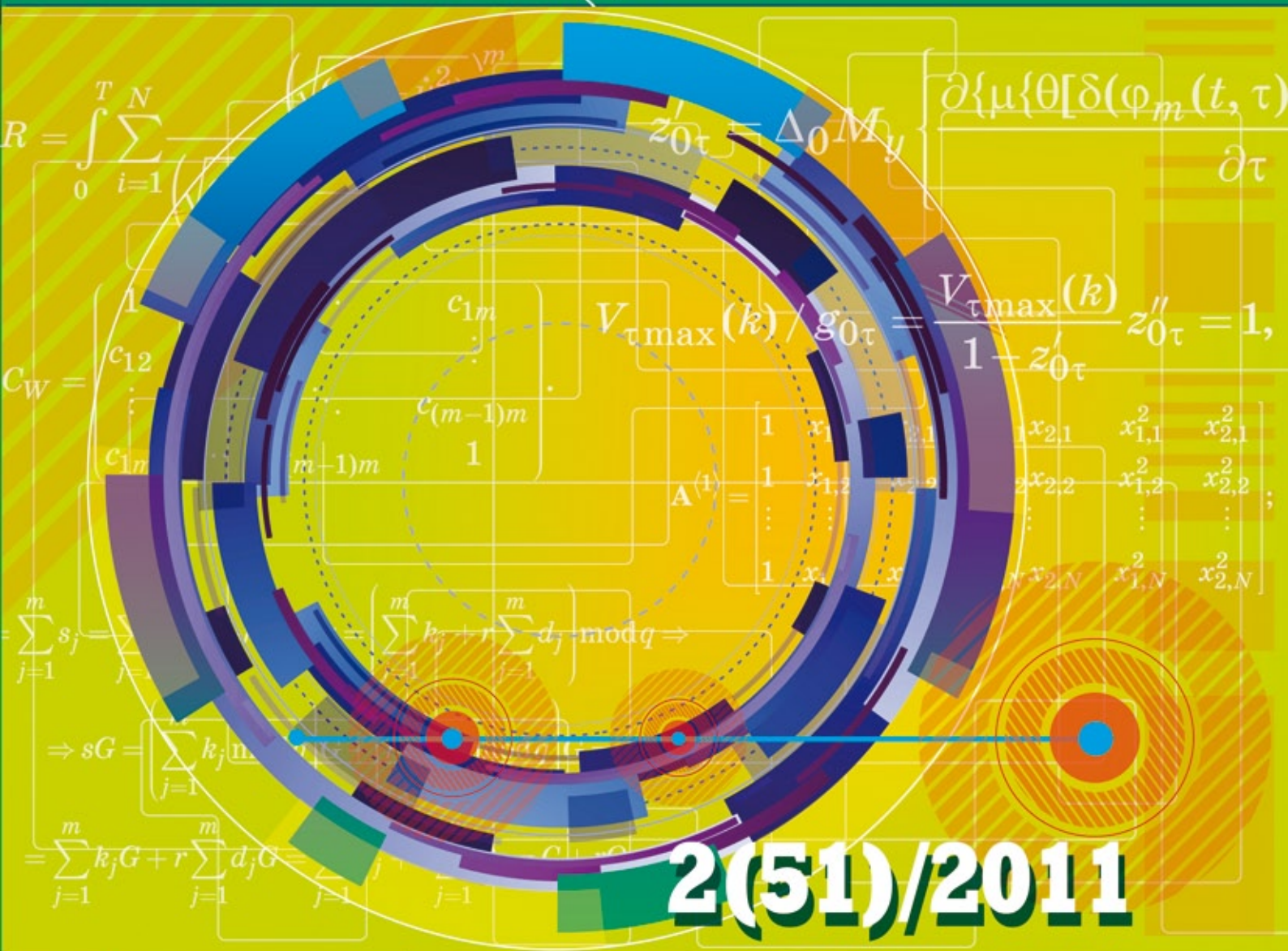
ISSN 1684–8853

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

НАУЧНЫЙ ЖУРНАЛ



2(51)/2011

НАУЧНЫЙ ЖУРНАЛ

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

2(51)/2011

РЕЦЕНЗИРУЕМОЕ ИЗДАНИЕ

Учредитель
ОАО «Издательство “Политехника”»

Адрес редакции: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Тел.: (812) 494-70-02
Факс: (812) 494-70-18
E-mail: 80x@mail.ru
Сайт: www.i-us.ru

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

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

Журнал распространяется по подписке. Подписку можно оформить через редакцию, а также в любом отделении связи по каталогам: «Роспечать»: № 48060, № 15385; «Пресса России»: № 42476.

ЛР № 010292 от 18.08.98.
Сдано в набор 04.03.11. Подписано в печать 20.04.11. Формат 60×84 1/8.
Бумага офсетная. Гарнитура SchoolBookC. Печать офсетная.
Усл. печ. л. 11,4. Уч.-изд. л. 14,6. Тираж 1000 экз. Заказ 123.
Оригинал-макет изготовлен в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.
Отпечатано с готовых диапозитивов в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.

УДК 531.3:681.5.01

УКЛОНЕНИЕ ПОДВИЖНОГО ОБЪЕКТА ОТ ОБНАРУЖЕНИЯ ГРУППОЙ НАБЛЮДАТЕЛЕЙ ПРИ МАЛЫХ ОТНОШЕНИЯХ СИГНАЛ/ПОМЕХА

Т. Г. Абрамянц,
канд. техн. наук, старший научный сотрудник
Е. П. Маслов,
доктор техн. наук, старший научный сотрудник
И. М. Рудько,
канд. техн. наук, старший научный сотрудник
В. П. Яхно,
канд. техн. наук, старший научный сотрудник
Институт проблем управления им. В. А. Трапезникова РАН

Приводится решение задачи об оптимизации закона уклонения подвижного объекта от обнаружения группой наблюдателей при малых отношениях сигнал/помеха. Вектор программного управления включает траекторию уклонения и закон изменения скорости на траектории.

Ключевые слова *— уклонение от обнаружения, вероятность обнаружения, группа наблюдателей, отношение сигнал/помеха, первый интеграл, алгоритм Дейкстры.*

Введение

Рассматриваемая в статье задача относится к классу задач об управлении, получивших в англоязычной литературе название *Optimal Transit Path Planning in Threat Environment*. Интерес к ним возрос в последнее время в связи с широким использованием беспилотных аппаратов различного назначения [1–3]. В русскоязычной литературе они получили название «задачи управления подвижными объектами в конфликтной среде» [4, 5]. Под конфликтной средой понимается совокупность объектов (они называются конфликтующими), сближение с которыми для управляемого объекта нежелательно в ходе выполнения им основной задачи. Целью управления объектом при движении его в конфликтной среде является минимизация негативного воздействия конфликтующих объектов на управляемый объект путем выбора маршрута его движения, параметров движения и/или режимов работы технических средств. К числу негативных воздействий принято относить обнаружение объекта. Задачи об оптимизации закона уклонения подвижного объекта от обнаружения рассматривались в ряде работ. Постановки задач отличаются предположениями о характеристиках информационных полей, в которых происходит обнаружение, классами допустимых законов управления, видом критериев качества, количеством обнаружителей, объемом и характером информации, доступной конфликтующим сторонам (см. статьи [1–5] и библиографию к ним).

Особенность задач уклонения от обнаружения состоит в том, что во всех случаях текущий уровень сигнала I на входе наблюдателя (сенсора) зависит от текущей дистанции D до уклоняющегося объекта, а для некоторых полей — и от величины текущей скорости v объекта. Для описания зависимостей широко используется степенная модель

$$I \sim \frac{v^m}{D^k}. \qquad (1)$$

Величина показателя степени k является характеристикой физического поля, в котором осуществляется обнаружение [2]. Содержательный смысл имеют значения $k = 1, 2, 3, 4$. Значение $k = 1$ соответствует процессу затухания волн на поверхности жидкости и убыванию уровня интенсивности первичного гидроакустического поля в мелком море. Значение $k = 2$ соответствует убыванию уровней интенсивностей теплового поля, первичного электромагнитного поля и первичного гидро-

акустического поля в глубоком море при их распространении в пространстве (пассивный режим обнаружения). Значение $k = 3$ соответствует убыванию уровня напряженности магнитного поля. Значение $k = 4$ соответствует убыванию уровней интенсивностей вторичного электромагнитного и гидроакустического полей (активный режим обнаружения). Величина показателя степени m характеризует зависимость уровня интенсивности излучаемого сигнала от скорости движения объекта. Такая зависимость имеет место для сигналов первичного гидроакустического поля [6, 7].

Постановка задачи

В настоящей статье решается задача об оптимизации закона уклонения подвижного объекта, перемещающегося на плоскости в течение заданного времени T из фиксированной начальной точки $A(x_A, y_A)$ в фиксированную конечную точку $B(x_B, y_B)$ маршрута, от обнаружения в пассивном режиме группой наблюдателей (сенсоров), расположенных в районе. Критерием является вероятность обнаружения объекта, т. е. вероятность обнаружения хотя бы один раз хотя бы одним сенсором за время движения объекта по маршруту. Оптимизация сводится к нахождению траектории и закона изменения скорости объекта, доставляющих минимум указанному критерию.

Критерий образуется следующим образом.

Обнаружение осуществляется по результатам обработки излученного объектом сигнала и принятого системой сенсоров при наличии случайных помех. Для практически важных случаев гауссовых сигналов и помех решение о наличии или отсутствии сигнала от объекта принимается отдельным сенсором периодически [6], после предварительной обработки поступившей на интервале наблюдения (усреднения) реализации гауссовых случайных величин $X_1, X_2, ..., X_n$ с нулевым математическим ожиданием. Обозначим символом $\sigma^2_{ш}$ дисперсию помех на входе сенсора, символом $\sigma^2_c = \sigma^2_c(v, D)$ — дисперсию сигнала, излученного объектом и поступившего на вход сенсора, зависящую от текущей скорости движения объекта v и текущего расстояния D между ним и сенсором. В отсутствие сигнала от объекта случайные величины X_i имеют дисперсию $\sigma^2_{ш}$, при наличии сигнала от объекта — дисперсию $\sigma^2_c + \sigma^2_{ш}$. Оптимальное правило принятия решения наблюдателем состоит в сравнении статистики $S(x) = \sum x_i^2$ с порогом h. Если $S(x) \le h$, то принимается решение, что сигнал от объекта отсутствует, а если $S(x) > h$, то принимается решение, что сигнал от объекта есть. Функция распределения вероятностей статистики $S(x)$ описывается функцией χ^2-распределения с n степенями свободы и имеет вид

$$F_n(x) = \frac{1}{2^{\frac{n}{2}}\Gamma\left(\frac{n}{2}\right)} \int_0^x u^{\frac{n}{2}-1} e^{-\frac{u}{2}} du,$$

где $\Gamma(\cdot)$ — гамма-функция; n — число степеней свободы (количество наблюдений в реализации), которое при аналоговых алгоритмах обработки определяется по формуле $n = 2T_0\Delta F$, где T_0 — длительность интервала усреднения; ΔF — ширина полосы пропускания приемной системы средства обнаружения. Вероятность обнаружения объекта отдельным сенсором по результатам обработки информации на одном интервале усреднения вычисляется по формуле

$$P_{обн}(v, D) = 1 - F_n\left(\frac{h_F}{\frac{\sigma^2_c(v, D)}{\sigma^2_{ш}} + 1}\right), \qquad (2)$$

где h_F — квантиль уровня $(1 - \alpha)$ для χ^2-распределения с n степенями свободы; $\alpha = P_{л.т}$ — вероятность ложной тревоги; $\sigma^2_c(v, D)/\sigma^2_{ш}$ — отношение сигнал/помеха (ОСП) на входе сенсора.

В гидроакустике [6] ОСП принято выражать в терминах отношения интенсивностей сигналов. В том случае, когда спектральные плотности мощности сигнала и помехи можно считать постоянными в пределах анализируемого частотного диапазона, формула (2) переписывается следующим образом:

$$P_{обн}(v, D) = 1 - F_n\left(\frac{h_F}{\frac{I_c(v, D)}{I_{ш}} + 1}\right). \qquad (3)$$

Полагая, что зависимость уровня интенсивности излученного объектом сигнала от его скорости и закон распространения гидроакустического сигнала в среде носят степенной характер, имеем для интенсивности сигнала на входе сенсора [6]

$$I_c(v, D) = I_c(v_0)\left(\frac{v}{v_0}\right)^m \left(\frac{D_0}{D}\right)^k, \qquad (4)$$

где $I_c(v_0)$ — интенсивность излучения объекта на некоторой эталонной скорости v_0, измеренная в стандартных условиях [6] на расстоянии $D_0 = 1$ м от объекта; v — текущая скорость движения объекта; D — текущее расстояние между ним и средством обнаружения.

Интенсивность помехи на входе приемной системы сенсора рассчитывается по формуле [6]

$$I_{ш} = \frac{I_n(f)}{A(f)}, \qquad (5)$$

где $I_n(f)$ — интенсивность помех в районе расположения сенсора; $A(f)$ — коэффициент концентрации антенной системы сенсора в полосе приема.

С учетом формул (4), (5) выражение для текущего ОСП на входе сенсора может быть записано в следующем виде:

$$\frac{I_{\text{с}}(v,D)}{I_{\text{ш}}} = I_{\text{с}}(v_0)\left(\frac{v}{v_0}\right)^m \frac{D_0^k}{D^k} / \frac{I_n(f)}{A(f)}. \tag{6}$$

В том случае, когда длительность интервала усреднения T_0 намного меньше времени движения T объекта по маршруту и в течение одного интервала усреднения скорость объекта и расстояние его до наблюдателя можно считать постоянными, вероятность обнаружения объекта хотя бы один раз за время движения по маршруту находится по формуле

$$P_{\text{обн}} = 1 - \prod_{j=1}^{J} (1 - P_{\text{обн}}(v_j, D_j)), \tag{7}$$

где $J = T/T_0$; v_j — скорость объекта; D_j — расстояние между объектом и наблюдателем на j-м интервале усреднения.

В случае, когда имеется N наблюдателей, принимающих решения об обнаружении независимо, вероятность обнаружения объекта хотя бы один раз хотя бы одним наблюдателем за время движения объекта по маршруту определяется по формуле

$$P_{\text{обн}}^{T} = 1 - \prod_{j=1}^{J} \prod_{i=1}^{N} (1 - P_{\text{обн}}(v_j, D_{ji})), \tag{8}$$

где D_{ji} — расстояние между объектом и i-м наблюдателем на j-м интервале усреднения.

В работе [8] показано, что в случае, когда ОСП на входе наблюдателя, описываемое формулой (6), мало в течение всего времени движения объекта по маршруту, при построении математической модели могут быть использованы следующие приближенные формулы.

Вероятность обнаружения объекта отдельным сенсором по результатам обработки информации на одном интервале усреднения

$$P_{\text{обн}}(v, D) = \alpha + q\frac{I_{\text{с}}(v, D)}{I_{\text{ш}}}, \tag{9}$$

где $q = \dfrac{h_F^{\frac{n}{2}}}{2^{n/2}\Gamma\left(\frac{n}{2}\right)} e^{-\frac{h_F}{2}}$.

Вероятность необнаружения объекта отдельным сенсором по результатам обработки последовательности наблюдений за все время движения его по маршруту

$$P_{\text{необн}} = \exp\left\{-\frac{1}{T_0}\int_0^T \left[\alpha + \frac{qI_{\text{с}}(v_0)}{I_{\text{ш}} v_0^m} \frac{\left(\sqrt{(\dot{x}^2 + \dot{y}^2)}\right)^m}{\left[\sqrt{(x-a)^2 + (y-b)^2}\right]^k}\right] \mathrm{d}t\right\}, \tag{10}$$

где символами $(a, b), (x, y), (\dot{x}, \dot{y})$ обозначены соответственно координаты наблюдателя в некоторой неподвижной системе координат, текущие координаты объекта и составляющие вектора текущей скорости объекта.

В случае N независимых наблюдателей, находящихся в пунктах с координатами (a_i, b_i), $i = 1, \ldots, N$, вероятность того, что ни один из них не обнаружит объект за время прохождения маршрута:

$$P_{\text{необн}}^{(N)} = \exp\left\{-\alpha T \sum_{i=1}^{N} \frac{1}{T_{0i}} - \frac{I_{\text{с}}(v_0)}{v_0^m} \sum_{i=1}^{N} \frac{q_i}{I_{\text{ш}i} T_{0i}} \int_0^T \frac{\left(\sqrt{(\dot{x}^2 + \dot{y}^2)}\right)^m}{\left(\sqrt{(x(t)-a_i)^2 + (y(t)-b_i)^2}\right)^k} \mathrm{d}t\right\}. \tag{11}$$

В случае, когда все сенсоры имеют одинаковые характеристики, используют одинаковые алгоритмы обработки информации и осуществляют прием в одних и тех же помеховых условиях, оптимизация (11) сводится к решению вариационной задачи о минимизации функционала (риска)

$$R = \int_0^T \sum_{i=1}^{N} \frac{\left(\sqrt{(\dot{x}^2 + \dot{y}^2)}\right)^m}{\left(\sqrt{(x(t)-a_i)^2 + (y(t)-b_i)^2}\right)^k} \mathrm{d}t \to \min_{(\dot{x}, \dot{y}, x, y)} \tag{12}$$

при наличии граничных условий

$$x(0)=x_A; \quad x(T)=x_B;$$
$$y(0)=y_A; \quad y(T)=y_B. \qquad (13)$$

Вариационная задача (12), (13) имеет следующую физическую интерпретацию. Подынтегральное выражение

$$F=\sum_{i=1}^{N}\frac{\left(\sqrt{(\dot{x}^2+\dot{y}^2)}\right)^m}{\left(\sqrt{(x(t)-a_i)^2+(y(t)-b_i)^2}\right)^k} \qquad (14)$$

пропорционально мгновенному уровню интенсивности сигнала, излученного объектом, прошедшего через среду распространения и принятого системой сенсоров. Соответственно, критерий (12) — это величина, пропорциональная интегральному уровню интенсивности сигнала, принятого системой сенсоров за время движения объекта по маршруту. Критерий (12) получил название энергетического риска, критерий (8) — вероятностного риска. Таким образом, при малых ОСП минимизация вероятностного риска сводится к минимизации энергетического риска.

Решение задачи

Уклонение объекта от обнаружения возможно на постоянной и переменной скорости. Исторически задача об оптимизации законов уклонения от обнаружения вначале решалась для случая движения уклоняющегося объекта на постоянной скорости [1–3]. При движении на постоянной скорости оптимизация закона уклонения сводится к оптимизации траектории уклонения. Величина скорости определяется видом траектории и заданным временем движения.

Развитие постановки состоит в построении такого закона управления подвижным объектом, при котором оптимизируется не только траектория уклонения, но и закон изменения скорости его движения по траектории. Постановка и решение такой задачи приведены в работах [4, 5]. Аналитическое решение задачи получено лишь при уклонении от одиночного сенсора; для случая уклонения обнаружения системой сенсоров предложены вычислительные алгоритмы.

Функционал (12) не зависит явно от времени — независимой переменной. Поэтому уравнения Эйлера для вариационной задачи (12), (13) имеют первый интеграл [9]. Было установлено [5], что этим первым интегралом является гамильтониан

$$\Phi=F-\dot{x}F_{\dot{x}}-\dot{y}F_{\dot{y}}, \qquad (15)$$

для которого на решениях уравнений Эйлера справедливы соотношения

$$\frac{d\Phi}{dt}=0; \qquad (16)$$

$$\Phi=(1-2m)F, \qquad (17)$$

нижние индексы в формуле (15) указывают переменные, относительно которых вычисляются частные производные.

Из соотношений (14), (16), (17) следует, что решение задачи (12), (13) обладает следующей важной для практики особенностью: движение объекта по оптимальной траектории уклонения с использованием оптимального закона изменения скорости порождает на входе наблюдателя сигнал, мгновенный уровень которого остается постоянным в течение всего времени движения. Оптимизация траектории уклонения с одновременной оптимизацией закона изменения скорости позволяет, при одном и том же интегральном уровне принятого сенсором сигнала, сформировать на его входе сигнал, мгновенный уровень которого меньше максимального мгновенного уровня сигнала, соответствующего движению по оптимальной траектории на постоянной скорости [4, 5]. Такая особенность оптимального закона уклонения на переменной скорости делает его перспективным для применения с точки зрения необнаружения объекта как по интегральному критерию, так и по мгновенному уровню сигнала.

Для решения оптимизационной задачи (12), (13) был разработан численный алгоритм, в основе которого лежит метод Дейкстры [10]; алгоритм использует постоянство подынтегральной функции в (14) и описан в работе [11]. В настоящей статье решение задачи приводится для случая $k = m = 2$, что соответствует изменению уровня интенсивности излучаемого сигнала пропорционально квадрату скорости объекта и распространению сигнала в среде по сферическому закону.

Решение задачи для случая одного сенсора $(N=1)$ было найдено аналитически [4, 5]. Функционал в этом случае имеет вид

$$R=\int_0^T\frac{\dot{x}^2+\dot{y}^2}{(x(t)-a_1)^2+(y(t)-b_1)^2}dt.$$

Введем полярную систему координат, полюс которой совпадает с положением сенсора, полярная ось проходит через начальную точку маршрута; начальные условия задачи в полярной системе имеют вид

$$\rho(0)=\rho_A,\ \psi(0)=0;\ \rho(T)=\rho_B,\ \psi(T)=\delta.$$

В указанной полярной системе уравнение оптимальной траектории уклонения имеет вид

$$\rho(\psi)=\rho_A\exp\left(\frac{\psi}{\delta}\ln\frac{\rho_B}{\rho_A}\right). \qquad (18)$$

Геометрический образ уравнения (18) — логарифмическая спираль, проходящая через граничные точки $A(x_A, y_A)$, $B(x_B, y_B)$ маршрута. Оптимальный закон изменения скорости

$$v(\psi) = c\rho(\psi) = \\ = c\rho_A \exp\left(\frac{\psi}{\delta}\ln\frac{\rho_B}{\rho_A}\right) = v_0 \exp\left(\frac{\psi}{\delta}\ln\frac{\rho_B}{\rho_A}\right), \quad (19)$$

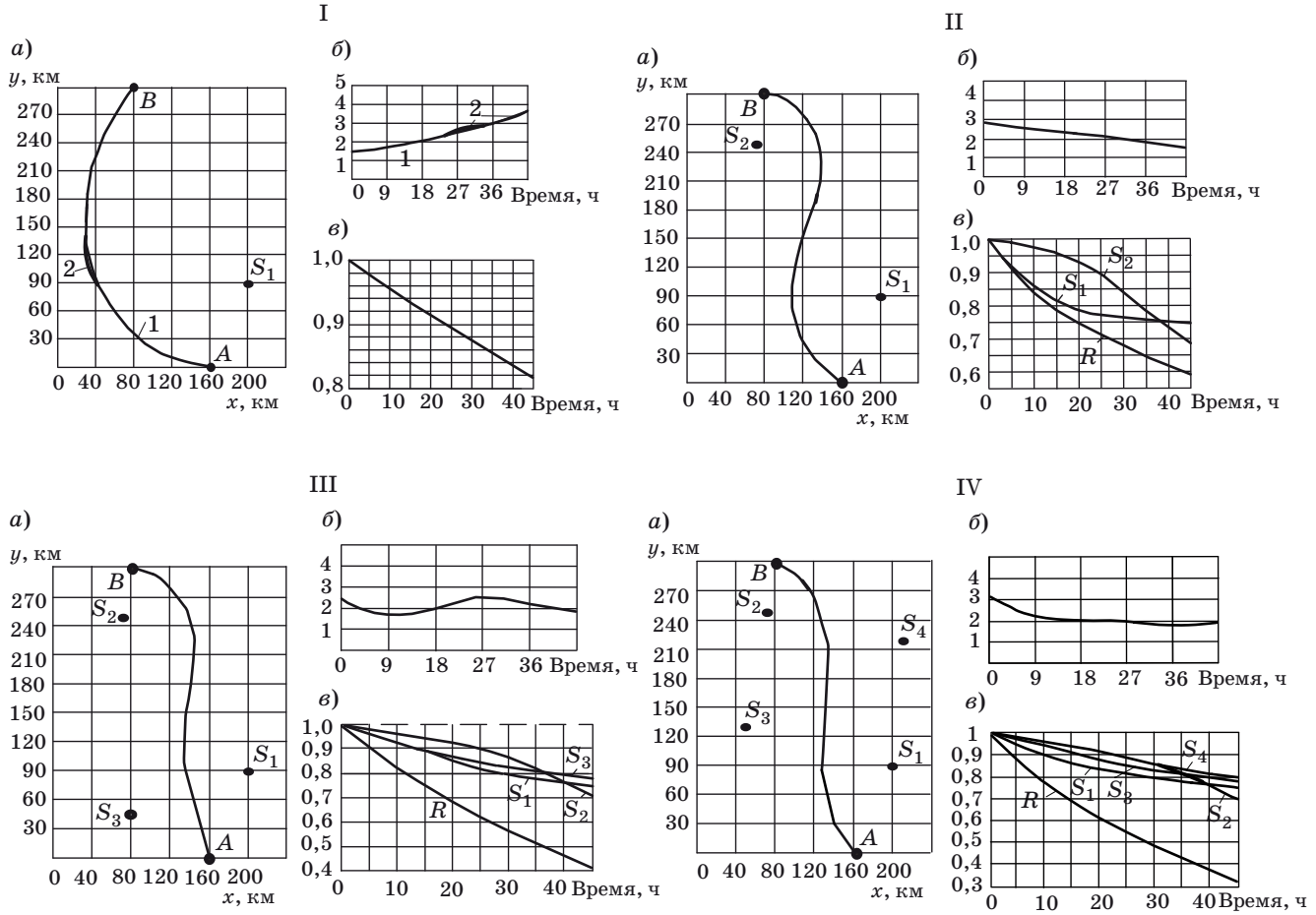
где v_0 — начальная скорость объекта; постоянная c определяется из условия прохождения объектом маршрута по оптимальной траектории с использованием оптимального закона изменения скорости за заданное время T:

$$c = \frac{1}{T}\sqrt{\delta^2 + \ln^2\frac{\rho_B}{\rho_A}}. \quad (20)$$

Аналитическое решение задачи об уклонении от обнаружения одиночным сенсором (18)–(20) было использовано для верификации результатов моделирования. Целями моделирования были построение оптимального закона уклонения объекта от обнаружения системой сенсоров; оценка вклада каждого сенсора в вероятность обнаружения объекта; оценка зависимости вероятности обнаружения объекта от числа сенсоров.

Результаты моделирования иллюстрируют рисунки I–IV, отличающиеся количеством наблюдателей (сенсоров) в регионе. На рисунках указаны положения начальной A и конечной B точек маршрута, количество и расположение сенсоров, обозначенных символами S_i, $i = 1, ..., 4$. Перемещение объекта происходит в регионе размером 240 × 300 км в течение 45 ч. Вероятность необнаружения объекта рассчитывалась по точной формуле (8).

На рисунке I, *а*, *б* изображены две траектории и два графика изменения скорости в задаче уклонения от обнаружения единственным наблюдателем S_1. Кривые *1*, полученные моделированием, и кривые *2*, иллюстрирующие теоретическое решение задачи уклонения [см. формулы (18), (19)], практически совпадают. Такая высокая точность аппроксимации позволяет рассматривать разработанный численный алгоритм в качестве приемлемого способа оптимизации закона управления подвижным объектом в задачах



■ *Оптимальный закон уклонения от обнаружения одним (I), двумя (II), тремя (III) и четырьмя (IV) наблюдателями: а — траектория; б — скорость, м/с; в — вероятность необнаружения*

уклонения от обнаружения. Кривая на рисунке I, *в* иллюстрирует зависимость вероятности необнаружения объекта как функции текущего момента времени.

На рисунках II–IV, *а–в* представлены результаты решения оптимизационной задачи для случая уклонения объекта от обнаружения системой наблюдателей.

На каждом рисунке изображены:

— составляющие оптимального закона управления подвижным объектом — оптимальная траектория уклонения и оптимальный закон изменения скорости как функция текущего момента времени (см. рисунки II–IV, *а*, *б*);

— значения вероятности необнаружения объекта как функции текущего момента времени, рассчитанные для каждого сенсора и системы сенсоров в целом: S_i — номер соответствующего сенсора; R — результирующая кривая, характеризующая вероятность необнаружения системой сенсоров.

Заключение

Сформулирована задача об оптимизации закона уклонения подвижного объекта от обнаружения системой наблюдателей. Критерием служит вероятность обнаружения объекта за время прохождения им маршрута. Оптимизация включает построение траектории уклонения и закона изменения скорости на оптимальной траектории. Показано, что при малых ОСП решение задачи об оптимизации по критерию «вероятность обнаружения» сводится к задаче минимизации интегрального уровня сигнала, принятого системой наблюдателей. Установлено, что оптимальный закон уклонения обеспечивает постоянство мгновенного уровня сигнала, поступающего на систему наблюдателей. Приводятся результаты моделирования.

Работа выполнена при финансовой поддержке программы Президиума РАН «Математическая теория управления» и гранта РФФИ № 10-08-90030-Бел_а.

Литература

1. **Zabarankin M., Uryasev S., Pardalos P.** Optimal Risk Path Algorithms // Cooperative Control and Opimizaton. Ch. 1 / Eds. R. Murphey, P. Pardalos. Dordrecht: Kluwer Acad., 2002. P. 271–303.
2. **Pachter L. S., Pachter M.** Optimal Paths for Avoiding a Radiating Source // Proc. 40 IEEE Conf. Des. and Contr. 2001. P. 3581–3586.
3. **Hallam C., Harrison R., Ward J.** A multiobjective optimal path algorithm // Digital Signal Processing. 2001. Vol. 11 (2). P. 133–143.
4. **Галяев А. А., Маслов Е. П., Рубинович Е. Я.** Об одной задаче управления движением объекта в конфликтной среде // Изв. РАН. Теория и системы управления. 2009. № 3. С. 134–140.
5. **Галяев А. А., Маслов Е. П.** Оптимизация законов уклонения подвижного объекта от обнаружения // Изв. РАН. Теория и системы управления. 2010. № 4. С. 52–62.
6. **Бурдик В. С.** Анализ гидроакустических систем. — Л.: Наука, 1988. — 392 с.
7. **Урик Р.** Основы гидроакустики. — Л.: Судостроение, 1978. — 445 с.
8. **Сысоев Л. П.** Критерий вероятности обнаружения на траектории в задаче управления движением объекта в конфликтной среде // Проблемы управления. 2010. № 6. С. 65–72.
9. **Краснов М. Л., Макаренко Г. И., Киселев А. И.** Вариационное исчисление. — М.: Наука, 1973. — 190 с.
10. **Dijkstra E.** A note of two problems in connection with graphs // Numerische Mathematik 1. 1959. P. 269–271.
11. **Абрамянц Т. Г., Маслов Е. П., Яхно В. П.** Уклонение подвижного объекта от обнаружения группой наблюдателей // Проблемы управления. 2010. № 5. С. 73–79.

УДК 681.518+519.724

ВЕРОЯТНОСТНЫЕ АДАПТИВНЫЕ АЛГОРИТМЫ ДИСКРЕТНОГО ПРЕДСТАВЛЕНИЯ АНАЛОГОВЫХ СИГНАЛОВ
Часть 1: Исследование свойств

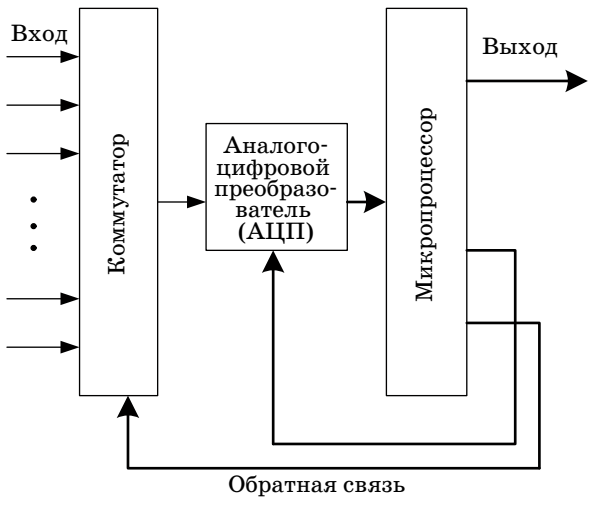
Э. П. Тихонов,
доктор техн. наук, доцент
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

Выполнено углубленное исследование ранее предложенного вероятностного метода адаптивной дискретизации. Показано, что данный метод основан на нелинейных вероятностных итерационных алгоритмах или отображениях, анализируемых в динамично развивающейся теории нелинейных систем. Рассмотрены вопросы сходимости предложенных алгоритмов на базе известного логистического отображения.

Ключевые слова *— временная дискретизация, адаптация, алгоритм, сходимость, погрешность, функция восстановления.*

Введение

Оптимизация процесса преобразования в цифровую временную последовательность аналоговых сигналов, поступающих с выходов различных преобразователей (датчиков) физических процессов в электрический сигнал на вход системы, остается одной из центральных проблем в информационных технологиях. Пример подобной многоканальной информационно-измерительной системы дан на рис. 1.



■ ***Рис. 1.*** *Многоканальная информационно-измерительная система*

Эта проблема стимулирует развитие и внедрение адаптивных методов и алгоритмов, предназначенных для решения задачи оптимизации временной дискретизации и сжатия информации при необходимом минимуме априорной информации о виде и характеристиках исходного сигнала. Минимум априорной информации о сигнале соответствует только самым общим исходным ограничениям, включая его принадлежность к достаточно широкому классу сигналов. Не акцентируя внимание на общих вопросах классификации известных методов адаптивной дискретизации, которые рассматривались, например, в работе [1], остановимся на углубленном исследовании вероятностного метода адаптивной дискретизации, предложенного [2] и в дальнейшем рассмотренного [3] автором.

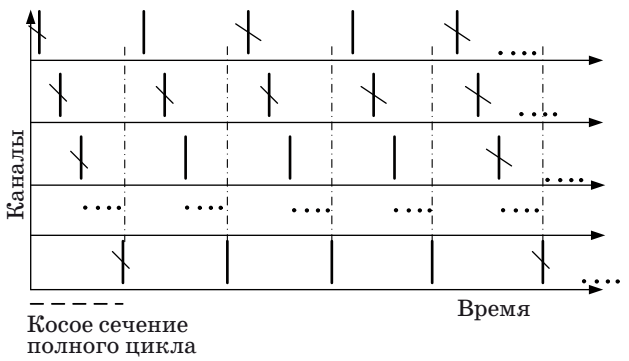
Исходная информация и уточненная постановка задачи

Вероятностный метод адаптивной дискретизации с точки зрения теории рассматриваемого вопроса интересен тем, что он основан на нелинейных вероятностных итерационных алгоритмах или отображениях [4], исследуемых в теории нелинейной динамики. Отображениям в последнее десятилетие уделяется особое внимание [5], и не только потому, что многие явления, обнаруженные при их исследовании, позволили найти ответы на давно назревшие вопросы в науке

и технике. Нелинейная динамика приблизилась вплотную к наиболее сложным вопросам гносеологии, а именно к вопросам самоорганизации, поставленным и исследуемым в последние десятилетия в синергетике — науке о самоорганизации [4–6]. Как следует из работы [6], самоорганизация — это выделение небольшого числа переменных, определяющих динамику всей системы. Конечно, это весьма общее, не охватывающее всех тонкостей процесса самоорганизации определение. Однако для рассматриваемой в настоящей работе темы оно отражает суть адаптивной дискретизации, заключающуюся в контролируемом сокращении объема информационного потока данных в каждом канале системы (см. рис. 1) до предела, необходимого для достижения общей поставленной цели. Следовательно, адаптивная дискретизация разрешает противоречие между бесконечным потоком информации и конечным ее представлением путем выделения по результатам дополнительного анализа в реальном масштабе времени из окружающей среды объема информации, существенного или, в определенном смысле, оптимального для функционирования динамической системы в целях достижения ею главной полезной функции. При этом любой адаптивный алгоритм дискретизации связан с решением обратной задачи, а именно с восстановлением исходной информации по дискретным отсчетам с погрешностью, не превышающей в определенном смысле заданной величины. Адаптивная дискретизация может осуществляться как во времени, так и в пространстве. Последний случай, согласно рис. 1, в основном и обуславливает наличие многоканальности в системе, при этом адаптивная дискретизация может быть как циклическая, так и адресная.

Восстановление сигнала при необходимости, например для графического представления измеряемого процесса, осуществляется по дискретным отсчетам сигнала в каждом канале с заданной или минимальной погрешностью восстановления, представляющей собой разность между исходным сигналом и его восстановленным значением. Каждый отсчет сигнала в каждом канале представляет собой результат преобразования аналоговой величины в цифровой двоичный код посредством АЦП, подключенного к выходу коммутатора (см. рис. 1), с точностью до величины кванта $\Delta q = E_0 2^{-N}$, где E_0 — диапазон преобразования входного сигнала в АЦП, а N — допустимое число двоичных разрядов. В дальнейшем будем предполагать, что для сигнала $y(t)$ в каждом канале выполняется ограничение $0 \le y(t) \le E_0$. Задача в дальнейшем рассматривается без учета многоканальности, так как в многоканальном варианте при циклическом опросе каналов один и тот же алгоритм адаптивной дискретизации реализуется программно в микропроцессоре независимо для каждого канала с запоминанием полученного результата в оперативном запоминающем устройстве. К записанному в запоминающем устройстве интервалу дискретизации для выбранного канала обращаются программно после полного цикла последовательного переключения каналов с реализацией алгоритма в каждом опрошенном канале. Под полным циклом (косым сечением) последовательного переключения каналов понимается число последовательных переходов с канала на канал от первого до последнего, включая переход от последнего до первого канала (рис. 2). Таким образом, интервал дискретизации в каждом канале кратен времени полного цикла переключения каналов. Благодаря этому неравномерность интервала дискретизации в каждом канале кратна времени полного цикла переключения каналов и интервал дискретизации в этом канале равен произведению числа полных пропущенных циклов на время одного полного цикла. Случай многоканальной адаптивной обработки информации с учетом зависимости информации между сигналами, поступающими по каждому каналу, требует отдельного рассмотрения. Очевидно, что подобная зависимость может возникнуть, если интервалы дискретизации в разных каналах по величине близки между собой. Тогда возможен адресный адаптивный выбор каналов, что сформировать программно значительно сложнее при достижении незначительных преимуществ.

Восстановление сигнала по дискретным отсчетам относится к традиционной задаче численной математики и широко применяется в многочисленных приложениях. Известно [7], что для сигналов, имеющих ограниченную спектральную функцию, интервал дискретизации устанавлива-



■ ***Рис. 2.*** *Условное обозначение переключения каналов и формирование косого сечения (зачеркивание обозначает считывание результата преобразования с АЦП в каждом канале в соответствии с установленным временным интервалом)*

ется в соответствии с теоремой Котельникова или просто с теоремой отсчетов. Этот интервал, как следует из теоремы, оптимален только для сигналов, принадлежащих к классу сигналов со строго ограниченным (финитным) частотным спектром. Интервал дискретизации теряет свою оптимальность при естественных отклонениях от заданных в теореме предельных условий восстановления сигнала, неизбежно возникающих в реальных практических ситуациях ее применения. Действительно, в технических системах восстановление сигнала по бесконечному числу отсчетов, обусловленных теоремой, невозможно, а автоматический контроль погрешности восстановления по конечному числу ряда Котельникова затруднителен. Поэтому при измерениях предпочитают полиномиальную [8] или, вернее, кусочно-полиномиальную форму восстановления сигнала. Последняя отличается тем, что сигнал восстанавливается оптимально в установленном смысле на каждом локальном временном фрагменте или временном секторе, на которые разбивается весь интервал, в течение которого осуществляется измерение сигнала.

Для того чтобы лучше представить назначение адаптивной дискретизации, обратимся к классической задаче интерполяции [9], являющейся частным случаем общей задачи восстановления сигнала. Суть классической задачи интерполяции состоит в том, что по известным дискретным отсчетам t_i, $i = 1, 2, ..., n$, следующим через временной интервал дискретизации, и значениям сигнала в этих дискретных отсчетах $y_i = y(t_i)$, $i = 1, 2, ..., n$, требуется найти аналитическое выражение восстанавливающей функции в виде заданного полинома. Восстанавливающая функция представляет приближенно с некоторой погрешностью на заданном временном интервале наблюдения $(0, T)$ исходную функцию. По условиям интерполяции, рассматриваемой в данном случае как частный случай восстановления, должны удовлетворяться в дискретных отсчетах равенства интерполяционной функции и входного сигнала в виде $\varphi(t_i) = y(t_i)$, $i = 1, 2, ..., n$. Эта задача не имеет однозначного решения, так как через эти точки можно провести бесконечное множество кривых. Однако можно ограничиться только определенным классом кривых, представленных в виде многочлена или полинома m-й степени

$$\varphi(t) = \varphi_m(t) = \sum_{i=0}^{m} a_i t^i,$$

где a_i — искомые коэффициенты, $m = 0, 1, 2, ...$.

Согласно классической теории интерполяции сигнала в форме Ньютона полиномом m-й степени с интервалом дискретизации τ_{0m} [9], оценка погрешности восстановления сигнала определяется по формуле

$$\delta(y(t), \varphi_m(t, \tau_{0m})) = $$
$$= y(t) - \varphi_m(t, \tau_{0m}) = \frac{y^{(m+1)}(\eta)}{(m+1)!}\Psi_m(t),$$

где $y^{(m+1)}(\eta)$ — $(m+1)$-я производная входного сигнала в точке η, принадлежащей интервалу интерполяции и находящейся в одном интервале с точками $i\tau_{0m}$ и t; $\Psi_m(t) = (t)(t - \tau_{0m})(t - 2\tau_{0m}) ... (t - m\tau_{0m})$ — многочлен $(m+1)$-й степени.

Следовательно, для равномерной функции меры погрешности восстановления имеем

$$\theta[\delta(y(t), \varphi_m(t, \tau_{0m}))] = $$
$$= |y(t) - \varphi_m(t)| = \frac{\left|y^{(m+1)}(\eta)\right|}{(m+1)!}|\Psi_m(t)|. \qquad (1)$$

Технически процесс адаптивной дискретизации можно представить в следующем виде. Пусть фиксирована степень интерполирующего полинома m. Предположим, что рассматривается одноканальная система с АЦП, на вход которого поступает сигнал. Этот сигнал преобразуется в цифровую последовательность с временным интервалом дискретизации, определяемым быстродействием АЦП и временем, необходимым для проведения дополнительных вычислений с целью определить погрешность интерполяции через конечную разность. Полученная оценка погрешности интерполяции сравнивается с заданной величиной. По результатам сравнения ставится задача поиска такого интервала дискретизации, при котором на интервале наблюдения $(0, T)$ исходная функция будет восстановлена с погрешностью, в определенном смысле равной заданной величине. При этом точки отсчета могут быть распределены на интервале $(0, T)$ равномерно или не равномерно. При равномерном распределении точек отсчета речь идет о дискретизации с постоянным интервалом дискретизации $\Delta t_i = \tau_0 = \text{const}$. В противном случае говорят о дискретизации с неравномерным интервалом. Обычно в технических задачах или медико-биологических исследованиях устанавливаются естественные ограничения на сигнал. Эти ограничения количественно оцениваются, например, накладываемыми численными ограничениями на его производные (или конечные разности) и максимально возможные значения. Эти ограничения связаны с частотой среза спектральной функции известным неравенством Бернштейна [10].

Для решения задачи поиска искомого постоянного интервала дискретизации по виду функции и величине погрешности восстановления необходимо построить соответствующий алгоритм. При этом алгоритм должен быть таким, чтобы в случае

изменения соответствующих характеристик сигнала (естественно, в определенных пределах) в случайные моменты времени обеспечивалась бы в реальном масштабе времени автоматическая перестройка на новый интервал дискретизации. Поскольку априори предсказать момент изменения характеристик сигнала невозможно, алгоритм поиска интервала дискретизации относится к алгоритмам адаптивного типа. Очевидно, что адаптивный поиск оптимального интервала дискретизации в указанном смысле попутно с общей задачей дискретизациий сигнала решает дополнительно задачу сокращения избыточности информации или сжатия данных. Под сокращением избыточности информации в данном случае понимается представление исходного сигнала таким числом дискретных отсчетов, которое необходимо и достаточно для его восстановления с заданной погрешностью.

Описание метода и формализация алгоритма

Итак, для того чтобы построить адаптивный алгоритм поиска оптимального интервала дискретизации, целесообразно исходить из некоторого начального значения интервала, получить для него погрешность восстановления сигнала по выбранному виду функции восстановления, сравнить полученную погрешность с заданной величиной и по результатам сравнения принять решение об изменении исходного интервала дискретизации. При принятии решения нужно установить, на какую величину требуется изменить исходный интервал дискретизации в большую или меньшую сторону, чтобы при последующем повторении описанных выше действий погрешность восстановления при тех же условиях приближалась бы к приемлемому значению. Поскольку о сигнале имеется только начальная ограничительная информация, то, естественно, невозможно сразу предсказать точное значение искомого интервала дискретизации, поэтому в адаптивном алгоритме на основании накопления информации по предыдущим результатам на каждом последующем этапе (такте) в соответствии с алгоритмом осуществляется только уточнение значения текущего интервала дискретизации. Следовательно, любой адаптивный алгоритм использует прошлую и текущую информацию для подстройки параметров системы в целях обеспечения оптимального в установленном смысле ее функционирования в настоящем и будущем при условии квазистационарности среды, в которой функционирует система. Таким образом, любой адаптивный алгоритм является алгоритмом экстраполяционного типа, т. е. предсказывающим алгоритмом. Если же соответствующие характеристики среды, обуславливающие входной сигнал системы, изменяются быстрее переходного процесса адаптации, то ошибка прогнозирования увеличивается и может достигнуть такого значения, что эффект адаптации полностью нивелируется. Заметим, что любой не адаптивный алгоритм дискретизации также в определенной степени является экстраполяционным, так как он однозначно устанавливает параметры системы для ее функционирования в будущем в неизменной среде или при таком ее минимально допустимом дрейфе, при котором ущерб функционирования системы с неизменными параметрами не являлся бы критическим.

Вывод адаптивного алгоритма поиска оптимального интервала дискретизации можно обосновать, используя, например, метод Эйлера для численного решения задачи Коши [11]. В результате этого вывода искомый итерационный алгоритм можно представить в виде

$$\tau[(k+1)\Delta t] = \\ = \tau(k\Delta t) - \Delta(k)\mu\{\theta[\delta(y(t), \varphi_m(t, \tau(k\Delta t)))], \delta_0\}, \quad (2)$$

где $\tau[(k+1)\Delta t]$ и $\tau(k\Delta t)$ — значения искомого интервала дискретизации на $(k+1)$-м и k-м шаге итерации; $\Delta(k)$ — некоторая последовательность, влияющая на изменение значения искомого интервала дискретизации на $(k+1)$-м шаге итерации в зависимости от его значения на k-м шаге итерации; $\delta(...)$ — текущая погрешность восстановления исходного сигнала $y(t)$ посредством функции восстановления $\varphi_m(t, \tau(k\Delta t))$ на интервале $\tau(k\Delta t)$; $\mu\{\theta[\delta(...)], \delta_0\}$ — некоторая функция, характеризующая величину отклонения текущей погрешности восстановления сигнала $y(t)$ на интервале $\tau(k\Delta t)$ от ее заданной величины δ_0; $\theta[\delta(...)]$ — функция меры (1), описывающая зависимость величины отклонения сигнала $y(t)$ от функции восстановления $\varphi_m(t, \tau(k\Delta t))$ и тем самым определяющая соответствующую характеристику погрешности восстановления; m — индекс, значение которого определяется порядком m интерполирующего полинома или иной функции восстановления; Δt — временной шаг итерации.

Для многоканального случая временной шаг итерации в (2) увеличивается кратно числу каналов, при этом его минимальное значение определяется не только необходимыми операциями, выполняемыми в соответствии с выбранным алгоритмом, а и временем переключения каналов в полном цикле. В дальнейшем для упрощения записи принимается, что $\Delta t = 1$. В алгоритме (2) в силу того, что входной сигнал $y(t)$ описывается моделью случайного процесса, интервал дискретизации в зависимости от изменения шага итерации изменяется случайно. Поэтому важной характеристикой алгоритма является дисперсия

интервала, которая после периода адаптации называется финальной дисперсией, величина которой определяет методическую случайную составляющую погрешности адаптивного интервала и является наряду со средним значением интервала важнейшей метрологической характеристикой алгоритма. Если в алгоритме учитывается информация на более удаленных значениях искомого интервала дискретизации, то итерационный алгоритм принимает вид

$$\tau(k+1) = \tau(k) - \Delta(k)\mu \times$$
$$\times\{\theta[\delta(\varphi_m(t, \tau(k), \tau(k-1), \ldots, \tau(k-m)), y(t))], \delta_0\}, \quad (3)$$

который отличается только «глубиной памяти» алгоритма на интервалы дискретизации, определяющие анализируемый локальный или кусочно-интерполяционный временной участок T_0 сигнала $y(t)$. Как следует из алгоритмов, предсказание интервала дискретизации на последующем такте итерации зависит от характеристики отклонения в виде некоторой функции $\mu\{...\}$ погрешности восстановления сигнала на текущем интервале дискретизации от заданной величины и некоторого заданного множителя $\Delta(k)$. Этот множитель можно назвать множителем доверия, в соответствии с которым корректируется текущий интервал дискретизации для оценки интервала на следующем такте итерации. Множитель доверия, очевидно, должен быть таким, чтобы в худшем случае он стабилизировал бы интервал дискретизации при допустимой флуктуации погрешности восстановления относительно заданной величины, а в лучшем случае он обладал бы экстраполяционными свойствами, т. е. изменялся в зависимости от результатов предсказания отклонения погрешности восстановления от заданной величины на предыдущем такте итерации. Таким образом, из алгоритмов (2) и (3) непосредственно вытекает, что чем меньше значение преобразования $\mu\{...\}$, характеризующее отклонение погрешности восстановления на текущем интервале дискретизации от заданной величины, тем меньше изменяется данный интервал, и наоборот. Этот вывод может служить основанием для выбора множителя $\Delta(k)$ и его увязки с характеристиками сигнала на основе, например, метода Ньютона [9]. Уточнение вида представленных алгоритмов определяется также особенностями построения соответствующей функции восстановления на текущем интервале дискретизации $\tau(k)$. В дальнейшем остановимся на исследовании алгоритма (2), так как алгоритм (3) можно свести к алгоритму (2). В этом случае $\tau(k) = \tau(k-1) = ... = \tau(k-m) = T_0/m$, а в соответствии с алгоритмом (2) адаптивно по соответствующей восстанавливающей функции и заданной погрешности находится интервал или фрагмент T_0.

Для того чтобы полностью определить алгоритм (2) для технических приложений, необходимо указать начальные значения и внести соответствующие ограничения на входящие в алгоритм параметры и переменные. Прежде всего, отметим, что искомый интервал дискретизации может принимать значения в пределах (τ_{min}, τ_{max}). Следовательно, для интерполяционного фрагмента $T_0 \in (\tau_{min}, \tau_{max})$. Минимальное значение интервала дискретизации определяется временем преобразования $\tau_{пр}$ аналогового амплитудного значения сигнала в цифровой код, т. е. $\tau_{min} = \tau_{пр}$. Целесообразно конкретизировать и вид последовательности $\Delta(k)$, по которой можно соответствующим образом классифицировать алгоритмы. Пусть для начала эта последовательность для всех k вырождается в некоторую постоянную величину, т. е. $\Delta(k) = \Delta_0$, для всех k. Сигнал $y(t)$ имеет также ограничения на значения и производные в виде $|y(t)| \le Y_{max}$ и $|y^{(m)}(t)| \le Y^{(m)}{}_{max}$ (где $y^{(m)}(t)$ — производная m-го порядка от сигнала $y(t)$, $m = 0, 1, 2, 3, ...$). Конкретизация представленных в общем виде преобразований также определяет соответствующий вид адаптивного алгоритма дискретизации. Метод и результат исследования сходимости текущего интервала дискретизации $\tau(k)$ к его установившемуся значению τ_{m0} при фиксированных характеристиках сигнала, заданной погрешности и функции восстановления зависит от преобразований $\mu\{...\}$ и $\theta[...]$. Вопрос выбора данных преобразований уже на начальном этапе синтеза решается с учетом различных влияющих факторов и исходных требований.

