Это вызвано возрастанием многоаспектной сложности процессов функционирования РКТ и все расширяющейся реализацией алгоритмов управления

в цифровом виде в бортовых цифровых вычислительных машинах [2].

В основе управляющего алгоритма лежит модель управляемого технологического процесса. При этом конечная результативность управляющего воздействия в немалой степени зависит и от качества алгоритма, и от используемой модели технологического процесса. Например, процедура динамического программирования — это общепризнанный по эффективности алгоритм решения оптимизационной задачи. Однако использование аналитической модели (например, в виде системы уравнений) при описании алгоритма значительно затрудняет применение метода динамического программирования, а иногда делает его невозможным. Известно, что для применения такого метода лучше всего подходят логико-алгебраические модели [3].

Управляющий алгоритм для технологического процесса, с одной стороны, сам является информационным объектом, не имеющим физической (материальной) сущности. С другой стороны, в разработке современное алгоритмическое обеспечение технологических процессов является чрезвычайно сложным и трудоемким видом технических изделий. Поэтому использование совершенной модели, как можно более простой, но адекватной управляемому процессу, позволит значительно сократить трудозатраты и затраты других видов ресурсов при создании управляющих алгоритмов.

В статье предложена классификация известных подходов к моделированию технологических процессов с конкретными примерами прикладной реализации. Дополнительно к известным в классификации участвует разработанный авторами структурно-логический подход к моделированию технологических процессов в предметной области, подробно изложенный в работе [4].

Определение технологического процесса в предметной области как динамической системы

Для анализа существующих подходов к моделированию технологических процессов необходимо привести определение технологического процесса с учетом особенностей предметной области испытаний и применения РКТ. Рассматриваемый технологический процесс является динамической системой, поэтому целесообразно трансформировать классическое определение, приведенное в работе [5].

Технологическим процессом в общем случае называется кортеж

$$\Sigma = <T, X, U, \Omega, Y, \Lambda, \mu, \eta>, \qquad (1)$$

где:

— $T \subseteq R$ — упорядоченное множество моментов времени, на котором развивается технологический процесс. Следует отметить возможность развития процесса не только во времени — существуют так называемые событийные процессы. При этом в качестве элементов множества T используются имена событий (или их номера), линейно упорядоченные по порядку наступления;

— X — множество состояний процесса, каждое состояние — вектор значений характеристик процесса, например, степень выполнения, потребляемые ресурсы;

— U — множество значений входных (управляющих) воздействий на органы управления процессом;

— $\Omega = \{\omega : T \to U\}$ — набор функций входных воздействий, который можно определить как «временную программу» управления процессом;

— Y — множество выходных величин, используемых для наблюдения за состоянием процесса. Так как в явном виде наблюдать за состоянием процессов функционирования объектов РКТ в подавляющем большинстве случаев нельзя, то в общем случае $X \neq Y$;

— $\Lambda = \{\lambda : T \to Y\}$ — набор функций порождения выходных величин;

— $\mu : T \times T \times X \times \Omega \to X$ — переходная функция состояния процесса;

— $\eta : T \times X \to Y$ — выходное отображение, определяющее поток выходных величин и позволяющее однозначно сопоставить конкретному состоянию процесса конкретное значение выходной величины.

Классифицируем технологический процесс в предметной области.

Процесс будет стационарным в случае, если:

— Ω замкнуто относительно оператора сдвига $z^\tau : \omega \to \omega'$, определяемого соотношением $\omega'(t) = \omega(t + \tau)$, $\forall t$, $\tau \in T$, что означает повторяемость программы управления процессом;

— $\forall s \in T : \mu(t; \tau, x, \omega) = \mu(t + s; \tau + s, x, z^s\omega)$, что означает равенство переходной функции состояния процесса для моментов времени, отстоящих на некоторую величину, которую можно назвать периодом;

— отображение η не зависит от t, что означает единственность выходных величин процесса для одного и того же состояния процесса, даже в разные моменты времени.

Анализ технологических процессов функционирования систем РКТ позволяет сделать вывод о том, что в подавляющем большинстве такие процессы не являются стационарными. Несомненно, есть возможность ограничить T таким образом, что в выбранном интервале будут выполняться условия стационарности процесса. Однако это не позволит создать унифицированный методический инструмент моделирования

и ограничит совместимость моделей различных этапов функционирования РКТ.

Технологический процесс называется процессом с непрерывным временем, если $T = R$, и с дискретным, если $T = N$, где R и N — множество вещественных и натуральных чисел.

Причиной однозначного отнесения процессов в рассматриваемой области к дискретным процессам следует назвать принцип получения информации о состоянии технологического процесса, т. е. технической реализации отображения η. Для получения информации о технологическом процессе при испытаниях и применении РКТ создана система информационно-телеметрического обеспечения. Принцип сбора измерительной информации в данной системе заключается в формировании совокупности пар $<y, t>$, где y — измеренное значение выходной величины Y; t — момент времени измерения выходной величины Y, $t \in T$. Формирование указанных пар может осуществляться с постоянным периодом (называемым периодом опроса измерительной системы) в случае жесткого принципа сбора измерений или с непостоянным в случае адаптивного принципа сбора измерений.

Процесс называется конечномерным размерности $\dim\Sigma$, если X является конечномерным линейным пространством размерности $\dim X_{\Sigma}$. Процесс будет конечным, если X конечно.

Размерность элементов x множества X определяется суммарным количеством оцениваемых параметров состояния процесса. Очевидно, что указанное количество всегда может быть точно определено. Поэтому процесс конечномерный. На практике путем применения процедуры агрегирования (объединения близких по различным критериям состояний x множества X) обеспечивают конечность процесса. Процедура агрегирования заключается в введении интервалов на значения элементов множества X, в пределах которых различные по значениям x состояния объединяются в единое по фактической интерпретации агрегированное состояние. Примером является задание на параметры РКТ допусковых границ, отделяющих исправное состояние от неисправного.

Технологический процесс является линейным, если:

— X, U, Ω, Y и Λ являются векторными пространствами на произвольном поле K;

— отображение $\mu(t; \tau, \cdot, \cdot)$ является K-линейным для любых t и τ;

— отображение η является K-линейным для любых t.

Условие векторного характера пространств X, U, Ω, Y и Λ сомнению не подлежит вследствие конечномерности процесса, что было показано ранее. Однако остальные условия линейности отображений $\mu(t; \tau, \cdot, \cdot)$ и η являются на практике в общем случае невыполнимыми.

Технологический процесс является гладким, если:

— $T = R$;

— X и Ω являются топологическими пространствами;

— $\mu \in C^1(T \to X)$, т. е. переходная функция μ является некоторым дифференциальным уравнением.

Условие гладкости не выполняется вследствие ранее принятой дискретности технологических процессов функционирования РКТ.

Таким образом, технологический процесс испытаний и эксплуатации РКТ, обработки и анализа измерительной информации является нестационарным конечномерным конечным нелинейным процессом с дискретным временем.

Классификация известных подходов к моделированию технологических процессов

Рассмотрим основные подходы к моделированию процессов: проведем их классификацию, сформируем и определим признаки сравнения, приведем примеры прикладной реализации подходов. Классификацию подходов к моделированию приведем в виде древовидной структуры (рис. 1) [6, 7].

Целесообразно выделить четыре группы подходов.

Первая группа — *алгебраическая* — основана на описании взаимодействующих процессов. Здесь процессы строятся на базисе атомарных операций с помощью набора алгебраических операций. Слово «алгебра» означает, что используется алгебраический/аксиоматический подход для описания поведения процесса. Алгебра процессов — это любая математическая структура, удовлетворяющая системе аксиом, описывающих требуемые свойства основных операторов. «Операция» в таком случае рассматривается как базовый элемент алгебры процессов.

Группа, объединяющая математические подходы, названа *функциональной*. В основе подходов данной группы находится преимущественное применение математических формализмов — функциональных зависимостей, определяющих текущее состояние моделируемого процесса как функции от аргументов различного рода. В качестве аргументов могут выступать время, ресурсы и другие величины. При этом может конструироваться целая система уравнений различной сложности.

Третья группа — это группа подходов, основанных на *темпоральной* (временно́й, событийной, пошаговой) логике. При этом в качестве

■ ***Рис. 1.*** Классификация подходов к моделированию процессов

модели процесса используется конечная система переходов. В качестве интерпретации процесса в этом случае применяется формула темпоральной логики линейного или ветвящегося времени (кортежа событий для событийных процессов).

При необходимости представления не траектории процесса, а смысловой причинно-следственной связи между операциями процесса используются подходы *структурной* группы.

Материальные подходы, позволяющие создать материальные (реальные) модели, не являются предметом рассмотрения в данной статье. Идеальные (абстрактные) подходы достаточно условно можно разделить по типам на формализованные и неформализованные (вербальные). В приведенных далее примерах подходов отдельные стороны содержания можно рассматривать и как систему традиционных математических представлений (**формализованный** тип), и как совокупность вербальных выражений на некотором языке (**неформализованный** тип).

Примерами ***простейшего знакового*** подхода к моделированию технологических процессов являются таблицы хронометража, диаграммы Ганта, технологические графики. Данный способ основан на простейших математических выражениях — системе рекурсивных функций. В работе [4] показано, что такой способ обладает крайне ограниченной моделирующей мощностью.

Сложные знаковые подходы могут быть разделены на алгебраические, в которых используются конструкции математической логики (алгебры) или языковые конструкции (лингвистика) и математические, в которых используются только традиционные математические представления.

К *алгебраической* группе можно отнести следующие подходы.

Логико-алгебраический подход оперирует термами процесса (этапами или состояниями процесса) и элементарными операциями (логическим сложением, умножением, отрицанием). Элементарной операцией может являться функция перехода, не имеющая математической интерпретации и определяющая детерминированную смену значения состояния процесса. Обобщенными примерами моделей, созданных в соответствии с логико-алгебраическим подходом, можно назвать конеч-

ные автоматы, сети Петри с их модификациями: G-сети [8], ВРС-сети (сети временных расстановок событий) [9], триады [10].

Инструмент конечных автоматов в практике представления технологических процессов функционирования РКТ встречает затруднения вследствие использования идеологии состояний, а не переходов, что при многообразии и многовариантности состояний технологических процессов слишком ресурсоемко.

Сети Петри и их модификации показали хорошую применимость для рассматриваемой предметной области. Примером успешного практического применения логико-алгебраического подхода (а именно G-сетей) является система анализа измерительной информации в автоматизированной системе управления подготовкой и пуском ракеты-носителя «Союз-2», развернутой, в частности, на космодроме «Плесецк» [2].

Логико-лингвистический подход [6] основан на конструкции формальных языков, состоящей из терминальных элементов, правил вывода и нетерминальных элементов. В этом случае технологический процесс описывается с помощью множества переменных высказываний {операция X выполняется, приостановлена, окончена и другие варианты состояния операции}, являющихся терминальными элементами, из которых составляются предложения о текущем состоянии процесса. Развитие процесса в этом случае описывается правилами вывода, определение текущего состояния — процедурой грамматического разбора информационных предложений. На основе логико-лингвистического подхода было создано унифицированное программное обеспечение автоматизированного анализа технического состояния РКТ «Байкал» [6]. Однако подобные модели нашли только ограниченное применение в рассматриваемой предметной области вследствие сложности интерпретации результатов вывода, т. е. получения новой информации и ее сопоставления с реальным состоянием моделируемого процесса.

Математические подходы следует разделить на аналитический, имитационный и комбинированный (аналитико-имитационный или комплексный).

Модель, созданная с помощью аналитического подхода, охватывает определенный аспект моделируемого технологического процесса посредством тех или иных математических конструкций (функций, функционалов, алгебраических или дифференциальных уравнений и т. д.). Такая модель позволяет получить конечные характеристики процесса (степень выполнения, затраченные ресурсы и т. п.) в виде некоторых формальных соотношений для количественного или качественного анализа. Показательными представителями аналитических моделей технологических процессов можно назвать модели непрерывной системной динамики, в частности на основе дифференциальных уравнений в той или иной форме [7]. В таких уравнениях в левой части находится переменная, отражающая какую-либо характеристику технологического процесса. В правой части представляется математическое выражение, содержащее аргументы времени, ресурса и т. д.

Достоинством аналитической модели является ее строгость и точность, позволяющие уточнить состояние процесса в любой момент, но только в случае достаточной адекватности модели реальному процессу. Недостатком такого способа моделирования технологических процессов следует назвать трудность представления логических взаимосвязей между операциями. Кроме того, недостаточно адекватно возможно передать особенности дискретного течения моделируемого процесса.

Имитационный подход к моделированию имеет распространение в области исследований технологических процессов [11]. Он применяется, когда есть необходимость идентифицировать поведение процесса при изменяющихся условиях. В своей сути имитационный подход содержит этап построения концептуальной (вербальной) модели процесса, этап алгоритмического описания последовательности элементарных или агрегированных операций и этап имитационных экспериментов, при проведении которых вносятся возмущения в условия выполнения процесса. Примером имитационной модели технологического процесса можно назвать многоразовое выполнение фрагмента (упрощенной) аналитической модели в рассмотренной ранее постановке. При этом в правой части уравнения состояния технологического процесса вводится переменная, определяемая факторами неопределенности с соответствующими статистическими характеристиками.

Основным достоинством имитационного подхода является возможность отражения адекватным образом несложной логики развития технологического процесса. Недостатком имитационного подхода является сложность интерпретации получаемых результатов или сложность придания фундаментальности выводам, которые значительно уступают фундаментальности выводов, получаемых при использовании аналитического подхода.

Для преодоления недостатков аналитического и имитационного подходов к моделированию широко развивается аналитико-имитационный или комплексный подход [12]. Отличительной особенностью такого подхода является введение типовой аналитической модели, представляющей

собой модель (сеть моделей), получившую определенную теоретическую проработку и обладающую достаточной степенью общности или универсальности. Введение подобных моделей позволяет, с одной стороны, унифицировать процесс построения алгоритмической имитационной модели, с другой стороны, получить фундаментальные результаты аналитической модели.

Представителей комплексного подхода к моделированию в настоящее время огромное количество. При рассмотрении методов комплексного моделирования принято говорить [13] об агрегатных моделях Бусленко Н. П., непрерывно-дискретных моделях Глушко В. М. и гибридных моделях. Однако, во-первых, показано [13], что данные модели приводятся друг к другу. Во-вторых, эти модели не являются в чистом виде самодостаточными, они определяют принцип глобального описания динамической системы или технологического процесса. Для прикладного применения таких моделей необходимо использовать соответствующие подмодели: в модели Бусленко — подмодель агрегата, в модели Глушко — подмодель процесса, в гибридной модели — подмодель гибридного автомата, чаще всего сетевого типа. Поэтому использовать такие модели в виде отдельных типов для классификации не следует, необходимо рассматривать их прикладные реализации.

Выделяются дискретные модели с сетевой структурой (прикладные разработки, например, в работах [8–10]), комплексные непрерывные модели системной динамики [14]. Все данные типы моделей объединяет использование некоторого унифицированного элемента (возможно, множества элементов), на основе композиции которых и создается искомая модель процесса. Достоинства и недостатки комплексных моделей в значительной степени определяются характеристиками унифицированного элемента.

Так, комплексные модели системной динамики в своей основе используют элементарные конечно-разностные или дифференциальные уравнения, связываемые между собой и образующие своеобразную динамическую сеть. Поэтому основным недостатком таких моделей является ограниченность моделирующей мощности. Достоинства же соответствуют достоинствам аналитических моделей.

Несмотря на то, что модели с сетевой структурой ранее уже относились к моделям, созданным в соответствии с логико-алгебраическим подходом, сетевые структуры возможно представить и в группе комплексного подхода при их рассмотрении с позиции использования технологии агентов. Данная технология подразумевает составление из конструктива сетевой структуры некоторого более крупного объекта, обладающего синергетическими свойствами, отсутствующими у элементов конструктива. Подобная технология реализуется достаточно просто именно с помощью моделей с сетевой структурой. Широкое прикладное применение такого подхода в системах комплексного (хотя и называемого в описаниях имитационного) моделирования доказывает его хорошую практическую направленность. Распространенными средами комплексного моделирования с CASE-средствами следует назвать AnyLogic, GPSS World, Rand Model Desinger.

Дискретные модели с сетевой структурой представляются наиболее результативными для использования в предметной области функционирования РКТ. Достоинствами моделей с сетевой структурой следует назвать наиболее полное соответствие типу моделируемых процессов. Очевидно, что дискретность и конечномерность модели уже лежат в основе сетевых моделей, состоящих из отдельных элементов (вершин и дуг). Множество возможных вариантов дуг и вершин реализуют нелинейность и нестационарность процесса.

Однако такие модели имеют и недостатки. Они заключаются в необходимости агрегирования, в общем случае, бесконечного числа состояний любого процесса, т. е. приведения его к конечному виду. Иначе громоздкость модели затмит все достоинства. Кроме того, существующие сетевые модели требуют особой доработки при важности учета времени.

Основным предназначением **неформализованного** (вербального) подхода является первоначальное изучение моделируемого процесса в целях дальнейшего, более качественного моделирования с использованием уже формализованной модели. И в отдельном виде вербальный подход не применим для установления показателей свойств моделируемого процесса. Кроме того, возможным является одновременная классификация подхода и среди сложных знаковых типов, и среди вербальных типов. Подобная одновременная классификация позволит более глубоко выяснить предназначение и особенности того или иного подхода к моделированию.

Неформализованные подходы следует разделить на ***концептуальные*** и ***неструктурированные*** на естественном языке. Предназначение последних — предварительное представление моделируемого процесса в виде мысленной модели. Задача концептуальных — первоначальное представление процесса, на котором следует остановиться подробнее и привести примеры использования в предметной области.

Концептуальный подход позволяет создать модель, отражающую с необходимой полнотой процесс-прототип в том или ином содержательном

его аспекте и записанную на естественном языке с использованием наивной логики. Различают дескриптивный и прескриптивный подходы к моделированию. *Дескриптивный* концептуальный подход создает модели описательного характера, *прескриптивный* концептуальный — модели нормативного, более строгого характера.

Результатом применения дескриптивного концептуального подхода можно назвать онтологическую модель, в соответствии с которой технологический процесс представляется в структурированном иерархическом виде классов и экземпляров классов, среди прикладных разработок можно назвать среду МИВАР. В предметной области онтологическая модель используется в системе комплексного анализа результатов применения космической техники на космодроме «Плесецк». Для удобства представления моделируемых процессов создана иерархия процесса функционирования ракеты-носителя по структуре: класс — экземпляр класса. Классы не являются одноранговыми элементами. Такой подход является удобным не для контроля и управления процессом, а для хранения больших объемов информации.

Еще одним примером дескриптивного подхода можно назвать представление процессов с помощью теоретико-множественных кортежей. В этом случае технологический процесс сопоставляется кортежу множеств и отношений. При этом множества содержат агрегированные состояния технологического процесса, характерные признаки состояний, а отношения определяют условия перехода процесса из одного состояния в другое. Примером можно назвать [15] модель процесса диагностирования технической системы, состоящую из σ-алгебры фазовых состояний процесса диагностирования, множества диагностических признаков и множества интервалов диагностических признаков, определяющих каждый искомый результат. Такая модель нашла достаточно широкое распространение у А. К. Дмитриева и его учеников для представления процессов анализа телеметрической информации в ракетно-космической отрасли.

Достоинством представления процесса с помощью теоретико-множественного кортежа, на первый взгляд, можно назвать обширнейшую моделирующую мощность. Однако это на самом деле является главным недостатком подхода. Так как практическое применение такого подхода к реальным технологическим процессам сталкивается с лавинообразным увеличением мощности множеств, превышающим вычислительные возможности ЭВМ. Поэтому теоретико-множественную модель целесообразно использовать лишь как вспомогательную или, как уже говорилось, предварительную модель.

Прескриптивные подходы можно разделить на характеристический и логический. Характеристический подход — это достаточно строгий способ описания не траектории развития процесса, а структуры его характеристик, целей, функций или задач. Прескриптивный логический подход позволяет получать менее формализованные варианты сетевых структур.

Примерами использования характеристического подхода являются дерево целей и задач и дерево показателей [7]. Дерево целей и задач — это нисходящий древесный граф: вершины вышестоящего уровня по отношению к вершинам нижестоящего уровня рассматриваются как цели, вершины нижестоящего уровня по отношению к вершинам вышестоящего уровня рассматриваются как задачи, которые необходимо решить для достижения этих целей. Множественность и иерархическая упорядоченность целей и задач, выполняемых процессом, предопределяет необходимость использования при оценивании его эффективности векторных показателей. Для систематизации показателей используется соответствующее дерево, где каждая вершина характеризует степень либо качество выполнения соответствующих частных задач или достижения поставленных целей.

Логические прескриптивные подходы формируют модели, использующие графовый аппарат, однако без математических формализмов. Примером такой модели можно назвать циклограмму логического функционирования бортовой аппаратуры ракеты-носителя, фрагмент которой показан на рис. 2.

Такие модели всегда являются совокупностью графических элементов, которую в общем случае можно назвать N-дольным ориентированным графом. Дольность графа определяется количеством типов вершин. В циклограммах логического функционирования бортовых систем обычно вершины двух типов, одна из которых обозначает моменты ввода внешней информации (управляющих воздействий), вторая определяет состояния бортовой системы. Дуги определяют направление развития процесса функционирования.

Представленные структуры (и характеристические, и логические) являются вспомогательными инструментами для более эффективного выбора основного подхода к моделированию технологического процесса из группы сложных знаковых.

На основе приведенного определения технологического процесса испытаний и эксплуатации РКТ, обработки и анализа измерительной информации можно предложить следующую этапность создания модели процесса.

1. На первом этапе необходимо создать предварительную модель технологического процесса с помощью, например, теоретико-множественного

■ ***Рис. 2.*** Циклограмма логического функционирования бортовой системы ракеты-носителя (фрагмент)

подхода. Такой подход хорошо адаптируется для моделирования нестационарных, нелинейных процессов с дискретным временем, так как множества и отношения между ними требуют минимума математических формализмов.

2. С целью обеспечить прикладной характер формируемой модели процесса необходимо построить дерево целей и задач моделируемого процесса, а также дерево показателей эффективности данного процесса.

3. Затем в целях восстановления логических этапов выполнения процесса следует создать, например, циклограмму логического функционирования технологического процесса испытаний и эксплуатации РКТ, обработки и анализа измерительной информации. При этом необходимо использовать графовый аппарат.

4. На заключительном этапе среди сложных знаковых подходов следует выбрать симбиоз математических и алгебраических подходов, содержащий максимальное число положительных сторон составляющих.

Это является только указанием направления поиска требуемого подхода к моделированию. Для уточнения подхода необходимо провести квалиметрию моделей, формируемых сложными знаковыми подходами.

Приведенная классификация подходов к моделированию технологических процессов в предметной области не должна считаться исключительной. В классификации представлены только основные общеизвестные способы и подходы. Кроме того, как уже говорилось, но вследствие важности замечания целесообразно еще раз отметить, что наиболее эффективное применение подходов требует их симбиоза.

Именно поэтому, не останавливаясь на содержимом (при необходимости см. работу [4]), структурно-логический подход следует классифицировать как симбиоз:

— комплексного подхода благодаря применению агентного принципа моделирования процессов;

— логико-алгебраического подхода благодаря использованию сетевой структуры на основе модифицированной сети Петри в качестве агента;

— логического подхода благодаря реализации в том числе графического аппарата представления траектории развития процесса.

Заключение

Задача высокоэффективного автоматического и в определенной степени автоматизированного управления технологическими процессами в предметной области функционирования РКТ, обработки и анализа измерительной информации является чрезвычайно важной. В основе управления без участия оператора находится управляющий алгоритм как последовательность управляющих воздействий на объект управления. Описание алгоритма заключается в формировании условий применения воздействий с помощью специального инструмента. Данный инструмент использует модель технологического процесса или объекта управления. Таким образом, эффективность управления зависит от качества модели технологического процесса. В данном случае под качеством модели понимается степень учета моделью всех особенностей моделируемого технологического процесса в предметной области.

В целях обоснованной классификации применимых подходов к моделированию технологический процесс испытаний и эксплуатации РКТ, обработки и анализа измерительной информации определен как нестационарный конечномерный

конечный нелинейный процесс с дискретным временем.

Широкий обзор известных подходов из теории моделирования позволил разделить подходы к моделированию технологических процессов на четыре группы: функциональную, алгебраическую, темпоральную и структурную. В данной статье рассмотрены основные представители групп.

Изложенный материал предназначен для классификации предложенного авторами структурно-логического подхода среди известных методов моделирования технологических процессов в рассматриваемой предметной области. На основании приведенной классификации подходов определена принадлежность разработанного структурно-логического подхода как симбиоза комплексного, логико-алгебраического и логического подходов.

Результаты могут быть использованы для:

— проведения квалиметрии разрабатываемого читателями подхода к моделированию технологических процессов;

— определения среди известных подходов наиболее пригодного для конкретного практического применения;

— определения актуальности и перспективности теоретических и практических исследований в области разработки и совершенствования специального программного обеспечения мониторинга технологических процессов.

Литература

1. **Калентьев А. А., Тюгашев А. А.** ИПИ/CALS технологии в жизненном цикле комплексных программ управления. — Самара: Изд-во Самарского научного центра РАН, 2006. — 285 с.
2. **Майданович О. В.** и др. Теория и практика построения автоматизированных систем мониторинга технического состояния космических средств / О. В. Майданович, В. А. Каргин, В. В. Мышко, М. Ю. Охтилев, Б. В. Соколов; под ред. О. В. Майдановича: монография. — СПб.: ВКА им. А. Ф. Можайского, 2011. — 219 с.
3. **Черноусько Ф. Л.** Динамическое программирование // Соросовский образовательный журнал. 1998. № 2. С. 139–144.
4. **Шмелев В. В.** Модели технологических процессов функционирования космических средств // Авиакосмическое приборостроение. 2015. № 4. С. 78–93.
5. **Kalman R. E., Falb P. L., Arbib M. A.** Topics in Mathematical System Theory. — N. Y.: McGraw-Hill, 1969. — 358 p.
6. **Мальцев В. Б.** Анализ состояния технических систем. — М.: МО РФ, 1993. — 181 с.
7. **Мануйлов Ю. С., Павлов А. Н., Новиков Е. А.** Системный анализ и организация автоматизированного управления космическими аппаратами / под общ. ред. Ю. С. Мануйлова. — СПб.: ВКА им. А. Ф. Можайского, 2010. — 266 с.
8. **Охтилев М. Ю.** Основы теории автоматизированного анализа измерительной информации в реальном времени. Синтез системы анализа: монография. — СПб.: ВКА им. А. Ф. Можайского, 1999. — 162 с.
9. **Рышков Ю. П., Охтилев М. Ю., Богомолов С. Е.** Актуальные вопросы автоматизированной обработки и анализа информационных процессов. — М.: МО РФ, 1992. — 140 с.
10. **Юдицкий С. А.** Моделирование динамики многоагентных триадных сетей. — М.: СИНТЕГ, 2012. — 112 с.
11. **Плотников А. М., Рыжиков Ю. И., Соколов Б. В.** Современное состояние и тенденции развития имитационного моделирования в Российской Федерации // Имитационное моделирование. Теория и практика. ИММОД-2011, Санкт-Петербург, 19–21 октября 2011 г.: в 2 т. — СПб.: ФГУП «ЦНИИТС», 2011. Т. 1. С. 51–61.
12. **Калинин В. Н, Соколов Б. В.** Многомодельный подход к описанию процессов управления космическими средствами // Теория и системы управления. 1995. № 1. С. 149–156.
13. **Парийская Е. Ю.** Сравнительный анализ математических моделей и подходов к моделированию и анализу непрерывно-дискретных систем // Дифференциальные уравнения и процессы управления. 1997. № 1. http://www.math.spbu.ru/diffjournal/RU/numbers/1997.1/article.1.4.html (дата обращения: 20.07.2016).
14. **Павловский Ю. Н.** Декомпозиция моделей управляемых систем. — М.: Знание, 1985. — 32 с.
15. **Дмитриев А. К., Кравченко И. Д.** Модель процесса диагностирования технического объекта при использовании непрерывных диагностических признаков // Изв. вузов. Приборостроение. 1994. Т. 37. № 11–12. С. 3–9.

UDC 681.518.3
doi:10.15217/issn1684-8853.2016.5.35

Comparative Analysis of Structural and Logical Approach to Rocket and Space Technology Modeling

Shmelev V. V.[a], PhD., Tech., Doctoral Candidate, valja1978@yandex.ru
Okhtilev M. Yu.[b], Dr. Sc., Tech., Professor, oxt@mail.ru
[a]A. F. Mozhaiskii Military Space Academy, 13, Zhdanovskaia St., 197198, Saint-Petersburg, Russian Federation
[b]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: The quality of technology control algorithms in rocket and space technology, as well as processing and analysis of measurement data, is determined not only by the results of testing the algorithms but also by the way they are specified. A simple model of the technological process which is at the same time fully adequate to the domain is a tool to describe the control algorithm, greatly increasing its quality. One of the promising directions in the modeling of processes is using the structural and logical approach. **Purpose:** The goal is to classify the known approaches to technological process modeling, taking into account the specific features of the domain, and to identify their strengths and weaknesses using practical implementation examples. **Results:** From the perspective of the classical definition of a dynamic system, a technological process in a domain is generally a time-dependent nonlinear finite process with discrete time. On this base, the known approaches to process modeling are classified into four groups: functional, algebraic, temporal and structural. These approaches are interpreted with references to illustrative examples of their application in Russian space industry, indicating their advantages and disadvantages. It is recommended to choose or create a technological process model step by step. The structural and logical approach is defined as a combination of the complex, logical-algebraic and logical approaches. **Practical relevance:** The obtained results can be used to improve the qualimetry of the technological process modeling approach developed by the readers, in order to substantiate the choice among the known approaches to the modeling, and to check the relevance and prospects of theoretical and practical research on the development of special software in this field.

Keywords — Rocket and Space Technology, Modeling of Technological Processes, Qualimetry of Models, Structural and Logical Approach.

References

1. Kalent'ev A. A., Tiugashev A. A. *IPI/CALS tekhnologii v zhiznennom tsikle kompleksnykh program upravleniia* [CALS Technologies in the Life Cycle Management of Complex Programs]. Samara, Samarskii nauchnyi tsentr RAN Publ., 2006. 285 p. (In Russian).
2. Maidanovich O. V., Kargin V. A., Myshko V. V., Okhtilev M. Yu., Sokolov B. V. *Teoriia i praktika postroeniia avtomatizirovannykh system monitoringa tekhnicheskogo sostoianiia kosmicheskikh sredstv* [The Theory and Practice of Construction of Automated Systems for Monitoring the Technical Condition of Space Vehicles]. Saint-Petersburg, 2011. 219 p. (In Russian).
3. Chernous'ko F. L. Dynamic Programming. *Sorosovskii obrazovatel'nyi zhurnal*, 1998, no. 2, pp. 139–144 (In Russian).
4. Shmelev V. V. Models of Processes of Functioning of Space Assets. *Aviakosmicheskoe priborostroenie*, 2015, no. 4, pp. 78–93 (In Russian).
5. Kalman R. E., Falb P. L., Arbib M. A. *Topics in Mathematical System Theory*. New York, McGraw-Hill, 1969. 358 p.
6. Mal'tsev V. B. *Analiz sostoianiia tekhnicheskikh sistem* [Analysis of the Technical Systems]. Moscow, Ministerstvo oborony Rossiiskoi Federatsii Publ., 1993. 181 p. (In Russian).
7. Manuilov Iu. S., Pavlov A. N., Novikov E. A. *Sistemnyi analiz i organizatsiia avtomatizirovannog oupravleniia kosmicheskimi apparatami* [Systems Analysis and Organization of Automated Spacecraft Control]. Saint-Petersburg, VKA im. A. F. Mozhaiskogo Publ, 2010. 266 p. (In Russian).
8. Okhtilev M. Yu. *Osnovy teorii avtomatizirovannogo analiza izmeritel'noi informatsii v real'nom vremeni. Sintez sistemy analiza* [Basic Theory of the Automated Analysis of the Measuring Data in Real Time. Synthesis Analysis]. Saint-Petersburg, VKA im. A.F. Mozhaiskogo Publ., 1999. 162 p. (In Russian).
9. Ryshkov Iu. P., Okhtilev M. Iu., Bogomolov S. E. *Aktual'nye voprosy avtomatizirovannoi obrabotki i analiza informatsionnykh protsessov* [Topical Issues of the Automated Processing and Analysis of Information Processes]. Moscow, Ministerstvo oborony Rossiiskoi Federatsii Publ., 1992. 140 p. (In Russian).
10. Iuditskii S. A. *Modelirovanie dinamiki mnogoagentnykh triadnykh setei* [Modeling the Dynamics of Multi-Agent Network Triad]. Moscow, SINTEG Publ., 2012. 112 p. (In Russian).
11. Plotnikov A. M., Ryzhikov Iu. I., Sokolov B. V. Current Status and Development Trend of the Simulation in the Russian Federation. *Trudy 5-i Vserossiiskoi nauchno-prakticheskoi konferentsii po imitatsionnomu modelirovaniiu i ego primeneniiu v nauke i promyshlennosti "Imitatsionnoe modelirovanie. Teoriia i praktika" IMMOD-2011* [Proc. of the 5th All-Russian Scientific-Practical Conference on Imitation-Onnomu Modeling and its Application in Science and Industry "Simulation. Theory and Practice"]. Saint-Petersburg, 2011, vol. 1, pp. 51–61 (In Russian).
12. Kalinin V. N., Sokolov B. V. The Multi-Model Approach to Describing Space Means Control Processes. *Teoriia i sistemy upravleniia*, 1995, no. 1, pp. 149–156 (In Russian).
13. Pariiskaia E. Iu. Comparative Analysis of Mathematical Models and Approaches to Modeling and Analysis of Discrete-Continuous Systems. *Differentsial'nye uravneniia i protsessy upravleniia*, 1997, no. 1. Available at: http://www.math.spbu.ru/diffjournal/RU/numbers/1997.1/article.1.4.html. (accessed 10 July 2016). (In Russian).
14. Pavlovskii Iu. N. *Dekompozitsiia modelei upravliaemykh system* [Decomposition Models of Control Systems]. Moscow, Znanie Publ., 1985. 32 p. (In Russian).
15. Dmitriev A. K., Kravchenko I. D. The Technical Object Process Model Diagnosis Using Continuous Diagnostic Features. *Izvestiia vuzov. Priborostroenie*, 1994, vol. 37, no. 11–12, pp. 3–9 (In Russian).

УДК 621.31:658.58:004.89
doi:10.15217/issn1684-8853.2016.5.45

ИНТЕЛЛЕКТУАЛЬНЫЕ МОДЕЛИ КОМПЛЕКСНОЙ ОЦЕНКИ ТЕХНИЧЕСКОГО СОСТОЯНИЯ ВЫСОКОВОЛЬТНЫХ ВЫКЛЮЧАТЕЛЕЙ

Д. К. Елтышев[a], *канд. техн. наук, доцент*
[a]*Пермский национальный исследовательский политехнический университет, Пермь, РФ*

Постановка проблемы: *оперативное обнаружение и устранение дефектов высоковольтных выключателей и другого электротехнического оборудования, особенно при его значительном износе, является важной задачей обеспечения надежности систем электроснабжения. Многофакторность процессов эксплуатации выключателей накладывает существенные ограничения на выбор способов контроля их состояния, когда имеющаяся информация зачастую является неполной и неоднозначной. Один из вариантов решения проблемы — использование интеллектуальных информационных технологий.* ***Методы:*** *построение иерархически структурированной базы знаний на основе нечетких импликативных правил, имитирующих мышление электротехнического персонала, оценивающего состояние выключателя и его элементов.* ***Результаты:*** *разработан метод оценки состояния высоковольтных выключателей по результатам мониторинга с использованием формализованных экспертных знаний для интеллектуального анализа полученных данных. Метод основан на выборе и структурной декомпозиции параметров оборудования, измеряемых без его отключения от питающей сети и определяющих состав переменных нечеткой иерархической модели. Сущность метода заключается в пошаговом определении уровня критичности состояния выключателя, его элементов и формировании обоснованных управляющих воздействий по поддержанию работоспособности. Особенностью подхода является использование алгоритмов оптимизации, кластеризации и экспертных оценок для структурно-параметрической идентификации нечетких моделей, что позволяет адаптировать их к условиям эксплуатации выключателей и точно оценить состояние при недостатке статистических данных и их накоплении. На основе информации с реальных электросетевых объектов сформирована нечеткая модель и разработано программное обеспечение для оценки состояния масляных выключателей средней мощности. Качество модели определялось сравнением результатов моделирования с экспериментальными данными и заключениями специализированных организаций. При этом установлено, что модель обеспечивает повышение количества верно распознанных состояний не менее чем на 5 % в сравнении с традиционными методами обработки данных.* ***Практическая значимость:*** *использование предложенных нечетких моделей в экспертно-диагностических системах электросетевых объектов позволит на 10–20 % снизить время простоя выключателей благодаря повышению достоверности оценок состояния и принятию обоснованных, оперативных решений.*

Ключевые слова *— техническое состояние, нечеткая иерархическая модель, база знаний, высоковольтный выключатель, комплексная оценка, принятие решений.*

Введение

Построение интеллектуальных электрических сетей является одной из ключевых тенденций в области реформирования электроэнергетической отрасли страны [1, 2]. Подобные сети требуют создания не только энергетической, но и информационной инфраструктуры объектов генерации, распределения и потребления электроэнергии с использованием современных информационно-управляющих технологий. Ситуация такова, что большинство оборудования электросетевых объектов практически выработало свой ресурс и не может обеспечить стабильное электроснабжение потребителей ввиду своей повышенной аварийности. По статистике [3–6], существенное число нештатных ситуаций в энергосистемах связано с работой маслонаполненного оборудования, в частности масляных высоковольтных выключателей (малообъемных и баковых), доля которых в парке электротехнического оборудования по-прежнему высока.

Поскольку высоковольтные выключатели выполняют задачу обеспечения надежной и безопасной работы как в нормальных, так и в аварийных режимах [3], они являются исключительно важными элементами и традиционных, и потенциально новых электрических сетей, построенных на базе концепции *Smart Grid* [2]. В условиях ограниченного финансирования темпы технического перевооружения электросетевых объектов достаточно невысоки, поэтому проблема снижения затрат на восстановление высоковольтного оборудования и ущерба от его отказов является весьма актуальной. Существенную роль в данном процессе играют методы и технологии оценки состояния выключателей, а также их отдельных элементов, используемые для своевременного обнаружения и оперативного устранения потенциально опасных дефектов.

Постановка задачи исследования

Территориальная распределенность электросетевых объектов, отсутствие единой методологии их обслуживания, устанавливающей однозначные критерии нормирования значений параметров высоковольтных выключателей и прочего

электротехнического оборудования, накладывают определенные ограничения на выбор методов, используемых для оценки их состояния [3, 7–9]. Достаточная сложность построения диагностических функций на множестве параметров оборудования обусловливает потребность в применении подходов, ориентированных на работу как с количественными, так и с качественными данными, в том числе в условиях их неполноты, неоднозначности и недостоверности [10–12]. Решение данной проблемы связано с использованием интеллектуальных технологий и систем [12, 13], основанных не только на статистических данных, но и на экспертных знаниях, позволяющих достаточно просто и эффективно формализовать задачу диагностики возможных неисправностей оборудования. Реализовать данный подход с высокой степенью достоверности результата позволяет аппарат нечеткой логики [12, 14, 15].

Учитывая многопараметричность выключателей, целесообразно выделять группы параметров, свойственных его отдельным элементам или методам проведения измерений. В этом случае модели комплексной оценки состояния могут быть построены по иерархическому принципу [15, 16], что позволяет анализировать результаты как на отдельных уровнях иерархии (по узлам и агрегатам оборудования), так и по объекту в целом.

Процесс моделирования состояния выключателя в этом случае предполагает решение следующих задач: 1) построения иерархии нечеткого логического вывода на основе формализации ключевых диагностических параметров; 2) определения вида функций принадлежности, структуры базы знаний и алгоритма интеллектуальной обработки информации; 3) определения критериев принятия решений по результатам комплексной оценки.