Рассмотрим вопросы, связанные с выбором вида функции восстановления, и отметим общие моменты, влияющие на вид функции восстановления, заданную погрешность восстановления и характеристики адаптивного алгоритма в целом. Во-первых, независимо от вида функции восстановления (в рассматриваемом случае степени полинома) адаптивный алгоритм должен обеспечить сходимость текущего интервала $\tau(k)$ к некоторому установившемуся оптимальному его значению τ_{0m} и поддерживать это значение, если вероятностные характеристики сигнала не зависят от текущего времени. Необходимо также определить само понятие оптимального интервала дискретизации. Для этого уточним общую модель сигнала $y(t)$ и вид преобразования $\mu\{...\}$ в алгоритме (2). Характеристику погрешности восстановления $\theta[...]$ в (2) можно определить либо как среднее отклонение восстановленного и истинного значения сигнала на текущем интервале $\tau(k)$, либо привязать к некоторой точке интервала $\tau(k)$, например к точке, где погрешность восстановления достигает максимального значения.

В настоящее время известна самая общая модель, в соответствии с которой можно описать сигнал $y(t)$, — это модель случайного нестационарного процесса. Однако для нашего случая целесообразно ввести частный случай этой общей модели в виде случайного кусочно-стационарного и кусочно-эргодического процесса, представляющего собой конкретизацию исходной общей модели нестационарного сигнала и охватывающую широкий круг практических приложений. При этом минимальный интервал, на котором должна обеспечиваться стационарность случайного процесса, определяется так называемым периодом адаптации, т. е. временем перехода от начального интервала дискретизации $\tau_{пр}$ или неоптимального значения интервала дискретизации к оптимальному интервалу дискретизации τ_{0m}. Если период адаптации превышает «изменчивость» сигнала, это приводит к определенным нарушениям установленной оптимальности, критичность которой к этим нарушениям в каждом отдельном случае будет разной и требует особого исследования.

Исходное преобразование $\mu\{...\}$ в алгоритме (2) представим в виде

$$\mu\{\theta[\delta(y(t), \varphi_m(t, \tau(k)))], \delta_0\} = \\ = \mu\{\theta_1[\delta(y(t), \varphi_m(t, \tau(k)))] - \theta_2[\delta_0(y(t), \phi(t, \tau(k)))]\},$$

где

$$\mu\{\theta[\delta(y(t), \varphi_m(t, \tau(k)))], \delta_0\} = \\ = \frac{\partial \Psi\{\theta[\delta(y(t), \varphi_m(t, \tau(k)))], \delta_0\}}{\partial \tau(k)},$$

а $\Psi\{...\}$ — преобразование, обладающее свойствами функции меры или функции качества. Например, в простейшем случае при контроле погрешности восстановления по абсолютной величине или квадрату разности получаем

$$\Psi\{...\} = \begin{cases} \left|\theta[\delta(y(t), \varphi_m(t, \tau(k)))] - \delta_0\right| \\ \text{для абсолютной меры приближения;} \\ [\theta[\delta(y(t), \varphi_m(t, \tau(k)))\}] - \delta_0]^2 \\ \text{для квадратичной меры приближения.} \end{cases}$$

При контроле погрешности восстановления по относительной величине (ε_0 — безразмерная величина) соответствующее преобразование можно уточнить, например, в виде

$$\Psi\{...\} = \Psi\{\left|\delta(y(t), \varphi_m(t, \tau(k)))\right| - \varepsilon_0 \left|y(t)\right|\}.$$

Обычно выполняется равенство преобразований $\theta_1[...] = \theta_2[...] = \theta[...]$.

Будем считать, что алгоритм (2) сходится к оптимальному интервалу дискретизации τ_{0m}, если для него выполняется условие

$$M_y\{\mu\{\theta[y(t), \delta(\varphi_m(t, \tau_{0m}))] - \\ - \theta[y(t), \varepsilon_0(\phi(t, \tau_{0m}))]\}\} = 0, \qquad (4)$$

где $M_y\{...\}$ — оператор определения математического ожидания по $y(t)$.

Итак, оптимальным интервалом дискретизации называется такой интервал τ_{0m}, для которого в среднем выполняется равенство погрешности восстановления сигнала $y(t)$ посредством восстанавливающей функции $\varphi_m(t)$ ее заданному в том или ином виде значению. Естественно, что равенство (4) удовлетворяется для некоторого среднего значения интервала, которым и является интервал τ_{0m}. Как уже отмечалось, помимо равенства (4) важной характеристикой оптимальности является дисперсия флуктуации текущего интервала дискретизации относительно оптимального значения, которая характеризует случайную составляющую погрешности установления оптимального интервала дискретизации. Если в алгоритм (2) не включаются влияющие факторы, то речь идет о характеристике методической случайной погрешности. В противном случае дисперсия флуктуации интервала дискретизации относительно оптимального значения оценивает полную случайную погрешность. Исследование алгоритма сконцентрировано на выяснении условия и вида сходимости алгоритма к искомому оптимальному значению в среднем и на определении величины дисперсии, т. е. на выяснении, при каких значениях параметров алгоритма и характеристик сигнала обеспечивается сходимость алгоритма или точность (величина, обратная к погрешности) установления и поддержания оптимального интервала дискретизации. Представление об установлении интервала дискретизации связано с переходным процессом в начальный момент функционирования системы и случаем, когда в процессе функционирования системы вероятностные характеристики сигнала изменяются. Понятие «изменяются» определяется через время перехода от предыдущего к текущему виду вероятностной характеристики сигнала.

Исследование сходимости

Таким образом, назначение алгоритма (2) состоит в том, чтобы осуществить поиск оптимального интервала дискретизации в установленном смысле, выполняя последовательно во времени действия, предписанные указанным алгоритмом. Выбор функции восстановления, а также вида преобразований, входящих в алгоритм (2), диктуется рядом требований, например требованием помехоустойчивости и эффективности сжатия данных, сложностью реализации алгоритма или объемом вычислений, скоростью и точно-

стью сходимости к оптимальному интервалу дискретизации. Рекомендации для оценки указанных характеристик можно получить в зависимости от той задачи, в интересах которой применяется адаптивный алгоритм. В общем случае алгоритм (2) как математический объект относится к итерационному стохастическому нелинейному уравнению в конечных разностях или просто отображению, ориентированному на поиск нуля функции регрессии [6, 12], зависящей от функции качества восстановления исходного сигнала по его дискретным отсчетам. Функция качества восстановления исходного сигнала относится к одной из важнейших характеристик, которая влияет на процесс поиска оптимального интервала дискретизации, т. е. на его сходимость, причем речь идет о сходимости в среднем. Сходимость алгоритма (2) к оптимальному интервалу дискретизации в общем случае при соответствующих ограничениях может быть доказана, в результате чего может быть получено уравнение для выражения оптимального интервала дискретизации через характеристики входного сигнала и параметры адаптивного алгоритма путем приведения этого уравнения к известному логистическому отображению. Для этого представим исходный алгоритм в виде

$$V_\tau(k+1) = V_\tau(k) - \Delta(k)\mu \times \\ \times \{\theta[\delta(\varphi(t, \tau_0 + V_\tau(k)), y(t))], \delta_0\}, \qquad (5)$$

где $V_\tau(k+1) = \tau_\tau(k+1) - \tau_0$ и $V_\tau(k) = \tau_\tau(k) - \tau_0$.

Пусть для τ_0 выполняется условие (4). Тогда, вычитая из правой и левой частей (5) значения τ_0 и разлагая в ряд Тейлора преобразование $\mu\{...\}$ относительно τ_0 с учетом непрерывности производных и $\Delta(k) = \Delta_0 = \text{const}$, переходим после усреднения к эквивалентному в указанном смысле алгоритму с точностью до малой величины третьего порядка

$$\bar{V}_\tau(k+1) = z''_{0\tau}\bar{V}_\tau(k)\left[\frac{1 - z'_{0\tau}}{z''_{0\tau}} - \bar{V}_\tau(k)\right], \qquad (6)$$

где $\bar{V}_\tau(k+1) = M_y\{\tau(k+1) - \tau_0\}$; $\bar{V}_\tau(k) = M_y\{\tau(k) - \tau_0\}$, $M_y\{...\}$ — оператор усреднения по множеству при фиксированном t;

$$z'_{0\tau} = \Delta_0 M_y\left\{\frac{\partial\{\mu\{\theta[\delta(\varphi_m(t,\tau), y(t))], \delta_0\}\}}{\partial\tau}\bigg|_{\tau=\tau_0}\right\};$$

$$z''_{0\tau} = \gamma_\tau \Delta_0 M_y\left\{\frac{\partial^2\left\{\mu\left\{\theta\left[\delta\left(\varphi_m(t,\tau), y(t)\right)\right], \delta_0\right\}\right\}}{\partial\tau^2}\bigg|_{\tau=\tau_0}\right\},$$

здесь γ_τ — постоянная разложения в ряд Тейлора относительно неподвижной точки τ_0, $\tau_0 \in [\tau_{\min}, \tau_{\max}]$; Δ_0 — априорно назначаемый шаг поиска (итерации).

Для последующего исследования сходимости в алгоритме (6) выполним замену переменных

$$\bar{V}_\tau(k) = g_{0\tau}Z_\tau(k),\ \bar{V}_\tau(k+1) = g_{0\tau}Z_\tau(k+1) \text{ и } g_{0\tau} = \frac{1 - z'_{0\tau}}{z''_{0\tau}}.$$

В результате получим известное [12] логистическое отображение в виде

$$Z_\tau(k+1) = (1 - z'_{0\tau})Z_\tau(k)[1 - Z_\tau(k)], \qquad (7)$$

которое имеет две неподвижные точки: $Z_{\tau 1} = 0$ и $Z_{\tau 2} = 1 - 1/z'_{0\tau}$. Первая точка устойчива, если $0 < 1 - z'_\tau < 1$ или $0 < z'_\tau < 1$. Это условие достигается выполнением требования

$$V_{\tau\max}(k) / g_{0\tau} = \frac{V_{\tau\max}(k)}{1 - z'_{0\tau}} z''_{0\tau} = 1,$$

которое определяет ограничение для диапазона изменения регулируемого параметра при соответствующем значении параметра $z'_{0\tau}$ для каждого значения k. Действительно, пусть для всех k выполняется равенство $V_{\tau\max} = \tau_{\max}$, тогда максимальное значение диапазона регулируемого параметра определяется из выражения

$$d_{\tau\max} = \frac{1 - z'_{0\tau}}{\gamma_\tau z''_{0\tau}}.$$

Из данного равенства вытекает, что, установив соответствующие соотношения для первой и второй производной функции регрессии, подбором параметра Δ_0 можно определить диапазон изменения регулируемого, т. е. измеряемого, значения интервала. Отметим, что если преобразование $\mu\{...\}$ линейное, то диапазон изменения не ограничен.

Из исследования [12] логистического отображения следует, что первая неподвижная точка устойчива, если $(1 - z'_{0\tau}) \in (0, 1]$. Это условие и определяет сходимость в среднем адаптивного алгоритма (7) и, следовательно, существование неподвижной точки для исходного алгоритма (2). Отображение (5) теряет устойчивость, если $(1 - z'_{0\tau}) \in (1,4]$. Условия, вытекающие из изменений $(1 - z'_{0\tau})$, позволяют установить границы для изменения параметра $z'_{0\text{р}}$, гарантирующие устойчивую сходимость синтезируемых адаптивных вероятностно-итерационных алгоритмов к искомой неподвижной точке. При этом усредненное отклонение $V_\tau(k)$ и, следовательно, систематическая погрешность с увеличением числа итераций стремится к нулю. Если пренебречь влиянием второй производной, то скорость сходимости к искомой неподвижной точке при $z'_{0\tau} < 1$ легко устанавливается из равенства

$$V_\tau(k) = V_\tau(0)(1 - z'_{0\tau})^k.$$

Систематическая погрешность находится по результату усреднения разности $V_\tau(k)$. Поэтому

наличие предела $\lim_{k\to\infty} V_\tau(k) = 0$ доказывает потенциальную несмещенность обобщенного алгоритма. Уточнение скорости сходимости с учетом второй производной обычно выполняется методом имитационного моделирования. В случае $\Delta(k) \neq$ $\neq$ const требования к сходимости исходного алгоритма сохраняются. Однако условия для установления максимального диапазона изменения регулируемого параметра несколько меняются. Поскольку «фокусирующая» последовательность a_n при увеличении числа итераций стремится к нулю, то диапазон устойчивой работы вероятностно-итерационных алгоритмов стремится к бесконечности, если усредненная первая производная ограничена. Следует учитывать, что для последовательности вида $\Delta(k) = \Delta_0/k$, где $\Delta_0 = \text{const} > 0$, $k = 1, 2, \ldots$, шаг поиска или постоянная Δ_0 должна выбираться такой, чтобы $0 < Z_\tau < 1$ для всех k.

При синтезе адаптивного алгоритма для поиска интервала дискретизации на основе итерационной процедуры с привлечением интерполирующего полинома m-й степени возникает вопрос о способе определения погрешности восстановления и оценки ее характеристик. При этом можно применять как равномерную меру, так и другие меры приближения, что и будет рассмотрено в следующей части статьи.

Литература

1. **Дедус Ф. Ф.** и др. Обобщенный спектрально-аналитический метод обработки информационных массивов. Задачи анализа изображений и распознавания образов / Под общ. ред. Ф. Ф. Дедуса. — М.: Машиностроение, 1999. — 357 с.
2. **Тихонов Э. П.** Некоторые вопросы сжатия информации с использованием самообучающегося автомата // Конф. по автоматическому контролю и методам электрических измерений: Тез. докл. и сообщений, Новосибирск, 13–17 сентября 1966 г. Новосибирск: Наука, 1966. С. 37.
3. **Тихонов Э. П.** Адаптивные измерительные алгоритмы для решения задач медицинской диагностики в условиях воздействия помех // Вестник СПб отдния Метрологической акад. / ВНИИМ им. Д. И. Менделеева. СПб., 2000. Вып. 7. С. 29–38.
4. **Малинецкий Г. Г., Потапов А. Б., Подлазов А. В.** Нелинейная динамика: Подходы, результаты, надежды (Синергетика: от прошлого к будущему). — М.: КомКнига, 2006. — 280 с.
5. **Кузнецов С. П.** Динамический хаос (курс лекций): учеб. пособие для вузов. Изд. 2-е, перераб. и доп. — М.: Физматлит, 2006. — 356 с.
6. **Малинецкий Г. Г.** Математические основы синергетики: Хаос, структуры, вычислительный эксперимент. Изд. 5-е, стер. — М.: ЛКИ, 2007. — 312 с.
7. **Жуков А. И.** Метод Фурье в вычислительной математике. — М.: Наука. Гл. ред. Физматлит, 1992. — 176 с.
8. **Немировский А. С.** Вероятностные методы в измерительной технике (измерение стационарных случайных процессов). — М.: Издат. Гос. ком. стандартов, мер и измерительных приборов, 1964. — 216 с.
9. **Гельфонд А. О.** Исчисление конечных разностей: учеб. пособие. Изд. 3-е, перераб. — М.: Наука. Гл. ред. Физматлит, 1967. — 375 с.
10. **Эдвардс Р.** Ряды Фурье в современном изложении: пер. с англ.; в 2 т. Т. 1. — М.: Мир, 2003. — 296 с.
11. **Бахвалов Н. С.** Численные методы (анализ, алгебра, обыкновенные дифференциальные уравнения). — М.: Наука. Гл. ред. Физматлит, 1973. — 631 с.
12. **Данилов Ю. А.** Лекции по нелинейной динамике. Элементарное введение. — М.: Постмаркет, 2001. — 184 с.

УДК 621.396.96

ЭФФЕКТИВНОСТЬ ПРОЕКЦИОННОГО ВРЕМЯ-ЧАСТОТНОГО РАЗРЕШЕНИЯ ГРУППОВЫХ РАССЕИВАТЕЛЕЙ

А. А. Чижов,
канд. техн. наук, доцент, заместитель начальника кафедры
А. С. Лебедев,
канд. техн. наук, преподаватель
А. В. Тараканов,
канд. техн. наук, преподаватель
А. Н. Курочкин,
адъюнкт
Военная академия войсковой ПВО им. Маршала Советского Союза А. М. Василевского

Приведен ряд оценок показателей разрешающей способности двумерных проекционных процедур обработки сигналов при часто встречающейся в приложениях функции рассогласования, характерной для локационных задач в условиях временных и частотных сдвигов эхо-сигналов отдельных рассеивателей.

Ключевые слова *— обратная задача рассеяния, сверхрэлеевское разрешение, групповой рассеиватель, разрешающая способность.*

Введение

В работе [1] рассмотрены вопросы аналитической оценки эффективности проекционного метода решения обратной задачи группового рассеяния, а также приведен расчетный пример для случая одномерного разрешения при функции рассогласования вида гауссоиды.

Заметно более высоких показателей разрешающей способности радиолокаторов по сравнению с одномерным (однопараметрическим) разрешением можно добиться при использовании процедур многомерного разрешения. Последние позволяют при прочих равных условиях обеспечить меньшие значения коэффициентов рассогласования между эхо-сигналами отдельных рассеивателей (отдельных целей из состава групповой сосредоточенной) и, в целом, функции неопределенностей в каждой практической задаче.

При некотором увеличении времени наблюдения и увеличении скоростей перемещения целей повышение размерности задачи разрешения естественно, так как помимо типовых параметров рассеивателей, таких как их радиальные дальности и скорости, а также пеленги, появляются и высшие производные этих параметров, что создает предпосылки для разработки многомерных систем технического зрения с достаточно высокой разрешающей способностью (многомерных радиовизоров).

В настоящей статье приведен ряд оценок показателей разрешающей способности двумерных проекционных процедур обработки сигналов при часто встречающейся в практических приложениях функции рассогласования

$$\rho(\Delta_1, \Delta_2) = \text{triang}\,\Delta_1 \,\text{sinc}\,\Delta_2,$$

где

$$\text{triang} = \Delta_1 \begin{cases} 1 - |\Delta_1| \text{ при } |\Delta_1| < 1; \\ 0 \text{ для других } \Delta_1. \end{cases}$$

Функция $\rho(\Delta_1, \Delta_2)$ является некоторой аппроксимацией главного лепестка типовых функций рассогласования для радиолокационных задач в условиях временных и частотных сдвигов эхо-сигналов отдельных рассеивателей.

Аналитическая оценка эффективности проекционного время-частотного разрешения

Многомерные функции рассогласования существенно расширяют «ассортимент» возможных конфигураций портретов групповых рассеивателей, подлежащих исследованию, и даже для двумерного случая вопросы исчерпывающей

оценки эффективности обработки наблюдаемых сигналов, а также анализ факторов, влияющих на эту эффективность, выходят за рамки одной статьи. Поэтому далее приведены результаты исследований только для случая парного рассеивателя (число отдельных рассеивающих элементов меньше или равно двум).

Корреляционная матрица ошибок проекционного оценивания вектора комплексных коэффициентов отражения обратна матрице Грама системы весовых сигналов [1]:

$$\mathbf{V} = \mathbf{Q}^{-1}. \qquad (1)$$

Необходимо подчеркнуть, что зависимость (1) указывает на целесообразность обобщения классического понятия функции неопределенностей Ф. Вудворда [2]. Так, функцию неопределенностей Ф следует определять величиной, обратной детерминанту матрицы Грама системы весовых сигналов:

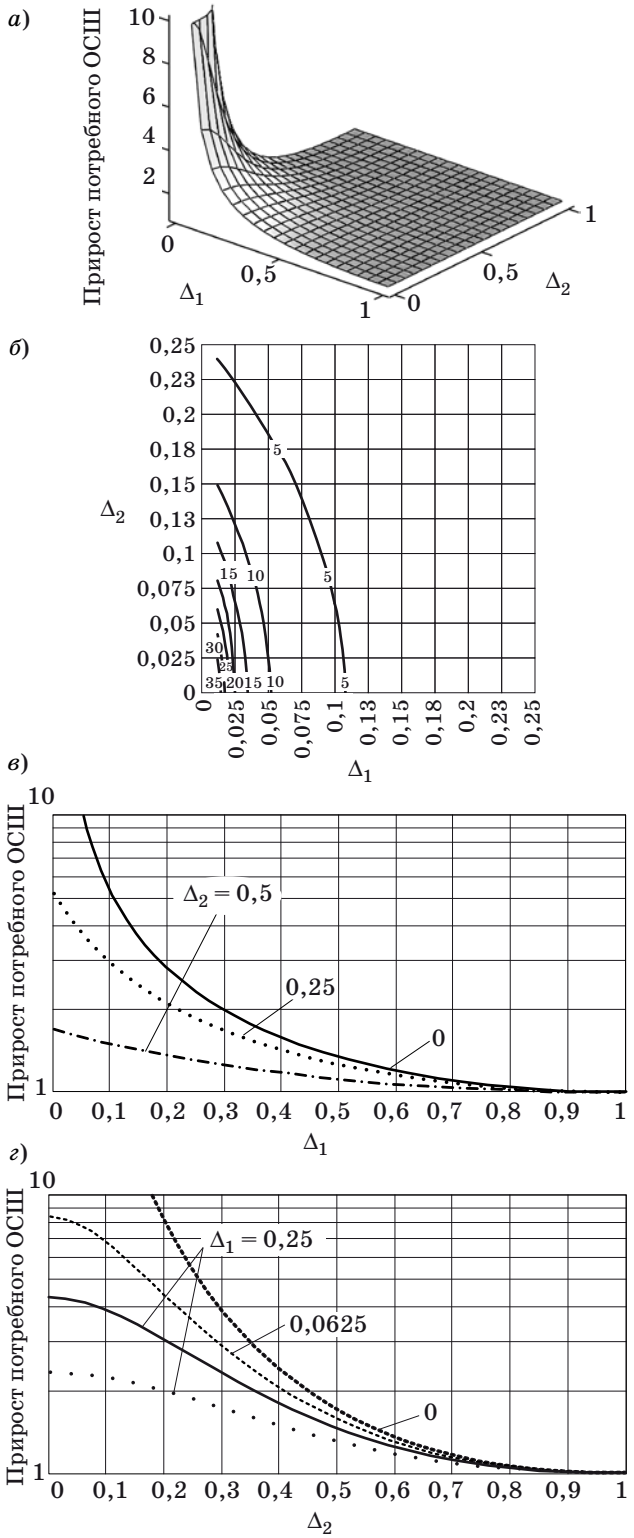
$$\Phi = |\mathbf{Q}|^{-1} = |\mathbf{V}|. \qquad (2)$$

Из выражения (2) непосредственно вытекает важнейшее теоретическое положение, определяющее потенциальную устойчивость проекционного решения обратной задачи группового рассеяния: *квадрат объема эллипсоида рассеяния проекционной оценки вектора коэффициентов отражения отдельных рассеивающих элементов не зависит от самих коэффициентов и равен значению функции неопределенностей.*

Рассчитанные в соответствии с (1) для рассматриваемой функции рассогласования графические зависимости (рис. 1, *а*) определяют прирост отношения сигнал/шум (ОСШ) по эхо-сигналам отдельных рассеивателей из состава парного, потребного для их обнаружения с заданными показателями эффективности относительно ситуации обнаружения одиночного рассеивателя. Для удобства анализа на рис. 1, *б—г* показано топографическое изображение, а также вертикальные сечения диаграммы рис. 1, *а*.

Анализ приведенных зависимостей позволяет сделать следующие выводы.

Области, где требуется существенный (более 5–10 раз) прирост потребного для обнаружения отдельных рассеивателей ОСШ, представляют собой оживал с осями симметрии Δ_1 и Δ_2 (см. рис. 1, *а*, *б*). Оживал, соответствующий более чем пятикратному приросту ОСШ, имеет поперечные размеры порядка 0,1 и 0,25 вдоль осей Δ_1 и Δ_2 (см. рис. 1, *б*). Оживал, соответствующий более чем десятикратному приросту ОСШ, имеет поперечные размеры порядка 0,05 и 0,15 вдоль осей Δ_1 и Δ_2 (см. рис. 1, *б*).



■ ***Рис. 1.*** *Прирост ОСШ, потребного для обнаружения отдельных рассеивателей из состава парного, для* $\rho(\Delta_1, \Delta_2) = \text{triang}\,\Delta_1 \,\text{sinc}\,\Delta_2$: *а — рассчитанные графические зависимости; б — топографическая диаграмма; в — вертикальные сечения двумерной диаграммы вдоль оси* Δ_1; *г — вертикальные сечения двумерной диаграммы вдоль оси* Δ_2

Указанные поперечные размеры оживала, естественно, равны аналогичным интервалам в соответствующих одномерных случаях. Однако особенность двумерной ситуации заключается в существовании достаточно значительных областей, где удаления отдельных рассеивателей по параметрам Δ_1 и Δ_2 меньше указанных поперечников, а потребный прирост в ОСШ не превышает указанных значений. Например, если удаление отдельных рассеивателей по параметру Δ_1 равно 0,05, а по параметру Δ_2 — 0,2 (см. рис. 1, *б*), то потребный энергетический прирост не превышает 5 раз для двумерного случая, хотя для одномерных ситуаций по отдельности потребности в энергетике возрастают десятикратно (см. рис. 1, *в*, *г*).

Анализ сечений (см. рис. 1, *в*, *г*) также показывает, что для рассматриваемой функции рассогласования сдвиги в положениях отдельных рассеивателей по параметру Δ_1 приводят к более существенному падению энергетических требований, чем сдвиги по параметру Δ_2, поэтому эквиэнергетические оживалы (см. рис. 1, *б*) более вытянуты вдоль оси Δ_2. Причины те же, что и причины более высокой эффективности одномерного разрешения при функции рассогласования $\rho(\Delta_1) = \text{triang}\ \Delta_1$ по сравнению с ситуацией $\rho(\Delta_2) = \text{sinc}\ \Delta_2$, а именно — более высокие значения коэффициента рассогласования во втором случае при фиксированных сдвигах по параметру (см. рис. 1, *в*, *г*).

Вид анализируемой двумерной функции рассогласования (помимо частоты встречаемости и важности для практических приложений) намеренно выбран таким, чтобы факторизация этой функции по отдельным параметрам приводила к разным одномерным функциям рассогласования. Это подчеркивает неоднородность многомерного разрешения по разрешаемым параметрам.

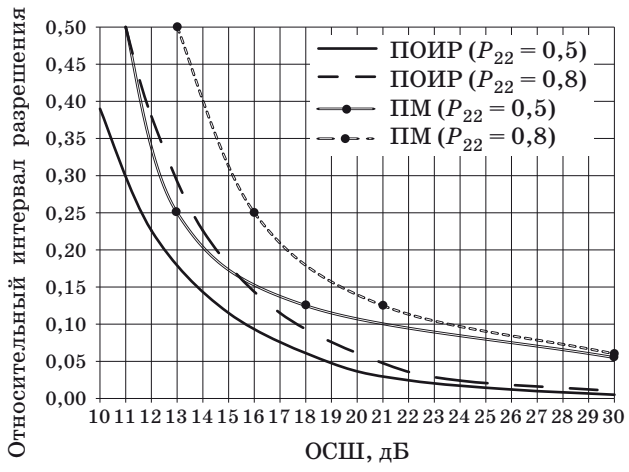
Оценка эффективности проекционного время-частотного разрешения с помощью имитационного математического моделирования

В качестве интегральной характеристики разрешающей способности радиолокатора может использоваться относительный интервал разрешения по какому-либо параметру. Под относительным интервалом разрешения понимается такое минимальное удаление между отдельными рассеивающими элементами (узлами сетки портрета), отнесенное к рэлеевскому пределу, при котором обеспечиваются требуемые показатели эффективности разрешения (далее — требуемые вероятности правильной оценки количества элементов группового рассеивателя при ограниченном сверху уровне ложных тревог).

Для выявления основных закономерностей многомерного разрешения из всего многообразия взаимных удалений рассеивателей по рассматриваемым параметрам удобно выбирать те ситуации, в которых сдвиги по отдельным параметрам равны (в рассматриваемом случае $\Delta_1 = \Delta_2 = \Delta$).

При таком подходе, например, можно графически отобразить одномерную зависимость интервала разрешения от ОСШ (более удобную для графического анализа в сравнении с двумерной). При этом под интервалом разрешения, по аналогии с одномерными ситуациями, понимается такое минимальное Δ, при котором достигаются заданные показатели эффективности разрешения (в частности, вероятности правильной оценки количества отдельных рассеивателей).

Рассчитанные аналитически (1) потенциально достижимые значения относительного интервала разрешения (ПОИР), а также оценки достигаемого с помощью проекционного метода (ПМ) относительного интервала разрешения, полученные с помощью имитационного математического моделирования [3], представлены на рис. 2. Моделирование соответствовало ситуации полной априорной неопределенности о положении отдельных рассеивающих элементов в составе парного. Амплитудные множители отдельных рассеивателей фиксированы и равны, взаимные фазы — случайны. ОСШ вычислялось по каждому рассеивателю. Полная априорная неопределенность процесса обработки нарушалась заданием внутренних отражающих границ для детальности пробной сетки по параметрам Δ_1 и Δ_2 (по параметру Δ_1 значение отражающей гра-



■ ***Рис. 2.*** *Относительные интервалы разрешения парного рассеивателя для функции рассогласования вида* $\rho(\Delta_1, \Delta_2) = \text{triang}\ \Delta_1\ \text{sinc}\ \Delta_2$ *при заданных вероятностях* P_{22} *правильной оценки количественного состава парного рассеивателя и вероятности ложной тревоги* $F = 0{,}05$

ницы принималось равным 0,125, по параметру Δ_2 — 0,5).

Результаты моделирования для рассматриваемого случая подтвердили как адекватность приведенных аналитических оценок, так и сравнительно высокую, приближающуюся к потенциально возможной, разрешающую способность проекционного радиолокатора.

Полунатурные экспериментальные исследования эффективности проекционного время-частотного разрешения

Для подтверждения возможности и эффективности проекционного время-частотного разрешения групповых рассеивателей в радиолокаторах с квазинепрерывным излучением (КНИ) и высокой частотой повторения (ВЧП) импульсов были проведены полунатурные эксперименты (функциональная схема экспериментальной установки показана на рис. 3).

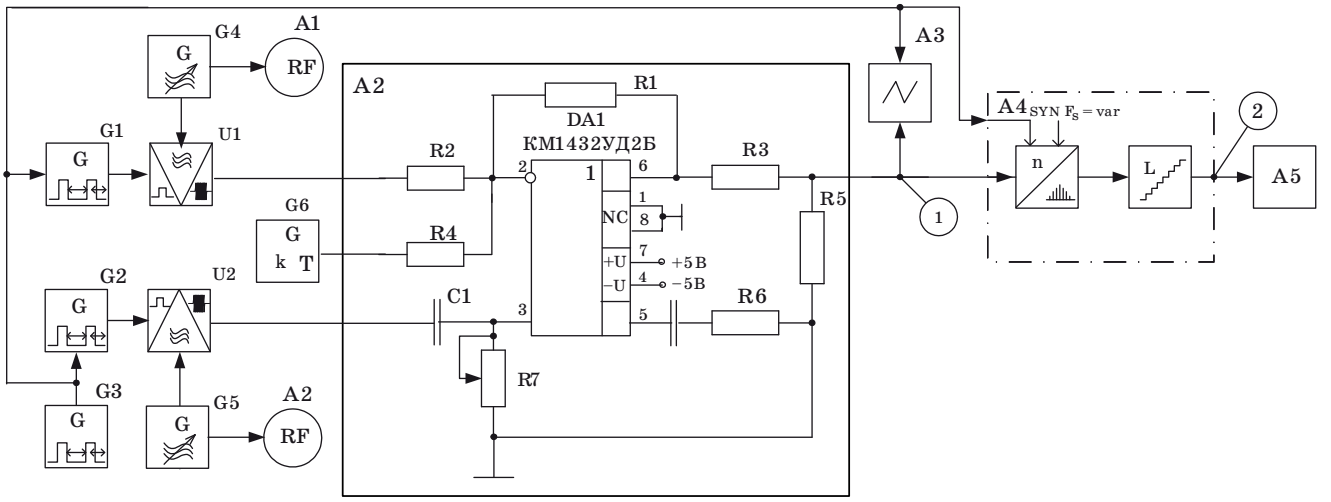
Генераторы высокочастотных сигналов *G*4, *G*5 формируют непрерывные гармонические колебания в диапазоне единиц—десятков мегагерц, поступающие одновременно на сигнальные входы импульсных модуляторов *U*1, *U*2. Контроль требуемой частоты сигналов осуществляется электронно-счетными частотомерами *A*1, *A*2.

На управляющие входы импульсных модуляторов подаются сигналы с генераторов импульсов *G*1, *G*2. Синхронизация всех элементов устройства осуществляется от генератора импульсов *G*3, синхроимпульсы с которого поступают также на осциллограф *A*4 и плату аналого-цифрового преобразователя (АЦП) *A*5. Для обеспечения задержки колебаний друг относительно друга и синхроимпульса генераторы *G*1, *G*2, *G*3 работают в режиме внешней синхронизации. Сформированные на выходах модуляторов прямоугольные радиоимпульсы подаются на вход сумматора *A*3. На него также поступает сигнал с генератора сигналов *G*6, используемого в качестве источника шумового напряжения (в собранной установке имеется также возможность регулировать ОСШ программно: подмешиванием к оцифрованному эхо-сигналу цифрового шума требуемой мощности). В сумматоре *A*3, выполненном на базе операционного усилителя (ОУ) в инвертирующем включении, осуществляется синфазное суммирование колебаний и образование аддитивной смеси сигнала с шумом. В режиме противофазного суммирования когерентных колебаний, в отличие от предыдущего случая, суммирование сигналов с выходов импульсных модуляторов *U*1, *U*2 осуществляется по обоим входам ОУ — так называемое параллельное суммирование. При использовании обоих входов ОУ сигналы имеют одинаковые по величине, но разные по знаку коэффициенты передачи.

Суммарный сигнал подается одновременно на осциллограф *A*4 (контрольная точка № 1) и плату АЦП *A*5. С выхода АЦП (контрольная точка № 2) цифровой сигнал подвергается обработке в соответствии с требуемым алгоритмом разрешения.

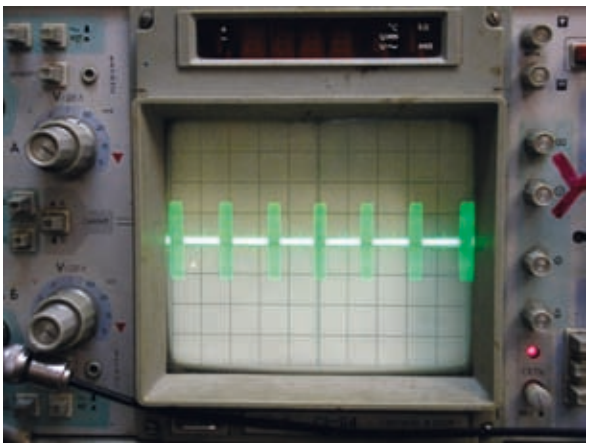
Вариант формирования сигналов для проведения полунатурного эксперимента по оценке разрешающей способности по радиальным дальности и скорости представлен на рис. 4, *а*, *б*.

Таким образом, сформированная на промежуточной частоте модель эхо-сигнала оцифро-

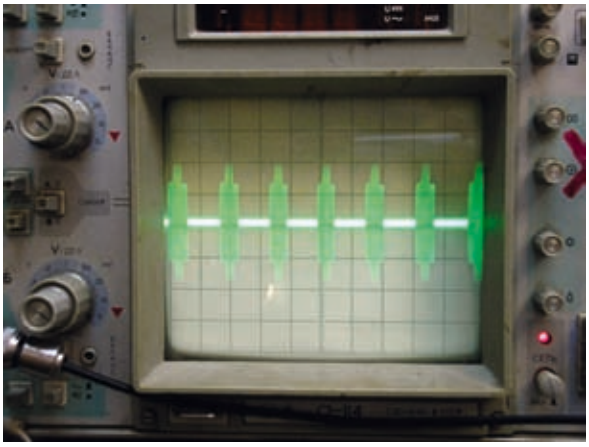


■ ***Рис. 3.*** *Функциональная схема полунатурной модели групповой цели*: *A1, A2 — частотомеры электронно-счетные Ч3-53*; *A3 — усилитель суммирующий*; *A4 — осциллограф С1-23*; *A5 — плата АЦП ADMDDC2WB-L и модуль синтезатора частоты ADMDDS9852A*; *A6 — персональная ЭВМ*; *G1—G3 — генераторы импульсов Г5-63*; *G4, G5 — генераторы сигналов высокочастотные Г4-176*; *G6 — генератор шума*; *U1, U2 — модуляторы*

а)



б)



■ ***Рис. 4.*** *Осциллограммы напряжений в контрольной точке № 1 при отсутствии шума: а — одиночный ВЧП-КНИ; б — два сигнала ВЧП-КНИ*

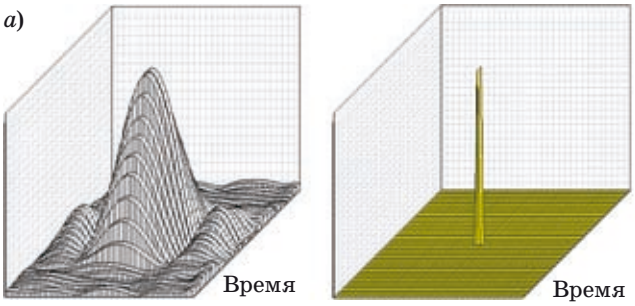
вывалась с помощью субмодуля цифрового приема ADMDDC2WB-L и поступала на обработку в ПЭВМ. В состав субмодуля ADMDDC2WB-L входит аналого-цифровой преобразователь и преобразователь дискретных отсчетов сигнала в отсчеты квадратурных составляющих комплексной огибающей (КО) эхо-сигнала DDC AD6620. Основные технические характеристики экспериментальной установки приведены в таблице.

Отдельные результаты полунатурного эксперимента показаны на рис. 5, *а*, *б*. В целом результаты обработки полунатурных моделей эхо-сигналов как одиночного, так и парного рассеивателей подтвердили приведенные выше аналитические оценки потенциальных возможностей проекционного метода разрешения (см. рис. 1). Так, доказана существенно более высокая эффективность проекционного разрешения по сравнению со стандартной корреляционно-фильтровой обработкой. При типовых ОСШ (13–20 дБ) наблюдалось радикальное превышение рэлеевского предела (от 4 до 10 раз), при этом оценки положений отдельных рассеивателей на плоскости «время-частота» с высокой степенью точности соответствовали их истинным параметрам.

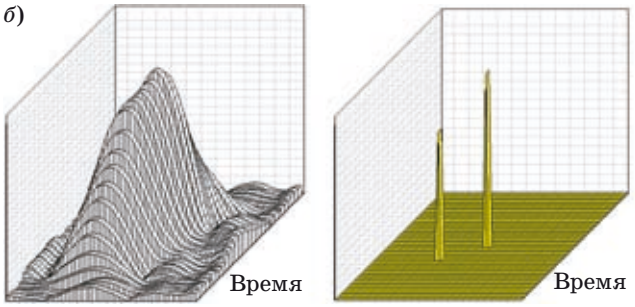
■ *Основные технические характеристики экспериментальной установки*

Параметр	Значение
Длительность импульса в когерентной пачке, мкс	10
Период следования импульсов в когерентной пачке, мкс	40
Значение промежуточной частоты, МГц	24
Количество импульсов в когерентной пачке	32
Частота отсчетов квадратурных составляющих КО эхо-сигнала с выхода DDC AD6620, МГц	2
Количество разрядов АЦП на отсчет квадратурной составляющей КО эхо-сигнала	14

а)



б)



■ ***Рис. 5.*** *Результаты обработки полунатурной модели эхо-сигнала одиночного (а) и парного (б) рассеивателей (на рис. б относительное отстояние рассеивателей порядка 0,25): слева — стандартная корреляционно-фильтровая обработка; справа — проекционное разрешение*

Заключение

Проекционные процедуры двумерного (многомерного) разрешения, т. е. разрешения по нескольким параметрам, характеризуются более

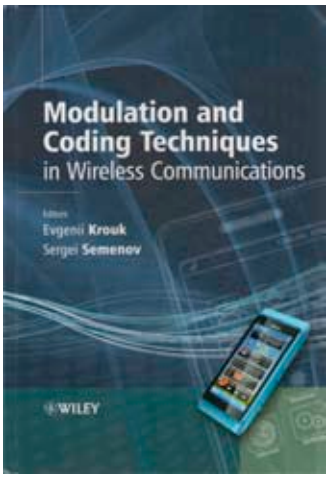
низкими требованиями к ОСШ по сравнению с одномерными процедурами [1]. Так, нередки ситуации, когда эхо-сигналы отдельных рассеивателей имеют такие частотные и временные сдвиги, при которых затруднительно их одномерное разрешение либо по времени, либо по частоте. При этом двумерное время-частотное разрешение возможно при несущественном повышении требований к ОСШ по сравнению с задачей обнаружения одиночного рассеивателя.

Еще более перспективным, особенно при увеличении длительности интервала когерентного накопления, представляется трехмерное разрешение: кроме анализируемых выше параметров к ним добавляется также и производная частоты эхо-сигнала, соответствующая случаю наличия радиальных ускорений у отдельных рассеивателей.

Исследования проводились при поддержке гранта президента Российской Федерации (№ МК-32.2009.10).

Литература

1. **Чижов А. А.** Аналитическая оценка эффективности разрешения групповых целей проекционными методами // Информационно-управляющие системы. 2009. № 6 (43). С. 12–17.
2. **Вудворд Ф. М.** Теория вероятностей и теория информации с применениями в радиолокации. — М.: Сов. радио, 1955. — 128 с.
3. **Чижов А. А., Тараканов А. В.** Цифровая модель первичной обработки сигналов в РЛС типа 9С32: Свидетельство об отраслевой регистрации разработки № 12335 / ФГНУ «Государственный координационный центр информационных технологий», 2009.



Krouk Evgenii, Semenov Sergei

Modulation and Coding Techniques in Wireless Communications. — UK.: John Wiley & Sons Ltd., 2011. — 680 p.: il. ISBN-978-0-4709-7677-7

Большое количество технических деталей, содержащихся в спецификациях стандартов, затрудняет определение взаимосвязи между стандартами и теоретическими результатами. Эта книга имеет целью охватить обе эти области, объясняя текущие и перспективные направления теории связи и показывая, как эти результаты используются в современных стандартах беспроводной связи.

Книга разделена на два основных раздела, описывающих методы модуляции, кодирования и множественного доступа. Вначале излагаются основы теории кодирования и модуляции, затем указывается, как эти концепции определяются и реализуются в современных системах беспроводной связи. Первый раздел посвящен основным процедурам и методам физического уровня сети, включая модуляцию, кодирование, выравнивание канала и множественный доступ. Во втором разделе рассматривается использование этих процедур и методов в широком диапазоне стандартов беспроводной связи, включая WLAN, WiMax, WCDMA, HSPA, LTE и cdma2000.

Книгу можно приобрести на сайте издательства Wiley: http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470745053.html

УДК 004.932.72'1

К ВОПРОСУ О ПОСТРОЕНИИ СИСТЕМЫ РАСПОЗНАВАНИЯ И ПОДСЧЕТА ЖИВОТНЫХ НА АЭРОФОТОСНИМКАХ
Часть 1: Анализ методов распознавания

В. В. Михайлов,
доктор техн. наук, ведущий научный сотрудник
Санкт-Петербургский институт информатики и автоматизации РАН
Я. В. Харин,
аспирант
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Рассматриваются основные принципы и этапы построения системы подсчета и распознавания объектов на фотографиях. Проводится обзор методов сегментации изображений и распознавания. Разбираются их существенные достоинства и недостатки для решения задачи подсчета количества животных.

Ключевые слова *— распознавание, сегментация, подсчет объектов.*

Введение

В настоящее время задача автоматического распознавания и подсчета объектов является актуальной и востребованной. Ее решение способно автоматизировать труд человека и повысить производительность. Видеонаблюдение, регулирование движения транспорта, контроль качества деталей на конвейере, оценка численности животных — вот далеко не полный перечень областей человеческой деятельности, где необходимо решение данной задачи. Следует заметить, что создание каждой системы требует учета особенностей объектов распознавания, а также особенностей фотоснимков либо видеоряда для обоснованного выбора методов распознавания.

В настоящей статье рассматриваются основные принципы построения компьютерной системы распознавания и подсчета для определения количества животных на аэрофотоснимках. Приводятся результаты качественного анализа методов, подходящих для решения поставленной задачи. Конкретным объектом при построении прототипа системы выбраны дикие северные олени.

Материалы и методы

Северные олени являются важнейшей компонентой полярных экосистем, основным источником питания, благосостояния и этнической самобытности коренных народов Севера. Величина допустимого промыслового изъятия диких северных оленей рассчитывается на основе данных авиаучетов о численности и половозрастном составе популяции. Основные группировки оленей фотографируются во время их скоплений на летних пастбищах, и количество животных в них подсчитывается. Ручная обработка снимков при численности популяции 500–600 тыс. особей занимает около 3 мес. Для определения квоты к началу промыслового сезона время обработки снимков должно быть снижено до 10–15 дней. Автоматизация процесса обработки фотоснимков позволит, таким образом, решить две задачи: освободить специалистов от выполнения рутинной работы и повысить качество функционирования промысловой системы. При съемке олени находятся на различном удалении от камеры, поэтому их изображения на снимках будут видны под различными углами (от 45 до 90°), изображения будут иметь различные размеры и могут перекрывать друг друга. Помехи: камни, земляные бугры, впадины и т. п. — легко идентифицируются при ручной обработке снимков, но могут создать трудности при работе автоматической системы распознавания.

Система распознавания и подсчета животных должна решать следующие задачи.

1. Распознавать и подсчитывать общее число животных на снимках. При этом животные могут быть представлены как локальными объекта-

ми, так и неразделимыми группами. Неоднородный по цвету и фактуре природный фон может содержать помехи — камни, овраги и т. д.

2. Распознавать и подсчитывать количество животных, имеющих визуально различимые признаки. Для северных оленей — это телята и взрослые самцы. Условия распознавания по фону и помехам соответствуют п. 1.

В качестве первичной информации при разработке системы использованы фотоснимки групп и скоплений животных, сделанные во время авиаучетов диких северных оленей на Таймыре в 2000, 2003 и 2009 гг. Кроме того, для получения количественных оценок правильности распознавания использовались автоматически сгенерированные изображения стад животных.

Необходимо ввести ряд понятий и определений. Под *объектами* понимаются некоторые сущности, запечатленные на снимке, подлежащие подсчету. *Класс объектов* — некоторая совокупность объектов, называемых *элементами класса*, обладающих рядом близких свойств. Измеряемые или вычисляемые *свойства объектов*, позволяющие отличить классы друг от друга, называются *признаками*.

В общем случае в решении задачи подсчета объектов можно выделить следующие этапы [1]: предобработка снимков, сегментация, шумоподавление и фильтрация, отнесение сегментированных областей к классам объектов, дополнительная обработка некоторых классов объектов, подсчет количества найденных объектов.

Предобработка

Первый этап необходим для подготовки изображения к распознаванию. На этом этапе производится отчистка изображений от помех и шумов. Под помехами и шумами понимаются сторонние возмущения, неселективные в отношении объектов и фона, действующие в системах создания, передачи и воспроизведения фотоснимков. Например, некоторые помехи могут быть результатом дефектных пикселей на матрице цифрового фотоаппарата или возникать в результате аппаратной дискретизации и квантования. При удалении помех важно выбрать такой способ очистки изображения, чтобы он не вызвал значительных искажений изображения, сохраняя объекты распознавания. В качестве фильтров для удаления помех и шумов служат различного рода усредняющие, частотные и пространственные фильтры [1, 2].

На этом этапе может быть увеличена яркость, повышена четкость изображения, могут быть применены операции усреднения и выравнивания гистограмм яркости. Если это требуется на последующих этапах, возможно снижение дисперсии яркости пикселей с сохранением резких перепадов яркости. Выбор преобразований должен учитывать метод сегментации для сохранения признаков объектов. При необходимости может быть осуществлен переход из одной цветовой модели в другую. При выполнении сегментации по цветовым признакам бывает удобно преобразовать изображение в цветовую модель HSV.

Сегментация

Под сегментацией понимается процесс проверки каждого отдельного пикселя для того, чтобы выяснить, принадлежит ли он к интересующим объектам или нет. Результатом сегментирования изображения является бинарное изображение, в котором выделены области, обладающие признаками объектов в соответствии с критериями сегментации и признаками фона. Метод сегментации выбирается в зависимости от особенностей конкретной решаемой задачи.

Если объекты имеют четкие и стабильные границы, то, как правило, применяются методы выделения границ. Изображения рассматриваются как функция двух переменных, при этом производится поиск максимума градиента этой функции. Примерами таких методов служат фильтры Робертса, Кирша, Превита и Собеля. Главной проблемой этих методов является слабая устойчивость к помехам и шуму, поэтому их целесообразно применять, например, при сегментации объекта на монотонном фоне.

Если на изображении присутствуют стабильные различия в яркости (интегральной или спектральной) или различия в каком-либо другом значимом признаке отдельных областей, то целесообразно применять пороговые методы. Такие методы позволяют выделить области изображения, для которых значение выбранного параметра выше либо ниже определенного порога. Например, когда объект имеет яркость большую, чем остальная часть изображения, применение порогового фильтра даст хорошие результаты.

При наличии связности внутри отдельных сегментов применяются методы наращивания областей. Идея состоит в том, что выбираются стартовые точки, после чего производится анализ соседних с ними точек в соответствии с некоторым критерием однородности. Этим критерием, например, может служить яркость в некотором диапазоне [2]. Количество стартовых точек должно быть равно количеству однородных областей на изображении. Метод водоразделов является одним из эффективных способов практической реализации идеи наращивания областей. Он основан на поиске локальных минимумов с последующей группировкой вокруг них областей по связности.

Если связь между пикселями изображения в пространстве признаков задана в математиче-

ской форме, то для сегментации могут быть применены методы теории графов. Суть методов в следующем: изображение представляется в виде взвешенного графа, вершинами которого являются пиксели изображения. Вес ребра графа отражает близость точек в некотором пространстве признаков. Для снижения размерности, как правило, рассматриваются ребра графа, связывающие близлежащие пиксели. Затем производится решение задачи поиска минимальной стоимости разреза графа. Таким образом, изображение разбивается на однородные области, однородностью которых можно управлять, задавая вес ребра графа. Помимо однородности цвета и текстуры сегментов, можно управлять размером областей, их формой, сложностью и т. д.

Методы сегментации могут использоваться совместно, если это позволяет улучшить выделение искомых объектов на изображениях. Примером этому может служить совместная работа пороговых методов сегментации и методов наращивания областей. В этом случае пороговый метод может выделить яркостные минимумы изображения, а метод водораздела выделит весь объект, имеющий яркостный минимум.

Шумоподавление и фильтрация

Третий этап необходим для удаления помех, возникающих при сегментации. Для этого, как правило, используется обработка с помощью аппарата математической морфологии, поскольку изображение на данном этапе представляется бинарным [3, 4]. Может производиться дополнительная обработка сегментированного изображения, например операция сглаживания бинарных областей или удаление областей определенной формы.