В качестве исходных данных для проведения комплексной оценки состояния высоковольтных выключателей используются значения вектора параметров оборудования $\mathbf{X} = (x_1, ..., x_n)$, которые являются наиболее информативными и достаточно полно характеризуют работу его отдельных элементов. Иерархия оценки строится по принципу структурной декомпозиции параметров и формирования зависимости вида

$$Y = f\Big(y_1 = f_1(x_1, \ldots, x_{n_1}), \ldots, y_i = f_i(x_{n_j}, \ldots, x_{n_i}), \ldots, y_m = f_m(x_{n_{i+1}}, \ldots, x_n)\Big), \quad (1)$$

где Y — обобщенный параметр технического состояния выключателя (результат комплексной оценки); y_i — промежуточные параметры оценки состояния.

Для выбора параметров выключателя принимаются критерии: простота и оперативность съема; возможность проведения мониторинга без отключения и разбора выключателя, а также относительно невысокие затраты; проверка различных узлов либо характеристик отдельного узла с возможностью определения и устранения дефектов на ранних этапах их развития [3, 6, 12].

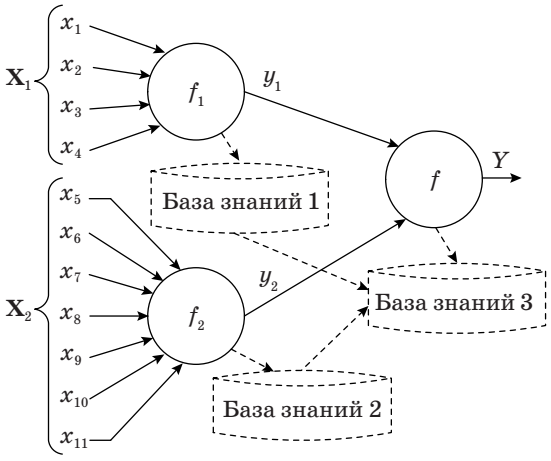
В составе нечетких иерархических моделей (НИМ), соответствующих структуре (1), переменные **X** и Y являются лингвистическими. При этом функции f и f_i представляют собой процедуры нечеткого логического вывода по соответствующей базе знаний, состоящей из набора нечетких импликаций «ЕСЛИ <**X**>, ТО <Y>». Интеллектуальная обработка данных в задаче (1) осуществляется на базе алгоритма Сугено [16].

Формирование системы иерархического нечеткого логического вывода

Формализация параметров, входящих в **X**, выполнена на примере высоковольтных масляных выключателей (МВ) (табл. 1) [17, 18] как одних из наиболее распространенных на большинстве действующих электросетевых объектов и нуждающихся в эффективной стратегии технического обслуживания и ремонта. Отметим, что существуют и другие важные параметры, оценку которых следует проводить при полном или частичном отключении выключателя от питающей сети в целях более детального анализа его состояния.

С учетом данных табл. 1 выбрана структура иерархического нечеткого логического вывода (рис. 1) для оценки состояния МВ, которая позволяет анализировать качество их работы по результатам тепловизионного контроля $y_1 = f(x_1, ..., x_4)$, визуального обследования $y_2 = f(x_5, ..., x_{11})$ и комплексно $Y = f(y_1, y_2)$.

Смысловая нагрузка лингвистических переменных x_i соответствует содержанию табл. 1.



■ ***Рис. 1.*** Дерево логического вывода к задаче комплексной оценки технического состояния МВ

■ ***Таблица 1.*** Параметры оценки состояния масляных выключателей

Обозначение и название параметра	Нормируемые значения	Метод/средство измерения
x_1 — избыточная температура болтовых контактных соединений узла	Менее 5 °С	Тепловизор, пирометр
x_2 — избыточная температура поверхности бака в зоне размещения дугогасительной камеры	Отсутствие локальных нагревов в точках контроля	То же
x_3 — избыточная температура поверхности бака в зоне размещения встроенных трансформаторов тока	Равномерное распределение температуры по поверхности бака	–"–
x_4 — разность температур по поверхности ввода	Равномерное распределение температуры по поверхности ввода	–"–
x_5 — внешнее состояние поверхности баков, привода и других элементов и систем	Отсутствие видимых дефектов, трещин, коррозии, оплавлений	Визуально
x_6 — внешнее состояние фарфоровых покрышек (изоляторов)	Отсутствие трещин, сколов, загрязнения фарфора, подтеков заливочной мастики	То же
x_7 — уровень шума внутри бака	Отсутствие шума и треска	Аудиально
x_8 — уровень масла в баке	В пределах шкалы маслоуказателя	Визуально
x_9 — наличие течи масла в баке	Отсутствует	То же
x_{10} — следы выброса масла из газоотводов	Отсутствуют	–"–
x_{11} — качество работы системы обогрева бака и привода	Своевременное включение (отключение) при температуре окружающей среды ниже минус 20 °С	Визуально; по результатам температурного контроля поверхности бака

■ ***Таблица 2.*** Структура нечетких импликаций на примере базы знаний 1

№ правила	Предпосылки (оценки контролируемых параметров)				Заключение
1	ЕСЛИ x_1 = «Н»	И x_2 = «Н»	И x_3 = «Н»	И x_4 = «Н»	ТО Y = «В норме»
...	...				
14	ЕСЛИ x_1 = «НС»	И x_2 = «Н»	И x_3 = «НС»	И x_4 = «Н»	ТО Y = «Удовлетворительное»
...	...				
63	ЕСЛИ x_1 = «ВС»	И x_2 = «НС»	И x_3 = «Н»	И x_4 = «ВС»	ТО Y = «Ниже нормы»
...	...				
79	ЕСЛИ x_1 = «В»	ИЛИ x_2 = «В»	ИЛИ x_3 = «В»	ИЛИ x_4 = «В»	ТО Y = «Критическое»

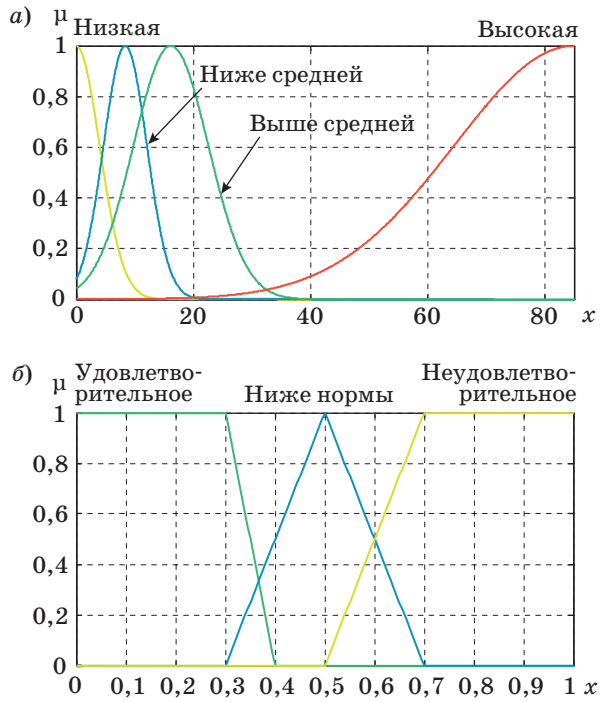
Примечание: Н — низкая, НС — ниже средней, ВС — выше средней, В — высокая.

Общее количество правил иерархической базы знаний, сформированных на основе экспертных мнений, равно 104 (табл. 2).

Вид и параметры функций принадлежности входных лингвистических переменных $\mathbf{X}_1 = (x_1, ..., x_4)$ формируются на основе нечеткой кластеризации [12] с использованием данных тепловизионного контроля выключателей. Для построения функций принадлежности переменных $\mathbf{X}_2 = (x_5, ..., x_{11})$ используется метод экспертных оценок (рис. 2) [16].

Термы выходной переменной Y и промежуточных переменных y_1 и y_2, характеризующие уровни критичности состояния МВ, соответствуют вербальным оценкам «В норме», «Удовлетворительное», «Ниже нормы», «Критическое» и выбраны по итогам анализа эксплуатационной и нормативно-технической документации, а также с учетом опыта электротехнического персонала, ответственного за обслуживание оборудования.

Функции принадлежности промежуточных переменных y_1 и y_2 не задаются, а для выход-



■ ***Рис. 2.*** Пример задания функций принадлежности для представления параметров **X** в виде лингвистических переменных: при помощи нечеткой кластеризации для x_1 (*а*); при помощи экспертных оценок для x_5 (*б*)

ной переменной Y могут быть заданы произвольно [16].

Расчет степеней принадлежности для оценки состояния выключателя по иерархической базе знаний осуществляется в два этапа [19]:

$$\mu_{d_u}(\mathbf{X}_i) = \bigvee_{t=1}^{e_u}\left[\omega_{ut}^{<D>} \cdot \bigwedge_{j=1}^{n_i} \mu_{a_j^{ut}}(x_j)\right]; \qquad (2)$$

$$\mu_{s_l}(\mathbf{X}) = \bigvee_{t=1}^{h_l}\left[\omega_{lt}^{<S>} \cdot \bigwedge_{i=1}^{m} \mu_{d_{i,u}^{lt}}(\mathbf{X}_i)\right], \qquad (3)$$

где $\mu_{a_j^{ut}}(x_j)$ — степень принадлежности значения переменной x_j к нечеткому терму a_j^{ut} в t-м правиле для u-го терма d_u промежуточной переменной; $\mu_{d_u}(\mathbf{X}_i)$ — степень принадлежности значений переменных, входящих в i-ю базу знаний, к оценке d_u промежуточной переменной; $\mu_{s_l}(\mathbf{X})$ — степень принадлежности значений вектора всех входных переменных к уровню (классу) состояния выключателя s_l; $\mu_{d_u^{lt}}(\mathbf{X}_i)$ — степень принадлежности переменных $\mathbf{X}_i$ к нечеткой оценке s_l выходной переменной Y в t-м правиле; $\omega_{ut}^{<D>}, \omega_{lt}^{<S>} \in [0,1]$ — веса t-го правила для значений d_u промежуточной переменной и s_l выходной переменной; e_u и h_l — количество правил, характеризующих оценки d_u и s_l; $\vee(\wedge)$ — операции нахождения максимума (минимума) нечетких множеств.

Решение, определяющее фактический уровень состояния выключателя по результатам вычислений (2) и (3), соответствует классу с максимальной степенью принадлежности [19]:

$$Y = \arg\max_{\{s_1,s_2,\ldots,s_L\}}\left(\mu_{s_1}(\mathbf{X}), \mu_{s_2}(\mathbf{X}), \ldots, \mu_{s_L}(\mathbf{X})\right). \qquad (4)$$

Таким образом, выражения (2)–(4) позволяют осуществить переход от значений технических параметров отдельных элементов выключателя, контролируемых в процессе мониторинга электросетевого объекта, к заключению о его фактическом состоянии.

Формирование критериев принятия решений по результатам комплексной оценки

Общие рекомендации по использованию результатов оценки состояния выключателей при помощи НИМ для принятия решений о проведении мероприятий, направленных на поддержание их работоспособности в процессе эксплуатации, приведены в табл. 3.

Дополнительно сформированы рекомендации по контролю состояния отдельных конструкционных элементов и параметров МВ (табл. 4) [17, 18] с целью локализовать опасные дефекты и оценить объемы работ по их ликвидации.

■ ***Таблица 3.*** Рекомендации по дальнейшей эксплуатации выключателя

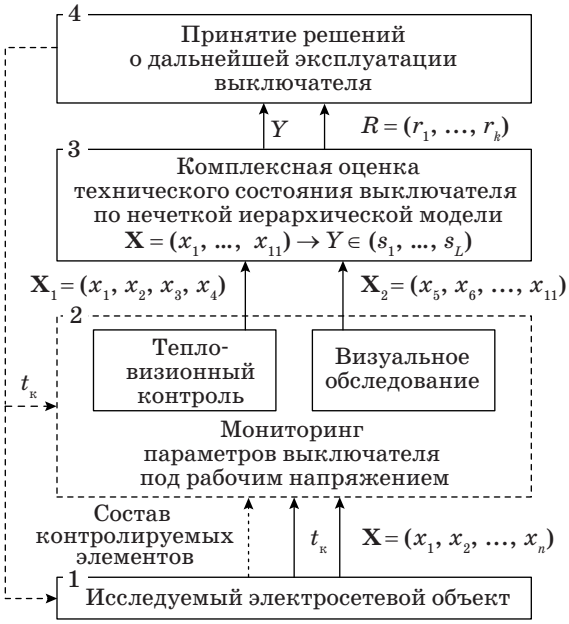
Состояние (класс) по НИМ	Заключение
«В норме»	Отсутствуют явные дефекты. Дальнейшая эксплуатация без ограничений с мониторингом состояния в штатном режиме (под рабочим напряжением)
«Удовлетворительное»	Малозначительный дефект. Эксплуатация в режиме мониторинга ключевых узлов с периодичностью, установленной на основе экспертных оценок инженерно-технического персонала
«Ниже нормы»	Развившийся дефект. Ограничение эксплуатации, мониторинг состояния с учащенной периодичностью. Расширенная диагностика в целях подтверждения факта наличия дефекта и его локализации. Устранение неисправности при ближайшем выводе из работы
«Критическое»	Критический дефект. Срочный ремонт с выводом из эксплуатации, локализацией и устранением дефекта в целях предупреждения аварийной ситуации

■ ***Таблица 4.*** Общие рекомендации по проведению мероприятий в случае неудовлетворительных результатов мониторинга элементов МВ

Параметр	Описание мероприятия
x_1	Зачистка, шлифовка и протяжка контактных соединений
x_2	Измерение переходного сопротивления токоведущей цепи каждого полюса выключателя. Установление учащенной периодичности мониторинга или ревизия дугогасительной камеры
x_3	Дополнительное обследование по программе [18] на предмет наличия витковых замыканий в обмотках встроенного трансформатора тока
x_4	Измерение тангенса угла диэлектрических потерь
x_5	Обеспечение целостности деталей выключателя, восстановление внешнего состояния (включая лакокрасочное покрытие). Проверка правильности положения указателя включенного или отключенного состояния выключателя
x_6	Чистка или замена
x_7	Отбор и анализ проб масла. Проверка на наличие утечек масла
x_8, x_9	Наружный осмотр для выявления мест утечек масла. Принятие мер, препятствующих отключению выключателем токов нагрузки и короткого замыкания (при значительном снижении уровня масла). Замена диафрагмы и маслоуказателя в случае их неисправности. Испытание бака, подтяжка или замена уплотняющих прокладок
x_{10}	Замена диафрагмы во избежание попадания влаги в масло. Проверка скоростных характеристик выключателя, состояния дугогасительной камеры и внутрибаковой изоляции
x_{11}	Восстановление работоспособности устройства подогрева бака (в условиях отрицательных температур окружающей среды)

Место нечеткой модели в структуре системы технического обслуживания и ремонта МВ по фактическому состоянию показано на рис. 3.

Согласно схеме, итоги комплексной оценки состояния выключателей по НИМ (блок № 3) и перечень полученных рекомендаций R являются основанием (блок № 4) для их замены либо проведения различных ремонтно-эксплуатационных мероприятий, включая расширенную диагностику с привлечением дополнительных методов и средств, а также профилактические ремонтно-восстановительные работы. Периодичность контроля параметров $t_к$ выключателей (блок № 2) в режиме on-line определяется их фактическим состоянием, а также результатами технического обслуживания и ремонта.



■ ***Рис. 3.*** Структурно-функциональная схема принятия решений при обслуживании МВ с мониторингом состояния под рабочим напряжением

Исследование нечетких иерархических моделей оценки состояния масляных выключателей

Практическая апробация возможностей использования НИМ осуществлялась на примере масляных баковых выключателей средней мощности (35 кВ). Формализация модели, расчеты и последующее моделирование производились с использованием специально разработанного программного обеспечения *ITSES*, позволяющего наглядно интерпретировать результаты оценки состояния МВ и сформировать рекомендации относительно их дальнейшей эксплуатации.

Для параметрической идентификации модели использовались статистические данные по эксплуатации выключателей на электросетевых объектах Пермского края (протоколы обследований, журналы оперативно-диспетчерских служб и т. д.) за 2010–2014 гг.

Для функций принадлежности переменных, входящих в $\mathbf{X}_1$, выбрана гауссова форма и четыре терма с вербальными оценками «Низкая», «Ниже средней», «Выше средней», «Высокая». Описание переменных x_5 и x_6 термами «Удовлетворительное», «Ниже нормы», «Неудовлетворительное» выполнено с помощью трапецеидальной

и треугольной функций. Для переменных x_7–x_{11} выбраны двухэлементные («В пределах нормы», «Ниже нормы») и трехэлементные («Отсутствует», «Незначительная», «Присутствует») терм-множества с функциями принадлежности треугольного типа.

Процедура нахождения весов правил базы знаний рассматривалась как задача минимизации (рис. 4) ошибки распознавания состояний *MRE*

$$\frac{1}{K}\sum_{k}^{K}\Delta_k(\mathbf{X}^{(k)},\Omega); \qquad (5)$$

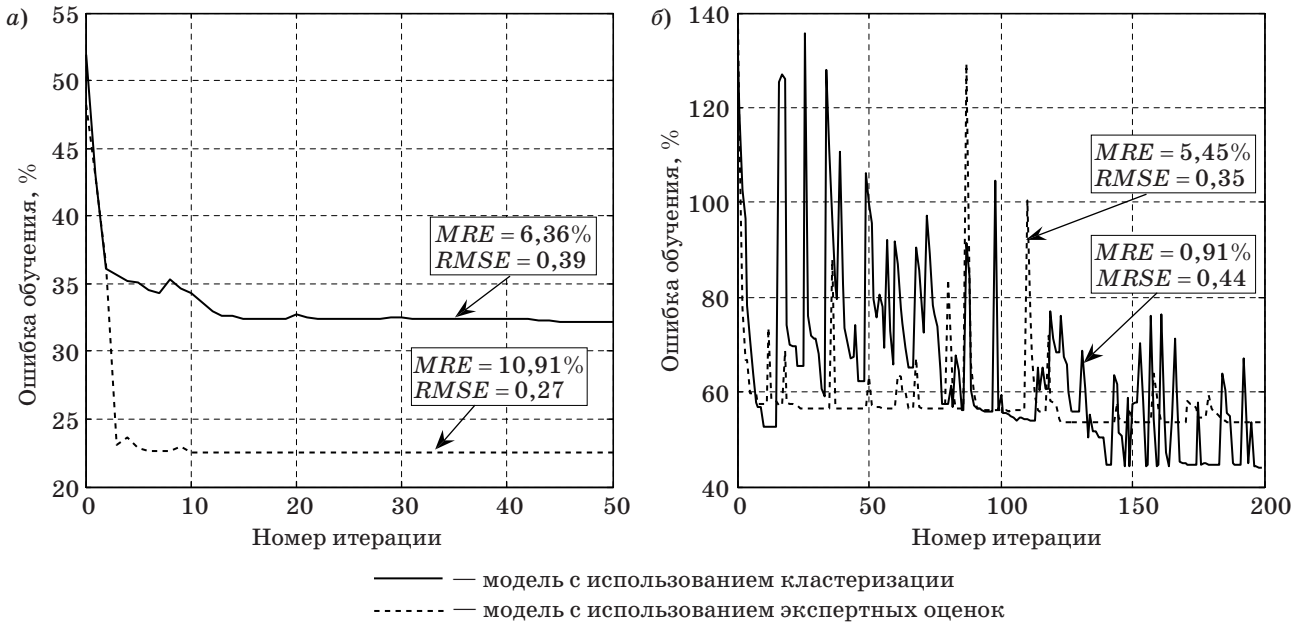
среднеквадратической невязки *RMSE* результатов моделирования и экспериментальных данных

$$\frac{1}{K}\sqrt{\sum_{k=1}^{K}\sum_{l=1}^{L}\left[\mu_{s_l}(Y^{(k)})-\mu_{s_l}(\mathbf{X}^{(k)},\Omega)\right]^2} \qquad (6)$$

и модифицированной функции [19]

$$\sqrt{\frac{1}{K}\sum_{k=1}^{K}\left[\begin{array}{c}\left[\Delta_k(\mathbf{X}^{(k)},\Omega)\cdot P+1\right]\times\\ \times\sum_{l=1}^{3}\left[\mu_{s_l}(Y^{(k)})-\mu_{s_l}(\mathbf{X}^{(k)},\Omega)\right]^2\end{array}\right]}, \qquad (7)$$

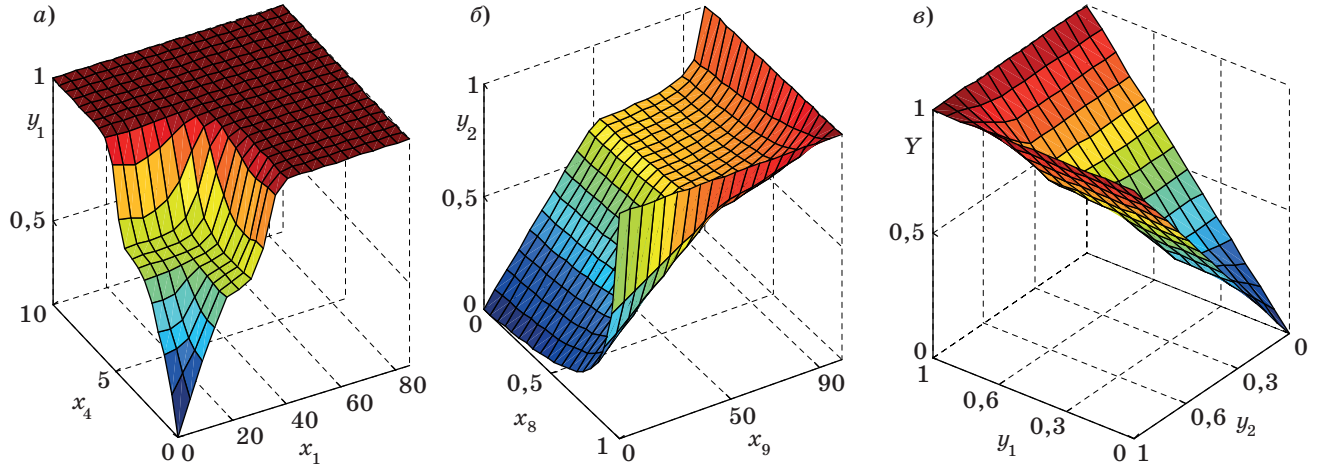
где $\mathbf{X}^{(k)}$ — вектор значений параметров выключателя из k-й строки обучающей выборки; $\mu_{s_l}(Y^{(k)})$ и $\mu_{s_l}(\mathbf{X}^{(k)},\Omega)$ — степени принадлежности значения переменной Y в k-й строке обучающей выборки и выхода НИМ с параметрами Ω при значениях входных переменных $\mathbf{X}^{(k)}$ к решению s_l; $\Delta_k(\mathbf{X}^{(k)}, \Omega)$ — результат распознавания состояния (равен нулю в случае успеха и единице в случае ошибки); P — коэффициент увеличения приоритета ошибочно распознанных состояний (при расчетах эмпирически выбран равным 17).



■ ***Рис. 4.*** Динамика процесса параметрической оптимизации НИМ для оценки состояния МВ: *а* — по критерию (5); *б* — по критерию (6)

■ ***Таблица 5.*** Оценка адекватности НИМ экспериментальным данным

Тип модели	Способ параметрической оптимизации	Оценка по критерию			
		Обучающая выборка		Полная выборка	
		MRE	*RMSE*	*MRE*	*RMSE*
На основе нечеткой кластеризации	Выражение (5)	3,63	0,53	4,29	0,38
	Выражение (6)	6,36	0,39	6,19	0,30
	Выражение (7)	0,91	0,44	2,38	0,29
На основе экспертных оценок	Выражение (5)	7,27	0,48	6,19	0,39
	Выражение (6)	10,91	0,27	12,85	0,21
	Выражение (7)	5,45	0,35	5,71	0,24



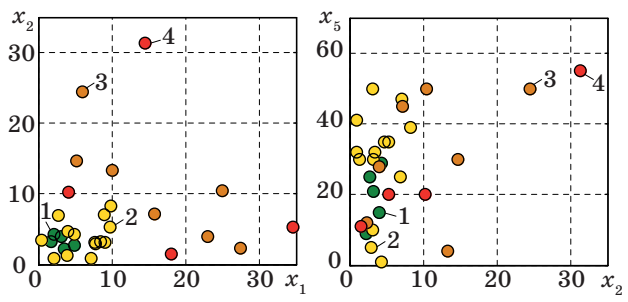
■ ***Рис. 5.*** Функции отклика: *а* — переменной y_1 при значениях x_2 и x_3, равных 0 °С; *б* — переменной y_2 при $x_5 = 10$ % и значениях x_6, x_7, x_{10}, x_{11}, равных нулю; *в* — выходной переменной Y

Результаты тестирования НИМ, построенных с учетом различных подходов к выбору параметров функций принадлежности (табл. 5), указывают на высокий уровень точности моделирования в сравнении с заключениями специализированных организаций.

Функциональные зависимости состояния МВ от результатов проведения визуального и тепловизионного обследований (рис. 5, *а–в*) имеют нелинейный характер, подтверждая гипотезу о сложно формализуемом характере задачи диагностики выключателей.

Связи значений параметров МВ, измеренных в ходе мониторинга, с уровнем их фактического состояния, оцененного при помощи программы *ITSES*, выборочно показаны на рис. 6.

Полученные оценки состояния выключателей использованы при определении направлений их дальнейшей эксплуатации, что позволило выявить ряд наиболее распространенных типов дефектов, преимущественно теплового характера, и предупредить их дальнейшее развитие.



■ ***Рис. 6.*** Пример оценки состояния МВ при заданных наборах значений диагностических параметров по классам: *1* — «В норме»; *2* — «Удовлетворительное»; *3* — «Ниже нормы»; *4* — «Критическое»

Заключение

В работе предложен метод комплексной оценки технического состояния высоковольтных выключателей по результатам мониторинга их ключевых диагностических параметров на основе построения НИМ.

Результаты исследования НИМ показывают, что для моделей, использующих алгоритмы кластеризации при формировании функций принадлежности и составной критерий оптимизации, количество ошибочно распознанных состояний МВ снижается в среднем до 10 %.

Эффект от практического использования данных результатов зависит от вида верно или неверно распознанного состояния выключателя и связан со снижением времени его простоя по причине плановых или внеплановых ремонтно-эксплуатационных работ. При исследовании выключателей мощностью 35 кВ было определено, что снижение времени может составлять до 20 %. К примеру, своевременное обнаружение развившихся и критических дефектов (таких как перегрев контактных соединений, нарушение контакта дугогасительной камеры, неудовлетворительное состояние вводов и др.) позволит сократить количество внезапных отказов выключателей и избежать возможного ущерба. При этом достоверные сведения о состоянии выключателя и возможность принятия обоснованных решений позволят оптимизировать объемы ремонтных работ в том случае, когда их проведение фактически не требуется, что не свойственно системе планово-предупредительных ремонтов.

Предлагаемый подход может быть использован для комплексной оценки состояния выключателей различного типа (не только масляных) и мощности. Для этого требуется анализ необходимости корректировки/расширения перечня

контролируемых параметров, а также дополнительная структурно-параметрическая идентификация НИМ [20].

Накопление данных по мониторингу ключевых параметров выключателей и других видов электротехнического оборудования с последующей формализацией НИМ могут послужить основой для создания интегрированной информационно-диагностической системы, направленной на обеспечение безаварийного функционирования объектов электроэнергетики.

Исследование выполнено при финансовой поддержке РФФИ № 14-07-96000 р_урала_а «Разработка интеллектуальной системы поддержки принятия решений обеспечения безаварийной работы энергетических объектов».

Литература

1. **Дорофеев В. В., Макаров А. А.** Активно-адаптивная сеть — новое качество ЕЭС России // Энергоэксперт. 2009. № 4. С. 29–34.
2. **Лидин С. С.** Интеллектуальные сети Smart Grid — будущее российской энергетики //Автоматизация и IT в энергетике. 2010. № 11(16). С. 4–8.
3. **Назарычев А. Н.** Методы и модели оптимизации ремонта электрооборудования объектов энергетики с учетом технического состояния. — Иваново: Изд-во Иван. гос. энерг. ун-та, 2002. — 168 с.
4. **Хренников А. Ю., Гольдштейн В. Г., Складчиков А. А.** Расследование технологических нарушений электрооборудования подстанций // Энергоэксперт. 2011. № 5(28). С. 74–83.
5. **Хорошев Н. И.** Оценка технического состояния силового маслонаполненного электротехнического оборудования в различных режимах его работы // Изв. Томского политехнического университета. 2013. Т. 323. № 4. С. 162–167.
6. **Кузнецов В. И., Сазонова И. Г., Коновалова Г. А.** О комплексном обследовании масляных баковых выключателей 110–220 кВ // Электрические станции. 2002. № 5. С. 77–78.
7. **Петроченков А. Б.** О подходах к оценке технического состояния электротехнических комплексов и систем // Изв. высших учебных заведений. Машиностроение. 2012. № 12. С. 16–20.
8. **Петроченков А. Б., Бочкарев С. В., Ромодин А. В., Елтышев Д. К.** Планирование процесса эксплуатации электротехнического оборудования с использованием теории марковских процессов // Электротехника. 2011. № 11. С. 20а–24.
9. **Петроченков А. Б., Солодкий Е. М.** К вопросу о подходах к анализу надежности сложных систем // Научно-технические ведомости СПбГПУ. 2011. № 121. С. 214–218.
10. **Khoroshev N. I., Kazantsev V. P.** Management Support of Electroengineering Equipment Servicing Based on the Actual Technical Condition // Automation and Remote Control. 2015. Vol. 76. N 6. P. 1058–1069. doi:10.1134/S0005117915060090
11. **Petrochenkov A. B.** An Energy-Information Model of Industrial Electrotechnical Complexes // Russian Electrical Engineering. 2015. Vol. 85. N 11. P. 692–696. doi:10.3103/S1068371214110108
12. **Елтышев Д. К.** Интеллектуализация процесса диагностики состояния электротехнического оборудования // Информатика и системы управления. 2015. № 1(43). С. 72–82.
13. **Городецкий А. Е., Курбанов В. Г., Тарасова И. Л.** Экспертная система анализа и прогнозирования аварийных ситуаций в энергетических установках // Информационно-управляющие системы. 2012. № 4. С. 59–63.
14. **Хорошев Н. И., Казанцев В. П.** Применение правил нечеткой логики при эксплуатации электротехнического оборудования // Электротехника. 2011. № 11. С. 59–64.
15. **Костерев Н. В., Бардик Е. И., Вожаков Р. В., Курач Т. Ю.** Нечеткие алгоритмы оценки технического состояния и прогнозирования остаточного ресурса электрооборудования // Науч. тр. ДонНТУ. Сер. Электротехника и энергетика. 2008. № 8. С. 65–70.
16. **Штовба С. Д.** Проектирование нечетких систем средствами MATLAB. — М.: Горячая Линия–Телеком, 2007. — 288 с.
17. РД 153-34.0-20.363-99. Основные положения методики инфракрасной диагностики электрооборудования и ВЛ. — М.: СПО ОРГРЭС, 2001. — 145 с.
18. РД 34.45-51.300-97. Объем и нормы испытаний электрооборудования. — М.: Атомиздат, 2001. — 154 с.
19. **Shtovba S. D., Pankevich O. D., Nagorna A. V.** Analyzing the Criteria for Fuzzy Classifier Learning // Automatic Control and Computer Sciences. 2015. Vol. 49. N 3. P. 123–132. doi:10.3103/S0146411615030098
20. **Ходашинский И. А.** Идентификация нечетких систем: методы и алгоритмы // Проблемы управления. 2009. № 4. С. 15–23.

UDC 621.31:658.58:004.89
doi:10.15217/issn1684-8853.2016.5.45

Intelligent Models for Complex Assessment of Technical Condition of High-Voltage Circuit Breakers

Eltyshev D. K.[a], PhD, Tech., Associate Professor, eltyshev@msa.pstu.ru
[a]Perm National Research Polytechnic University, 29, Komsomol'skii Pr., 614990, Perm, Russian Federation

Purpose: Early detection and prevention of defects in high-voltage circuit breakers and other electrical equipment, especially when wear and tear is high, is an important task to ensure the reliability of power supply systems. The circuit breaker operation processes are multifactorial, imposing significant limitations on the choice of methods to control their condition when the available information is often incomplete and ambiguous. One of the ways to effectively solve the problem is the use of intelligent information technologies. **Methods:** Construction of a hierarchically structured knowledge base on the basis of fuzzy implicative rules which simulate thinking of electrical staff assessing the state of a circuit breaker and its elements. **Results:** There has been proposed a method of assessing the condition of high-voltage circuit breakers by the results of monitoring with the use of formalized expert knowledge for data mining. The method is based on the selection and structural decomposition of the equipment parameters which are measured without disconnecting from the power supply and which determine the variables of the hierarchical fuzzy model. The method is step-by-step determination of the criticality level for the circuit breaker and its elements, and forming reasonable control actions to maintain their operability. This approach is characterized by the use of optimization, clustering and expert analysis algorithms for structural and parametrical identification of fuzzy models. This allows you to adapt the models to the operating conditions of the circuit breakers and accurately assess their state in the case of statistical data shortage and its accumulation. On the basis of information from actual power grid facilities, there has been developed a fuzzy model and software for the assessment of medium-power oil circuit breakers. The quality of the model was determined by comparing the simulation results with experimental data and by conclusions of specialized organizations. It has been found out that the model provides an increase in the amount of true detected states of not less than 5 % compared to the traditional data processing methods. **Practical relevance:** The use of the proposed fuzzy models in expert-diagnostic systems of power grid facilities can reduce the downtime of circuit breakers by 10–20 % due to improving the condition assessment accuracy and making reasonable and timely decisions.

Keywords — Technical Condition, Hierarchical Fuzzy Model, Knowledge Base, High-Voltage Circuit Breakers, Complex Assessment, Decision Making.

References

1. Dorofeev V. V., Makarov A. A. Active-adaptive Network — a New Quality of UES of Russia. *Energoekspert*, 2009, no. 4, pp. 29–34 (In Russian).
2. Ledin S. S. Intelligent Networks Smart Grid — the Future of the Russian Power Industry. *Avtomatizatsiia i IT v energetike*, 2010, no. 11(16), pp. 4–8 (In Russian).
3. Nazarychev A. N. *Metody i modeli optimizatsii remonta elektrooborudovaniia ob"ektov energetiki s uchetom tekhnicheskogo sostoianiia* [Methods and Models of Power Facilities Electrical Equipment Repair Optimization Based on Technical Condition]. Ivanovo, Ivanovskii gosudarstvennyi energeticheskii universitet Publ., 2002. 168 p. (In Russian).
4. Khrennikov A. Yu., Gol`dshtein V. G., Skladchikov A. A. The Investigation of Technological Violations of Substations Electrical Equipment. *Energoekspert*, 2011, no. 5(28), pp. 74–83 (In Russian).
5. Khoroshev N. I. Assessment of Technical Condition of Power Oil-filled Engineering Equipment in Different Operation Modes. *Izvestiia Tomskogo politekhnicheskogo universiteta*, 2013, vol. 323, no. 4, pp. 162–167 (In Russian).
6. Kuznetsov V. I., Sazonova I. G., Konovalova G. A. About Complex Inspection of Dead-tank Oil Circuit Breakers 110–220 kV. *Elektricheskie stantsii*, 2002, no. 5, pp. 77–78 (In Russian).
7. Petrochenkov A. B. On Approaches to Assess the Technical State of Electrical Engineering Complexes and Systems. *Izvestiia vysshikh uchebnykh zavedenii. Mashinostroenie*, 2012, no. 12, pp. 16–20 (In Russian).
8. Petrochenkov A. B., Bochkarev S. V., Romodin A. V., Eltyshev D. K. The Planning Operation Process of Electrotechnical Equipment Using the Markov Process Theory. *Russian Electrical Engineering*, 2011, vol. 82, no. 11, pp. 592–595. doi:10.3103/S1068371211110113
9. Petrochenkov A. B., Solodkii E. M. The Question of Approach to Analyzing the Reliability of Complex Systems. *Nauchno-tekhnicheskie vedomosti SPbGPU*, 2011, no. 121, pp. 214–218 (In Russian).
10. Khoroshev N. I., Kazantsev V. P. Management Support of Electroengineering Equipment Servicing Based on the Actual Technical Condition. *Automation and Remote Control*, 2015, vol. 76, no. 6, pp. 1058–1069. doi:10.1134/S0005117915060090
11. Petrochenkov A. B. An Energy-information Model of Industrial Electrotechnical Complexes. *Russian Electrical Engineering*, 2015, vol. 85, no. 11, pp. 692–696. doi:10.3103/S1068371214110108
12. Eltyshev D. K. Intellectualization of Diagnostics of Electric Machinery. *Informatika i sistemy upravleniia*, 2015, no. 1(43), pp. 72–82 (In Russian).
13. Gorodetsky A. E., Kurbanov V. V., Tarasova I. L. Expert System of Analysis and Forecasting Emergencies in Power Generating Systems. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2012, no. 4, pp. 59–63 (In Russian).
14. Khoroshev N. I., Kazantsev V. P. Application of Fuzzy Logic Rules during Operation of Electrotechnical Equipment. *Russian Electrical Engineering*, 2011, vol. 82, no. 11, pp. 632–637. doi:10.3103/S1068371211110071
15. Kosterev N. V., Bardik E. I., Vozhakov R. V., Kurach T. Iu. Fuzzy Algorithms for Technical Condition Assessment and Prediction of a Residual Resource of Electrical Equipment. *Nauchnye trudy DonNTU*. Ser. *Elektrotekhnika i energetika*, 2008, no. 8, pp. 65–70 (In Russian).
16. Shtovba S. D. *Proektirovanie nechetkikh sistem sredstvami MATLAB* [Design of Fuzzy Systems by Means of MATLAB]. Moscow, Goriachaia Liniia–Telekom Publ., 2007. 288 p. (In Russian).
17. Guidance Document 153-34.0-20.363-99. The Main Provisions of Methods of Infrared Diagnostics of Electrical Equipment and Overhead Lines. Moscow, SPO ORGRES Publ., 2001. 145 p. (In Russian).
18. Guidance Document 34.45-51.300-97. The Volume and Norms of Electrical Equipment Testing. Moscow, Atomizdat Publ., 2001. 154 p. (In Russian).
19. Shtovba S. D., Pankevich O. D., Nagorna A. V. Analyzing the Criteria for Fuzzy Classifier Learning. *Automatic Control and Computer Sciences*, 2015, vol. 49, no. 3, pp. 123–132. doi:10.3103/S0146411615030098
20. Hodashinsky I. A. Identification of Fuzzy Systems: Methods and Algorithms. *Problemy upravleniia*, 2009, no. 4, pp. 15–23 (In Russian).

УДК 004.056
doi:10.15217/issn1684-8853.2016.5.54

МЕТОДИКИ И ПРОГРАММНЫЙ КОМПОНЕНТ ОЦЕНКИ РИСКОВ НА ОСНОВЕ ГРАФОВ АТАК ДЛЯ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ

Е. В. Дойникова[a], *научный сотрудник*
И. В. Котенко[a], *доктор техн. наук, профессор*
[a]*Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, РФ*

Постановка проблемы: *тема реагирования на компьютерные атаки остается актуальной, так как количество компьютерных угроз год от года не уменьшается, информационные технологии применяются повсеместно, а сложность и размер сетевых инфраструктур растет. Соответственно, растет и необходимость в усовершенствовании механизмов оценки защищенности и выбора мер реагирования. Для адекватного реагирования на атаки необходим грамотный всесторонний анализ рисков системы, дающий значимую и реально отражающую ситуацию по защищенности оценку. Хотя исследователями были предложены различные подходы, универсального решения найти не удалось.* ***Цель:*** *разработка методик оценки риска, адекватно отражающих текущую ситуацию по защищенности на основе автоматизированной обработки доступных данных по безопасности; разработка реализующего их программного средства; оценка эффективности методик на основе экспериментов.* ***Результаты:*** *разработаны и реализованы в рамках программного средства методики оценки рисков, основанные на ранее предложенной авторами комплексной системе показателей защищенности. Уточнены некоторые аспекты вычисления показателей для оценки рисков, отличающие предложенные методики от аналогичных работ. Выбор методики в программном компоненте осуществляется в зависимости от текущей ситуации и требований пользователя программного средства. Для проверки результатов работы методик проведены эксперименты. На основе экспериментов выделены достоинства и недостатки предложенных методик.* ***Практическая значимость:*** *разработанные методики и программный компонент позволят повысить защищенность информационных систем за счет предоставления значимой и адекватной оценки защищенности системы.*

Ключевые слова *— методика оценки рисков, показатели защищенности, граф атак, граф зависимостей сервисов, инциденты безопасности.*

Введение

Вопросы оценки рисков компьютерных сетей широко рассмотрены в литературе, в том числе в отечественных и международных стандартах [1–4], корпоративных стандартах [5, 6] и множестве исследовательских работ [7–12]. Популярность данной тематики не снижается, так как количество компьютерных угроз год от года растет, соответственно, растет и необходимость в усовершенствовании механизмов оценки защищенности.

Для адекватного реагирования на атаки необходим грамотный всесторонний анализ рисков системы, дающий значимую и реально отражающую ситуацию по защищенности оценку. Исследователями были предложены различные подходы, в том числе к определению риска на основе вероятностей атак [7, 8] и возможного ущерба от атак [9, 10]; основанные на определении поверхности атаки [11]; учитывающие возможные финансовые потери [12].

В процессе изучения данной темы авторами был предложен подход, объединяющий модели, методики и алгоритмы вычисления показателей [13]. Данному подходу присущи следующие особенности: унификация представления входных данных на основе открытых стандартов для автоматизации процесса; совместный учет характеристик различных объектов оценки (программно-аппаратного обеспечения, уязвимостей, атак, атакующего, инцидентов безопасности и контрмер) для более точной оценки ситуации по защищенности; применение графов зависимости сервисов и байесовских графов атак для вычисления показателей; иерархическое деление показателей на группы, позволяющее получать оценку на основе минимального количества данных.

В работе [13] рассматривались модели и методики вычисления показателей защищенности, применяемые для выбора контрмер. В настоящей статье описывается программный компонент оценки защищенности, реализующий интегрированный комплекс методик оценки рисков. Компонент позволяет гибко выбирать методику в зависимости от текущей ситуации и требований пользователя программного средства. Также в исследовании рассматриваются некоторые аспекты вычисления показателей для оценки рисков, отличающие его от аналогичных работ. Описывается архитектура прототипа программного средства и элементы интерфейса. На экспериментах показана реализация методик в программном средстве, резуль-

таты их работы, выделены достоинства и недостатки.

Таким образом, основной вклад данной работы состоит в сведении ряда показателей защищенности в полноценные методики оценки рисков, демонстрации результатов работы реализующего их программного средства и оценке соответствия методик заявленным требованиям на основе экспериментов.

Методики оценки риска

В зависимости от применяемых для определения уровня риска входных данных и показателей защищенности и в соответствии с традиционным делением методик оценки рисков выделяются методики статической (включая базовую и детальную) и динамической оценки риска.

Входными данными методик оценки риска являются модель компьютерной сети (КС) и модель атак; показатели защищенности разных уровней (топологического, графа атак, атакующего и инцидентов), выделенных в зависимости от применяемых входных данных [13].

Общая схема методик в рамках процесса оценки защищенности представлена на рис. 1. Методики включают следующие этапы:

1) сбор входных данных: компонент оценки риска получает данные от компонента обработки входных данных и компонента вычисления показателей;

2) определение методики вычислений: в зависимости от получаемых входных данных выбирается методика определения уровня риска;

3) вычисление значения риска и получение оценки защищенности.

Выходными данными работы методик являются значения риска для объектов сети и оценка защищенности.

Базовая статическая методика оценки риска

Простым и очевидным решением для верхнеуровневой оценки риска является применение оценок CVSS для уязвимостей [14].

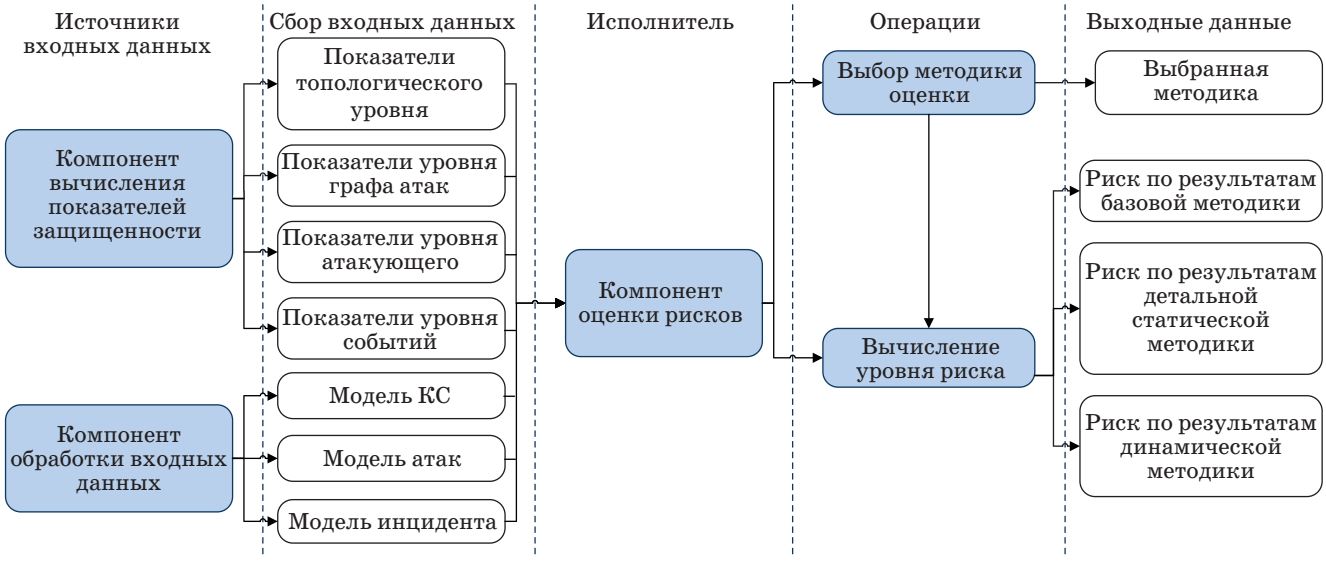
Уровень риска предлагается определять на основе модифицированного контекстного уравнения CVSS, так как оно позволяет учитывать связь между оценкой уязвимости и критичностью активов. Для учета критичности активов воспользуемся показателем CVSS *SecurityRequirements* (требования безопасности). Данный показатель может принимать три значения (0,5; 1,0; 1,51) и устанавливается вручную для каждой системы. Заменим его показателем *Criticality*, который определяет ценность актива для организации. Показатель вычисляется с учетом финансовой ценности активов и зависимостей между свойствами безопасности активов. Шкала возможных значений показателя: 0 – 100 ([0:0,01) — ничтожно малая; [0,01:0,1) — малая; [0,1:1) — значительная; [1:10) — повреждающая; [10:100) — серьезная; 100 — смертельная). Преобразование шкалы для применения в уравнении оценки риска приведено в табл. 1.

Контекстное уравнение CVSS

$$Risk = \text{round\_to\_1\_decimal}(AdjustedBase)$$

в раскрытом виде выглядит следующим образом:

$$Risk = \text{round\_to\_1\_decimal}(((0{,}6 \times AdjustedImpact) + (0{,}4 \times Exploitability) - 1{,}5) \times f(AdjustedImpact)).$$



■ ***Рис. 1.*** Общая схема методик определения уровня риска

■ ***Таблица 1***. Преобразование оценок критичности актива для применения в уравнении оценки риска

Критичность	Значение
[0:0,01)	0
[0,01:0,1)	0,5
[0,1:1)	1
[1:10)	1,2
[10:100)	1,4
100	1,51

Здесь *Exploitability* — возможность использования уязвимости; $f(AdjustedImpact) = \begin{cases} 0, \text{ если } AdjustedImpact = 0 \\ 1{,}176, \text{ если } AdjustedImpact \neq 0 \end{cases}$,

$$AdjustedImpact = \min(10{,}10{,}41 \times (1 - (1 - ConfImpact \times ConfReq) \times (1 - IntegImpact \times IntegReq) \times (1 - AvailImpact \times AvailReq))),$$

где *ConfImpact*, *IntegImpact*, *AvailImpact* — влияние на конфиденциальность, целостность и доступность в результате эксплуатации уязвимости соответственно; *ConfReq*, *IntegReq*, *AvailReq* — требования безопасности, которые в данном контексте рассматриваются как критичность актива, т. е. уравнение принимает вид

$$AdjustedImpact = \min(10{,}10{,}41 \times (1 - (1 - ConfImpact \times Criticality(c)) \times (1 - IntegImpact \times Criticality(i)) \times (1 - AvailImpact \times Criticality(a)))),$$

где *Criticality*(*c*), *Criticality*(*i*) и *Criticality*(*a*) — критичность конфиденциальности, целостности и доступности актива соответственно.

Таким образом, риск может принимать значения от 0 до 10. После того как определен риск каждой уязвимости хоста, оценка риска для экземпляра программно-аппаратного обеспечения определяется как максимальная из данных оценок, а оценка риска для хоста — как максимальная из оценок для программно-аппаратного обеспечения. Уровень риска для КС в целом определяется максимальной оценкой риска хостов как «высокий»/«средний»/«низкий» в соответствии с уровнями CVSS-оценок. Таким образом, можно выделить наиболее незащищенные участки системы.

Разработка данной методики включала выделение показателей, применяемых для вычисления уровня риска, преобразование уравнения CVSS для включения показателя критичности, преобразование шкалы значений показателя критичности для включения в уравнение CVSS, формирование правил определения уровня риска для КС в целом и ее объектов (уязвимостей, программного обеспечения, хостов).

Детальная статическая методика оценки рисков и динамическая методика

В рамках детальной статической методики и динамической методики риск предлагается определять на основе классического уравнения для вычисления риска [2]

$$Risk = AttackImpact \times AttackPotentiality,$$

где *AttackImpact* — ущерб от атаки (комбинация разрушительности атаки и критичности актива); *AttackPotentiality* — вероятность атаки.

Риск определяется для узлов графа атак (каждый узел соответствует атакующему действию). Граф атак задается следующим образом: $G = (S, L, Pc)$, где S — множество узлов графа (атакующих действий); L — множество связей ($L \subseteq S \times S$); Pc — дискретные локальные распределения условных вероятностей.

Значение риска варьируется от 0 до 100. При этом риск от 0 до 0,1 принимается низким (т. е. риском можно пренебречь), риск от 0,1 до 1 — средним (меры необходимо принять), риск от 1 до 10 — высоким (меры необходимо принять как можно скорее), а от 10 до 100 — критическим (меры необходимо принять немедленно).

Риск для атаки (последовательности атакующих действий) определяется как произведение минимальной вероятности из узлов атаки на графе на максимальный ущерб; риск для хоста — как максимальный из рисков всех атак, проходящих через хост; риск для КС — как максимальный из рисков хостов.

Предлагаемая авторами методика определения *AttackPotentiality* для узлов графа использует и развивает работы, применяющие байесовские графы атак [15, 8]. Отличиями являются метод формирования графа атак и метод вычисления локальных вероятностей компрометации узлов.

Байесовский граф атак был выбран для интеграции с динамической методикой, так как позволяет учитывать влияние событий на состояние системы и прогнозировать развитие атаки, а также определять предыдущие шаги атаки.

Алгоритм определения *AttackPotentiality* включает три шага: определение локальных вероятностей узлов; определение дискретных условных распределений вероятностей и определение полных вероятностей.

Локальные вероятности компрометации узлов найдем на основе индекса CVSS *Exploitability*:

$$Exploitability = 20 \times AccessVector \times AccessComplexity \times Authentication,$$

где *AccessVector* определяет доступность уязвимости, *AccessComplexity* определяет сложность эксплуатации уязвимости и *Authentication* определяет, требуется ли дополнительная аутентификация при эксплуатации уязвимости [8].

Поскольку предлагаемый граф атак построен таким образом, что переход из состояния в состояние возможен только в случае наличия доступа к соответствующему узлу, переопределим формулу определения *Exploitability* для определения локальной вероятности узла S_i, соответствующего атакующему действию a_i, следующим образом:

$$p(a_i) = 2 \times AccessVector \times AccessComplexity \times \times Authentication,$$

если $S_i \in S_r$, где S_r — множество корневых (входных) узлов графа. В этом случае локальная вероятность успешной компрометации узла может принимать значения от 0,1 до 1,0 (в соответствии с возможными значениями индексов CVSS). Если $S_i \notin S_r$:

$$p(a_i) = 2 \times AccessComplexity \times Authentication.$$

Локальная вероятность успешной компрометации узла может принимать значения от 0,3 до 1,0. Вероятность того, что узел не будет скомпрометирован, определяется как $1 - p(a_i)$.

Для определения условных распределений вероятностей всех узлов $Pc(S_i|Pa(S_i))$ (т. е. вероятностей компрометации узла S_i с учетом различных комбинаций состояний его предков $Pa(S_i)$) применяется обратный обход графа атак в глубину, начиная с терминальных узлов (узлов, у которых нет потомков) и заканчивая узлами, доступными атакующему. Типы связей между узлами-предками учитываются в соответствии с работой [15]. В случае связей типа «И» между узлами-предками (для успешной компрометации узла-потомка необходимо, чтобы все узлы-предки были скомпрометированы)

$$Pc(S_i \mid Pa(S_i)) = \begin{cases} 0, & \exists S_i \in Pa(S_i) \mid S_i = 0 \\ p(S_i), & \text{иначе} \end{cases}.$$

В случае связей типа «ИЛИ» между узлами-предками (для успешной компрометации узла-потомка необходимо, чтобы хотя бы один узел-предок был скомпрометирован)

$$Pc\left(S_i \mid Pa(S_i)\right) = \begin{cases} 0, & \forall S_i \in Pa(S_i) \mid S_i = 0 \\ p(S_i), & \text{иначе} \end{cases}.$$

Безусловные вероятности компрометации узлов графа (вероятности атаки) определяются на основе локальных вероятностей и распределений условных вероятностей по формуле полной вероятности путем маргинализации по известным вероятностям: $Pr(S_1, \ldots, S_n) = \prod_{i=1}^{n} Pc\left(S_i \left| Pa[S_i] \right.\right)$.

Показатель ущерба от атаки (*AttackImpact*) для узла вычисляется на основе критичности актива R_k ($k \in [1, l]$, l — количество всех программных активов организации) и разрушительности соответствующего атакующего действия a_i в результате успешной эксплуатации уязвимости v_i ($i \in [1, m]$, m — множество всех уязвимостей данного актива) путем их перемножения. Критичность актива определяется по параметрам конфиденциальности $cCrit_k$, целостности $iCrit_k$ и доступности $aCrit_k$ так же, как в базовой методике. Разрушительность атакующего действия определяется на основе базовых показателей CVSS в виде вектора $[ConfImpact_{k,i}(c)\ IntegImpact_{k,i}(i)\ AvailImpact_{k,i}(a)]$, где $ConfImpact_{k,i}(c)$ — влияние на конфиденциальность актива R_k в случае успешной реализации атакующего действия a_i, использующего уязвимость v_i; $IntegImpact_{k,i}(i)$ — влияние на целостность актива R_k; $AvailImpact_{k,i}(a)$ — влияние на доступность актива R_k. $ConfImpact_{k,i}(c)$, $IntegImpact_{k,i}(i)$ и $AvailImpact_{k,i}(a)$ могут принимать значения {0,0; 0,275; 0,660} в соответствии с возможными значениями показателей CVSS влияние на конфиденциальность, влияние на целостность и влияние на доступность. Общий ущерб определяется суммированием ущерба по трем свойствам:

$$AttackImpact = cCrit_k \times ConfImpact_{k,i}(c) + + iCrit_k \times IntegImpact_{k,i}(i) + + aCrit_k \times AvailImpact_{k,i}(a).$$

В динамическом случае *AttackPotentiality* для узла S графа определяется с учетом модели инцидента ev, включающей показатель надежности информации $p(ev|S)$, который определяет вероятность того, что инцидент ev действительно произошел. Тогда вероятность того, что узел скомпрометирован, определяется как $p(ev|S)$:

$$p(S \mid ev) = \frac{p(ev \mid S) \times p(ev)}{p(S)} = = \frac{p(ev \mid S) \times \left(p(ev \mid S) \times p(S) + p(ev \mid \neg S) \times p(\neg S) \right)}{p(S)},$$

где $p(S)$ — вероятность компрометации узла до поступления инцидента; $p(ev|\neg S)$ — вероятность того, что инцидент ev не произошел (false positive).

Узел графа, соответствующий инциденту безопасности, определяется на основе следующих шагов: а) определение хоста, для которого обнаружен инцидент; б) определение узлов графа атак, соответствующих данному хосту; в) выделение узлов, дающих привилегии и (или) ведущих к ущербу, соответствующему инциденту безопасности (полученный набор узлов используется для переопределения вероятностей; если ни одного

узла не выбрано, то инцидент определяется как использование уязвимости 0-дня).

Вероятности узлов-потомков путей атак, проходящих через скомпрометированный узел, пересчитываются с учетом новой вероятности компрометации узла, для которого поступил инцидент безопасности.

Прототип и эксперименты

Архитектура прототипа

Разработанные методики реализованы в рамках системы оценивания защищенности КС. Архитектура системы представлена на рис. 2.

Компонент обработки данных получает входные данные от администратора, компонента сбора информации (который получает входные данные от сенсоров, сетевых сканеров, хостовых программных агентов, SIEM-системы и обрабатывает получаемые данные), компонента моделирования атак и генерирует обработанные входные данные. Полученные данные применяются как входные данные для компонента оценки защищенности.

Компонент оценки защищенности включает набор функций, реализующих методики вычисления показателей различного уровня и методику оценки защищенности. При поступлении новых данных показатели пересчитываются.

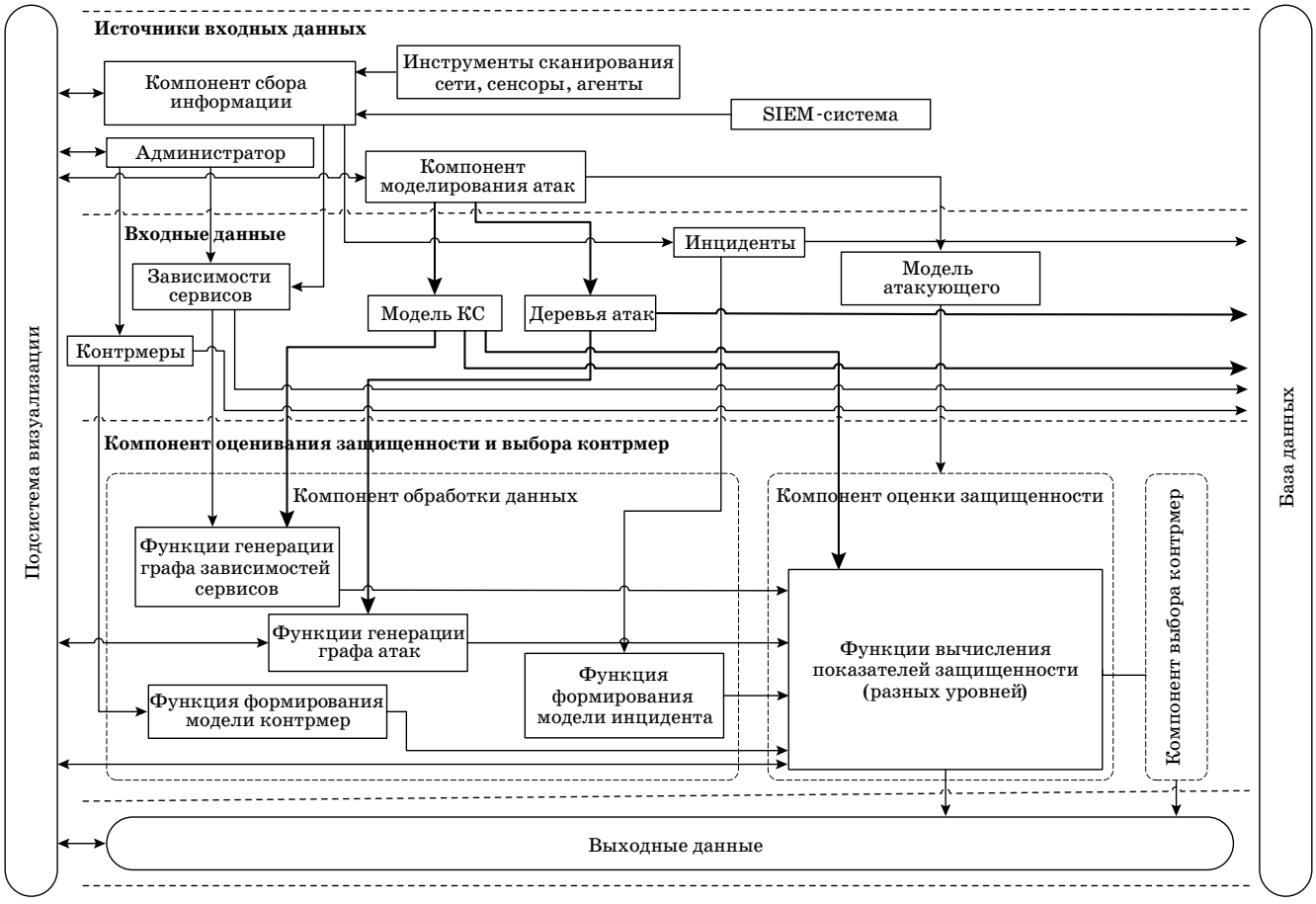
Выходные данные компонента (вычисленные показатели защищенности и оценка риска) передаются системе визуализации и компоненту выбора контрмер.

Прототип был реализован на языке Java с использованием принципов объектно-ориентированного программирования, на Microsoft Windows, Intel Core i7 CPU и 12 GB RAM.

Входные данные

Для проведения экспериментов использовались различные спецификации КС. Одна из спецификаций состояла из 10 хостов (рис. 3).

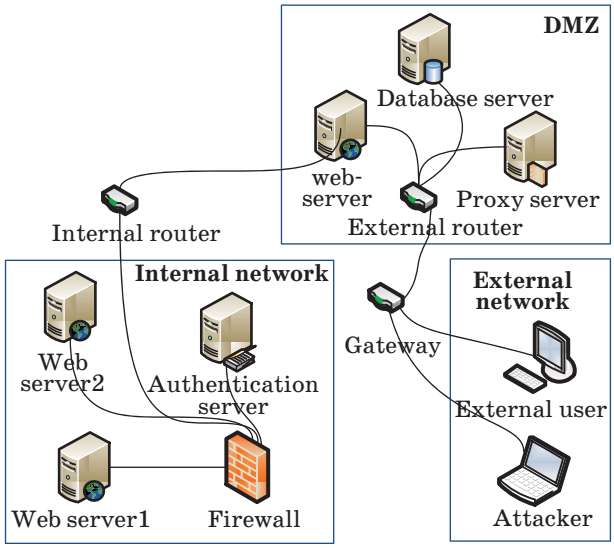
Ресурсы сети и значения их критичности представлены в табл. 2. Значения критичности определены по параметрам конфиденциальности, целостности и доступности на основе критичности бизнес-сервисов и зависимости их свойств безопасности от свойств безопасности программно-аппаратного обеспечения хостов.



■ *Рис. 2.* Архитектура системы оценивания защищенности и выбора контрмер

■ ***Таблица 2.*** Ресурсы тестовой сети и значения критичности

Сервис	Хост	Критичность
Веб-приложение (web application)	Web server1	[10,0 10,0 10,0]
ОС (cpe:/o:microsoft:windows_server_2008::r2:x64)	То же	[10,0 10,0 10,0]
ApacheStruts2 (cpe:/a:apache:struts:2.0.0)	–"–	[7,0 10,0 10,0]
JBoss AS (cpe:/a:redhat:jboss_community_application_server:5.0.1)	– "–	[10,0 10,0 10,0]
port tcp/443	– "–	[0,0 8,0 10,0]
port http/8080	– "–	[0,0 8,0 10,0]
Веб-приложение (web application)	Web server2	[10,0 10,0 10,0]
ApacheStruts2 (cpe:/a:apache:struts:2.0.0)	То же	[7,0 10,0 10,0]
ОС (cpe:/o:microsoft:windows_server_2008::r2:x64)	– "–	[10,0 10,0 10,0]
port http/8080	– "–	[0,0 8,0 10,0]
port tcp/443	– "–	[0,0 8,0 10,0]
JBoss AS (cpe:/a:redhat:jboss_community_application_server:5.0.1)	– "–	[10,0 10,0 10,0]
Сервис аутентификации (authentication service)	Authentication server	[20,0 20,0 20,0]
ОС (cpe:/o:suse:linux_enterprise_server:9)	То же	[20,0 20,0 20,0]
port tcp/ldaps 636	– "–	[0,0 16,0 20,0]
LDAP (slapd service)	– "–	[20,0 20,0 20,0]
ОС (cpe:/o:linux:linux_kernel:2.6.27.33)	DB server	[20,0 20,0 20,0]
SQL (cpe:/a:oracle:mysql:5.5.25)	То же	[20,0 20,0 20,0]
port tcp/443	– "–	[20,0 20,0 20,0]
Citrix (cpe:/a:citrix:ica_client:6.1)	Firewall	[20,0 20,0 20,0]
ОС (cpe:/o:linux:linux_kernel:2.6.27.33)	То же	[20,0 20,0 20,0]



■ ***Рис. 3.*** Топология тестовой сети

Представим результаты экспериментов для внешнего атакующего с высоким уровнем навыков. На рис. 4 изображен граф атакующих действий для тестовой сети в окне интерфейса пользователя программного средства.

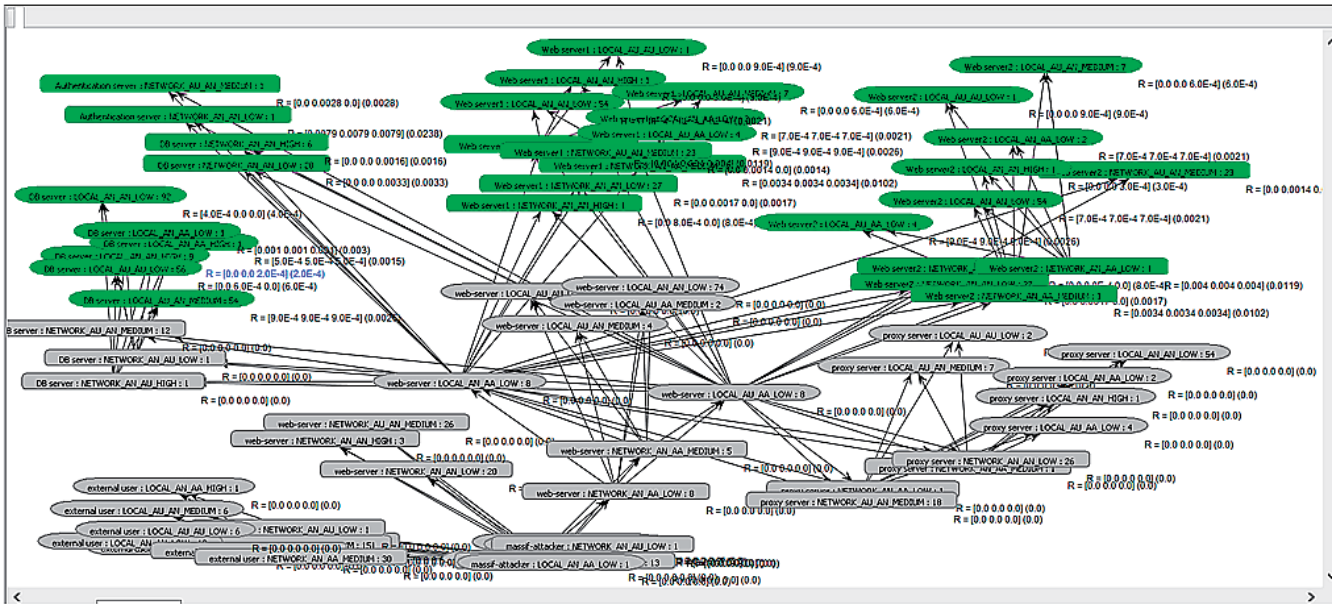
Каждый узел графа соответствует атакующему действию, которое может быть осуществлено путем эксплуатации одной из уязвимостей. Стрелки показывают возможность перехода от одного атакующего действия к другому. Уязвимости объединены в группы по совпадению таких параметров, как вектор доступа к уязвимости (*AccessVector*), требования аутентификации для эксплуатации уязвимости (*Authentication*), сложность доступа к уязвимости (*AccessComplexity*) и привилегии на хосте, получаемые после успешной эксплуатации уязвимости (*GainedPrivileges*). Данные параметры определяются на основе значений в открытой базе уязвимостей NVD [16, 17]. Каждый узел графа в окне интерфейса задан вектором в формате

H_NAME: *AccessVector_Authentication_*

GainedPrivileges_AccessComplexity,

где H_NAME — название хоста.

Для каждого узла отображается значение риска его успешной компрометации R в формате $R = [ConfRisk\ IntegRisk\ AvailRisk]$ (*FullRisk*), где *ConfRisk*, *IntegRisk*, *AvailRisk* — риск нарушения конфиденциальности, целостности и доступности соответственно; *FullRisk* — суммарный риск



■ ***Рис. 4.*** Граф атакующих действий для тестовой сети

по параметрам конфиденциальности, целостности и доступности.

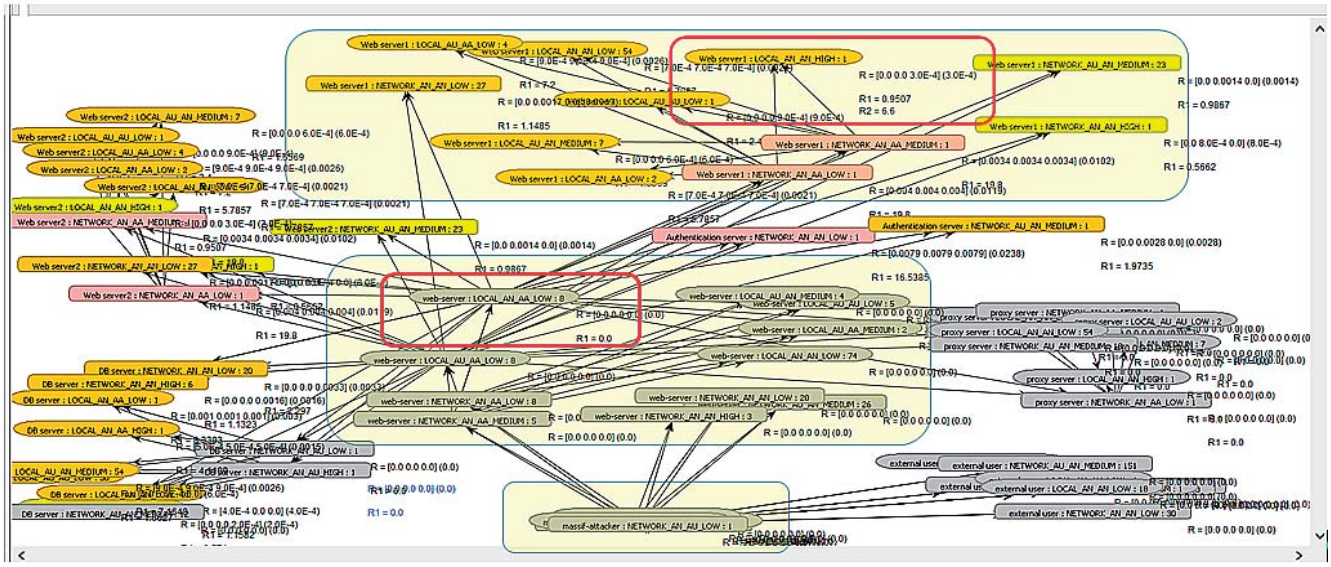
В программном средстве используется цветовая индикация узлов: зеленый — для низкого уровня риска, желтый — для среднего, оранжевый — для высокого и красный — для критического. Серым обозначаются узлы, для которых риск равен 0. Как видно из рисунка, риск находится в пределах нормы (т. е. низкий).

Эксперименты

Для применения динамической методики необходимы данные об инцидентах безопасности. При проведении экспериментов использовались сгенерированные данные, имитирующие реальные последовательности атак и инцидентов в сети на основе шаблонов CAPEC [18] (табл. 3). Это позволило проанализировать реакцию системы на разные типы последовательностей [19].

■ ***Таблица 3.*** Примеры последовательностей атак и инцидентов безопасности для экспериментов

Последовательность атакующих действий	Последовательность инцидентов безопасности
Attacker: CAPEC-170: Web Application Fingerprinting web-server: CAPEC-76: Manipulating Input to File System Calls web-server: CAPEC-224: Fingerprinting Web server1: CAPEC-10_descr Web server1: CAPEC-285: ICMP Echo Request Ping Web server1: CAPEC-10_descr	**Инцидент 1:** хост Attacker CAPEC-10_event **Инцидент 2:** хост Web server1 CAPEC-10_event **Инцидент 3:** хост Web server1 CAPEC-10_event
Attacker: CAPEC-299: TCP SYN Ping web-server: CAPEC-10_descr web-server: CAPEC-300: Port Scanning Web server1: CAPEC-10_descr	**Инцидент 1:** хост web-server CAPEC-10_event **Инцидент 2:** хост Web server1 CAPEC-10_event
Attacker: CAPEC-327: TCP Options Probe Attacker: CAPEC-76: Manipulating Input to File System Calls web-server: CAPEC-139: Relative Path Traversal web-server: CAPEC-328: TCP 'RST' Flag Checksum Probe Web server2: CAPEC-244: Cross-Site Scripting via Encoded URI Schemes Web server2: CAPEC-329: ICMP Error Message Quoting Probe Web server2: CAPEC-45: Buffer Overflow via Symbolic Links	**Инцидент 1:** хост Web server2 CAPEC-45 [An attacker creating or modifying Symbolic links is a potential signal of attack in progress. An attacker deleting temporary files can also be a sign that the attacker is trying to replace legitimate resources with malicious ones.]
Attacker: CAPEC-322: TCP (ISN) Greatest Common Divisor Probe Attacker: CAPEC-10_descr Attacker: CAPEC-323: TCP (ISN) Counter Rate Probe Attacker: CAPEC-76: Manipulating Input to File System Calls web-server: CAPEC-10_descr web-server: CAPEC-324: TCP (ISN) Sequence Predictability Probe Web server2: CAPEC-67: String Format Overflow in syslog() Web server2: CAPEC-325: TCP Congestion Control Flag (ECN) Probe Web server2: CAPEC-78: Using Escaped Slashes in Alternate Encoding	**Инцидент 1:** хост Attacker CAPEC-10_event **Инцидент 2:** хост web-server CAPEC-10_event **Инцидент 3:** хост Web server2 CAPEC-78 [An attacker can use a fuzzer in order to probe for this vulnerability. The fuzzer should generate suspicious network activity noticeable by an intrusion detection system.]



■ ***Рис. 5.*** Фрагмент интерфейса системы оценивания защищенности после поступления инцидентов безопасности

■ ***Таблица 4.*** Значения вероятности и риска для узлов графа после поступления инцидентов

Узел	Нет инцидента		Инцидент 1	
	Вероятность	Риск	Вероятность	Риск
web-server: LOCAL_AN_AA_LOW	0,0023	0,0	1,0	0,0
proxy server: LOCAL_AU_AN_MEDIUM	0,00009	0,0	0,2510	0,0
proxy server: LOCAL_AN_AN_HIGH	0,00005	0,0	0,1440	0,0
Web server1: NETWORK_AN_AN_HIGH	0,0003	0,0008 (низкий)	0,206	0,566 (средний)
Web server1: NETWORK_AU_AN_MEDIUM	0,0005	0,0014 (низкий)	0,3588	0,9867 (средний)
Web server1: NETWORK_AN_AA_MEDIUM	0,0005	0,0102 (низкий)	0,98	19,8 (критический)
Web server1: LOCAL_AN_AN_HIGH*	0,0005	0,0003 (низкий)	0,144	0,95 (средний)
Web server1: LOCAL_AU_AN_MEDIUM	0,00009	0,0006 (низкий)	0,2511	1,6569 (высокий)
Web server1: LOCAL_AN_AN_LOW	0,0001	0,0021 (низкий)	0,2922	5,79 (высокий)
Web server1: LOCAL_AN_AA_LOW	0,0001	0,0021 (низкий)	0,2922	5,79 (высокий)
Web server1: LOCAL_AU_AU_LOW	0,0001	0,0008 (низкий)	0,3636	2,4 (высокий)
Web server1: LOCAL_AU_AA_LOW	0,0001	0,0027 (низкий)	0,3636	7,2 (высокий)
Web server1: NETWORK_AN_AA_LOW	0,0006	0,012 (низкий)	0,98	19,8 (критический)
Web server2: NETWORK_AN_AN_LOW	0,0006	0,0017 (низкий)	0,4176	1,1485 (высокий)
Web server2: LOCAL_AN_AA_LOW	0,00007	0,003 (низкий)	0,2106	8,31 (высокий)
Web server2: LOCAL_AN_AN_HIGH	0,00003	0,0002 (низкий)	0,1038	0,571 (средний)
Web server2: NETWORK_AN_AA_ LOW	0,0006	0,0102 (низкий)	0,98	19,8 (критический)
Web server2: LOCAL_AU_AA_LOW	0,0001	0,0026 (низкий)	0,3636	7,2 (высокий)
Web server2: LOCAL_AU_AU_LOW	0,0001	0,0009 (низкий)	0,3636	2,4 (высокий)
Web server2: NETWORK_AN_AA_MEDIUM	0,0005	0,012 (низкий)	0,98	19,8 (критический)
Web server2: LOCAL_AN_AN_LOW	0,0001	0,0021 (низкий)	0,2922	5,79 (высокий)
DB server: NETWORK_AN_AN_HIGH	0,0003	0,0016 (низкий)	0,2059	1,1323 (высокий)
DB server: LOCAL_AN_AN_LOW	0,00007	0,0004 (низкий)	0,2106	1,1582 (высокий)
DB server: LOCAL_AU_AU_LOW	0,0001	0,0006 (низкий)	0,3023	1,6627 (высокий)
DB server: LOCAL_AU_AN_MEDIUM	0,00006	0,0026 (низкий)	0,1809	7,164 (высокий)
DB server: LOCAL_AN_AA_HIGH	0,000037	0,0015 (низкий)	0,1038	4,11 (высокий)
Authentication server: NETWORK_AU_AN_MEDIUM	0,0005	0,0028 (низкий)	0,3588	1,9735 (высокий)
Authentication server: NETWORK_AN_AN_LOW	0,0006	0,0237 (низкий)	0,4176	16,54 (критический)

* *Примечание*: после поступления второго инцидента значения показателей изменились только для узла Web server1: LOCAL_AN_AN_HIGH: вероятность = 1,0; риск = 6,6 (высокий).