Распознавание

Входными данными для распознавания объектов являются изображения, полученные в результате процессов сегментации и шумоподавления. Помимо этого, здесь могут использоваться любые изображения, полученные на предыдущих этапах, и исходное изображение.

Широкое распространение при обнаружении и распознавании получили корреляционные методы, работающие с объектами в пространстве изображений или с признаками объекта в пространстве признаков [5, 6]. При работе с объектами задается эталон объекта, после чего производится многошаговая корреляция. По сути, данный метод реализует полный перебор в пространстве изображений (пространстве сигналов).

Методы, основанные на пространстве признаков, обладают значительно меньшей размерностью по сравнению с пространством сигналов. Признаки могут сравниваться как с использованием порогов по величине сходства, так и без порога. При этом решение о принадлежности к тому или иному классу может приниматься на основе разнотипных признаков: метрических, статистических, логических, текстурных, структурно-лингвистических. При необходимости выполняется корреляционная обработка признаков, полученных от эталона и входного изображения.

Главной задачей при этом является выбор признаков. Набор признаков, используемых для распознавания объектов, должен удовлетворять следующим условиям:

— близости значений признака для объектов одного класса, существенное различие значений признака для объектов разных классов;

— набор признаков должен быть полным, т. е. в совокупности должен обеспечивать идентификацию объектов любого из классов;

— общее количество признаков должно быть минимальным.

Свойства природных объектов в значительной мере варьируют, объекты могут иметь разные размеры, изображения объектов могут перекрывать друг друга. На изображениях могут быть помехи, близкие по цветовой гамме и форме к искомым объектам. По этой причине можно говорить не о строгом распознавании, а о распознавании с некоторой вероятностью. При этом для уменьшения вероятности ошибок в минимальный набор могут вводиться добавочные, избыточные признаки.

Дополнительная обработка

Дополнительная обработка классов объектов после распознавания проводится для подготовки к последующим действиям над ними, которые требует решаемая задача. Например, на этом этапе может производиться оценка расстояния до распознанных объектов, проверка правильности распознавания пользователем или с помощью логических, синтаксических и прочих методов. Возможен итерационный возврат к предшествующим этапам обработки изображений и распознавания. Так, если были выявлены ошибки при распознавании, информация об этом может поступать на предшествующие этапы для их исправления [7].

Результаты анализа методов распознавания

Предобработка

На данном этапе в связи с необходимостью поиска признаков объектов был выбран медианный фильтр [2]. Выбранный фильтр показал лучшие результаты удаления помех по сравнению с линейными сглаживающими фильтрами, сохранив при этом четкость изображения.

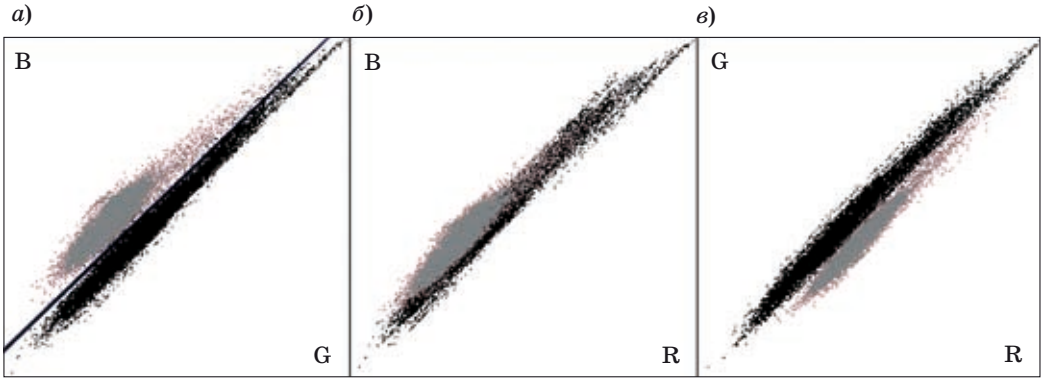
■ ***Рис. 1.*** *Удаление шумов с помощью медианного фильтра*: *слева — исходное изображение*; *справа — результат фильтрации*

При использовании медианного фильтра важно определить размер окна фильтра. Если окно имеет слишком большой размер, то происходит снижение четкости изображения объектов. При оптимальном размере окна фильтр удаляет мелкие шумы и помехи, не снижая в общем четкости изображения. Практическим путем было установлено, что для удаления помех на представленных снимках размер окна должен составлять 0,1–0,5 от среднего размера объекта. Пример работы медианного фильтра показан на рис. 1. Как видно из рисунка, практически все мелкие аддитивные помехи в результате фильтрации со снимка удалены.

Сегментация

Поскольку объекты распознавания находятся на неоднородном фоне и имеют разные оттенки цвета, то методы выделения границ не смогут дать хороший результат. Распознаваемые объекты, как правило, контрастируют на зеленом фоне. В связи с этим был выбран пороговый метод сегментации. В качестве порога используется отношение спектральной яркости одной составляющей цвета к другой. Для отбора спектральной пары был проделан эксперимент, в котором использовались участки изображений объектов и фона, полученных из аэрофотоснимков. При проведении эксперимента были взяты фрагменты всех имеющихся в наличии типов фотографий. Другими словами, из множества снимков были перенесены объекты на одно изображение. На другое изображение были помещены фоновые цвета снимков. После чего оба изображения подверглись анализу: каждому пикселю изображения объектов и фона была поставлена в соответствие точка на координатной плоскости. Координатами точки являются значения яркости составляющих цвета. В результате получены три графика скоплений точек, соответствующих различным спектральным парам (рис. 2). Черные точки на графиках соответствуют пикселям фона, серые — пикселям объектов.

Видно, что скопления точек на рис. 2, *а* не перекрывают друг друга, в отличие от рис. 2, *б* и *в*. Именно эта спектральная пара была использована нами для отделения объектов от фона. Для решения задачи сегментации проведем прямую, разграничивающую скопления точек. Преобразовав уравнение прямой в неравенство, можно выделить либо только верхнее скопление точек, либо только нижнее. На изображении будут выделяться пиксели объекта или фона в зависимо-



■ ***Рис. 2.*** *Цветовые зависимости фона и объектов распознавания*: *а — для зеленой и голубой компонент цвета*; *б — для красной и голубой, в — для красной и зеленой*

сти от поставленного в неравенстве знака. Коэффициенты уравнения прямой были рассчитаны из условия минимума суммы точек, попадающих в чужую область. При этом вероятность ошибочного отнесения области изображения фона к объекту составила около 2 %, тогда как вероятность ошибочного отнесения области изображения объекта к фону — 0,001 %. Приведенные числа являются результатом эксперимента на эталонных изображениях, по которым производился поиск порога. При сегментации других изображений вероятность ошибки может существенно возрасти. Помимо этого, при вычислениях не учитывалась возможность наличия на изображении предметов, например камней, похожих по цветовым характеристикам на животных.

Результат сегментации изображения пороговым методом представлен на рис. 3. Выбранный метод устойчив к сложным формам объектов, которые возникают в результате наложения изображений единичных объектов друг на друга.

Использованный нами алгоритм сегментации позволяет выделять объекты любой формы и обладает высоким быстродействием благодаря простому методу проверки принадлежности пикселя к объекту. Однако, как можно заметить на рис. 3, некоторые участки изображения были ошибочно сегментированы.

Были опробованы методы теории графов. Вначале был применен метод сегментации SWA (*Segmentation by Weighted Aggregation*) [8]. Его суть состоит в построении пирамиды взвешенных графов, где каждый верхний слой получен из нижнего путем объединения вершин графа, вес ребер между которыми минимален. В качестве параметра веса ребра графа была взята разница пикселей в цветовом пространстве. Результаты работы метода представлены на рис. 4.

Получившееся изображение можно обработать пороговым фильтром, чтобы привести его к бинарному виду (рис. 5).

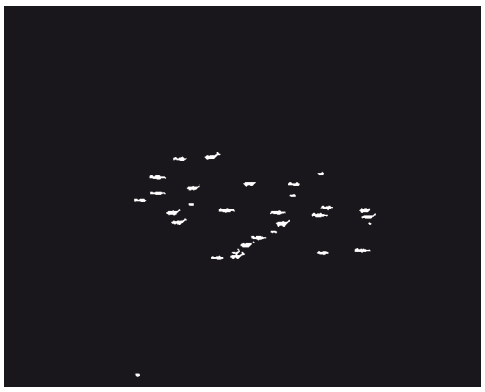
Этот алгоритм сегментации выделил только объекты. Его достоинством является высокая надежность. К недостаткам можно отнести сложность вычислений, что негативно сказывается на быстродействии системы.

При наличии двух бинарных изображений появляется возможность учитывать результаты каждого из способов совместно. Например, можно применить операцию логического «И» для двух изображений и получить одно, являющееся результатом работы обоих методов (рис. 6).

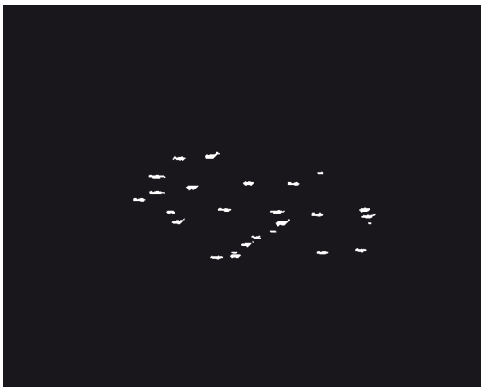
При совмещении методов увеличивается общее количество операций, а значит, ухудшается быстродействие системы. Одновременно с этим, когда применяется несколько методов сегмента-

■ ***Рис. 3.*** *Результаты сегментации изображения пороговым методом: сверху — исходное изображение; снизу — сегментированное*

■ ***Рис. 4.*** *Результаты применения алгоритма SWA: сверху — до обработки; снизу — после обработки*



■ ***Рис. 5.*** *Результат работы порогового фильтра после применения сегментации методом SWA*



■ ***Рис. 6.*** *Логическое сложение результатов пороговой сегментации и сегментации с помощью метода SWA*

ции, использующих различные признаки объекта, общая вероятность ошибки значительно снижается. В рассматриваемом случае время выполнения сегментации увеличивается незначительно. Это связано с небольшим количеством операций для выполнения порогового метода сегментации. Кроме того, оба метода дополняют друг друга, так как используют различные признаки объектов. Метод SWA основан на связности пикселей. Пороговый метод использует цветовые характеристики объектов. При ошибочной сегментации области изображения одним методом второй метод исправит ошибку первого. Таким образом, при совмещении двух методов получен значительный выигрыш в надежности системы при незначительном уменьшении ее быстродействия. Использование комбинации этих методов является хорошим решением для снижения погрешности распознавания. После объединения результатов двух методов уменьшилось также количество контуров, перекрывающих друг друга.

Для оценки погрешности системы сегментации был проведен эксперимент на автоматически сгенерированных изображениях стад [9]. При генерации использовался реальный, но одинаковый для всех изображений фон и фигурки животных с естественными цветовыми характеристиками. Число объектов на таких изображениях известно заранее. В результате проведения этого теста на 91 изображении стад было установлено, что погрешность подсчета с применением описанной системы составляет около 8 % при относительно небольшой дисперсии, равной 1,02. При вычитании из данной погрешности доли ошибок, связанных с наложением объектов друг на друга, погрешность составляет 3 %.

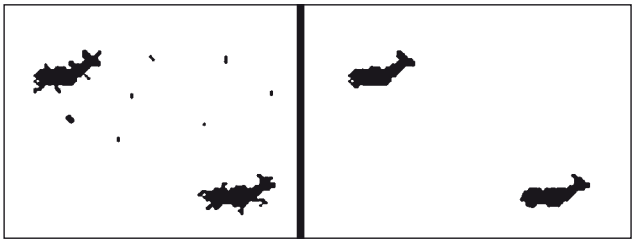
Шумоподавление и фильтрация

На этом этапе в описываемой системе производится сглаживание сегментированных областей и удаление мелких помех. Необходимость сглаживания вызвана тем, что границы объекта после применения сегментации могут быть крайне неровными, вследствие чего может быть затруднен анализ сегментированных областей на последующих этапах. Сглаживание выполняется с помощью набора операций математической морфологии — операции эрозии и масштабного преобразования [5]. Такой подход, помимо сглаживания, удаляет мелкие помехи, которые, как правило, присутствуют в большом количестве после проведения сегментации пороговыми методами (рис. 7).

Как можно заметить, в результате сглаживания границы областей стали более ровными, удалены мелкие шумы. Степень сглаживания и размер удаляемых помех зависит от выбора размера окна, операций эрозии и масштабного преобразования. Эксперименты показали, что размер окна должен составлять около 10 % от среднего размера объекта.

Распознавание

Для распознавания северных оленей на аэрофотоснимках были выбраны признаковые методы. Эти методы позволяют решить поставленную задачу в условиях, когда животные на снимках находятся под разным освещением, в разных позах, имеют разный размер, цвет. Другими словами, объекты имеют множество эталонов, определить каждый из которых не представляется воз-



■ ***Рис. 7.*** *Сглаживание изображения после сегментации: слева — до сглаживания; справа — после сглаживания*

можным, что является причиной отказа от корреляционных методов.

Было выделено 3 класса объектов: одиночные животные; животные, перекрывающие друг друга; прочие объекты. В качестве признаков выбраны форма сегментированной области, ее площадь, вытянутость.

Вытянутость области определяется двумя параметрами: протяженностью области по осям X и Y. Вычисляются эти параметры путем нахождения разности между максимальными значениями координат, принадлежащих области, и минимальными. Площадь соответствует количеству пикселей в области. О форме области можно судить по такому параметру, как округлость, которая определяется соотношением

$$c = \frac{p^2}{S},$$

где p — периметр области; S — площадь области.

Округлость области является безразмерной величиной. Если область является окружностью, то тогда округлость принимает минимальное значение $4\pi = 12{,}57$. Для квадрата это значение равно 16. Как правило, округлость стремится к большим значениям для вытянутых объектов.

Затем были определены пороговые параметры для каждого класса статистическим методом. Некоторые параметры, такие как округлость сегментированной области, имеют постоянное пороговое значение на всех изображениях, другие, такие как площадь, требуют адаптивного подхода на каждом изображении в связи с различным масштабом объектов. Для объекта, находящегося в отдалении от других, параметр округлости лежит в диапазоне от 14 до 35. Округлость области сегментированного изображения, соответствующая скоплению животных, лежит в диапазоне от 35 до 300. Области, имеющие значение округлости более 300, как правило, являются крупными помехами. Пороговые значения других параметров, соответствующие определенному классу, можно вычислить при обработке фотографий дискретного масштаба. Достичь этого можно, производя фотосъемку с определенной высоты. Например, значение площади области в пикселях, соответствующее одному животному, лежит в диапазоне от 75 до 200 при условии, что съемка была произведена на высоте 500 м. Группировка, состоящая из нескольких животных, может иметь размер на сегментированном изображении до 1600 пикселей. Области площадью более 2000 пикселей, как правило, являются крупными помехами.

Заключение

Анализ методов сегментации и распознавания объектов подтвердил принципиальную возможность автоматического распознавания и подсчета диких северных оленей на фоне летней тундры по реальным аэрофотоснимкам. Примененные методы показали весьма хорошие результаты при подсчете изображений животных на «простых» снимках (зеленый фон, отсутствие помех).

Однако были выявлены и недостатки методов, требующие доработки. При смене цветового баланса снимка результаты сегментации могут оказаться неудовлетворительными. Кроме того, темные участки на снимке (овраги, ущелья и т. п.) при выбранном методе сегментации идентифицируются как объекты, их надо выявлять на этапе шумоподавления и фильтрации. Для распознавания и подсчета объектов в скоплениях кроме геометрических характеристик должны быть использованы цветовые особенности окраски животных. Решению этих задач будет посвящена дальнейшая работа.

Литература

1. **Ерош И. Л., Сергеев М. Б., Соловьев Н. В.** Обработка и распознавание изображений в системах превентивной безопасности: учеб. пособие / СПбГУАП. — СПб., 2005. — 154 с.
2. **Гонсалес Р., Вудс Р.** Цифровая обработка изображений. — М.: Техносфера, 2005. — 1072 с.
3. **Фурман Я. А., Юрьев А. Н., Яншин В. В.** Цифровые методы обработки и распознавания бинарных изображений / КрасГУ. — Красноярск, 1992. — 248 с.
4. http://www.rusnauka.com/23_D_2009/Informatica/49967.doc.htm (дата обращения: 15.10.2010).
5. **Яне Б.** Цифровая обработка изображений. — М.: Техносфера, 2007. — 584 с.
6. http://www.ci.ru/inform06_06/p_24.htm (дата обращения: 17.10.2010).
7. **Форсайт Д., Понс Ж.** Компьютерное зрение. Современный подход. — М.: Вильямс, 2004. — 928 с.
8. http://cgm.computergraphics.ru/content/view/147 (дата обращения: 21.10.2010).
9. **Михайлов В. В., Карташев Н. К.** DEER COUNTER — программа-тренажер для выработки навыка визуальной оценки количества животных в группировке // Биологические ресурсы Крайнего Севера: перспективы охраны и рационального использования. — СПб.: ГУАП, 2010. С. 205–212.

УДК 004.8:681.3.06

О ВОЗМОЖНОСТИ ПОВЫШЕНИЯ КАЧЕСТВА МНОГОМЕРНЫХ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ТЕХНОЛОГИЧЕСКОЙ ИНФОРМАЦИИ, СОБИРАЕМОЙ НА ТЭС

С. В. Поршнев,
доктор техн. наук, профессор
И. В. Соломаха,
аспирант
Уральский федеральный университет имени первого Президента России Б. Н. Ельцина

Предложено для описания связей между технологическими показателями, собираемыми информационной системой тепловой электрической станции, использовать нелинейные математические модели, создаваемые на основе метода группового учета аргументов. Приведены результаты сравнительного анализа качества аппроксимации изучаемых зависимостей при использовании линейных и нелинейных математических моделей, свидетельствующие о целесообразности применения последних для описания связей между технологическими показателями.

Ключевые слова *— тепловая электрическая станция, информационная система, технологическая информация, технологический показатель, факторный анализ, метод группового учета аргументов.*

Введение

Теория управления, а также практический опыт организации функционирования сложных технических объектов показывают, что с возрастанием масштабов этих объектов существенно возрастают роль и значение информационных систем, основной задачей которых является обеспечение учета и управление функционированием объектов на основе сбора, обработки и представления информации о фактических показателях производственной и финансовой деятельности предприятия. Осуществление оперативного контроля над производственной деятельностью, анализ текущей производственной ситуации, принятие управленческих решений — все эти функции сводятся, в конечном итоге, к работе с информацией. И от того, насколько эта информация своевременна, достоверна и полна, зависит конечный успех деятельности всего предприятия. Таким образом, информация превратилась сегодня в ключевой ресурс повышения эффективности деятельности предприятия.

Вышесказанное в полной мере относится и к предприятиям электроэнергетической отрасли, в частности тепловым электрическим станциям (ТЭС). Например, на Сургутской ГРЭС-1 с 2003 г. функционирует информационная система, с помощью которой осуществляются сбор, анализ и хранение технологической информации, в том числе значения технологических показателей энергоблоков станции, характеризующих текущий режим работы станции. В то же время проведенный анализ показал, что эффективность использования полученной информации, в том числе ее роль в принятии управленческих решений руководством ТЭС, недостаточна. Следует отметить, что данная ситуация характерна не только для Сургутской ГРЭС-1, но и для предприятий других отраслей промышленности, например газотранспортной [1]. В этой связи разработка методов анализа технологической информации представляется весьма актуальной.

Многомерные математические модели

Одним из возможных направлений исследований является разработка математических моделей блоков ТЭС, позволяющих описывать связь между показателями. Подобные математические модели дают возможность прогнозировать значения выбранного (зависимого) показателя при изменении значений одного или нескольких независимых показателей. Например, наличие мате-

матической модели, описывающей связь между выработкой электроэнергии блоком (зависимая переменная), отпуском тепла внешнему потребителю и температурой холодного воздуха на входе дутьевого вентилятора (независимые переменные), позволяет определить ожидаемое значение выработки электроэнергии блоком в условиях заданного отпуска тепла внешнему потребителю при прогнозируемом резком понижении температуры окружающей среды. Это, в свою очередь, дает возможность сформировать реальный план выработки и отпуска электроэнергии потребителю, в котором учтены изменения климатических условий, что представляется весьма актуальным в современных условиях балансирующего рынка электроэнергии.

В рамках выбранного направления исследований авторами проведен анализ технико-экономических показателей (ТЭП), собираемых и рассчитываемых в информационном комплексе Сургутской ГРЭС-1 [2]. На основе результатов анализа для последующего построения математических моделей, описывающих связи между ТЭП, выделена группа энергоблоков (станционный № 4–7), по которым в период с 2003 по 2006 г. собраны среднемесячные значения 46 ТЭП. При вы-

■ ***Таблица 1****. Состав выделенных факторов*

Множество	Показатель	Переменная	Единица измерения
{Фактор 1}	Выработка электроэнергии блоком	$x_{1,1}$	МВт/ч
	Выработка пара котлом	$x_{1,2}$	т
	Выработка тепла котлом	$x_{1,3}$	Гкал
	Выработка тепла котлом (уточненная)	$x_{1,4}$	Гкал
	Расход топлива на котел	$x_{1,5}$	т у. т.*
	Расход топлива на отпуск электроэнергии	$x_{1,6}$	т у. т.
	Расход воды на впрыск в промперегрев	$x_{1,7}$	т
	Расход питательной воды	$x_{1,8}$	т
	Расход электроэнергии на собственные нужды котла	$x_{1,9}$	МВт/ч
	Расчетный расход топлива на выработку электроэнергии	$x_{1,10}$	т
	Расход электроэнергии на собственные нужды турбины	$x_{1,11}$	МВт/ч
	Отпуск электроэнергии	$x_{1,12}$	МВт/ч
	Нормативный расход топлива на выработку электроэнергии	$x_{1,13}$	т у. т.
{Фактор 2}	Отпуск тепла внешнему потребителю	$x_{2,1}$	Гкал
	Расчетный расход топлива на выработку тепла	$x_{2,2}$	г/кВт · ч
	Нормативный расход топлива на выработку тепла	$x_{2,3}$	т у. т.
	Отпуск тепла из второго отбора сверх нужд регенерации	$x_{2,4}$	Гкал
	Невозврат конденсата от потребителя	$x_{2,5}$	т
	Отпуск тепла внешним потребителям с паром второго отбора	$x_{2,6}$	Гкал
	Удельный расход топлива на отпуск тепла	$x_{2,7}$	г/кВт · ч
	Расход электроэнергии на тепловую установку	$x_{2,8}$	МВт/ч
	Отпуск тепла внешнему потребителю	$x_{2,9}$	Гкал
{Фактор 3}	Температура охлажденной воды на входе в конденсатор	$x_{3,1}$	°С
	Номинальный относительный расход тепла на собственные нужды котла	$x_{3,2}$	%
	Температура холодного воздуха на входе дутьевого вентилятора	$x_{3,3}$	°С
	Температура уходящих газов после дымососа	$x_{3,4}$	°С
	Температура воздуха перед регенеративным воздухоподогревателем	$x_{3,5}$	°С
{Фактор 4}	Содержание кислорода в уходящих газах	$x_{4,1}$	%
	Давление пара холодного промперегрева	$x_{4,2}$	кгс/см^2
	Давление пара горячего промперегрева	$x_{4,3}$	кгс/см^2
	Температура питательной воды фактическая за подогревателями высокого давления	$x_{4,4}$	°С

* т у. т. — тонна условного топлива.

боре последних использовался критерий информативности, предложенный в работе [3].

Если принять, что число информативных признаков соответствует числу выделенных показателей, то обработка данных, включая задачи классификации, создания новой структуры признакового пространства и интерпретации, представляет определенные трудности. Как известно [4, 5], решение данных задач значительно упрощается, если подвергнуть размерность признакового пространства редукции. Такое сжатие в большинстве случаев оказывается возможным, поскольку на практике некоторые признаки оказываются коррелированными между собой и, следовательно, избыточны с точки зрения содержащейся в них информации. Сжатие сводится к преобразованию исходного 46-мерного пространства данных X в другое пространство Y, в котором можно выбрать подмножество латентных переменных меньшей размерности без существенной потери информации. Для уменьшения размерности задачи мы использовали метод главных компонент (ГК) [4, 5], состоящий в вычислении собственных значений корреляционной матрицы технологических параметров. Проведенный анализ позволил сделать вывод о том, что из 46 ТЭП наиболее значимыми оказываются всего 22 показателя, сгруппированные в 4 фактора (множества) (табл. 1).

Анализ результатов факторного исследования

Проведем анализ полученных результатов с технологической точки зрения. Из табл. 1 видно, что множество {Фактор 1} содержит показатели, определяемые выработкой электроэнергии энергоблоком. Учитывая, что анализируются ТЭП конденсационных энергоблоков, вырабатывающих в основном электроэнергию, можно объединить в один фактор следующий ряд показателей, имеющих с выработкой электроэнергии тесную функциональную связь: выработка пара и тепла котлом; расход топлива на котел и на отпуск электроэнергии; расход питательной воды и отпуск электроэнергии. Выработка пара котлом пропорциональна количеству вырабатываемой электроэнергии, а выработка тепла котлом при неизменных параметрах пара перед турбиной пропорциональна выработке пара. Расход топлива на котел связан с расходом тепла через КПД котельного агрегата, который (КПД) изменяется незначительно. Расход топлива на отпуск электроэнергии для конденсационных энергоблоков, у которых отпуск тепла мал, очень близок к расходу топлива на котел. Следовательно, расход питательной воды должен совпадать с расходом пара с учетом технологических пароводяных потерь, составляющих для конкретных энергоблоков менее 1 % от расхода питательной воды.

Отпуск электроэнергии отличается от выработки электроэнергии на долю собственных нужд, составляющую для данного случая величину не более 4–5 % от вырабатываемой электроэнергии. Это, по-видимому, и является причиной объединения отпуска и выработки электроэнергии в один фактор.

Расход воды на впрыск в промперегрев практически пропорционален нагрузке энергоблоков, а следовательно, и выработке электроэнергии. Основной показатель множества {Фактора 1} — выработка электроэнергии Э энергоблоком зависит от электрической нагрузки, мощности N энергоблока:

$$Э = \sum_{i=1}^{n} N_i \tau_i,$$

где N_i — мощность энергоблока в i-м периоде; τ_i — длительность i-го периода; n — количество временных периодов в анализируемом интервале (1 месяц) с постоянной электрической нагрузкой.

Все рассмотренные выше показатели должны иметь существенную корреляционную связь с мощностью энергоблока. Иная ситуация складывается с расходом электроэнергии на собственные нужды турбин и котлов. Эти показатели для анализируемых энергоблоков не зависят от электрической мощности, однако зависят от времени работы энергоблока. Особенность использования энергоблоков Сургутской ГРЭС-1 состоит в том, что значительную часть времени блоки работают в базовой части электрического графика с нагрузкой, близкой к номинальной. Вследствие этого выработка электроэнергии пропорциональна суммарному времени работы энергоблока, а расход электроэнергии на собственные нужды пропорционален выработке. Таким образом, все включенные в {Фактор 1} показатели связаны с определяющим показателем — выработкой электроэнергии блоком — и могут рассматриваться совместно.

Множество {Фактор 2} связано с отпуском тепловой энергии от энергоблока, также оно объединяет показатели, характеризующие отпуск тепла от энергоблока с горячей водой. Ряд конденсационных энергоблоков Сургутской ГРЭС-1 отпускают небольшое количество теплоты с паром производственному предприятию, находящемуся недалеко от ГРЭС. Для множества {Фактора 2} определяющим параметром является отпуск тепла внешнему потребителю. Остальные показатели в данном факторе зависят от определяющего — отпуска тепла внешнему потребителю. Это относится также к удельному расходу топлива на отпуск тепла, который должен умень-

шаться при увеличении количества отпускаемой тепловой энергии. Отпуск тепла производится от бойлеров, а расход электроэнергии на тепловую установку определяется расходом сетевой воды через бойлеры.

Корреляционные связи между показателями, включенными в множество {Фактор 3}, являются менее значимыми, чем аналогичные связи между показателями, составляющими множество {Фактор 1}. Здесь определяющим показателем является температура охлаждающей воды на входе в конденсатор.

Эта температура должна быть близка к температуре воды в водоеме Сургутской ГРЭС-1 и коррелировать с температурой наружного воздуха. В летние месяцы динамика изменения температуры холодного воздуха на всасе дутьевого вентилятора и воздуха перед регенеративным воздухоподогревателем (РВП) должна быть аналогична динамике изменения температуры охлаждающей воды на входе в конденсатор. В зимние месяцы эта связь может нарушаться. По технологическим требованиям температура воздуха перед РВП должна быть не менее (или близка) 30 °С. Для этого в зимние месяцы реализуется рециркуляция горячего воздуха перед РВП. Температура холодного воздуха в зимние месяцы зависит от положения шибера на линии холодного воздуха, определяющего место забора воздуха на всасе вентилятора — с улицы или из помещения котельного цеха. Температура уходящих газов в значительной мере зависит как от температуры холодного воздуха, так и от паропроизводительности котельного агрегата. Влияние первого показателя, по-видимому, сильнее, что и привело к включению температуры уходящих газов в множество {Фактор 3}. Номинальный относительный расход тепла на собственные нужды котла является расчетной величиной и зависит в первую очередь от температуры наружного воздуха.

В множество {Фактор 4} вошли показатели, характеризующие экологические параметры ТЭС, определяющим является содержание кислорода в уходящих газах.

Многомерные статистические модели ТЭП

Проведенная группировка факторов означает, что в соответствии с базовым подходом, используемым в факторном анализе [4], для описания связей между технологическими показателями, вошедшими в описанные выше множества, следует использовать линейные математические модели вида

$$x_{1,k} = a_0 + a_1 x_{2,l} + a_2 x_{3,m} + a_3 x_{4,n}; \qquad (1)$$

$$x_{2,l} = a_0 + a_1 x_{1,k} + a_2 x_{3,m} + a_3 x_{4,n}; \qquad (2)$$

$$x_{3,m} = a_0 + a_1 x_{1,k} + a_2 x_{2,l} + a_4 x_{4,n}; \qquad (3)$$

$$x_{4,m} = a_0 + a_1 x_{1,k} + a_2 x_{2,l} + a_3 x_{3,n}, \qquad (4)$$

где $k = \overline{1,13}$, $l = \overline{1,9}$, $m = \overline{1,5}$, $n = \overline{1,4}$. Коэффициенты a_0, a_1, a_2, a_3 в моделях (1)–(4) находятся в соответствии с методом наименьших квадратов (МНК). Полное число возможных сочетаний переменных (количество математических моделей) составило 9360.

Для примера на рис. 1 представлены:

— зависимость среднемесячных значений выработки электроэнергии блоком ($x_{1,1}$);

— аналогичная зависимость, рассчитанная по следующей математической модели:

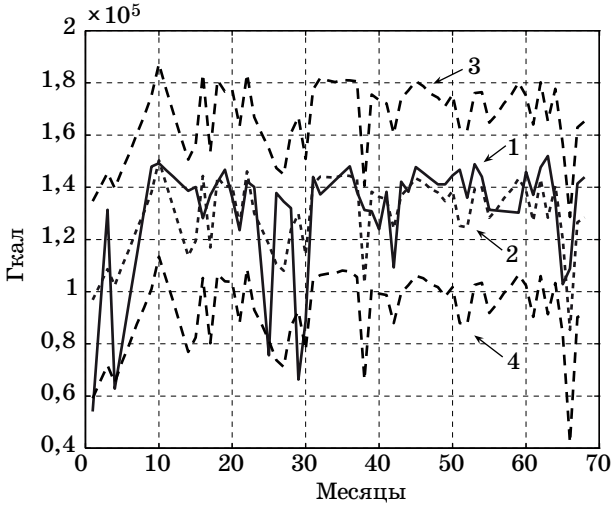
$$x_{1,1} = 2{,}593 \cdot 10^5 + 3{,}426 \cdot 10^0 \cdot x_{2,1} + 6{,}800 \cdot 10^2 \cdot x_{3,1} + (-1{,}126 \cdot 10^5) \cdot x_{4,1},$$

где $x_{2,1}$ — отпуск тепла внешнему потребителю, $x_{3,1}$ — температура охлаждающей воды на входе в конденсатор, $x_{4,1}$ — содержание кислорода в уходящих газах;

— доверительные интервалы математической модели.

У обсуждаемой математической модели коэффициент детерминации R = 58 %, дисперсия остатков (разностей между исходными значениями и соответствующими значениями) — $1{,}879 \cdot 10^4$ Гкал.

Для интегральной оценки надежности полученных факторных моделей было проведено исследование рядов остатков всех математических моделей на соответствие нормальному закону распределения. Обобщенные результаты по каж-



■ ***Рис. 1.*** *Зависимости выработки электроэнергии блоком от номера отсчета: кривая 1 — исходная; кривая 2 — рассчитанная по линейной модели; кривые 3 и 4 — соответственно верхняя и нижняя границы доверительных интервалов*

■ ***Таблица 2.*** *Результаты исследования законов распределения рядов остатков*

Принадлежность зависимой переменной	Соответствие распределения остатков гипотезе о нормальности распределения остатков	
	Да, шт. (%)	Нет, шт. (%)
{Фактор 1}	1862 (80)	478 (20)
{Фактор 2}	959 (41)	1381 (59)
{Фактор 3}	2218 (95)	122 (5)
{Фактор 4}	2088 (89)	252 (11)
Итого	7127 (76)	2233 (24)

дому из выделенных множеств технологических показателей представлены в табл. 2.

В целом остатки 76 % моделей имеют нормальный закон распределения, что, с нашей точки зрения, является в известной мере подтверждением возможности описания связей между выделенными факторами линейных моделей.

В то же время необходимо отметить, что остатки более половины (59 %) возможных моделей вида (2) имеют закон распределения, отличный от нормального. Это свидетельствует о недостаточно высоком в рассматриваемом случае качестве линейных математических моделей. Данные результаты позволяют сделать предположение о возможности получения более качественной аппроксимации зависимостей между выделенными факторами при использовании более сложных математических моделей.

В связи с тем, что на сегодняшний день отсутствуют теоретические обоснования рекомендаций по выбору тех или иных функциональных зависимостей между выделенными факторами, в качестве базового нами выбран метод группового учета аргумента (МГУА), разработанный А. Г. Ивахненко [6] для прогнозирования сложных многофакторных процессов, не имеющих теоретического описания. Основной результат теории МГУА состоит в том, что при неточных зашумленных данных и коротких выборках минимум критерия указывает нефизическую модель (решающее правило), точность которой выше, а структура — проще структуры полной физической модели.

Напомним, что в МГУА осуществляется последовательное по заданному критерию апробирование моделей-кандидатов, в качестве которых наиболее часто используют полиномиальные опорные функции в виде полинома Колмогорова — Габора:

$$y = a_0 + \sum_{i=1}^{M} a_i x_i + \sum_{i=1}^{M}\sum_{j=1}^{M} a_{ij} x_i x_j + \sum_{i=1}^{M}\sum_{j=1}^{M}\sum_{k=1}^{M} a_{ijk} x_i x_j x_k,$$

где M — число переменных; $\mathbf{x} = (x_1, x_2, \ldots, x_M)$ — вектор входных переменных; $\mathbf{a} = (a_1, a_2, \ldots, a_M)$ — вектор коэффициентов слагаемых.

Вектор коэффициентов **a** находят по обучающей выборке (набору значений $\bar{x}_n$, $\bar{y}_n$, $n = 1, N$, $N \geq M$) с помощью МНК. На практике оказывается удобным использовать многорядный алгоритм [6], в котором правило итерации остается для всех рядов одним и тем же. Здесь на первом ряду используется частное описание вида

$$y^{\langle 1\rangle} = a_0^{\langle 1\rangle} + a_1^{\langle 1\rangle} x_i + a_2^{\langle 1\rangle} x_j + a_3^{\langle 1\rangle} x_i x_j + a_4^{\langle 1\rangle} x_i^2 + a_5^{\langle 1\rangle} x_j^2;$$

на втором ряду

$$y^{\langle 2\rangle} = a_0^{\langle 2\rangle} + a_1^{\langle 2\rangle} y_i^{\langle 1\rangle} + a_2^{\langle 2\rangle} y_j^{\langle 1\rangle} + a_3^{\langle 2\rangle} y_i^{\langle 1\rangle} y_j^{\langle 1\rangle} + a_4^{\langle 2\rangle} (y_i^{\langle 1\rangle})^2 + a_5^{\langle 2\rangle} (y_j^{\langle 1\rangle})^2;$$

на третьем

$$y^{\langle 3\rangle} = a_0^{\langle 3\rangle} + a_1^{\langle 3\rangle} y_i^{\langle 2\rangle} + a_2^{\langle 3\rangle} y_j^{\langle 2\rangle} + a_3^{\langle 3\rangle} y_i^{\langle 2\rangle} y_j^{\langle 2\rangle} + a_4^{\langle 3\rangle} (y_i^{\langle 2\rangle})^2 + a_5^{\langle 3\rangle} (y_j^{\langle 2\rangle})^2 \qquad (5)$$

и т. д.

Выбор данного алгоритма обусловлен тем, что, как видно из (5), здесь используются полиномы, зависящие от двух переменных степени не выше второй. В этой связи при выполнении на каждом ряду моделей процедуры обращения информационной матрицы $(\mathbf{A}^T\mathbf{A})^{-1}$, где **A** — регрессионные матрицы:

$$\mathbf{A}^{\langle 1\rangle} = \begin{bmatrix} 1 & x_{1,1} & x_{2,1} & x_{1,1}x_{2,1} & x_{1,1}^2 & x_{2,1}^2 \\ 1 & x_{1,2} & x_{2,2} & x_{1,2}x_{2,2} & x_{1,2}^2 & x_{2,2}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{1,N} & x_{2,N} & x_{1,N}x_{2,N} & x_{1,N}^2 & x_{2,N}^2 \end{bmatrix};$$

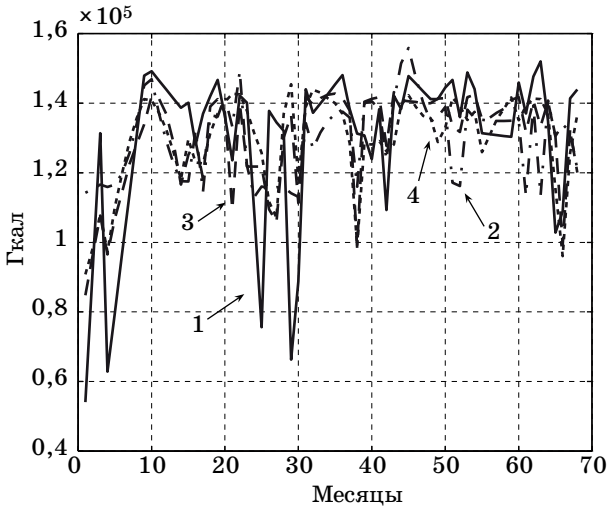
$$\mathbf{A}_1^{\langle 2\rangle} = \begin{bmatrix} 1 & y^{\langle 1\rangle}{}_{1,1} & y^{\langle 1\rangle}{}_{2,1} & y^{\langle 1\rangle}{}_{1,1} y^{\langle 1\rangle}{}_{2,1} & \left[y^{\langle 1\rangle}{}_{1,1}\right]^2 & \left[y^{\langle 1\rangle}{}_{2,1}\right]^2 \\ 1 & y^{\langle 1\rangle}{}_{1,2} & y^{\langle 1\rangle}{}_{2,2} & y^{\langle 1\rangle}{}_{1,2} y^{\langle 1\rangle}{}_{2,2} & \left[y^{\langle 1\rangle}{}_{1,2}\right]^2 & \left[y^{\langle 1\rangle}{}_{2,2}\right]^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & y^{\langle 1\rangle}{}_{1,N} & y^{\langle 1\rangle}{}_{2,N} & y^{\langle 1\rangle}{}_{1,N} y^{\langle 1\rangle}{}_{2,N} & \left[y^{\langle 1\rangle}{}_{1,N}\right]^2 & \left[y^{\langle 1\rangle}{}_{2,N}\right]^2 \end{bmatrix}$$

и т. д.

Опишем подробно методику построения математических моделей МГУА на примере построения зависимости показателя выработки электроэнергии блоком ($x_{1,1}$) от показателей $x_{2,1}$, $x_{3,1}$ и $x_{4,1}$.

При реализации многорядного алгоритма МГУА:

1. На первом ряду в соответствии с вычислительной процедурой МНК были вычислены коэффициенты следующих полиномов:



■ ***Рис. 2.*** *Зависимость выработки электроэнергии блоком (кривая 1) и полиномов 1-го уровня (2 — $y_1^{\langle 1\rangle}$, 3 — $y_2^{\langle 1\rangle}$, 4 – $y_3^{\langle 1\rangle}$) от номера отсчета*

$$y_1^{\langle 1\rangle} = a_{0,1}^{\langle 1\rangle} + a_{1,1}^{\langle 1\rangle}x_{2,1} + a_{2,1}^{\langle 1\rangle}x_{3,1} + a_{3,1}^{\langle 1\rangle}x_{2,1}x_{3,1} + a_{4,1}^{\langle 1\rangle}x_{2,1}^2 + a_{5,1}^{\langle 1\rangle}x_{3,1}^2;$$

$$y_2^{\langle 1\rangle} = a_{0,1}^{\langle 1\rangle} + a_{1,1}^{\langle 1\rangle}x_{2,1} + a_{2,1}^{\langle 1\rangle}x_{4,1} + a_{3,1}^{\langle 1\rangle}x_{2,1}x_{4,1} + a_{4,1}^{\langle 1\rangle}x_{2,1}^2 + a_{5,1}^{\langle 1\rangle}x_{4,1}^2;$$

$$y_3^{\langle 1\rangle} = a_{0,1}^{\langle 1\rangle} + a_{1,1}^{\langle 1\rangle}x_{3,1} + a_{2,1}^{\langle 1\rangle}x_{4,1} + a_{3,1}^{\langle 1\rangle}x_{3,1}x_{4,1} + a_{4,1}^{\langle 1\rangle}x_{3,1}^2 + a_{5,1}^{\langle 1\rangle}x_{4,1}^2.$$

2. В каждой точке ($x_{2,1,k}$, $x_{3,1,k}$, $x_{4,1,k}$), $k = \overline{1,68}$ вычислены значения аппроксимирующих полиномов $y_{1,k}^{\langle 1\rangle}, y_{2,k}^{\langle 1\rangle}, y_{3,k}^{\langle 1\rangle}$ (рис. 2).

3. Вычислены дисперсии остатков каждого из полиномов 1-го уровня (табл. 3).

4. Выбраны для построения полиномов 2-го уровня полиномы $y_2^{\langle 1\rangle}$, $y_3^{\langle 1\rangle}$, имеющие наименьшую дисперсию.

5. На втором ряду в соответствии с вычислительной процедурой МНК вычислены коэффициенты полинома

■ ***Таблица 3.*** *Дисперсии остатков полиномов первого уровня*

Номер полинома	Дисперсия остатков
$y_1^{\langle 1\rangle}$	$1{,}922 \cdot 10^4$
$y_2^{\langle 1\rangle}$	$1{,}705 \cdot 10^4$
$y_3^{\langle 1\rangle}$	$1{,}806 \cdot 10^4$

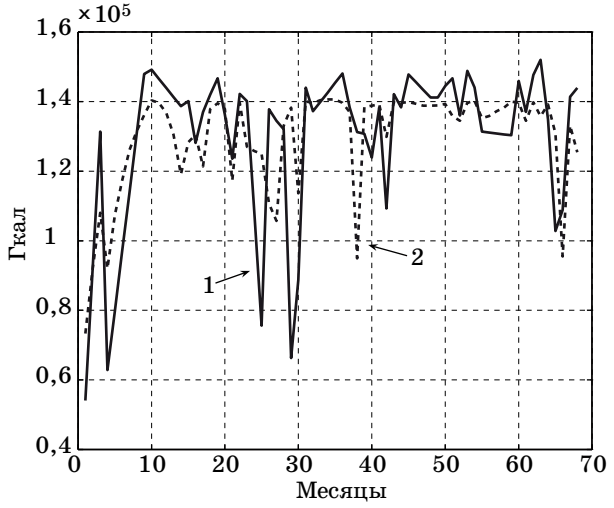
$$y_1^{\langle 2\rangle} = a_{0,1}^{\langle 2\rangle} + a_{1,1}^{\langle 2\rangle}y_2^{\langle 1\rangle} + a_{2,1}^{\langle 2\rangle}y_3^{\langle 1\rangle} + a_{3,1}^{\langle 2\rangle}y_2^{\langle 1\rangle}y_3^{\langle 1\rangle} + a_{4,1}^{\langle 2\rangle}\left[y_2^{\langle 1\rangle}\right]^2 + a_{5,1}^{\langle 2\rangle}\left[y_3^{\langle 1\rangle}\right]^2.$$

6. В каждой точке ($x_{2,1,k}$, $x_{3,1,k}$, $x_{4,1,k}$), $k = \overline{1,68}$ вычислены значения аппроксимирующего полинома $y_{1,k}^{\langle 2\rangle}$ (рис. 3).

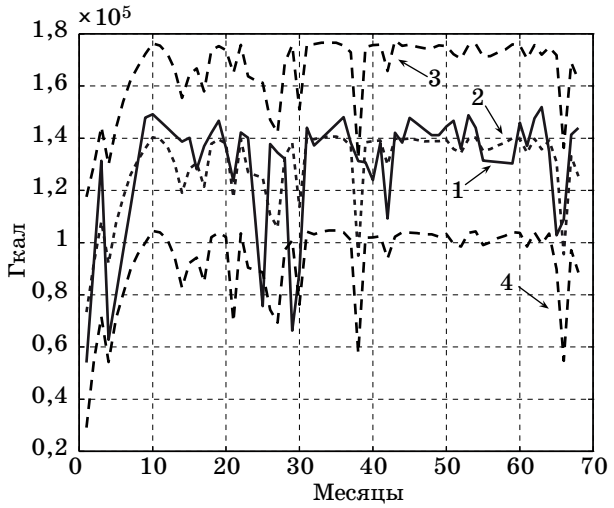
7. Вычислена дисперсия остатков полинома 2-го уровня, составившая $1{,}681 \cdot 10^4$ Гкал.

В связи с тем, что дисперсия остатков при переходе от полиномов 1-го уровня к полиному 2-го уровня практически не изменилась, дальнейшее построение полиномов было прекращено. Зависимость исходных данных и значений полинома 2-го уровня от номера отсчета и границы доверительных интервалов представлены на рис. 4. У обсуждаемой математической модели коэффициент детерминации $R = 66$ %, дисперсия остатков модели — $1{,}681 \cdot 10^4$ Гкал. Таким образом, коэффициент детерминации математической модели, построенной с помощью МГУА, оказался на 10 % выше, чем у линейной математической модели, а дисперсия остатков, соответственно, на 12 % меньше. Следовательно, нелинейная математическая модель в рассмотренном случае обеспечивает более высокое качество аппроксимации.

Для количественного сравнения качества линейных и нелинейных математических моделей были вычислены дисперсии их остатков (соответственно $D1_j$ и $D2_j$, $j = 1, 2, ..., 2340$) и проведено их сравнение; с помощью критериев χ^2 и Фишера выполнена проверка на нормальность распределений остатков; вычислены коэффициенты детерминации линейных и нелинейных моде-



■ ***Рис. 3.*** *Зависимость выработки электроэнергии блоком (кривая 1) и полинома 2-го уровня (кривая 2) от номера отсчета*



■ ***Рис. 4.*** *Зависимости выработки электроэнергии блоком (кривая 1) и полинома 2-го уровня (кривая 2) от номера отсчета (кривые 3 и 4 — соответственно верхняя и нижняя границы доверительных интервалов)*

лей ($R1_j$ и $R2_j$ соответственно) и проведено их сравнение.

Результаты сравнительного анализа свойств остатков линейных (М1) и нелинейных (М2) моделей представлены в табл. 4. Видно, что по качеству нелинейные математические модели, построенные с помощью МГУА, как и в ранее рассмотренном примере, оказываются лучше по сравнению с линейными моделями. В частности, можно отметить следующие их преимущества.

1. У всех нелинейных математических моделей 1-го и 3-го классов дисперсии рядов остатков D оказываются меньше аналогичных величин у линейных математических моделей, а коэффициенты детерминации R, соответственно, больше.

2. Из 2340 нелинейных математических моделей 2-го класса у 2330 моделей (99,53 %) дисперсии рядов остатков D оказываются меньше аналогичных величин для линейных математических моделей, а коэффициенты детерминации R, соответственно, больше.

3. Из 2340 нелинейных математических моделей 4-го класса у 2337 моделей (99,86 %) дисперсии рядов остатков D оказываются меньше аналогичных величин для линейных математических моделей, а коэффициенты детерминации R, соответственно, больше.

4. У нелинейных математических моделей в сравнении с линейными оказывается больше количество моделей, остатки которых имеют нормальный закон распределения: на 14, 17, 3 и 9 % для моделей 1-, 2-, 3- и 4-го классов соответственно.

Таким образом, полученные результаты свидетельствуют, что вопреки устоявшемуся в факторном анализе подходу — использовать для описания связей между факторами линейные математические модели — применение в рассматриваемом случае нелинейных математических моделей, построенных с помощью МГУА, обеспечивает более высокое качество аппроксимации анализируемых данных. Использование линейных и нелинейных математических моделей позволяет технологам задавать произвольные значения факторов и согласно полученной регрессионной модели рассчитывать значение зависимого фактора и его доверительный интервал. Математические модели также позволяют выполнять количественную оценку и оценку поведения ТЭП при значительных изменениях одного или нескольких ТЭП модели, в свою очередь полученные оценки дадут возможность технологам имитировать различные ситуации (в том числе и критические), за счет чего повысится отказоустойчивость системы в целом.

Заключение

Развиваемый в статье подход основан на комплексном использовании факторного анализа, позволяющего уменьшить пространство информационных параметров, описывающих состояние системы, и нелинейных математических моделей, построенных в соответствии с МГУА, которые описывают связь между показателями в пространстве меньшей размерности. Представляется перспективным применение данного метода при обработке информации, собираемой информационными системами сложных технических объектов (например, ТЭС, газоперекачивающих агрегатов и т. п.).

■ ***Таблица 4.*** *Результаты сравнительного анализа остатков линейных и нелинейных моделей*

№ класса математической модели	Принадлежность зависимой переменной	Доля моделей, у которых $D1_j < D2_j$	Нормальный закон распределения, %		Доля моделей, у которых $R1_j > R2_j$
			М1	М2	
1	{Фактор 1}	0	80	94	0
2	{Фактор 2}	10	41	68	10
3	{Фактор 3}	0	95	98	0
4	{Фактор 4}	3	90	99	3

Литература

1. **Поршнев С. В.** и др. Диагностика газоперекачивающих агрегатов на основе анализа технологической информации. — Екатеринбург: УрО РАН, 2007. — 205 с.
2. **Соломаха И. В., Аронсон К. Э., Поршнев С. В.** Опыт анализа технологической информации, собираемой на тепловых электрических станциях // Науч. тр. Междунар. науч.-практ. конф. «СВЯЗЬ-ПРОМ 2008» и 5-го Евро-Азиатского форума «СВЯЗЬПРОМ-ЭКСПО 2008». Екатеринбург: Компания РеалМедиа, 2008. С. 29–32.
3. **Соломаха И. В.** Анализ технологической информации собираемой АСУТП теплоэлектростанции// Информатика и управление в технических системах: Одиннадцатая Всерос. студ. науч.-техн. интернет-конф. http://webconf.rtf.ustu.ru (дата обращения: 09.01.08).
4. **Дубров А. М.** Обработка статистических данных методом главных компонент. — М.: Статистика, 1978. — 136 с.
5. **Лоул Д., Максвелл А.** Факторный анализ как статистический метод: пер. с англ. Ю. Н. Благовещенского. — М.: Мир, 1967. — 143 с.
6. **Ивахненко А. Г.** Индуктивный метод самоорганизации моделей сложных систем. — Киев: Наук. думка, 1982. — 290 с.

УДК 681.3

АНАЛИЗ ТЕКСТОВЫХ СООБЩЕНИЙ В СИСТЕМАХ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И. С. Лебедев,
канд. техн. наук, доцент
Санкт-Петербургский государственный университет
Ю. Б. Борисов,
аспирант
Санкт-Петербургский государственный университет информационных технологий, механики и оптики

Описываются модели формализации естественно-языковых сообщений для систем мониторинга информационной безопасности открытых вычислительных сетей. Рассматриваются особенности обработки и анализа сообщений.

Ключевые слова *— формализация естественного языка, обработка сообщений, вычисление информационных структур.*

Введение

В условиях социальных преобразований, происходящих в мире, возникает необходимость непрерывного наблюдения за различными информационными событиями. Интеграция глобальных вычислительных сетей в огромное количество сфер деятельности человека обуславливает появление информационных ресурсов, отражающих политические, социальные, экономические новости. Сообщения блогеров, комментаторов лент новостных агентств и порталов, участников «Живого Журнала» содержат информацию о личных отношениях к происходящему в общественной жизни. Вследствие чего возникает задача автоматизированной обработки информации с целью определить и проанализировать политический, социальный, экономический спектр мнений.

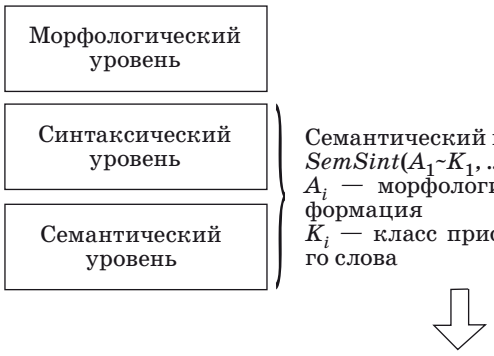
Существующая легкость использования информационного пространства, предоставляемого глобальными вычислительными сетями, участившееся применение различных ресурсов сети Интернет для проведения всевозможных PR-акций, информационных компаний, направленных на решение политических, экономических, идеологических задач, наносит определенный урон хозяйствующим субъектам и требует анализа огромного количества текстов для выявления внешних и внутренних источников информационных угроз.

Однако сложность методов, позволяющих в автоматическом режиме идентифицировать структуру и значение обрабатываемых естественно-языковых сообщений, заставляет производить их обработку с применением «ручных» технологий [1]. Вместе с тем высокая степень интеграции и использования ПЭВМ наряду с внедрением информационных технологий дает возможность разрабатывать и реализовывать в информационных системах более эффективные методы и алгоритмы вычисления слабоструктурированных данных [2].

Формализации естественно-языковых конструкций

Аналитические модели описания естественного языка (ЕЯ) в большинстве случаев являются узкоспециализированными и сложными с точки зрения адаптации под конкретные виды задач обработки текстовой информации открытых компьютерных сетей. Для повышения качества обработки документов на ЕЯ в предметной области обнаружения информационных угроз необходимо решить вопрос о формализации семантической составляющей.

Одним из подходов, который может быть применен для обработки относительно коротких текстовых сообщений, является семантическая модель ЕЯ профессора СПбГУ В. А. Тузова [3]. В ней выделяется три уровня: морфологический, семантико-синтаксический, семантический (рис. 1):



■ ***Рис. 1.*** *Семантическая модель языка В. А. Тузова*

$$M = <W, Se, K>, \quad (1)$$

где W — множество словоформ; Se — множество семантических шаблонов; K — множество классов.

Особенностью предложенной В. А. Тузовым модели ЕЯ является объединенный семантико-синтаксический уровень. Каждое слово обладает морфологическими и семантико-синтаксическими характеристиками, на основе которых строится семантический предикат.

Общий шаблон описания словоформы в словаре Тузова можно представить в следующем виде:

$$W(Z1{:}!\text{Им}\{K_1\}_g, Z2{:}!\text{Род}\{K_2\}_g, Z3{:}!\text{Дат}\{K_3\}_g, Z4{:}!\text{Вин}\{K_4\}_g, Z5{:}!\text{Тв}\{K_5\}_g, Z6{:}!\text{Пред}\{K_6\}_g),$$

где $\{K_1\}_g$ ... $\{K_6\}_g$ — набор классов, соответствующий данной словоформе.

Однако семантический словарь Тузова, применяемые для решения аналогичных задач словари Шведовой, Ефремовой, лингвистические базы данных компаний АОТ, RCO и др. очень сильно отличаются по структуре, количеству классов, числу входящих в них слов. Вследствие чего подобные продукты должны быть подвержены дополнительной адаптации под конкретную задачу анализа текста, связанной с уточнением состава и вида (например, древовидный или линейный) классификатора словоформ. Использование словарных баз данных (БД) в большинстве случаев требует знаний лингвиста и может быть сложным для специалиста в области информационной безопасности, которому необходимо настроить фильтр, осуществляющий контент-анализ текстовых сообщений.

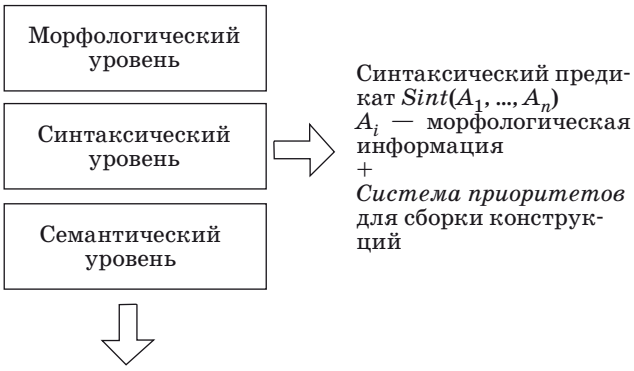
Модель ЕЯ Тузова предполагает возможность анализа любого предложения естественного (русского) языка. Формирование применяемой в ней семантической БД происходило путем автоматизированной обработки различных, в том числе художественных, текстов. Учитывая «произвольный» порядок слов, где, например, образующее связь с существительным прилагательное может быть отделено от него оборотами и находиться в любых частях предложения, для построения структуры ЕЯ-конструкции необходим перебор всех аргументов на предмет вычисления возможности образования связей. С другой стороны, несмотря на поддержку и развитие данной модели определенные сложности при вычислении результата анализа предложения происходят, когда встречаются неоднозначные словоформы, что влияет на построение информационных объектов текста [4, 5]. Реализация систем, базирующихся на приводимой модели, требует значительных затрат на поддержку.

Части недостатков лишена адаптированная модель, предназначенная для поиска определенной тематической информации [6]. В ней, аналогично семантической модели Тузова, также выделяются уровни — морфологии, синтаксиса и семантики. Однако последние отделены друг от друга. Синтаксический уровень содержит информацию о связях между словами, а семантический определяет правила анализа, синтеза и обработки полученных конструкций (рис. 2):

$$M = <W, Si, Ks>, \quad (2)$$

где Si — множество синтаксических шаблонов, $Si \in Se$; Ks — множество классов, $Ks \in K$.

Особенность приводимой модели состоит в использовании масштабируемых предикатов описания информации аргументов словоформ предметно-ориентированных словарных БД ЕЯ, что позволяет осуществлять идентификацию, сравнение конструкций и построение управляющих правил обработки на уровне связей.



■ ***Рис. 2.*** *Адаптированная модель языка*

Масштабируемый предикат по своему составу идентичен семантическому предикату предыдущей модели. Однако вместо семантического класса в нем используются классы идентификационного множества, влияющие на тип и семантическое значение ЕЯ-конструкции в рамках тематики предметной области.

Рассмотрим подход к их построению на основе вычисления структуры предложения и особенности использования.

Вычисление структуры предложения

В нашем случае анализ стилистики текстов блогов, лент новостных агентств показывает почти полное отсутствие «длинных» предложений, которые встречаются у русских классиков. Среднее количество слов в таких сообщениях около 10, что подтверждается данными статистических исследований, опубликованных на сайтах, посвященных классической лингвистике. Прилагательные и уточняющие существительные в родительном и творительном падежах, обороты, идентифицируемые словом «который», причастия не разбросаны по тексту сообщений, а тяготеют к базовым, образующим конструкцию с существительным. Оценка обработки источников текстовой информации сети Интернет может быть осуществлена через подходы, основанные на ошибках первого и второго рода. Для этого словарные БД адаптируют под конкретную предметную область. Ограничения предметной области позволяют избавиться от значительного количества неоднозначных словоформ и использовать для идентификации часто встречающихся последовательностей терминов синтаксический анализатор. Описание одного из решений для синтаксического анализатора можно найти на сайте компании АОТ (www.aot.ru). Принцип действия алгоритма состоит в упорядоченном последовательном переборе около 40 правил.

Однако при анализе текста в системах мониторинга основную часть информации предоставляют существительные. Обнаружение этих частей речи с последующим присоединением к ним подчиненных прилагательных, наречий, причастий позволяет при образовании связи не тратить ресурсы на вычисление типа образовавшейся конструкции. Приводимый алгоритм использует описания словоформ частей речи, основанные на шаблоне, содержащем синтаксическую информацию о потенциальных связях:

$$W(Z1{:}!\text{Им}, Z2{:}!\text{Род}, Z3{:}!\text{Дат}, Z4{:}!\text{Вин}, Z5{:}!\text{Тв}, Z6{:}!\text{Пред}).$$

В предикате конкретной словоформы лишние связи удаляются. Например, для подавляющего числа существительных синтаксический шаблон будет выглядеть следующим образом:

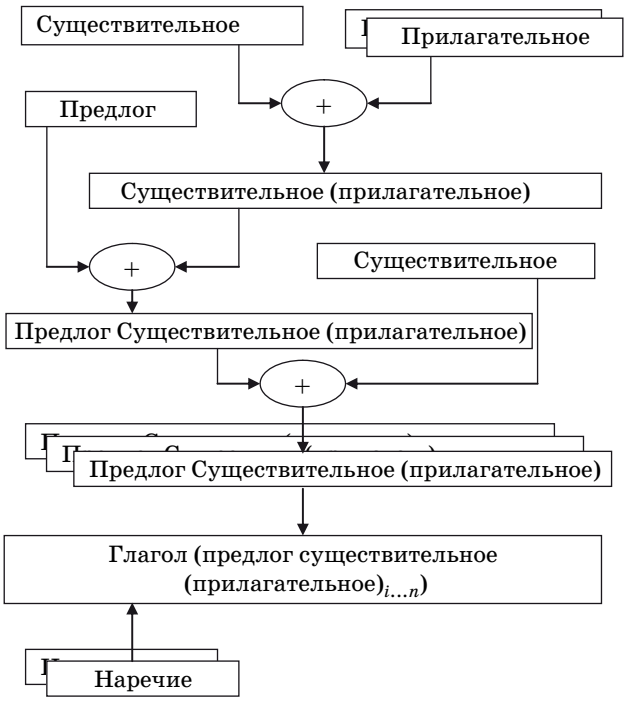
$$W(Z1{:}!\text{Род}).$$

Типовые шаблоны частей речи, особенности их использования приведены в работе [6]. Наибольший приоритет отдается анализу возможности образования связей между двумя ближайшими словоформами.

Рассмотрим упрощенный алгоритм свертки предложения, не акцентируя внимание на таких частях речи и предложения, как числительные, союзы, частицы, причастия, деепричастия, подчиненные предложения. В простом распространенном предложении могут содержаться (или не содержаться) следующие части речи: глаголы, существительные, прилагательные, наречия. На рис. 3 показана последовательность шагов свертки предложения.

1. Присоединение подчиненных прилагательных к существительным.

На этом шаге основная информация берется из морфологического описателя словоформы. При первом просмотре предложения слева направо ищутся ближайшие, согласующиеся по падежу, роду и числу, прилагательные и существительные. Так как прилагательное может находиться справа от существительного, то необходим аналогичный просмотр справа налево, на котором осуществляется попытка присоединения



■ ***Рис. 3.*** *Упрощенный алгоритм свертки предложения*

оставшихся прилагательных, не вошедших в конструкцию.

Ввиду ограниченности объема не будем останавливаться на отдельных ситуациях, когда прилагательные не согласуются по морфологической информации со своими существительными, например:

Средства и методы — проверенные.

Подобных ситуаций конечное количество, и они поддаются довольно строгому описанию и формализации.

2. Присоединение предлогов к конструкциям существительных и прилагательных. Особенностью шага является то, что предлог всегда находится слева от конструкции существительного. Основная информация для реализации свертки — это синтаксический описатель предлога и морфологический описатель конструкции существительного. Информация по предлогу содержит падеж и класс присоединяемого существительного.

3. Присоединение конструкций существительных к другим объектам осуществляется на основании анализа синтаксического описателя левой конструкции и морфологического и синтаксического описателя правой конструкции. Производится слева направо. Вне зависимости от описаний объекты существительных в родительном падеже присоединяются к конструкциям, стоящим слева.

4. Все созданные конструкции подставляются в предикат глагольной функции на основании своей синтаксической информации.

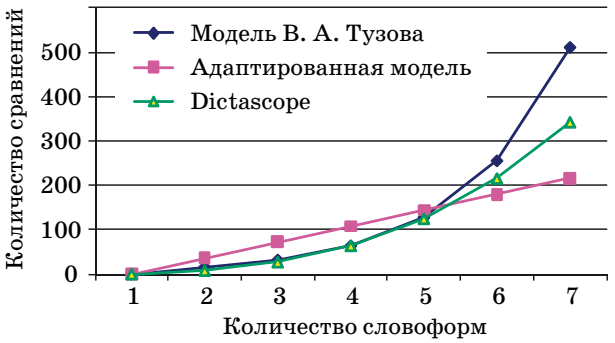
5. Наречия и собранные конструкции, не вошедшие в описатель глагола, приписываются к нему со своим семантико-грамматическим типом.

Следует отметить, что русский язык является довольно регулярным и исключения из правил составляют не более 10 %.

Причастные, деепричастные обороты, подчиненные предложения, начинающиеся со слова *который*, составные конструкции типа *если ... то*, вложенные предложения отделяются перед анализом. Над ними выполняются действия алгоритма свертки, а затем полученные конструкции присоединяются к основному предложению.

В зависимости от стилистических особенностей текстов предметной области, при отсутствии грамматических ошибок синтаксический анализатор выдает 60–80 % адекватных структур.

Первоначальное получение структуры и наложение на нее семантической информации позволяет уменьшить вычислительную сложность и избавиться от лавинообразного роста зависимости количества анализа связей от количества словоформ конструкций (рис. 4). (Оценка модели *Dictascope* приводится согласно публикациям [7, 8].)



■ ***Рис. 4.*** *Зависимость количества проверок связей от количества словоформ*

Полученная структура является основой для вычисления идентификационного множества классов предикатов адаптированной модели.

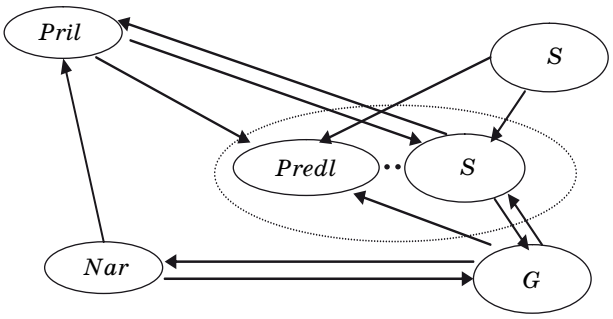
Построение идентификационного множества классов аргументов

Для реализации анализа текстовой информации в системе мониторинга необходимо изначально настроить идентификационное множество классов $k_1 \ldots k_n$ в БД с позиции тематики обрабатываемого текста. Для этого применимы анализаторы различных разработчиков. В результате обработки синтаксическим анализатором предложение приобретает вид функциональной записи, содержащей структуру и связи между его конструкциями:

$$F(w_i \rightarrow \{s\}_i), \qquad (3)$$

где w_i — слова в предложении, каждому из которых соответствует свой набор связей $\{s\}_i$ с другими словами.

Структура, представленная на рис. 5, позволяет формализовать связи, которые образуют другие части речи относительно предложно-падежной формы существительного. Вершины этого



■ ***Рис. 5.*** *Связи между частями речи относительно предложно-падежной формы существительного*

графа составляют глагол G, прилагательное Pril, предлог Predl, существительное S, наречие Nar. Каждая стрелка в графе определена совокупностью вопросов, которую можно задать от различных частей речи к предложно-падежной форме существительного или от нее.

Первая группа — падежные вопросы. Она практически однозначно определяется предложно-падежной формой и поддается формализации на уровне синтаксического шаблона. Вторая группа — смысловые вопросы. Для их формализации требуется классификатор существительных, описывающих семантическую принадлежность.

Прогон тематических текстов через синтаксический анализатор позволяет построить информационные структуры и провести их статистический анализ на предмет вычисления термов предметной области. Частота встречаемости слова, содержащие его лексические конструкции дают информацию для построения классификатора, уточнения синонимов. Особенностью подхода является то, что в основу классификатора может быть положен синтаксический анализатор и словарная БД стороннего разработчика.

Следующий этап — создание предикативного описания словоформ, базирующегося на «новом» классификаторе.

В случае, когда полученным классам можно поставить в соответствие, например, классификатор Тузова, возникает возможность доработать описание его словаря. Таким образом, при поиске, например, текстов экстремистской направленности значение слова МОЧИТЬ в его словаре необходимо преобразовать в два предиката:

МОЧИТЬ N%~МОКРЫЙ$12/113/15(Z1: ДОЖДЬ$122153\
ЖИВОЙ$124~!Им,Z2: !Тв,Z3: !Вин,Z4: НЕЧТО$1~!вПред,Z5:
НЕЧТО$1~!До)

→

МОЧИТЬ *G*(*Z*1:!Им, *Z*2:!Род, *Z*3:!Дат, *Z*4:!Вин, *Z*5:!Тв, *Z*6:!Пред)
МОЧИТЬ N%~УБИВАТЬ$1010 (*Z*1*:* ЖИВОЙ$348.352~!Им, *Z*2:!Род, *Z*3:!Дат, *Z*4: ЖИВОЙ$348.352~!Вин, *Z*5:!Тв, *Z*6:!Пред)

Конструкция, основанная на втором предикате, будет нести для системы мониторинга больше информации, чем конструкция, использующая первый предикат. Возможность подставить первый аргумент второго предиката определяется морфологической информацией и принадлежностью к классу ЖИВОЙ, участвующей в образовании связи словоформы. С другой стороны, класс ЖИВОЙ$124 в исходном предикате является «очень общим» для конкретной задачи. Для уменьшения вероятности ложной тревоги необходимо убрать часть подклассов в словаре Тузова (например, «*животные*», «*растения*») и детализировать подклассы, описывающие значения «*человек*», «*соц.группа*» и т. д.

Таким образом, адаптированная модель ЕЯ использует в описаниях словоформ масштабируемые предикаты связей, аргументы которых содержат информацию о морфологических характеристиках и классах идентификаторов присоединяемых слов, что позволяет унифицировать описания, упростить их структуру.

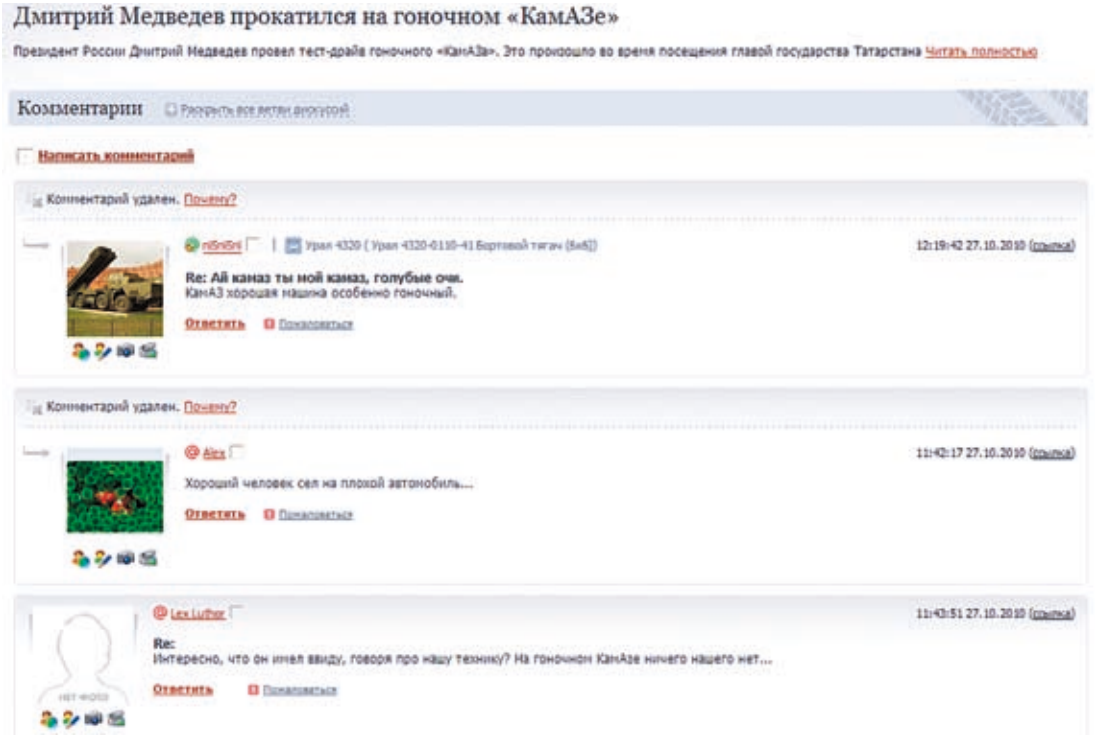
Анализ сообщений блогов и комментариев

Обеспечение экономической, социальной, политической безопасности обуславливает необходимость аудита информационного поля, одной из задач которого является анализ реакции пользователей на различные события.

Современные системы обработки комментариев направлены на получение эмоциональной оценки сообщений. Для этого применяются подходы, основанные на статистическом анализе, в котором словоформы сообщений сопоставляются с семантическими шкалами, например *хорошо-плохо*. Каждому слову такой шкалы ставится в соответствие числовое значение. Количество словоформ семантической шкалы в комментариях позволяет оценить общий эмоциональный фон. Однако в процессе ведения «дискуссий» часть идентификаторов может относиться не к обсуждаемому событию, а к другим объектам. Например, второй комментарий на рис. 6 показывает, что прилагательное *хороший* относится к существительному *человек*, а прилагательное *плохой* определяет существительное *автомобиль*. В случае простого наложения шкалы *хорошо-плохо* приводимые словоформы, характеризующие эмоциональную окраску, будут влиять друг на друга. Если построить структуру ЕЯ-конструкции, то становится очевидным, что определяются различные информационные объекты.

Учитывая стиль и особенности написания комментариев в сети Интернет, заключающиеся в использовании специфических выражений, синтаксических ошибках при построении фраз и предложений, необходимо отметить, что в автоматическом режиме не всегда удается построить адекватную структуру анализируемого сообщения [9]. В этом случае необходим универсальный подход к созданию конструкций ЕЯ на уровне синтаксических связей. В данной задаче обработка информации может основываться на вычислении трех видов элементов: *объектов, характеристик* и *действий* [10].

Поэтому модель, ложащуюся в основу получаемой информационной структуры, можно описать следующим образом:

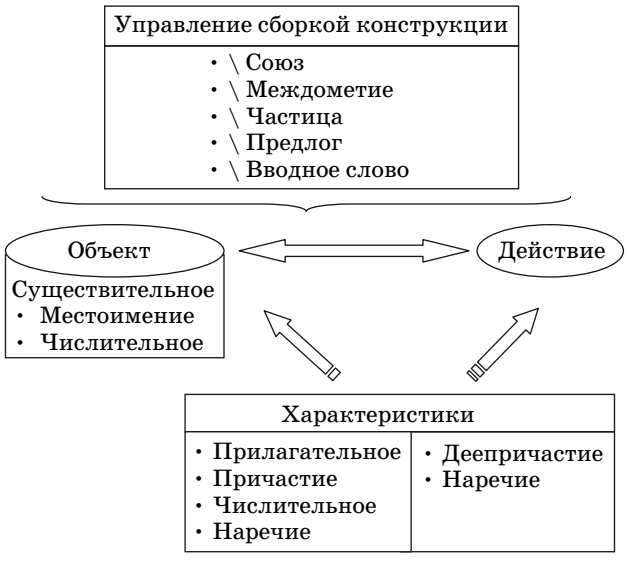


■ ***Рис. 6.*** *Пример комментариев сети Интернет*

$$M = <W, H>, \quad (4)$$

где H — характеристики: $H = \{O|D|C\}$, здесь O — объект; D — действие; $C = \{C_o, C_d\}$ — словоформы, характеризующие объекты (C_o) и действия (C_d).

Универсальная структура представления ЕЯ на примере русского (рис. 7) состоит из объектов, действий, характеристик и слов, осуществляющих управление сборкой конструкции.



■ ***Рис. 7.*** *Универсальная структура представления ЕЯ*

Если рассмотреть простое распространенное предложение на любом ЕЯ, то можно сопоставить полученные морфологические идентификаторы согласно описанной ниже системе.

1. Объекты предложения — существительные.

2. Действие — глагол со своей группой, которая определяется структурой графа предложения.

3.1. Характеристики объектов — прилагательные, причастия, наречия, подчиненные существительные.

3.2. Характеристики действий — наречия, деепричастия.

4. Управляющие слова — простые и составные предлоги, союзы, знаки препинания.

Подготовительный этап для простейшего алгоритма создания структуры информационных объектов предложения на основе морфологического анализа состоит из следующих шагов:

1) поиск объектов предложения;

2) поиск управляющих слов;

3) поиск ближайших характеристик объектов предложения;

4) проверка на возможность образования групп объектов;

5) определение действий;

6) поиск характеристик действий.

Для реализации алгоритма необходимо точно определить роль словоформы в предложении и создать систему приоритетов выбора последовательности частей речи.

Задача, решаемая с помощью данной модели, состоит в том, чтобы при обработке текстов сообщений с неправильным синтаксисом постараться получить отдельные связанные ЕЯ-конструкции, на основе которых определить информационный объект, его характеристики, свойства и действия. Модель является упрощением предыдущих, описанных в статье, ее достоинство заключается в том, что предложенный подход по созданию структуры универсален для большинства ЕЯ, быстро реализуем без существенных затрат на морфологическом и синтаксическом уровне.

В практической реализации данная модель применена в рамках задач мониторинга и создания рейтинга высказываний по событиям, обсуждаемым в сети Интернет.

Заключение

Подход к выбору аналитических моделей представления естественного языка в системах мониторинга, обрабатывающих ЕЯ-сообщения, основывается на обеспечении требуемых характеристик (адекватности, полноты, точности) представления и отражения текстовой информации в базы данных и базы знаний.

Задачи обработки текстовой информации, стилистические особенности документов позволяют определить уровни формализации моделей представления ЕЯ и систематизировать совокупность требуемых характеристик.

Анализ стилистических особенностей обрабатываемой текстовой информации предметной области при мониторинге сообщений позволяет упростить структуру и сложность применения внешних и внутренних управляющих правил, обеспечивающих построение ЕЯ-конструкции.

Степень детализации свойств вычисляемой информации зависит от структуры представления предметной области в БД информационной системы.

Литература

1. **Боярский К. К., Каневский Е. А., Лезин Г. В.** Концептуальные модели в базах знаний // Научно-технический вестник СПбГИТМО (ТУ). Вып. 6. Информационные, вычислительные и управляющие системы. 2002. С. 57–62.
2. **Ермаков А. Е., Плешко В. В.** Семантическая интерпретация в системах компьютерного анализа текста // Информационные технологии. 2009. № 6. С. 2–7.
3. **Тузов В. А.** Компьютерная семантика русского языка. — СПб.: Изд-во СПбГУ, 2004. — 400 с.
4. **Леонтьева Н. Н.** Роль связей в семантической разметке корпуса текстов // Тр. Междунар. конф. «Корпусная лингвистика — 2004». СПб.: Изд-во СПбГУ, 2004. С. 195–206.
5. **Лебедев И. С.** Способ формализации связей в конструкциях текста при создании естественно-языковых интерфейсов // Информационно-управляющие системы. 2007. № 3. С. 23–26.
6. **Лебедев И. С.** Построение семантически связанных информационных объектов текста // Прикладная информатика. 2007. № 5 (11). С. 83–89.
7. **Разработка** пилотной версии системы синтаксического анализа русского языка: Отчет о НИОКР/ ВНТИЦ; Руководитель работы В. В. Окатьев; Инв. № 02200803750. СПб., 2008. http://www.vntic.org.ru (дата обращения: 15.11.2010).
8. **Окатьев В. В., Ерехинская Т. Н., Скатов Д. С.** Модели и методы учета пунктуации при синтаксическом анализе предложений русского языка // Материалы Междунар. конф. «Диалог 2009», Бекасово, 27–31 мая 2009 г. М.: РГГУ, 2009. Вып. 8 (15). С. 423–429.
9. **Ронжин А. Л.** Особенности автоматического распознавания разговорной русской речи // Анализ разговорной русской речи: Тр. первого междисциплинарного семинара АРЗ-2007. СПб.: ГУАП, 2007. С. 42–55.
10. **Лебедев И. С.** Построение шаблонов кода по текстам спецификаций // Информационно-управляющие системы. 2009. № 5. С. 39–43.

УДК 685.310.11

МОДЕЛЬ СТРУКТУРНО-ФУНКЦИОНАЛЬНОГО АНАЛИЗА СОВМЕСТНОЙ ОБРАБОТКИ И ПЕРЕДАЧИ ДАННЫХ

Л. И. Гололобов,
канд. техн. наук, доцент
Военно-морской институт радиоэлектроники им. А. С. Попова

Описывается модель структурно-функционального анализа совместной обработки и передачи данных операторами и техническими средствами. В модели совмещены структура и функции с приоритетом функции над структурой.

Ключевые слова *— структура, функции, совместная обработка и передача данных.*

Деятельность оператора и функционирование техники в процессе обработки и передачи данных настолько взаимосвязаны, что их анализ раздельно на моделях подсистем «человек» и «техника» не может быть исчерпывающим.

Предлагается модель структурно-функционального анализа совместной обработки и передачи данных операторами и техническими средствами, в которой деятельность операторов и функционирование технических средств представлены как единый процесс. В модели совмещены структура и функции с приоритетом функции над структурой. Описывается структура временных затрат деятельности операторов и функционирования техники, состав и связи между операторами через используемые ими технические средства, анализируется компьютерная и информационная деятельность, индивидуальная и групповая работа, иерархическая схема взаимодействия операторов в режиме команд и докладов. Техническими средствами служат отдельные ЭВМ; ЭВМ, объединенные в локальные вычислительные сети; компьютерные сети из нескольких локальных вычислительных сетей, соединенных через систему обмена данными. Функциональность реализуется на множестве решаемых задач через детализацию действий оператора на технике. Характеристикой функционирования являются временные затраты операторов и используемых ими технических средств, представляющих в терминах производительности реактивность (время отклика) системы «человек—техника».

В данной работе акцент сделан на логику и свойства самой модели, совмещающей для анализа деятельность операторов и функционирование техники. Показано, что логика и свойства модели справедливы при любых временных затратах.

Модель построена в виде матрицы сложной структуры (табл. 1), обладает наглядностью, возможностью быстро определить проблемные места производительности.

Основным свойством модели является *совместимость* деятельности операторов и функционирования техники, чем обеспечивается анализ целостного технологического процесса обработки и передачи данных.

В работе i-го оператора ($i = 1, 2, ..., l$) можно выделить компьютерную и информационную составляющие, как две стороны деятельности. Работа с использованием клавиатуры, экрана и мыши относится к компьютерной (манипуляторной) деятельности. Решение задач характеризует информационную (содержательную) сторону деятельности.

В модели суммарные временные затраты i-го оператора и используемых им технических средств на компьютерную деятельность $T_i = X_i + F_i$ и состоят из временных затрат T_{ij} технических средств на взаимодействие i-го с j-м оператором $\left(X_i = \sum_{j=1}^{l} T_{ij} \right)$ и временных затрат i-го оператора $F_i = K_i + D_i + M_i$, где K_i — время использования i-м оператором клавиатуры, D_i — дисплея, M_i — манипулятора мышь, $i, j = 1, 2, ..., l$. Отклонение суммарных временных затрат T_i i-го оператора и технических средств от срока исполнения работ S_i в модели $Q_i = T_i - S_i$.

■ ***Таблица 1.*** *Матричная модель структурно-функционального анализа совместной обработки и передачи данных операторами и техническими средствами*

	1	2	...	j	...	l	$l+1$	$l+2$	$l+3$	$l+4$	$l+5$	$l+6$	$l+7$	$l+8$
1	T_{11}	T_{12}	...	T_{ij}		T_{1l}	X_1	K_1	D_1	M_1	F_1	T_1	Q_1	S_1
2	T_{21}	T_{22}	...	T_{2j}	...	T_{2l}	X_2	K_2	D_2	M_2	F_2	T_2	Q_2	S_2
.	.	.	...	.	...	.	.	.	.	.	.	.	.	.
i	T_{i1}	T_{i2}	...	T_{ij}	...	T_{il}	X_i	K_i	D_i	M_i	F_i	T_i	Q_i	S_i
.	.	.	...	.	...	.	.	.	.	.	.	.	.	.
l	T_{l1}	T_{l2}	...	T_{lj}	...	T_{ll}	X_l	K_l	D_l	M_l	F_l	T_l	Q_l	S_l
$l+1$	Y_1	Y_2	...	Y_j	...	Y_l		K	D	M	F	T	Q	S
$l+2$	B_1	B_2	...	B_j	...	B_l	B	0	0	0	0	0	0	0
$l+3$	U_1	U_2	...	U_j	...	U_l	U	0	0	0	0	0	0	0
$l+4$	G_1	G_2	...	G_j	...	G_l	G	0	0	0	0	0	0	0
$l+5$	W_1	W_2	...	W_j	...	W_l	W	0	0	0	0	0	0	0
$l+6$	R_1	R_2	...	R_j	...	R_l	R	0	0	0	0	0	0	0
$l+7$	V_1	V_2	...	V_j	...	V_l	V	0	0	0	0	0	0	0
$l+8$	T_1	T_2	...	T_j	...	T_l	T	0	0	0	0	0	0	0

Суммарные временные затраты всех операторов и технических средств

$$T = Z + F, Z = X, F = K + D + M,$$

где $X = \sum_{i=1}^{l} X_i$, $K = \sum_{i=1}^{l} K_i$, $D = \sum_{i=1}^{l} D_i$, $M = \sum_{i=1}^{l} M_i$;

$$T = \sum_{i=1}^{l} X_i + \sum_{i=1}^{l} F_i. \qquad (1)$$

Включенных рабочих станций — l, работающих операторов — l или меньше l.

Отклонение суммарных временных затрат для всех операторов и технических средств от сроков исполнения S равно $Q = T - S$, $Q = \sum_{i=1}^{l} Q_i$, $S = \sum_{i=1}^{l} S_i$.

Временные затраты T_j j-го оператора и используемых им технических средств на информационную деятельность представлены временными задержками T_{ji} технических средств на взаимодействие j-го с i-м оператором $\left(Y_j = \sum_{i=1}^{l} T_{ji}\right)$ и временем V_j j-го оператора, которое состоит из времени B_j на вход в систему, U_j — на работу с базами данных, G_j — формирование документа, W_j — передачу и R_j — прием документа: $T_j = Y_j + V_j$, $V_j = B_j + U_j + G_j + W_j + R_j$.

Суммарные временные затраты всех операторов и технических средств

$$T = Z + V, Z = Y, V = B + U + G + W + R,$$

где $Y = \sum_{j=1}^{l} Y_j$, $B = \sum_{j=1}^{l} B_j$, $U = \sum_{j=1}^{l} U_j$, $G = \sum_{j=1}^{l} G_j$,

$W = \sum_{j=1}^{l} W_j$, $R = \sum_{j=1}^{l} R_j$;

$$T = \sum_{j=1}^{l} Y_j + \sum_{j=1}^{l} V_j. \qquad (2)$$

Модели (1) и (2) названы моделями совместимости, так как в них реализуется *свойство совместимости* временных затрат операторов и технических средств, достигается совместимость деятельности и функционирования техники.

Очевидно, что матрица временных задержек технических средств $|T_{ij}|$ является общей для анализа временных затрат на компьютерную и информационную деятельность. Если в матрице $i = j$ и $T_{ij} \neq 0$, имеет место индивидуальная работа i-го оператора, он не взаимодействует с другими операторами. В случае $T_{ij} = 0$ и $F_i = 0$ i-я рабочая станция включена, но i-й оператор не работает. Если $i \neq j$ и $T_{ij} \neq 0$, то имеет место групповая работа (взаимодействие) операторов. Если все элементы T_{ij} матрицы $|T_{ij}|$, расположенные ниже диагональных (T_{ij}, $i = j$), равны нулю, а все или часть элементов, находящихся выше диагональных, не равны нулю, то имеет место иерархическое взаимодействие операторов в режиме команд. Если же все элементы выше диагональных равны нулю, а все или часть элементов, расположенных ниже диагональных, не равны нулю, то операторы на-

ходятся в состоянии докладов. В общем случае имеют место все виды деятельности: компьютерная и информационная, индивидуальная и групповая, режим команд и докладов.

Цель структурно-функционального анализа совместной обработки и передачи данных — выявить через отклонение Q суммарных временных затрат T операторов и технических средств от сроков исполнения S, в каком сегменте системы «человек—техника» возникли проблемы с производительностью в виде дефицита времени. Отклонение Q определяет оперативность обработки и передачи данных. Если $Q = 0$, работы выполняются в срок, при $Q < 0$ — досрочно. Если $Q > 0$, работы в установленные сроки не завершаются, возникает дефицит времени. Q — операционная напряженность, *важное свойство работ*.

Рассмотрим пример иерархического человекомашинного взаимодействия на структуре информационных задач (идентификация пользователя, работа с базами данных, формирование, передача и прием документов), которые широко распространены в вычислительных сетях.

Пусть вычислительная сеть состоит из 5 рабочих станций, в которой работают 4 оператора. Работа — решение одной или нескольких задач. Задачи между операторами распределены следующим образом:

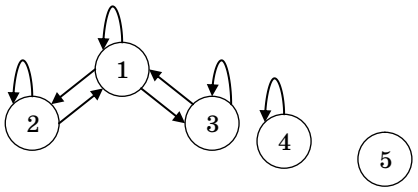
оператор 1 — 1Ф(121), 1ПК(121)2, 1Ф(109,113), 1ПК(109,113)3, 1Д(213)2, 1Д(420)3;
оператор 2 — 2К(121)1, 2Ф(213), 2ПД(213)1;
оператор 3 — 3К(109,113)1, 3Ф(420), 3ПД(420)1;
оператор 4 — 4БД(30 × 254),

где ПК(ПД) — передача команды (доклада); К(Д) — прием команды (доклада); БД — индивидуальная работа с базой данных (добавление, замена, удаление информации в базе данных); Ф — формирование документа; 1Ф(121) — оператор 1 формирует документ (команду, распоряжение и т. п.) объемом 121 символ; 1ПК(121)2 — оператор 1 посылает сообщение (команду, распоряжение и т. п.) из 121 символа оператору 2; 2К(121)1 — оператор 2 принимает сообщение (команду, распоряжение и т. п.) длиной 121 символ от оператора 1; 1Д(213)2 — оператор 1 принимает сообщение (доклад) объемом 213 символов от оператора 2; 4БД(30 × 254) — оператор 4 вводит (индивидуальная работа) в базу данных 30 записей, каждая запись длиной 254 символа, включая пробелы.

Матрица связей между операторами показана на рис. 1. Взаимодействие операторов в виде графа представлено на рис. 2. На рисунках видно, что введен 5-й фиктивный (отсутствующий) оператор для отображения в модели включенной 5-й рабочей станции.

$$\begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix} \\ \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

■ ***Рис. 1.*** *Матрица связей*



■ ***Рис. 2.*** *Граф взаимодействия операторов*

Информация о квалификации операторов, объеме обрабатываемых и передаваемых данных, сроках исполнения, характере решаемых задач и виде выполняемых работ представлена в табл. 2, где к уже имеющимся сокращениям добавлены следующие: Г — групповая работа (взаимодействие) операторов; И — индивидуальная работа оператора. Квалификация оператора записывается в виде 1(3) — низкая (1) квалификация оператора с быстродействием 3 с на обработку символа (поиск символа на клавиатуре, ввод, контроль правильности ввода на экране и замена при ошибочном вводе); 2(2,5) — средняя (2) квалификация с быстродействием оператора 2,5 с/символ; 3(2) — высокая (3) квалификация оператора с быстродействием 2 с/символ. Значения быстродействия операторов низкой, средней и высокой квалификации являются результатом тестирования работы операторов на ЭВМ [1].

Функционирование технических средств вычислительной сети описано графом на рис. 3

■ ***Таблица 2.*** *Дополнительная информация по организации работ*

Характеристика	Значения				
Номер оператора i	1	2	3	4	5
Квалификация оператора	3(2)	2(2,5)	2(2,5)	1(3)	0
Объем данных N_i, в клавиатурных символах	121, 109, 113	213	420	30 × 254	0
Срок исполнения S_i, мин	15	12	20	240	0
Характер задач	Ф, ПК, Д	К, Ф, ПД	К, Ф, ПД	БД	0
Вид работ	И, Г	Г, И	Г, И	И	0

(*1–5* — рабочие станции, *6* — среда передачи данных, *7* — сервер информационных услуг). Связи между элементами сети показаны на рис. 4.

Объем данных, обрабатываемых *i*-м оператором в рассматриваемых задачах:

$$N_i = nb_i + nu_i + ng_i + nw_i + nr_i + m1_i + m2_i + m3_i + m4_i + m5_i,$$

где число символов, обрабатываемых клавиатурой / мышью с использованием экрана: $nb_i / m1_i$ — при входе в систему; $nu_i / m2_i$ — во время работы с базой данных; $ng_i / m3_i$ — при подготовке документа; $nw_i / m4_i$ — при передаче и $nr_i / m5_i$ — приеме документа.

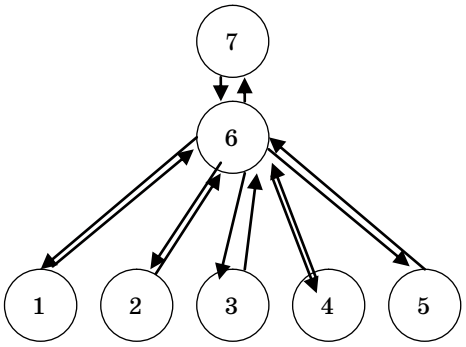
Пусть для входа в систему 1-й оператор обрабатывает $nb_1 = 27$ клавиатурных символов (имя пользователя и пароль), используя клавиатуру и экран, $m1_1 = 3$ экранных символа с помощью экрана и мыши (курсор в поле имени, в поле пароля и нажатие кнопки OK). Операторы 2, 3, 4 обрабатывают соответственно $nb_2 = 35$, $nb_3 = 31$, $nb_4 = 23$, $nb_5 = 0$ клавиатурных символов и выполняют $m1_2 = 3$, $m1_3 = 3$, $m1_4 = 3$, $m1_5 = 0$ действий мышью. Формированием документов заняты 1-, 2- и 3-й операторы. Они вводят с помощью клавиатуры и экрана соответственно $ng_1 = 343$, $ng_2 = 213$, $ng_3 = 420$ символов, оператор 4 вводит в базу данных $nu_4 = 7620$ символов. Оператор 1 высокой квалификации при вводе клавиатурных символов допускает до 5 % ошибок (заменяет до 18 символов) и 18 раз использует мышь для выделения символов, $m1_3 = 18$. Операторы 2 и 3 средней квалификации редактируют на экране до 10 % (22 из 213, 42 из 420 соответственно) и оператор 4 — до 15 % (1143 из 7620) клавиатурных символов и используют мышь до $m3_2 = 22$, $m3_3 = 42$ и $m3_4 = 1143$ раз. Если операторы 1–4 используют кнопку-команду «Сохранить» панели инструментов при наборе до 100 символов, то 1-й оператор использует мышь 4, 2-й — 3, 3-й — 5 и 4-й — до 88 раз. Во время передачи данных операторы 1–3 набирают письмо и адрес получателя (оператор 1 — из $nw_1 = 71$ и 93 символов — письмо, из 21 и 27 символов — адрес; оператор 2 — из $nw_2 = 87$ — письмо, из 20 — адрес; оператор 3 — из $nw_3 = 85$ — письмо, из 23 — адрес), присоединяют мышью файл, содержащий сформированный документ, и отправляют адресату, действуя мышью ($m4_1 = 2 \times 6$, $m4_2 = 6$, $m4_3 = 6$ раз). Для приема документов используется мышь, чтобы открыть папку «Входящие», письмо и документ к нему ($m5_1 = 2 \times 3$, $m5_2 = 3$, $m5_3 = 3$ раз). У фиктивного 5-го оператора $nb_5 = 0$, $nu_5 = 0$, $ng_5 = 0$, $nw_5 = 0$, $nr_5 = 0$ и $m1_5 - m5_5 = 0$.

Временные затраты *i*-го оператора на обработку *s*-го символа клавиатурой обозначим через $tnbklv_{is}$, $tnukl_{is}$, $tngklv_{is}$, $tnwklv_{is}$, $tnrklv_{is}$, на экране — через $tnbscr_{js}$, $tnuscr_{js}$, $tngscr_{js}$, $tnwscr_{js}$, $tnrscr_{js}$ и мышью — через $tm1_{is}$, $tm2_{is}$, $tm3_{is}$, $tm4_{is}$, $tm5_{is}$.

Допустим, что время на обработку *s*-го символа (поиск, ввод с клавиатуры, просмотр на экране, устранение ошибки, если имеет место) операторами высокой (2 с), средней (2,5 с) и низкой (3 с) квалификации в равных долях распределено между временными затратами на использование клавиатуры, экрана, мыши и соответственно равно 0,67; 0,83 и 1 с.

Объем данных, обрабатываемых *i*-м оператором с учетом отмеченной специфики, представлен в табл. 3.

С учетом данных табл. 3 временные затраты на компьютерную деятельность у 1-го оператора:



■ ***Рис. 3.*** *Граф функционирования технических средств*

$$\begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\ \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

■ ***Рис. 4.*** *Матрица связей между элементами компьютерной сети*

■ ***Таблица 3.*** *Объем обрабатываемых данных с учетом исправления ошибок*

№ оператора *i*	nb_i	nu_i	ng_i	nw_i	nr_i	$m1_i$	$m2_i$	$m3_i$	$m4_i$	$m5_i$
1	27	0	361	212	0	3	0	22	12	6
2	35	0	235	107	0	3	0	25	6	3
3	31	0	462	108	0	3	0	47	6	3
4	23	8763	0	0	0	3	1231	0	0	0
5	0	0	0	0	0	0	0	0	0	0

$$K_1 = tnbklv_1 + tnuklv_1 + tngklv_1 + tnwklv_1 + tnrklv_1 = 27 \times 0{,}67 + 0 \times 0{,}67 + 361 \times 0{,}67 + 212 \times 0{,}67 + 0 \times 0{,}67 = 600 \times 0{,}67 = 402 \text{ с};$$

$$D_1 = tnbscr_1 + tnuscr_1 + tngscr_1 + tnwscr_1 + tnrscr_1 = 27 \times 0{,}67 + 0 \times 0{,}67 + 361 \times 0{,}67 + 212 \times 0{,}67 + 0 \times 0{,}67 = 402 \text{ с};$$

$$M_1 = tm1_1 + tm2_1 + tm3_1 + tm4_1 + tm5_1 = 3 \times 0{,}67 + 0 \times 0{,}67 + 22 \times 0{,}67 + 12 \times 0{,}67 + 6 \times 0{,}67 = 43 \times 0{,}67 = 28{,}81 \text{ с};$$

$$F_1 = K_1 + D_1 + M_1 = 402 + 402 + 28{,}81 = 832{,}81 \text{ с}.$$

Временные затраты на компьютерную деятельность 2-, 3- и 4-го операторов вычисляются аналогично и соответственно равны:

$K_2 = 312{,}91$ с	$D_2 = 312{,}91$ с
$K_3 = 498{,}83$ с	$D_3 = 498{,}83$ с
$K_4 = 8786$ с	$D_4 = 8786$ с
$M_2 = 30{,}71$ с	$F_2 = 656{,}53$ с
$M_3 = 48{,}97$ с	$F_3 = 1046{,}63$ с
$M_4 = 1234$ с	$F_4 = 18806$ с

Такой показатель производительности технических средств как реактивность существенно влияет на поведение оператора. Согласно исследованиям Миллера [2], возможны следующие варианты поведения в зависимости от времени отклика:

— 0,1 с считается пределом, до которого оператор полагает, что технические средства на его действия реагируют мгновенно, т. е. кроме отображения результатов никакой другой обратной связи не требуется;

— если время отклика находится в пределах от 0,1 до 1 с, поведение оператора не меняется, хотя он и замечает задержку и у него теряется ощущение непосредственной работы с данными;

— пока время отклика остается в пределах 1–10 с, внимание оператора еще сосредоточено на работе с данными; если оно превышено, оператор отвлекается на другие дела в ожидании завершения процесса, в этом случае необходима обратная связь с процессом, чтобы оператор знал, чего ему ожидать.

Задержки более 10 с отрицательно влияют на обработку и передачу данных в темпе проводимых мероприятий.