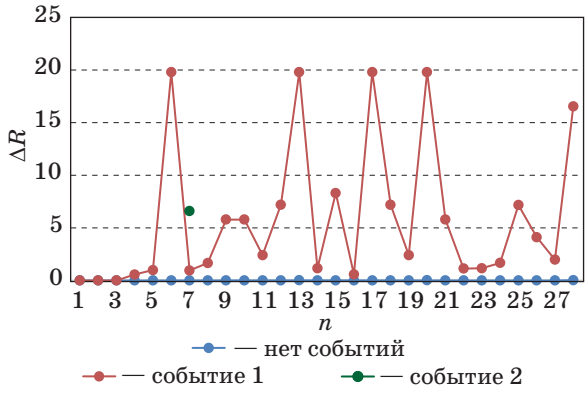
Фрагмент интерфейса системы оценивания защищенности после пересчета значений риска для сгенерированной последовательности атаки и последовательности инцидентов представлен на рис. 5: R обозначает исходное значение риска для узла графа, R_N — значение после обработки N-го инцидента безопасности. Последовательность атаки: CAPEC-299: TCP SYN Ping с хоста Attacker -> CAPEC-10_descr на хосте web-server -> CAPEC-300: Port Scanning на хосте web-server -> CAPEC-10_descr на хосте Web server1, где CAPEC-10_descr — CAPEC-10: Buffer Overflow via Environment Variables на хосте web-server. Узлы графа, соответствующие последовательности атаки, выделены прямоугольниками бледно-желтого цвета. Последовательность инцидентов: Инцидент 1 (хост web-server, шаблон атаки CAPEC-10): CAPEC-10_event -> Инцидент 2 (хост Web server1, шаблон атаки CAPEC-10) CAPEC-10_event, где CAPEC-10_event — «If the application does bound checking, it should fail when the data source is larger than the size of the destination buffer. If the application's code is well written, that failure should trigger an alert». Узлы графа, на которые отображены инциденты безопасности, выделены красной рамкой.

Новые значения вероятности и риска для узлов графа после поступления инцидентов приведены в табл. 4. Учет инцидентов безопасности позволяет зафиксировать повышение риска для узла Web server1 с низкого до критического, когда необходимо срочно приводить в действие контрмеры.

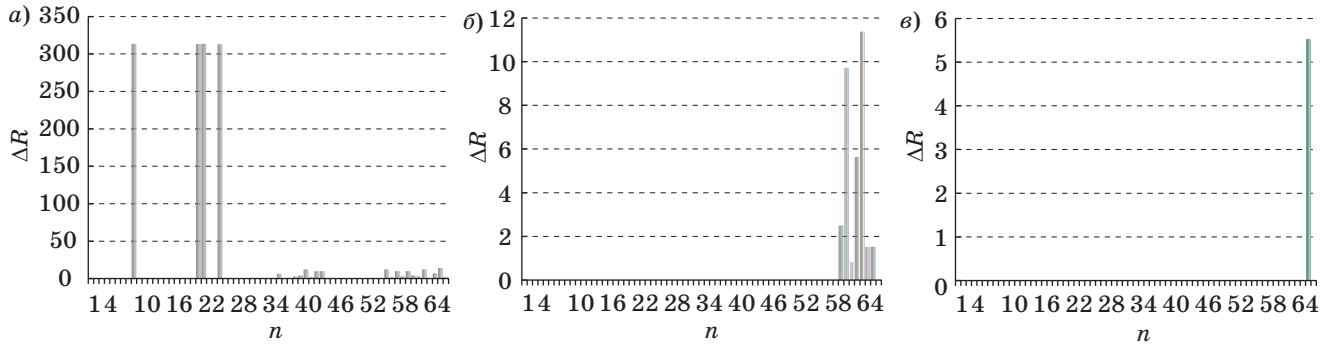
Сравнение с посланной на вход инструмента оценивания защищенности атакой показывает, что для узлов, входящих в атаку, уровень риска вырос как минимум до среднего (см. рис. 5). При этом важно отметить, что точность локализации атаки зависит от количества узлов графа (а соответственно, хостов сети), находящихся на одном уровне поддерева (в одной подсети). Для более точного определения цели атаки можно использовать различные характеристики атакующего. Тем не менее для проведенных экспериментов реально атакуемые узлы попадают во множество узлов, для которых выросло значение риска, что позволяет эффективно применять контрмеры на уровне подсети. Точность повышается при поступлении новых инцидентов безопасности, но она также зависит от внешнего фактора (точности поступившего инцидента).

На рис. 6 приведены значения риска для обрабатываемых узлов графа атак (в соответствии с табл. 4) до поступления инцидентов (синяя кривая), после поступления первого инцидента (красная кривая) и после поступления второго инцидента (зеленая точка), когда риск изменяется только для одного узла. Реально атакованные узлы Web server1 (точки *4–13*) имеют высокий уровень риска. При этом узел web-server (точка *1*) имеет низкий уровень риска, что объясняется его низкой критичностью.

Изменение значений риска в результате проведения различных атак на хосты сети показано на рис. 7: видно существенное изменение уровня риска для ряда узлов после поступления первого инцидента (рис. 7, *а*); после поступления второго инцидента количество узлов, для которых изменилось значение риска, основательно снизилось,



■ ***Рис. 6.*** График изменения значений риска ΔR для узлов графа n после поступления последовательности инцидентов безопасности



■ ***Рис. 7.*** График изменения значений риска ΔR для узлов графа n после поступления первого (*а*), второго (*б*) и третьего (*в*) инцидентов безопасности для различных атак на хосты сети

и можно локализовать узел, на который нацелена атака (рис. 7, *б*); после третьего инцидента количество затронутых узлов уменьшилось еще заметнее (рис. 7, *в*). Таким образом, уровень риска позволяет отследить наиболее критичные узлы сети, а изменение уровня риска позволяет локализовать цель атаки.

Так же, как и для атаки из примера на рис. 6, полученные оценки рисков сравнивались с реально атакованными узлами. Сравнение показало, что атакованным узлам назначаются высокие оценки, точность совпадения зависит от количества инцидентов, расположения атакованных хостов в сети, точности информации о поступающих событиях.

Таким образом, эксперименты подтвердили, что дополнительная информация влияет на изменение уровня риска и позволяет локализовать узлы для реализации контрмер.

В отличие от аналогичных работ в этой области, инструмент использует комплекс показателей, позволяющих учесть при оценке риска большее количество параметров. Так, подходы на основе вероятностей атак [7, 8] не учитывают зависимости между критичностью ресурсов и навыки атакующего; подходы, учитывающие возможный ущерб от атак [9, 10], не рассматривают вероятность атаки; подходы, учитывающие возможные финансовые потери [12], обычно не используют детальную оценку рисков. В предлагаемом инструменте мы попытались объединить достоинства всех перечисленных подходов, чтобы более точно отразить ситуацию для последующего рационального выбора контрмер.

Заключение

В работе предлагается компонент оценки рисков, интегрированный с SIEM-системой. Компонент реализует комплекс методик оценки рисков, основанных на показателях защищенности. Описываются некоторые особенности вычисления показателей. Описывается обобщенная архитектура программного компонента и элементы его интерфейса. Проведены эксперименты с использованием разработанного программного средства, демонстрирующие работу методик. По результатам экспериментов выделены достоинства и недостатки предложенных методик. Подтверждено влияние дополнительных данных на точность оценок. Приведено краткое сравнение с аналогичными подходами.

В будущем планируется детальнее рассмотреть характеристики и мотивацию различных типов атакующих для повышения точности оценки рисков.

Работа выполнена при финансовой поддержке РФФИ (проекты № 14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338) и при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007.

Литература

1. ГОСТ Р ИСО/МЭК 27004–2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. — Введ. 2011-12-01. — М.: Стандартинформ, 2012. — 56 с.
2. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. — Введ. 2010-11-30. — М.: Стандартинформ, 2011. — 47 с.
3. ISO/IEC 27005:2011. Information Technology. Security Techniques. Information Security Risk Management (second edition). — Switzerland: ISO/IEC, 2011. — 68 p.
4. ISO/IEC 27035:2011. Information Technology. Security Techniques. Information Security Incident Management. — Switzerland: ISO/IEC, 2011. — 78 p.
5. The Center for Internet Security. The CIS Security Metrics, 2009. https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf (дата обращения: 28.09.2016).
6. **Singhal A., Ou X.** Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs // NIST Interagency Report 7788. Gaithersburg, Aug. 2011, National Institute of Standards and Technology. — 24 p.
7. **Chunlu W., Yancheng W., Yingfei D., Tianle Z.** A Novel Comprehensive Network Security Assessment Approach // IEEE Intern. Conf. on Communications. IEEE, 2011. P. 1–6.
8. **Poolsappasit N., Dewri R., Ray I.** Dynamic Security Risk Management Using Bayesian Attack Graphs // IEEE Transactions on Dependable and Security Computing. 2012. Vol. 9. N 1. P. 61–74.
9. **Kheir N., Cuppens-Boulahia N., Cuppens F., Debar H.** A Service Dependency Model for Cost-Sensitive Intrusion Response // ESORICS'10. 2010. P. 626–642.
10. **Wu Y.-S.,** et al. Automated Adaptive Intrusion Containment in Systems of Interacting Services Computer Networks/ Y.-S. Wu, B. Foo, Y.-C. Mao, S. Bagchi, E. H. Spafford// The Intern. Journal of Computer and Telecommunications Networking. 2007. Vol. 51. P. 1334–1360.
11. **Manadhata P. K., Wing J. M.** An Attack Surface Metric // IEEE Transactions on Software Engineering. 2010. P. 371–386.
12. **Cremonini M., Martini P.** Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA) // Proc. of Fourth

Workshop on the Economics of Information Security, June 2–3, 2005. http://www.infosecon.net/workshop/pdf/23.pdf (дата обращения: 28.09.2016).
13. **Котенко И. В., Дойникова Е. В.** Методика выбора контрмер на основе комплексной системы показателей защищенности в системах управления информацией и событиями безопасности // Информационно-управляющие системы. 2015. № 3. С. 60–69. doi:10.15217/issn1684-8853.2015.3.60
14. **Mell P., Scarfone K.** A Complete Guide to the Common Vulnerability Scoring SystemVersion 2.0. 2007. https://www.first.org/cvss/cvss-v2-guide.pdf (дата обращения: 28.09.2016).
15. **Frigault M., Wang L., Singhal A. and Jajodia S.** Measuring Network Security Using Dynamic Bayesian Network // 2008 ACM Workshop on Quality of Protection, Oct. 2008. P. 23–30.
16. NVD website. https://nvd.nist.gov/ (дата обращения: 30.06.2016).
17. **Федорченко А. В., Чечулин А. А., Котенко И. В.** Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей // Информационно-управляющие системы. 2014. № 5. С. 72–79.
18. Common Attack Pattern Enumeration and Classification (CAPEC). https://capec.mitre.org (дата обращения: 30.06.2016).
19. **Kotenko I. and Doynikova E.** The CAPEC based Generator of Attack Scenarios for Network Security Evaluation // Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2015): proc. of the IEEE 8th Intern. Conf., Warsaw, Poland, Sept. 24–26, 2015. P. 436–441.

UDC 004.056
doi:10.15217/issn1684-8853.2016.5.54

Techniques and Software Tool for Risk Assessment on the Base of Attack Graphs in Information and Security Event Management Systems

Doynikova E. V.[a], Researcher, doynikova@comsec.spb.ru
Kotenko I. V.[a], Dr. Sc., Tech., Professor, ivkote@comsec.spb.ru
[a]Saint-Petersburg Institute for Informatics and Automation of the RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation

Introduction: The problem of response to computer attacks is still very important. Information technologies are used everywhere, computer networks become more complex and huge, therefore the number of computer threats always stays large. The procedures of security assessment and countermeasure selection should be constantly improved. Accurate and comprehensive risk analysis providing a valid and valuable assessment is crucial for giving the best response to an attack. Though researches have suggested a number of various approaches, a universal solution has not been found yet. **Purpose:** The goal is to develop risk assessment techniques which would accurately reflect the current security situation on the base of the available security data automatically processed, in order to develop a software tool implementing these techniques, and to evaluate their efficiency on experimental basis. **Results:** Techniques for security assessment have been developed and implemented as a software tool. The developed techniques are based on the complex system of security metrics suggested earlier by the authors. Some technique-specific aspects of calculating the security metrics have been reconsidered. The developed software tool allows you to choose a technique according to the current situation and user's demands. The techniques have been tested, and their advantages and disadvantages have been outlined. **Practical relevance:** The developed techniques and software tool can enhance information system security by providing valid and valuable assessment of the current security situation.
Keywords — Risk Assessment Technique, Security Metrics, Attack Graph, Service Dependency Graph, Security Incidents.

References

1. State Standard R ISO/IEC 27004–2011. Information Technology. Security Techniques. Information Security Management. Measurement. Moscow, Standartinform Publ., 2012. 56 p. (In Russian).
2. State Standard R ISO/IEC 27005–2010. Information Technology. Security Techniques. Information Security Risk Management. Moscow, Standartinform Publ., 2011. 47 p. (In Russian).
3. ISO/IEC 27005:2011. Information Technology. Security Techniques. Information Security Risk Management (second edition). Switzerland, ISO/IEC, 2011. 68 p.
4. ISO/IEC 27035:2011. Information Technology. Security Techniques. Information Security Incident Management. Switzerland, ISO/IEC, 2011. 78 p.
5. *The Center for Internet Security. The CIS Security Metrics.* 2009. Available at: https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf (accessed 28 September 2016).
6. Singhal A., Ou X. *Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs.* NIST Interagency Report 7788. Gaithersburg, National Institute of Standards and Technology, 2011. 24 p.
7. Chunlu W., Yancheng W., Yingfei D., Tianle Z. A Novel Comprehensive Network Security Assessment Approach. *Proc. of the IEEE International Conference on Communications*, Kyoto, 2011, IEEE, pp. 1–6.
8. Poolsappasit N., Dewri R., Ray I. Dynamic Security Risk Management using Bayesian Attack Graphs. *Proc. IEEE Transactions on Dependable and Security Computing*, 2012, vol. 9, no. 1, pp. 61–74.
9. Kheir N., Cuppens-Boulahia N., Cuppens F., Debar H. A Service Dependency Model for Cost-Sensitive Intrusion Response. *Proc. ESORICS'10*, 2010, pp. 626–642.
10. Wu Y.-S., Foo B., Mao Y.-C., Bagchi S., Spafford E. H. Automated Adaptive Intrusion Containment in Systems of Interacting Services Computer Networks. *The International Journal of Computer and Telecommunications Networking*, 2007, vol. 51, pp. 1334–1360.
11. Manadhata P. K., Wing J. M. An Attack Surface Metric. *Proc. IEEE Transactions on Software Engineering*, 2010, pp. 371–386.
12. Cremonini M., Martini P. Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). *Proc. Fourth Workshop on the Economics of*

Information Security, 2005. Available at: http://www.infosecon.net/workshop/pdf/23.pdf (accessed 28 September 2016).
13. Kotenko I. V. and Doynikova E. V. Countermeasure Selection in Security Management Systems. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 3, pp. 60–69 (In Russian). doi:10.15217/issn1684-8853.2015.3.60
14. Mell P., Scarfone K. *A Complete Guide to the Common Vulnerability Scoring SystemVersion 2.0*. 2007. Available at: https://www.first.org/cvss/cvss-v2-guide.pdf (accessed 28 September 2016).
15. Frigault M., Wang L., Singhal A. and Jajodia S. Measuring Network Security Using Dynamic Bayesian Network. *Proc. 2008 ACM Workshop on Quality of Protection*, 2008, pp. 23–30.
16. *NVD website*. Available at: https://nvd.nist.gov/ (accessed 30 June 2016).
17. Fedorchenko A. V., Chechulin A. A., Kotenko I. V. Open Vulnerability Bases and their Application in Security Analysis Systems of Computer Networks. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 5, pp. 72–79 (In Russian).
18. *Common Attack Pattern Enumeration and Classification (CAPEC)*. Available at: https://capec.mitre.org (accessed 30 June 2016).
19. Kotenko I. and Doynikova E. The CAPEC based Generator of Attack Scenarios for Network Security Evaluation. *Proc. IEEE 8th International Conference "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications" (IDAACS'2015)*, Warsaw, Poland, 2015, pp. 436–441.

Уважаемые авторы!

При подготовке рукописей статей необходимо руководствоваться следующими рекомендациями.

Статьи должны содержать изложение новых научных результатов. Название статьи должно быть кратким, но информативным. В названии недопустимо использование сокращений, кроме самых общепринятых (РАН, РФ, САПР и т. п.).

Объем статьи (текст, таблицы, иллюстрации и библиография) не должен превышать эквивалента в 20 страниц, напечатанных на бумаге формата А4 на одной стороне через 1,5 интервала Word шрифтом Times New Roman размером 13, поля не менее двух сантиметров.

Обязательными элементами оформления статьи являются: индекс УДК, заглавие, инициалы и фамилия автора (авторов), ученая степень, звание (при отсутствии — должность), полное название организации, аннотация и ключевые слова на русском и английском языках, электронные адреса авторов, которые по требованию ВАК должны быть опубликованы на страницах журнала. При написании аннотации не используйте аббревиатур и не делайте ссылок на источники в списке литературы.

Статьи авторов, не имеющих ученой степени, рекомендуется публиковать в соавторстве с научным руководителем, наличие подписи научного руководителя на рукописи обязательно; в случае самостоятельной публикации обязательно предоставляйте заверенную по месту работы рекомендацию научного руководителя с указанием его фамилии, имени, отчества, места работы, должности, ученого звания, ученой степени — эта информация будет опубликована в ссылке на первой странице.

Формулы набирайте в Word, не используя формульный редактор (Mathtype или Equation), при необходимости можно использовать формульный редактор; для набора одной формулы не используйте два редактора; при наборе формул в формульном редакторе знаки препинания, ограничивающие формулу, набирайте вместе с формулой; для установки размера шрифта никогда не пользуйтесь вкладкой Other…, используйте заводские установки редактора, не подгоняйте размер символов в формулах под размер шрифта в тексте статьи, не растягивайте и не сжимайте мышью формулы, вставленные в текст; в формулах не отделяйте пробелами знаки: + = −.

Для набора формул в Word никогда не используйте Конструктор (на верхней панели: «Работа с формулами» — «Конструктор»), так как этот ресурс предназначен только для внутреннего использования в Word и не поддерживается программами, предназначенными для изготовления оригинал-макета журнала.

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

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

— рисунки, графики, диаграммы, блок-схемы предоставляйте в виде отдельных исходных файлов, поддающихся редактированию, используя векторные программы: Visio 4, 5, 2002-2003 (*.vsd); Coreldraw (*.cdr); Excel (*.xls); Word (*.doc); AdobeIllustrator (*.ai); AutoCad (*.dxf); Matlab (*.ps, *.pdf или экспорт в формат *.ai);

— если редактор, в котором Вы изготавливаете рисунок, не позволяет сохранить в векторном формате, используйте функцию экспорта (только по отношению к исходному рисунку), например, в формат *.ai, *.esp, *.wmf, *.emf, *.svg;

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

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

В редакцию предоставляются:

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

— экспертное заключение.

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

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

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

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

— при использовании web-материалов указывайте адрес сайта и дату обращения.

Список литературы оформляйте двумя отдельными блоками по образцам lit.dot на сайте журнала (http://i-us.ru/paperrules) по разным стандартам: Литература — СИБИД РФ, References — один из мировых стандартов.

Более подробно правила подготовки текста с образцами изложены на нашем сайте в разделе «Оформление статей».

Контакты
Куда: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Кому: Редакция журнала «Информационно-управляющие системы»
Тел.: (812) 494-70-02
Эл. почта: ius.spb@gmail.com
Сайт: www.i-us.ru

УДК 004.056
doi:10.15217/issn1684-8853.2016.5.66

СОВМЕЩЕНИЕ ПОЛИТИК БЕЗОПАСНОСТИ, ОСНОВАННОЕ НА АЛГОРИТМАХ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

С. В. Белим[a], *доктор физ.-мат. наук, профессор*
Н. Ф. Богаченко[a], *канд. физ.-мат. наук, доцент*
Ю. С. Ракицкий[a], *канд. техн. наук, доцент*
[a]*Омский государственный университет им. Ф. М. Достоевского, Омск, РФ*

Введение: *проблема совмещения нескольких политик безопасности в одной информационной среде является актуальной задачей администрирования компьютерных систем. Современные стандарты защиты информации в автоматизированных системах требуют наличия как минимум двух политик безопасности. Большинство предлагаемых методов решения задачи совмещения политик безопасности сводится к поиску идеального подхода, при котором настройки всех совместно используемых политик безопасности не противоречат друг другу. На практике не всегда удается найти такие настройки, кроме того, отсутствует доказательство самого факта существования идеального подхода. Одним из перспективных путей поиска ответов на поставленные вопросы является методика, основанная на алгоритмах поддержки принятия решений.* ***Результаты:*** *предложен алгоритм совмещения нескольких политик безопасности, который для каждого запроса на доступ принимает решение о том, какая политика безопасности будет задействована. Алгоритм использует взвешенную сумму уровней разрешения отдельных политик безопасности и метод анализа иерархий. Представлены формулы расчета уровня разрешения запрашиваемого доступа для дискреционной и мандатной политик безопасности. В дискреционной политике уровень разрешения запрашиваемого доступа определяется такими числовыми характеристиками, как общее число разрешенных прав доступа, число запрашиваемых прав доступа, число запрещенных прав доступа. Для мандатной политики вычисление уровня разрешения запрашиваемого доступа зависит от типа используемой решетки ценностей. Метод анализа иерархий находит свое применение, когда в системе действует две пары политик безопасности: одна связана с конфиденциальностью, другая — с целостностью. Предложено два дерева решения метода анализа иерархий для расчета итогового уровня разрешения запрашиваемого доступа.* ***Практическая значимость:*** *наличие весовых коэффициентов в предложенном алгоритме совмещения нескольких политик безопасности позволяет осуществлять настройку степени влияния тех или иных правил безопасности для перекрытия различных каналов утечки информации. Представленный подход может быть полезен при построении информационных систем с собственной подсистемой безопасности и проектировании дополнительных систем защиты информации.*

Ключевые слова *— совмещение политик безопасности, уровень разрешения, алгоритм принятия решений, метод анализа иерархий.*

Введение

Проблема совмещения различных политик безопасности возникает достаточно часто при администрировании компьютерных систем. Стандарты защиты информации в автоматизированных системах подразумевают наличие более одной политики разграничения доступа. Так, в «Оранжевой книге» использование только дискреционного разделения доступа относит компьютерную систему к одному из классов безопасности группы «С», тогда как добавление мандатного контроля доступа позволяет претендовать на более высокий класс защищенности группы «В». Причем «Оранжевой книгой» подразумевается именно добавление мандатной политики безопасности (МПБ) с сохранением возможностей дискреционной политики безопасности (ДПБ). В качестве еще одного примера совмещения политик безопасности можно привести системы управления базами данных, функционирующие на базе операционных систем семейства Windows. В системах управления базами данных наиболее распространенной является ролевая политика безопасности, но при этом данные хранятся в файлах, доступ к которым разграничивается операционной системой. В операционных системах базовой является ДПБ, но при этом реализуется на определенном уровне МПБ. Таким образом, требуется сопряжение трех различных политик безопасности.

Стандартным подходом является поиск идеального решения, при котором настройки одной политики безопасности не противоречат настройкам другой политики безопасности. В настоящее время предложен ряд различных решений. Работы [1, 2] посвящены совместной реализации ролевой и мандатной концепций разграничения доступа. Теоретико-графовый подход к решетке ценностей МПБ позволил совместить требования на орграф сущностей компьютерной системы и со стороны ролевой, и со стороны мандатной моделей. Предложен алгоритм создания политики безопасности, включающей в себя мандатное и ролевое разграничения доступа. Авторы работы [3] предлагают изменить базовые координаты матрицы доступов: правила доступа устанавливаются не между субъектом и объектом,

а между «субъектом доступа, запрашивающим доступ к объекту», и «субъектом доступа, создавшим этот объект». Показано, что такой подход позволяет дискреционный и мандатный механизмы контроля доступа использовать совместно. В работе [4] рассмотрено расширение дискреционной модели Take-Grant, учитывающее механизм мандатного разграничения доступа. В статье [5] предложен универсальный язык, позволяющий описать и реализовать глобальную комплексную политику безопасности для системы, состоящей из различных информационных сред, каждая из которых имеет собственную модель обеспечения безопасности и домен администрирования. Этот язык реализуется монитором событий. Конфликты между политиками безопасности разрешаются путем явного вызова администратора для принятия приоритетного решения. В работе [6] матрицу доступов ДПБ предлагается расширить до куба доступов, в котором помимо традиционных субъектов и объектов добавлена третья размерность — пользователи или группы пользователей. Эта дополнительная размерность позволяет организовать механизм группового управления доступом, оставаясь в рамках ДПБ. В работе [7] представлена модель управления доступом для работы с XML-документами. В этой модели комбинируются преимущества ролевой и мандатной политик разграничения доступа. В частности, для определения прав доступа предлагается использовать не списки управления доступом, а подход, основанный на метках безопасности.

Однако есть принципиальная проблема реализации идеального подхода, состоящая в отсутствии доказательства того, что идеальное решение существует. Более того, практическая реализация одновременного администрирования нескольких политик безопасности показывает, что не всегда удается добиться настроек, обеспечивающих правильное функционирование системы. Данная статья посвящена новому подходу к совмещению нескольких политик безопасности в одной компьютерной системе, основанному на алгоритмах поддержки принятия решений.

Постановка задачи и общий подход к решению

Рассмотрим систему, в которой одновременно реализованы дискреционная и мандатная политики безопасности. Согласно общепринятому мнению, которое получило воплощение практически во всех стандартах информационной безопасности, МПБ обеспечивает более высокий уровень защиты информации и доминирует над ДПБ, которая обеспечивает базовый уровень защиты данных. При возникновении противоречий между настройками двух политик безопасности традиционно используется два подхода. Согласно первому подходу доступ запрещен, если он запрещен хотя бы одной политикой безопасности. Во втором случае МПБ занимает доминирующее положение, и решение о разрешении доступа принимается исходя из ее настроек. Первый подход легко приводит к полной неработоспособности системы, второй — практически к выключению ДПБ. Более того, МПБ ориентирована на систему в целом. Администратор определяет метки безопасности субъектов и объектов системы, которые могут изменяться только при смене состояния системы в целом, но не в отдельно взятом доступе. Тем не менее возможны исключительные ситуации. Например, администратору необходимо разрешить доступ конкретного субъекта к конкретному объекту, противоречащий МПБ. Администратор следит за содержимым объекта и может гарантировать отсутствие утечки информации через данный субъект, но не может дать гарантии отсутствия утечки через другие субъекты с тем же уровнем доступа. Данное разрешение может быть реализовано с помощью введения некоторых дополнительных меток безопасности для каждого конкретного случая, что приводит к существенному увеличению и запутыванию решетки ценностей и, как следствие, усложнению администрирования системы. Другой подход состоит в привлечении ДПБ, которая в одном заданном случае должна доминировать над МПБ. Другими словами, в системе может быть реализована надстройка, которая принимает решение о доминировании той или иной политики безопасности в каждом конкретном случае.

Сформулируем постановку задачи более строго. Пусть в системе действует две политики безопасности, которые принимают решения на основе алгоритмов S_1 и S_2. Необходимо реализовать алгоритм S, который для каждого запроса на доступ будет принимать решение о том, какая политика безопасности будет задействована. Следует отметить, что использование алгоритма S действительно необходимо только в том случае, когда решения, принимаемые S_1 и S_2, противоречат друг другу.

Традиционно в рамках политики безопасности на запрос о доступе принимается решение из множества $\{0, 1\}$, в котором нулевое значение соответствует отказу в доступе, а единичное — разрешению доступа. Для принятия решения о возможности доступа расширим область значений алгоритма принятия решения заданной политики безопасности до множества $\{-T, ..., -1, 0, 1, ..., T\}$, где T — целое положительное число. Значения из данного интервала будем называть *уровнем разрешения* и обозначать

буквой t. Доступ разрешен, если $t \geq 0$. Чем выше уровень разрешения t, тем выше уровень доверия к доступу. Таким образом, уровень разрешения можно связать с вероятностью утечки информации при заданном доступе: чем выше вероятность p, тем меньше должен быть уровень разрешения t. С другой стороны, количественная оценка уровня разрешения t — это в некотором роде априорная информация о возможности утечки информации при запрашиваемом доступе. В первом приближении $p = 0{,}5 - (t \,/\, 2T)$.

При изложенном подходе решение о предоставлении доступа той или иной политикой безопасности (тем или иным алгоритмом) сводится к вычислению соответствующего уровня разрешения. При этом алгоритму S необходимо принимать решение t исходя из уровней разрешения t_1 и t_2 отдельных политик безопасности S_1 и S_2. Введем коэффициент доминирования r, показывающий, во сколько раз решение, принимаемое политикой безопасности S_1, более значимо, чем решение, принимаемое политикой S_2. В этом случае окончательное решение может быть вычислено как взвешенная сумма решений двух политик безопасности:

$$t = \frac{r}{r+1} t_1 + \frac{1}{r+1} t_2. \qquad (1)$$

Равнозначность политик безопасности достигается при $r = 1$. Следует отметить, что t не обязательно является целым числом: $t \in [-T, T]$.

Совмещение мандатной и дискреционной политик безопасности

Рассмотрим наиболее распространенный случай совмещения мандатной и дискреционной политик безопасности.

Для МПБ ограничимся простейшим вариантом линейной решетки ценностей с L уровнями безопасности. Тогда уровень разрешения может быть найден как разность между уровнем доверия субъекта $C(S)$ и уровнем секретности объекта $C(O)$:

$$t_1 = \big(C(S) - C(O)\big) \frac{T}{L-1}. \qquad (2)$$

Поскольку $C : S \cup O \to \{0, \ldots, L-1\}$ (S — множество субъектов, O — множество объектов), то $t_1 \in [-T, T]$.

Для ДПБ уровень разрешения может устанавливаться произвольно администратором для каждого доступа. Если администратор хочет присвоить доступу высший приоритет, то он назначает $t_2 = T$. Поэтому ограничимся случаем назначения уровня разрешения по умолчанию. Будем считать, что общее количество возможных видов доступа равно M. Пусть субъект запрашивает доступ к объекту по нескольким видам доступа. В случае запрета доступа будем считать, что

$$t_2 = -k \frac{T}{M}, \qquad (3)$$

где k — количество запрещенных доступов из списка запрашиваемых доступов. Если доступ разрешен, то положим

$$t_2 = h \frac{T}{M}, \qquad (4)$$

где h — количество разрешенных, но не запрашиваемых видов доступа.

Пример 1. Рассмотрим модельный пример функционирования такой системы. Положим $T = 4$. Пусть МПБ строится на основе линейной решетки ценностей с пятью уровнями: $SL = \{0, 1, 2, 3, 4\}$. Для ДПБ определены четыре вида доступа: $R = \{r, w, a, f\}$. В некоторый момент времени поступает запрос на доступ (S, O, r), которому в матрице доступов соответствует ячейка $\mathbf{M}[S, O] = \{r, w, a\}$, уровень секретности объекта $C(O) = 2$, уровень доверия субъекта $C(S) = 1$. В этом случае $t_1 = C(S) - C(O) = -1$, $t_2 = 2$. При равноправии политик безопасности по формуле (1) получаем $t = 1/2 > 0$, т. е. доступ разрешен, несмотря на запрет МПБ. Если же повысить приоритет МПБ в 3 раза, согласно формуле (1): $t = -1/4 < 0$. В этом случае доступ будет запрещен.

При совмещении мандатной и дискреционной политик безопасности был рассмотрен простейший случай линейной решетки ценностей. Однако в реальных системах МПБ может быть задана нелинейной решеткой ценностей, т. е. множество меток безопасности будет являться частично упорядоченным. При таком подходе к реализации политик безопасности может возникнуть ситуация, при которой уровень доверия субъекта $C(S)$ и уровень секретности объекта $C(O)$ окажутся несравнимыми. В этом случае определить уровень разрешения как разность между уровнем доверия субъекта $C(S)$ и уровнем секретности объекта $C(O)$ [см. формулу (2)] нельзя. Это означает, что нужен другой подход к определению уровня разрешения, задаваемого МПБ.

Классическая модель МПБ определяет оператор $\sup(\cdot,\cdot)$, задающий для любой пары элементов l_1 и l_2 из базового множества уровней безопасности SX единственный элемент наименьшей верхней границы: $\sup(l_1, l_2) = l$ тогда и только тогда, когда $(l_1 \leq l) \wedge (l_2 \leq l) \wedge (\forall l' \in SX: ((l_1 \leq l') \wedge (l_2 \leq l')) \Rightarrow (l \leq l'))$.

Введем оператор $\mathrm{dif}(\cdot,\cdot)$, показывающий «расстояние» от уровня безопасности l_1 до наименьшей верхней границы уровней безопасности l_1, l_2: $\mathrm{dif}(l_1, \sup(l_1, l_2)) = \sup(l_1, l_2) - l_1$. Такой подход возможен, поскольку элементы решетки l_1 и $\sup(l_1, l_2)$ будут всегда сравнимы по определению. Данный оператор позволяет определить количе-

ство уровней решетки ценностей от элемента l_1 до $\sup(l_1, l_2)$. Отметим, что данная величина всегда будет неотрицательной.

Будем определять уровень разрешения t_1 для несравнимых в решетке уровня доверия субъекта $C(S)$ и уровня секретности объекта $C(O)$ как отрицательный модуль разностей расстояний уровня доверия субъекта $C(S)$ и уровня секретности объекта $C(O)$ до наименьшей верхней границы $\sup(C(S), C(O))$:

$$t_1 = -1 \cdot \left| \left(\mathrm{dif}\left(C(S), \sup\left(C(S), C(O)\right)\right) - \right.\right. \\ \left.\left. - \mathrm{dif}\left(C(O), \sup\left(C(S), C(O)\right)\right)\right)\right| \frac{T}{H}, \quad (5)$$

где H — максимальное значение оператора dif. Очевидно, что $0 \le H \le (L-1)$, $L = |SX|$.

Когда уровень доверия субъекта $C(S)$ и уровень секретности объекта $C(O)$ являются несравнимыми, доступ не предоставляется, поэтому величина должна быть отрицательной. При этом, поскольку определяется разность «расстояний» между уровнями в решетке, вычисляется абсолютное значение разности.

Пример 2. Пусть МПБ строится на основе нелинейной решетки ценностей с восемью уровнями секретности: $SX = \{0, 1a, 1b, 1c, 2ab, 2c, 3, 4\}$. При этом $0 \le 1a$, $0 \le 1b$, $0 \le 1c$ (уровни $1a$, $1b$, $1c$ несравнимы), $1a \le 2ab$, $1b \le 2ab$, $1c \le 2c$ (уровни $2ab$, $2c$ несравнимы), $2ab \le 3$, $2c \le 3$, $3 \le 4$. Несложно проверить, что $H = 3$. Пусть поступает запрос на доступ субъекта S к объекту O, $C(O) = 1c$, $C(S) = 2ab$. В этом случае $\sup(C(S), C(O)) = 3$, $\mathrm{dif}(C(S), \sup(C(S), C(O))) = 1$, $\mathrm{dif}(C(O), \sup(C(S), C(O))) = 2$. При $T = 3$ по формуле (5) получаем $t_1 = -1 \cdot |1 - 2| = -1$.

Обобщая предложенные правила вычисления уровней разрешения, приведем схему алгоритма S, который для каждого запроса на доступ принимает решение о предоставлении доступа на основе решений мандатной и дискреционной политик безопасности.

1. Вычислить уровень разрешения МПБ t_1:

1.1) если МПБ строится на основе линейной решетки ценностей, для расчета t_1 применить формулу (2);

1.2) иначе решетка ценностей МПБ является нелинейной, для расчета t_1 применить формулу (5).

2. Уровень разрешения ДПБ t_2 назначить по умолчанию в соответствии с матрицей доступов:

2.1) если доступ запрещен, для расчета t_2 применить формулу (3);

2.2) иначе доступ разрешен, для расчета t_2 применить формулу (4).

3. Принять решение о предоставлении доступа:

3.1) если $t_1 < 0$ и $t_2 < 0$, то доступ запретить;

3.2) иначе, если $t_1 \ge 0$ и $t_2 \ge 0$, то доступ разрешить;

3.3) иначе вычислить обобщенный уровень разрешения t по формуле (1). Если $t < 0$, то доступ запретить, иначе — доступ разрешить.

Применение метода анализа иерархий

Часто в одной системе действует по две мандатные и дискреционные политики безопасности: одна пара связана с конфиденциальностью, другая — с целостностью. В этом случае для вычисления уровня разрешения удобнее воспользоваться методом анализа иерархий (МАИ) со следующим деревом решения: вершина иерархии — уровень разрешения t; критерии: ДПБ и МПБ — дискреционная и мандатная политики безопасности; альтернативы: политика целостности и политика конфиденциальности. Отметим, что МАИ неоднократно применялся для решения задач информационной безопасности, в частности, в статьях [8–10] метод был использован для построения модели ролевого разграничения доступа.

Согласно МАИ, необходимо заполнить три матрицы парных сравнений: одна — для уровня критериев и две — для уровня альтернатив. Пусть, как и ранее, r ($r > 0$) — коэффициент доминирования, показывающий, во сколько раз решение, принимаемое МПБ, более значимо, чем решение ДПБ. Предпочтительность политики конфиденциальности по сравнению с политикой целостности оценивается двумя подобными параметрами: r_1 ($r_1 > 0$) — для дискреционной модели, r_2 ($r_2 > 0$) — для мандатной модели. Тогда матрицы парных сравнений задаются табл. 1.

Идеальная согласованность этих матриц следует из того факта, что для двумерной обратно симметричной матрицы **M** всегда выполняется условие: $\forall i, j, k$ имеет место равенство

■ ***Таблица 1***

t	ДПБ	МПБ
ДПБ	1	$1/r$
МПБ	r	1

ДПБ	цел.[1]	конф.[2]
цел.	1	$1/r_1$
конф.	r_1	1

МБП	цел.	конф.
цел.	1	$1/r_2$
конф.	r_2	1

[1] цел. — целостность.

[2] конф. — конфиденциальность.

$[\mathbf{M}]_{ij} = [\mathbf{M}]_{ik} \times [\mathbf{M}]_{kj}$. В этом случае относительные весовые коэффициенты определяются нормированными столбцами (например, первыми) всех трех матриц парных сравнений, а формулы для вычисления относительных приоритетов политики целостности и политики конфиденциальности принимают следующий вид:

$$R^{\text{цел}} = \frac{1}{1+r_1}\frac{1}{1+r} + \frac{1}{1+r_2}\frac{r}{1+r};$$

$$R^{\text{конф}} = \frac{r_1}{1+r_1}\frac{1}{1+r} + \frac{r_2}{1+r_2}\frac{r}{1+r} = 1 - R^{\text{цел}}.$$

Окончательное решение о предоставлении доступа теперь может быть вычислено по формулам

$$t = R^{\text{цел}} t^{\text{цел}} + R^{\text{конф}} t^{\text{конф}},$$

$$t^{\text{цел}} = \frac{1}{1+r} t^{\text{цел}}_{\text{ДПБ}} + \frac{r}{1+r} t^{\text{цел}}_{\text{МПБ}},$$

$$t^{\text{конф}} = \frac{1}{1+r} t^{\text{конф}}_{\text{ДПБ}} + \frac{r}{1+r} t^{\text{конф}}_{\text{МПБ}},$$

где верхний индекс означает политику конфиденциальности или целостности, а нижний — дискреционное или мандатное разграничение доступа. Пары величин $t^{\text{цел}}_{\text{ДПБ}}$ и $t^{\text{цел}}_{\text{МПБ}}$, а также $t^{\text{конф}}_{\text{ДПБ}}$ и $t^{\text{конф}}_{\text{МПБ}}$ вычисляются аналогично паре уровней разрешения t_1 и t_2 по алгоритму S, изложенному в предыдущем разделе. Анализируя полученные формулы, можно сделать следующие выводы.

1. Так как $R^{\text{цел}}$ и $R^{\text{конф}}$ принадлежат интервалу (0, 1), то применение МАИ в тех случаях, когда величины $t^{\text{цел}}$ и $t^{\text{конф}}$ имеют одинаковые знаки, не изменит решение о предоставлении доступа.