Пусть в процессе обработки и передачи данных временные затраты технических средств, используемых операторами в компьютерной деятельности (загруженность сети низкая: работают всего 4 оператора, объем обрабатываемых и передаваемых данных для сети мал), оказались равными

$$\begin{bmatrix} T_{11}T_{12}T_{13}T_{14}T_{15} \\ T_{21}T_{22}T_{23}T_{24}T_{25} \\ T_{31}T_{32}T_{33}T_{34}T_{35} \\ T_{41}T_{42}T_{43}T_{44}T_{45} \\ T_{51}T_{52}T_{53}T_{54}T_{55} \end{bmatrix} = \begin{bmatrix} 0{,}023 & 0{,}019 & 0{,}032 & 0 & 0 \\ 0{,}011 & 0{,}009 & 0 & 0 & 0 \\ 0{,}047 & 0 & 0{,}031 & 0 & 0 \\ 0 & 0 & 0 & 0{,}097 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Суммарные временные затраты операторов и технических средств:

$$T_1 = X_1 + F_1 = 0{,}074 + 832{,}81 = 832{,}884 \text{ с};$$
$$T_2 = X_2 + F_2 = 0{,}020 + 656{,}53 = 656{,}55 \text{ с};$$
$$T_3 = X_3 + F_3 = 0{,}078 + 1046{,}63 = 1046{,}708 \text{ с};$$
$$T_4 = X_4 + F_4 = 0{,}097 + 18806 = 18\,806{,}097 \text{ с};$$
$$T = X + F = 21\,342{,}239 \text{ с}.$$

Временные затраты на информационную деятельность 1-го оператора:

$$B_1 = tnbklv_1 + tnbscr_1 + tm1_1 = 27 \times 0{,}67 + 27 \times 0{,}67 + 3 \times 0{,}67 = 57 \times 0{,}67 = 38{,}19 \text{ с};$$

$$U_1 = tnuklv_1 + tnuscr_1 + tm2_1 = 0 \times 0{,}67 + 0 \times 0{,}67 + 0 \times 0{,}67 = 0 \text{ с};$$

$$G_1 = tngklv_1 + tngscr_1 + tm3_1 = 361 \times 0{,}67 + 361 \times 0{,}67 + 22 \times 0{,}67 = 744 \times 0{,}67 = 498{,}48 \text{ с};$$

$$W_1 = tnwklv_1 + tnwscr_1 + tm4_1 = 212 \times 0{,}67 + 212 \times 0{,}67 + 12 \times 0{,}67 = 436 \times 0{,}67 = 292{,}12 \text{ с};$$

$$R_1 = tnrklv_1 + tnrscr_1 + tm5_1 = 0 \times 0{,}67 + 0 \times 0{,}67 + 6 \times 0{,}67 = 4{,}02 \text{ с};$$

$$V_1 = B_1 + U_1 + G_1 + W_1 + R_1 = 38{,}19 + 0 + 498{,}48 + 292{,}12 + 4{,}02 = 832{,}81 \text{ с}.$$

Аналогично временные затраты на информационную деятельность 2-, 3- и 4-го операторов:

$B_2 = 60{,}59$ с	$U_2 = 0$ с	$G_2 = 410{,}85$ с
$B_3 = 53{,}95$ с	$U_3 = 0$ с	$G_3 = 805{,}93$ с
$B_4 = 49$ с	$U_4 = 18757$ с	$G_4 = 0$ с
$W_2 = 182{,}6$ с	$R_2 = 2{,}49$ с	$V_2 = 656{,}53$ с
$W_3 = 184{,}26$ с	$R_3 = 2{,}49$ с	$V_3 = 1081{,}19$ с
$W_4 = 0$ с	$R_4 = 0$ с	$V_4 = 18806$ с

Временные затраты технических средств на информационную деятельность получены транспонированием матрицы

$$\begin{bmatrix} T_{11}T_{12}T_{13}T_{14}T_{15} \\ T_{21}T_{22}T_{23}T_{24}T_{25} \\ T_{31}T_{32}T_{33}T_{34}T_{35} \\ T_{41}T_{42}T_{43}T_{44}T_{45} \\ T_{51}T_{52}T_{53}T_{54}T_{55} \end{bmatrix}$$ в матрицу

$$\begin{bmatrix} T_{11}T_{21}T_{31}T_{41}T_{51} \\ T_{12}T_{22}T_{32}T_{42}T_{52} \\ T_{13}T_{23}T_{33}T_{43}T_{53} \\ T_{14}T_{24}T_{34}T_{44}T_{54} \\ T_{15}T_{25}T_{35}T_{45}T_{55} \end{bmatrix} = \begin{bmatrix} 0{,}023 & 0{,}011 & 0{,}047 & 0 & 0 \\ 0{,}019 & 0{,}009 & 0 & 0 & 0 \\ 0{,}032 & 0 & 0{,}031 & 0 & 0 \\ 0 & 0 & 0 & 0{,}097 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Суммарные временные затраты операторов и технических средств на информационную деятельность:

$$T_1 = Y_1 + V_1 = 0{,}074 + 832{,}81 = 832{,}884 \text{ с};$$

■ ***Таблица 4.*** *Временные затраты совместной обработки и передачи данных*

	1	2	3	4		*X*	*K*	*D*	*M*	*F*	*T*	*Q*	*S*
1	0,023	0,019	0,032	0	0	0,074	402	402	28,81	832,81	832,884	−67,116	900
2	0,011	0,009	0	0	0	0,020	312,91	312,91	30,71	656,53	656,55	−63,45	720
3	0,047	0	0,031	0	0	0,078	498,83	498,83	48,97	1046,63	1046,708	−153,292	1200
4	0	0	0	0,097	0	0,097	8786	8786	1234	18806	18806,097	**4406,097**	14400
5	0	0	0	0	0	0	0	0	0	0	0	**0**	0
Y	0,081	0,028	0,063	0,097	0	0,269	9999,74	999,74	1342,49	21341,97	**21342,239**	**4122,239**	17220
B	38,19	60,59	53,95	49	0	201,73	0	0	0	0	0	0	0
U	0	0	0	18757	0	18757	0	0	0	0	0	0	0
G	498,48	410,85	805,93	0	0	1749,82	0	0	0	0	0	0	0
W	292,12	182,6	184,26	0	0	658,98	0	0	0	0	0	0	0
R	4,02	2,49	2,49	0	0	9	0	0	0	0	0	0	0
V	832,81	656,53	1046,63	18806	0	21341,97	0	0	0	0	0	0	0
T	832,884	656,55	1046,708	18806,097	0	**21342,239**	0	0	0	0	0	0	0

$$T_2 = Y_2 + V_2 = 0{,}020 + 656{,}53 = 656{,}55 \text{ с};$$

$$T_3 = Y_3 + V_3 = 0{,}079 + 1046{,}63 = 1046{,}708 \text{ с};$$

$$T_4 = Y_4 + V_4 = 0{,}025 + 18\,806 = 18\,806{,}097 \text{ с};$$

$$T = Y + V = 0{,}197 + 21\,341{,}97 = 21\,342{,}239 \text{ с}.$$

Из расчетов и табличного распределения (табл. 4) временных затрат видно, что суммарные временные затраты операторов и технических средств на компьютерную деятельность ($X + F = 21\,342{,}239$ с) равны суммарным временным затратам операторов и техники ($Y + V = 21\,342{,}239$ с) на информационную деятельность. Важность *свойства взаимной однозначности* временных затрат заключается в том, что анализ совместной обработки и передачи данных можно проводить, используя компьютерную или информационную составляющие процесса или обе одновременно.

Из анализа временных затрат совместной обработки и передачи данных видно (см. табл. 4), что операторы 1–3 завершили работу досрочно ($Q_i < 0$, $i = 1 - 3$, $Q_1 = -67{,}116$ с, $Q_2 = -63{,}45$ с, $Q_3 = -153{,}292$ с). У 4-го оператора появился большой дефицит времени ($Q_4 > 0$, $Q_4 = 4406{,}097$ с) и оперативная напряженность в работе. Очевидно, что проблема с производительностью возникла в сегменте системы «человек—техника», связанном по времени с обновлением баз данных.

На параметры совместной обработки и передачи данных (показатели производительности системы «человек—техника») воздействуют внешние и внутрисистемные факторы.

К внешним факторам, прежде всего, относятся размах и темп проводимых мероприятий. Масштабы мероприятий обуславливают объем обрабатываемых и передаваемых данных, темп — сроки исполнения.

К внутрисистемным факторам следует отнести объем обрабатываемых и передаваемых данных, сроки исполнения работ, состав, квалификацию и структуру взаимодействия операторов, допустимые временные затраты на обработку данных, продолжительность работы операторов, состав решаемых задач, тип подключений к компьютерной сети, характеристики программно-аппаратного обеспечения клиента и сервера в распределенной обработке данных, возможности среды передачи данных и другие факторы.

Очевидно, что объем данных и сроки исполнения в системе «человек—техника» изменить невозможно. На другие внутрисистемные факторы влияют рациональным выбором ресурсов системы «человек—техника» под процесс совместной обработки и передачи данных. Оценка результатов выбора проводится с использованием модели структурно-функционального анализа.

Предлагаемое технологическое решение в виде модели структурно-функционального анализа, в которой реализована идея совместимости работы человека на технике и функционирования технических средств, дает возможность исследовать обработку и передачу данных как целостный процесс, адекватный технологическому единству людей, информации и техники, и выявлять проблемы производительности комплексно с учетом деятельности и функционирования техники.

Литература

1. **Ротштейн А. П., Кузнецов П. Д.** Проектирование бездефектных человекомашинных технологий. — Киев: Техника, 1992. — 180 с.
2. **Тестирование** производительности Web-приложений Microsoft.NET: пер. с англ. — М.: Русская редакция, 2003. — 352 с.

УДК 004.492.3

АЛГОРИТМ ОБНАРУЖЕНИЯ И ОБХОДА АНТИОТЛАДОЧНЫХ И АНТИЭМУЛЯЦИОННЫХ ПРИЕМОВ

А. Е. Антонов,
аспирант
А. С. Федулов,
доктор техн. наук, профессор
Смоленский филиал Московского энергетического института (технического университета)

Проведен обзор принципов работы отладчиков и эмуляторов, их уязвимостей. Предложен новый алгоритм обнаружения антиотладочных и антиэмуляционных приемов, а также модификация отладчика для задач анализа вредоносного кода.

Ключевые слова *— эмулятор, отладчик, антиотладочные и антиэмуляционные приемы, вредоносное программное обеспечение.*

Введение

Одним из эффективных методов анализа вредоносного программного обеспечения (ПО) является выполнение кода в среде отладчика или эмулятора. Отладчики обычно используются как инструмент вирусного аналитика, в свою очередь эмуляторы встраиваются в антивирусные продукты для автоматического поиска опасного или нежелательного ПО. Действительно, ряд задач анализа вредоносного кода, например поиск полиморфных вирусов, можно решить, только запустив программный код на выполнение и отслеживая результаты его работы. Чтобы препятствовать работе отладчиков и эмуляторов, авторами вредоносного кода разработан ряд методов. В настоящее время поиск и деактивация таких методов может быть эффективно проведена только в ручном режиме при тщательном анализе алгоритма защиты. В работе предложен алгоритм для обнаружения защищенного от отладчиков и эмуляторов кода. Предлагаемый алгоритм не только облегчает поиск антиотладочных и антиэмуляционных приемов, но и может работать в автоматическом режиме (без участия аналитика).

Принципы работы и уязвимости отладчика и эмулятора

Отладчик — приложение, которое либо перехватывает окружение отлаживаемой программы во время ее выполнения, либо исполняет ее в виртуальной машине, таким образом помогая находить ошибки. Отладчик позволяет контролировать окружение выполнения (например, память), в котором функционирует отлаживаемая программа [1, с. 627]. В дальнейшем под отладчиком мы будем понимать приложение, работающее в том же окружении, что и отлаживаемая программа, и использующее отладочные возможности процессора и операционной системы (ОС).

Существуют две разновидности отладчиков — пользовательского режима и режима ядра [2, с. 143]. Первые в большинстве своем используют функции ОС, например интерфейс отладки *Debug API* (*Application Program Interface*) ОС Windows, вторые — непосредственно возможности отладки процессоров. Далее в работе рассматривается архитектура процессора x86 и ОС Windows как наиболее распространенные.

Любой отладчик должен обеспечивать трассировку приложения и установку точек останова. Трассировка обычно задается выбором специального режима процессора (при котором после каждой инструкции управление передается отладчику). Существует три типа точек останова [3]: аппаратные — используют специальные отладочные регистры, программные — вставляют в выполняемый код специальные команды останова (int 3) и на доступ к памяти — изменяют атрибут доступа к странице памяти и при обращении к ней производят обработку.

Для защиты от отладчика программа может использовать следующие методы [4, с. 226]:

1) проверку регистров, флагов процессора, отвечающих за аппаратную отладку, например проверку того, установлен ли флаг трассировки (*Trace Flag — TF*), а также изменение этих флагов и регистров, что может вести к аварийному завершению отладчика;

2) проверку целостности кода для защиты от программных точек прерывания;

3) поиск структур отладчика в памяти, например в контексте потока (*Thread Infomation Block*) — для этой цели можно использовать функцию *IsDebuggerPresent* (*Debug API* ОС Windows);

4) поиск конкретных отладчиков в системе.

В основе эмулятора лежит другой принцип работы. Эмулятор — это система, имитирующая работу процессора, оперативной памяти, аппаратного обеспечения и ОС [5, с. 279]. В общем случае эмулятор может имитировать ту же систему, на которой он запущен. Таким образом, его можно использовать при анализе вредоносного ПО, поскольку программа, исполняемая в эмуляторе, не может влиять на реальную систему [5]. Далее мы будем рассматривать эмуляторы для имитации выполнения программ переносимого формата исполняемых файлов (*Portable Executable*), работающих в ОС Windows.

Эмулятор загружает программный код в буфер и, читая последовательно инструкции, имитирует их выполнение. При этом все изменения происходят в переменных эмулятора (виртуальные регистры, виртуальный стек, буфер с программой), а не на реальной машине. Процесс имитации проходит в несколько этапов [6]:

- анализ — выявляет размер, параметры имитируемой инструкции;
- пересчет адресов — должен быть выполнен для всех инструкций, обращающихся к памяти, поскольку нет практической возможности загрузить программу в буфер по адресу, который бы она имела, исполняясь на реальной машине;
- проверка адресов — выявляет ошибки адресации;
- проверка дополнительных условий (например, для операции div — деление — эмулятор проверяет неравенство операнда нулю);
- непосредственно имитация инструкции, при которой эмулятор согласно коду инструкции меняет состояние виртуальных регистров, виртуального стека и буфера с кодом и данными программы;
- перевод указателя инструкций (*Extended Instruction Pointer — EIP*) на следующую команду.

Принципиально алгоритм работы эмулятора имеет два существенных недостатка: значительное время имитации команды по сравнению с ее выполнением на реальной машине и сложность правильного имитирования всевозможных инструкций процессора и функций ОС. Для полной эмуляции ОС фактически необходимо переписать все ее функции заново. Исходя из этих недостатков программа может предпринять следующие атаки на эмулятор, чтобы обнаружить его или прекратить эмуляцию [4]:

- использовать неизвестные эмулятору команды процессора (например, MMX, SSE, SSE2 или недокументированные инструкции). Не зная текущую команду, эмулятор не сможет продолжить выполнение кода;
- использовать команды, реализованные в эмуляторе, с ошибками (если команда выполняется ошибочно, то последующая работа программ будет некорректна);
- использовать неизвестные эмулятору возможности системы (имитировать все API-функции ОС Windows практически невозможно);
- реализовать длинные циклы, вычисляющие какой-либо параметр для исполняемого кода. На реальной машине такой код будет выполняться достаточно быстро, а эмуляция подобных циклов займет значительное время (для имитации одной команды процессора требуется выполнить десятки или даже сотни инструкций).

Антиотладочные и антиэмуляционные приемы в значительной мере распространены во вредоносном ПО. На данный момент для их обнаружения может быть использован сигнатурный анализ для поиска подозрительных мест по известным сигнатурам. Также в некоторых случаях эмулятор или отладчик может сообщить о потенциальном антиотладочном приеме. Эмулятор, например, может встретить неизвестную команду, которую расценит как попытку антиэмуляции. Отладчик может дополнительно проверять, не сбросила ли программа флаги и регистры отладки. Однако описанные методы не способны находить новые антиотладочные приемы, неизвестные на момент создания отладчика или эмулятора, что во многом затрудняет анализ вредоносного ПО.

Алгоритм обнаружения новых антиэмуляционных и антиотладочных приемов

Как видно из приведенного выше описания, методы защиты от отладчиков и эмуляторов используют различные механизмы. На основании этого предлагается алгоритм поиска новых антиотладочных и антиэмуляционных приемов, заключающийся в сравнении работы одного и того же кода в отладчике и эмуляторе. Действительно, приемы для обхода отладчика во многих случаях будут успешно выполняться в среде эмулятора. И наоборот, код, который невозможно ис-

полнить в эмуляторе, будет корректно работать в отладчике.

Рассмотрим особенности алгоритма для поиска антиотладочных и антиэмуляционных приемов. На каждом шаге работы выполняется одна инструкция в среде эмулятора и отладчика и сравнивается результат ее выполнения. Инструкции процессора x86 могут влиять на регистры (в том числе на регистр флагов и на EIP), а также на содержимое оперативной памяти.

В простейшем случае нам достаточно сравнивать указатель инструкций. Его расхождение будет означать, что программа исполняется по разным веткам алгоритма, что в свою очередь говорит об ошибочности работы отладчика или эмулятора. Однако легко сформировать атаку против такого отладчика-эмулятора (листинг 1).

Листинг 1. *Алгоритм обнаружения отладчика-эмулятора, проверяющего только значение EIP.*

```
EAX = 1, если присутствует отладчик, иначе 0
ECX = 1, если обнаружен эмулятор, иначе 0
EAX = EAX + ECX
если EAX<>0, обнаружен отладчик или эмулятор
```

Следовательно, необходимо также сравнение и регистров общего назначения, и регистра флагов на каждом шаге. Для частных случаев возможно организовать обман предложенного метода, при котором значения регистров (в том числе регистра флагов и EIP) будут одинаковы, а различаться будут только состояния памяти (листинг 2). Поэтому для надежности и отсечения подобных вариантов следует производить сравнение содержимого памяти после некоторых, изменяющих ее, инструкций. Например, к «опасным» инструкциям можно отнести те, которые не содержат в качестве операнда регистры (stos, lods, movs, cmps и ряд других), а также сложные инструкции, которые могут быть реализованы в эмуляторе не полностью или с ошибками.

Листинг 2. *Пример обмана эмулятора-отладчика, проверяющего целостность кода и работоспособность инструкции add.*

```
Start:
    mov ecx,End-Start+4 ; +4, чтобы захватить переменную for_add
    mov edi,Start
    mov esi, DataCopy
    add dword [for_add],0FFFFFFFFh ; for_add = 0
    ;Предполагается, что инструкция
    ;ADD реализована в эмуляторе с ошибкой
    ;и в случае переполнения операнда не производит сложения.
    repe cmpsb ; Сравнивать байты по адресам EDI и ESI,
                ; пока они равны
    jnz EmulatorDebuggerDetected
    jmp NotDetected
End:
    for_add dd 1
CodeCopyStart:
    Точная копия байт от Start до End, для сравнения.
CodeCopyEnd:
    for_add_test dd 0
```

К достоинствам алгоритма для поиска антиотладочных и антиэмуляционных приемов относятся:

1) возможность находить новые, ранее неизвестные антиотладочные или антиэмуляционные приемы в автоматическом режиме;

2) локализация местонахождения приема, вызвавшего расхождение. Действительно, для обнаружения антиотладочного или антиэмуляционного приема аналитику достаточно проанализировать последовательность инструкций, выполненных до расхождения и ведущих к разным состояниям отладчика и эмулятора;

3) устойчивость к приемам, направленным против виртуальных машин.

Недостатки данного алгоритма:

1) он не способен без дополнительного анализа отличить антиотладочные приемы от антиэмуляционных. В качестве средств дополнительного анализа могут быть использованы, например, сигнатурный или эвристический анализ. Эвристический анализ может, в частности, учитывать тот факт, что исследуемая программа после обнаружения отладчика или эмулятора обычно сразу завершается, а в противном случае выполняет свои функции;

2) за антиэмуляционный прием может быть принята случайная ошибка в эмуляторе, ведущая к неправильному выполнению инструкции процессора и, как следствие, к расхождению выполнения кода в предложенном алгоритме. Однако вероятность такой ошибки уменьшается с улучшением качества эмулятора;

3) скорость выполнения кода при анализе в предложенном алгоритме меньше, чем в эмуляторе и отладчике. Действительно, после каждой операции необходимо проводить дополнительное сравнение полученных результатов, что требует определенных временных затрат. Поэтому алгоритм не способен обнаруживать атаки, использующие тот факт, что в эмуляторе код выполняется значительно медленнее, чем на реальной машине. Для обнаружения таких атак необходимо использовать другие методы.

Итак, предлагаемый алгоритм способен в автоматическом режиме обнаруживать новые антиотладочные и антиэмуляционные приемы, а также помогает их локализовать для дополнительного анализа экспертом.

Реализация программы для поиска антиотладочных и антиэмуляционных приемов

Для демонстрации предлагаемого алгоритма была реализована программа, осуществляющая поиск антиотладочных и антиэмуляционных приемов в автоматическом режиме.

Для отладки анализируемого кода используется отладочной интерфейс *Windows Debug API*, выполняющий программу в пошаговом режиме (установлен *TF*). Для имитации инструкций используется модифицированный эмулятор от свободно распространяемого антивируса *Exploision Antivirus v.11*. Рассмотрим некоторые особенности реализации.

• Значение регистров эмулятора при запуске инициализируется регистрами отладчика. Это необходимо для последующей проверки регистров на эквивалентность.

• Эмулятор имитирует расположение стека по адресу стека отладчика. Это необходимо для эквивалентности указателя стека (*Extended Stack Pointer*).

• Эмулятор пересчитывает регистр EIP, имитируя расположение кода по базовому адресу образа (*ImageBase*), хотя реально код расположен по другому адресу.

• В процессе выполнения программа не сверяет *TF* регистра флагов.

• Для упрощения разработки сравнение участков памяти не осуществляется.

Проведем демонстрацию предложенного алгоритма обнаружения обманных приемов на примерах.

Пример 1. Защищенный код сверяет значение *TF* и, в случае если он установлен, сообщает об отладке (листинг 3). После сравнения *TF* исследуемый код продолжит выполняться по разным путям в отладчике и эмуляторе, что и обнаружит разработанное приложение.

Листинг 3. *Поиск отладчика по флагу трассировки.*

```
pushfd          ;сохраним регистр флагов в стек
pop eax         ;загрузим его в EAX
and eax,$100    ;сбросим все, кроме TF
test eax,eax    ;проверим, установлен ли TF
jnz .Debug      ;если установлен, нас отлаживают
```

Пример 2. В структуре блока переменных окружения процесса (*Process Enviroment Block — PEB*) есть поле *NtGlobalFlag*, которое может использоваться для выявления отладчика. Это поле находится по смещению 0x68 от начала *PEB*. Поле представлено рядом флагов. Значение, которое предполагает присутствие отладчика, складывается из значений следующих полей:

• FLG_HEAP_ENABLE_TAIL_CHECK (0x10)

• FLG_HEAP_ENABLE_FREE_CHECK (0x20)

• FLG_HEAP_VALIDATE_PARAMETERS (0x40)

Листинг 4. *Поиск отладчика с помощью NtGlobalFlag.*

```
mov eax,[fs:30h]
mov al, [eax+68h]
and al,70h
cmp al,70h
je .Debug
```

После команды mov al, [eax+68h] регистр al будет содержать разные значения в отладчике и эмуляторе, что обнаружит антиотладочный прием.

Пример 3. Воспользуемся приемом CALL-POP для определения реального адреса кода. Поскольку в эмуляторе код будет загружен по адресу, отличному от *ImageBase*, сравнивая «виртуальное» расположение кода с реальным, мы можем обнаружить наличие эмулятора (листинг 5). Реализованная программа успешно находит такой прием.

Листинг 5. *Обнаружение эмулятора по реальному адресу расположения кода.*

```
    call .Next      ;call-pop прием
.Next:
    pop eax         ;в EAX — адрес указателя .Next
    cmp eax,.Next   ;сравним EAX с реальным расположением
    jnz .Emul       ;переход, если мы в эмуляторе
```

Пример 4. Следующий прием (листинг 6) использует системное прерывание int 2e + inc edx для выявления отладчика. Поскольку эмулятор не может правильно выполнить команду, содержимое регистра eax будет отличаться в отладчике и эмуляторе, что обнаружит антиэмуляционный прием.

Листинг 6. *Обнаружение эмулятора по реальному адресу расположения кода.*

```
    mov eax,-1
    int 2eh ;это прерывание неправильно выполняется в эмуляторе
dt_:
    inc edx ;в отладчике int 2eh + inc edx выполнится как одна
команда (системное прерывание), и вернет значение 0xC000001C
    cmp eax, 0xc000001c ; STATUS_INVALID_SYSTEM_SERVICE
    jnz .aniEmu
;Переход если код выполняется в эмуляторе
```

Итак, разработанное приложение способно обнаруживать ряд обманных приемов.

Модификация отладчика для анализа вредоносного программного обеспечения

Поиск приемов обхода отладчика или эмулятора не всегда является целью. Во многих случаях (например, для поиска и анализа вредоносного кода) более важно имитировать правильное исполнение кода, обходя всевозможные защиты. В настоящее время некоторые отладчики (*OllyDebugger*, *Syser* [3]) применяют специальный метод анти-антиотладки. В процессе выполнения программы отладчик, используя сигнатурный анализ, пытается обнаружить известные ему антиотладочные приемы и подменяет результат их работы, таким образом не давая обнаружить свое присутствие. Однако таким методом можно обнаруживать только предопределенные антиотладочные приемы.

Для обхода антиотладочных приемов возможно дополнительно использовать предложенный

ранее алгоритм одновременного выполнения кода в отладчике и эмуляторе.

• Если программа отлаживается в ручном режиме, аналитику возможно выдавать сообщение о наличии расхождения регистров, памяти в отладчике или эмуляторе. Также возможно в диалоговом режиме предложить использовать значение регистров отладчика или эмулятора для дальнейшего исследования программы.

• Если исследование производится в автоматическом режиме, например для определения степени опасности ПО, то в случае наличия расхождения система может инициировать в памяти еще одну копию отладчика и эмулятора. Первая пара отладчик—эмулятор инициируется значениями регистров и памяти отладчика, вторая — эмулятора. Преимуществами данной модификации отладчика являются:

— незначительная, в сравнении с виртуальными машинами, ресурсоемкость;

— увеличенная устойчивость к антиотладочным приемам.

Недостатки обусловлены недостатками описанного в первой части статьи алгоритма:

— меньшая, по сравнению с отладчиком, скорость работы;

— подверженность случайным ошибкам, не являющимся антиотладочными или антиэмуляционными приемами, что может привести к увеличению затрат времени на дополнительный анализ.

Заключение

В работе проведен анализ наиболее существенных принципов построения и уязвимостей отладчиков и эмуляторов с точки зрения их использования во вредоносном ПО.

По итогам проведенного анализа предложен новый алгоритм детектирования антиотладочных и антиэмуляционных приемов, основанный на параллельном выполнении кода в отладчике и эмуляторе. Алгоритм был реализован программно. Рядом примеров проиллюстрирована его работоспособность.

Результаты работы могут быть использованы для более эффективного анализа вредоносного кода.

Литература

1. **Foster J. C., Price M.** Sockets, Shellcode, Porting, and Coding. — Syngress, 2005. — 667 p.
2. **Робинс Д.** Отладка приложений для Microsoft .NET и Microsoft Windows: пер. с англ. — М.: Русская Редакция, 2004. — 736 с.
3. **Касперски К.** Энциклопедия антиотладочных приемов // Хакер. 2008. № 11–16.
4. **Szor P.** The art of computer virus research and defense. — Addison-Wesley Professional, 2005. — 744 p.
5. **Mollin R. A.** Introduction to Cryptography. Second ed. — Taylor&Francis, 2006. — 413 p.
6. **Агафонов А.** Эмуляция программного кода // UINC.RU: Underground Information Center, 2004. http://www.uinc.ru/articles/47/ (дата обращения: 10.12.09).

УДК 681.322

МНОГОАЛФАВИТНЫЙ БЛОЧНЫЙ ШИФР СО СКРЫТОЙ НУМЕРАЦИЕЙ БЛОКОВ

А. П. Алексеев,
канд. техн. наук, доцент
М. И. Макаров,
аспирант
Поволжский государственный университет телекоммуникаций и информатики

Рассматривается шифр многоалфавитной замены, основанный на интегральном преобразовании, работа которого строится таким образом, чтобы выходное распределение чисел криптограммы было равномерным. В шифре используется дробление криптограммы на блоки, скрытая нумерация каждого блока и пересылка блоков по нескольким каналам связи.

Ключевые слова *— криптография, стеганография, адаптивный многоалфавитный шифр, пространственно-временной метод распыления информации.*

Введение

Шифры одноалфавитной замены не являются криптостойкими. Значительно надежнее шифры многоалфавитной замены. В этих шифрах каждому символу открытого текста ставится в соответствие не один, а несколько символов алфавита замены. Многоалфавитные шифры замены повышают криптостойкость. Тем не менее существует возможность взлома и многоалфавитных шифров, которые продолжают наследовать статистическую картину распределения частоты появления символов открытого текста.

Представляет интерес разработка и совершенствование криптостойких шифров многоалфавитной замены, для чего может быть использован различный математический аппарат, например интегральное исчисление.

Для увеличения криптостойкости шифра предлагается с помощью многоалфавитной замены и интегральных преобразований обеспечить равномерное распределение числовых данных криптограммы, разбить криптограмму на блоки различной длины, скрытно пронумеровать блоки и передать их по разным каналам связи.

Разработка шифра многоалфавитной замены

Основная идея построения шифра заключается в формировании криптограммы в виде равномерной смеси вещественных чисел.

Равномерность распределения вещественных чисел в криптограмме достигается тем, что в процессе шифрования ведется анализ получающегося распределения чисел шифрограммы. С этой целью непрерывно строится гистограмма распределения. При этом очередные элементы шифровки формируются таким образом, чтобы они попали в те места распределения, где наблюдаются провалы (глобальные минимумы). Возможность изменять (варьировать) положение очередного элемента криптограммы на числовой оси имеется благодаря тому, что при шифровании используются многоалфавитная замена и интегральное преобразование [1].

Алгоритм шифрования таков, что осуществляется непрерывный анализ выходного распределения и выполняется такая коррекция (адаптация) шифра, при которой обеспечивается приближение формируемых чисел к равномерному закону распределения.

Многоалфавитное шифрование предполагает, что каждый символ открытого текста многократно встречается в таблице замен на различных участках числовой оси. В табл. 1 приведен фрагмент некоторой упрощенной таблицы многоалфавитной замены (ТМЗ). При этом считается, что буква «е» встречается в открытом тексте чаще, а буква «д» — реже других. По этой причине для буквы «е» выделено 6 интервалов многоалфавитной замены, а для буквы «д» — только 2.

Рассмотрим, как осуществляется шифрование с помощью ТМЗ. Предположим, что нужно

■ ***Таблица 1***. *Фрагмент ТМЗ*

Интервалы замены в алфавите открытого текста					
а	б	в	г	д	е
[5...6)	[2...3)	[4...5)	[3...4)	[1...2)	[6...7)
[8...9)	[10...11)	[11...12)	[7...8)	[9...10)	[12...13)
[13...14)	[14...15)	[17...18)	[15...16)	–	[16...17)
[18...19)	–	[21....22)	[20...21)	–	[19...20)
[23...24)	–	–	–	–	[22...23)
–	–	–	–	–	[24...25)

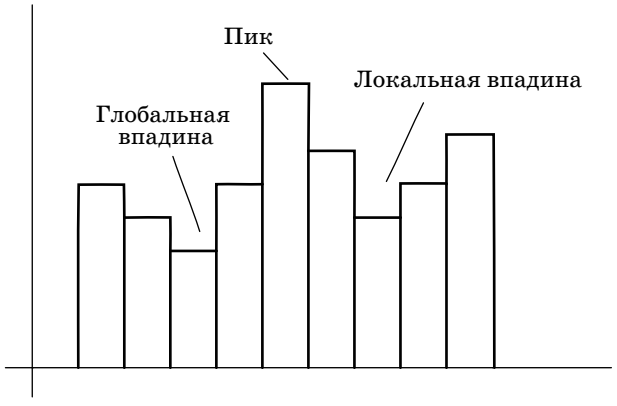
зашифровать фразу «где абба». Шифровку можно создать бесконечным числом способов. При этом каждую букву допустимо заменять любым вещественным числом из указанных интервалов. Приведем две криптограммы для указанной фразы:

1) 15,33 — 9,101 — 22,99 — 18,06 — 14,57 — 2,331 — 5,064;

2) 7,105 — 1,102 — 12,98 — 8,473 — 10,16 — 14,91 — 23,26.

В предлагаемом шифре после многоалфавитной замены осуществляется интегральное преобразование каждого полученного числа. Это дает возможность один из пределов интегрирования выбирать по случайному закону [2]. При этом нужно находить очередной предел интегрирования таким образом, чтобы формируемое число криптограммы попало в зону наибольшего провала (в зону глобальной впадины) на гистограмме.

Для шифрования адаптивным (подстраиваемым) шифром необходимо постоянно решать такую задачу: по найденному числу в выходном распределении выбирать такое значение предела интегрирования, которое обязательно попадет в заданный интервал гистограммы. Эту идею иллюстрирует рис. 1. После зашифрования очередного символа гистограмма достраивается (пополняется). На гистограмме выделяется максимальное значение (пик), минимальное значение (глобальная впадина) и провалы (локальные впадины). Формирование криптограммы ведется так, чтобы с максимально возможной степенью выровнять имеющееся выходное распределение.



■ ***Рис. 1***. *Гистограмма выходного распределения*

Предположим, что наибольший провал на гистограмме наблюдается в интервале чисел $[c_i, c_{i+1}]$. Пусть при этом для интегрального преобразования используется некоторая подынтегральная функция $f(x)$:

$$I = \int_a^b f(x)\mathrm{d}x.$$

Для того чтобы уменьшить глубину глобальной впадины на гистограмме, генерируют случайное число a из интервала $[c_i, c_{i+1}]$. По ТМЗ определяется значение интеграла I, которое соответствует шифруемому символу. По известному значению нижнего предела интегрирования a и величине интеграла I находят значение верхнего предела интегрирования b:

$$b = \varphi(a, I).$$

Полученные числа a и b передают в линию. Эти числа являются элементами криптограммы (шифровкой). Заметим, что пределы интегрирования можно формировать и в обратном порядке: сначала выбирать b, а потом вычислять a.

На приемной стороне известны вид использованного интегрального преобразования (подынтегральная функция) и конфигурация ТМЗ. Эти два элемента определяются секретным сеансовым ключом. Поэтому процесс дешифрации криптограммы не вызывает затруднений. Он сводится к вычислению определенного интеграла по известным значениям нижнего и верхнего пределов интегрирования и определению принятого символа по ТМЗ.

Таким образом, сформированная величина a обязательно попадет в зону глобального минимума гистограммы, а верхний предел интегрирования b случайно окажется в одной из зон гистограммы.

Величину b в процессе шифрования также можно приблизить к одной из локальных впадин на гистограмме (эта величина даже может попасть в зону глобальной впадины). Для этого нужно произвести расчеты верхнего предела интегрирования b при имеющемся значении нижнего предела интегрирования a, поочередно выбирая допустимые значения интеграла I из ТМЗ. При расчете верхнего предела интегрирования b желательно не допустить попадания этого числа в зону пика гистограммы. Все другие результаты расчетов являются приемлемыми.

Число интервалов k на гистограмме, предназначенной для контроля выходного распределения, можно примерно оценить по формуле Стержесса:

$$k \approx 1 + 3{,}32 \lg n, \qquad (1)$$

где n — число элементов (вещественных чисел) в криптограмме.

Зависимость числа интервалов в гистограмме k от длины (числа символов) зашифрованного текста n следующая:

n	100	1000	10 000	100 000	1 000 000
k	7,64	10,96	14,28	17,6	20,92

С учетом того, что при шифровании каждый символ открытого текста s заменяется двумя вещественными числами ($n = 2s$), при длине открытого текста (сообщения) $s = 500$ символов число интервалов k на гистограмме оценивается числом 10,96 (это значение округляется до целого числа 11).

На передающей стороне ТМЗ служит для замены символа открытого текста на некоторое вещественное число. Это число эквивалентно значению определенного интеграла, для которого определяются значения верхнего и нижнего пределов интегрирования. На приемной стороне ТМЗ используется для определения значения принятого символа по величине определенного интеграла, вычисленного с помощью полученных значений верхнего и нижнего пределов интегрирования. ТМЗ является элементом секретного ключа.

Рассмотрим порядок формирования ТМЗ.

1. Вначале нужно определить длину открытого текста, подлежащего шифрованию. Пусть $S_{\max} = 50\,000$ символов. Тогда число вещественных чисел, из которых будет состоять криптограмма, $n = 100\,000$.

2. По формуле (1) следует оценить число необходимых интервалов на гистограмме. Для выбранного значения $S_{\max}$ число интервалов $k = 17{,}6$.

3. Определить общее число интервалов в ТМЗ t, которое должно быть на один-два порядка больше числа k. Кроме того, число интервалов в ТМЗ должно быть в 3–4 раза больше числа символов в алфавите открытого текста. Таким образом, число интервалов в ТМЗ лежит в пределах 176–1760. Примем $t = 1000$.

4. Найти сумму нормированных частот символов открытого текста

$$sg = \sum_{i=1}^{r} g_i,$$

где r — число символов в алфавите открытого текста ($r = 256$ при использовании всех символов таблицы СР-1251 и $r = 33$ при использовании только русских строчных или заглавных букв); g_i — нормированная частота.

Нормированные частоты появления символов в открытом тексте g_i получают путем деления абсолютных частот на наименьшее значение абсолютной частоты.

5. Вычислить число интервалов замен для каждого i-го символа алфавита открытого текста

$$t_i = \frac{g_i t}{\sum_{i=1}^{r} g_i}.$$

Для примера вычислим число интервалов замен для букв «а» и «б»:

$$t_{\text{а}} = \frac{619 \cdot 1000}{7939} = 78; \quad t_{\text{б}} = \frac{105 \cdot 1000}{7939} = 13.$$

6. Задать диапазон (ширину) гистограммы и ее положение на числовой оси. Это означает, что задаются значения $a_{\min}$ и $b_{\max}$ (для случаев, когда определенный интеграл принимает только положительные значения). Задать ширину и положение на числовой оси ТМЗ, т. е. определить значения $I_{\min}$ и $I_{\max}$. Перечисленные величины связаны между собой, и соотношения между ними зависят от вида подынтегральной функции:

$$I_{\max} = \varphi(a_{\min}, b_{\max}); \; I_{\min} \approx 0.$$

Например, для подынтегральной функции $f(x) = x^4$ правая граница для ТМЗ вычисляется по формуле

$$I_{\max} = \frac{b_{\max}^5 - a_{\min}^5}{5}.$$

Вычислить ширину одного интервала замен

$$\Delta = \frac{I_{\max} - I_{\min}}{t}.$$

Пусть $\Delta = 0{,}1$.

7. Составить ТМЗ, в которой ширина каждого интервала замен равна Δ, а общее число интервалов замен равно t. Все интервалы замен образуют непрерывный интервал чисел шириной Δt. Для рассматриваемого случая $\Delta t = 0{,}1 \cdot 1000 = 100$. Каждому интервалу замен ставят в соответствие один из символов алфавита открытого текста. При этом число интервалов замен для буквы «а» равно $t_{\text{а}}$, для буквы «б» равно $t_{\text{б}}$ и т. д. Интервалы замен для каждого символа располагаются на числовой оси в случайном порядке.

Конфигурация ТМЗ является одним из элементов секретного ключа. Вторым элементом ключа является вид подынтегральной функции. Заметим, что криптоанализ рассматриваемого шифра усложняется еще за счет того, что выбираемое из ТМЗ число и один из пределов интегрирования выбираются по случайному закону.

Примеры шифрования с помощью адаптивного многоалфавитного шифра.

Предположим, что в текущий момент времени необходимо зашифровать букву «в». В качестве

первого ключевого элемента используется табл. 1. Вторым элементом секретного ключа является вид подынтегральной функции. Пусть $f(x) = x^4$.

Предположим, что на гистограмме, сформированной на предыдущих шагах шифрования, наблюдается глобальная впадина в диапазоне чисел [6...10).

Для зашифрования буквы «в» по случайному закону из табл. 1 выбирается один из четырех интервалов замен. Допустим, что выбран интервал 3, т. е. (17...18]. Из этого интервала генерируется случайное число, например $I = 17{,}58$.

Для заполнения провала на гистограмме генерируется случайное число a из интервала [6...10). Пусть $a = 8{,}02$. С учетом формулы Ньютона—Лейбница для выбранной подынтегральной функции получаем

$$b = \sqrt[5]{5I + a^5}.$$

Расчет верхнего предела интегрирования дает значение $b = 8{,}024$. Таким образом, оба числа a и b попали в зону глобальной впадины. «Рассеяние» (отличие, отклонение) пределов интегрирования в рассмотренном случае небольшое.

В качестве подынтегральной функции желательно выбрать функцию, у которой с изменением аргумента существенно меняются амплитуда и частота колебаний.

При выборе вида подынтегральной функции $f(x)$ и нахождении первообразной $F(x)$ можно воспользоваться следующими соображениями.

Представим подынтегральную функцию в виде

$$f(x) = \omega'(x)\sin\omega(x). \qquad (2)$$

Тогда с учетом известного соотношения

$$F'(x) = f(x)$$

для подынтегральной функции (2) получим

$$F(x) = -\cos\omega(x).$$

В качестве $\omega(x)$ можно использовать большой класс функций, например

$$\omega(x) = Ax + C\sin Bx.$$

Тогда

$$f(x) = (A + BC\cos Bx)\sin(Ax + C\sin Bx).$$

В этом случае первообразная определяется выражением

$$F(x) = -\cos(Ax + C\sin Bx).$$

Понятно, что первообразная должна быть использована при вычислении нижнего и верхнего пределов интегрирования, которые являются элементами шифра. Коэффициенты A, B и C можно использовать в качестве элементов ключа рассмотренного шифра.

Пространственно-временное распыление информации

Процедура дробления криптограммы на несколько блоков и передачи их по нескольким каналам связи создает перед криптоаналитиками дополнительный барьер защиты. Очевидно, что помимо традиционных проблем с атакой на шифр возникают проблемы с перехватом (или поиском мест хранения) всех сообщений и выстраиванием их в нужном порядке.

Под каналами связи будем понимать не только традиционные каналы связи (радио, радиорелейные, спутниковые, кабельные, почтовые), но и передачу информации с помощью мультимедийных контейнеров (графики, текста, звука, видео), при этом сама криптограмма может быть стеганографически скрыта в указанных контейнерах. Передачу можно осуществлять с помощью электронной почты, мессенджеров, чатов, SMS, MMS, web-страниц, микроблогов, файлообменных сетей.

Предлагается передачу блоков криптограммы осуществлять не последовательно и не непрерывно, а в порядке, который определяет генератор псевдослучайных чисел. При этом он определяет, какой из множества блоков криптограммы передается, по какому каналу и в какой момент времени. Таким образом, сформированная псевдослучайная последовательность становится элементом секретного ключа. Помимо информационных блоков по каналам связи можно передавать маскирующие (дезинформирующие) блоки.

Каждый информационный блок на передаче получает порядковый номер, с помощью которого сообщение на приеме восстанавливается в исходной последовательности, вне зависимости от порядка и времени поступления блоков в канал связи. В данном шифре стеганограммой будет являться порядковый номер блока криптограммы.

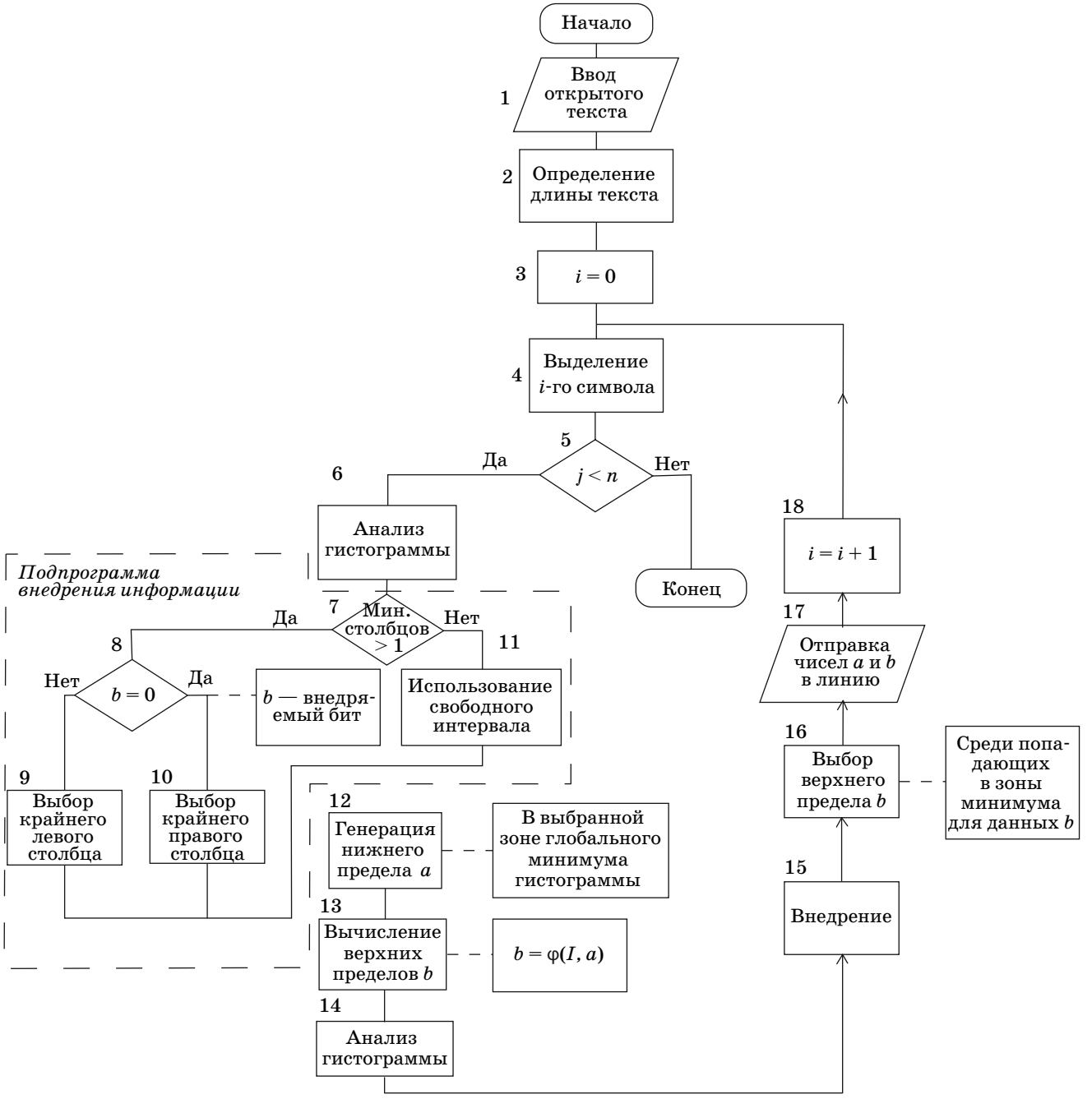
Естественно, что номера блоков должны оставаться скрытыми от противника. Скрытая нумерация блоков может осуществляться криптографическими или стеганографическими способами. В первом случае блок криптограммы должен содержать порядковый номер этого блока. Номер блока должен быть зашифрован тем же ключом, что и вся криптограмма. Известны технические решения, в которых номер блока шифруется шифром, который отличается от основного.

Для реализации шифра с пространственно-временным распылением информации необходимо выполнить две операции: разбить криптограмму на блоки и скрытно пронумеровать эти блоки.

Стеганографическое внедрение информации

Одно из направлений современной стеганографии занимается исследованием внедрения информации в криптограммы [3–6]. За основу разрабатываемого шифра был взят адаптивный многоалфавитный шифр с интегральным преобразованием [2].

Номер каждого блока криптограммы представляют в двоичной системе счисления. При сокрытии считывается внедряемый бит двоичного числа, и если он равен 1, то при шифровании выбирается столбец, ближайший к началу гистограммы (если допустимо, то используется крайний левый столбец). Если внедряемый бит равен 0, то выбирается столбец гистограммы (точнее, интервал) с максимальным удалением от начала числовой оси (крайний правый столбец). Если отсутствует выбор среди столбцов (т. е. остается единственный допустимый интервал гистограммы), то внедрение стеганограммы переносится на следующие шаги алгоритма (рис. 2). На прием-



■ ***Рис. 2.*** *Блок-схема алгоритма внедрения информации*

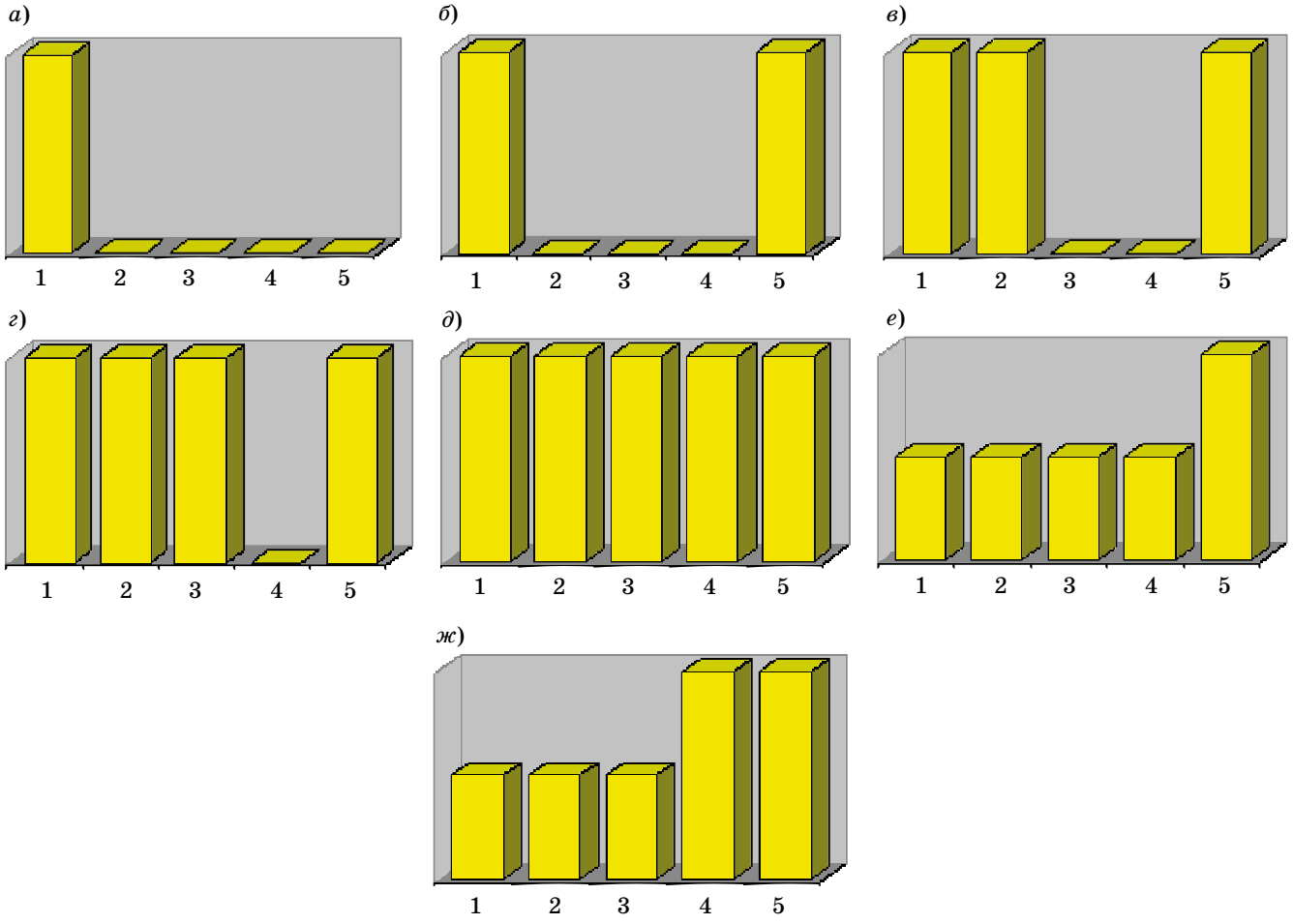
ной стороне после расшифрования переданного сообщения по полученным нижним и верхним пределам интегрирования и вычисленным значениям интеграла производится поэтапное восстановление (реконструкция) гистограммы. При этом на приеме необходимо восстановить последовательность заполнения гистограммы, реализованную на передающей стороне.

Рассмотрим **пример**, в котором таблица многоалфавитной замены составлена так, что при заданной подынтегральной функции, например x^4, выбор предела интегрирования может осуществляться из всех интервалов гистограммы. Допустим, что число интервалов (столбцов гистограммы) пять. Пусть очередному блоку криптограммы требуется присвоить порядковый десятичный номер 44 (двоичное число 101100).

В первоначальном состоянии гистограммы (в момент начала шифрования) все интервалы гистограммы пустые. Так как первый бит (старший бит числа) скрываемой стеганограммы равен 1, то выбирается предел интегрирования из интервала столбца *1* гистограммы (крайний левый столбец, рис. 3, *а*).

Далее производится предварительный расчет второго предела интегрирования для всех возможных значений интеграла для данной шифруемой буквы. В этом примере ТМЗ составлена так, что предел интегрирования может попасть в любой столбец. На данном этапе идет выбор между интервалами (столбцами) *2, 3, 4* и *5*. Так как второй бит скрываемой стеганограммы равен 0, то выбирается число (предел интегрирования) из столбца *5* (крайний правый столбец, рис. 3, *б*).