2. Если $r_1 \geq 1$ и $r_2 \geq 1$, то $R^{\text{цел}} \leq R^{\text{конф}}$. Если $r_1 < 1$ и $r_2 < 1$, то $R^{\text{цел}} > R^{\text{конф}}$. В обоих случаях формулы МАИ могут быть заменены формулой $t = \frac{1}{1+r'} t^{\text{цел}} + \frac{r'}{1+r'} t^{\text{конф}}$, где r' — параметр, характеризующий, во сколько раз решение, принимаемое политикой конфиденциальности, более значимо, чем решение политики целостности.

3. Применение МАИ дает наиболее интересные результаты в ситуации, когда $t^{\text{конф}}$ и $t^{\text{цел}}$ имеют разные знаки и $((r_1 > 1) \wedge (r_2 < 1)) \vee ((r_1 < 1) \wedge (r_2 > 1))$.

Пример 3. Пусть $t^{\text{цел}}_{\text{ДПБ}} = 3$, $t^{\text{цел}}_{\text{МПБ}} = -1$, $t^{\text{конф}}_{\text{ДПБ}} = 2$, $t^{\text{конф}}_{\text{МПБ}} = -2$. Положим $r = 2$. Тогда $t^{\text{цел}} = 1/3$, $t^{\text{конф}} = -2/3$. Очевидно, что для разрешения доступа необходимо потребовать, чтобы предпочтительность политики конфиденциальности (r_i) для одной из моделей разграничения доступа была меньше предпочтительности политики целостности ($1/r_j$) для другой модели. Пусть $r_1 = 2$, $r_2 = 1/3$, тогда $R^{\text{цел}} = 11/18$, $R^{\text{конф}} = 7/18$, $t = -1/18 < 0$. Таким образом, доступ будет запрещен, приоритет получит политика конфиденциальности. Если же $r_1 = 1$, $r_2 = 1/5$, тогда $R^{\text{цел}} = 13/18$, $R^{\text{конф}} = 5/18$, $t = 1/6 > 0$. Доступ будет разрешен, и приоритет получит политика целостности.

Рассмотрим далее другой вариант дерева решения МАИ: вершина иерархии — уровень разрешения $\hat{t}$; критерии: политика целостности и политика конфиденциальности; альтернативы: ДПБ и МПБ — дискреционная и мандатная политики безопасности.

Пусть решение, принимаемое политикой конфиденциальности, в x раз более значимо, чем решение политики целостности. Предпочтительность мандатной модели разграничения доступа по сравнению с дискреционной оценивается двумя параметрами: x_1 — для политики целостности, x_2 — для политики конфиденциальности. Тогда матрицы парных сравнений задаются табл. 2.

Формулы для вычисления относительных приоритетов дискреционной и мандатной политик безопасности принимают следующий вид:

$$X_{\text{ДПБ}} = \frac{1}{1+x_1}\frac{1}{1+x} + \frac{1}{1+x_2}\frac{x}{1+x};$$

$$X_{\text{МПБ}} = \frac{x_1}{1+x_1}\frac{1}{1+x} + \frac{x_2}{1+x_2}\frac{x}{1+x} = 1 - X_{\text{ДПБ}}.$$

Окончательное решение о предоставлении доступа теперь может быть вычислено по формулам

$$\hat{t} = X_{\text{ДПБ}} \hat{t}_{\text{ДПБ}} + X_{\text{МПБ}} \hat{t}_{\text{МПБ}},$$

$$\hat{t}_{\text{ДПБ}} = \frac{1}{1+x} t^{\text{цел}}_{\text{ДПБ}} + \frac{x}{1+x} t^{\text{конф}}_{\text{ДПБ}},$$

$$\hat{t}_{\text{МПБ}} = \frac{1}{1+x} t^{\text{цел}}_{\text{МПБ}} + \frac{x}{1+x} t^{\text{конф}}_{\text{МПБ}}.$$

Пример 4. Пусть, как и прежде, $t^{\text{цел}}_{\text{ДПБ}} = 3$, $t^{\text{конф}}_{\text{ДПБ}} = 2$, $t^{\text{цел}}_{\text{МПБ}} = -1$, $t^{\text{конф}}_{\text{МПБ}} = -2$. Положим $x = 3$. Тогда $\hat{t}_{\text{ДПБ}} = 9/4$, $\hat{t}_{\text{МПБ}} = -7/4$. Пусть $x_1 = 1$, $x_2 = 1/3$, тогда $X_{\text{ДПБ}} = 11/16$, $X_{\text{МПБ}} = 5/16$, $\hat{t} = 1 > 0$. Таким образом, доступ будет разрешен, приоритет получит ДПБ. Если же $x_1 = 1/2$, $x_2 = 2$, тогда

■ *Таблица 2*

$\hat{t}$	цел.	конф.
цел.	1	$1/x$
конф.	x	1

цел.	ДПБ	МПБ
ДПБ	1	$1/x_1$
МПБ	x_1	1

конф.	ДПБ	МПБ
ДПБ	1	$1/x_2$
МПБ	x_2	1

$X_{ДПБ} = 5/12$, $X_{МПБ} = 7/12$, $\hat{t} = -1/12 < 0$. Доступ будет запрещен, и приоритет получит МПБ.

Используя представленные ранее формулы для вычисления уровней разрешения t и $\hat{t}$, несложно доказать следующее **утверждение:**

$$\text{если } r = x_1 = x_2 \text{ и } r_1 = r_2 = x, \text{ то } t = \hat{t}.$$

Таким образом, в случае совпадения приоритетов в разрезе выбранной модели разграничения доступа и в разрезе политик конфиденциальности и целостности оба подхода к построению дерева решения МАИ приводят к одному и тому же уровню разрешения. В конечном итоге выбор дерева решения зависит от порядка администрирования, определенного в системе.

Заключение

Предложенный подход к построению единой политики безопасности обладает рядом преимуществ по сравнению с традиционным требованием одновременного разрешения доступа всеми активными политиками безопасности. Наличие весовых коэффициентов позволяет администратору достаточно гибко настраивать степени влияния различных правил безопасности. Использование двух различных по типу политик безопасности имеет смысл, если они перекрывают различные каналы утечки информации. В связи с этим выбор весовых коэффициентов в алгоритме принятия решений необходимо осуществлять на основе анализа вероятности различных атак.

Следует подчеркнуть, что необходимость принятия решения о доминировании одной политики безопасности над другой возникает только в случае противоречий разрешений по одному и тому же запросу на доступ. С одной стороны, в системах, допускающих непротиворечивое администрирование безопасности, таких конфликтов не возникает. С другой стороны, если между двумя политиками безопасности никогда не возникает противоречий, то одну из политик безопасности можно отключить без ущерба защищенности системы.

Предложенный подход может найти применение в проектировании дополнительных систем защиты информации, а также в программных комплексах с собственной подсистемой безопасности.

Литература

1. **Белим С. В., Богаченко Н. Ф., Ракицкий Ю. С.** Теоретико-графовый подход к проблеме совмещения ролевой и мандатной политик безопасности // Проблемы информационной безопасности. Компьютерные системы. 2010. № 2. С. 9–17.
2. **Белим С. В., Богаченко Н. Ф., Ракицкий Ю. С.** Совмещение ролевой и мандатной политик безопасности // Проблемы обработки и защиты информации. Кн. 1: Модели политик безопасности компьютерных систем: Коллективная монография. — Омск: Полиграфический центр КАН, 2010. — С. 117–132.
3. **Щеглов К. А., Щеглов А. Ю.** Новый подход к защите данных в информационной системе // Известия высших учебных заведений. Приборостроение. 2015. Т. 58. № 3. С. 157–166.
4. **Bishop M.** Applying the Take-Grant Protection Model. Technical Report. — Dartmouth College Hanover, NH, USA, 1990. — 26 p.
5. **Ribeiro C., Zuquete A., Ferreira P., Guedes P.** SPL: An Access Control Language for Security Policies with Complex Constraints // Proc. of the Network and Distributed System Security Symposium. Sun Diego, CA. 2001. https://scholar.google.co.uk/citations?view_op=view_citation&hl=ru&user=3PHaUacAAAAJ&citation_for_view=3PHaUacAAAAJ:LPZeul_q3PIC (дата обращения: 18.07.2016).
6. **Lunsford D. L., Collins M. R.** The CRUD Security Matrix: A Technique for Documenting Access Rights // Proc. of the 7th Annual Security Conf. Las Vegas, NV, 2008. http://ocean.otr.usm.edu/~w300778/is-doctor/pubpdf/sc2008.pdf (дата обращения: 18.07.2016).
7. **Kocatürk M. M., Gündema T. I.** Fine-Grained Access Control System Combining MAC and RBAC Models for XML // Informatica. 2008. Vol. 19. Iss. 4. P. 517–534.
8. **Богаченко Н. Ф., Белим С. В., Белим С. Ю.** Использование метода анализа иерархий для построения ролевой политики безопасности // Проблемы информационной безопасности. Компьютерные системы. 2013. № 3. С. 7–17.
9. **Белим С. В., Богаченко Н. Ф.** Применение метода анализа иерархий для оценки рисков утечки полномочий в системах с ролевым разграничением доступа // Информационно-управляющие системы. 2013. № 6. С. 67–72.
10. **Белим С. В., Белим С. Ю., Богаченко Н. Ф.** Построение ролевого разграничения доступа с использованием метода анализа иерархий // Проблемы обработки и защиты информации. Кн. 4: Алгоритмы защиты данных. — Омск: Изд-во Омского гос. ун-та, 2015. — С. 7–47.

UDC 004.056
doi:10.15217/issn1684-8853.2016.5.66

The Security Policies Joint Implementation Based on Decision Support Algorithms

Belim S.V.[a], Dr. Sc., Phis.-Math., Professor, sbelim@mail.ru
Bogachenko N. F.[a], PhD, Phis.-Math., Associate Professor, nfbogachenko@mail.ru
Rakitskiy Yu. S.[a], PhD, Tech., Associate Professor, yrakitsky@gmail.com
[a]Dostoevsky Omsk State University, 55, A, Mira St., 644077, Omsk, Russian Federation

Introduction: The problem of joint implementation of several security policies in one information environment is a topical issue in computer system administrating. The modern standards of information security in automated systems requre that at least two security policies are available. Most of the offered methods to solve the joint implementation problem can be reduced to the search for an ideal solution when the settings of all the shared security policies do not contradict each other. In practice, it is not always possible to find such settings, and the very existence of an ideal solution is not proved. An approach based on decision-making support algorithms is a promising way to find answers to these questions. **Results:** An algorithm of combining several security policies is offered. For each request for access, it makes a decision on what security policy will be involved. This algorithm uses a weighed sum of permission levels for separate security policies, and the Analytic Hierarchy Process. Formulas are presented to calculate the permission level of the required access for the discretionary and mandatory security policies. In the discretionary security policy, the permission level of a required access is defined by such numerical characteristics as the total number of the allowed access rights, the number of the required access rights, and the number of the forbidden access rights. For the mandatory security policy, the calculation of the permission level of a required access depends on the type of the security lattice. The analytic hierarchy process finds application when two couples of security policies work in the system, one couple related to confidentiality, an the other one related to integrity. Two solution trees are offered for analytic hierarchy process to calculate the total permission level of the required access. **Practical relevance:** The algorithm proposed for joint implementation of security policies contains weight factors. This allows us to set up the level of influence for different security rules so that various channels of information leakage overlap. The proposed approach can be useful in building information systems with their own security subsystems, or in the development of extra systems of information security.

Keywords — Joint Implementation of Security Policies, Permission Level, Decision-Making Support Algorithms, Analytic Hierarchy Process.

References

1. Belim S. V., Bogachenko N. F., Rakitsky J. S. Theoretical-Graph Approach to the Problem of Combining Role-Based and Mandatory Security Policies. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2010, no. 2, pp. 9–17 (In Russian).
2. Belim S. V., Bogachenko N. F., Rakitsky J. S. Combining of Role-Based and Mandatory Security Policies. In: *Problemy obrabotki i zashchity informatsii. Kniga 1. Modeli politik bezopasnosti komp'iuternykh sistem* [Problems of Information Processing and Security. Book 1. Models of Security Policies of Computer Systems]. Omsk, Poligraficheskii tsentr KAN Publ., 2010, pp. 117–132 (In Russian).
3. Shcheglov K. A., Shcheglov A. Yu. New Approach to Data Securing in Information System. *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie*, 2015, vol. 58, no. 3, pp. 157–166 (In Russian).
4. Bishop M. *Applying the Take-Grant Protection Model. Technical Report*. Dartmouth College Hanover, NH, USA, 1990. 26 p.
5. Ribeiro C., Zuquete A., Ferreira P., Guedes P. SPL: An Access Control Language for Security Policies with Complex Constraints. *Proc. of the Network and Distributed System Security Symp.*, Sun Diego, CA, 2001. Available at: https://scholar.google.co.uk/citations?view_op=view_citation&hl=ru&user=3PHaUacAAAAJ&citation_for_view=3PHaUacAAAAJ:LPZeul_q3PIC (accessed 18 July 2016).
6. Lunsford D. L., Collins M. R. The CRUD Security Matrix: A Technique for Documenting Access Rights. *Proc. of the 7th Annual Security Conf.*, Las Vegas, NV, 2008. Available at: http://ocean.otr.usm.edu/~w300778/is-doctor/pubpdf/sc2008.pdf (accessed 18 July 2016).
7. Kocatürk M. M., Gündema T. I. Fine-Grained Access Control System Combining MAC and RBAC Models for XML. *Informatica*, 2008, vol. 19, iss. 4, pp. 517–534.
8. Bogachenko N. F., Belim S. V., Belim S. Yu. Using Analytic Hierarchy Process for Building of Role Based Access Control. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2013, no. 3, pp. 7–17 (In Russian).
9. Belim S. V., Bogachenko N. F. Using a Hierarchy Analysis Method to Assess Permission Leakage Risks in Systems with a Role Based Access Control. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2013, no. 6, pp. 67–72 (In Russian).
10. Belim S. V., Belim S. Yu., Bogachenko N. F. Creation of Role-Base Access Control with Use of Analytic Hierarchy Process. In: *Problemy obrabotki i zashchity informatsii. Kniga 4. Algoritmy zashchity dannykh* [Problems of Information Processing and Security. Book 4. Algorithms of Data Security]. Omsk, OmSU Publ., 2015, pp. 7–47 (In Russian).

УДК 004.93’1
doi:10.15217/issn1684-8853.2016.5.73

ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА НАДЕЖНОСТИ ВЕРИФИКАЦИИ ПОДПИСИ СЕТЯМИ КВАДРАТИЧНЫХ ФОРМ, НЕЧЕТКИМИ ЭКСТРАКТОРАМИ И ПЕРСЕПТРОНАМИ

П. С. Ложников[а], *канд. техн. наук, доцент*
А. Е. Сулавко[а], *канд. техн. наук, старший преподаватель*
А. В. Еременко[б], *канд. техн. наук, доцент*
Д. А. Волков[а], *аспирант*
[а]*Омский государственный технический университет, Омск, РФ*
[б]*Омский университет путей сообщения, Омск, РФ*

Введение: *проблемы защиты информации с каждым годом становятся актуальней, поэтому требования к биометрическим системам ужесточаются. Цель работы: сравнить нечеткие экстракторы, нейросетевые преобразователи биометрия-код и сети квадратичных форм по надежности биометрической аутентификации на основе подписи субъекта.* ***Результаты:*** *проведен анализ научной литературы и серия вычислительных экспериментов на основе реальных биометрических данных. По результатам экспериментов нечеткие экстракторы значительно уступают другим системам по надежности аутентификации и длине ключа, сети Байеса — Пирсона — Хемминга показывают наилучший результат.* ***Практическая значимость:*** *полученные результаты будут интересны исследователям и разработчикам биометрических систем.*

Ключевые слова *— особенности воспроизведения подписи, биометрия, нечеткие экстракторы, искусственные нейронные сети, аутентификация.*

Введение

Проблемы защиты информации от несанкционированного доступа не теряют актуальности [1]. Одно из направлений по противодействию этому виду угроз — усовершенствование биометрических средств аутентификации. На данный момент идет «борьба за повышение» надежности биометрических систем с одновременным выполнением требований по защите биометрических эталонов субъектов, прописанных в ГОСТ Р 52633.0-2006 [4] (5.2, 5.3). Надежность определяется вероятностью ошибок 1-го и 2-го рода — ложного отказа в доступе «Своему» и ложного доступа «Чужого».

Статические образы (отпечатка пальца, сетчатки, радужки) не являются секретными, их можно скопировать, изготовив физический или цифровой муляж (для удаленной аутентификации). Поэтому усилия многих исследователей сконцентрированы на повышении надежности аутентификации по динамическим биометрическим признакам (особенностям воспроизведения рукописного или голосового образа и клавиатурного почерка). Для регистрации клавиатурного почерка можно разработать скрытый перехватчик на основе руткит-методик (обнаружить который крайне сложно [2]), голос может быть перехвачен посредством микрофона. В этом смысле лучше использовать параметры рукописных паролей. На настоящий момент динамические признаки дают более высокий процент ошибочных решений при аутентификации, чем статические. Но потенциал динамических образов значительно выше, так как они могут быть тайными (а их длина неограниченна [3]).

Существует несколько подходов к реализации методики принятия решений в биометрических системах с обеспечением защиты эталонных описаний образов субъектов [4]. Однако сопоставительные экспериментальные данные по их эффективности не нашли достаточного отражения в литературе. Настоящая работа посвящена актуальной научной проблеме: экспериментальной оценке надежности существующих методов биометрической аутентификации на основе особенностей воспроизведения рукописных образов с возможностью защиты биометрического эталона и некоторых вариантов модернизации данных методов.

Сравнение существующих подходов по данным научной литературы

Изначально сложилось два основных подхода к реализации связи «аутентификатор — субъект» с защитой биометрического эталона: нейросетевые преобразователи «биометрия-код» (НПБК) [4] и «нечеткие экстракторы» [5]. По определению, данному в монографии казахстанских и российских ученых [6], а также в ГОСТ Р 52633.0-2006 [4], «нейросетевой преобразователь “биометрия-код” — это заранее обученная искусственная нейронная сеть с большим числом входов и выходов,

преобразующая частично случайный вектор входных биометрических параметров "Свой" в однозначный код криптографического ключа (длинного пароля) и преобразующая любой иной случайный вектор входных данных в случайный выходной код». Таким образом, код доступа, получаемый из данных легального пользователя (выходной код «Свой»), должен быть фиксированным, а код из данных других субъектов (выходной код «Чужой» или все «Чужие») — случайной строкой бит. Основное отличие обозначенных методов от обычной биометрической аутентификации — это обезличивание эталонных описаний образов (отказ от необходимости хранить эталон либо хранение эталона в виде, не позволяющем восстановить исходные биометрические характеристики субъекта). Надежность системы аутентификации определяется вероятностью ошибок 1-го и 2-го рода — ложного отказа в доступе «Своему» и ложного доступа «Чужого».

Нейросетевые преобразователи «биометрия-код»

Сдерживающим фактором в применении нейронных сетей является сложный процесс их обучения. Малые нейронные сети быстро обучаются, но принимают низкокачественные решения. По мере увеличения размеров (количества слоев, нейронов и их входов) решения становятся более достоверными (на уровне людей-экспертов или лучше), но при этом растет сложность обучения нейросети, появляются проблемы «тупиков» и «зацикливания обучения», в результате этот процесс становится неприемлемо долгим либо неосуществимым [3, 7]. Для биометрии требуются сверхбыстрые алгоритмы обучения (выполняемые за несколько секунд на обычном персональном компьютере) [3]. Для данной цели не могут быть использованы итерационные алгоритмы, поскольку они теряют устойчивость при увеличении числа входов нейронов или при снижении качества биометрических данных [6]. Решение проблемы предложено в стандарте ГОСТ Р 52633.5-2011 [8]. Рекомендуется использовать прямое вычисление модулей весовых коэффициентов через математические ожидания и среднеквадратические отклонения биометрических параметров «Свой» и «Чужой». Благодаря этому процедуры обучения становятся рекордно быстрыми и устойчивыми [6]. Для обучения сети требуется не менее 21 образца данных «Свой» и 64 независимых образца данных «Чужой» (образцы от разных субъектов).

Другим сдерживающим фактором в использовании НПБК на практике является сложность тестирования их надежности [6]. Высоконадежные биометрические устройства с вероятностью ошибочных решений 10^{-12} и выше проще создать, чем доказательно проверить эту вероятность прямым численным экспериментом [6]. Для НПБК не годится упрощенная схема Бернулли [6], а для атак прямого подбора необходимы объемные базы данных биометрических признаков, собрать которые невозможно по причине нехватки населения Земли. Для тестирования предложены процедуры морфинга, определенные в ГОСТ Р 52633.2-2010, используя которые удается оценить «нано» и «пико» вероятности ошибок 2-го рода биометрической аутентификации на тестовых базах, состоящих из 10 000 естественных биометрических образов [6].

Особенностью НПБК является то, что для малых нейронных сетей слабые корреляционные связи между биометрическими параметрами слабо влияют на результирующую энтропию генерируемого кода, а для больших нейронных сетей ситуация становится обратной — из-за слабых корреляционных связей энтропия падает, что упрощает атаки перебора. Границей деления нейронных сетей на большие и малые являются 16 выходных разрядов [6].

Другой особенностью НПБК является процедура обогащения. Обогащение позволяет работать с «плохими биометрическими данными» и восстанавливать до 50 % ошибок исходных данных [9]. При высоком уровне первичного обогащения данных обыкновенные нейроны (персептроны) оказываются малоэффективными. Более эффективны искусственные нейроны с несколькими выходными дискретными состояниями [6]. Практика показала, что использование операции циклического сдвига при настройке формы нелинейного элемента нейрона не является оптимальной. Более качественные результаты получаются, если определенным участкам области значений сумматора нейрона (вне интервала «Свой») задавать выходные коды случайным образом. При таком способе усиливаются хеширующие свойства обученного нейрона по отношению к образам все «Чужие», нелинейные элементы с длительными монотонными участками хуже перемешивают данные [6]. В работе [7] предложено использовать трид-нейроны с двумя выходными состояниями, которые имеют два порога квантования. Использование трид-нейронов позволяет повысить длину генерируемого кода в два раза, а энтропию кодов — в полтора раза, если квантователь выходных значений не является монотонной дискретной функцией.

По требованиям ГОСТ Р 52633.0-2006 [4] при поступлении на вход НПБК образца данных «Чужой» вероятности значений «0» и «1» разрядов выходного кода должны быть равными (допускается разница в количестве различных значений разрядов не более 10 %). Для того чтобы поднять качество хеширования, могут быть использованы различные механизмы размножения ошибок, например, сложение по модулю 2 части выходного кода «Свой» от изолированного потока

нейронов и записанных в дискретной форме параметров обученной нейронной сети остальных нейронов (весовых коэффициентов нейронов и номеров связей между нейронами) [6]. Шифрование параметров нейронов на выходах других нейронов также предлагается использовать при запуске в недоверенной среде для защиты таблиц нейросетевых функционалов от анализа в целях восстановления эталона субъекта [6, 10]. Данный принцип защиты называется защищенным нейросетевым (биометрическим) контейнером [10]. Размер ключа выбирается по конструктивным особенностям и возможностям нейронной сети. Данная схема уязвима к атаке Г. Б. Маршалко, которая строится на наблюдении большого числа выходов у незащищенных нейронов [10]. Чтобы снизить эффективность таких атак на биометрию, следует отказаться от создания одного длинного ключа и использовать множество ключей увеличивающейся длины [6]. Тем не менее сегодня защищенные нейросетевые контейнеры являются наиболее эффективным средством хранения оцифрованной биометрии [10].

Нужно отметить, что длина эффективного кода (аутентификатора) зависит от количества информативных признаков, простое увеличение количества нейронов не ведет к аналогичному росту эффективного кода, так как энтропия генерируемого кода не соответствует его длине [10]. Вместе с тем для того чтобы снизить вероятность ошибок 2-го рода до уровня парольной защиты (~10^{-8}), необходимо использовать достаточно большое число выходов у НПБК.

Для обучения НПБК необходимо, чтобы биометрические данные имели закон распределения, близкий к нормальному, для контроля за этим используется критерий Пирсона, а также его модификации [11, 12].

Достоинством биометрических сетей является то, что биометрический шаблон человека не хранится более в памяти компьютера, вместо него хранятся весовые коэффициенты между нейронами (не существует эффективного способа восстановления параметров распределения биометрических признаков из данных нейросетевого биометрического контейнера) [1]. Защитные свойства усиливаются при использовании защищенных нейросетевых контейнеров. Обогащение данных нейронами является сильной стороной технологии по сравнению с квантованием «сырых» биометрических данных.

Нечеткие экстракторы

Данный подход активно развивается за рубежом и основан на использовании кодов, исправляющих ошибки, применяемых к «сырым», не обогащенным биометрическим данным для корректировки нестабильных бит генерируемого ключа. Известны схожие версии изложения данного подхода (многие из которых упоминаются и описываются в работах [13–16]): Fuzzy Vault («нечеткое хранилище») [17], Fuzzy Commitment [18] и т. д. Некоторые из них обладают бóльшим числом недостатков, чем классический «нечеткий экстрактор» (Fuzzy Extractor), который является общей схемой выработки ключевой последовательности, построенной на использовании классических самокорректирующих кодов. Далее объединим все указанные и аналогичные схемы общим названием — нечеткий экстрактор.

К принципиальным недостаткам нечетких экстракторов относятся:

1. Высокая избыточность классических самокорректирующих кодов, из-за которой длина генерируемого ключа оказывается низкой. К примеру, не существует кодов, способных исправлять 50 % ошибок, так как такие коды имеют огромную избыточность и пренебрежимо малую информационную часть [6, 10].

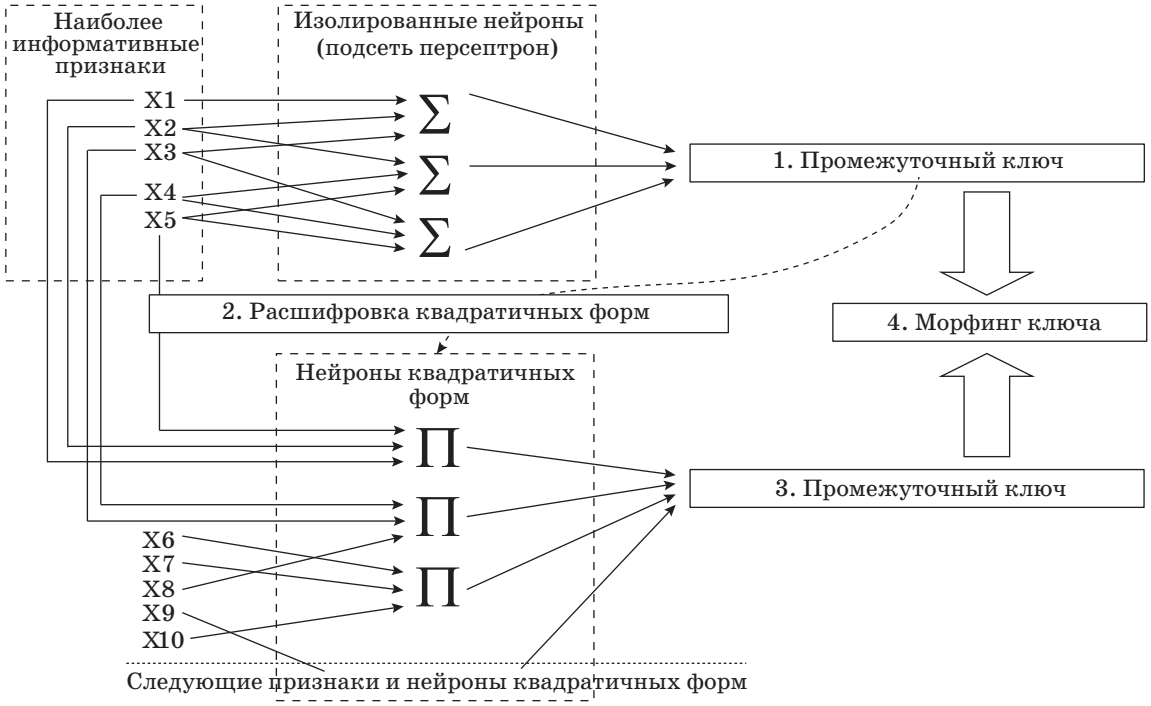
2. Уязвимости нечетких экстракторов [19], позволяющие ускорить перебор значений биометрических параметров в целях фальсификации ключа доступа. Считается, что наложение на биометрические данные гаммы в виде строки бит является надежной защитой для обеих составляющих только в случае равновероятной единичной ошибки в битовом представлении вектора биометрических признаков, чего на практике не наблюдается [19].

3. Нечеткие экстракторы квантуют «сырые» биометрические данные и не учитывают параметры распределения значений признаков, в результате они должны давать более высокий процент ошибок по сравнению с НПБК, которые в свою очередь располагают этими данными, кодируя их весовыми коэффициентами нейронов [6, 10, 19].

Для решения первой проблемы в работе [9] предложены коды, разработанные специально для биометрии. Они позволяют хранить синдромы ошибок отдельно от открытой строки в виде усеченной хеш-функции (последние 3 бита), поэтому извлекаемый из открытой строки ключ доступа будет длинней. В работе [20] показана связь эффективности коррекции ошибок с методами группирования битов с разной вероятностью единичной ошибки. Несмотря на предпринятые в данном направлении усилия, единого подхода для решения этого вопроса до сих пор не выработано. Поэтому вторая проблема экстракторов не считается решенной в полной мере. Третья проблема фактически не решается.

Сети квадратичных форм и модификация персептронов

В качестве альтернативы нейронным сетям по ГОСТ Р 52633.5-2011 [8] предлагается использовать сети квадратичных форм [21, 22] либо мо-



■ ***Рис. 1.*** Схема выработки ключа (аутентификатора) с использованием гибридной нейронной сети и принципа защищенного нейросетевого контейнера

дификации персептронов данного стандарта [7, 22], к которым относятся сети трид-нейронов [7] и нейроны с четной функцией двухстороннего квантования [22] (вместо нечетной ступенчатой квантующей функции). Функция [22] имеет два порога (правый и левый компаратор), при попадании в заданный интервал нейрон выдает значение, на которое настроен, в противном случае — обратное ему значение.

Основное отличие сети квадратичных форм заключается в строении искусственного нейрона. Классический нейрон и нейрон стандарта ГОСТ Р 52633.5-2011 [8] состоит из сумматора и линейной (нелинейной) пороговой функции на выходе нейрона, которая трансформирует полученную сумму обработанных параметров от каждого синапса (входа нейрона) в бинарное значение «0» или «1» [3, 6, 10]. Нейрон квадратичной формы может быть основан на метрике Евклида, Пирсона, Махаланобиса и др. [3]. К преимуществам квадратичных форм можно отнести отсутствие необходимости обучения на образцах «Чужой» и возможность нелинейного разделения собственных областей эталонов в пространстве признаков [3] (персептрон осуществляет линейное разделение). Очевидным недостатком является необходимость хранения параметров законов распределения признаков.

Проблема хранения эталона субъекта может быть решена по принципу защищенного нейросетевого контейнера [6, 10]. В настоящей работе для этого предлагается построить гибридную сеть из обычных (или модифицированных) нейронов и нейронов квадратичных форм. Параметры нейронов квадратичных форм шифруются на выходах изолированных нейронов подсети персептронов. Этот принцип иллюстрируется на рис. 1. Необходимо подготовить такие изолированные нейроны, на входы которых будут подаваться значения наиболее информативных признаков. При верной выдаче фрагмента ключа изолированными нейронами параметры нейронов квадратичных форм будут расшифрованы правильно. В результате будет формироваться оставшаяся часть ключа. В противном случае сеть должна генерировать случайный шум, так как расшифрованные значения весовых коэффициентов будут некорректны (либо не будут соответствовать эталону субъекта). Можно определить несколько потоков изолированных нейронов, чтобы шифровать данные многократно, каждый раз осуществляя морфинг нового промежуточного ключа на основе предыдущего и генерируемого очередным потоком, что усилит защиту весовых коэффициентов [6, 10]. Однако данный вопрос выходит за рамки задач, поставленных в статье.

Достоинства и недостатки существующих подходов

Требования к нейросетевым преобразователям «биометрия-код» изложены в семействе отечественных стандартов ГОСТ Р 52633, число которых существенно превышает число за-

■ ***Таблица 1***. Преимущества и недостатки преобразователей «биометрия-код»

Подход	Преимущества	Недостатки
Персептроны ГОСТ Р 52633.5-2011 и их модификации	1. Обогащает данные 2. Хорошо стандартизован 3. Маскирует биометрический эталон 4. Возможность создания защищенного нейросетевого контейнера [10]	Требуется обучать сеть на образцах данных «Чужой» (других субъектов)
Нечеткий экстрактор	1. Не требуется обучать сеть на образцах данных «Чужой» (образцах других субъектов) 2. Простота реализации на практике	1. Не учитывает параметры распределения признаков 2. Помехоустойчивые коды крайне избыточны, длина ключа оказывается низкой 3. Возможно ускорить перебор биометрических данных для фальсификации ключа [19]
Сети квадратичных форм	1. Не требуется обучать сеть на образцах данных «Чужой» 2. Обогащает данные 3. Возможность создания защищенного нейросетевого контейнера [10]	Возникает необходимость хранить параметры распределения значений признаков

рубежных аналогичных стандартов для нечетких экстракторов (ISO/IEC 24745:2011, ISO/IEC 24761:2009, ISO/IEC 19792:2009) [6], т. е. данный подход лучше стандартизован. Но каждый из рассмотренных подходов обладает как преимуществами, так и недостатками (табл. 1).

Экспериментальное сравнение существующих подходов

Для сравнения описанных подходов допустимо использовать любой рукописный образ. Личный автограф не является секретным, но очевидно является наиболее стабильным рукописным образом. Поэтому для проведения опытов решено использовать подпись. В эксперименте участвовало 65 субъектов.

Используемое пространство признаков

Для ввода подписей в настоящем исследовании испытуемые пользовались графическим планшетом фирмы Wacom. Подпись состоит из функций положения пера на планшете $x(t)$, $y(t)$ и давления пера на планшет $p(t)$, где t — время в дискретной форме. Будем обозначать значения этих функций через x_i, y_i, p_i. Необходимо определить признаки — величины, характеризующие владельца подписи. Далее использовались признаки из работ [23, 24].

Образцы подписи отличаются по продолжительности (количеству отсчетов). Первоначально необходимо привести их к единой продолжительности, выполнив операцию нормирования, состоящую из следующих этапов:

1) исключаются все отчеты с нулевым давлением в начале и конце подписи;

2) производится одномерное преобразование Фурье для $x(t)$, $y(t)$ и $p(t)$;

3) производится обратное преобразование Фурье для указанных функций с учетом того, что размерность на выходе должна соответствовать числу, которое является ближайшим меньшим кратным степени 2.

Часть пространства признаков формировалась посредством построения матрицы расстояний между отчетами подписи. Элементы r_{ij} (расстояние между i-й и j-й координатами) матрицы в 3-мерном пространстве (давление — третье измерение) вычисляются по формуле

$$r_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + (p_i - p_j)^2}. \qquad (1)$$

Аналогичным образом вычисляется матрица расстояний в 2-мерном пространстве (без учета давления).

Поскольку при расчете получается слишком много элементов, что требует слишком высоких вычислительных ресурсов, то необходимо производить вычисления расстояний с некоторым шагом. Далее производится нормирование полученной матрицы по длине подписи: $r'_{ij} = r_{ij}/r_{12} + r_{23} + \ldots + r_{(n-1)n}$. Нормированные элементы r'_{ij} полученной матрицы являются биометрическими признаками.

Вычисляются некоторые признаки, характеризующие внешний вид подписи:

1) отношение длины подписи к ее ширине;

2) центр подписи, описываемый координатами C_X, C_Y, C_P;

3) угол наклона подписи. Под углом подписи понимается косинус среднего угла наклона ломаной траектории подписи к оси абсцисс:

$$\theta = \frac{1}{N-1}\sum_{i=1}^{N}\frac{x_{i+1} - x_i}{\sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2}};$$

4) угол наклона между центрами половин подписи. После того как был найден центр подписи, разобьем множество $(X, Y, Z) = \{(x_i, y_i, p_i)\}$ на два подмножества $L = \{(x_i, y_i, p_i) | x_i \le C_X\ C_X\}$ и $R = \{(x_i, y_i, p_i) | x_i > C_X\}$ и найдем центры этих подмножеств:

$$C_{X_L} = \frac{1}{|L|}\sum_{x_i \in L}^{N} x_i,\ C_{Y_L} = \frac{1}{|L|}\sum_{y_i \in L}^{N} y_i,$$

$$C_{P_L} = \frac{1}{|L|}\sum_{p_i \in L}^{N} p_i;$$

$$C_{X_R} = \frac{1}{|R|}\sum_{x_i \in R}^{N} x_i,\ C_{Y_R} = \frac{1}{|R|}\sum_{y_i \in R}^{N} y_i,$$

$$C_{P_R} = \frac{1}{|R|}\sum_{p_i \in R}^{N} p_i.$$

Следующая категория признаков основана на использовании преобразования Фурье. Функции, которые подвергаются разложению по формуле (2): $p(t)$ на планшет и функция скорости пера на планшете $v(t)$, значения которой вычисляются по формуле (3). При использовании $v(t)$ исчезает зависимость от того, под каким углом расположен планшет относительно руки подписанта. Можно воспользоваться быстрым или обычным дискретным преобразованием Фурье. В отличие от дискретного, которое имеет сложность порядка $O(N^2)$, быстрое преобразование Фурье имеет сложность $O(N\log_2 N)$.

$$X_k = \sum_{i=0}^{N-1} x_i e^{\frac{-j2\pi ki}{N}}, \qquad (2)$$

где X_k — k-я гармоника в комплексной форме $\mathrm{Re}_k + j\mathrm{Im}_k$; x_i — i-е значение функции; N — количество отсчетов в дискретном сигнале. Исходный дискретный сигнал представляется в виде суммы функций:

$$f(t_i) = \sum_{k=0}^{N-1}\left[\frac{\mathrm{Re}_k}{N}\cos\left(\frac{2\pi k t_i}{T}\right) - \frac{\mathrm{Im}_k}{N}\sin\left(\frac{2\pi k t_i}{T}\right)\right] =$$

$$= \sum_{k=0}^{N-1} A_k \cos\left(2\pi t_n / T_k + \varphi_k\right) =$$

$$= \sum_{k=0}^{N-1} A_k \cos\left(2\pi t_i v_k + \varphi_k\right) = \sum_{k=0}^{N-1} G_k(t_i),$$

$$v_i = \sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2}. \qquad (3)$$

Далее будем функцию $G_k(t) = A_k \cos\frac{2\pi t_n}{T_k + \varphi_k}$ называть k-й гармоникой. Амплитуды вычисляются в соответствии с формулой

$$A_k = \frac{1}{N}\sqrt{\mathrm{Re}_k^2 + \mathrm{Im}_k^2}. \qquad (4)$$

Далее производится расчет энергии функции по формуле

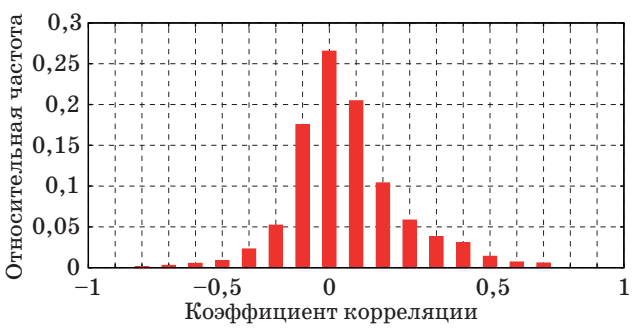
$$E_p = \int_{-\infty}^{\infty} A^2(t)\mathrm{d}t. \qquad (5)$$

На следующем шаге производится деление амплитуды каждой гармоники на значение энергии сигнала. Эта операция называется нормированием амплитуд по энергии и осуществляется в целях приведения различных реализаций подписи к одному масштабу. Решено использовать 16 нормированных амплитуд первых наиболее низкочастотных гармоник функции давления и функции скорости пера на планшете в качестве признаков по аналогии с работой [23].

Помимо описанных характеристик признаками в настоящей работе являются коэффициенты парной корреляции между функциями $x(t)$, $y(t)$ и $p(t)$ (и их производными). Установлено, что данные коэффициенты корреляции для каждого рукописного образа подписи субъекта близки по значениям и более существенно различаются для рукописных образов подписей различных субъектов [25]. Все указанные признаки имеют распределение значений, близкое к нормальному, что проверялось критерием хи-квадрат Пирсона. Общее число признаков 236. На рис. 2 представлена гистограмма относительных частот коэффициентов парной корреляции между сечениями признаков, полученных при статистической обработке всех имеющихся на момент проведения эксперимента подписей.

Модель нечеткого экстрактора

Для выработки ключа-аутентификатора нечетким экстрактором необходимы биометрические данные и дополнительная информация, хранящаяся на общедоступном сервере (носителе), из которой нельзя восстановить эталон (не существует простого способа это сделать). Данная информация называется открытой строкой. Сначала генерируется случайная равномерно распределенная битовая последовательность,

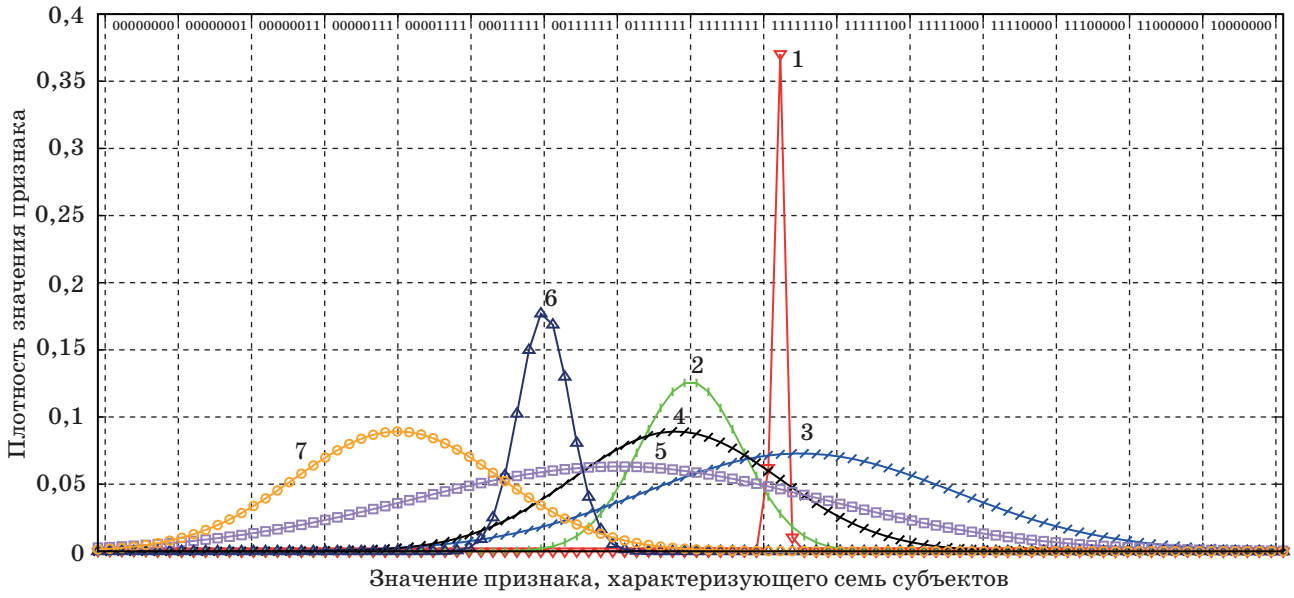


■ ***Рис. 2.*** Распределение коэффициентов парной корреляции между признаками по всем реализациям подписей всех испытуемых

которая является ключом. Далее осуществляется помехоустойчивое кодирование ключа доступа (к битовой последовательности добавляются синдромы ошибок помехоустойчивых кодов). На полученную избыточную строку накладывается гамма в виде битового представления эталонных биометрических данных (обычно берется вектор средних значений признаков). На выходе получается открытая строка, которую можно хранить на общедоступном сервере [5]. Для получения ключа субъект вводит новую реализацию признаков, которая «вычитается» от открытой строки, к результату этой операции применяются корректирующие коды (Адамара, Хемминга, Рида — Соломона и др.) [26]. Если расстояние Хемминга между введенным вектором признаков и эталонным вектором (который накладывался на избыточную строку) не превышает исправляющей способности кода, то после декодирования будет восстановлен исходный ключ доступа, в противном случае ключ будет другой. Длина ключа будет тем меньше, чем больше исправляющая способность кода.

В настоящем исследовании решено сравнить экстракторы на базе кодов Адамара и Рида — Соломона. Эквидистантные коды Адамара, обладая большим кодовым расстоянием, позволяют исправить и большое количество ошибок, зависящее от размера блока. Достоинством кодов Адамара является сравнительно высокая скорость работы. Коды БХЧ (Боуза — Чоудхури — Хоквингема) — это широкий класс циклических кодов, которые отличаются возможностью установки определенных корректирующих свойств. Широко используемым подмножеством кодов БЧХ являются коды Рида — Соломона. Это такие коды БЧХ, у которых мультипликативный порядок алфавита символов кодового слова делится на длину кода. Согласно теореме о границе Рейгера, коды Рида — Соломона являются оптимальными с точки зрения соотношения длины пакета и возможности исправления ошибок — используя $2t$ дополнительных проверочных символов исправляется t ошибок (и менее) [26]. Код Рида — Соломона является одним из наиболее мощных кодов, исправляющих групповые ошибки [26].

На эффективность нечеткого экстрактора влияет способ предварительного квантования «сырых» биометрических данных. В рамках эксперимента решено дискретизировать значения признака в соответствии с преобразованием $y = f(x)$, где x — значение признака, а y принадлежит множеству {0, 1, 3, 7, 15, 31, 63, 127, 255, 254, 252, 248, 240, 224, 192, 128}. Значения y представляются в двоичном виде. Суть операции преобразования иллюстрирует рис. 3. Данное преобразование существенно уменьшает количество единичных ошибок на этапе квантования, что сказывается на вероятностях ошибок 1-го и 2-го рода (они также снижаются). Кроме того, возрастает длина генерируемого ключа. Однако энтропия квантованных данных сильно падает, что, конечно, отрицательно сказывается на защитных свойствах экстрактора (ключ и биометрию субъекта более нельзя считать надежно защищенной, если ее хранить в открытой строке). Также этот способ требует знания границ области значений признаков, т. е. экстрактор нужно обучить на образцах данных «Чужой», следовательно, одно из преимуществ экстрактора исчезает (см. табл. 1). Но даже при таком способе квантования нечеткий экстрактор работает хуже нейронных сетей,



■ ***Рис. 3.*** Квантование «сырых» биометрических данных

как можно убедиться далее. Более «честным» способом квантования является квантование данных, предложенное в работах [23, 27]. Но при таком способе в описанном пространстве признаков и при увеличении количества испытуемых до 65 (в работах [23, 27] оценки ошибок носили предварительный характер, надежность оценивалась на малых выборках и малом количестве испытуемых — 12–14) ошибки выработки ключа оказываются значительны (сумма ошибок 1-го и 2-го рода превышает 0,5). В настоящем исследовании предлагается модификация нечеткого экстрактора с оценкой стабильности битового представления признаков по формуле [8, 19]

$$\omega_i = 2 \cdot |0{,}5 - P_{0,i}| = 2 \cdot |0{,}5 - P_{1,i}|, \qquad (6)$$

где $P_{0,i}$ — вероятность (относительная частота) появления нуля в i-м разряде кода; $P_{1,i}$ — вероятность (относительная частота) появления единицы в i-м разряде кода.

Для каждого субъекта выбирается определенное количество признаков, для которых произведения вычисляемых по формуле (6) величин будет наивысшим.

При использовании описанной модификации нужно хранить дополнительную информацию о номерах стабильных признаков. Для усиления защитных свойств экстрактора данную информацию целесообразно держать в секрете, т. е. требуется отдельный сервер или носитель. Реализацию такого экстрактора нельзя назвать простой, т. е. этим нивелируется одно из преимуществ подхода (см. табл. 1). Но вероятность ошибок при этом снижается.

Модель нейронной сети

В ГОСТ Р 52633.5-2011 [8] рекомендуется использовать однослойные или двухслойные нейронные сети (сети с большим количеством слоев являются избыточными, и для их применения необходимо специальное обоснование [6]). Первый слой осуществляет обогащение данных, второй играет роль кодов, исправляющих ошибки [8]. Алгоритм из ГОСТ Р 52633.5-2011 служит для послойного обучения сети нейронов: сначала осуществляется обучение первого слоя, далее эти же обучающие данные подаются на вход второго слоя сети, и вычисляются весовые коэффициенты нейронов второго слоя. Модули весов нейронов вычисляются детерминированно по нижеприведенным формулам (7) и (8) [8]

$$\mu_i = |E_{\text{ч}}(x_i) - E_{\text{с}}(x_i)|/\sigma_{\text{ч}}(x_i) \cdot \sigma_{\text{с}}(x_i), \qquad (7)$$

где $E_{\text{с}}(x_i)$ — математическое ожидание (среднее значение) значений признака для образа «Свой»; $\sigma_{\text{с}}(x_i)$ — среднеквадратичное отклонение значений признака для образа «Свой»; $E_{\text{ч}}(x_i)$ и $\sigma_{\text{ч}}(x_i)$ — аналогичные показатели для образа «Чужой». Знак весового коэффициента при условии, что нейрон должен выдавать единицу («1»), выбирается исходя из правила: «+», если $E_{\text{ч}}(x_i) < E_{\text{с}}(x_i)$, иначе «–». Если нейрон должен выдавать ноль («0»), знаки весовых коэффициентов инвертируются:

$$\mu_i = a_2\omega_i/E(\omega_i), \qquad (8)$$

где a_2 — стабилизирующий коэффициент для нейронов второго слоя, экспериментально подбираемый для каждой задачи выработки ключа; ω_i — показатель стабильности i-го разряда выходного кода нейронов первого слоя, вычисляемый по формуле (6) [8, 19]; $E(\omega_i)$ — математическое ожидание (среднее значение) показателей стабильности разрядов выходного кода нейронов первого слоя.

Алгоритм обучения позволяет настроить сеть на выдачу заданного ключа и случайной битовой последовательности при поступлении образа неизвестного пользователя.

При использовании второго слоя необходимо перейти от промежуточных кодов «0» и «1» к эквивалентным «–1» и «1». Число входов нейронов второго слоя рекомендуется выбирать от 0,2 до 0,8 от числа нейронов первого слоя. Рекомендации по выбору количества нейронов первого и второго слоя аналогичные и описаны в стандарте [8]. Связи нейронов первого слоя с нейронами второго слоя задаются случайно. Обработчики признаков связывают с нейронами первого слоя сначала последовательно, а при превышении номера нейрона над числом признаков — случайно. Далее осуществляется корректировка знаков весовых коэффициентов, которая носит эмпирический характер, с целью добиться желаемой вероятности ошибок аутентификации [8]. Выход сумматора нейрона любого слоя на этапе принятия решений определяется по формуле

$$y = \sum_{i=1}^{m} \mu_i v_i + \mu_0, \qquad (9)$$

где v_i — i-й вход нейрона; m — число входов; μ_i — весовой коэффициент i-го входа; μ_0 — нулевой вес, отвечающий за переключатель квантования нейрона.

Модели сетей квадратичных форм

В настоящей работе проверяется три модели сетей квадратичных форм на основе соответствующих мер близости: Пирсона, Байеса — Пирсона и Евклида. Метрика Пирсона заключается в получении интегральной оценки близости (расстояния) входного образца к эталону образа по формуле

$$\chi = \sum_{i=1}^{m} \frac{(E(v_i) - v_i)^2}{\sigma(v_i)^2}, \qquad (10)$$

где v_i — i-й вход нейрона; $E(v_i)$ — математическое ожидание (среднее значение) i-го входа нейрона; $\sigma(v_i)$ — среднеквадратичное отклонение i-го входа нейрона.

Данная метрика не учитывает корреляционных связей между признаками образа, поэтому с ростом корреляционных связей ее мощность падает [21]. В этом случае рекомендуется пользоваться метрикой Байеса — Пирсона [21], рассчитываемой по формуле

$$\chi = \sum_{j=1}^{m}\sum_{i=1}^{m}\left|\frac{|E(v_i)-v_i|}{\sigma(v_i)} - \frac{|E(v_j)-v_j|}{\sigma(v_j)}\right|. \qquad (11)$$

Метрика Байеса — Пирсона [21] не содержит в явной форме вычислительных операций с коэффициентами корреляции, однако коэффициенты многомерной корреляции биометрических данных сильно влияют на нее [21]. Таким образом, данная метрика позволяет определять близость образца не только к эталону образа, но и близость к эталону корреляционных связей образа. Следовательно, эта метрика должна лучше работать в пространстве сильно коррелирующих признаков, чем метрика Пирсона.

Последней рассматриваемой квадратичной формой является метрика Евклида, вычисляемая по формуле

$$\varepsilon = \sqrt{\sum_{i=1}^{m}\left(E(v_i)-v_i\right)^2}. \qquad (12)$$

Данная метрика является более слабой, так как не учитывает среднеквадратичное отклонение биометрического параметра.

Сеть квадратичных форм можно реализовать с одним слоем нейронов или двумя слоями нейронов. Первый слой состоит из нейронов, рассчитывающих выход по одной из указанных выше формул, от этого зависит тип сети: Пирсона — Хемминга, Байеса — Пирсона — Хемминга, Евклида — Хемминга (могут существовать и другие виды нейронов на базе иных квадратичных форм), либо это гибридная сеть, если она состоит из различных типов нейронов (такой вариант в рамках статьи не рассматривается). Полученное значение далее сравнивается с пороговым. Для каждого нейрона имеется свое оптимальное пороговое значение, которое подбирается эмпирически, исходя из произведения $\theta = \chi_{max} a_1$, где χ_{max} — максимальное значение квадратичной формы при поступлении на вход обучающих примеров образа «Свой»; a_1 — стабилизирующий коэффициент, экспериментально подбираемый для каждого пространства признаков. Далее при превышении порога нейрон выдает единицу («1»), иначе ноль («0»). При необходимости настройки на нужный выходной ключ нейрон можно перепрограммировать, инвертировав данные выходные значения. Флаг инверсии будет также являться параметром нейрона наряду с параметрами распределения признаков. Ввиду того, что нейрон сравнивает вычисляемую величину с пороговым значением и на выходе выдает бинарное значение, квадратичные формы называют не только по имени метрики, но и по имени Хемминга.

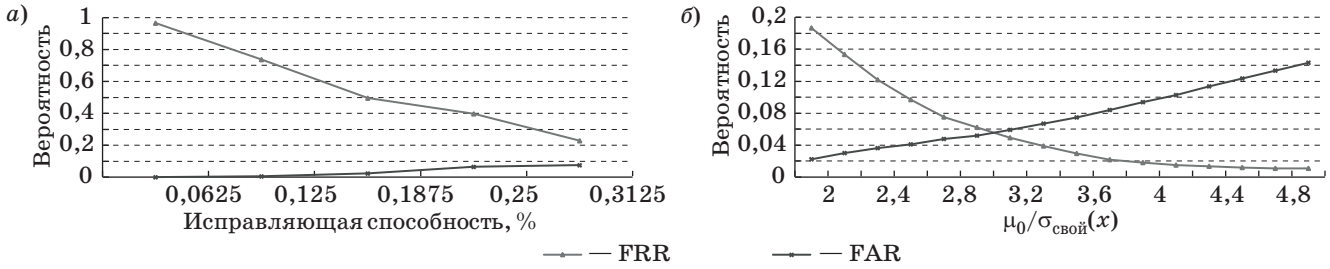
Второй слой нейронной сети можно полностью скопировать из стандарта ГОСТ Р 52633.5-2011 [8]. Второй слой играет роль кодов, исправляющих ошибки, его можно применить к любой нейросети, будь то сеть квадратичных форм, персептрон или его модификация. В качестве альтернативы второго слоя можно применить схемы [13] восстановления ошибочных бит ключа. В рамках данной работы второй слой квадратичных форм не рассматривается.

Результаты проведенного эксперимента

Проведено натурное моделирование (вычислительный эксперимент с реальными биометрическими данными субъектов, как при натурном, только информация подавалась на вход алгоритмов в автоматическом режиме). Каждым испытуемым было введено не менее 50 образцов подписи. Часть этих данных использовалась для обучения, остальные — для экспериментальной оценки надежности аутентификации (выработки ключа доступа). Количество образцов обучающей выборки решено сделать идентичным для нейронных сетей, сетей квадратичных форм и нечетких экстракторов: 21 реализация образа «Свой» и 64 реализации образа «Чужой» для персептронов (по одной реализации на каждого другого испытуемого). Вероятности ошибок 1-го и 2-го рода подсчитывались следующим образом: $FRR = er_1/ex_1$, $FAR = er_2/ex_2$, где er — количество ошибок соответствующего рода, ex — количество опытов для выявления ошибки соответствующего рода. Также подсчитывалась сумма ошибок 1-го и 2-го рода *ErrorRate* (ER) как площадь пересечения функций плотностей вероятности расстояний Хемминга от генерируемых кодов реализациями образов «Свой» до ожидаемого (идеального) кода и от генерируемых кодов реализациями образов «Чужой». Указанные плотности аппроксимировались нормальным законом распределения для кодов «Чужой» и бета-распределением для кодов «Свой» [6, 10]. Оптимальным размером блока для кодов Адамара является 6 бит, так как при этом значении достигается наименьший процент ошибок. Коды Рида — Соломона целесообразно использовать с максимально возможной исправляющей способностью (рис. 4, *а*, *б*). Тестирование нейронных сетей

будет проводиться без построения защищенного нейросетевого контейнера. Данное требование формулировалось в работах [4, 6] по отношению к стандартизованным персептронам. Лучшие результаты (по наименьшей сумме FFR и FAR) проведенного натурного моделирования приведены в табл. 2.

Получаемая длина ключа завышена (энтропия вырабатываемого кода не соответствует его длине), в особенности у экстракторов, так как используемый способ квантования дает низкую энтропию биокода, при иной методике квантования показатели FRR, FAR и ER для нечетких экстракторов становятся в разы выше.



■ ***Рис. 4.*** Вероятности ошибок выработки ключа нечетким экстрактором на основе кодов Рида — Соломона (*а*) и нейронной сетью по ГОСТ Р52633.5-2011 с одним слоем (*б*) при использовании 236 признаков

■ ***Таблица 2.*** Основные результаты эксперимента

Сравнение НПБК с нечеткими экстракторами				
Способ, количество признаков	FRR	FAR	ER	Длина ключа, бит
Экстрактор (коды Адамара), 228	0,148	0,05	0,075	304
Экстрактор (коды Рида — Соломона), 236	0,228	0,076	0,308	360
Экстрактор (коды Рида — Соломона), 90	0,191	0,033	0,21	150
НПБК (1 слой), 236	0,029	0,074	0,068	236
НПБК (2 слоя), 236	0,045	0,051	0,056	236
Сравнение НПБК с сетями квадратичных форм				
Способ (236 признаков)	FRR	FAR	ER	Число входов нейрона
Сеть Пирсона — Хемминга	0,044	0,046	0,057	59
Сеть Байеса — Пирсона — Хемминга	0,045	0,039	0,056	59
Сеть Евклида — Хемминга	0,097	0,118	0,302	59
Персептрон ГОСТ Р 52633.52011	0,028	0,076	0,067	59
Персептрон (2 компаратора)	0,029	0,077	0,064	59
Персептрон (третичное квантование)	0,033	0,079	0,068	59
Сеть Пирсона — Хемминга	0,041	0,054	0,058	118
Сеть Байеса — Пирсона — Хемминга	0,045	0,051	0,060	118
Сеть Евклида — Хемминга	0,084	0,155	0,314	118
Персептрон ГОСТ Р 52633.5-2011	0,029	0,074	0,068	118
Персептрон (2 компаратора)	0,027	0,077	0,064	118
Персептрон (третичное квантование)	0,035	0,080	0,068	118
Сеть Пирсона — Хемминга	0,032	0,066	0,059	177
Сеть Байеса — Пирсона — Хемминга	0,036	0,064	0,062	177
Сеть Евклида — Хемминга	0,066	0,211	0,320	177
Персептрон ГОСТ Р 52633.5-2011	0,02	0,1	0,067	177
Персептрон (2 компаратора)	0,017	0,109	0,066	177
Персептрон (третичное квантование)	0,021	0,11	0,068	177

Заключение

По результатам проведенного эксперимента нечеткие экстракторы уступают в надежности аутентификации нейросетевым преобразователям «биометрия-код», выполненным по ГОСТ Р 52633.5-2011. Защитные свойства нечетких экстракторов также хуже и имеют большее число недостатков. Этот вывод подтверждается данными из научной литературы. По данным экспериментальных оценок сети квадратичных форм Пирсона — Хемминга и Байеса — Пирсона — Хемминга превосходят персептроны из ГОСТ Р 52633.5-2011 по надежности выработки ключа доступа. Сеть Евклида — Хемминга работает значительно хуже других сетей квадратичных форм. Замена нечетной ступенчатой квантующей функции персептрона из ГОСТ Р 52633.5-2011 на четную функцию двухстороннего ограничения не дала заметного повышения эффективности работы. Аналогичные результаты получены и при использовании трид-нейронов. Сеть Пирсона — Хемминга при увеличении входов нейронов работает лучше сети Байеса — Пирсона — Хемминга, однако при уменьшении количества входов сеть Байеса — Пирсона — Хемминга становится более эффективной, чем сеть Пирсона — Хемминга. Наилучший результат в рамках эксперимента получен на основе сети Байеса — Пирсона — Хемминга с 59 входами каждого нейрона при 236 признаках, вероятности ошибок составили: FRR = 0,045, FAR = 0,039, сумма ошибок 1-го и 2-го рода была наименьшей — 0,084.

Работа выполнена при финансовой поддержке РФФИ (грант № 16-07-01204).

Литература

1. The Global State of Information Security® Survey 2016. PricewaterhouseCoopers. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html (дата обращения: 27.06.2016).
2. **Хогланд Г.** Руткиты: внедрение в ядро Windows. — СПб.: Питер, 2007. — 285 с.
3. **Иванов А. И.** Нейросетевые алгоритмы биометрической идентификации личности / под ред. А. И. Галушкина. –– М.: Радиотехника, 2004. — 144 с. — (Научная серия «Нейрокомпьютеры и их применение». № 15).
4. ГОСТ Р 52633.0-2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. — М.: Стандартинформ, 2006. — 24 с.
5. **Dodis Y., Reyzin L., Smith A.** Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy// EUROCRYPT. April 13, 2004. P. 523–540.
6. **Ахметов Б. С.** и др. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа / Б. С. Ахметов, А. И. Иванов, В. А. Фунтиков, А. В. Безяев, Е. А. Малыгина: монография. — Алматы: Издательство LEM, 2014. — 144 с.
7. **Волчихин В. И.** и др. Перспективы использования искусственных нейронных сетей с многоуровневыми квантователями в технологии биометрико-нейросетевой аутентификации / В. И. Волчихин, А. И. Иванов, В. А. Фунтиков, Е. А. Малыгина // Изв. высших учебных заведений. Поволжский регион. 2013. № 4(28). С. 86–96.
8. ГОСТ Р52633.5-2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа. — М.: Стандартинформ, 2011. — 20 с.
9. **Безяев А. В., Иванов А. И., Фунтикова Ю. В.** Оптимизация структуры самокорректирующегося биокода, хранящего синдромы ошибок в виде фрагментов хеш-функций // Вестник УрФО. Безопасность в информационной сфере. 2014. № 3(13). С. 4–13.
10. **Иванов А. И.** Нейросетевая защита конфиденциальных биометрических образов гражданина и его личных криптографических ключей: монография. —Пенза: ПНИЭИ, 2014. — 57 с.
11. **Ахметов Б. С., Иванов А. И., Серикова Н. И.** Алгоритм искусственного повышения числа степеней свободы при анализе биометрических данных по критерию согласия хи-квадрат // Вестник Национальной академии наук Республики Казахстан. 2014. № 5. С. 28.
12. **Иванов А. И.** и др. Сравнение мощности хи-квадрат критерия и критерия Крамера — фон Мизеса для малых тестовых выборок биометрических данных/ А. И. Иванов, А. И. Газин, С. Е. Вятчанин, К. А. Перфилов // Надежность и качество сложных систем. 2016. № 2(14). С. 21–28.
13. **Васильев В. И.** Интеллектуальные системы защиты информации: учеб. пособие. 2-е изд., испр. и доп. — М.: Машиностроение, 2012. — 199 с.
14. **Busch C.** Biometrics and Security / NIS Net – Winter School FINSE. April 27, 2010. http://www.nisnet, no/filer/Finse 10/Biometrics_and_ Security_ Busch.pdf (дата обращения: 27.06.2016).
15. **Cavoukian A., Stoianov A.** Biometric Encryption Chapter from the Encyclopedia of Biometrics. http://www.ipc.on.ca/images/Resours/bio-encrypt-chp.pdf (дата обращения: 27.06.2016).
16. **Куликова О. В.** Биометрические криптографические системы и их применение. http://www.pvti.ru/data/file/bit/bit_3_2009_10.pdf (дата обращения: 27.06.2016).
17. **Juels A., Sudan M.** A Fuzzy Vault Scheme // Designs, Codes and Cryptography. February 2006. Vol. 38. Iss. 2. P. 237–257. doi:10.1007/s10623-005-6343-z

18. **Juels A., Wattenberg M.** A Fuzzy Commitment Scheme // Proc. ACM Conf. Computer and Communications Security. 1999. P. 28–36.
19. **Иванов А. И.** и др. О многообразии метрик, позволяющих наблюдать реальные статистики распределения биометрических данных «нечетких экстракторов» при их защите наложением гаммы / А. И. Иванов, С. А. Сомкин, Д. Ю. Андреев, Е. А. Малыгина // Вестник УрФО. Безопасность в информационной сфере. № 2(12). 2014. С. 16–23.
20. **Scotti F.,** et al. Privacy-aware Biometrics: Design and Implementation of a Multimodal Verification System / F. Scotti, S. Cimato, M. Gamassi, V. Piuri, R. Sassi // 2008 Annual Computer Security Applications Conf. IEEE. 2008. P. 130–139.
21. **Ложников П. С.** и др. Биометрическая идентификация рукописных образов с использованием корреляционного аналога правила Байеса/ П. С. Ложников, А. И. Иванов, Е. И. Качайкин, А. Е. Сулавко // Вопросы защиты информации. 2015. № 3. С. 48–54.
22. **Иванов А. И., Ложников П. С., Качайкин Е. И.** Идентификация подлинности рукописных автографов сетями Байеса — Хэмминга и сетями квадратичных форм // Вопросы защиты информации. 2015. № 2. С. 28–34.
23. **Lozhnikov P. S., Sulavko A. E., Volkov D. A.** Application of Noise Tolerant Code to Biometric Data to Verify the Authenticity of Transmitting Information // Control and Communications (SIBCON), Omsk, Russia, May 21–23, 2015. P. 1–3. doi:10.1109/SIBCON.2015.7147126
24. **Еременко А. В.** и др. Генерация криптографических ключей на основе подписей пользователей компьютерных систем/ А. В. Еременко, Майков В. Б., Ступко К. О., Мироненко О. Е. // Аппроксимация логических моделей, алгоритмов и задач — АЛМАЗ'2: материалы Второй Междунар. конф., Омск, 27–30 апреля 2015 г. С. 23–27.
25. **Еременко А. В.** Повышение надежности идентификации пользователей компьютерных систем по динамике написания паролей: автореф. дис. ... канд. техн. наук. — Омск: СибАДИ, 2011. — 20 с.
26. **Robert H. Morelos-Zaragoza.** The Art of Error Correcting Coding. — John Wiley & Sons, 2006. — 320 p.
27. **Еременко А. В., Сулавко А. Е.** Способ двухфакторной аутентификации пользователей компьютерных систем на удаленном сервере с использованием клавиатурного почерка // Прикладная информатика. 2015. № 6. С. 48–59.

UDC 004.93'1
doi:10.15217/issn1684-8853.2016.5.73

Experimental Evaluation of Reliability of Signature Verification by Quadratic Form Networks, Fuzzy Extractors and Perceptrons

Lozhnikov P. S.[a], PhD, Tech, Associate Professor
Sulavko A. E.[a], PhD, Tech, Senior Lecturer
Eremenko A. V.[b], PhD, Tech, Associate Professor
Volkov D. A.[a], Post-Graduate Student
[a]Omsk State Technical University, 11, Mira Ave., 644050, Omsk, Russian Federation
[b]Omsk Transport University, 35, Karl Marx Ave., 644046, Omsk, Russian Federation

Purpose: The problems of information security become more and more pressing, therefore the demands to biometric systems become tougher. Our objective is to compare fuzzy extractors, neural network biometry-code converters and networks of quadratic forms by their authentication reliability, on the base of signature features. **Results:** We have analyzed the literature and conducted a series of numerical experiments based on real biometric data. The main result of the experiments is that fuzzy extractors are significantly inferior to the other system by their authentication reliability and the key length. The best performance was provided by Bayesian–Pearson networks. **Practical relevance:** The results will be of interest to researchers and developers of biometric systems.

Keywords — Signature Reproduction Features, Biometrics, Fuzzy Extractors, Artificial Neural Networks, Authentication.

References

1. *The Global State of Information Security® Survey 2016. PricewaterhouseCoopers.* Available at: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html (accessed 27 June 2016).
2. Hogland G. *Rutkity: vnedrenie v iadro Windows* [Rootkits: Subverting the Windows Kernel]. Saint-Petersburg, Piter Publ., 2007. 285 p. (In Russian).
3. Ivanov A. I. *Neirosetevye algoritmy biometricheskoi identifikatsii lichnosti* (Nauchnaia seriia "Neirokomp'iutery i ikh primenenie", no. 15) [Neural Network Algorithms for Biometric Identification (Science Series "Neurocomputers and their Application", no. 15]. A. I. Galushkin ed. Moscow, Radiotekhnika Publ., 2004. 144 p. (In Russian).
4. State Standard R52633.0-2006. Data Protection. Information Protection Technique. Requirements for Highly Reliable Means of Biometric Authentication. Moscow, Standartinform Publ., 2006. 24 p. (In Russian).
5. Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy. *EUROCRYPT*, April 2004, pp. 523–540.
6. Ahmetov B. S., Ivanov A. I., Funtikov V. A., Bezjaev A. V., Malygina E. A. *Tekhnologiia ispol'zovaniia bol'shikh neironnykh setei dlia preobrazovaniia nechetkikh biometricheskikh dannykh v kod kliucha dostupa* [Technology of Using Large Neural Networks for Fuzzy Transformation of Biometric Data in the Access Code Key].

Almaty, Izdatel'stvo LEM Publ., 2014. 144 p. (In Russian).
7. Volchihin V. I., Ivanov A. I., Funtikov V. A., Malygina E. A. Prospects of Using Artificial Neural Networks with Multi-Level Quantizers Technology in Biometrics-Neural Network Authentication. *Izvestiia vysshikh uchebnykh zavedenii. Povolzhskii region*, 2013, no. 4(28), pp. 86–96 (In Russian).
8. State Standard R 52633.5-2011. Data Protection. Information Protection Technique. Automatic Learning Neural Network Converters Biometry-Code Access. Moscow, Standartinform Publ., 2011. 20 p. (In Russian).
9. Bezjaev A. V., Ivanov A. I., Funtikova Ju. V. Optimization of the Structure of Bio-Self-Correcting Code Storing Error Syndromes as Fragments of Hash Functions. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere*, 2014, no. 3(13), pp. 4–13 (In Russian).
10. Ivanov A. I. *Neirosetevaia zashchita konfidentsial'nykh biometricheskikh obrazov grazhdanina i ego lichnykh kriptograficheskikh kliuchei* [Neural Protection of Sensitive Biometric Images of the Citizen and his Personal Cryptographic Keys]. Penza, PNIEI Publ., 2014. 57 p. (In Russian).
11. Ahmetov B. B., Ivanov A. I., Serikova N. I. The Algorithm is an Artificial Increase in the Number of Degrees of Freedom in the Analysis of the Biometric Data on the Criterion of the Consent of The Chi-Square. *Vestnik Natsional'noi akademii nauk Respubliki Kazakhstan*, 2014, no. 5, pp. 28 (In Russian).
12. Ivanov A. I., Gazin A. I., Perfilov K. A., Vyatchanin S. E. Noise Elimination of Quantization Biometric Data While Using Multivariate Test Cramer – Von Mizes in Small Samples. *Nadezhnost' i kachestvo slozhnykh system*, 2016, no. 2(14), pp. 21–28 (In Russian).
13. Vasil'ev V. I. *Intellektual'nye sistemy zashchity informatsii* [Intelligent Information Security Systems]. Moscow, Mashinostroenie Publ., 2012. 199 p. (In Russian).
14. Busch C. Biometrics and Security. *NISNet – FINSE Winter School*, April 27, 2010. Available at: http://www.nisnet, no/filer/Finse 10/Biometrics_and_ Security_ Busch:pdf (accessed 26 June 2016).
15. Cavoukian A., Stoianov A. *Biometric Encryption Chapter from the Encyclopedia of Biometrics*. Available at: http://www.ipc.on.ca/images/Resours/bio-encrypt-chp.pdf (accessed 26 June 2016).
16. Kulikova O. V. *Biometricheskie kriptograficheskie sistemy i ikh primenenie* [Biometric Cryptographic Systems and their Applications]. Available at: http://www. pvti.ru/ data/file/bit/bit_3_2009_10.pdf (accessed 26 June 2016).
17. Juels A., Sudan M. A Fuzzy Vault Scheme. *Designs, Codes and Cryptography*, February 2006, vol. 38, iss. 2, pp. 237–257. doi: 10.1007/s10623-005-6343-z
18. Juels A., Wattenberg M. A Fuzzy Commitment Scheme. *Proc. ACM Conf. Computer and Communications Security*, 1999, pp. 28–36.
19. Ivanov A. I., Somkin S. A., Andreev D. Ju., Malygina E. A. The Variety of Metrics that Allow to Observe the Real Statistical Distribution of Biometric Data "Fuzzy Extractors" under the Protection of their Scale Overlay. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere*, 2014, no. 2(12), pp. 16–23 (In Russian).
20. Scotti F., Cimato S., Gamassi M., Piuri V., Sassi R. Privacy-aware Biometrics: Design and Implementation of a Multimodal Verification System. *2008 Annual Computer Security Applications Conf.*, IEEE, 2008, pp. 130–139.
21. Lozhnikov P. S., Ivanov A. I., Kachaykin E. I., Sulavko A. E. Biometric Identification of Manuscript Images Using Analog Correlation Bayes Rule. *Voprosy zashchity informatsii* [Issues of Protection of Information], 2015, no. 3, pp. 48–54 (In Russian).
22. Ivanov A. I., Lozhnikov P. S., Kachaykin E. I. Identification of the Authenticity of Handwritten Autographs Bayesian-Hamming Networks and Quadratic Forms Networks. *Voprosy zashchity informatsii* [Issues of Protection of Information], 2015, no. 2, pp. 28–34 (In Russian).
23. Lozhnikov P. S., Sulavko A. E., Volkov D. A. Application of Noise Tolerant Code to Biometric Data to Verify the Authenticity of Transmitting Information. *Control and Communications (SIBCON)*, Omsk, Russia, May 21–23, 2015, pp. 1–3. doi:10.1109/SIBCON.2015.7147126
24. Eremenko A. V., Majkov V. B., Stupko K. O., Mironenko O. E. The Generation of Cryptographic Keys Based on the Signatures of Computer System Users. *Materialy Vtoroi Mezhdunarodnoi konferentsii "Approksimatsiia logicheskikh modelei, algoritmov i zadach – ALMAZ'2* [Proc. of the Second Intern. Conf. "Approximation of Logic Models, Algorithms and Tasks"], Omsk, April 27–30, 2015, pp. 23–27 (In Russian).
25. Eremenko A. V. *Povyshenie nadezhnosti identifikatsii pol'zovatelei komp'iuternykh sistem po dinamike napisaniia parolei*. Dis. kand. tehn. nauk [Improving the Reliability of Computer Systems Users Identification by the Dynamics of Writing Passwords. PhD tech. sci. diss.]. Omsk, SibADI Publ., 2011. 20 p. (In Russian).
26. Robert H. Morelos-Zaragoza. *The Art of Error Correcting Coding*. John Wiley & Sons, 2006. 320 p.
27. Eremenko A. V., Sulavko A. E. A Method of Two-Factor Authentication of Computer Systems Users on a Remote Server by Using Keyboard Handwriting. *Prikladnaia informatika* [Applied Informatics], 2015, no. 6, pp. 48–59 (In Russian).

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая SCOPUS и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, снижая рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста: входите на страницу http://www.researcherid.com, слева под надписью «New to ResearcherID?» нажимаете на синюю кнопку «Join Now It's Free» и заполняете короткую анкету. По указанному электронному адресу получаете сообщение с предложением по ссылке заполнить полную регистрационную форму на ORCID. Получаете ID.

УДК 004.42
doi:10.15217/issn1684-8853.2016.5.86

ВАРИАНТ АРХИТЕКТУРЫ УПРАВЛЯЮЩЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ РАЗРЕШЕНИЯ ПРОБЛЕМНЫХ СИТУАЦИЙ НА ПРЕДПРИЯТИИ

В. Н. Шведенко[а], *доктор техн. наук, профессор*
О. В. Щекочихин[б], *канд. техн. наук, доцент*
П. В. Шведенко[б], *аспирант*
[а]*ООО «РЕГУЛ +», Санкт-Петербург, РФ*
[б]*Костромской государственный университет, Кострома, РФ*

Постановка проблемы: *монолитные информационно-управляющие системы предприятия обладают большой инерцией в плане расширения функциональных возможностей, что не позволяет оперативно реагировать на изменения в материальной системе. Одним из методов разрешения указанной проблемы является переход к интегрированным информационным системам. Однако известные подходы не дают возможности быстро интегрировать новое приложение в информационную систему и создают проблемы при автоматизации управленческих воздействий в нестандартных ситуациях.* ***Цель:*** *разработка теоретических основ построения архитектуры интегрированной информационной системы, способной настраиваться на разрешение проблемной ситуации без изменения ее архитектуры.* ***Результаты:*** *предложено наделять информационную систему свойством поведения. Поведение системы — это процесс целенаправленного изменения во времени состояния системы. Функция поведения информационной системы появляется в момент возникновения проблемной ситуации в материальной системе при отсутствии опыта разрешения этой проблемной ситуации. При проектировании систем с поведением наделение системы новыми функциями должно происходить без изменения ее архитектуры. Дано теоретико-множественное описание отражения деятельности предприятия через систему показателей и метамодель проблемной ситуации. Разработан алгоритм поиска данных, необходимых для информационной поддержки разрешения проблемной ситуации. Предложен вариант архитектуры интегрированной информационной системы на основе многослойной шины данных.*

Ключевые слова *— поведение информационной системы, интеграция информационных систем, системы управления предприятием, метамодель.*

Введение

Материальная система современного предприятия очень динамична, что выражается в существенных изменениях организационных структур, приобретении нового технологического оборудования, изменении технологических и производственных процессов, модернизации бизнес-процессов в организационном управлении, пересмотре нормативной базы, диверсификации и т. п.

Монолитные информационно-управляющие системы предприятия обладают большой инерцией в плане расширения функциональных возможностей, что не позволяет оперативно реагировать на изменения в материальной системе. Одним из методов разрешения указанной проблемы является переход к интегрированным информационным системам (ИИС) [1–4]. Однако и в ИИС при расширении их функциональных возможностей имеют место такие ограничения, как необходимость фиксации структур данных для обеспечения целостности; сложность в сопоставлении информационных ресурсов в разных системах метаданных; узкоспециализированные, частные решения; трудоемкость, а следовательно, высокая стоимость разработки, внедрения и владения [5–10].