Рассмотрим процесс шифрования второй буквы открытого текста. Интервал выбирается среди столбцов с номерами *2, 3* и *4*. Так как нужно скрыть бит со значением 1 (третий бит), то выбирается столбец *2* (крайний левый среди минимально заполненных, рис. 3, *в*). Для значения второго предела интегрирования выбирается область определения среди столбцов *3* и *4*. При сокрытии четвертого бита стеганограммы, который равен 1, выбирается *3*-й диапазон (крайний левый среди минимально заполненных, рис. 3, *г*). Следующий этап — выбор интервала для первого предела интегрирования третьей буквы. В этой ситуации выбора нет, так как есть только один



■ ***Рис. 3.*** *Этапы (а—ж) построения гистограммы*

допустимый интервал — *4*-й, откуда и выбирается очередной предел интегрирования. В подобных случаях (когда нет выбора между двумя допустимыми столбцами) скрыть очередной бит стеганограммы невозможно. В такой ситуации сокрытие информации не происходит, а идет штатное формирование криптограммы (рис. 3, *д*).

Затем выбирается второй предел интегрирования для третьей буквы. Сейчас интервалов с минимальным заполнением пять — *1, 2, 3, 4* и *5*. Теперь требуется скрыть пятый бит стеганограммы, равный 0. Выбирается крайний правый столбец — *5*-й (рис. 3, *е*). Далее выбирается первый предел интегрирования для четвертой буквы из интервалов с номерами *1, 2, 3* и *4*. Так как требуется скрыть бит, равный 0, то выбирается *4*-й интервал (крайний правый допустимый, рис. 3, *ж*).

Разбиение криптограммы на отдельные блоки

Разбиение криптограммы на блоки происходит в тех местах алгоритма (в те моменты времени), когда при шифровании все столбцы гистограммы имеют одинаковую высоту.

Таким образом, каждый блок криптограммы на приеме можно расшифровывать отдельно, задав все начальные значения гистограммы нулевыми. Это приведет к верному расшифрованию каждого блока криптограммы и правильному извлечению скрытого номера блока.

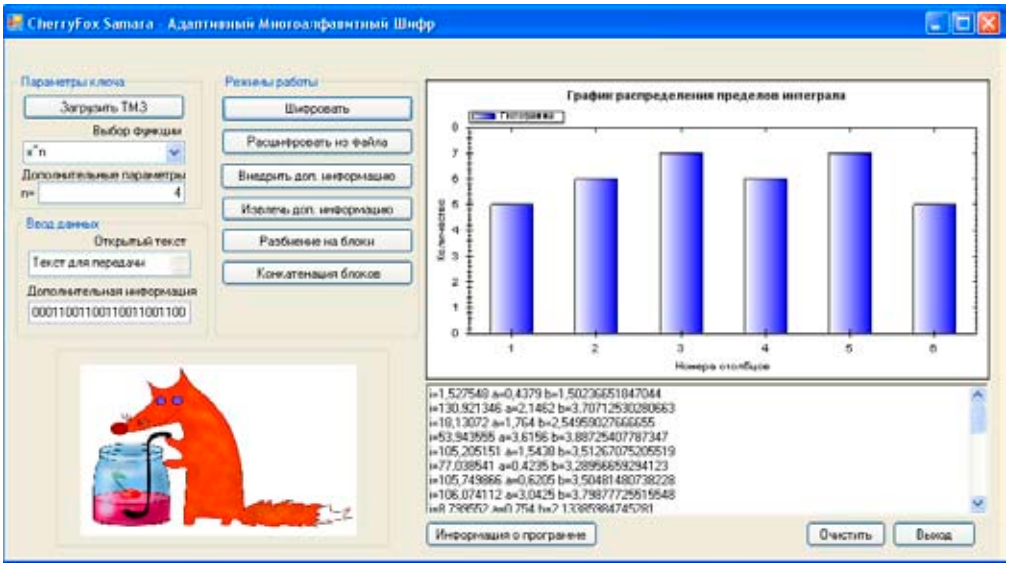
Разбиение на блоки позволяет осуществить раздельную передачу шифра по различным (нескольким) каналам связи, в произвольном порядке и в псевдослучайные моменты времени. Передачу информационных блоков можно перемежать передачей маскирующих блоков. Таким образом увеличивается безопасность передаваемой информации. Перед криптоаналитиком помимо основной задачи по взлому и перехвату шифра возникают дополнительные препятствия, такие как разделение маскирующих блоков и блоков, содержащих криптограмму (информационных), определение (пеленгация) каналов связи и определение времени передачи блоков. В качестве каналов связи могут выступать глобальная сеть Internet, беспроводные локальные сети Wi-Fi, сети сотовой связи (пересылка по MMS). Стеганографическое сокрытие блоков шифра в мультимедиа-контейнерах усложняет задачу на тот случай, если канал связи будет запеленгован.

Проверка рассмотренного способа шифрования с разбиением на блоки была осуществлена с помощью разработанной программы *CherryFox Samara* (рис. 4). Криптограмма объемом 10 КБ была разбита на 8 блоков. Пересылка блоков криптограммы осуществлялась с помощью мессенджера ICQ, размещением на HTML-странице, по электронной почте и размещением на FTP-сервере. На приемной стороне блоки были получены в произвольном порядке и расшифрованы без ошибок.

Характеристики разработанного метода

Оценка скоростей шифрования предлагаемого шифра и наиболее известных шифров осуществлялась на ЭВМ со следующими характеристиками: Windows XP SP2, процессор Celeron, тактовая частота 1,6 ГГц, ОЗУ 3 ГБ.

Результаты испытаний представлены в табл. 2.



■ ***Рис. 4.*** *Интерфейс программы CherryFox Samara*

■ ***Таблица 2.*** *Сравнительная характеристика шифров*

Процесс	AES (МБ)	ГОСТ 28147-89 (МБ)	Адаптивный шифр (КБ)	С внедрением (Б/с)
Шифрование	11,5	6,25	15,1	208
Расшифрование	11,8	7,69	32	162

Адаптивный многоалфавитный шифр использовал ТМЗ с 1280 интервалами для 256 символов кодовой таблицы СР-1251 и подынтегральной функцией x^2.

В криптограмме каждый символ открытого текста заменяется двумя пределами интегрирования, представленными одним разрядом целой части, а после запятой — тремя (для верхнего) и четырьмя (для нижнего). Таким образом, расширение шифртекста по отношению к открытому тексту осуществляется в 9 раз.

Имеются способы, позволяющие существенно сжать получающуюся криптограмму. В пределе эти способы могут обеспечить расширение криптограммы по сравнению с исходным текстом лишь в 2 раза.

Достоинством шифра является стойкость к перебору числа возможных ключей. В данном способе шифрования ключевыми элементами являются таблица многоалфавитной замены и вид подынтегральной функции. Представляет интерес оценка числа различных конфигураций ТМЗ (другими словами, оценка числа ключей).

Пусть имеется алфавит символов открытого текста, состоящий из m символов. Таблица многоалфавитной замены должна удовлетворять следующим требованиям: число интервалов должно быть больше числа символов $n > m$, все интервалы должны быть размещены таким образом, чтобы образовать непрерывную числовую ось и чтобы любому символу открытого текста не соответствовали никакие два смежных интервала ТМЗ.

Обозначим число всевозможных различных способов формирования (конфигураций) ТМЗ символом A_n^m. В ходе исследования была доказана справедливость рекуррентной формулы

$$A_{n+1}^m = (m-1)A_n^m + mA_n^{m-1}.$$

Таким образом, для 256 символов (например, кодовая таблица СР-1251) с 1000 интервалов в ТМЗ число комбинаций составит $1{,}74 \cdot 10^{2404}$. Проведенные расчеты говорят о большом числе ключей, которые могут быть использованы в этом шифре. Заметим, что расчеты произведены для одной подынтегральной функции. Понятно, что число ключей линейно возрастает с увеличением числа подынтегральных функций.

Заключение

Разработанный шифр создает перед криптоаналитиками дополнительный барьер, состоящий в необходимости перехвата всех блоков криптограммы, передаваемых по разным каналам связи. Проведенная экспериментальная проверка пересылки блоков криптограммы по нескольким каналам подтверждает эффективность предлагаемой идеи.

Один из вариантов реализации рассмотренного способа шифрования сводился к размещению пронумерованных блоков шифрограммы на нескольких серверах (или сайтах). Принимающая сторона после скачивания всех файлов отбирала по номерам файлы (блоки), необходимые для восстановления (синтеза) исходного сообщения.

Литература

1. **Алексеев А. П.** Математические методы формирования многоалфавитных шифров замены // Инфокоммуникационные технологии. 2009. Т. 7. № 2. С. 21–25.
2. **Алексеев А. П., Блатов И. А., Макаров М. И., Похлебаев В. А.** Многоалфавитный адаптивный шифр, основанный на интегральных преобразованиях // Инфокоммуникационные технологии. 2010. Т. 8. № 1. С. 70–75.
3. **Simmons G. J.** Subliminal Channels: Past and Present // European Transactions on Telecommunications. Aug. 1994. Vol. 4. N 4. P. 459–473.
4. **Simmons G. J.** The Subliminal Channels of the U. S. Digital Signature Algorithm (DSA) // State and Progress of Research in Cryptography: Proc. of the Third Symp. Rome: Fondazone Ugo Bordoni, 1993. P. 35–54.
5. **Шнайер Б.** Прикладная криптография. — М.: ТРИУМФ, 2002. — 816 с.
6. **Белим С. В., Федосеев А. М.** Исследование скрытых каналов передачи информации в алгоритме цифровой подписи ГОСТ Р 34.10-2001 // Изв. Челябинского научного центра. 2007. Вып. 2(36). С. 17–19.

УДК 681.3

РАСШИРЕНИЕ ФУНКЦИОНАЛЬНОСТИ СТАНДАРТОВ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Д. Н. Молдовян,
аспирант
Е. С. Дернова,
канд. техн. наук, преподаватель
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Д. К. Сухов,
аспирант
Санкт-Петербургский институт информатики и автоматизации РАН

Рассмотрена реализация схем слепой и слепой коллективной подписи, использующих процедуры проверки подлинности электронной цифровой подписи, рекомендуемые российскими стандартами.

Ключевые слова *— электронная цифровая подпись, слепая подпись, открытый ключ, стандарты электронной цифровой подписи, коллективная слепая подпись.*

Введение

Электронная цифровая подпись (ЭЦП) широко применяется для решения различных практических задач электронного документооборота и других современных информационных технологий. Важными типами схем ЭЦП являются протоколы слепой [1, 2] и коллективной [3, 4] ЭЦП. Протокол коллективной подписи позволяет сформировать единую ЭЦП фиксированного размера как криптографическую сумму индивидуальных цифровых подписей практически произвольного числа подписывающих. Схемы слепой ЭЦП применяются в системах тайного электронного голосования и системах электронных денег. Протоколы данного вида решают задачу обеспечения неотслеживаемости (анонимности), которая состоит в том, что требуется подписать электронное сообщение M таким способом, что подписывающий 1) не может ознакомиться с сообщением в процессе формирования подписи и 2) впоследствии при получении сообщения M и подлинной подписи к нему не может однозначно идентифицировать пользователя, предоставлявшего данное сообщение для формирования ЭЦП. Прикладной интерес представляют также схемы ЭЦП, объединяющие возможности протоколов указанных двух типов, которые впервые были предложены в работе [5] как протоколы слепой коллективной ЭЦП. Для практических приложений важным является использование процедур формирования и проверки ЭЦП, рекомендуемых официальными стандартами.

В настоящей работе рассматривается построение схем слепой и слепой коллективной ЭЦП с использованием процедур формирования и проверки ЭЦП, рекомендуемых ГОСТ Р 34.10–94 [6] и Р 34.10–2001 [7, 8].

Схемы слепой ЭЦП на основе российских стандартов

Стандарт ЭЦП ГОСТ Р 34.10–94 рекомендует использование простого числа p, размер которого $|p|$ удовлетворяет условиям $1022 \le |p| \le 1024$ бит. При этом число p выбирается таким, что значение $p - 1$ содержит большой простой делитель $2^{511} \le q \le 2^{512}$ соответственно. Специфицируемые стандартом процедуры генерации и проверки ЭЦП используют число $\alpha < p$ такое, что $\alpha \ne 1$ и $\alpha^q \bmod p = 1$ (α является генератором циклической подгруппы конечного простого поля $GF(p)$, имеющей порядок q). Формирование ЭЦП в соответствии с ГОСТ Р 34.10–94 [6] осуществляется следующим образом.

1. Генерируется случайное число k, удовлетворяющее условию $1 < k < q$.

2. Формируется рандомизирующий параметр ЭЦП — значение $R = (\alpha^k \bmod p) \bmod q$, являющийся первой частью подписи.

3. По ГОСТ Р 34.11–94 вычисляется хэш-функция H от подписываемого сообщения M.

4. Вычисляется второй элемент ЭЦП в виде числа $S = kH + zR \bmod q$, где z — личный секретный ключ пользователя, формирующего свою подпись к сообщению M. Если $S = 0$, то следует перейти к шагу 1 и процедура генерации подписи повторяется.

Процедура проверки подлинности ЭЦП состоит в выполнении следующих шагов.

1. Выполняется проверка условий $r < q$ и $s < q$. Если хотя бы одно из этих условий не выполняется, то подпись признается недействительной.

2. Вычисляется (по ГОСТ Р 34.11–94) хэш-функция H от подписываемого сообщения M.

3. Вычисляется значение

$$R^* = (\alpha^{S/H} y^{-R/H} \bmod p) \bmod q. \qquad (1)$$

4. Сравниваются значения R и R^*. Если $R = R^*$, то подпись признается действительной.

Протокол слепой ЭЦП на основе ГОСТ Р 34.10–94 строится с использованием двух «ослепляющих» множителей, формируемых в виде $y^{\mu} \bmod p$ и $\alpha^{\varepsilon} \bmod p$. Множители такого типа использовались ранее в схеме слепой подписи на основе алгоритма ЭЦП Шнорра [9, 10]. Разработанный протокол слепой ЭЦП на основе ГОСТ Р 34.10–94 описывается следующим образом.

1. Подписывающий генерирует случайное значение $k < q$, вычисляет число $\rho = \alpha^k \bmod p$ и направляет его пользователю А, который намерен представить некоторое электронное сообщение M для получения к нему слепой ЭЦП подписывающего, из которой пользователь А сможет самостоятельно вычислить правильное значение ЭЦП, которое пройдет процедуру проверки ЭЦП по ГОСТ Р 34.10–94.

2. Пользователь А генерирует случайные равновероятные значения $\mu, \varepsilon \in \{1, 2, \ldots, q-1\}$, вычисляет значения $\rho' = \rho y^{\mu} \alpha^{\varepsilon} \bmod p$, $R' = \rho' \bmod q$ и $R = R'/H + \mu \bmod q$, где H — значение хэш-функции от подписываемого документа, вычисленное по ГОСТ Р 34.11–94. Значение R', которое остается неизвестным подписывающему, представляет собой первый элемент подлинной ЭЦП. Значение R представляет собой первый элемент формируемой слепой подписи.

3. Пользователь А отправляет подписывающему значение R, из которого нельзя вычислить R', поскольку для любого значения R' существует пара значений μ и ε, которые связывают значение R' с полученным числом R.

4. Подписывающий вычисляет значение $S = k + zR \bmod q$, где z — его секретный ключ, передает вычисленный элемент слепой подписи пользователю А.

5. Пользователь А вычисляет значение $S' = H(S + \varepsilon) \bmod q$, которое является вторым элементом подписи.

Полученная в соответствии с этим протоколом ЭЦП (R', S') является подлинной, т. е. она вместе со значением хэш-функции H от сообщения M проходит уравнение проверки ЭЦП, специфицируемое ГОСТ Р 34.10–94. Корректность работы описанной схемы слепой ЭЦП доказывается следующим путем.

Доказательство корректности. Элемент слепой подписи S вычисляется на шаге 4 по формуле $S = k + zR \bmod q$, из которой с учетом того, что число α имеет порядок q по модулю p, следует справедливость сравнения $\alpha^S \equiv \alpha^k \alpha^{zR} \bmod p$, откуда имеем $\rho \equiv \alpha^k \equiv \alpha^S \alpha^{-zR} \bmod p$. Учитывая, что $R' = H(R - \mu) \bmod q$, вычисление правой части уравнения проверки подлинности ЭЦП (1) для подписи (R', S') и значения хэш-функции H дает следующее:

$$\rho^* = y^{-\frac{R'}{H}} \alpha^{\frac{S'}{H}} = y^{-\frac{H(R-\mu)}{H}} \alpha^{\frac{H(S+\varepsilon)}{H}} = y^{-R+\mu} \alpha^{S+\varepsilon} =$$
$$= y^{-R} \alpha^S y^{\mu} \alpha^{\varepsilon} = \rho y^{\mu} \alpha^{\varepsilon} = \rho' \Rightarrow \rho^* \bmod q = R'. \qquad (2)$$

Последнее равенство означает, что подпись (R', S') к сообщению M является подлинной.

Рассмотренный протокол обеспечивает анонимность пользователя, предоставляющего сообщение для получения подписи вслепую в том смысле, что нельзя однозначно установить пользователя, предоставлявшего данное сообщение для формирования слепой ЭЦП (предполагается, что число сообщений, подписанных данным подписывающим с помощью протокола слепой подписи, $N > 1$). Подписывающий при предъявлении ему его подлинной подписи (R', S') к сообщению M не может установить пользователя, который предоставлял ему этот документ на подпись, с вероятностью выше значения d/N, где N — количество документов, подписанных (данным подписывающим) с помощью протокола слепой подписи; d — число документов, предоставлявшихся данным пользователем, поскольку любая подпись (R', S') может быть с равной вероятностью отнесена к каждой из N выполненных процедур протокола слепой подписи.

Действительно, любая тройка значений (ρ, R, S) из множества таких троек, которые известны подписывающему из N выполненных им процедур подписывания сообщений вслепую, может быть ассоциирована с произвольной подлинной подписью (R', S'), относящейся к некоторому сообщению, представленному значением хэш-функции H. Это связано с тем, что тройки (ρ, R, S) и (R', S', H) в соответствии с описанным протоколом слепой ЭЦП связаны случайными рав-

новероятными значениями μ и ε с помощью следующих соотношений: $\rho = \alpha^S y^{-R} \bmod p$ и $\rho' = \alpha^{S'/H} y^{-R'/H} \bmod p = \alpha^S y^{-R} y^{\mu} \alpha^{\varepsilon} \bmod p$, т. е. $\rho' = \rho y^{\mu} \alpha^{\varepsilon} \bmod p$, поэтому тройка (R', S', H) с равной вероятностью могла бы быть порождена из любой тройки (ρ, R, S), фигурировавшей в одной из N выполненных процедур слепого подписывания сообщений. (Отметим, что значение ρ однозначно определяется парой чисел R и S.)

Стандарт ЭЦП ГОСТ Р 34.10–2001 по построению подобен рассмотренному выше стандарту. Основное отличие состоит в том, что в нем вычисления выполняются не в циклической подгруппе конечного поля, а в конечной группе другой природы, в качестве которой используется эллиптическая кривая (ЭК) над конечным полем. Групповой операцией в группе точек ЭК является композиция или сложение точек ЭК. Аналогами операций умножения и возведения в степень по модулю, используемых в стандарте ЭЦП ГОСТ Р 34.10–94, в ГОСТ Р 34.10–2001 являются операции сложения точек ЭК и умножения точки на число соответственно. В силу указанной аналогии рассмотренный выше протокол слепой подписи может быть реализован также и на основе ГОСТ Р 34.10–2001.

ГОСТ Р 34.10–2001 регламентирует использование простого числа p — модуля ЭК, которая задается в декартовой системе координат уравнением вида $y^2 = x^3 + ax + d \bmod p$, где $a, b \in GF(p)$; простого числа q — порядка циклической подгруппы точек ЭК; точки G с координатами (x_G, y_G) такой, что $G \neq O$, $qG = O$, где O — бесконечно удаленная точка, являющаяся нейтральным элементом (нулем) группы точек ЭК. Секретным ключом является достаточно большое целое число $d < q$, а открытым ключом — точка $Q = dG$. Формирование подписи (R, S) осуществляется в соответствии со следующим алгоритмом.

1. Генерируется случайное целое число k $(0 < k < q)$.

2. Вычисляется точка $C = kG$ и определяется значение $r = x_C \bmod q$, где x_C — координата точки C.

3. Вычисляется значение $s = (rd + ke) \bmod q$, где $e = H \bmod q$, H — значение хэш-функции от подписываемого сообщения.

Подписью являются два числа (r, s). Проверка подписи заключается в вычислении координат точки C^*:

$$C^* = (se^{-1} \bmod q)G + ((q - r)e^{-1} \bmod q)Q, \quad (3)$$

определении значения $r^* = x_{C^*} \bmod q$ и проверке выполнения равенства $r^* = r$.

Протокол слепой подписи на основе рассмотренного алгоритма реализуется следующим образом.

1. Подписывающий генерирует случайное число $k < q$, вычисляет точку ЭК $C = kG$ и направляет ее пользователю А, который намерен получить слепую ЭЦП к сообщению M.

2. Пользователь А генерирует случайные значения $\mu, \varepsilon \in \{1, 2, \ldots, q - 1\}$, вычисляет точку ЭК $C' = C + \mu Q + \varepsilon G$ с координатами $(x_{C'}, y_{C'})$, значения $r' = x_{C'} \bmod q$, $e = H \bmod q$, где H — значение хэш-функции, вычисленное от M, и $r = r'e^{-1} + \mu \bmod q$. Значение r', которое остается неизвестным подписывающему, представляет собой первый элемент формируемой ЭЦП. Значение r является рандомизирующим элементом слепой ЭЦП.

3. Пользователь А отправляет подписывающему значение r, из которого нельзя вычислить r' (для любого r' существует пара чисел μ и ε, которые связывают значения r' и r).

4. Подписывающий вычисляет значение $s = k + dr \bmod q$, где d — его секретный ключ, передает вычисленный второй элемент s слепой подписи пользователю А.

5. Пользователь А вычисляет значение $s' = e(s + \varepsilon) \bmod q$, которое является вторым элементом подписи.

Вычисленная подпись (r', s') является подлинной ЭЦП к сообщению M.

Доказательство корректности. Элемент слепой подписи S вычисляется на шаге 4 по формуле $s = k + dr \bmod q$, из которой следует выполнимость соотношения $sG = kG + drG$. Из последнего уравнения получаем $C = kG = sG - drG$. Вычисление правой части проверочного уравнения (3) для ЭЦП (r', s') и значения хэш-функции H (которое определяет значение $e = H \bmod q$) дает следующее:

$$(s'e^{-1} \bmod q)G - r'Q =$$
$$= (s + \varepsilon \bmod q)G - (r - \mu \bmod q)Q = (sG - rQ) +$$
$$+ \varepsilon G + \mu Q = C + \varepsilon G + \mu Q = C' \Rightarrow r^* = x_{C'} = r'.$$

В соответствии с процедурой проверки ЭЦП выполнение равенства $r^* = r$ означает подлинность подписи (r', s'). Схема слепой ЭЦП на основе ГОСТ Р 34.10–2001 обеспечивает анонимность субъектов, предоставляющих электронные сообщения для подписывания, что легко доказывается по аналогии со случаем слепой ЭЦП на основе ГОСТ Р 34.10–94.

Протоколы слепой коллективной подписи

Протоколы слепой коллективной ЭЦП на основе ГОСТ Р 34.10–94 и Р 34.10–2001 разработаны путем встраивания в описанные в предыдущем разделе схемы слепой ЭЦП механизма свертки открытых ключей всех субъектов, входящих в коллектив подписывающих, ранее апробированного в работах [3, 4]. Схема слепой коллективной ЭЦП на основе ГОСТ Р 34.10–94 описывается следующим образом.

Пусть пользователь А желает подписать вслепую электронное сообщение M у m подписывающих, владеющих открытыми ключами $y_i = \alpha^{z_i} \bmod p$, где z_i — личный секретный ключ i-го подписывающего ($i = 1, 2, ..., m$). Предполагается, что проверка коллективной ЭЦП осуществляется по проверочному уравнению, специфицируемому ГОСТ Р 34.10–94 с использованием коллективного открытого ключа y в виде произведения открытых ключей всех подписывающих $y = y_1 y_2 ... y_m \bmod p$. Процедура формирования коллективной подписи вслепую состоит в выполнении следующих шагов.

1. Каждый i-й подписывающий генерирует случайное число $k_i (1 < k_i < q)$ и вычисляет свое индивидуальное рандомизирующее значение $\rho_i = \alpha^{k_i} \bmod p$.

2. Подписывающие вычисляют общее рандомизирующее значение ρ путем перемножения всех индивидуальных рандомизирующих значений ρ_i, т. е. в виде $\rho = \prod_{i=1}^{m} \rho_i \bmod p$. Значение ρ направляется пользователю А.

3. Пользователь А генерирует случайные значения $\mu, \varepsilon \in \{1, 2, ..., q-1\}$, вычисляет значения $\rho' = \rho y^{\mu} \alpha^{\varepsilon} \bmod p$, $R' = \rho' \bmod q$ и $R = R'/H + \mu \bmod q$, где H — значение хэш-функции от подписываемого документа. Значение R является первым элементом слепой коллективной подписи, а R' — первым элементом коллективной подписи к сообщению M.

4. Пользователь А отправляет подписывающим значение R.

5. Каждый i-й подписывающий вычисляет значение $S_i = k_i + z_i R \bmod q$, где z_i — его секретный ключ.

6. Подписывающие вычисляют свертку значений S_i в виде суммы $S = \sum_{i=1}^{m} S_i \bmod q$ и направляют ее пользователю А. Значение S является вторым элементом слепой коллективной подписи.

7. Пользователь А вычисляет значение $S' = H(S + \varepsilon) \bmod q$, которое является вторым элементом коллективной подписи.

Полученная в соответствии с этим протоколом ЭЦП (R', S') является подлинной, что подтверждается следующим доказательством.

Доказательство корректности. Элемент слепой подписи S, вычисляемый на шаге 6, может быть представлен в виде

$$S = \sum_{i=1}^{m} S_i \bmod q = \sum_{i=1}^{m} (k_i + z_i R) \bmod q = \left(\sum_{i=1}^{m} k_i + R \sum_{i=1}^{m} z_i \right) \bmod q.$$

Из последнего соотношения с учетом того, что число α имеет порядок q по модулю p, следует справедливость сравнения

$$\alpha^S \equiv \alpha^{\sum_{i=1}^{m} k_i} \alpha^{R \sum_{i=1}^{m} z_i} \equiv \rho y^R \bmod p,$$

из которого имеем $\rho \equiv \alpha^S y^{-R} \bmod p$. Учитывая, что $R' = H(R - \mu) \bmod q$, вычисление правой части проверочного уравнения (1) в случае проверяемой коллективной подписи (R', S') и значения хэш-функции H дает соотношения, совпадающие с (2), т. е. правая часть проверочного уравнения равна элементу R' проверяемой подписи, следовательно, подпись (R', S') к сообщению M является подлинной. Действительно, подстановка значений R' и S' в (1) дает

$$R^* = \left(y^{-\frac{R'}{H}} \alpha^{\frac{S'}{H}} \bmod p \right) \bmod q =$$

$$= \left(y^{-\frac{H(R-\mu)}{H}} \alpha^{\frac{H(S+\varepsilon)}{H}} \bmod p \right) \bmod q =$$

$$= (y^{-R+\mu} \alpha^{S+\varepsilon} \bmod p) \bmod q = (y^{-R} \alpha^S y^{\mu} \alpha^{\varepsilon} \bmod p) \bmod q =$$

$$= (R y^{\mu} \alpha^{\varepsilon} \bmod p) \bmod q = R' \Rightarrow R^* \bmod q = R'.$$

Протокол слепой коллективной подписи на основе ГОСТ Р 34.10–2001 реализуется следующим образом.

1. Каждый i-й подписывающий генерирует случайное число k_i, $1 < k_i < q$, вычисляет точку ЭК $C_i = k_i G$.

2. Подписывающие вычисляют результирующую точку $C = C_1 + C_2 + ... + C_m$ и направляют ее пользователю А, который намерен получить слепую подпись к электронному сообщению M.

3. Пользователь А генерирует случайные значения $\mu, \varepsilon \in \{1, 2, ..., q-1\}$, вычисляет точку ЭК $C' = C + \mu Q + \varepsilon G$ с координатами ($x_{C'}$, $y_{C'}$), значения $r' = x_{C'} \bmod q$ и $r = (r'/e + \mu) \bmod q$, где $e = H \bmod q$; H — значение хэш-функции от подписываемого сообщения. Значение r' является первым элементом формируемой подписи.

4. Пользователь А отправляет подписывающему значение r.

5. Каждый i-й подписывающий вычисляет значение $s_i = k_i + d_i r \bmod q$, где d_i — его личный секретный ключ.

6. Подписывающие вычисляют значение $s = s_1 + s_2 + ... + s_m \bmod q$, которое является элементом слепой подписи, и передают значение s пользователю А.

7. Пользователь А вычисляет значение $s' = e(s + \varepsilon) \bmod q$, которое является вторым элементом подписи.

Проверка подлинности коллективной ЭЦП выполняется по проверочному уравнению (3), в которое вместо индивидуального открытого ключа подставляется коллективный открытый ключ, равный точке $Q = Q_1 + Q_2 + ... + Q_m$.

Подписывающие не могут вычислить пару чисел (r', s'), которая представляет собой подпись, полученную пользователем А в результате выполнения протокола слепой коллективной ЭЦП.

Подпись (r', s') является подлинной и соответствует сообщению M. Корректность последнего протокола легко доказать по аналогии с доказательствами корректности приведенных выше протоколов. Действительно, подстановка значений r' и s' в (3) дает

$$C^* = (s'e^{-1} \bmod q)G - r'e^{-1}Q = (s + \varepsilon \bmod q)G - \\ - (r - \mu \bmod q)Q = (sG - rQ) + \varepsilon G + \mu Q = \\ = C + \varepsilon G + \mu Q = C' \Rightarrow r^* = x_{C^*} = x_{C'} = r'. \quad (4)$$

Описанные в этом разделе схемы слепой ЭЦП на основе российских стандартов ЭЦП решают задачу обеспечения анонимности. Доказательство этого выполняется аналогично для случаев использования обоих приведенных стандартов. Рассмотрим случай ГОСТ Р 34.10–2010.

Пусть коллектив подписавших получил некоторый документ M и коллективную подпись к нему в виде пары чисел (r', s'). Покажем, что любое из зарегистрированных им значений слепой подписи (r, s) может быть соотнесено с (r', s'). Вычисление долей подписи индивидуальными подписывающими выполнялось по формуле $s_i = k_i + d_i r \bmod q$, поэтому имеем

$$s = \sum_{j=1}^{m} s_j = \sum_{j=1}^{m} k_j + d_j r \bmod q = \left(\sum_{j=1}^{m} k_j + r \sum_{j=1}^{m} d_j \right) \bmod q \Rightarrow$$

$$\Rightarrow sG = \left(\sum_{j=1}^{m} k_j \bmod q \right) G + \left(r \sum_{j=1}^{m} d_j \bmod q \right) G =$$

$$= \sum_{j=1}^{m} k_j G + r \sum_{j=1}^{m} d_j G = \sum_{j=1}^{m} C_j + r \sum_{j=1}^{m} Q_j = C + rQ.$$

Из уравнения проверки подлинности ЭЦП и соотношений (4) для правильной подписи имеем

$$C' = s'e^{-1}G - r'e^{-1}Q = C + (s'e^{-1}G - r'e^{-1}Q) - \\ - (sG - rQ) = C + (s'e^{-1} - s \bmod q)G + \\ + (r - r'e^{-1} - s \bmod q)Q = C + \varepsilon G + \mu Q.$$

Следовательно, для каждой из сформированных слепых коллективных подписей (r, s) имеется единственная пара значения μ и ε, которая связывает (r, s) с (r', s'). Поскольку данные значения формировались субъектами, представлявшими электронные сообщения для получения слепой ЭЦП, то любая из сформированных слепых подписей с одинаковой вероятностью может быть связана с данной конкретной подписью (r', s').

Заключение

Предложенные схемы слепой и коллективной слепой ЭЦП используют проверочные уравнения, рекомендуемые стандартами ЭЦП ГОСТ Р 34.10–94 и Р 34.10–2001. Это означает, что разработанные протоколы могут быть положены в основу расширения функциональности этих стандартов, благодаря чему механизмы ЭЦП могут найти более широкое применение в информационных технологиях, в частности при построении систем электронных денег и систем тайного электронного голосования.

Работа выполнена в рамках исследований по Федеральной целевой программе «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (конкурсная заявка № НК-563П/59).

Литература

1. **Chaum D.** Blind Signatures for Untraceable Payments // Intern. Conf. Advances in Cryptology: Proc. CRYPTO'82. Plenum Press, 1983. P. 199–203.
2. **Chaum D.** Security Without Identification: Transaction Systems to Make Big Brother Obsolete // Communication of the ACM. Oct. 1985. Vol. 28. N 10. P. 1030–1044.
3. **Молдовян А. А., Молдовян Н. А.** Новые алгоритмы и протоколы для аутентификации информации в АСУ // Автоматика и телемеханика. 2008. № 7. С. 157–169.
4. **Ананьев М. Ю., Гортинская Л. В., Молдовян Н. А.** Протоколы коллективной подписи на основе свертки индивидуальных параметров // Информационно-управляющие системы. 2008. № 2. С. 22–27.
5. **Moldovyan N. A., Moldovyan A. A.** Blind Collective Signature Protocol Based on Discrete Logarithm Problem // Intern. Journal of Network Security. 2010. Vol. 11. N 2. P. 106–113.
6. **ГОСТ** Р 34.10–94. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — М.: Изд-во стандартов, 1994. — 18 с.
7. **ГОСТ** Р 34.10–2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — М.: Изд-во стандартов, 2001. — 12 с.
8. **Рябко Б. Я., Фионов А. Н.** Криптографические методы защиты информации. — М.: Горячая линия — Телеком, 2005. — 229 с.
9. **Pointcheval D., Stern J.** Security arguments for digital signatures and blind signatures // J. Cryptology. 2000. Vol. 13. N 3. P. 361–396.
10. **Молдовян Н. А.** Теоретический минимум и алгоритмы цифровой подписи. — СПб.: БХВ-Петербург, 2010. — 290 с.

УДК 519.71

СТАТИСТИЧЕСКАЯ ЛИНЕАРИЗАЦИЯ МНОГОМЕРНЫХ СТОХАСТИЧЕСКИХ СИСТЕМ ПО ИНФОРМАЦИОННОМУ КРИТЕРИЮ

К. Р. Чернышев,
канд. физ.-мат. наук
Институт проблем управления им. В. А. Трапезникова РАН

Предложена конструктивная процедура построения линейной входо-выходной модели, которая представляет собой статистический эквивалент некоторой нелинейной многомерной динамической стохастической системы с гауссовым входным процессом в виде белого шума. Ключевым моментом такой процедуры является использование в качестве критерия статистической линеаризации условия покомпонентного совпадения взаимной информации входного и выходного процессов системы и взаимной информации входного и выходного процессов модели. Данный подход позволяет получить явные соотношения, определяющие элементы весовых матриц линеаризованной модели.

Ключевые слова *— взаимная информация, входо-выходная модель, гауссова плотность распределения, информационный критерий, меры зависимости, многомерная система, статистическая линеаризация.*

Введение

Решение задачи идентификации систем всегда основано на применении тех или иных мер зависимости случайных величин (процессов), идет ли речь о представлении исследуемых систем в виде входо-выходного соотношения или в пространстве состояний. Наиболее часто в качестве такой меры выступают традиционные линейные ковариационные или корреляционные меры зависимости, использование которых непосредственно вытекает из самой постановки задачи идентификации на основе среднеквадратического критерия. Их основным достоинством является удобство использования, включая как возможность построения явных аналитических выражений для определения искомых характеристик, так и относительную простоту построения их оценок, в том числе и на основе наблюдения зависимых данных. Однако главным недостатком мер зависимости, основанных на линейной корреляции, является, как известно, возможность их обращения в нуль даже в случае существования детерминированной зависимости между парой исследуемых переменных [1–3].

Именно на преодоление этого недостатка направлено использование в задачах идентификации более сложных, нелинейных, мер зависимости, таких как дисперсионная функция, являющаяся аналогом известного в литературе дисперсионного отношения, максимальная корреляция, взаимная информация по Шеннону. При этом две последние меры, как известно, являются *состоятельными*, по терминологии А. Н. Колмогорова, мерами зависимости, т. е. обращающимися в нуль тогда и только тогда, когда случайные процессы (величины) в данной паре являются стохастически независимыми. В этом, в первую очередь, состоит привлекательность применения максимальной корреляции и взаимной информации в задачах идентификации, особенно в случае рассмотрения нелинейных систем.

К задачам нелинейной идентификации, решение которых существенно определяется характеристиками зависимости входных и выходных процессов системы, относится статистическая линеаризация входо-выходного отображения исследуемых систем. При этом известные подходы к статистической линеаризации основаны на применении либо обычных корреляционных функций, либо дисперсионных функций, что, в силу указанных выше причин, может приводить к построению моделей, выход которых тождественен нулю. В частности, возможность такой ситуации иллюстрируется в последнем разделе примером. Предлагаемый в настоящей работе подход на-

правлен на исключение отмеченных недостатков, связанных с применением корреляционных и дисперсионных (основанных на корреляционном отношении) мер зависимости при идентификации систем на основе линеаризованных представлений их входо-выходных моделей. В его рамках рассматривается постановка задачи статистической линеаризации многомерных систем с дискретным временем по информационному критерию, обобщающая подход, представленный в работе [4] для одномерных систем.

Предварительные замечания

Применение состоятельных мер зависимости имеет свои особенности и ограничения. В этих рамках шенноновская взаимная информация выглядит предпочтительнее максимальной корреляционной функции, вычисление которой сопряжено с необходимостью использовать сложную итеративную процедуру определения первого собственного числа и пару первых собственных функций стохастического ядра $p_{yw}(y, w, \tau)\Big/\sqrt{p_w(w)p_y(y)}$ [1, 5], где $p_w(w)$, $p_y(y)$, $p_{yw}(y, w, \tau)$ представляют собой маргинальные и совместную плотности распределения случайных процессов $w(s)$ и $y(t)$ соответственно, $\tau = t - s$. К использованию взаимной информации приводит выбор в качестве критерия идентификации теоретико-информационного критерия. Примером такого подхода является работа [6], в которой постановка задачи идентификации ограничена рассмотрением класса *линейных гауссовых* систем и естественным образом приводит к использованию следующего соотношения для взаимной информации $I(Y, X)$ многомерного нормального распределения:

$$I(Y,X) = -\frac{1}{2}\ln\left(\frac{\det(Q_{\mathbf{ZZ}})}{\det(Q_{\mathbf{YY}})\det(Q_{\mathbf{XX}})}\right). \qquad (1)$$

В формуле (1) приняты следующие обозначения: $\mathbf{Z}$ — нормально распределенный случайный вектор с ковариационной матрицей $Q_{\mathbf{ZZ}}$, $\dim\mathbf{Z} = n + m$, причем $\mathbf{Z} = (\mathbf{X}^T\ \mathbf{Y}^T)^T$, где $\dim\mathbf{X} = n$, $\dim\mathbf{Y} = m$; $Q_{\mathbf{XX}}$, $Q_{\mathbf{YY}}$ — ковариационные матрицы случайных векторов $\mathbf{X}$ и $\mathbf{Y}$ соответственно. При этом целью работы [6] является демонстрация эквивалентности ряда критериев идентификации и управления для *линейных гауссовых* систем. В то же время нельзя не отметить, что в этих рамках в принципе исчезает сам смысл обращения к подобному информационному критерию, поскольку в данном случае достаточно использовать обычный среднеквадратический критерий (как хорошо известно, в случае нормальности совместного распределения максимальная корреляция линейна и совпадает с обычной).

Постановка задачи

Пусть в некоторой многомерной (MIMO — multi input / multi output) нелинейной динамической стохастической системе $Y(t) = (y_1(t), ..., y_n(t))^T$ — n-мерный выходной случайный процесс системы, предполагающийся стационарным и эргодическим; $W(s) = (w_1(s), ..., w_m(s))^T$ — m-мерный входной случайный процесс системы, предполагающийся в данной постановке задачи белым гауссовым шумом с известной ковариационной матрицей C_W, а зависимость компонент входных и выходных процессов системы характеризуется (конечно, неизвестными исследователю) плотностями распределения

$$p_{y_i,w_j}(y, w, \tau),\ i = 1, ..., n,\ j = 1, ..., m,\ \tau = 1, 2, ... \qquad (2)$$

Ради простоты построения, но без потери общности, компоненты данных процессов $Y(t)$ и $W(s)$ предполагаются имеющими нулевые средние и единичные дисперсии

$$\mathbf{M}\{y_i(t)\} = \mathbf{M}\{w_j(s)\} = 0,\ \mathbf{D}\{y_i(t)\} = \mathbf{D}\{w_j(s)\} = 1,\ i = 1, ..., n,\ j = 1, ..., m, \qquad (3)$$

где $\mathbf{M}\{\cdot\}$, $\mathbf{D}\{\cdot\}$ — символы математического ожидания и дисперсии соответственно. В сделанных предположениях

$$C_W = \begin{pmatrix} 1 & c_{12} & \cdots & c_{1m} \\ c_{12} & \ddots & & \vdots \\ \vdots & & \ddots & c_{(m-1)m} \\ c_{1m} & \cdots & c_{(m-1)m} & 1 \end{pmatrix}. \qquad (4)$$

Также процессы $Y(t)$ и $W(s)$ предполагаются стационарно связанными в строгом смысле.

Линейная *входо-выходная* модель системы, характеризуемой плотностями распределения (2), ищется в виде

$$\hat{Y}(t;\mathbf{G}) = \sum_{k=1}^{\infty} G(k)W(t-k),\ t = 1, 2, ..., \qquad (5)$$

где $\hat{Y}(t;\mathbf{G}) = (\hat{y}_1(t;\mathbf{G}),\ldots,\hat{y}_n(t;\mathbf{G}))^T$ — выходной процесс модели, $\mathbf{G} = \{G(k),\ k\in[1, \infty)\}$, $G(k)$, $k = 1, 2, ...$ — матричнозначные (размерностью $n \times m$) коэффициенты весовой функции линеаризованной модели, подлежащие идентификации в соответствии с условием совпадения взаимной информации i-й компоненты выходного процесса $y_i(t)$ и j-й компоненты входного процесса $w_j(s)$ системы, характеризуемой плотностями распределения (2), и взаимной информации i-й компоненты выходного процесса $\hat{y}_i(t, \mathbf{G})$ и j-й компоненты входного процесса $w_j(s)$ модели (5) для всех $i = 1, ..., n$, $j = 1, ...,$

m. Аналитически данный критерий имеет следующий вид:

$$I_{y_i w_j}(\tau) = I_{\hat{y}_i(\mathbf{G}) w_j}(\tau),\ \tau = 1, 2, \ldots. \qquad (6)$$

Безусловно, с точки зрения задачи статистической линеаризации условие (6) необходимо дополнить условием совпадения математических ожиданий выходных процессов системы и модели

$$\mathbf{M}\{y_i(t)\} = \mathbf{M}\{\hat{y}_i(t;\mathbf{G})\} = 0,\ i = 1, \ldots, n. \qquad (7)$$

Очевидно, что в рамках данной постановки задачи условие (7) выполняется автоматически.

Далее, следуя условию нормировки (3), на компоненты выходного процесса модели (5) налагается условие единичности дисперсии

$$\mathbf{D}\{\hat{y}_i(t;\mathbf{G})\} = 1,\ i = 1, \ldots, n, \qquad (8)$$

и, как следствие, строки матричнозначных коэффициентов модели (5) должны удовлетворять условию

$$\sum_{k=1}^{\infty} \vec{g}_i(k) C_W \vec{g}_i^T(k) = 1,\ i = 1, \ldots, n, \qquad (9)$$

где $\vec{g}_i(k) = (g_{i1}(k), \ldots, g_{im}(k))$ — i-я строка матрицы $G(k)$ из (5).

Соотношение (9) очевидным образом определяется цепочкой

$$1 = \mathbf{D}\{\hat{y}_i(t;\mathbf{G})\} = \mathbf{D}\left\{\sum_{k=1}^{\infty} \vec{g}_i(k) W(t-k)\right\} =$$

$$= \sum_{k=1}^{\infty} \vec{g}_i(k) \mathbf{M}\{W(t-k) W^T(t-k)\} \vec{g}_i^T(k) +$$

$$+ \sum_{p \neq q} \vec{g}_i(p) \mathbf{M}\{W(t-p) W^T(t-q)\} \vec{g}_i^T(q) = \sum_{k=1}^{\infty} \vec{g}_i(k) C_W \vec{g}_i^T(k)$$

в силу описания модели (5) и условий нормировки (3), (4), (8).

Выражения (6) и (7) представляют собой, таким образом, критерий статистической линеаризации системы, характеризуемой плотностями распределения (2). В терминах плотностей распределения условие (6) записывается в виде

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \left(\ln \frac{p_{y_i, w_j}(y, w, \tau)}{p_{y_i}(y) p_{w_j}(w)}\right) p_{y_i, w_j}(y, w, \tau)\, \mathrm{d}y\, \mathrm{d}w =$$

$$= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \left(\ln \frac{p_{\hat{y}_i(\mathbf{G}), w}(\hat{y}(\mathbf{G}), w, \tau)}{p_{\hat{y}_i(\mathbf{G})}(\hat{y}(\mathbf{G})) p_{w_j}(w)}\right) \times$$

$$\times\, p_{\hat{y}_i(\mathbf{G}), w_j}(\hat{y}(\mathbf{G}), w, \tau)\, \mathrm{d}\hat{y}(\mathbf{G})\, \mathrm{d}w,$$

$$i = 1, \ldots, n,\ j = 1, \ldots, m,\ \tau = 1, 2, \ldots,$$

где $p_{y_i, w_j}(y, w, \tau)$, $p_{\hat{y}_i(\mathbf{G}), w_j}(\hat{y}(G), w, \tau)$ — соответственно совместные плотности распределения i-й компоненты выходного и j-й компоненты входного процессов системы, характеризуемой плотностями распределения (2), и i-й компоненты выходного и j-й компоненты входного процессов модели (5); $p_{y_i}(y)$, $p_{\hat{y}_i(\mathbf{G})}(\hat{y}(\mathbf{G}))$ и $p_{w_j}(w)$ — соответственно маргинальные плотности распределения i-х компонент выходных процессов $Y(t)$ системы, характеризуемой плотностями распределения (2), модели $\hat{Y}(t;\mathbf{G})$ (5) и j-й компоненты входного процесса системы, характеризуемой плотностями распределения (2), равно как и модели (5), $W(s)$, $\tau = t - s$.

Метод решения

Пусть

$$v_i\langle -\tau; t\rangle = \sum_{j=1}^{\tau-1} \vec{g}_i(j) W(t-j) + \sum_{j=\tau+1}^{\infty} \vec{g}_i(j) W(t-j),$$

$$\tau = 1, 2, \ldots$$

— последовательность случайных величин, которые очевидно являются гауссовыми с нулевыми средними и дисперсиями, имеющими в силу (9) вид

$$\mathbf{D}\{v_i\langle -\tau; t\rangle\} = \sum_{j=1}^{\tau-1} \vec{g}_i(j) C_W \vec{g}_i^T(j) +$$

$$+ \sum_{j=\tau+1}^{\infty} \vec{g}_i(j) C_W \vec{g}_i^T(j) = 1 - \vec{g}_i(\tau) C_W \vec{g}_i^T(\tau),$$

$$\tau = 1, 2, \ldots .$$

Тогда, в рамках введенных обозначений, $(m+1)$-мерный случайный вектор

$$V_i(t, \tau) = \left(v_i\langle -\tau; t\rangle, w_1(t-\tau), \ldots, w_m(t-\tau)\right)^T$$

является гауссовым с ковариационной матрицей

$$C_{V_i(t,\tau)} =$$

$$= \begin{pmatrix} 1 - \vec{g}_i(\tau) C_W \vec{g}_i^T(\tau) & 0 & \cdots & \cdots & 0 \\ 0 & 1 & c_{12} & \cdots & c_{1m} \\ \vdots & c_{12} & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & c_{(m-1)m} \\ 0 & c_{1m} & \cdots & c_{(m-1)m} & 1 \end{pmatrix},$$

а для двумерного случайного вектора $(\hat{y}_i(t;\mathbf{G})\ w_j(t-\tau))^T$ можно записать следующее соотношение:

$$\begin{pmatrix} \hat{y}_i(t;\mathbf{G}) \\ w_j(t-\tau) \end{pmatrix} = A_{ij}(\tau) V_i(t, \tau),$$

где $(2 \times (m+1))$-мерная матрица $A_{ij}(\tau)$ имеет вид

$$A_{ij}(\tau) = \begin{pmatrix} 1 & g_{i1}(\tau) & \cdots & g_{ij}(\tau) & g_{i(j+1)}(\tau) & \cdots & g_{im}(\tau) \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix},$$

и, как и всюду, $g_{i1}(\tau)$, ..., $g_{im}(\tau)$ — элементы i-й строки матрицы $G(\tau)$ из (5).

Следовательно, случайный вектор $(\hat{y}_i(t;\mathbf{G})\ w_j(t-\tau))^T$ является гауссовым с ковариационной матрицей $C_{(\hat{y}_i w_i)}(\tau)$, определяемой соотношением

$$C_{(\hat{y}_i w_i)}(\tau) = A_{ij}(\tau) C_{V_i(t,\tau)} A_{ij}^T(\tau).$$

Вычисление произведения трех матриц в правой части дает

$$C_{(\hat{y}_i w_i)}(\tau) = \begin{pmatrix} 1 & \gamma_{ij}(\tau) \\ \gamma_{ij}(\tau) & 1 \end{pmatrix},$$

где $\gamma_{ij}(\tau)$ — j-я компонента вектор-столбца $C_W \vec{g}_i^T(\tau)$.

Таким образом, в силу формулы (1) следует, что взаимная информация $I_{\hat{y}_i(\mathbf{G}) w_j}(\tau)$ выходного и входного процессов модели (5) имеет вид

$$I_{\hat{y}_i(\mathbf{G}) w_j}(\tau) = -\frac{1}{2}\ln(1-\gamma_{ij}^2(\tau)),\ \tau = 1, 2, \ldots.$$

Тогда из условия (6) следуют искомые выражения для строк $\vec{g}_i(\tau)$ матричнозначных весовых коэффициентов $G(\tau)$, $\tau = 1, 2, \ldots$ модели (5):

$$\vec{g}_i^T(\tau) = C_W^{-1}\ \mathbf{I}_{y_i W}(\tau),\ \tau = 1, 2, \ldots, \qquad (10)$$

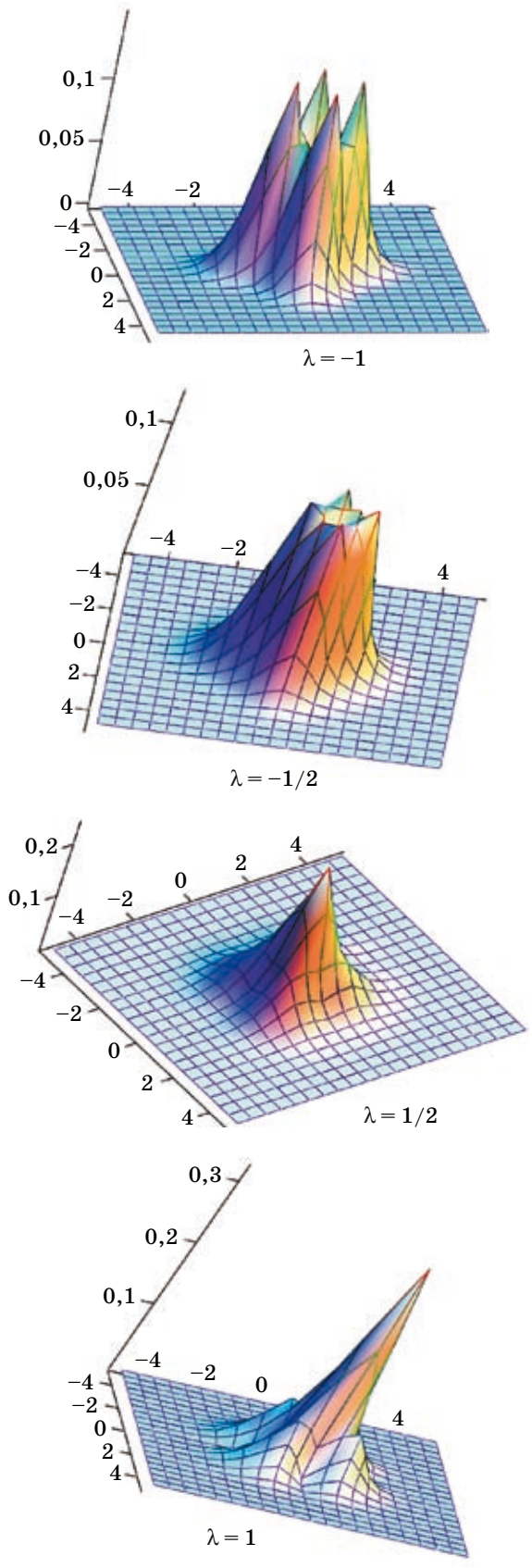
где

$$\mathbf{I}_{y_i W}(\tau) = \begin{pmatrix} \mathrm{sign}(\mathbf{m}_{y_i|w_1}(\tau)) \times \sqrt{1-\exp(-2I_{y_i w_1}(\tau))} \\ \vdots \\ \mathrm{sign}(\mathbf{m}_{y_i|w_j}(\tau)) \times \sqrt{1-\exp(-2I_{y_i w_j}(\tau))} \\ \vdots \\ \mathrm{sign}(\mathbf{m}_{y_i|w_m}(\tau)) \times \sqrt{1-\exp(-2I_{y_i w_m}(\tau))} \end{pmatrix}.$$

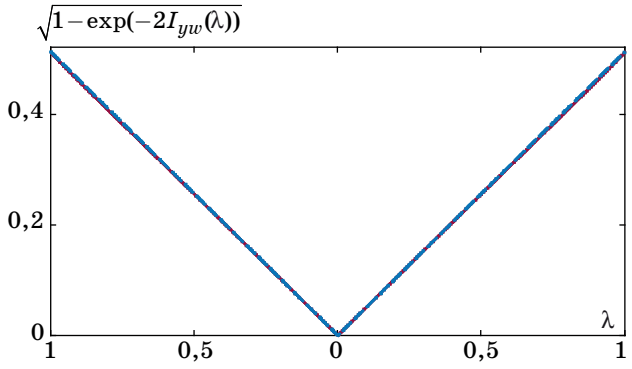
В формуле (10) $\mathbf{m}_{y_i|w_j}(\tau)$ — регрессия $y_i(t)$ на $w_j(t-\tau)$; $\mathrm{sign}(x) = 1$ при $x \geq 0$, $\mathrm{sign}(x) = -1$ при $x < 0$ — знак соответствующей функции регрессии соответствует «взаимной ориентации» входного и выходного процессов; подкоренное выражение всегда неотрицательно, поскольку взаимная информация принимает значения на положительной полуоси $[0, +\infty)$.

Таким образом, обращение в нуль весовых коэффициентов линеаризованной модели (5) системы (2) эквивалентно обращению в нуль взаимной информации выходного и входного процессов системы (2). В свою очередь, последнее возможно лишь тогда, когда данные процессы стохастически независимы. При этом, как отмечено выше, существуют примеры, когда традиционные меры зависимости обращаются в нуль при наличии стохастической зависимости между переменными.

Так, можно рассмотреть следующую плотность распределения, принадлежащую классу распределений О. В. Сарманова [7, 8], которая имеет вид



■ ***Рис. 1.*** *Форма плотности (11) при различных значениях параметра* λ



■ ***Рис. 2.*** *Близость значений выражения (12) и $S_{yw}(\lambda)$ при различных значениях параметра λ в плотности (11)*

$$p_\lambda(y,w)=\frac{e^{-\frac{w^2+y^2}{2}}}{2\pi}\times$$
$$\times\left(1+\lambda\left(2e^{-\frac{3}{2}w^2}-1\right)\left(2e^{-\frac{3}{2}y^2}-1\right)\right),$$
$$-1\le\lambda\le 1. \qquad (11)$$

Ее маргинальные плотности являются стандартными гауссовыми. Для плотности (11) коэффициент корреляции и дисперсионное отношение равны нулю, а максимальный коэффициент корреляции имеет вид

$$S_{yw}(\lambda)=\left(\frac{4}{\sqrt{7}}-1\right)|\lambda|.$$

Значение параметра λ оказывает существенное влияние на форму плотности (11) (рис. 1).

При этом величина $\sqrt{1-\exp(-2I_{yw}(\lambda))}$ из выражения (10), соответствующая плотности $p_\lambda(y, w)$ в (11), зависит от модуля параметра λ строго монотонно (рис. 2) и обращается в нуль только при $\lambda = 0$, что эквивалентно независимости случайных величин.

На рис. 2 показана зависимость значений

$$\sqrt{1-\exp(-2I_{yw}(\lambda))} \qquad (12)$$

от параметра λ в плотности (11) в сравнении с соответствующими значениями максимального коэффициента корреляции $S_{yw}(\lambda)$, наглядно демонстрирующая практически полное их совпадение.

Таким образом, если, например, стохастическая зависимость (2) между компонентами выходного процесса, $y_i(t)$, и входного процесса, $w_j(s)$, некоторой нелинейной системы определяется плотностью распределения (конечно, предполагаемой неизвестной исследователю) вида (11) с параметром $\lambda = \lambda_{ij}(\tau)$, $\tau = t - s$, то применение как традиционных корреляционных, так и дисперсионных методов статистической линеаризации привело бы, при построении модели (5), к представлению компонент выходного процесса системы как тождественного нуля, что исключается при использовании данного теоретико-информационного подхода.

Заключение

В настоящей работе для многомерных нелинейных систем с белым гауссовым векторнозначным входным шумом рассмотрена задача определения статистически эквивалентных линейных входо-выходных моделей из условия покомпонентного совпадения взаимной информации входного и выходного процессов системы и входного и выходного процессов модели. Получаемые в конечном итоге уравнения для элементов весовых матриц линеаризованной модели определяют их как функции взаимной информации входного и выходного процессов системы, обращающиеся в нуль только при обращении в нуль взаимной информации, т. е. при стохастической независимости данных компонент входного и выходного процессов системы.

Литература

1. **Сарманов О. В.** Максимальный коэффициент корреляции (несимметричный случай) // Докл. АН СССР. 1958. Т. 121. № 1. С. 52–55.
2. **Rényi A.** On measures of dependence // Acta Math. Hung. 1959. Vol. 10. N 3–4. P. 441–451.
3. **Дисперсионная** идентификация / Под ред. Н. С. Райбмана. — М.: Наука, 1981. — 320 с.
4. **Чернышев К. Р.** Информационные меры зависимости в статистической линеаризации // Автоматика и телемеханика. 2002. № 9. С. 74–84.
5. **Сарманов О. В., Захаров Е. К.** Меры зависимости между случайными величинами и спектры стохастических ядер и матриц // Математический сборник. 1960. Т. 52(94). № 4. С. 953–990.
6. **Stoorvogel A. A., van Schuppen J. H.** System identification with information theoretic criteria // Identification, adaptation, learning / Ed. by S. Bittanti and G. Picci. — Berlin: Springer-Verlag, 1996. P. 289–338.
7. **Сарманов О. В.** Замечания о некоррелированных гауссовских зависимых случайных величинах // Теория вероятностей и ее применения. 1967. Т. 12. № 1. С. 141–143.
8. **Kotz S., Balakrishnan N., Johnson N. L.** Continuous Multivariate Distributions. Vol. 1. Models and Applications. Second ed. — N. Y.: Wiley, 2000. — 752 p.

УДК 378.4

МОДЕЛЬ УПРАВЛЕНИЯ РИСКАМИ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Т. П. Костюкова,
доктор техн. наук, профессор
И. А. Лысенко,
старший преподаватель
Уфимский государственный авиационный технический университет

Изложен подход по управлению рисками образовательного учреждения. Приведена классификация внешних и внутренних рисков. Предложена модель управления рисками, обеспечивающая учет их влияния, повышение оперативности и качества принятия управленческих решений в вузе.

Ключевые слова *— образовательное учреждение, внешние риски, внутренние риски, оценка рисков, управление рисками.*

Введение

В процессе функционирования и развития общества исключительно важную роль играет социальный институт высшего образования, благодаря которому накопленные трудом предшествующих поколений материальные и духовные ценности, знания, опыт, традиции передаются новому поколению людей и усваиваются им. Изменение условий функционирования рынка образовательных услуг в современных условиях социально-экономического развития актуализирует вопросы, связанные с управлением рисками в образовательных учреждениях (ОУ), поскольку усиление самостоятельности вузов и их независимости влечет за собой увеличение управленческих и особенно финансовых рисков за неправильно принятые решения. В этой связи возникает необходимость поиска эффективных внутривузовских механизмов управления рисками, тем более что на сегодняшний день общепризнанный теоретический подход к проблеме управления рисками в сфере образования отсутствует.

Управление рисками в образовательной деятельности вуза

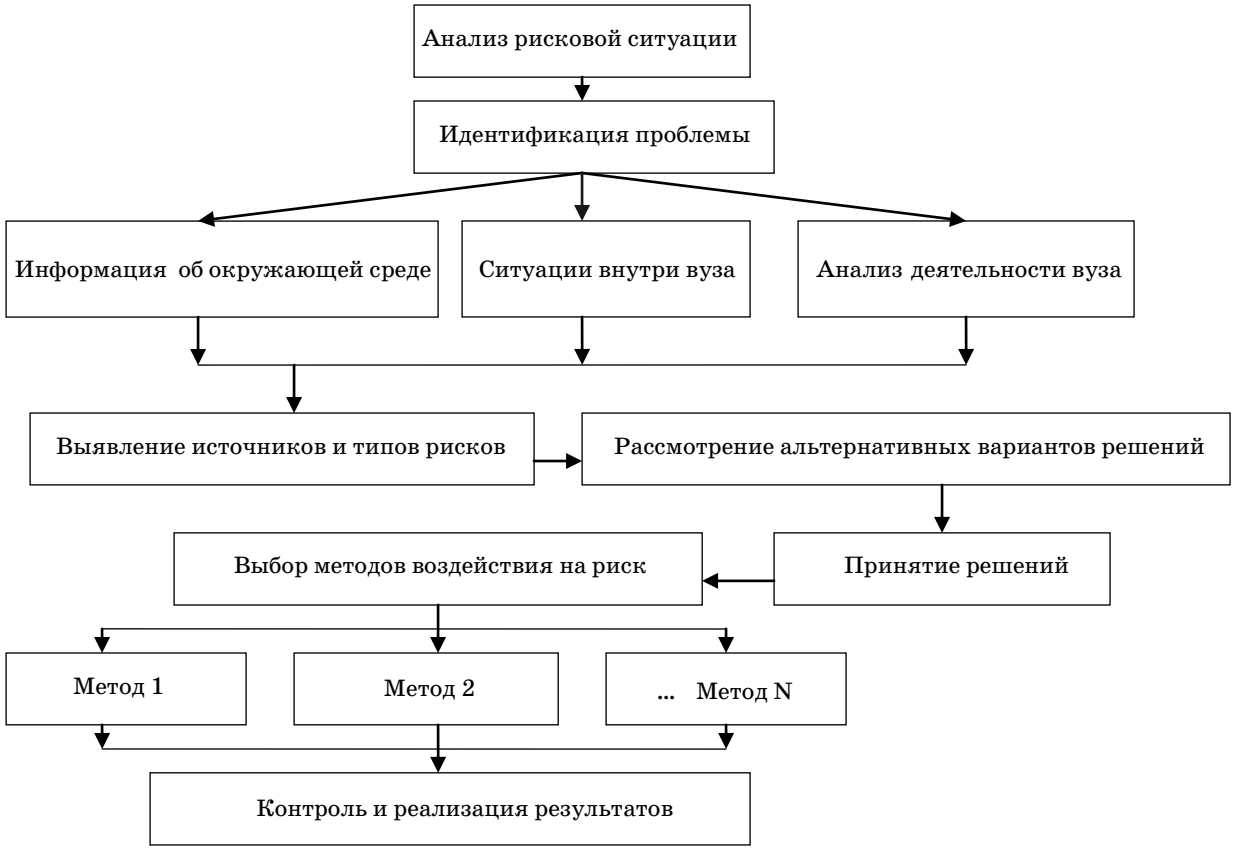
Образование — достаточно специфическая область, для которой характерны свои особые риски, отличные от традиционно рассматривающихся в теории риск-менеджмента. Поэтому важно не только идентифицировать риски образовательной деятельности, но и систематизировать их, осуществлять их анализ, взаимозависимость между собой и степень влияния на достижение главной цели вуза — оказание качественных образовательных услуг.

Для реализации функции управления риском в ОУ целесообразно осуществлять эту функцию с помощью специальной подсистемы в системе управления вузом или специализированного подразделения в организационной структуре вуза, которое на основе полученной информации с использованием различных методов теории риска разрабатывает мероприятия для снижения уровня риска или удержания его в допустимых пределах. Большинство передовых ОУ внедряют свою систему оценки и управления рисками, при этом они сталкиваются со значительными трудностями: отсутствием стандартизированных методик и затруднением адаптации используемых; отсутствием сравнительной базы экономических показателей, специалистов и структур по управлению рисками.

В соответствии с представленной [1] классификацией рисков ОУ в таблице выделены основные внутренние и внешние риски ОУ, влияющие на качество подготовки выпускников вуза, и предложена модель управления рисками образовательных организаций (рисунок), в соответствии с которой для каждой группы образовательных рисков вырабатываются свои пути решения, т. е. методы управления данными рисками.

■ *Риски образовательного учреждения*

Внешние риски	Внутренние риски
Переход на новую систему финансирования	Обеспечение должного уровня качества образовательных услуг
Уменьшение бюджетной составляющей финансирования	Несоответствие предлагаемого набора образовательных услуг требованиям рынка
Экономический кризис	Недостаточный контингент студентов 1-го курса
Конкуренция вузов	Высокая цена образовательных услуг
Сокращение контингента студентов	Неэффективность работы PR-служб
Изменение конъюнктуры рынка труда	Имидж ОУ на рынке
Недофинансирование или задержка финансирования из федерального бюджета	Повышение статуса ОУ за счет развития сети филиалов
Сокращение объемов финансируемых хоздоговорных и госбюджетных НИР	Снижение качества образования в ОУ за счет развития сети филиалов
Переход учреждений бюджетной сферы на новую систему оплаты труда	Структура управления образовательным учреждением
Изменение психологического климата в обществе	Недостаточное развитие материальной базы
Изменение законодательства РФ в области образования (переход на уровневую систему образования)	Неэффективная кадровая политика (повышение квалификации преподавателей, программы обмена преподавателями, привлечение сторонних специалистов и др.)
Зависимость от мировых тенденций	Низкий уровень заработной платы и социального пакета сотрудников
Изменение формы собственности вуза	Неэффективное использование внебюджетных средств



■ *Модель управления рисками образовательных организаций*

Неотъемлемым компонентом образовательной деятельности в условиях рыночных отношений является существование неопределенности, обусловленное непостоянством рыночного спроса и предложения на образовательные услуги, поэтому комплектование вуза необходимым количеством студентов подвержено значительному риску. Наиболее сложным при этом является вопрос цены на образовательные услуги вуза, в связи с чем приведен пример нейтрализации внутреннего риска вуза (см. таблицу) «Недостаточный контингент студентов 1-го курса» [2], а также расчет точки безубыточности организации процесса производства образовательных услуг [3].

При условии приема вузом на N специальностей на бюджетной и коммерческой основах согласно лицензии может быть принято M человек, из них m — на бюджетной основе.

Ожидаемая прибыль R_j от приема студентов на j-ю специальность может быть определена как $R_j = Q_j - C_j b_j^*$, где Q_j — доход вуза (кафедры); C_j — переменные затраты на подготовку специалиста по j-й специальности; b_j^* — спрос на j-ю специальность:

$$Q_j = \begin{cases} S_{бj} b_j, b_j < x_j \\ S_{бj} x_j + S_{кj}(b_j - x_j), x_j \le b_j \le (x_j + y_j); \\ S_{бj} x_j + S_{кj} y_j, b_j > (x_j + y_j) \end{cases}$$

$$b_j^* = \begin{cases} b_j, b_j < x_j \\ b_j, x_j \le b_j \le (x_j + y_j), \\ x_j + y_j, b_j > (x_j + y_j) \end{cases}$$

здесь x_j — количество бюджетных мест, выделенных на j-ю специальность; y_j — количество коммерческих мест, выделенных на j-ю специальность; $S_{бj}$ — средства, выделяемые на одного бюджетного студента j-й специальности; $S_{кj}$ — плата за обучение одного студента на коммерческой основе по j-й специальности.

Прибыль от приема студентов на N специальностей может быть определена с учетом ограничений

$$\sum_{j=1}^{N} x_j \le m, \ \sum_{j=1}^{N} (x_j + y_j) \le M$$

по формуле

$$\sum_{j=1}^{N} R_j = \sum_{j=1}^{N} Q_j - \sum_{j=1}^{N} C_j b_j^* - K,$$

где переменная K — постоянные издержки вуза на организацию учебного процесса.

Задача оптимизации плана приема студентов на 1-й курс сводится к оптимизации целевой функции — ожидаемой прибыли R_j и нахождению оптимального контингента студентов, что позволит нейтрализовать рисковую ситуацию «Недостаточный контингент студентов 1-го курса» (см. таблицу).

На основе метода «стоимостной анализ безубыточности» [4] и данных по общим издержкам на организацию образовательного процесса одного из факультетов Уфимского государственного авиационного технического университета [3] произведен расчет точки безубыточности организации процесса производства образовательных услуг.

Общие затраты $V = f_v(q, X) + K$ на образовательные услуги для q принятых на обучение выражаются через постоянные K и переменные X издержки образовательного учреждения и являются случайной величиной. Величины X и K — случайные, поэтому для определения точки безубыточности организации процесса производства образовательных услуг q_0 использован вероятностный подход, в качестве функции выбрано уравнение прямой $V = Xq + K$. При фиксированном числе студентов q величина прибыли $R = (y - X)q - K$ и имеет нормальный закон распределения. Точка безубыточности $q_0 = K/(y - X)$ и является случайной величиной. Поскольку величины V, X и K являются случайными, величина прибыли при фиксированном числе студентов также является случайной, поэтому введена вероятность P увеличения прибыли R больше минимального значения R_0: $P(R > R_0) = P_0$, где P_0 — заданное значение вероятности (уровень надежности). Для нормального закона распределения при известных числовых характеристиках $P(R > R_0) = 1 - \Phi_0((R_0 - m_r)/S_r)$, где Φ_0 — функция Лапласа, m_r, S_r — математическое ожидание и среднеквадратическое отклонение соответственно случайной величины R. Для нормального закона распределения прибыли $R_0 = m_r - zS_r$, где z — квантиль нормированного нормального закона.

Предложенные расчеты может использовать служба маркетинга вуза при выборе различных вариантов цены обучения студентов и заданного уровня надежности, руководствуясь желаемой минимальной прибылью. Построение зависимости минимальной прибыли $R_0 = R(q)$ при определенном уровне надежности P_0 и фиксированной цене обучения позволяет определить количество студентов, обеспечивающих заданную минимальную прибыль, а также оценить ожидаемую минимальную прибыль, если известно прогнозное значение числа студентов на новый учебный год.

Заключение

Таким образом, прогнозирование и управление рисками способствует повышению оператив-

ности и качеству принятия управленческих решений в вузе. Внедрение подсистемы управления рисками в вузе на основе предложенной модели позволит:

— сформировать реестр рисков вуза;

— провести количественную и качественную оценку выявленных рисков;

— выбрать способы и методы реагирования на риски;

— детально проработать мероприятия по управлению рисками;

— организовать регулярный мониторинг выявленных рисков и контроль выполнения мероприятий по управлению рисками.

Литература

1. **Костюкова Т. П., Лысенко И. А.** Концепция оценки рисков в образовательной деятельности вуза // Информатика: проблемы, методология, технологии: Материалы Девятой Междунар. науч.-метод. конф., 12–13 февраля 2009 г. Воронеж: Издательско-полиграфический центр ВГУ, 2009. Т. 1. С. 363–366.
2. **Костюкова Т. П., Лысенко И. А.** Теоретические основы информатизации управления вузом на примере оптимизации плана приема студентов // Университеты в образовательном пространстве региона: опыт, традиции и инновации: Материалы науч.-метод. конф., Петрозаводск, 21–23 ноября 2007 г. / ПетрГУ. Петрозаводск, 2007. Ч. 1. С. 184–187.
3. **Костюкова Т. П., Лысенко И. А.** Управление рисками в образовательной деятельности вуза на примере Уфимского государственного авиационного технического университета // Системы управления и информационные технологии. Рубрика «Перспективные исследования». М.; Воронеж: Научная книга. 2010. № 1.1 (39). С. 162–166.
4. **Краковский Ю. М., Карнаухова В. К.** Выбор цены образовательной услуги на основе имитационно-аналитической процедуры // Университетское управление. 2004. № 4 (32). С. 33–37.

УДК 330.101.5

ЛОГИКО-ВЕРОЯТНОСТНАЯ МОДЕЛЬ ОПЕРАЦИОННОГО РИСКА БАНКА

Е. И. Карасева,
аспирант
А. Г. Степанов,
доктор пед. наук, доцент
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Предложены структурная, логическая и вероятностная модели операционного риска банка с внутренними, внешними и повторными инициирующими событиями для вычисления резервирования под операционный риск. Изложены результаты исследований логико-вероятностной модели операционного риска банка и анализа вкладов инициирующих и повторных событий в риск.

Ключевые слова *— операционный риск, структурная, логическая, вероятностная модели риска, внешние, внутренние и повторные инициирующие события, резервирование капитала, управление, анализ.*

Введение

В работе [1] обсуждается состояние мировой экономической науки на современном этапе и отмечается, что она подошла к своему естественному рубежу, за которым ничего конструктивного нет. Однако резервы развития экономической науки далеко не исчерпаны. Имеющиеся результаты в других областях научных знаний позволяют решать существующие и новые задачи экономики на основе, например, информационных инновационных интеллектуальных технологий ($И^3$-технологий) [2] с логико-вероятностными (ЛВ) моделями. Ниже рассматривается использование $И^3$-технологии для моделирования, оценки и анализа резервирования капитала под операционный риск банка.

Проблема операционного риска

В условиях глобализации мирового рынка, кризиса и реформ главной задачей государства является обеспечение устойчивости экономики. Устойчивость достигается за счет обеспечения стабильности функционирования банков, фирм и предприятий, заводов и фабрик, страховых и инвестиционных компаний и др. Негативные моменты в банковской сфере часто вызваны некачественным управлением рисками. Существует целый ряд банковских рисков, и нужно минимизировать каждый из них. Операционный риск имеет особое значение, так как относится ко всем направлениям деятельности банка, и его уменьшение — одна из сложных задач, с которой сталкиваются специалисты [3].

Базельский комитет дает следующее определение операционного риска: «Операционный риск — риск прямых или косвенных потерь от неадекватных или ошибочных внутренних процессов, действий персонала, компьютерных систем банка, внешних событий» [4]. Операционный риск оценивается величиной убытков (ожидаемых и непредвиденных потерь), которые должны быть «покрыты» соответствующим размером отчисляемого на операционный риск капитала [5]. Кроме того, с 1 июля 2010 года вступило в силу Положение Банка России «О порядке расчета размера операционного риска». Положение устанавливает порядок расчета размера риска для включения его в норматив достаточности капитала банка (Н1), установленного Инструкцией Банка России № 110-И «Об обязательных нормативах банков» [6]. Операционный риск рассчитывается как средняя сумма чистых процентных и непроцентных доходов за 3 года, умноженная на коэффициент $\alpha = 0{,}15$. Однако у этого способа расчета есть отрицательные стороны, так как два банка с одинаковым уровнем доходов должны будут включить в расчет Н1 одинаковый размер операционного риска вне зависимости от того, какие внутренние процедуры контроля ими применяются и управляют ли они этими риска-

ми вообще. Базельский комитет предлагает использовать также стандартизированный (*The Standardised Approach — TSA*) и продвинутые (*Advanced Measurement Approaches — AMA*) методы. Заявляя об использовании продвинутого метода, банк может применять собственные модели операционного риска. Естественно, что частота и размеры операционных убытков в банках, использующих продвинутые подходы, ниже, чем в тех, где управлению операционным риском не уделяется должного внимания. Поэтому и распределение капитала на покрытие операционного риска банка, применяющего передовые методы, как правило, в полтора раза ниже, чем при использовании базового индикативного подхода [7].

12 сентября 2010 года Базельский комитет по банковскому надзору одобрил глобальную реформу мирового банковского сектора, получившую название «Базель-3». Она призвана повысить финансовую устойчивость мировой финансовой и банковской систем за счет увеличения банковских ликвидных резервов и улучшения их качества.

Цель данной работы — разработать и исследовать ЛВ-модели операционного риска для оценки, анализа и минимизации резервирования капитала под риск. ЛВ-модели показали высокую эффективность в задачах кредитного риска, риска портфеля ценных бумаг и при решении других экономических проблем [8]. Отметим, что ЛВ-модели для управления операционным риском банка ранее не использовались.

В литературе не описана модель операционного риска, которая учитывала бы связь внутренних и внешних событий, инициирующих риск. Недостаточно учитываются взаимосвязи операционного риска по направлениям бизнеса. Вследствие этого невозможен эффективный анализ и управление операционными рисками. Актуальна задача разработки адекватной математической модели операционного риска по отдельным направлениям бизнеса и в целом для банка. Это позволит сократить потери, обосновать резервирование капитала под операционный риск, выполнить требования Базельского комитета к методикам оценки резервирования под капитал.

Структурная модель операционного риска банка

Логико-вероятностная модель операционного риска банка является комплексной. Она включает в себя модели по восьми стандартным направлениям бизнеса банка: оказание банковских услуг корпоративным клиентам, органам государственной власти и местного самоуправления на рынке капиталов (Corporate finance); операции и сделки на рынке ценных бумаг и срочных финансовых инструментов (Trading and sales); банковское обслуживание физических лиц (Retail banking); банковское обслуживание юридических лиц (Commercial banking); осуществление платежей и расчетов (кроме платежей и расчетов, осуществляемых в рамках обслуживания своих клиентов (Payment and settlement)); агентские услуги (Agency services and custody); управление активами (Asset management); брокерская деятельность (Retail brokerage) [5].

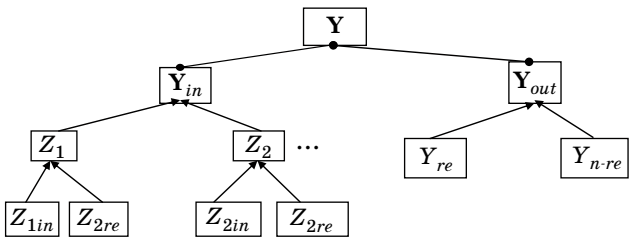
На операционный риск банка оказывают влияние внутренние и внешние инициирующие события, некоторые могут быть повторными (repeated). Повторные события — это события, которые оказывают непосредственное влияние на несколько бизнес-процессов, например изменение действующего законодательства, технические сбои при осуществлении транзакций и т. д.

Предлагается общий принцип решения этой проблемы, который заключается в том, что в ЛВ-модели операционного риска для каждого направления бизнеса банка разделяют внешние и внутренние инициирующие события. Тогда некоторые внешние инициирующие события могут оказаться общими (повторными) для отдельных операционных рисков.

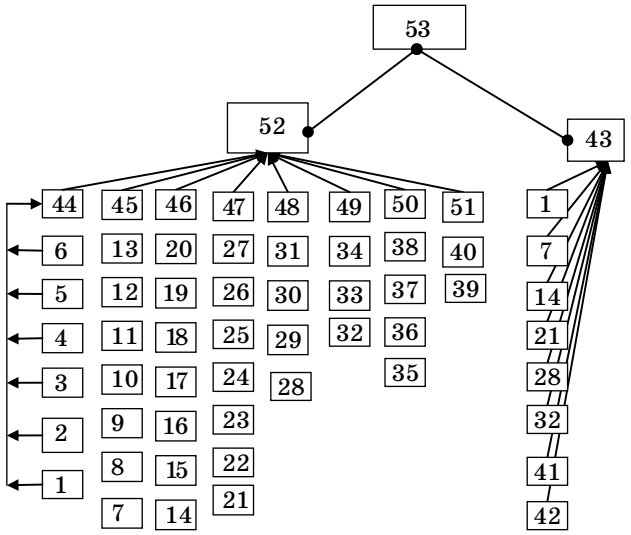
Схема связей внешних, внутренних и повторных событий в структурной модели операционного риска показана на рис. 1. Здесь сложное событие **Y** (финансовые потери вследствие операционного риска) состоит из объединения логической (Л) операцией И внутреннего $\mathbf{Y}_{in}$ и внешнего $\mathbf{Y}_{out}$ производных событий.

Внутреннее производное событие $\mathbf{Y}_{in}$ вызывают инициирующие события Z_1, ..., Z_n с Л-связью ИЛИ. В каждом из событий Z_1, ..., Z_n в свою очередь выделяют внутренние Z_{in} и повторные Z_{re} события. Внешнее производное событие $\mathbf{Y}_{out}$ вызывают повторные Y_{re} и бесповторные $Y_{n\text{-}re}$ события, объединенные Л-связью ИЛИ. К бесповторным инициирующим событиям относятся те, которые косвенно влияют на бизнес-процесс, например мировой финансовый кризис, дефолт партнеров.

Таким образом, выделяется конечное множество повторных событий, встречающихся как во внутренних $\mathbf{Y}_{in}$, так и во внешних $\mathbf{Y}_{out}$ событиях



■ ***Рис. 1.*** *Внутренние, внешние и повторные события операционного риска*



■ ***Рис. 2.*** *Структурная модель операционного риска банка*

операционного риска. На рис. 2 такими событиями являются события *1*, *7*, *14*, *21*, *28*, *32*. Они входят во внешнее событие *43*. События *41* — мировой финансовый кризис и *42* — дефолт партнеров не являются во внешнем событии *43* повторными.

Опишем повторные инициирующие события:

Y_1 — внезапное изменение действующего экономического законодательства;

Y_7 — сбои в работе биржевых серверов (стихийные бедствия, кибератаки), крах фондовой биржи;

Y_{14} — технические сбои при осуществлении транзакций;

Y_{21} — сбои в работе инфраструктуры (отключение электроэнергии);

Y_{28} — внезапное изменение экономической ситуации;

Y_{32} — невыполнение партнерами своих обязательств.

Производные и инициирующие события ЛВ-модели операционного риска

Событие Y_{53} появляется от действия внутреннего производного события Y_{52} и внешнего — Y_{43}. Внутренний операционный риск возникает в банковской деятельности при следующих событиях: Y_{44}, Y_{45}, ..., Y_{51}. Опишем производные и инициирующие события ЛВ-модели операционного риска (см. рис. 2).

Y_{43} — производное событие внешних инициирующих событий. Оно включает в себя повторные Y_1, Y_7, Y_{14}, Y_{21}, Y_{28}, Y_{32} и бесповторные Y_{41}, Y_{42} события.

Y_{44} — оказание банковских услуг корпоративным клиентам, органам государственной власти и местного самоуправления на рынке капиталов: Y_1 — повторный; Y_2 — размещение эмиссионных ценных бумаг, первичное размещение эмиссионных и гарантированное размещение ценных бумаг; Y_3 — оказание банковских услуг при слиянии, поглощении или приватизации юридических лиц; Y_4 — секьюритизация; Y_5 — исследование рынков; Y_6 — инвестиционный консалтинг.

Y_{45} — операции и сделки на рынке ценных бумаг и срочных финансовых инструментов: Y_7 — повторный; Y_8 — приобретение ценных бумаг в целях получения инвестиционного дохода или перепродажи; Y_9 — срочные сделки с ценными бумагами, иностранной валютой, драгоценными металлами, деривативами; Y_{10} — выполнение функций маркет-мейкера; Y_{11} — позиции, открываемые за собственные средства; Y_{12} — операции РЕПО; Y_{13} — другие операции.

Y_{46} — банковское обслуживание физических лиц: Y_{14} — повторный; Y_{15} — предоставление кредита (займов); Y_{16} — привлечение денежных средств во вклады; Y_{17} — открытие и ведение банковских счетов физических лиц; Y_{18} — доверительное управление денежными средствами и (или) ценными бумагами; Y_{19} — предоставление консультаций по вопросам инвестирования; Y_{20} — обслуживание банковских карт, кассовое обслуживание.

Y_{47} — банковское обслуживание юридических лиц: Y_{21} — повторное; Y_{22} — предоставление кредитов (займов); Y_{23} — привлечение депозитов; Y_{24} — открытие и ведение банковских счетов юридических лиц; Y_{25} — осуществление платежей по поручению юридических лиц; Y_{26} — операции с векселями; Y_{27} — выдача банковских гарантий и поручительств, факторинговые, форфейтинговые операции, лизинговые операции, кассовое обслуживание, инкассация, оказание консультационных информационных услуг.

Y_{48} — осуществление платежей и расчетов (кроме платежей и расчетов, осуществляемых в рамках обслуживания своих клиентов): Y_{28} — повторное; Y_{29} — осуществление расчетов на нетто-основе, клиринг; Y_{30} — осуществление валовых расчетов; Y_{31} — инкассовые операции.

Y_{49} — агентские услуги: Y_{32} — повторное; Y_{33} — доверительное хранение документов, ценных бумаг, депозитарных расписок, денежных средств и иного имущества; Y_{34} — осуществление агентских функций для эмитентов и функций платежного агента.

Y_{50} — управление активами: Y_{35} — доверительное управление ценными бумагами; Y_{36} — доверительное управление денежными средствами; Y_{37} — доверительное управление другим имуществом.

Y_{51} — брокерская деятельность: Y_{39} — брокерские услуги (в том числе розничные); Y_{40} — другие брокерские услуги.

Кортежи для описания производных событий модели операционного риска

Введем описание производных событий модели операционного риска банка в виде кортежей (см. рис. 2). Производные события (по направлениям бизнеса банка) являются функцией инициирующих событий, перечисляемых в скобках:

43 (1, 7, 14, 21, 28, 32, 41, 42);
44 (1, 2, 3, 4, 5, 6);
45 (7, 8, 9, 10, 11, 12, 13); (1)
46 (14, 15, 16, 17, 18, 19, 20);
47 (21, 22, 23, 24, 25, 26, 27);
48 (28, 29, 30, 31);
49 (32, 33, 34);
50 (35, 36, 37, 38);
51 (39, 40);
52 (44, 45, 46, 47, 48, 49, 50, 51);
53 (43, 52).

Кортежи для производных событий ЛВ-модели операционного риска удобны для изменения структурной модели риска и планирования модельных исследований на компьютере при введении и исключении повторных и инициирующих событий.

Логико-вероятностная модель появления финансовых потерь от операционного риска можно записать, соединяя соответствующие инициирующие события операцией Л-сложения ИЛИ.

Вероятность появления потерь от инициирующего события Y_i равна P_i, а вероятность отсутствия потерь от этого события равна $1 - P_i$. Поэтому в записи производных событий в виде кортежей знак Л-операции опущен и его нужно вводить в зависимости от постановки задачи.

Машинное представление структурной модели операционного риска банка

Обозначим события и Л-переменные идентификаторами в виде порядкового номера события на структурной модели операционного риска банка, которая вводится в некоммерческий программный комплекс А. С. Можаева (АСМ) для компьютерного моделирования [9].

Для компьютерных исследований запись модели операционного риска приведена в табл. 1. Модель имеет 53 вершины (события). Максимальное число заходящих дуг в вершину — 8. Число инициирующих вершин — 42 (пронумерованы от 1 до 42). Инициирующие события имеют вероятности, определяемые по статистическим данным или экспертным методом.

Событие 52 является производным событием от внутренних инициирующих событий. Событие 43 является производным событием от внешних инициирующих событий. Событие 53 является объединением внешних и внутренних событий Л-связью И. Инициирующие события 1, 7, 14, 21, 28, 32 являются повторными, поскольку входят во внутренние и внешние события.

Производные события являются функциями инициирующих событий. В производных событиях 43, 44, ..., 51 события в скобках связаны Л-операцией ИЛИ. Для производного события 53 события в скобках связаны Л-операцией И.

Внешнее событие 43 (1, 7, 14, 21, 28, 32, 41, 42) состоит из повторных событий 1, 7, 14, 21, 28, 32, которые входят во внутренние и внешние события. Внешние инициирующие события 41 и 42 являются бесповторными.

Машинное табличное представление операционного риска банка в целях его моделирования

■ ***Таблица 1.*** *Машинное табличное представление модели операционного риска*

Производное событие		Инициирующие события для производных событий															
1		2		3		4		5		6		7		8		9	
№	связь	№	связь	№	связь	№	связь	№	связь	№	связь	№	связь	№	связь	№	связь
43	2	1	1	7	1	14	1	21	1	28	1	32	1	41	1	42	1
44	2	1	1	2	1	3	1	4	1	5	1	6	1	0	0	0	0
45	2	7	1	8	1	9	1	10	1	11	1	12	1	13	1	0	0
46	2	14	1	15	1	16	1	17	1	18	1	19	1	20	1	0	0
47	2	21	1	22	1	23	1	24	1	25	1	26	1	27	1	0	0
48	2	28	1	29	1	30	1	31	1	0	0	0	0	0	0	0	0
49	2	32	1	33	1	34	1	0	0	0	0	0	0	0	0	0	0
50	2	35	1	36	1	37	1	38	1	0	0	0	0	0	0	0	0
51	2	39	1	40	1	0	0	0	0	0	0	0	0	0	0	0	0
52	2	44	1	45	2	46	2	47	2	48	2	49	2	50	2	51	2
53	2	43	102	52	102	0	0	0	0	0	0	0	0	0	0	0	0

в программном некоммерческом комплексе АСМ приведено в табл. 1.

В каждом из столбцов 1–9 указывается номер события и тип его логической связи: 1 и 2 — Л-сложение, если оно происходит от инициирующего или от производного события соответственно; 102 — Л-умножение, если оно генерирует от производного события; 0 — связь отсутствует.

Логическая модель операционного риска в минимальной дизъюнктивной нормальной форме имеет $K = 74$ слагаемых. Фрагмент записи Л-функции операционного риска:

$$Y = Y_{40}Y_{42} \vee Y_{40}Y_{41} \vee Y_{39}Y_{42} \vee \vee Y_{39}Y_{41} \vee Y_{38}Y_{42} \vee Y_{38}Y_{41} \vee Y_{37}Y_{42} \ldots.$$

Многочлен вероятностной (В) функции также имеет $K = 74$ слагаемых. Фрагмент записи В-функции операционного риска:

$$P = \{Y = 0\} = Q_1Q_7Q_{14}Q_{21}Q_{28}Q_{32}P_{40}P_{42} + + Q_1Q_7Q_{14}Q_{21}Q_{28}Q_{32}P_{40}P_{41}Q_{42} + \ldots.$$

Резервирование под операционный риск

Программный некоммерческий комплекс АСМ не только строит Л- и В-функции финансовых потерь от операционного риска, но может оценить возможные финансовые потери в деньгах и, следовательно, резервирование под операционный риск. Для этого нужно задать денежные ресурсы по каждому из восьми направлений деятельности банка. Возможные финансовые потери Q_{52} вычисляются от событий внутреннего операционного риска по следующей формуле:

$$Q_{52} = P_{44}Q_{44} + P_{45}Q_{45} + \ldots + P_{51}Q_{51}, \qquad (2)$$

где Q_{44}, ..., Q_{51} — финансовые ресурсы по направлениям деятельности банка; P_{44}, ..., P_{51} — операционный риск по направлениям деятельности банка, под которым понимаем вероятность возможных потерь капитала.

Обратим внимание, что полученная формула (2) имеет ту же структуру, что и формула для расчета резервирования под операционный риск по требованиям Базельского комитета. Объем резервирования достигает 15 % валового дохода [4].

Ее существенное отличие от традиционных формул [3, 5] заключается в том, что здесь вероятности P_{44}, ..., P_{51} получены в результате Л-сложения инициирующих событий, а не арифметического сложения весов в скоринговых или экспертных методиках. Математически корректное Л-сложение дает точные результаты и позволяет оценить вклады в операционный риск всех инициирующих событий.

Итоговое событие Y_{53} и возможные финансовые потери всего банка, зависящие от внутренних и внешних инициирующих событий, вычисляются при соединении событий Y_{43} и Y_{52} логической операцией И.

Влияние внутренних инициирующих событий на операционный риск банка

Выполнены расчетные исследования по влиянию внутренних и внешних инициирующих событий на внутренний операционный риск банка. Операционный риск зависит от вероятностей инициирующих событий 1–42 (табл. 2). Значение операционного риска банка зависит от внешних и внутренних инициирующих событий. Рассмотрим пример расчетного исследования операционного риска банка. В каждом варианте приняты одинаковые вероятности для инициирующих событий $P_1 - P_{42}$.

По полученным результатам можно сделать следующие выводы.

1. Требование Базельского комитета о введении резервирования под операционный риск вполне оправдано, так как внутренний операционный риск банка высок ($P = 0{,}7162$ — вариант 3, столбец 3) и потери по направлениям бизнеса банка с большой вероятностью произойдут.

2. Чем больше вероятности инициирующих событий, тем больше операционный риск банка.

3. Чем больше вероятности инициирующих событий, тем больше отличаются оценки операционного риска при логическом и арифметическом сложении событий. При арифметическом сложении вероятностей риска по направлениям

■ ***Таблица 2.*** *Связь внутреннего операционного риска с вероятностями инициирующих событий*

Вариант	Вероятность инициирующих событий P_1–P_{42}	Внутренний операционный риск P_{52}	
		логический	арифметический
1	2	3	4
1	0,0031	0,1168	0,124
2	0,01	0,3310	0,4
3	0,031	0,7162	1,24

■ ***Таблица 3.*** *Внутренний операционный риск по направлениям бизнес-деятельности*

Идентификаторы производных событий	Операционный риск по направлениям при $P_{av} = 0{,}031$	Число событий в производном событии	Вес (β-коэффициент)
1	2	3	4
P_{44}	0,17216	6	0,18
P_{45}	0,19783	7	0,18
P_{46}	0,19783	7	0,12
P_{47}	0,19783	7	0,15
P_{48}	0,11835	4	0,18
P_{49}	0,09014	3	0,15
P_{50}	0,11835	4	0,12
P_{51}	0,06104	2	0,12

бизнеса могут получиться даже абсурдные оценки риска (больше 1 — вариант 3, столбец 4).

4. Если риски инициирующих событий малы (меньше 0,001), то оценки операционного риска при логическом и арифметическом сложении событий практически равны.

Значения внутреннего операционного риска по направлениям бизнеса банка (для событий 44–51) при средней вероятности инициирующих событий $P = 0{,}031$ представлены в табл. 3. Вероятности производных событий P_{44}, ..., P_{51} близки к весам направлений бизнеса банка (столбец 4), приведенным в работах [3, 5].

Влияние повторных событий на операционный риск банка

Выполнены расчетные исследования по влиянию внутренних, внешних и повторных инициирующих событий на внутренний и полный операционные риски банка. Результаты исследования влияния повторных событий на операционный риск банка приведены в табл. 4. Во всех вариантах вероятности инициирующих событий равны 0,031.

Повторные внешние инициирующие события могут входить в разные производные внутренние события. Это влияет на общий операционный риск. Например, дополнительно введем повторное внешнее событие Y_1 вместо события Y_{21} в производное событие Y_{51} и повторное внешнее событие Y_7 вместо события Y_{29} в производное событие Y_{52} (вариант 4). Число слагаемых в Л- и В-функциях риска уменьшится с 224 до 218, вероятность операционного риска также сократится (P_{57} = = 0,1706 вместо 0,1723).

В варианте 3 табл. 4 количество слагаемых равно 8, так как действует формула Л-поглощения

$$A \wedge (B \vee A) = A,$$

где A — логическая переменная для обозначения дизъюнкции внешних инициирующих событий; $B \vee A$ — логическая переменная для обозначения дизъюнкции внутренних инициирующих событий, включающих в себя также внешние инициирующие события, которые в рассматриваемом случае являются повторными.

■ ***Таблица 4.*** *Влияние повторных событий на операционный риск*

Вариант	Описание варианта	N (количество вершин)	N_i (количество инициирующих событий)	Y (вершина события)	K (количество слагаемых)	P_y (вероятность события)
1	Во внешних событиях 6 повторных и 2 не повторных	53	42	53	74	0,2053
2	Во внешних событиях все 8 повторных	59	48	59	320	0,1595
3	Во внешних событиях все 8 повторных по одному по каждому направлению деятельности банка	51	40	51	8 (Л-поглощение)	0,2226
4	Во внешних событиях 2 повторных и 6 не повторных	57	46	57	224	0,1722
5	2 внешних повторных события введены 2 раза во внутренние события	57	44	57	218	0,1706

Значимости и вклады инициирующих событий

Значимости и вклады инициирующих событий в операционный риск банка учитывают как место событий в модели риска, так и вероятности событий. В табл. 5 приведены значимости и вклады для варианта 4 из табл. 4. Значимости и вклады позволяют анализировать, а также управлять операционным риском банка.

Заметим, что значимости и вклады повторных событий 1 и 21 велики, так как они входят во внутренние и внешние инициирующие события. Вклады событий 41–46, входящие только во внешние события и не являющиеся повторными, в 2 раза меньше.

Если снизить вероятность возникновения события P_{21} с 0,031 до 0,021 (например, путем дополнительной установки независимого электроснабжения), то операционный риск P_{57} снизится с 0,1722 до 0,1637. То есть если фонд резервирования под операционный риск равен 100 тыс. дол.

■ ***Таблица 5.*** *Значимости и вклады инициирующих событий в риск при $P_{av} = 0{,}031$*

Номер события	Значимость события	Вклад на минус	Вклад на плюс
1	0,85258	−0,02643	+0,82615
2	0,05042	−0,00156	+0,04885
21	0,85258	−0,02643	+0,82615
23	0,05042	−0,00156	+0,04885
...	...	...	...
40	0,00548	−0,00156	+0,04885
41	0,55975	−0,01735	+0,54239
42	0,55975	−0,01735	+0,54239
43	0,55975	−0,01735	+0,54239
44	0,55975	−0,01735	+0,54239
45	0,55975	−0,01735	+0,54239
46	0,55975	−0,01735	+0,54239

■ ***Таблица 6.*** *Структурные значимости и вклады инициирующих событий в операционный риск при* $P_{av} = 0{,}5$

Номер события	Значимость события	Вклад на минус	Вклад на плюс
1	0,00781	−0,00390	+0,00390
2	+1,79E-12	−8,95E-13	+8,95E-13
21	0,00781	−0,00390	+0,00390
23	+1,79E-12	−8,95E-13	+8,95E-13
...	...	...	...
40	0,00781	−8,95E-13	+8,95E-13
41	0,00781	−0,00390	+0,00390
42	0,00781	−0,00390	+0,00390
43	0,00781	−0,00390	+0,00390
44	0,00781	−0,00390	+0,00390
45	0,00781	−0,00390	+0,00390
46	0,00781	−0,00390	+0,00390

США, то при снижении риска события он может быть установлен в размере 95 тыс. 64 дол. США.

Еще более разительны отличия структурных значимостей и вкладов [10] повторных событий, которые подсчитываются при $P_{av} = 0{,}5$ (табл. 6). Значимости и вклады повторных событий 1 и 21 на несколько порядков больше значимостей и вкладов внутренних инициирующих событий.

Заключение

Необходимость управления операционным риском определяется значительным размером возможных операционных убытков, которые могут создавать угрозу финансовой устойчивости банка. В настоящее время отсутствуют адекватные математические модели для оценки и анализа операционного риска всего банка и направлений его бизнеса. Впервые предложена методика построения ЛВ-модели операционного риска банка, объединяющая ЛВ-модели риска по направлениям бизнес-процессов. ЛВ-модель операционного риска банка учитывает внутренние, внешние и повторные инициирующие события. Данная методика может использоваться не только для банков, но и для бизнес-процессов любых компаний.

Предложено описание производных событий модели операционного риска с помощью кортежей, удобное для организации и проведения исследований. Разработаны и исследованы структурная, логическая и вероятностная модели операционного риска для всего банка и по направлениям его бизнеса. Получена ЛВ-модель для вычисления резервирования под операционный риск. Проведены исследования по влиянию повторных событий на операционный риск. Изложены результаты исследований значимостей и вкладов инициирующих и повторных событий в операционном риске банка. Разработаны методики анализа и управления операционным риском на основе вычисления значимостей и вкладов инициирующих событий.

Использование ЛВ-моделей снижает неопределенность в оценке и управлении операционным риском по сравнению со скоринговыми методиками и экспертными оценками.

Литература

1. **Балацкий Е. Б.** Мировая экономическая наука на современном этапе: кризис или прорыв? // Науковедение. 2001. № 2. http://vivovoco.rsl.ru/VV/PAPERS/ECCE/BALA.HTM (дата обращения: 20.10.2010).
2. **Соложенцев Е. Д., Карасев В. В.** И^3-технологии для управления риском в экономике // Журнал экономической теории. 2010. № 2. С. 151–162.
3. **Бухтин М. А.** Методика и практика управления операционными рисками в коммерческом банке / ИБД АРБ. — М., 2006. — 64 с.
4. **Международная** конвергенция измерения капитала и стандартов капитала: Уточненные рамочные подходы. http://www.cbr.ru/today/pk/print.asp?file=Basel.htm (дата обращения: 08.09.2010).
5. **Сазыкин Б. В.** Управление операционным риском в коммерческом банке. — М.: Вершина, 2008. — 272 с.
6. www. consultant.ru (дата обращения: 15.10.2010).
7. **Новикова А.** Практика применения продвинутых подходов управления операционными рисками // Аналитический банковский журнал. 2010. № 6 (180). http://bankir.ru/technology/article/6042517 (дата обращения: 01.09.2010).
8. **Соложенцев Е. Д.** Управление риском и эффективностью в экономике. Логико-вероятностный подход. — СПб.: Изд-во СПбГУ, 2009. — 270 с.
9. **Можаев А. С.** Универсальный графоаналитический метод, алгоритм и программный модуль построения монотонных логических функций работоспособности систем // Моделирование и анализ безопасности и риска в сложных системах: Тр. Междунар. научной школы МА БР-2003, Санкт-Петербург, 20–23 августа 2003 г. / СПбГУАП. СПб., 2003. С. 101–110.
10. **Рябинин И. А.** Надежность и безопасность структурно-сложных систем. 2-е изд. — СПб.: Изд-во СПбГУ, 2007. — 276 с.

УДК 551.52

ВЫСОТНО-СТРАТИФИЦИРОВАННЫЙ ТРЕХВОЛНОВЫЙ МЕТОД ИЗМЕРЕНИЯ ПАРАМЕТРОВ СОЛНЕЧНОЙ РАДИАЦИИ В БЕРЕГОВЫХ ЗОНАХ В ВИДИМОЙ ОБЛАСТИ СВЕТА

Ф. Г. Агаев,
доктор техн. наук, профессор
Э. А. Ибрагимов,
аспирант
Национальное аэрокосмическое агентство Азербайджана

Рассмотрен высотно-стратифицированный трехточечный трехволновый метод для измерения дискретных значений солнечной постоянной по результатам фотометрических измерений на береговой зоне. Даны необходимые формулы для проведения вычислений.