Для того чтобы снять вышеуказанные ограничения, предлагается наделять информационную систему свойством поведения [11]. При проектировании системы с поведением должно соблюдаться условие неизменности ее архитектуры при наделении новыми функциями.

Метод создания интегрированной информационно-управляющей системы с поведением на основе сервис-ориентированной архитектуры

Функция поведения активизируется, когда для оценки проблемной ситуации требуются новые информационные ресурсы или новые алгоритмы их обработки. Проблемные ситуации разделяются на типовые и оригинальные. Функция поведения информационной системы появляется в момент возникновения проблемной ситуации в материальной системе при отсутствии опыта разрешения этой проблемной ситуации. Материальная система предприятия рассматривается как набор бизнес-процессов, которые имеют вход и выход определенного ресурса, структуру в виде отдельных этапов. Информационная система имеет контакт с материальной системой в центрах ответственности (ЦО), где происходит смена состояния ресурса, осуществляется анализ и принимаются управленческие решения.

Модель сетевой структуры управления будет иметь следующий вид:

$$W_i = \bigcup_{j=1}^{P} (A_j B_j F_j C_j D_j Q_j),$$

где A — дерево целей; B — множество решаемых системой управления задач; F — множество функций управления; C — множество объектов управления; D — множество бизнес-процессов; P — совокупность лиц, принимающих решения; Q — множество ресурсов.

При исполнении бизнес-процесса возможна обработка только заранее описанных ситуаций. При возникновении неописанной заранее ситуации бизнес-процесс вызывает необоснованные расходы ресурсов.

Множество ресурсов не однородно и представляет собой объединение множеств $Q = Q_1 \cup Q_2 \cup Q_3$, где Q_1, Q_2, Q_3 — множество приложений, источников данных и доступных функций приложений.

Выделяются следующие виды источников данных: базы данных, информационные системы предприятия, статистическая отчетность, ресурсы интернета, справочные системы и т. п. Как правило, полученная информация не является достаточной и требует аналитической обработки и соответствующих форматов вывода.

Приложение должно производить алгоритмические преобразования входной информации и выдавать результат в заранее заданном формате. Обрабатываемая информация должна позволять оценивать состояние процесса или состояние элемента материальной системы на заданном промежутке времени. Для использования приложения в ИИС его необходимо оценивать по следующему набору свойств: интегрируемость в операционную и сетевую среду информационной системы предприятия, возможность работы с заданным видом информационного ресурса, возможность получения выборки данных из ресурса по необходимым характеристикам и временному интервалу.

Методы обработки данных, реализуемые приложением, подразделяются на следующие группы: статистическая обработка данных, корреляционный анализ, многофакторный анализ, интеллектуальный анализ данных с использованием нейронных сетей, когнитивный анализ.

Варианты разрешения проблемной ситуации представляют собой многомерную структуру, проекция которой на трехмерное пространство является кубом, по осям координат которого располагаются:

1) приложения — Q_1;

2) источники данных — Q_2;

3) методы обработки (функции приложения) — Q_3.

Разрешение проблемной ситуации рассматривается как функция трех аргументов $U = f(Q_1, Q_2, Q_3)$.

В работе предлагается новый метод построения информационно-управляющей системы, которая позволяет разрешать проблемные ситуации посредством функции поведения. По заданным признакам проблемной ситуации определяются условия выбора метода обработки, приложения и источника данных.

Предлагается использовать сервис-ориентированную архитектуру — в информационной системе имеется набор независимых сервисов, которые обеспечивают получение данных из ее подсистем или обработку данных отдельным приложением в соответствии с выбранным вариантом разрешения проблемной ситуации (рисунок). Допускается, что сервис может выдавать избыточные данные. Для каждой проблемной ситуации в единой сервисной шине создается отдельный логический слой, обслуживающий обработку проблемной ситуации. Это позволяет уменьшить сложность архитектуры информационной системы за счет того, что при неизменном количестве элементов системы количество связей уменьшается, так как каждый слой обеспечивает связь центра ответственности за ресурс с сервисами соответствующих приложений. Увеличение количества элементов в системе влечет линейное увеличение связей по формуле $2n$, где n — количество элементов системы.

Управляющий модуль занимается оценкой проблемной ситуации, подготовкой нового логического слоя шины данных для информационного обеспечения принятия управленческого решения.

Информационная система автоматически передает в ЦО информацию о состоянии материальной системы в соответствии с деревом целей.

Множество вариантов разрешения проблемной ситуации расширяемо. Для добавления в информационную систему описания новой проблемной ситуации необходимо выделить ее характеристики, которыми являются показатели текущего состояния элементов материальной системы и их нормативные значения.

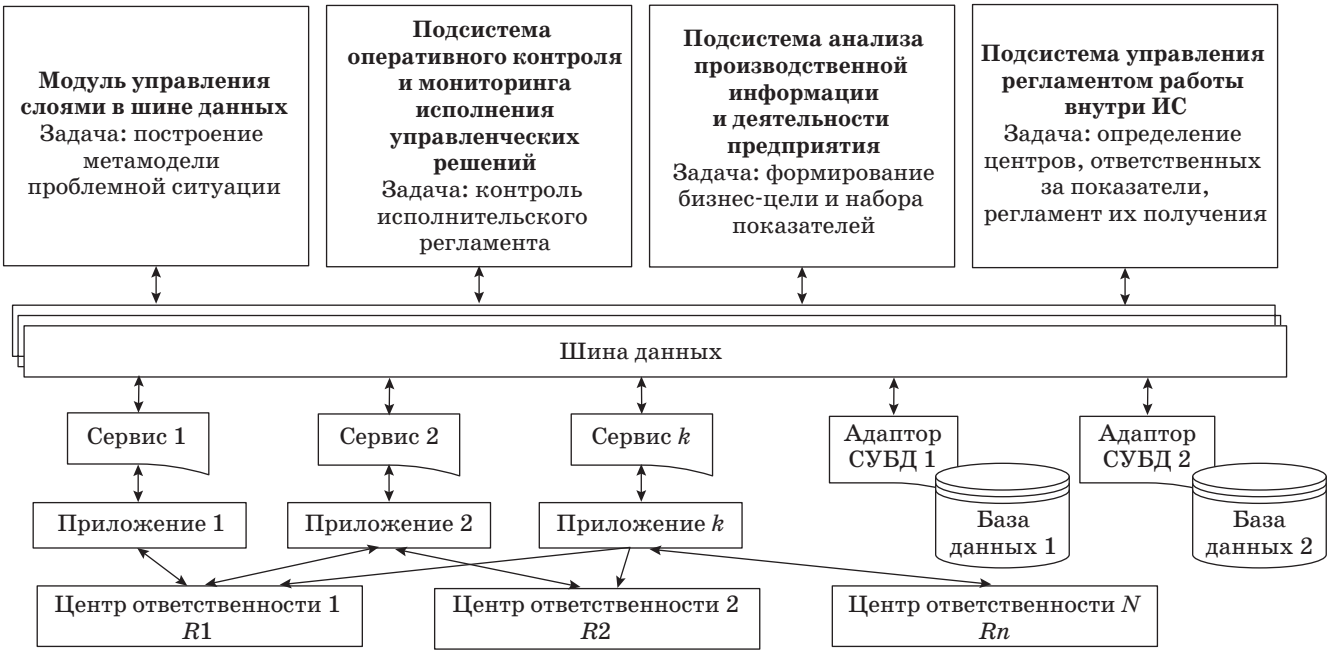
Формирование новых решений возможно через метамоделирование проблемных ситуаций. Метамодель отражения проблемной ситуации состоит из:

1) PR — множества показателей на предприятии;

2) $PR^{D_i} = PR^{C_0^{D_i}} \cup PR^{C_1^{D_i}} \cup \ldots \cup PR^{C_{n-1}^{D_i}}$ — множества комбинаций показателей по проблемным ситуациям, где C — множество объектов управления, D — множество бизнес-процессов;

3) PN — множества нормативных значений показателей;

4) PT — временного интервала измерения показателя.



■ Структурная схема информационной системы управления предприятием на основе сервис-ориентированной архитектуры

Информационная система управления настроена на сбор и мониторинг множества показателей деятельности предприятия, которые собираются в ЦО.

В центрах ответственности осуществляется оперативный сбор первичных данных и их обработка. Каждый ЦО за ресурс есть элемент множества R и представляет собой кортеж информации:

$$R = \{R_j\},$$
$$R_j = (P_j, C_j, H, PR),$$

где $C_j \in C$ — информационный объект; H — набор правил работы с информационным объектом в рамках описываемого бизнес-процесса; PR — множество показателей, которые характеризуют работу ЦО.

Элемент множества PR представляет собой кортеж информации:

$$PR_k = (PF, PN, Pl, Pu, n),$$

где $PF, PN, Pl, Pu \subset C$ — свойства информационного объекта ЦО; PF содержит фактическое значение показателя; PN содержит нормативное значение показателя; Pl, Pu определяют нижнюю и верхнюю границу допустимого диапазона значений показателя; n — имя показателя, дополнительная характеристика, которая требуется для придания смысловой характеристики показателя в системе показателей.

Если $PN = PF$, то работа ЦО по этому показателю оценивается как нормальная.

Если $PF \in [Pl, Pu]$, то работа ЦО по этому показателю оценивается как штатная.

Если $PF \notin [Pl, Pu]$, то работа ЦО по этому показателю оценивается как нештатная.

Объединение множеств показателей ЦО образует множество показателей деятельности предприятия на текущий момент времени.

Потребность в информационном ресурсе, который выдается приложением, определяется потоком задач, которые активизируются по результатам исполнения процессов или состояния элементов материальной системы.

По набору показателей, значения которых имеют отклонения от нормы в течение заданного лага времени, происходит идентификация проблемной ситуации.

При добавлении нового показателя необходимо привлекать бизнес-аналитика для определения признаков проблемной ситуации.

Поиск проблемной ситуации, выявление возможных альтернатив разрешения проблемной ситуации осуществляются информационной системой автоматически.

Для принятия решения по проблемной ситуации может понадобится новый сервис, новое приложение или новый источник данных.

Если ИИС имеет источник данных и приложение, предоставляющее необходимые методы их обработки, то достаточно разработать или настроить новый сервис для интеграции приложения.

Если ИИС имеет только источник данных, но не имеет инструментов их обработки, то необходимо выбрать их из существующих или разработать новое приложение и интегрирующий сервис.

Если ИИС для разрешения проблемной ситуации не имеет источника данных, то его необходимо сформировать либо подключить, а также подключить приложение для обработки этих данных.

После построения метамодели проблемной ситуации проектируется новая схема бизнес-процесса и размещается в репозиторий метамоделей.

При возникновении аналогичной проблемной ситуации ее разрешение будет проходить автоматически, путем извлечения из репозитория метамодели проблемной ситуации и метамодели бизнес-процесса ее разрешения. При исполнении бизнес-процесса в соответствующие центры ответственности выдаются команды, которые должны разрешить проблемную ситуацию. Таким образом реализуется функция поведения в информационной системе управления предприятием.

Вариант архитектуры реализован с использованием средств Oracle APEX. Возможности Oracle scheduler используются для мониторинга сервисов в модуле управления слоями шины данных, исполнения регламента бизнес-процессов. В целях поддержки работы шины данных используются хранимые процедуры, позволяющие динамически формировать SQL-запросы и осуществлять их выполнение.

Заключение

Рассмотрена проблема быстрого реагирования информационной системы управления предприятием на изменения внешней и внутренней среды. Предлагается наделить информационную систему свойством поведения. Дано теоретико-множественное описание отражения деятельности предприятия через систему показателей и метамодель проблемной ситуации, которое необходимо для формирования информационных потоков и структур баз данных информационной системы. Выделяются следующие компоненты: структура информационных объектов, структуры показателей деятельности материальной системы и структуры процессов получения и обработки данных. Предложен вариант архитектуры ИИС на основе многослойной шины данных.

Литература

1. **Жижимов О. Л., Федотов А. М., Шокин Ю. И.** Технологическая платформа массовой интеграции гетерогенных данных // Вестник НГУ. Сер. Информационные технологии. 2013. Т. 11. № 1. С. 24–41.
2. **Волков А. А., Шведенко В. Н.** Модель формирования параллельных структур в объектно-ориентированных СУБД// Программные продукты и системы. 2011. № 3. С. 14–17.
3. **Веселова Н. С., Шведенко В. Н.** Моделирование информационных ресурсов предприятия при процессной организации системы управления // Программные продукты и системы. 2014. № 4(108). С. 260–264.
4. **Кузькин А. А., Смирнов С. В., Басов О. О.** Модель обеспеченности стратегии развития информационных технологий в организации // Научно-технический вестник информационных технологий, механики и оптики. 2015. Т. 15. № 2. С. 305–312.
5. **Oleynik P. P.** Using Metamodel of object System for Domain-Driven Design the Database Structure // Proc. 12th IEEE East-West Design and Test Symposium (EWDTS'2014). Kiev, Ukraine, 2014. Art. 7027052. doi: 10.1109/EWDTS.2014.7027052
6. **Jaeger P. T.,** et al. Where is the Cloud? Geography, Economics, Environment, and Jurisdiction in Cloud Computing/ P. T. Jaeger, J. Lin, J. M. Grimes, S. N. Simmons // First Monday. 2009. Vol. 14. N 5. http://firstmonday.org/ojs/index.php/fm/article/view/2456/2171 (дата обращения: 03.08.2014).
7. **Sadiku M. N. O., Musa S. M., Momoh O. D.** Cloud Computing: Opportunities and Challenges // IEEE Potentials. 2014. Vol. 33. N 1. P. 34–36.
8. **Gagnon S.,** et al. The Next Web Apps Architecture: Challenges for SaaS Vendors/ S. Gagnon, V. Nabelsi, K. Passerini, K. Cakici // IT Professional. 2011. Vol. 13. N 5. P. 44–50.
9. **Владимиров А. В.** Агентное взаимодействие в информационной системе предприятия с адаптацией механизмов работы и интерфейса пользователя // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 6(88). С. 105–111.
10. **Сысолетин Е. Г., Аксенов К. А., Круглов А. В.** Интеграция гетерогенных информационных систем современного промышленного предприятия // Современные проблемы науки и образования. 2015. № 1. www.scienceeducation.ru/121-19030 (дата обращения: 25.05.2016).
11. **Шведенко В. Н., Щекочихин О. В., Шведенко П. В.** Критерии оценки и модели информационных систем, обладающих свойством поведения // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 4. С. 649–654. doi: 10.17586/2226-1494-2016-16-4-649-654

UDC 004.42
doi:10.15217/issn1684-8853.2016.5.86

A Possible Architecture for a Company's Management Information System Resolving Problem Situations

Shvedenko P. V.[a], Dr. Sc., Tech., Professor, shvn.d3@mail.ru
Shchekochikhin O. V.[b], PhD, Tech., Associate Professor, slim700@yandex.ru
Shvedenko P. V.[b], Graduate Student, pitk1@mail.ru
[a]OOO "REGUL+", P.O.Box 17, 193231, Saint-Petersburg, Russian Federation
[b]Kostroma State University of Technology, 17, Dzerzhinskogo St., 156005, Kostroma, Russian Federation

Purpose: Monolithic information management systems of companies do not readily enhance their functionality, responding too slowly to the changes in the material system. One of the ways to resolve this problem is choosing integrated information systems. However, the known approaches do not allow us to rapidly integrate a new application into the information system, creating problems for the automation of management actions in unusual situations. **Purpose:** We need to develop a theoretical basis in order to build an integrated information system architecture which can be easily configured to resolve a difficult situation. **Results:** It is proposed to endow an information system with the property of behavior. The behavior of a system is a process of targeted changes in the system status with time. A behavior function of an information system appears when a problem situation arises in the material system, without any experience of solving such a problem. When designing systems with behavior, a system should be endowed with new functions without changing its architecture. We have given a set-theoretic description of company activity using a system of indicators and a metamodel of the problem situation. We have developed an algorithm of search for the data which are necessary for information support of a problem situation. A possible architecture is proposed for an integrated information system based on a multi-layered data bus.

Keywords — Information System Behavior, Integration of Information Systems, Company Management Systems, Metamodel.

References

1. Zhizhimov O. L., Fedotov A. M., Shokin Iu. I. Technology Platform Mass Integration of Heterogeneous Data. *Vestnik NGU.* Ser. *Informatsionnye Tekhnologii*, 2013, vol. 11, no. 11. pp. 24–41 (In Russian).
2. Volkov A. A., Shvedenko V. N. The Model of Formation of Parallel Structures in the Object-Oriented Database. *Programmnye Produkty i Sistemy*, 2011 no. 3, pp. 14–17 (In Russian).
3. Veselova N. S., Shvedenko V. N. Modeling of Information Resources of the Enterprise with the Organization of Process Control System. *Programmnye Produkty i Sistemy*, 2014, no. 4(108), pp. 260–264 (In Russian).
4. Kuz'kin A. A., Smirnov S. V., Basov O. O. Model Provision Strategy for the Development of Information Technologies in Organizations. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2015, vol. 15, no. 2, pp. 305–312 (In Russian).
5. Oleynik P. P. Using Metamodel of Object System for Domain-Driven Design the Database Structure. *Proc. 12th IEEE East-West Design and Test Symposium (EWDTS'2014)*, Kiev, Ukraine, 2014. Art. 7027052. doi:10.1109/EWDTS.2014.7027052
6. Jaeger P. T., Lin J., Grimes J. M., Simmons S. N. Where is the Cloud? Geography, Economics, Environment, and Jurisdiction in Cloud Computing. *First Monday*, 2009, vol. 14, no. 5. Available at: http://firstmonday.org/ojs/index.php/fm/article/view/2456/2171 (accessed 3 August 2014).
7. Sadiku M. N. O., Musa S. M., Momoh O. D. Cloud Computing: Opportunities and Challenges. *IEEE Potentials*, 2014, vol. 33, no. 1, pp. 34–36.
8. Gagnon S., Nabelsi V., Passerini K., Cakici K. The Next Web Apps Architecture: Challenges for SaaS Vendors. *IT Professional*, 2011, vol. 13, no. 5, pp. 44–50.
9. Vladimirov A. V. Agent Based Interaction in the Enterprise Information System Adaptation Mechanisms of Work and the User Interface. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2013, vol. 6(88), pp. 105–111 (In Russian).
10. Sysoletin E. G., Aksenov K. A., Kruglov A. V. Integration of Heterogeneous Information Systems of Modern Industrial Enterprise. *Sovremennye problemy nauki i obrazovaniia*, 2015, no. 1 (In Russian). Available at: www.scienceeducation.ru/121-19030 (accessed 25 May 2016).
11. Shvedenko V. N., Shchekochikhin O. V., Shvedenko P. V. Evaluation Criteria and Models of Information Systems, with the Property of Behavior. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2016, vol. 16, no. 4, pp. 649–654 (In Russian). doi: 10.17586/2226-1494-2016-16-4-649-654

УДК 519.2
doi:10.15217/issn1684-8853.2016.5.91

ИССЛЕДОВАНИЕ ПОТОКОВЫХ МОДЕЛЕЙ УПРАВЛЕНИЯ ЗАПАСАМИ МЕТОДОМ *R*-АППРОКСИМАЦИИ

А. А. Назаров[a], *доктор техн. наук, профессор*
В. И. Бронер[a], *аспирант*
[a]*Национальный исследовательский Томский государственный университет, Томск, РФ*

Постановка проблемы: *при рассмотрении математических моделей систем управления запасами с релейным управлением с произвольной функцией распределения объемов потребления возникает сложность при исследовании интегро-дифференциального уравнения, решением которого является плотность распределения вероятностей значений количества запасов в системе.* ***Цель:*** *развитие методов исследования математических моделей систем управления запасами с аппроксимацией функции распределения объемов потребления.* ***Методы:*** *исследование моделей управления запасами с построением R-аппроксимации функции распределения объемов потребления, аналогичной гиперэкспоненциальной аппроксимации.* ***Результаты:*** *построена математическая модель управления запасами с релейным управлением при непрерывном поступлении ресурса в систему и произвольной функцией распределения объемов потребления. Получена функция, аппроксимирующая распределение объемов потребления, причем в некоторых случаях она является гиперэкспоненциальным распределением; может являться распределением, но не гиперэкспоненциальным; и третий случай, когда аппроксимирующая функция не является распределением, но ее применение допустимо. Найдена плотность распределения вероятностей значений объема ресурса в произвольный момент времени на основе R-аппроксимации. Результаты имитационного моделирования показали достаточно широкую область применения метода при гамма- и логнормальном распределениях объемов потребления запасов.* ***Практическая значимость:*** *результаты исследований могут быть использованы при моделировании реальных систем управления запасами, таких как страховые компании, водохранилища, склады и другие, в случае, когда по реальным данным о потреблении можно оценить первые три момента распределения объемов потребления товара или ресурса.*

Ключевые слова *— математическое моделирование, управление запасами, релейное управление, R-аппроксимация.*

Введение

Теория управления запасами активно развивается в последние десятилетия. В рамках данной теории, как правило, рассматриваются различные одноперiодные математические модели, например, в работе Маутаза Куджа (Moutaz Khouja) [1] описывается одноперiодная модель, которая заключается в том, чтобы найти такой объем запасов, который максимизирует ожидаемую прибыль по возможному спросу. Такая модель предполагает, что если в конце заданного периода остаются запасы, то продавец вынужден отпускать товар со скидкой или утилизировать его [2]. Если количество запасов меньше, чем спрос на товар, то имеет место упущенная прибыль. Данная классическая задача является отражением многих реальных жизненных ситуаций, связанных со скоропортящейся или сезонной продукцией, и часто используется для принятия решений, например, в модной и спортивной отраслях, в производстве и розничной торговле [3]. Стоит отметить, что аналогичная модель также может быть применена в сфере услуг [4].

Исследователями рассматриваются два подхода к решению класса задач, описанного выше. В рамках первого подхода ожидаемые затраты, связанные недооцененным/переоцененным спросом, сведены к минимуму. Во втором подходе ожидаемая прибыль максимизируется. Оба подхода дают схожие результаты. Е. А. Сильвер (E. A. Silver), Д. Ф. Пайк (D. F. Pyke), Р. П. Петерсон (R. P. Peterson) отметили [5], что задача максимизации средней ожидаемой прибыли не всегда соответствует действиям управляющего звена компании, в отличие от задачи максимизации вероятности достижения целевой прибыли. Впоследствии исследователи предложили задачи, обобщающие данную задачу, в которых цель состоит в максимизации вероятности достижения целевой прибыли [6–11].

В работах отечественных авторов в большинстве своем рассматриваются потоковые модели страховых компаний различного вида с некоторым потоком (как правило, простейшим) поступления ресурса в качестве страховых премий и потоком потребления — денежными выплатами. Так как любая компания заинтересована оптимизировать уровень запасов, в данном случае — капитала компании, то в подобных работах управление заключается в изменении «скорости» денежных притоков и оттоков в зависимости от некоторого порогового значения денежных ресурсов, определяемого самой компанией.

Например, в работах [12–18] рассматриваются потоковые математические модели деятельности фонда социального страхования с релейным управлением капиталом фонда. Исследуются [12] основные характеристики деятельности фонда социального страхования в случае, когда на вход системы управления запасами с непрерывной

скоростью поступают денежные средства, моменты страховых выплат образуют пуассоновский поток, а величины выплат подчиняются экспоненциальному закону распределения. Рассматривается некоторое пороговое значение денежных средств фонда, сверх которого производятся выплаты по социальным программам с непрерывной скоростью. В случае, когда у фонда нет достаточно средств, т. е. денежный уровень ниже порогового значения, система функционирует в режиме без выплат по социальным программам.

В работах [13, 14] рассматриваются и исследуются модели фонда социального страхования при релейном управлении (также рассмотрено [13] релейно-гистерезисное управление) капиталом такого фонда. В отличие от предыдущих моделей [12], в данных моделях рассматривается вариант, когда выплаты по страховым случаям и выплаты на финансирование социальных программ образуют пуассоновские потоки событий с постоянной и переменной интенсивностями соответственно, а величины выплат являются одинаково распределенными независимыми случайными величинами с экспоненциальной функцией распределения.

Построена и исследована [15] математическая модель деятельности некоммерческого фонда в случае, когда на вход системы поступает пуассоновский поток платежей постоянной интенсивности с экспоненциально распределенными величинами платежей, при этом управление заключается в том, что до достижения порогового значения ресурс расходуется с постоянной скоростью, а при превышении этого значения скорость потребления увеличивается. А в работе [17] на основе диффузионного приближения исследуется модель, аналогичная приведенной в работе [15].

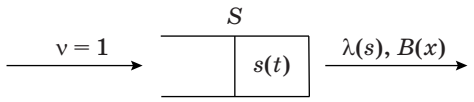
Найдено [18] выражение для функции скорости выделения средств на социальные программы в диффузионном приближении для процесса изменения капитала фонда в условиях математической модели [12].

В перечисленных работах, как правило, рассматриваются выплаты с экспоненциальным распределением их значений.

В данной работе рассматривается аналогичная указанным [13, 14] модель с произвольным распределением объемов потребления, исследование которой предлагается провести с помощью метода R-аппроксимации функции распределения объемов потребления.

Математическая модель

Рассмотрим систему управления запасами (рисунок), на вход которой с постоянной скоростью $\nu = 1$ непрерывно поступают некоторые ресурсы.



■ Система управления запасами

Обозначим объем накопленных ресурсов в системе к моменту времени t через $s(t)$. Будем полагать, что запросы на потребление ресурса будут поступать в случайные моменты времени, а величины запросов — партии случайного объема.

Пусть моменты потребления образуют пуассоновский поток с кусочно-постоянной интенсивностью $\lambda(s)$, зависящей от значений $s(t) = s$ величин накопленных запасов к моменту времени t поступления заявки на расходование ресурса:

$$\lambda(s) = \begin{cases} \lambda_1, s < S; \\ \lambda_2, s \geq S, \end{cases} \quad (1)$$

где S — некоторое пороговое значение уровня запасов $s(t)$.

Будем считать, что объемы потребления, т. е. величины запроса на потребление ресурсов, имеют произвольную функцию распределения $B(x)$.

Стоит отметить, что возможна ситуация, когда процесс $s(t)$ принимает отрицательные значения, т. е. $s(t) < 0$, и система продолжает функционировать, откладывая исполнение заявки на потребление ресурсов до момента накопления необходимого количества.

Для данной системы условие существования стационарного режима имеет вид

$$\lambda_1 b < 1 < \lambda_2 b, \quad (2)$$

где b — среднее значение объема одной партии на потребление ресурсов.

Таким образом, при $\lambda_1 < 1/b < \lambda_2$ в случае, когда $s(t) < S$, объем ресурса в системе будет увеличиваться в среднем, а в противном случае при достижении уровня S и его превышении, т. е. $s(t) \geq S$, в связи с возрастанием интенсивности потребления объем ресурса будет уменьшаться.

Из описания математической модели следует, что случайный процесс $s(t)$ является марковским с непрерывным временем t и непрерывным множеством значений $-\infty < s < \infty$.

Обозначим его стационарную плотность распределения

$$P(s) = \frac{\partial P\{s(t) < s\}}{\partial s}$$

и запишем следующее равенство:

$$P(s + \Delta t) = P(s)(1 - \lambda(s)\Delta t) + \\ + \Delta t \int_0^\infty \lambda(s + x) P(s + x) \mathrm{d}B(x) + o(\Delta t),$$

из которого получим уравнение

$$P'(s)+\lambda(s)P(s)=\int_0^\infty \lambda(s+x)P(s+x)\mathrm{d}B(x). \qquad (3)$$

Решение этого уравнения при произвольной функции распределения $B(x)$ вызывает определенные затруднения, поэтому рассмотрим решение уравнения (3) методом R-аппроксимации, аналогичной гиперэкспоненциальной аппроксимации, предложенной в работе Ю. И. Рыжикова [19], которая реализуется следующим образом.

Вначале уравнение (3) решается в частном случае, когда функция $B(x)$ является гиперэкспоненциальной, т. е. имеет вид

$$B(x)=q(1-\mathrm{e}^{-\mu_1 x})+(1-q)(1-\mathrm{e}^{-\mu_2 x}), \qquad (4)$$

где $\mu_k > 0$ и $0 < q < 1$, и решение $P_R(s)$ интегродифференциального уравнения (3) записывается в явном виде функции, зависящей от параметров q, μ_1 и μ_2 гиперэкспоненциального распределения $R(x)$.

Далее, реализуя явную аппроксимацию, методом моментов определяются значения параметров q, μ_1 и μ_2 функции $R(x)$, аппроксимирующей функцию распределения $B(x)$. Здесь можно оценить точность такой аппроксимации, хотя это не будет иметь принципиального значения.

Затем, подставляя полученные значения параметров q, μ_1 и μ_2 в решение $P_R(s)$, найденные при гиперэкспоненциальной функции распределения $R(x)$, реализуем этап неявной аппроксимации функцией $P_R(s)$ решения $P(s)$ уравнения (3) с произвольной функцией распределения $B(x)$.

Естественным завершением метода R-аппроксимации является исследование свойств аппроксимирующей функции $P_R(s)$, определение области ее применимости и точности предлагаемой аппроксимации, что имеет принципиальное значение, так как аппроксимация допустима лишь тогда, когда она удовлетворяет заданной точности.

На первом этапе метода R-аппроксимации найдем решение уравнения (3) при гиперэкспоненциальном распределении объемов потребления (4).

Нетрудно показать, что решение уравнения (3) в этом случае имеет вид

$$P(s)=\begin{cases} C_1\mathrm{e}^{z_1(s-S)}+C_2\mathrm{e}^{z_2(s-S)}, & s\le S; \\ C\mathrm{e}^{\gamma(s-S)}, & s\ge S, \end{cases} \qquad (5)$$

где

$$z_{1,2}=\frac{1}{2}\left\{\kappa-\lambda_1\pm\sqrt{(\kappa-\lambda_1)^2-4\mu_1\mu_2(1-\lambda_1 b)}\right\};$$

$$\gamma=\frac{1}{2}\left\{\kappa-\lambda_2-\sqrt{(\kappa-\lambda_2)^2+4\mu_1\mu_2(\lambda_2 b-1)}\right\},$$

$$\kappa=\mu_1+\mu_2;$$

причем $z_1 > 0$, $z_2 > 0$, $\gamma < 0$.

Константы C_1, C_2, C определяются равенствами

$$C_1=\frac{\lambda_2}{\lambda_1}\frac{a_{12}a_{23}-a_{13}a_{22}}{a_{12}a_{21}-a_{11}a_{22}}\frac{1}{X};$$

$$C_2=\frac{\lambda_2}{\lambda_1}\frac{a_{13}a_{21}-a_{11}a_{23}}{a_{12}a_{21}-a_{11}a_{22}}\frac{1}{X};\quad C=\frac{1}{X},$$

где $X=a_{3,1}\dfrac{\lambda_2}{\lambda_1}\dfrac{a_{1,2}a_{2,3}-a_{1,3}a_{2,2}}{a_{1,2}a_{2,1}-a_{1,1}a_{2,2}}+$

$+a_{3,2}\dfrac{\lambda_2}{\lambda_1}\dfrac{a_{1,3}a_{2,1}-a_{1,1}a_{2,3}}{a_{1,2}a_{2,1}-a_{1,1}a_{2,2}}-a_{3,3}$, a_{kv} — элементы матрицы $\mathbf{A}=\begin{pmatrix} 1/(z_1-\mu_1) & 1/(z_2-\mu_1) & 1/(\gamma-\mu_1) \\ 1/(z_1-\mu_2) & 1/(z_2-\mu_2) & 1/(\gamma-\mu_2) \\ 1/z_1 & 1/z_2 & 1/\gamma \end{pmatrix}$.

На втором этапе метода R-аппроксимации выполним аппроксимацию функции распределения $B(x)$ функцией

$$R(x)=q(1-\mathrm{e}^{-\mu_1 x})+(1-q)(1-\mathrm{e}^{-\mu_2 x}), \qquad (6)$$

формально совпадающей с гиперэкспоненциальным распределением (4), но параметры q, μ_1 и μ_2 функции $R(x)$ могут принимать достаточно произвольные значения. В частности, параметр q может принимать значения, большие единицы, и, более того, параметры q, μ_1 и μ_2 могут быть комплексными, как это будет показано в табл. 1 для системы с гамма-распределением объемов потребления.

Будем полагать значения параметров μ_1 и μ_2 с отрицательными действительными частями недопустимыми, т. е. в этом случае метод R-аппроксимации неприемлем, как это будет показано в табл. 2 для системы при некоторых значениях параметров с логарифмически нормальным распределением объемов потребления.

Вообще говоря, функция $R(x)$ может и не являться функцией распределения.

Значения параметров q, μ_1 и μ_2 функции $R(x)$ найдем методом моментов, приравнивая первые три начальных момента a_1, a_2, a_3 функции распределения $B(x)$ к соответствующим интегральным характеристикам функции $R(x)$.

Получим систему, состоящую из трех нелинейных уравнений относительно неизвестных q, μ_1 и μ_2:

$$\begin{cases} \dfrac{q}{\mu_1}+\dfrac{1-q}{\mu_2}=a_1; \\ \dfrac{q}{\mu_1^2}+\dfrac{1-q}{\mu_2^2}=\dfrac{a_2}{2}; \\ \dfrac{q}{\mu_1^3}+\dfrac{1-q}{\mu_2^3}=\dfrac{a_3}{6}. \end{cases} \qquad (7)$$

Для решения системы введем следующие обозначения:

$$\mu_1=1/x;\quad \mu_2=1/y. \qquad (8)$$

Тогда систему можно представить следующим образом:

$$\begin{cases} qx+(1-q)y=a_1; \\ qx^2+(1-q)y^2=\dfrac{a_2}{2}; \\ qx^3+(1-q)y^3=\dfrac{a_3}{6}. \end{cases} \quad (9)$$

Из первого уравнения системы получим выражения

$$q=\frac{a_1-y}{x-y};\ 1-q=\frac{x-a_1}{x-y}, \quad (10)$$

последовательно подставляя которые во второе и третье уравнения системы (9) получим систему уравнений

$$\begin{cases} a_1(x+y)-xy=\dfrac{a_2}{2}; \\ a_1(x^2+xy+y^2)-xy(x+y)=\dfrac{a_3}{6}. \end{cases} \quad (11)$$

Обозначив $u = x + y$, $v = xy$, получим систему

$$\begin{cases} a_1u-v=\dfrac{a_2}{2}; \\ a_1(u^2-v)-uv=\dfrac{a_3}{6}, \end{cases}$$

решение u и v которой имеет вид

$$u=\frac{3a_1a_2-a_3}{3(2a_1{}^2-a_2)};\ v=\frac{3a_2{}^2-2a_1a_3}{6(2a_1{}^2-a_2)}. \quad (12)$$

Решая систему (11) для неизвестных x и y, получим

$$x=\frac{1}{2}\left\{u+\sqrt{u^2-4v}\right\};\ y=\frac{1}{2}\left\{u-\sqrt{u^2-4v}\right\}, \quad (13)$$

а значения параметра q определяются из (10).

В зависимости от полученных значений параметров q, μ_1 и μ_2 возможны три приемлемых варианта функции $R(x)$:

1) гиперэкспоненциальная функция распределения;

2) функция распределения, не являющаяся гиперэкспоненциальной;

3) не является функцией распределения, но ее применение допустимо, так как позволяет найти аппроксимацию распределения $P(s)$, обладающую допустимой погрешностью, которая устанавливается имитационным моделированием, и один неприемлемый, когда функция $R(x)$ неограниченна.

Имитационное моделирование

Рассмотрим в качестве распределения объемов потребления $B(x)$ гамма-распределения и проведем R-аппроксимацию по первым трем моментам функции распределения $B(x)$.

Пусть гамма-распределение $B(x)$ имеет параметры формы α и масштаба β, тогда первые три начальных момента будут иметь вид

$$a_1=\frac{\alpha}{\beta};\ a_2=\frac{\alpha(\alpha+1)}{\beta^2};\ a_3=\frac{\alpha(\alpha+1)(\alpha+2)}{\beta^3}. \quad (14)$$

Пусть $\alpha = \beta$, тогда среднее значение будет равно единице, а параметры аппроксимирующей функции $R(x)$ будут иметь вид

$$q=\frac{1}{2}+\frac{2\alpha-1}{D};\ \mu_1=\frac{6\alpha}{2(\alpha+1)+D};$$

$$\mu_2=\frac{6\alpha}{2(\alpha+1)-D}, \quad (15)$$

где $D=\sqrt{2(\alpha+1)(2-\alpha)}$.

Нетрудно показать, что при $\alpha < 1$ параметры q, μ_1 и μ_2 функции $R(x)$ удовлетворяют всем требованиям на параметры гиперэкспоненциального распределения, т. е. они принимают действительные положительные значения и $0 < q < 1$.

При $1 < \alpha < 2$ параметры q, μ_1 и μ_2 действительные и положительные, но q принимает значения, большие единицы, и тем не менее $R(x)$ остается функцией распределения, естественно, не гиперэкспоненциальной.

При $\alpha > 2$ параметры μ_1 и μ_2, а также q и $1 - q$ являются комплексно сопряженными, поэтому функция $R(x)$ принимает действительные значения, хотя и не является функцией распределения, так как ее производная в окрестности точки $x = 0$ принимает отрицательные значения, но, тем не менее, как будет показано ниже в численных примерах в табл. 1, ее применение вполне приемлемо для исследования рассматриваемой модели управления запасами.

Построим R-аппроксимацию $B(x)$ при различных значениях параметра формы α, а также воспользуемся расстоянием Колмогорова для оценки качества Δ_R явной аппроксимации функции распределения $B(x)$ и Δ неявной аппроксимации распределения $F_R(x)$ стационарной функции распределения значений объема в системе управления запасами, полученной на основе R-аппроксимации:

$$\Delta_R=\sup_{-\infty<x<\infty}|B(x)-R(x)|;$$

$$\Delta=\sup_{-\infty<x<\infty}|F(x)-F_R(x)|,$$

где $F(x)$ — эмпирическая функция распределения того же объема, полученная на основе имитационного моделирования при следующих значениях параметров: $S = 10$, $\nu = 1$, $\lambda_1 = 0{,}8$ и $\lambda_2 = 1{,}2$.

Результаты исследования представлены в табл. 1.

■ ***Таблица 1.*** *R*-аппроксимация гамма-распределения объемов потребления

α	$R(x)$				$P_R(s)$			
	q	μ_1	μ_2	Δ_R	z_1	z_2	γ	Δ
0,2	0,220	0,268	3,732	0,245	3,136	0,064	−0,070	0,014
0,6	0,594	0,677	3,323	0,049	3,053	0,147	−0,152	0,005
1,2	1,246	1,147	2,853	0,007	2,980	0,220	−0,217	0,006
1,6	2,025	1,445	2,555	0,008	2,950	0,250	−0,243	0,005
2	∞	2,000	2,000	0	2,927	0,273	−0,261	0,004
3	0,5−1,768i	2−0,707i	2+0,707i	0,025	2,888	0,312	−0,291	0,009
10	0,5−1,432i	2−1,206i	2+1,206i	0,139	2,812	0,388	−0,347	0,001

Исходя из представленных результатов, можно сделать вывод о том, что применение метода *R*-аппроксимации для исследования рассматриваемой модели системы управления запасами целесообразно не только тогда, когда $R(x)$ достаточно точно аппроксимирует функцию распределения $B(x)$ (в частности, при $0{,}6 < \alpha < 5$), но и в случаях $\alpha < 0{,}6$ и $\alpha > 5$, когда аппроксимация $R(x)$ функции $B(x)$ имеет погрешность $\Delta_R > 0{,}1$, а точность аппроксимации $F_R(x)$ окончательного распределения достаточно высокая, так как $\Delta < 0{,}01$.

При $\alpha > 2$ функция $R(x)$, аппроксимирующая $B(x)$, распределением не является, но ввиду того, что точность аппроксимации высокая, применение *R*-аппроксимации допустимо.

Отметим также, что функция $P(x)$, определяемая равенством (5), является плотностью распределения при $\alpha < 2$, что вполне естественно, так как $R(x)$ в этом случае является функцией распределения. Но также и при $\alpha > 2$, когда *R*-аппроксимация определяет функцию $R(x)$, которая не является функцией распределения, тем не менее $P(x)$ остается плотностью распределения, что еще раз убеждает в целесообразности применения метода *R*-аппроксимации для исследования рассматриваемой модели системы управления запасами.

Аналогичное исследование было проведено для случая, когда $B(x)$ является наиболее неудобным для аппроксимации логнормальным распределением. Для того чтобы среднее значение было равно единице, необходимо выполнение следующего условия: $\mu = -\sigma^2/2$, где μ и σ^2 — параметры логнормального распределения (логарифмические среднее и дисперсия).

Результаты исследования представлены в табл. 2, откуда можно сделать вывод о том, что при $1{,}5 \le \exp(\sigma^2) < 2$ применение *R*-аппроксимации является недопустимым, так как параметр μ_2 в этом случае принимает отрицательные значения. В остальных случаях аппроксимация функции распределения $B(x)$ объемов потребления является допустимой несмотря на то, что погрешность аппроксимации достаточна велика (при $\exp(\sigma^2) = 1{,}1$ или $\exp(\sigma^2) > 2$). Однако имитационное моделирование показало, что стационарная функция распределения значений объема запасов, полученная на основе *R*-аппроксимации, достаточно точно ($\Delta < 0{,}01$) описывает реальный процесс.

■ ***Таблица 2.*** *R*-аппроксимация логнормального распределения объемов потребления

$\exp(\sigma^2)$	$R(x)$				$P_R(s)$			
	q	μ_1	μ_2	Δ_R	z_1	z_2	γ	Δ
1,1	0,5 − 1,476i	2 − 1,2i	2 + 1,2i	2,881	0,387	−0,347	0,151	0,003
1,3	5,555	2,154	2,885	3,922	0,317	−0,300	0,065	0,002
1,49	1,361	1,352	50,991	51,273	0,269	−0,268	0,187	0,003
1,51	1,308	1,316	−48,991	0,265	−48,74	−48,61	∞	–
1,7	1,054	1,097	−1,420	0,230	−1,354	−1,280	$1{,}7\cdot10^{17}$	–
1,98	1	1	−0,032	0,200	−0,032	−0,2	0,119	–
2,2	0,004	0,173	1,021	0,257	0,138	−0,191	0,010	0,006
2,4	0,015	0,219	1,059	0,343	0,135	−0,180	0,083	0,005
2,6	0,024	0,221	1,093	0,391	0,124	−0,17	0,071	0,006
3,0	0,029	0,195	1,138	0,430	0,103	−0,154	0,058	0,005

Заключение

В данной работе построена математическая модель системы управления запасами с релейным управлением при произвольной функции распределения $B(x)$ объемов потребления ресурса. Построена функция $R(x)$, аппроксимирующая функцию $B(x)$, на основе которой найдено аналитическое выражение для стационарной плотности $P(x)$ распределения вероятностей значений объема запасов. Путем имитационного моделирования установлена область применимости R-аппроксимации для гамма- и логнормального распределений объемов потребления ресурсов. Предложенный подход может быть применен к аналогичным задачам при других функциях распределения объемов расходования ресурсов.

Литература

1. **Khouja M.** The Single-period (News-vendor) Problem: Literature Review and Suggestions for Future Research // Omega. 1999. Vol. 27. Iss. 5. P. 537–553. doi:10.1016/S0305-0483(99)00017-1
2. **Nahmias S.** Production and Operations Management. 3rd ed. — Boston, MA: Irwin, 1996. — 858 p.
3. **Gallego G., Moon I.** The Distribution Free Newsboy Problem: Review and Extensions the Distribution Free Newsboy Problem: Review and Extensions // The Journal of the Operational Research Society. 1993. Vol. 44. N 8. P. 825–834. doi:10.1057/jors.1993.141
4. **Weatherford L. R., Pfeifer P. E.** The Economic Value of Using Advance Booking of Orders // Omega. 1994. Vol. 22. Iss. 1. P. 105–111. doi:10.1016/0305-0483(94)90011-6
5. **Silver E. A., Pyke D. F., Peterson R. P.** Inventory Management and Production Planning and Scheduling. 3rd ed. — N. Y.: John Wiley, 1998. — 784 p.
6. **Ismail B., Louderback J.** Optimizing and Satisficing in Stochastic Cost-Volume-Profit Analysis // Decision Sciences. 1979. Vol. 10. P. 205–217. doi:10.1111/j.1540-5915.1979.tb00019
7. **Kabak I., Schiff A.** Inventory Models and Management Objectives // Sloan Management Review. 1978. N 10. P. 53–59.
8. **Lau H.** The Newsboy Problem under Alternative Optimization Objectives // Journal of Operational Research Society. 1980. N 31. P. 525–535. doi:10.1057/jors.1980.96
9. **Lau A., Lau H.** Maximizing the Probability of Achieving a Target Profit Level in a Two-product Newsboy Problem // Decision Sciences. 1988. N 19. P. 392–408. doi:10.1111/j.1540-5915.1988.tb00275
10. **Li J., Lau H., Lau A. H.** Two-product Newsboy Problem with Satisfying Objective and Independent Exponential Demands // IIE Trans. 1991. N 23. P. 29–39. doi:10.1080/07408179108963839
11. **Sankarasubramanian E., Kumaraswamy S.** Note—Note on «Optimal Order Quantity for Pre-determined Level of Profit» // Management Science. 1983. N 29. P. 512–514. doi:org/10.1287/mnsc.29.4.512
12. **Змеев О. А.** Математическая модель деятельности фонда социального страхования при экспоненциальных страховых выплатах // Вестник Томского государственного университета. 2003. № 280. С. 130–135.
13. **Вальц О. В., Змеев О. А.** Математическая модель деятельности фонда социального страхования при экспоненциальных страховых выплатах и со случайными расходами на социальные программы // Вестник Томского государственного университета. 2004. № 284. С. 37–41.
14. **Китаева А. В., Терпугов А. Ф.** Модель фонда социального страхования при релейном управлении капиталом и экспоненциально распределенных страховых выплатах и выплатах по социальным программам // Вестник Томского государственного университета. 2006. № 293. С. 35–37.
15. **Лившиц К. И., Шифердекер И. Ю.** Математическая модель деятельности некоммерческого фонда при релейном управлении капиталом // Вестник Томского государственного университета. Приложение. 2006. № 18. С. 302–308.
16. **Лившиц К. И., Сухотина Л. Ю., Шифердекер И. Ю.** Пуассоновская модель деятельности некоммерческого фонда при релейном управлении капиталом // Вестник Томского государственного университета. Приложение. 2006. № 19. С. 302–312.
17. **Лившиц К. И., Шифердекер И. Ю.** Диффузионная аппроксимация математической модели деятельности некоммерческого фонда при релейном управлении капиталом // Вестник Томского государственного университета. 2006. № 293. С. 38–44.
18. **Китаева А. В., Терпугов А. Ф.** Управление капиталом фонда социального страхования // Вестник Томского государственного университета. 2006. № 290. С. 167–168.
19. **Рыжиков Ю. И.** Теория очередей и управление запасами. — СПб.: Питер, 2001. — 384 с.

UDC 519.2
doi:10.15217/issn1684-8853.2016.5.91

_R_-approximation Method for Stochastic Inventory Control Models

Nazarov A. A.[a], Dr. Sc., Tech., Professor, nazarov.tsu@gmail.com
Broner V. I.[a], Post-Graduate Student, valsubbotina@mail.ru
[a]National Research Tomsk State University, 36, Lenin Ave., 634050, Tomsk, Russian Federation

Purpose: It is difficult to study mathematical models of inventory management systems with on/off control when the demand has an arbitrary distribution function. The difficulty is the integral-differential equation whose solution is the probability density function of the inventory levels. **Purpose:** The idea is to develop methods for studying mathematical models of inventory management with an approximation of the demand distribution function. **Methods:** For the research of inventory control models, we build an *R*-approximation of the demand distribution function, similar to the hyper-exponential approximation. **Results:** We have built a mathematical model for the inventory management with on/off control when the rate of the product flow is continuous and the demand has an arbitrary distribution function. We have obtained a function which approximates the demand distribution. This function can be a hyper-exponential distribution, otherwise it can be a distribution but not hyper-exponential; in the third case, this function is not a distribution but still can be used. Using *R*-approximation, we have also obtained the probability density of the inventory levels. The simulation results showed that this method can be applied in a fairly wide area for gamma- and lognormal distribution of the demand. **Practical relevance:** The results can be used for modeling real inventory management systems, such as insurance companies, reservoirs, warehouses, etc. when we can estimate the three moments of the demands distribution using real data about the demand.

Keywords — Mathematical Modeling, Inventory Management, On/Off Control, R-Approximation.

References

1. Khouja M. The Single-period (News-vendor) Problem: Literature Review and Suggestions for Future Research. *Omega*, 1999, vol. 27, iss. 5, pp. 537–553. doi:10.1016/S0305-0483(99)00017-1
2. Nahmias S. *Production and Operations Management*. 3rd ed. Boston, MA, Irwin, 1996. 858 p.
3. Gallego G., Moon I. The Distribution Free Newsboy Problem: Review and Extensions. *The Journal of the Operational Research Society*, 1993, vol. 44, no. 8, pp. 825–834. doi:10.1057/jors.1993.141
4. Weatherford L. R., Pfeifer P. E. The Economic Value of Using Advance Booking of Orders. *Omega,* 1994, vol. 22, iss. 1, pp. 105–111. doi:10.1016/0305-0483(94)90011-6
5. Silver E. A., Pyke D. F., Peterson R. P. *Inventory Management and Production Planning and Scheduling*. 3rd ed. New York, John Wiley, 1998. 784 p.
6. Ismail B., Louderback J. Optimizing and Satisficing in Stochastic Cost-Volume-Profit Analysis. *Decision Sciences*, 1979, vol. 10, pp. 205–217. doi:10.1111/j.1540-5915.1979.tb00019.x
7. Kabak I., Schiff A. Inventory Models and Management Objectives. *Sloan Management Review*, 1978, no. 10, pp. 53–59.
8. Lau H. The Newsboy Problem under Alternative Optimization Objectives. *Journal of Operational Research Society*, 1980, no. 31, pp. 525–535. doi:10.1057/jors.1980.96
9. Lau A., Lau H. Maximizing the Probability of Achieving a Target Profit Level in a Two-product Newsboy Problem. *Decision Sciences*, 1988, no. 19, pp. 392–408. doi:10.1111/j.1540-5915.1988.tb00275
10. Li J., Lau H., Lau A. H. A Two-product Newsboy Problem with Satisfying Objective and Independent Exponential Demands. *IIE Trans.*, 1991, no. 23, pp. 29–39. doi:10.1080/07408179108963839
11. Sankarasubramanian E., Kumaraswamy S. Note—Note on «Optimal Order Quantity for Pre-determined Level of Profit». *Management Science*, 1983, no. 29, pp. 512–514. doi:org/10.1287/mnsc.29.4.512
12. Zmeyev O. A. The Model of the Social Insurance Fund with Exponential Distributed Insurance Payments. *Vestnik Tomskogo gosudarstvennogo universiteta*, 2003, no. 280, pp. 130–135 (In Russian).
13. Valts O. V., Zmeyev O. A. Mathematical Model of Advertising Campaign Taking into Account the Effect of "Boring" of Advertisement. *Vestnik Tomskogo gosudarstvennogo universiteta*, 2004, no. 284, pp. 37–41 (In Russian).
14. Kitaeva A. V., Terpugov A. F. The Model of the Social Insurance Fund on the Relay Management of Capital and Exponential Distributed Insurance Payments and Payments on Social Programs. *Vestnik Tomskogo gosudarstvennogo universiteta*, 2006, no. 293, pp. 35–37 (In Russian).
15. Livshits K. I., Shiferdeker I. Yu. Mathematical Model of Uncomercial fund Functioning under the Relay Control of its Capital. *Vestnik Tomskogo gosudarstvennogo universiteta. Prilozhenie*, 2006, no. 18, pp. 302–308 (In Russian).
16. Livshits K. I., Suhotina L. Yu., Shiferdeker I. Yu. Puasson Model of Uncomercial Fund Functioning under the Relay Control of its Capital. *Vestnik Tomskogo gosudarstvennogo universiteta. Prilozhenie*, 2006, no. 19, pp. 302–312 (In Russian).
17. Livshits K. I., Shiferdeker I. Yu. Diffusion Approximation of the Mathematical Model of the Non-profit Foundation with the Relay Money Management. *Vestnik Tomskogo gosudarstvennogo universiteta*, 2006, no. 293, pp. 38–44 (In Russian).
18. Kitaeva A. V., Terpugov A. F. Control of the Social Insurance Fund's Surplus. *Vestnik Tomskogo gosudarstvennogo universiteta*, 2006, no. 290, pp. 167–168 (In Russian).
19. Ryizhikov Yu. I. *Teoriya ocheredey i upravlenie zapasami* [The Teory of Queues and Inventory Managament]. Saint-Petersburg, Piter Publ., 2001. 384 p. (In Russian).

УДК 621.396:681.323
doi:10.15217/issn1684-8853.2016.5.98

СИНТЕЗ НЕРЕКУРСИВНЫХ ДИСКРЕТНЫХ ФИЛЬТРОВ ВО ВРЕМЕННОЙ ОБЛАСТИ

С. И. Зиатдинов[a], *доктор техн. наук, профессор*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Введение: *переход от непрерывных фильтров к нерекурсивным дискретным фильтрам с использованием отсчетов импульсных характеристик непрерывных фильтров-аналогов приводит к ошибкам в формировании переходных процессов. Вместе с тем динамические свойства фильтров в полном объеме определяются их переходными характеристиками. Синтез нерекурсивных дискретных фильтров на базе переходных характеристик позволяет обеспечить их динамические свойства, совпадающие с динамическими свойствами непрерывных фильтров.* ***Цель:*** *разработка методики синтеза нерекурсивных дискретных фильтров с использованием переходных характеристик.* ***Методы:*** *представление импульсной характеристики дискретного фильтра в виде первой конечной разности его переходной характеристики и нахождение с использованием интеграла наложения выходного сигнала.* ***Результаты:*** *получена новая методика синтеза нерекурсивного дискретного фильтра, позволяющая при заданном входном сигнале и известной переходной характеристике фильтра найти его выходной сигнал. Выдвинутые теоретические положения подтверждены конкретным примером.* ***Практическая значимость:*** *полученная методика позволяет при решении задач фильтрации сигналов в помехах и шумах использовать нерекурсивные дискретные фильтры, динамические свойства которых совпадают с динамическими свойствами непрерывных фильтров-аналогов.*

Ключевые слова *— частотная передаточная функция, импульсная и переходная характеристики, нерекурсивные дискретные фильтры, разностные уравнения, коэффициенты.*

Введение

При обработке сигналов самое широкое распространение получили разнообразные фильтры, с помощью которых решаются задачи фильтрации, дифференцирования, интегрирования, экстраполяции и т. д. В каждом конкретном случае фильтр должен обладать определенными частотными свойствами.

В современных условиях все чаще приходится сталкиваться с цифровыми методами обработки на базе персональных компьютеров или специализированных вычислителей. При этом стоит задача преобразования непрерывных фильтров в дискретные. В настоящее время достаточно хорошо отработана методика синтеза дискретных фильтров по их непрерывным аналогам.

Можно выделить два основных метода синтеза: синтез дискретных фильтров в частотной области и синтез дискретных фильтров во временной области. При синтезе дискретных фильтров в частотной области [1] должны воспроизводиться амплитудно-частотные и фазо-частотные характеристики непрерывных фильтров с минимальными погрешностями. Преобразование частотной передаточной функции непрерывного фильтра в частотную передаточную функцию дискретного фильтра осуществляется на базе билинейного преобразования, которое используется для создания в основном фильтров верхних частот и режекторных фильтров.

В случае синтеза дискретных фильтров во временной области применяется метод инвариантной импульсной характеристики, при котором отсчеты импульсной характеристики непрерывного фильтра используются для вычисления коэффициентов линейного разностного уравнения дискретного фильтра.

Для дискретных фильтров импульсная характеристика представляется последовательностью масштабированных отсчетов непрерывной импульсной характеристики $h(t)$ [2]:

$$h[i] = Th(t_i),$$

где $i = 0, 1, 2, \ldots$ — номер отсчета импульсной характеристики; T — период следования отсчетов входного и выходного сигналов дискретного фильтра; $t_i = iT$ — текущее дискретное время.

В результате алгоритм работы дискретного фильтра определяется дискретной сверткой отсчетов обрабатываемого сигнала $x(t)$ и импульсной характеристики $h(t)$ фильтра [2, 3]

$$y[k] = \sum_{i=0}^{k} x[i]h[k-i], \; k = 0, 1, 2, \ldots .$$

Выходной сигнал дискретного фильтра в общем виде можно описать линейным разностным уравнением с постоянными коэффициентами:

$$\begin{aligned} y[k] &= a_0 x[k] + a_1 x[k-1] + \ldots + a_n x[k-n] - \\ &- b_1 y[k-1] - b_2 y[k-2] - \ldots - b_n y[k-n] = \\ &= \sum_{i=0}^{n} a_i x[k-i] - \sum_{i=1}^{n} b_i y[k-i], \end{aligned} \quad (1)$$

где n — порядок разностного уравнения; a_i, b_i — постоянные коэффициенты.

При этом синтез дискретного фильтра для заданного порядка n заключается в выборе постоянных коэффициентов a_i, b_i, которые определяют вид частотной характеристики фильтра.

На практике широко используются как нерекурсивные, так и рекурсивные дискретные фильтры.

Нерекурсивные дискретные фильтры

Для нерекурсивных дискретных фильтров разностное уравнение (1) записывается следующим образом:

$$y[k] = a_0 x[k] + a_1 x[k-1] + \ldots + a_n x[k-n] = \sum_{i=0}^{n} a_i x[k-i]. \quad (2)$$

При этом порядок уравнения n рассчитывается так, чтобы произведение nT было больше длительности переходного процесса в фильтре $nT > t_{\text{п}}$, а коэффициенты a_i принимаются равными отсчетам импульсной характеристики $h[i]$:

$$a_0 = h[0],\ a_1 = h[1],\ \ldots,\ a_n = h[n].$$

Тогда выражение (2) для выходного сигнала нерекурсивного дискретного фильтра принимает хорошо известный вид

$$y[k] = h[0]x[k] + h[1]x[k-1] + \ldots + h[n]x[k-n] = \sum_{i=0}^{n} h[i]x[k-i]. \quad (3)$$

Покажем, что в общем случае данное соотношение является неверным, т. е. не отражает точно истинные физические процессы, протекающие в дискретном фильтре.

В качестве примера рассмотрим фильтр нижних частот (ФНЧ) первого порядка с частотной передаточной функцией в непрерывном варианте

$$W(j\omega) = \frac{1}{1 + j\omega\tau},$$

где τ — постоянная времени фильтра.

Данной частотной передаточной функции соответствуют импульсная и переходная характеристики вида [1]

$$h(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \frac{1}{1 + j\omega\tau} e^{j\omega t}\,\mathrm{d}\omega = \omega_{\text{ср}} e^{-\omega_{\text{ср}} t};$$

$$g_{\text{н}}(t) = 1 - e^{-\omega_{\text{ср}} t}, \quad (4)$$

где $\omega_{\text{ср}} = \dfrac{1}{\tau}$ — частота среза фильтра.

В соответствии с (3) переходная характеристика рассматриваемого нерекурсивного дискретного фильтра, как его реакция на единичное входное воздействие, записывается следующим образом:

$$g[k] = h[0]1[k] + h[1]1[k-1] + \ldots + h[n]1x[k-n] = \sum_{i=0}^{n} h[i]1[k-i], \quad (5)$$

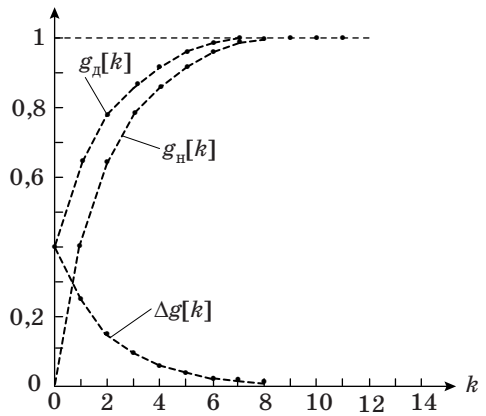
где $1[k]$ — единичный решетчатый входной сигнал.

Синтезированный нерекурсивный дискретный фильтр должен по своим параметрам соответствовать непрерывному фильтру, т. е. переходная характеристика дискретного фильтра (5) должна с точностью до постоянного множителя равняться переходной характеристике непрерывного фильтра (4) в дискретные моменты времени $t_i = iT$.

На рисунке показаны переходные характеристики рассматриваемого непрерывного ФНЧ $g_{\text{н}}[k]$ и нерекурсивного дискретного ФНЧ $g_{\text{д}}[k]$ для случая $T\omega_{\text{ср}} = 0{,}4$. Здесь же представлено отклонение переходных характеристик непрерывного и дискретного фильтров $\Delta g[k] = g_{\text{д}}[k] - g_{\text{н}}[k]$.

Анализируя представленные результаты расчетов, можно отметить, что для ФНЧ первого порядка на протяжении длительности переходного процесса $t_{\text{п}} \approx 8T$ отклонение переходной характеристики дискретного фильтра от переходной характеристики непрерывного фильтра изменяется от 40 % практически до нуля относительно установившегося значения $g_{\text{н}}[\infty] = 1$. Расчеты, проведенные для ФНЧ второго порядка, показывают, что указанное отклонение переходных характеристик составляет 10 %.

Таким образом, существующая методика определения коэффициентов разностного уравнения нерекурсивных дискретных фильтров на базе импульсной характеристики является неточной и в результате не обеспечивает требуемого качества работы дискретных фильтров в пределах переходного процесса.



■ Переходные характеристики ФНЧ и отклонение переходных характеристик

В полном объеме физические процессы, протекающие в фильтрах, описываются их переходными характеристиками. В связи с этим рассмотрим синтез нерекурсивных дискретных фильтров на базе их переходных характеристик.

В общем виде выходной сигнал нерекурсивного фильтра определяется интегралом наложения

$$y(t) = \int_0^t x(t-\tau)h(\tau)\mathrm{d}\tau. \qquad (6)$$

При этом импульсная характеристика фильтра $h(t)$ связана с его переходной характеристикой $g(t)$ соотношением

$$h(t) = \frac{\mathrm{d}g(t)}{\mathrm{d}t} = \lim_{\Delta t \to 0} \frac{g(t) - g(t-\Delta t)}{\Delta t}. \qquad (7)$$

После подстановки (7) в (6) получим

$$y(t) = \lim_{\Delta t \to 0_0} \int_0^t x(t-\tau)\frac{g(\tau) - g(\tau-\Delta t)}{\Delta t}\mathrm{d}\tau. \qquad (8)$$

Будем считать, что за время Δt не происходит заметных изменений переходной характеристики. Тогда, положив $\Delta t = T$ и заменяя интеграл в (8) суммой, получим

$$y(k) = \sum_{i=0}^{n} x[k-i]\{g[i] - g[i-1]\} = \sum_{i=0}^{n} x[k-i]\Delta g[i], \qquad (9)$$

где $\Delta g[i] = g[i] - g[i-1]$; $g[i]$ — отсчеты переходной характеристики фильтра.

Для $k = 0, 1, 2, \ldots$ на основании (9) можно записать следующую систему уравнений:

$$y[0] = x[0]\Delta g[0];$$
$$y[1] = x[1]\Delta g[0] + x[0]\Delta g[1];$$
$$y[2] = x[2]\Delta g[0] + x[1]\Delta g[1] + x[0]\Delta g[2];$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$y[k] = x[k]\Delta g[0] + x[k-1]\Delta g[1] + \ldots + x[0]\Delta g[k].$$

Представим данную систему в виде

$$y[0] = a_0 x[0];$$
$$y[1] = a_0 x[1] + a_1 x[0];$$
$$y[2] = a_0 x[2] + a_1 x[1] + a_2 x[0];$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \qquad (10)$$
$$y[k] = a_0 x[k] + a_1 x[k-1] + \ldots + a_k x[0],$$

где коэффициенты $a_0 = \Delta g[0]$, $a_1 = \Delta g[1]$, ..., $a_k = \Delta g[k]$.

Расчет переходных характеристик нерекурсивных дискретных фильтров как нижних, так и верхних частот первого порядка с коэффициентами, вычисленными с использованием соотношений (10), показал совпадение с переходными характеристиками соответствующих непрерывных фильтров на всем протяжении переходных характеристик. Для фильтров более высоких порядков при $T\omega_{ср} = 0{,}4$ отклонение переходных характеристик непрерывных и дискретных фильтров не превышает десятых долей процентов и резко уменьшается с уменьшением произведения $T\omega_{ср}$.

Заключение

Известная методика расчетов коэффициентов разностного уравнения нерекурсивных дискретных фильтров на базе отсчетов импульсной характеристики не обеспечивает правильной реализации переходных процессов.

Методика расчетов коэффициентов с использованием отсчетов переходной характеристики позволяет получить динамические свойства нерекурсивных дискретных фильтров, совпадающие с динамическими свойствами непрерывных фильтров-аналогов как в переходном, так и в установившемся режимах.

Предложенная методика является общей и может быть распространена на нерекурсивные и рекурсивные дискретные фильтры как нижних, так и верхних частот практически любых порядков.

Литература

1. **Воробьев С. Н.** Цифровая обработка сигналов. — М.: Академия, 2013. — 318 с.
2. **Гоноровский И. С.** Радиотехнические цепи и сигналы. — М.: Радио и связь, 1986. — 512 с.
3. **Alan V. Oppenheim, Ronald W. Schafer.** Discrete-Time Signal Processnig. — Prentice Hall, 1989. — 1120 p.

UDC 621.396:681.323
doi:10.15217/issn1684-8853.2016.5.98

Synthesis of Non-Recursive Discrete Filters in Temporal Range

Ziatdinov S. I.[a], Dr. Sc., Tech., Professor, kaf53@guap.ru
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St.,
Saint-Petersburg, Russian Federation

Introduction: The transition from continuous filters to non-recursive discrete filters using the readings of impulsive characteristics of continuous filters-analogs leads to mistakes in forming transient processes. At the same time, the dynamic properties of the filters are fully determined by their transient characteristics. Synthesis of non-recursive discrete filters based on transient characteristics provides that their dynamic properties coincide with the dynamic properties of continuous filters. **Purpose:** The goal is to create a method for the synthesis of non-recursive discrete filters using transient characteristics. **Method:** We represent the impulsive characteristic of a discrete filter as the first final difference of its transient characteristic, and find the output signal using an imposition integral. **Results:** A new technique has been obtained for the synthesis of non-recursive discrete filter, which allows you to calculate the output signal of a filter when its input signal is given and the transient characteristic known. The theoretical results are substantiated by an example. **Practical relevance:** The obtained technique allows you to solve the problems of filtering signals in noises by using non-recursive discrete filters whose dynamic properties coincide with the dynamic properties of continuous filters-analogs.

Keywords — Frequency Transmission Function, Impulse and Transient Characteristic, Non-Recursive Discrete Filters, Difference Equation, Coefficients.

References

1. Vorobiev C. N. *Tsifrovaia obrabotka signalov* [Digital Signal Processing]. Moscow, Akademiia Publ., 2013. 318 p. (In Russian).
2. Gonorovskii I. S. *Radiotekhnicheskie tsepi i signaly* [Radio Circuits and Signals]. Moscow, Radio i sviaz' Publ., 1986. 512 p. (In Russian).
3. Alan V. Oppenheim, Ronald W. Schafer. *Discrete-Time Signal Processnig*. Prentice Hall, 1989. 1120 p.

СВЕДЕНИЯ ОБ АВТОРАХ

БАЛОНИН Николай Алексеевич

Профессор кафедры вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1982 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина) по специальности «Автоматика и телемеханика».
В 2008 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 90 научных публикаций, в том числе трех монографий.
Область научных интересов — теория динамических систем, теория идентификации, теория операторов, теория матриц, вычислительные методы, интернет-робототехника, интернет-книги с исполняемыми алгоритмами, научные социальные сети.
Эл. адрес: korbendfs@mail.ru

БОГАЧЕНКО Надежда Федоровна

Доцент кафедры информационной безопасности Омского государственного университета им. Ф. М. Достоевского.
В 1997 году окончила Омский государственный университет по специальности «Прикладная математика».
В 2000 году защитила диссертацию на соискание ученой степени кандидата физико-математических наук.
Является автором 65 научных публикаций.
Область научных интересов — модели безопасности компьютерных систем, прикладное программирование.
Эл. адрес: nfbogachenko@mail.ru

БУРЯЧЕНКО Владимир Викторович

Старший преподаватель кафедры информатики и вычислительной техники Сибирского государственного аэрокосмического университета им. академика М. Ф. Решетнёва, Красноярск.
В 2011 году окончил магистратуру Сибирского государственного аэрокосмического университета им. академика М. Ф. Решетнёва по специальности «Интеллектуальные системы».
В 2014 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 23 научных публикаций и двух свидетельств на регистрацию программных продуктов.
Область научных интересов — цифровая обработка изображений и видеопоследовательностей, стабилизация видео.
Эл. адрес:
buryachenko@sibsau.ru

БЕЛИМ Сергей Викторович

Профессор, заведующий кафедрой информационной безопасности Омского государственного университета им. Ф. М. Достоевского.
В 1996 году окончил Омский государственный университет по специальности «Физика».
В 2009 году защитил диссертацию на соискание ученой степени доктора физико-математических наук.
Является автором 118 научных публикаций.
Область научных интересов — модели безопасности компьютерных систем, интеллектуальные системы защиты информации.
Эл. адрес: sbelim@mail.ru

БРОНЕР Валентина Игоревна

Аспирант кафедры теории вероятностей и математической статистики факультета прикладной математики и кибернетики Национального исследовательского Томского государственного университета.
В 2015 году окончила Томский государственный университет по специальности «Прикладная математика и информатика».
Является автором 17 научных публикаций.
Область научных интересов — теория управления запасами, математическое моделирование.
Эл. адрес: valsubbotina@mail.ru

ВОЛКОВ Данил Андреевич

Аспирант кафедры комплексной защиты информации Омского государственного технического университета.
В 2014 году окончил Омский государственный университет им. Ф. М. Достоевского по специальности «Компьютерная безопасность».
Является автором десяти научных публикаций.
Область научных интересов — искусственный интеллект, информационные технологии, информационная безопасность, распознавание образов.
Эл. адрес: vlkv.d.a@gmail.com

ДОЙНИКОВА Елена Владимировна

Младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН.
В 2009 году окончила с отличием Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина) по специальности «Компьютерная безопасность».
Является автором более 50 научных публикаций.
Область научных интересов — безопасность компьютерных сетей, методы анализа рисков компьютерных сетей, управление информационными рисками.
Эл. адрес:
doynikova@comsec.spb.ru

ЕРЕМЕНКО Александр Валериевич

Доцент кафедры инфокоммуникационных систем и информационной безопасности Омского государственного университета путей сообщения.
В 2006 году окончил Сибирскую государственную автомобильно-дорожную академию по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем».
В 2012 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 30 научных публикаций.
Область научных интересов — искусственный интеллект, информационные технологии, информационная безопасность, распознавание образов.
Эл. адрес: nexus-@mail.ru

КОТЕНКО Игорь Витальевич

Профессор, заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН.
В 1983 году окончил Военно-космическую академию им. А. Ф. Можайского по специальности «Математическое обеспечение автоматизированных систем управления», в 1987 году — Военную академию связи по специальности «Инженерная автоматизированных систем управления».
В 1999 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 450 научных публикаций.
Область научных интересов — безопасность компьютерных сетей, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей и др.
Эл. адрес: ivkote@comsec.spb.ru

ЕЛТЫШЕВ Денис Константинович

Доцент кафедры микропроцессорных средств автоматизации Пермского национального исследовательского политехнического университета.
В 2008 году окончил магистратуру Пермского государственного технического университета по специальности «Автоматизация и управление».
В 2013 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 40 научных публикаций и одного свидетельства на регистрацию программ для ЭВМ.
Область научных интересов — теория принятия решений, методы мягких вычислений и их использование в прикладных задачах проектирования экспертных систем и т. д.
Эл. адрес: eltyshev@msa.pstu.ru

ЗИАТДИНОВ Сергей Ильич

Профессор кафедры информационно-сетевых технологий Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1970 году окончил Ленинградский институт авиационного приборостроения по специальности «Электронные устройства».
В 2001 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором 140 научных публикаций и 16 патентов на изобретения.
Область научных интересов — аналоговая и цифровая обработка сигналов, автоматические системы управления.
Эл. адрес: kaf53@guap.ru

ЛОЖНИКОВ Павел Сергеевич

Заведующий кафедрой комплексной защиты информации Омского государственного технического университета.
В 2000 году окончил Омский государственный технический университет по специальности «Автоматизированные системы обработки информации и управление».
В 2005 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 100 научных публикаций и четырех патентов на изобретения.
Область научных интересов — искусственный интеллект, информационные технологии, информационная безопасность, распознавание образов.
Эл. адрес: lozhnikov@gmail.com

МАРТЫНОВА Любовь Александровна

Ведущий научный сотрудник научно-исследовательского центра «Системы освещения обстановки» АО «Концерн «ЦНИИ «Электроприбор», Санкт-Петербург.
В 1985 году окончила Ленинградский кораблестроительный институт по специальности «Прикладная математика».
В 2013 году защитила диссертацию на соискание ученой степени доктора технических наук.
Является автором 80 научных публикаций.
Область научных интересов — системный анализ, математическое моделирование, оценка эффективности, обработка разнородной информации.
Эл. адрес:
martynowa999l@bk.ru

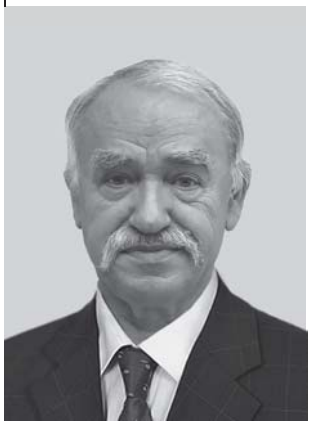
ОХТИЛЕВ Михаил Юрьевич

Профессор, заведующий кафедрой компьютерных технологий и программной инженерии Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1982 году окончил Военный инженерный Краснознаменный институт им. А. Ф. Можайского по специальности «Автоматизированная обработка и анализ информации».
В 2000 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 190 научных публикаций, в том числе трех монографий.
Область научных интересов — теория программирования, теория алгоритмов, системы реального времени, математическая логика и др.
Эл. адрес: oxt@mail.ru

РОЗЕНГАУЗ Михаил Борисович

Старший научный сотрудник АО «Концерн «ЦНИИ «Электроприбор», Санкт-Петербург.
В 1972 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина) по специальности «Системы автоматического управления».
В 1991 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 37 научных публикаций.
Область научных интересов — теория надежности, техническая диагностика.
Эл. адрес:
rozengauz@hotmail.com

НАЗАРОВ Анатолий Андреевич



Профессор, заведующий кафедрой теории вероятностей и математической статистики Национального исследовательского Томского государственного университета. Почетный работник высшего профессионального образования РФ.
В 1970 году окончил Томский государственный университет по специальности «Математика».
В 1985 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 150 научных публикаций, включая шесть монографий.
Область научных интересов — теория телетрафика массового обслуживания, теория управления запасами, методы асимптотического анализа, математическое моделирование.
Эл. адрес:
nazarov.tsu@gmail.com

РАКИЦКИЙ Юрий Сергеевич

Доцент кафедры информационной безопасности Омского государственного университета им. Ф. М. Достоевского.
В 2008 году окончил Омский государственный университет по специальности «Компьютерная безопасность».
В 2011 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 16 научных публикаций.
Область научных интересов — модели безопасности компьютерных систем, защита программ и данных.
Эл. адрес:
yrakitsky@gmail.com

СЕРГЕЕВ Михаил Борисович

Профессор, заведующий кафедрой вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения, директор НИИ информационно-управляющих систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики.
В 1980 году окончил ЛЭТИ.
В 2001 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 100 научных публикаций и 14 патентов на изобретения.
Область научных интересов — теория разрядных вычислений, методы проектирования спецпроцессоров для систем контроля и управления и др.
Эл. адрес: mbse@mail.ru

СУЛАВКО
Алексей
Евгеньевич

Старший преподаватель кафедры комплексной защиты информации Омского государственного технического университета.
В 2009 году окончил Сибирскую государственную автомобильно-дорожную академию по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем».
В 2014 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 35 научных публикаций и одного патента на изобретение.
Область научных интересов — искусственный интеллект, информационные технологии, информационная безопасность, распознавание образов.
Эл. адрес: sulavich@mail.ru

ФАВОРСКАЯ
Маргарита
Николаевна

Профессор, заведующая кафедрой информатики и вычислительной техники Сибирского государственного аэрокосмического университета им. академика М. Ф. Решетнёва, Красноярск.
В 1980 году окончила Рыбинский авиационный технологический институт по специальности «Конструирование и производство электронно-вычислительной аппаратуры».
В 2011 году защитила диссертацию на соискание ученой степени доктора технических наук.
Является автором около 160 научных публикаций.
Область научных интересов — распознавание образов, цифровая обработка изображений, кластерный анализ, интеллектуальные технологии обработки данных и др.
Эл. адрес: favorskaya@sibsau.ru

ШВЕДЕНКО
Петр
Владимирович

Аспирант кафедры автоматики и микропроцессорной техники Костромского государственного университета, лауреат стипендии Правительства Российской Федерации.
В 2016 году с отличием окончил магистратуру Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики по специальности «Информационная безопасность».
Является автором 33 научных публикаций.
Область научных интересов — информационные системы и процессы, системный анализ, управление и обработка информации.
Эл. адрес: pitk1@mail.ru

ТОМИЛИНА
Анастасия
Игоревна

Магистрант Сибирского государственного аэрокосмического университета им. академика М. Ф. Решетнёва, Красноярск.
В 2014 году окончила бакалавриат Сибирского государственного аэрокосмического университета им. академика М. Ф. Решетнёва по специальности «Информационные системы».
Область научных интересов — цифровая обработка изображений и видеопоследовательностей, стабилизация видео.
Эл. адрес:
nastomila@gmail.com

ШВЕДЕНКО
Владимир
Николаевич

Профессор кафедры защиты информации Костромского государственного университета, научный руководитель проекта ООО «РЕГУЛ+», Санкт-Петербург. Почетный работник высшего профессионального образования РФ.
В 1977 году окончил Костромской технологический институт по специальности «Технология машиностроения, металлорежущие станки и инструменты».
В 2006 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором 150 научных публикаций и трех патентов на изобретения.
Область научных интересов — информационные системы и процессы, системный анализ, управление и обработка информации.
Эл. адрес: shvn.d3@mail.ru

ШМЕЛЕВ
Валентин
Валерьевич

Докторант кафедры технологий и средств комплексной обработки и передачи информации в АСУ Военно-космической академии им. А. Ф. Можайского, Санкт-Петербург.
В 2000 году окончил Военно-космическую академию им. А. Ф. Можайского по специальности «Бортовые радиоэлектронные системы космических аппаратов».
В 2006 г. защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 50 научных публикаций.
Область научных интересов — автоматизированная обработка измерительной информации космических средств, контроль и диагностирование технического состояния, экспертные системы.
Эл. адрес:
valja1978@yandex.ru

ЩЕКОЧИХИН Олег Владимирович

Доцент, заведующий кафедрой защиты информации Костромского государственного университета.
В 2003 году окончил Костромской государственный университет по специальности «Информатика».
В 2009 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 40 научных публикаций.
Область научных интересов — информационные системы управления предприятиями, проектирование интегрированных информационных систем, информационная безопасность гетерогенных информационных систем.
Эл. адрес: slim700@yandex.ru

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

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

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (ius.spb@gmail.com).

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

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

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