Ключевые слова *— солнечная радиация, трехволновый метод, видимая область солнечного спектра.*

Введение

Измерение параметров солнечной радиации важно в таких отраслях, как солнечная энергетика, атмосферное зондирование, климатология и др. Для калибровки солнечных фотометров, являющихся важным средством зондирования атмосферы, важно определение величины солнечной постоянной на рабочей длине волны. Классически данная задача решается методом диаграмм Ленгли, который предполагает проведение следующих операций [1].

1. С использованием закона Бугера—Бера для видимой области света

$$I(h,\lambda)=I_0(\lambda)e^{-m(h)\cdot\tau(h,\lambda)}, \qquad (1)$$

где $I(h, \lambda)$ — интенсивность оптического сигнала на длине волны λ на входе фотометра, расположенного на высоте h; $I_0(\lambda)$ — значение солнечной постоянной; $m(h)$ — оптическая воздушная масса на высоте h; $\tau(h, \lambda)$ — оптическая толщина атмосферы при заданных λ и h, вычисляют следующее выражение:

$$\ln I(h,\lambda)=\ln I_0(\lambda)-m(h)\tau(h,\lambda). \qquad (2)$$

2. Экстраполируя зависимость (2) до точки $m(h) = 0$, графически вычисляют величину $I_0(\lambda)$.

Основной недостаток данного способа заключается во влиянии нестабильности $\tau(h, \lambda)$ на полученный результат. Применение этого способа в береговых промышленных зонах связано с дополнительными трудностями, к которым относятся:

— наличие смеси в атмосфере береговых зон как крупнодисперсного морского аэрозоля, так и мелкодисперсного техногенного аэрозоля, степень временной нестабильности которых различна;

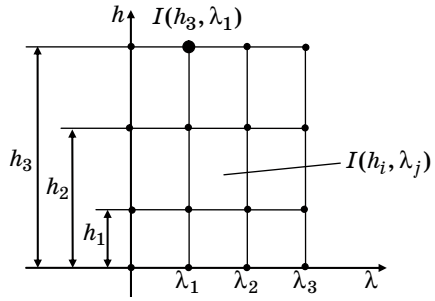
— зависимость долевого состава аэрозольной смеси в береговых зонах от высоты исследуемой местности.

Учитывая трудности в использовании метода диаграмм Ленгли в береговой зоне, авторы настоящей статьи предлагают новый высотно-стратифицированный трехволновый метод измерения солнечной постоянной.

Предлагаемый метод измерения солнечной постоянной

В береговой зоне выбираются три стратифицированные высотные точки на местности, где проводятся фотометрические измерения на трех фиксированных длинах волн λ_1, λ_2 и λ_3 (рисунок). В результате проведенных измерений получаем следующий набор данных:

$$\begin{vmatrix} I(h_1,\lambda_1); I(h_1,\lambda_2); I(h_1,\lambda_3) \\ I(h_2,\lambda_1); I(h_2,\lambda_2); I(h_2,\lambda_3) \\ I(h_3,\lambda_1); I(h_3,\lambda_2); I(h_3,\lambda_3) \end{vmatrix}. \qquad (3)$$



■ *Схема проведения фотометрических измерений на плоскости* (h_i, λ_j), $i,j=\overline{1,3}$

Далее для выбранных высот h_i вводятся коэффициенты коррекции для длин волн λ_1 и λ_3:

для высоты h_1: $k(h_1, \lambda_1)$ и $k(h_1, \lambda_3)$;

для высоты h_2: $k(h_2, \lambda_1)$ и $k(h_2, \lambda_3)$;

для высоты h_3: $k(h_3, \lambda_1)$ и $k(h_3, \lambda_3)$.

Для проведения вычислений вводятся функции промежуточного преобразования [2]

$$z_1 = \frac{I_1^{k(h_1,\lambda_1)}(h_1,\lambda_1)\cdot I_3^{k(h_1,\lambda_3)}(h_1,\lambda_3)}{I_2(h_1,\lambda_2)}; \quad (4)$$

$$z_2 = \frac{I_1^{k(h_2,\lambda_1)}(h_2,\lambda_1)\cdot I_3^{k(h_2,\lambda_3)}(h_2,\lambda_3)}{I_2(x_2,\lambda_2)}; \quad (5)$$

$$z_3 = \frac{I_1^{k(h_3,\lambda_1)}(h_3,\lambda_1)\cdot I_3^{k(h_3,\lambda_3)}(h_3,\lambda_3)}{I_2(h_3,\lambda_2)}. \quad (6)$$

С учетом (3) и (4) имеем

$$z_1 = \frac{I_0^{k(h_1,\lambda_1)}(\lambda_1)\cdot I_0^{k(h_1,\lambda_3)}(\lambda_3)}{I_0(\lambda_2)}\exp\{-[k(h_1,\lambda_1)\cdot m_1\tau\times$$
$$\times(h_1,\lambda_1)+k(h_1,\lambda_3)\cdot m_1\tau(h_1,\lambda_3)-m_1\tau(h_1,\lambda_2)]\}. \quad (7)$$

Применительно к береговой зоне атмосферный аэрозоль, как было сказано выше, можно представить в виде суммы мелкодисперсного $\tau_f(h_i, \lambda_j)$ и крупнодисперсного аэрозоля $\tau_c(h_i, \lambda_j)$, т. е.

$$\tau_i(h_i,\lambda_j)=\tau_f(h_i,\lambda_j)+\tau_c(h_i,\lambda_j),\ i=\overline{1,3},\ j=\overline{1,3}. \quad (8)$$

С учетом (7) и (8) корректирующие коэффициенты $k(h_1, \lambda_1)$ и $k(h_1, \lambda_3)$ вычисляются путем решения следующей системы уравнений:

$$\begin{gathered} k(h_1,\lambda_1)\cdot\tau_f(h_1,\lambda_1)+k(h_1,\lambda_3)\cdot\tau_f(h_1,\lambda_3)=\tau_f(h_1,\lambda_2); \\ k(h_1,\lambda_1)\cdot\tau_c(h_1,\lambda_1)+ \\ +k(h_1,\lambda_3)\cdot\tau_c(h_1,\lambda_3)=\tau_c(h_1,\lambda_2). \end{gathered} \quad (9)$$

С учетом (4), (7) и (9) имеем

$$\frac{I_1^{k(h_1,\lambda_1)}(h_1,\lambda_1)\cdot I_3^{k(h_1,\lambda_3)}(h_1,\lambda_3)}{I_2(h_1,\lambda_2)} = \frac{I_0^{k(h_1,\lambda_1)}(\lambda_1)\cdot I_0^{k(h_1,\lambda_3)}(\lambda_3)}{I_0(\lambda_2)}=a_1. \quad (10)$$

Аналогично вышесказанному для высот h_2 и h_3 получаем следующую систему трансцендентных уравнений:

$$\left.\begin{aligned} \frac{I_0^{k(h_1,\lambda_1)}(\lambda_1)\cdot I_0^{k(h_1,\lambda_3)}(\lambda_3)}{I_0(\lambda_2)}&=a_1 \\ \frac{I_0^{k(h_2,\lambda_1)}(\lambda_1)\cdot I_0^{k(h_2,\lambda_3)}(\lambda_3)}{I_0(\lambda_2)}&=a_2 \\ \frac{I_0^{k(h_3,\lambda_1)}(\lambda_1)\cdot I_0^{k(h_3,\lambda_3)}(\lambda_3)}{I_0(\lambda_2)}&=a_3 \end{aligned}\right\}. \quad (11)$$

Решение системы (11) относительно $I_0(\lambda_1)$, $I_0(\lambda_2)$ и $I_0(\lambda_3)$ позволяет вычислить значения солнечной постоянной на длинах волн λ_1, λ_2 и λ_3.

Заключение

Следовательно, отдельные дискретные величины солнечной постоянной могут быть измерены путем проведения трехволновых измерений на трех высотно-стратифицированных точках, расположенных на береговой зоне. Полученные в настоящей статье результаты могут быть применены для проведения солнечно-радиационных исследований в промышленно-береговых зонах при калибровке солнечных фотометров. При этом, естественно, следует учесть, что на морской береговой промышленной зоне существуют источники как крупнодисперсных, так и мелкодисперсных аэрозолей. Например, сжигание попутного углеводородного газа в нефтедобывающих платформах приводит к значительному загрязнению морской атмосферы мелкодисперсной сажей. В то же время пузырьковый механизм образования морских соляных частиц является причиной загрязнения атмосферы крупнодисперсным гигроскопическим аэрозолем.

В заключение отметим, что правильная оценка солнечной радиации, поступающей на земную атмосферу, является важной для решения таких задач, как климатический подсчет радиационного баланса на поверхности Земли, калибровка солнечной фотометрической аппаратуры, исследование эффективности термопреобразователей солнечной энергии и др.

Литература

1. **Langley** Analyses. http://www.agu.org/pubs/toc/g.1/g1/g1.191/1999GL 900267/node3.html (дата обращения: 28.05.2010).
2. **Асадов Х. Г., Сулейманов Ш. Т.** Синтез трехволновых скорректированных измерителей малых компонент атмосферы в УФ-диапазоне // Метрология. 2007. № 9. С. 3–7.

УДК 681.326.3

МАТЕМАТИЧЕСКИЕ И ИМИТАЦИОННЫЕ МОДЕЛИ СИГНАЛОВ ДЛЯ ОТЛАДКИ АЛГОРИТМОВ ОБРАБОТКИ ИНФОРМАЦИИ В БОРТОВЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ КОНТРОЛЯ

В. Б. Кублановский,
генеральный директор, главный конструктор
ОАО «НИИ ВС «Спектр»

Предлагаются математические и имитационные модели входных информационных и мешающих сигналов, наблюдаемых в автоматизированных системах контроля бортовой аппаратуры летательных аппаратов. Модели основаны на экспериментальных данных, предназначены для отладки аппаратуры и программного обеспечения автоматизированных бортовых систем контроля, работающих в условиях жестко ограниченных временных и аппаратных ресурсов.

Ключевые слова *— математическая модель, имитационная модель, информационный параметр, алгоритм обработки, система контроля.*

В силу особенностей статистических характеристик входных информационных сигналов бортовой автоматизированной системы контроля (БАСК), а также сложности нелинейных алгоритмов их обработки единственным надежным методом проектирования аппаратуры и отладки программного обеспечения БАСК является метод математического моделирования. Именно поэтому вопросы синтеза эффективных алгоритмов моделирования информационных и мешающих входных сигналов БАСК, основанных на эмпирических данных, полученных в результате эксплуатации аналогичных систем контроля, чрезвычайно актуальны.

Бортовая автоматизированная система контроля является информационно-измерительной системой, предназначенной для сбора, хранения и обработки информации о параметрах аппаратуры летательного аппарата. Входной информационный поток БАСК состоит из нескольких тысяч сигналов, информация в которых представлена в аналоговой, цифровой, бинарной и кодовой формах. Сложность аппаратуры БАСК, содержащей значительное количество аппаратных средств обработки сигналов, а также сложность программного обеспечения приводят к необходимости построения простых, но адекватных математических моделей сигналов, которые требуются как для синтеза алгоритмов обработки и аппаратных средств, так и для тестирования аппаратуры БАСК в целом.

Будем считать, так же как и в работе [1], что все вопросы, связанные с дискретизацией по времени и по уровню, решены в системе сбора информации, тогда в качестве математической модели наблюдаемых процессов можно принять математическую модель временных рядов [2]. В результате анализа записей БАСК-124 и последней версии БАСК-225 выяснилось, что большинство каналов регистрации БАСК содержат как гауссову помеху, которая в отличие от классических моделей временных рядов может иметь существенную корреляцию, так и негауссову помеху, в которой часто присутствуют аномальные выбросы. Более того, один и тот же канал может содержать гауссову коррелированную помеху, негауссову помеху и аномальные выбросы, обусловленные электромагнитными наводками и сбоями аппаратуры. При наличии таких помех в информационных каналах БАСК классические методы обработки временных рядов, особенно методы прогнозирования, могут оказаться не только слабо эффективными, но и вообще неработоспособными.

Ниже рассмотрим математические модели аномальных выбросов, негауссовых аддитивных

помех и гауссовой коррелированной помехи, а также алгоритмы их моделирования.

Для математического описания помех с аномальными выбросами можно использовать распределения с «утяжеленными хвостами», к которым относятся распределение Лапласа, а также составные распределения Тьюкки и Хьюбера. Если же информационный сигнал и помеха представляют собой неотрицательно определенные последовательности, то для описания аномальных выбросов используют экспоненциальное распределение, логарифмически-нормальное распределение и распределение Хьюбера с соответствующе подобранным засоряющим распределением [3]. Отметим, что модели Тьюкки и Хьюбера при определенном выборе параметров могут использоваться и для описания негауссовых распределений, т. е. эти модели применяются и для учета редких больших аномальных выбросов, и для описания небольших изменений распределений отсчетов временных рядов.

Модель Лапласа. Плотность распределения вероятностей отсчетов временного ряда x_i в соответствии с этой моделью записывается в виде

$$w(x_i) = 0,5\alpha \exp(-\alpha|x_i|),\ -\infty < x_i < \infty, \qquad (1)$$

где α — параметр распределения. Это распределение называют также двусторонним экспоненциальным распределением. Распределение имеет «утяжеленные хвосты» и часто используется для оценки робастности алгоритмов обработки сигналов. «Длинные хвосты» распределения Лапласа приводят к эффекту возникновения аномальных выбросов, но в силу того, что распределение определяется лишь одним параметром, его не очень удобно использовать в этих целях. Его нельзя применять, например, в ситуациях, когда информационный сигнал наблюдается в нормальных помехах и с известной вероятностью появляются аномальные отсчеты элементов временного ряда.

Модель Тьюкки является более гибкой, но и более сложной моделью, в соответствии с которой плотность распределения вероятностей отсчетов временного ряда x_i записывается в виде

$$w(x_i) = (1-\xi_i)\frac{1}{\sqrt{2\pi}\sigma_1}\exp\left\{-\frac{x_i^2}{2\sigma_1^2}\right\} + \\ + \xi_i \frac{1}{\sqrt{2\pi}\sigma_2}\exp\left\{-\frac{x_i^2}{2\sigma_2^2}\right\}, \qquad (2)$$

где ξ_i — случайная величина, распределенная по закону Бернулли, принимающая значения 0 с вероятностью p и 1 с вероятностью $(1 - p)$. В выражении (2), представляющем собой смесь двух нормальных распределений, обычно полагают $\sigma_2 >> \sigma_1$, что, собственно, и обеспечивает «утяжеление хвоста» основного нормального распределения. Эта математическая модель при близких σ_1 и σ_2 и p, близкой к 0,5, может использоваться для описания негауссовой помехи, т. е. для описания небольших отличий от нормального распределения. При резко отличающихся σ_1 и σ_2 и p, близкой к 1, модель Тьюкки применяется для описания аномальных выбросов. Модель Тьюкки удобно использовать и для моделирования коррелированной негауссовой помехи. Для этого достаточно моделировать две последовательности нормальных случайных величин с требуемыми корреляционными характеристиками и «перемешивать» элементы этих коррелированных последовательностей с вероятностью p.

Модель Хьюбера является обобщением модели Тьюкки. Плотность распределения вероятностей отсчетов временного ряда x_i в соответствии с моделью Хьюбера записывается в виде

$$w(x_i) = (1-\xi_i)w_1(x_i) + \xi_i w_2(x_i), \qquad (3)$$

область определения $w(x_i)$ зависит от распределений $w_1(x_i)$ и $w_2(x_i)$, которые могут быть любыми; ξ_i — случайная величина, выполняющая «засорение» основного распределения $w_1(x_i)$ выборками из распределения $w_2(x_i)$, в качестве которого можно использовать и распределение Лапласа, и δ-функцию. В частности, эта модель позволяет моделировать помеху в виде коррелированного нормального шума (основное распределение) и аномальные выбросы, возникающие с вероятностью p, которые могут иметь и постоянное известное значение (сбои в старших разрядах), и быть случайными по своей величине (электромагнитные наводки). Эта модель подходит и для моделирования неотрицательно определенных временных рядов.

Экспоненциальная модель используется для моделирования неотрицательно определенных временных рядов. Плотность распределения вероятностей записывается в виде

$$w(x_i) = \alpha \exp(-\alpha|x_i|),\ x_i \ge 0, \qquad (4)$$

где α — параметр распределения; $w(x_i) = 0$ при $x_i < 0$. Экспоненциальная модель относится к распределениям с «утяжеленными хвостами» и часто применяется для тестирования робастности алгоритмов обработки сигналов [4].

Логарифмически-нормальное распределение, как и экспоненциальное, используется для моделирования неотрицательно определенных временных рядов. Плотность распределения вероятностей записывается в виде

$$w(x_i) = \frac{1}{\sqrt{2\pi}\sigma x_i}\exp\left\{-\frac{(\ln x_i - m_i)^2}{2\sigma^2}\right\},\ x_i \ge 0, \qquad (5)$$

где m_i и σ^2 — параметры распределения, определяющие математическое ожидание и дисперсию отсчетов логарифмов x_i; $w(x_i) = 0$ при $x_i < 0$.

Имитационные модели входных сигналов БАСК представляют собой алгоритмы моделирования перечисленных выше распределений. В том случае, когда отсчеты временных рядов являются независимыми случайными величинами, моделирование этих распределений не представляет труда, так как соответствующие алгоритмы содержатся практически во всех математических пакетах. Имитационные модели коррелированных сигналов как гауссовых, так и негауссовых требуют отдельного рассмотрения, в частности, они могут быть построены методами, изложенными в работе [5].

Подводя итог, отметим, что практически единственным методом исследования алгоритмов обработки сигналов в БАСК является метод математического моделирования, для реализации которого необходимы математические и имитационные модели входных сигналов. В работе предложено использовать пять основных моделей временных рядов, наблюдаемых системами БАСК. Рассмотренные модели являются достаточно простыми, и в то же время они выбраны на основе анализа реальных записей информационных и мешающих сигналов БАСК-124 и БАСК-225. Для отладки программного обеспечения БАСК потребуется создание имитаторов этих временных рядов, которые могут быть реализованы как аппаратно, так программно.

Литература

1. **Кублановский В. Б., Кошелев С. В.** Математические модели и алгоритмы сглаживания входных сигналов бортовых автоматизированных систем контроля // Информационно-управляющие системы. 2010. № 2(45). С. 71–74.
2. **Андерсон Т.** Статистический анализ временных рядов / Пер. с англ. И. Г. Журбенко, В. П. Носко. — М.: Мир, 1976. — 756 с.
3. **Хьюбер Дж. П.** Робастность в статистике: пер. с англ. — М.: Мир, 1984. — 304 с.
4. **Кублановский В. Б., Песин Ф. Я.** Технология разработки и отладки программного обеспечения бортовых автоматизированных систем контроля летательных аппаратов // Радиопромышленность. 1998. Вып. 1. С. 38–44.
5. **Шепета А. П.** Синтез нелинейных формирующих фильтров для моделирования входных сигналов локационных систем // Тр. Междунар. науч.-техн. конф. (докл.), май 1994 г. / АН Украины, НПО Квант. Киев, 1994. Вып. 1. С. 81–85.

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

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

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

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

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

XIII МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ «КОГНИТИВНОЕ МОДЕЛИРОВАНИЕ В ЛИНГВИСТИКЕ»

22–29 сентября 2011 г.

Место проведения: Греция, Корфу, Отель Dassia Chandris 4*

Организаторы
Институт языкознания Российской академии наук (Россия)
Казанский государственный университет (Россия)
Новый болгарский университет (Болгария)
Афинский национальный университет имени Каподистрии (Греция)
Университет Задара (Хорватия)
ITHEA Международное научное сообщество и Институт информационных теорий и приложений
Университет Александр Иоан Куза (Румыния)
Софийский университет «Св. Климент Охридский» (Болгария)
Московский государственный лингвистический университет (Россия)
Национальный исследовательский технологический университет МИСиС (Россия)
Брюссельский свободный университет (Бельгия)
Веб-журнал балканской русистики
Научный и образовательный центр лингвистики (Россия)
Российская ассоциация лингвистов-когнитологов (Россия)

Направления работы конференции
Общие темы:
Когнитивные модели языковых явлений
Формальные модели в языке и познании
Когнитивно-ориентированные компьютерные приложения и языковые ресурсы
Общие проблемы когнитивной науки
Модели и исследования по областям:
Восприятие и производство речи
Психолингвистика и психосемантика
Семиотика, семантика и прагматика
Обработка языка, память и мышление
Детская речь и усвоение языка
Лингвистическая типология
Перевод и познание
Расстройства речи, языковые патологии
Когнитивные аспекты теологии
Когнитивные аспекты развития и использования информационных технологий
Когнитивные механизмы принятия решений
Когнитивная лингвистика:
Теория метафоры
Ментальный лексикон и лексическая онтология
Наивная картина мира и вербальная форма
Концептуализация и вербализация знания
Когнитивные механизмы обработки текста
Видо-мотивированные аспекты человеческого языка
Мышление и обработка языка
Когнитивная славистика

Публикация материалов
По результатам конференции будет опубликован сборник трудов, содержащий расширенные тезисы (2 страницы на английском).
Лучшие доклады будут рекомендованы для публикации в форме журнальной статьи в издательской системе ITA FOI ITHEA (www.foibg.com).

Контрольные сроки
Представление тезисов для прохождения процедуры раннего рецензирования (ранняя регистрация и подтверждение необходимы тем участникам, которые планируют обращаться в национальные и международные научные фонды с заявкой на получение тревел-грантов) — 2 апреля 2011 г.
Раннее подтверждение приема заявки в программу — 16 мая 2011 г.
Представление тезисов для обычной процедуры рецензирования — 2 июня 2011 г.
Подтверждение приема заявки в программу — 16 июня 2011 г.
Представление окончательной версии тезисов — 30 июня 2011 г.

Дополнительная информация и справки
Председатель оргкомитета: Поляков Владимир Николаевич
Эл. адрес: cml2011@mail.ru
Сайт: www.cml.msisa.ru

СВЕДЕНИЯ ОБ АВТОРАХ

АБРАМЯНЦ Тамара Гургеновна

Старший научный сотрудник Института проблем управления РАН.
В 1961 году окончила Московский энергетический институт по специальности «Автоматика и телемеханика».
В 1989 году защитила диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 50 научных публикаций.
Область научных интересов — теория управления системами с неполной информацией.
Эл. адрес: abramnc@ipu.ru

АЛЕКСЕЕВ Александр Петрович

Доцент кафедры вычислительной техники и информатики Поволжского государственного университета телекоммуникаций и информатики. Мастер связи, награжден медалью «Изобретатель СССР».
В 1971 году окончил Куйбышевский электротехнический институт связи по специальности «Автоматическая электросвязь».
В 1986 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 140 научных публикаций, в том числе 10 книг, автор 55 изобретений.
Область научных интересов — контрольно-измерительная техника, дефектоскопия, информатика, защита информации.
Эл. адрес: apa@bk.ru

БОРИСОВ Юрий Борисович

Аспирант кафедры безопасных информационных технологий Санкт-Петербургского государственного университета информационных технологий, механики и оптики.
В 2008 году окончил Санкт-Петербургский государственный университет информационных, технологий, механики и оптики по специальности «Организация и технология защиты информации».
Является автором двух научных публикаций.
Область научных интересов — информационная безопасность в системах электронных расчетов, мониторинг и прогнозирование информационных угроз.
Эл. адрес: komidomik@mail.ru

АГАЕВ Фахраддин Гюльали оглы

Гражданин Азербайджана.
Профессор, директор Института космических исследований природных ресурсов Национального аэрокосмического агентства Азербайджана.
В 1977 году окончил Азербайджанский государственный педагогический институт им. В. И. Ленина по специальности «Математика».
В 2002 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 200 научных публикаций.
Область научных интересов — математика, дистанционное зондирование, кибернетика.
Эл. адрес: directoraf@rambler.ru

АНТОНОВ Алексей Евгеньевич

Ассистент кафедры вычислительной техники филиала Московского энергетического института (технического университета) в г. Смоленске.
В 2008 году окончил филиал Московского энергетического института (технического университета) в г. Смоленске по специальности «Информационное и программное обеспечение автоматизированных систем».
Является автором шести научных публикаций.
Область научных интересов — методы и средства защиты информации, вредоносное программное обеспечение и методы борьбы с ним, сети ЭВМ.
Эл. адрес: enton@freemail.ru

ГОЛОЛОБОВ Леонид Иванович

Доцент, старший научный сотрудник Военно-морского института радиоэлектроники им. А. С. Попова.
В 1963 году окончил Высшее военно-морское училище радиоэлектроники, в 1974 году — Военно-морскую академию.
В 2001 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 80 научных публикаций.
Область научных интересов — информационные и сетевые технологии, исследование процессов обработки и передачи данных человеком и техническими средствами, автоматизация управленческой деятельности.
Эл. адрес: lig01@mail.ru

ДЕРНОВА
Евгения
Сергеевна

Преподаватель кафедры автоматизированных систем обработки информации и управления Санкт-Петербургского государственного электротехнического университета «ЛЭТИ».
В 2007 году окончила Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» по специальности «Компьютерная безопасность».
В 2009 году защитила диссертацию на соискание ученой степени кандидата технических наук.
Является автором 30 научных публикаций и трех изобретений.
Область научных интересов — информационная безопасность, криптографические протоколы.
Эл. адрес: evgeshka19@mail.ru

КАРАСЕВА
Екатерина
Ивановна

Аспирант кафедры прикладных информационных технологий в экономике и менеджменте Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2007 году окончила Белорусский государственный экономический университет по специальности «Финансы и кредит».
Является автором пяти научных публикаций.
Область научных интересов — операционные, валютные рыночные риски, методы моделирования рисков.
Эл. адрес: matatka@hotbox.ru

КУБЛАНОВСКИЙ
Вениамин
Борисович

Генеральный директор ОАО «НИИ вычислительных средств «Спектр» холдинговой компании «Ленинец».
В 1972 году окончил Ленинградский институт точной механики и оптики по специальности «Электронные вычислительные машины».
Является автором восьми научных публикаций и 17 авторских свидетельств на изобретения.
Область научных интересов — системный анализ, математическое моделирование, программирование, проектирование бортовых авиационных комплексов.
Эл. адрес: jsc.spectr@gmail.com

ИБРАГИМОВ
Эльмир
Али оглы

Гражданин Азербайджана.
Аспирант Института космических исследований природных ресурсов Национального аэрокосмического агентства Азербайджана.
В 2004 году окончил Государственную нефтяную академию по специальности «Электрические машины и приборы».
Является автором восьми научных публикаций.
Область научных интересов — дистанционное зондирование, измерительная техника.
Эл. адрес:
elmir.ibrahimov@yahoo.com

КОСТЮКОВА
Татьяна
Петровна

Профессор кафедры экономической информатики Уфимского государственного авиационного технического университета, почетный работник высшего профессионального образования РФ.
В 1968 году окончила Уфимский авиационный институт по специальности «Электрические машины и аппараты».
В 1999 году защитила диссертацию на соискание ученой степени доктора технических наук.
Является автором более 250 научных публикаций и трех запатентованных изобретений.
Область научных интересов — информационные технологии в науке и производстве.
Эл. адрес: ktp@ufanet.ru

КУРОЧКИН
Александр
Николаевич

Адъюнкт очной адъюнктуры Военной академии войсковой ПВО ВС РФ им. Маршала Советского Союза А. М. Василевского.
В 1999 году окончил Военную академию ПВО СВ РФ.
Является автором 11 научных публикаций.
Область научных интересов — сверхрэлеевское разрешение радиолокационных целей, повышение эффективности РЛС разведки войсковой ПВО.
Эл. адрес: alexlana888@mail.ru

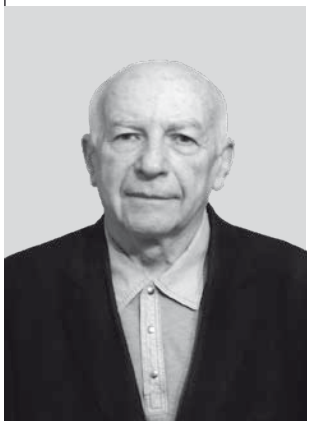
ЛЕБЕДЕВ Александр Сергеевич

Преподаватель кафедры радиолокационного вооружения Военной академии войсковой ПВО ВС РФ им. Маршала Советского Союза А. М. Василевского.
В 2001 году окончил Военный университет войсковой ПВО ВС РФ.
В 2008 году защитил диссертацию на соискание ученой степени кандидата технических наук по специальности «Военная электроника, аппаратура комплексов военного назначения».
Является автором 20 научных публикаций.
Область научных интересов — сверхрэлеевское разрешение, разрешение в радиолокационных головках самонаведения.
Эл. адрес: leas97@rambler.ru

ЛЫСЕНКО Ирина Алексеевна

Старший преподаватель кафедры экономической информатики Уфимского государственного авиационного технического университета.
В 1980 году окончила Уфимский авиационный институт по специальности «Автоматизированные системы управления».
Является автором более 20 научных публикаций.
Область научных интересов — информационные технологии в образовании и производстве.
Эл. адрес: irina.lys@mail.ru

МАСЛОВ Евгений Петрович



Заведующий лабораторией Института проблем управления РАН.
В 1961 году окончил Одесский институт инженеров связи по специальности «Радиотехника».
В 1972 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 100 научных публикаций.
Область научных интересов — теория управления системами с неполной информацией.
Эл. адрес: e-mas1@yandex.ru

ЛЕБЕДЕВ Илья Сергеевич

Доцент кафедры информационных систем в экономике Санкт-Петербургского государственного университета, заместитель начальника отдела Санкт-Петербургского филиала ОАО «НПК «Тристан».
В 1998 году окончил Санкт-Петербургское высшее военное училище ПВО.
В 2002 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 40 научных публикаций.
Область научных интересов — информационные технологии, компьютерная лингвистика.
Эл. адрес: isl_box@mail.ru

МАКАРОВ Максим Игоревич

Аспирант, ассистент кафедры вычислительной техники и информатики Поволжского государственного университета телекоммуникаций и информатики.
В 2008 году окончил Поволжскую государственную академию телекоммуникаций и информатики по специальности «Программное обеспечение вычислительной техники и автоматизированных систем».
Является автором 14 научных публикаций
Область научных интересов — стеганография, криптография, сетевые технологии.
Эл. адрес: moox700@gmail.com

МИХАЙЛОВ Владимир Валентинович

Профессор, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН.
В 1957 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина).
В 1999 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором 165 научных публикаций.
Область научных интересов — системный анализ, обработка данных, моделирование в области экологии.
Эл. адрес: mwwcari@mail.ru

МОЛДОВЯН
Дмитрий
Николаевич

Младший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН, аспирант Санкт-Петербургского государственного электротехнического университета «ЛЭТИ».
В 2009 году окончил Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» по специальности «Компьютерная безопасность».
Является автором 25 научных публикаций и четырех изобретений.
Область научных интересов — криптографические протоколы и применение конечных алгебраических структур в синтезе криптосхем с открытым ключом.
Эл. адрес: mdn.spectr@mail.ru

РУДЬКО
Игорь
Михайлович

Старший научный сотрудник Института проблем управления РАН.
В 1969 году окончил Московский энергетический институт по специальности «Автоматика и телемеханика».
В 1991 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 40 научных публикаций и трех изобретений.
Область научных интересов — теория и применение цифровой обработки сигналов, обработка гидролокационной информации.
Эл. адрес: igor-rudko@mail.ru

СТЕПАНОВ
Александр
Георгиевич

Доцент, заведующий кафедрой информационных технологий в экономике и менеджменте Санкт-Петербургского государственного университета аэрокосмического приборостроения, почетный работник высшего профессионального образования РФ.
В 1972 году окончил Ленинградский институт авиационного приборостроения по специальности «Радиоинженер».
В 2005 году защитил диссертацию на соискание ученой степени доктора педагогических наук.
Является автором более 100 научных публикаций.
Область научных интересов — методика преподавания информатики в высшей школе, цифровая обработка сигналов.
Эл. адрес: georgich_spb@mail.ru

ПОРШНЕВ
Сергей
Владимирович

Профессор, заведующий кафедрой автоматики и информационных технологий Уральского федерального университета имени первого Президента России Б. Н. Ельцина, лауреат премии им. С. И. Мосина.
В 1984 году окончил Новосибирский государственный университет по специальности «Физика».
В 2000 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 350 научных публикаций и трех запатентованных изобретений.
Область научных интересов — математическое моделирование, информационные и информационно-управляющие системы, методы и алгоритмы обработки сигналов в информационных системах.
Эл. адрес:
sergey_porshnev@mail.ru

СОЛОМАХА
Илья
Викторович

Аспирант кафедры автоматики и информационных технологий Уральского федерального университета имени первого Президента России Б. Н. Ельцина.
В 2005 году окончил Уральский государственный технический университет по специальности «Информатика и вычислительная техника».
В 2006 году окончил Уральский государственный технический университет по специальности «Вычислительные машины, комплексы, системы и сети».
Область научных интересов — методы и алгоритмы обработки технологической информации, собираемой АСУ ТП.
Эл. адрес: iluxa_s@mail.ru

СУХОВ
Дмитрий
Константинович

Аспирант, научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН.
В 2006 году окончил Технологический институт Южного федерального университета по специальности «Комплексная защита объектов информатизации».
Является автором трех научных публикаций.
Область научных интересов — информационная безопасность, аутентификация информации и субъектов.
Эл. адрес: dimonfsb@gmail.com

ТАРАКАНОВ Андрей Викторович

Преподаватель кафедры радиолокационного вооружения Военной академии войсковой ПВО ВС РФ им. Маршала Советского Союза А. М. Василевского.
В 2004 году окончил Военный университет войсковой ПВО ВС РФ.
В 2010 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 27 научных публикаций.
Область научных интересов — сверхрэлеевское разрешение радиолокационных целей, современные методы спектрального оценивания.
Эл. адрес: retter82@mail.ru

ФЕДУЛОВ Александр Сергеевич

Профессор, заместитель директора по учебно-методической работе, заведующий кафедрой вычислительной техники филиала Московского энергетического института (технического университета) в г. Смоленске.
В 1982 году окончил Смоленский филиал Московского энергетического института по специальности «Конструирование, технология и производство ЭВА».
В 2007 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором 80 научных публикаций.
Область научных интересов — СППР, интеллектуальный анализ данных, математическое и программное обеспечение ВМ.
Эл. адрес: fedulov_a@mail.ru

ЧЕРНЫШЕВ Кирилл Романович

Старший научный сотрудник Института проблем управления им. В. А. Трапезникова РАН.
В 1985 году окончил факультет прикладной математики Московского института электронного машиностроения.
В 1999 году защитил диссертацию на соискание ученой степени кандидата физико-математических наук.
Является автором более 80 научных публикаций.
Область научных интересов — идентификация систем управления.
Эл. адрес: myau@ipu.ru

ТИХОНОВ Эдуард Прокофьевич

Доцент кафедры биомедицинской электроники и охраны среды Санкт-Петербургского государственного электротехнического университета «ЛЭТИ», член-корреспондент Метрологической академии.
В 1963 году окончил Ленинградский институт авиационного приборостроения.
В 2009 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 190 научных публикаций, в том числе более 60 авторских свидетельств и патентов на изобретения.
Область научных интересов — кибернетика, информатика, моделирование, информационно-измерительные системы, биомедицинская инженерия.
Эл. адрес: edikleti@yandex.ru

ХАРИН Ярослав Вячеславович

Аспирант Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2010 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения.
Является автором одной публикации.
Область научных интересов — программирование, распознавание образов.
Эл. адрес: aferook@yandex.ru

ЧИЖОВ Анатолий Анатольевич

Доцент, заместитель начальника кафедры радиолокационного вооружения Военной академии войсковой ПВО им. Маршала Советского Союза А. М. Василевского.
В 1998 году окончил Военную академию ПВО СВ РФ.
В 2001 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 100 научных публикаций и пяти запатентованных изобретений.
Область научных интересов — сверхрэлеевское разрешение, оптимизация стохастических систем.
Эл. адрес: rtshouse@mail.ru

ЯХНО
Виктор
Павлович

Старший научный сотрудник Института проблем управления РАН.
В 1966 году окончил Московский физико-технический институт по специальности «Системы автоматического управления».
В 1983 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 50 научных публикаций.
Область научных интересов — системы контроля и управления.
Эл. адрес: vic@rlt.ru

УВАЖАЕМЫЕ АВТОРЫ!

При подготовке рукописей статей редакция просит Вас руководствоваться следующими рекомендациями.

Объем статьи (текст, таблицы, иллюстрации и библиография) не должен превышать эквивалента в 16 страниц, напечатанных на бумаге формата А4 на одной стороне через 1,5 интервала в Word шрифтом Times New Roman размером 13.

Обязательными элементами оформления статьи являются: индекс УДК, заглавие, инициалы и фамилия автора (авторов), ученая степень, звание, полное название организации, аннотация (7–10 строк) и ключевые слова на русском и английском языках, подрисуночные подписи.

Формулы в текстовой строке набирайте в Word, не используя формульный редактор (Mathtype или Equation), только в том случае, если средства Word не позволяют набрать формулу или символ (например, простая дробь, символы с «крышками» и т. д.), используйте имеющийся в Word формульный редактор Mathtype или Equation; формулы, стоящие в отдельной строке, могут быть набраны как угодно; при наборе формул в формульном редакторе знаки препинания, ограничивающие формулу, набирайте вместе с формулой; для установки размера шрифта никогда не пользуйтесь вкладкой Other..., используйте вкладку Define; в формулах не отделяйте пробелами знаки: + = −.

Для набора формул в Word никогда не используйте Конструктор (на верхней панели: «Работа с формулами» — «Конструктор»), т. к. 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 изготавливаются в векторных программах: Visio 4, 5, 2002–2003 (*.vsd); Coreldraw (*.cdr); Excel; Word; AdobeIllustrator; AutoCad (*.dxf); Компас; Matlab (экспорт в формат *.ai);

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

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, факс, эл. адрес), 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.

Более подробную информацию см. на сайте: www.i-us.ru

УДК 531.3:681.5.01

Уклонение подвижного объекта от обнаружения группой наблюдателей при малых отношениях сигнал/помеха

Абрамянц Т. Г., Маслов Е. П., Рудько И. М., Яхно В. П. Информационно-управляющие системы, 2011. № 2. С. 2–7.

Приводится решение задачи об оптимизации закона уклонения подвижного объекта от обнаружения группой наблюдателей при малых отношениях сигнал/помеха. Вектор программного управления включает траекторию уклонения и закон изменения скорости на траектории.

Ключевые слова — уклонение от обнаружения, вероятность обнаружения, группа наблюдателей, отношение сигнал/помеха, первый интеграл, алгоритм Дейкстры.

Список лит.: 11 назв.

UDK 531.3:681.5.01

Avoidance of a Moving Object from Detection by a Group of Observers Subject to Small Signal/Noise Ratios

Abramyantz T. G., Maslov E. P., Rudko I. M., Yahno V. P. IUS, 2011. N 2. P. 2–7.

The problem of avoidance of a moving object from detection by group of observers subject to small signal/noise ratios is discussed. The program control vector includes the trajectory and the law of motion velocity. An optimal solution is presented.

Keywords — Avoidance from Detection, Probability of Detection, Group of Observers, First Integral, Dijkstra Algorithm.

Refs: 11 titles.

УДК 681.518+519.724

Вероятностные адаптивные алгоритмы дискретного представления аналоговых сигналов. Часть 1: Исследование свойств

Тихонов Э. П. Информационно-управляющие системы, 2011. № 2. С. 8–15.

Выполнено углубленное исследование ранее предложенного вероятностного метода адаптивной дискретизации. Показано, что данный метод основан на нелинейных вероятностных итерационных алгоритмах или отображениях, анализируемых в динамично развивающейся теории нелинейных систем. Рассмотрены вопросы сходимости предложенных алгоритмов на базе известного логистического отображения.

Ключевые слова — временная дискретизация, адаптация, алгоритм, сходимость, погрешность, функция восстановления.

Список лит.: 12 назв.

UDK 681.518+519.724

Probabilistic Adaptive Algorithms for Discrete Representation of Analog Signals. Part 1: Examination of properties

Tikhonov E. P. IUS, 2011. N 2. P. 8–15.

This article is based on an in-depth study of the probabilistic adaptive discretization technique that was proposed earlier. It is shown that this technique relies on nonlinear probabilistic iterative algorithms or representations analyzed in the dynamically developing theory of nonlinear systems. The issues of the introduced algorithms' convergence are also examined in this work on the basis of logistic representation .

Keywords — Temporary Sampling, Adaptation, Algorithm, Convergence, Inaccuracy, Function of Reconstruction.

Refs: 12 titles.

УДК 621.396.96

Эффективность проекционного время-частотного разрешения групповых рассеивателей

Чижов А. А., Лебедев А. С., Тараканов А. В., Курочкин А. Н. Информационно-управляющие системы, 2011. № 2. С. 16–21.

Приведен ряд оценок показателей разрешающей способности двумерных проекционных процедур обработки сигналов при часто встречающейся в приложениях функции рассогласования, характерной для локационных задач в условиях временных и частотных сдвигов эхо-сигналов отдельных рассеивателей.

Ключевые слова — обратная задача рассеяния, сверхрэлеевское разрешение, групповой рассеиватель, разрешающая способность.

Список лит.: 3 назв.

UDK 621.396.96

The Efficiency of the Projective Time-Frequency Resolution of the Permission Group Dispersion Targets

Chizhov A. A., Lebedev A. S., Tarakanov A. V., Kurochkin A. N. IUS, 2011. N 2. P. 16–21.

Some estimates of resolution indicators of the two-dimensional projective procedures of signal processing are shown for the mismatch function quite often found in applications, characteristic for radar problems under conditions when time and frequency shifts of the echo signals of separate dispersion targets exist.

Keywords — Inverse Problem of Dispersion, Super-Resolution, Group Dispersion Target, Resolution Capacity.

Refs: 3 titles.

УДК 004.932.72'1

К вопросу о построении системы распознавания и подсчета животных на аэрофотоснимках. Часть 1: Анализ методов распознавания

Михайлов В. В., Харин Я. В. Информационно-управляющие системы, 2011. № 2. С. 22–28.

Рассматриваются основные принципы и этапы построения системы подсчета и распознавания объектов на фотографиях. Проводится обзор методов сегментации изображений и распознавания. Разбираются их существенные достоинства и недостатки для решения задачи подсчета количества животных.

Ключевые слова — распознавание, сегментация, подсчет объектов.

Список лит.: 9 назв.

UDK 004.932.72'1

On the Developing of an Animal Recognition and Counting System for Aerial Photographs. 1. Analysis of Recognition Methods

Mikhailov V. V., Kharin Y. V. IUS, 2011. N 2. P. 22–28.

Basic principles and stages of system counting and recognizing objects on photos are described. A review of recognition methods is produced. Explained is the choice of the selected methods for the system of recognizing and counting animals. Their advantages and limitations are discussed.

Keywords — Recognizing, Segmentation, Counting Objects.

Refs: 9 titles.

УДК 004.8:681.3.06

О возможности повышения качества многомерных математических моделей технологической информации, собираемой на ТЭС

Поршнев С. В., Соломаха И. В. Информационно-управляющие системы, 2011. № 2. С. 29–36.

Предложено для описания связей между технологическими показателями, собираемыми информационной системой тепловой электрической станции, использовать нелинейные математические модели, создаваемые на основе метода группового учета аргументов. Приведены результаты сравнительного анализа качества аппроксимации изучаемых зависимостей при использовании линейных и нелинейных математических моделей, свидетельствующие о целесообразности применения последних для описания связей между технологическими показателями.

Ключевые слова — тепловая электрическая станция, информационная система, технологическая информация, технологический показатель, факторный анализ, метод группового учета аргументов.

Список лит.: 6 назв.

UDK 004.8:681.3.06

On the Possibility of Improvement of Quality of the Multidimensional Mathematical Models of the Technological Information Collected on Thermal Power Plants

Porshnev S. V., Solomakha I. V. IUS, 2011. N 2. P. 29–36.

It is suggested to use the nonlinear mathematical models created on the basis of a group method of data handling for the description of connections between the technological indicators collected by the information system of a thermal power plant. The results of a comparative analysis of quality of approximation of the researched dependences are presented while using linear and nonlinear mathematical models that testify the expediency of their use to describe the connections of the technological indicators.

Keywords — a Thermal Power Plant, Information System, the Technological Information, a Technological Indicator, Factor Analysis, a Group Method of Data Handling.

Refs: 6 titles.

УДК 681.3

Анализ текстовых сообщений в системах мониторинга информационной безопасности

Лебедев И. С., Борисов Ю. Б. Информационно-управляющие системы, 2011. № 2. С. 37–43.

Описываются модели формализации естественно-языковых сообщений для систем мониторинга информационной безопасности открытых вычислительных сетей. Рассматриваются особенности обработки и анализа сообщений.

Ключевые слова — формализация естественного языка, обработка сообщений, вычисление информационных структур.

Список лит.: 10 назв.

UDK 681.3

Formalization Models of Natural-Language Messages in Information Security Monitoring Systems of Open Computer Networks

Lebedev I. S., Borisov Y. B. IUS, 2011. N 2. P. 37–43.

Formalization models of natural-language messages in open computer networks' information security systems are described. Processing and analysis features of messages are reviewed.

Keywords — Natural Language Formalization, Messages Processing, Information Structures Calculation.

Refs: 10 titles.

УДК 685.310.11

Модель структурно-функционального анализа совместной обработки и передачи данных

Гололобов Л. И. Информационно-управляющие системы, 2011. № 2. С. 44–49.

Описывается модель структурно-функционального анализа совместной обработки и передачи данных операторами и техническими средствами. В модели совмещены структура и функции с приоритетом функции над структурой.

Ключевые слова — структура, функции, совместная обработка и передача данных.

Список лит.: 2 назв.

UDK 685.310.11

A Model of Structurally Functional Analysis of Joint Processing and Data Transmission

Gololobov L. I. IUS, 2011. N 2. P. 44–49.

A model of the structurally functional analysis of joint processing and data transmission by operators and technical means is described. In this model, structure and functions with a function over structure are combined.

Keywords — Structure, Functions, Joint Processing and Data Transmission.

Refs: 2 titles.

УДК 004.492.3

Алгоритм обнаружения и обхода антиотладочных и антиэмуляционных приемов

Антонов А. Е., Федулов А. С. Информационно-управляющие системы, 2011. № 2. С. 50–54.

Проведен обзор принципов работы отладчиков и эмуляторов, их уязвимостей. Предложен новый алгоритм обнаружения антиотладочных и антиэмуляционных приемов, а также модификация отладчика для задач анализа вредоносного кода.

Ключевые слова — эмулятор, отладчик, антиотладочные и антиэмуляционные приемы, вредоносное программное обеспечение.

Список лит.: 6 назв.

UDK 004.492.3

Detection and Bypassing of Anti-debugging and Anti-emulation Techniques

Antonov A. E., Fedulov A. S. IUS, 2011. N 2. P. 50–54.

The paper contains a brief overview of debugger and emulator techniques, and vulnerabilities of such techniques. A new algorithm for detection of anti-debugging and anti-emulation tricks, as well as a way of using debugger and emulator together for malware analysis purpose are suggested.

Keywords — Emulator, Debugger, Anti-debugging and Anti-emulation Techniques, Malware Analysis.

Refs: 6 titles.

УДК 681.322

Многоалфавитный блочный шифр со скрытой нумерацией блоков

Алексеев А. П., Макаров М. И. Информационно-управляющие системы, 2011. № 2. С. 55–62.

Рассматривается шифр многоалфавитной замены, основанный на интегральном преобразовании, работа которого строится таким образом, чтобы выходное распределение чисел криптограммы было равномерным. В шифре используется дробление криптограммы на блоки, скрытая нумерация каждого блока и пересылка блоков по нескольким каналам связи.

Ключевые слова — криптография, стеганография, адаптивный многоалфавитный шифр, пространственно-временной метод распыления информации.

Список лит.: 6 назв.

UDK 681.322

Multi-Alphabet Block Cipher with Hidden Block Numbering

Alekseev A. P., Makarov M. I. IUS, 2011. N 2. P. 55–62.

The article deals with multi-alphabet cipher substitution, based on an integral transform that works such a way that the output distribution of the elements of the cryptogram has a uniform distribution. The method of information protection uses fragmentation of the cryptogram on the blocks, hidden numbering of each block, and sends blocks across multiple communication channels.

Keywords — Cryptography, Steganography, Adaptive Multi-Alphabet Cipher, Spatio-Temporal Method of Spraying Information.

Refs: 6 titles.

УДК 681.3

Расширение функциональности стандартов электронной цифровой подписи

Молдовян Д. Н., Дернова Е. С., Сухов Д. К. Информационно-управляющие системы, 2011. № 2. С. 63–67.

Рассмотрена реализация схем слепой и слепой коллективной подписи, использующих процедуры проверки подлинности электронной цифровой подписи, рекомендуемые российскими стандартами.

Ключевые слова — электронная цифровая подпись, слепая подпись, открытый ключ, стандарты электронной цифровой подписи, коллективная слепая подпись.

Список лит.: 10 назв.

UDK 681.3

Functionality Extension of the Digital Signature Standards

Moldovyan D. N., Dernova E. S., Sukhov D. K. IUS, 2011. N 2. P. 63–67.

We discuss implementations of the blind digital signature (DS) and collective blind DS schemes based on the DS verification equation specified by the Russian DS standards.

Keywords — Digital Signature, Blind Signature, Public Key, Signature Standards, Blind Collective Signature.

Refs: 10 titles.

УДК 519.71

Статистическая линеаризация многомерных стохастических систем по информационному критерию

Чернышев К. Р. Информационно-управляющие системы, 2011. № 2. С. 68–72.

Предложена конструктивная процедура построения линейной входо-выходной модели, которая представляет собой статистический эквивалент некоторой нелинейной многомерной динамической стохастической системы с гауссовым входным процессом в виде белого шума. Ключевым моментом такой процедуры является использование в качестве критерия статистической линеаризации условия покомпонентного совпадения взаимной информации входного и выходного процессов системы и взаимной информации входного и выходного процессов модели. Данный подход позволяет получить явные соотношения, определяющие элементы весовых матриц линеаризованной модели.

Ключевые слова — взаимная информация, входо-выходная модель, гауссова плотность распределения, информационный критерий, меры зависимости, многомерная система, статистическая линеаризация.

Список лит.: 8 назв.

UDK 519.71

Statistical Linearization of Multi Input / Multi Output Stochastic Systems by the Information Theoretic Criterion

Chernyshev K. R. IUS, 2011. N 2. P. 68–72.

A constructive procedure of deriving a linear input/output model that is statistically equivalent to a multi input / multi output dynamic stochastic system driven by a white-noise Gaussian process is proposed. A key issue of such procedure is using the condition of component-wise coincidence of the mutual information of the input and output processes of the system and the input and output processes of the model as an identification criterion. The approach allows to derive explicit relationships determining elements of the weighting matrices of the linearized model. Here, using such unreal preliminary assumption as a known joint probability distribution of the system and model output processes is eliminated.

Keywords — Mutual Information, Input/Output Model, Gaussian Distribution Density, Information Criterion, Measure of Dependence, Multi Input/Multi Output System Statistical Linearization.

Refs: 8 titles.

УДК 378.4

Модель управления рисками образовательного учреждения

Костюкова Т. П., Лысенко И. А. Информационно-управляющие системы, 2011. № 2. С. 73–76.

Изложен подход по управлению рисками образовательного учреждения. Приведена классификация внешних и внутренних рисков. Предложена модель управления рисками, обеспечивающая учет их влияния, повышение оперативности и качества принятия управленческих решений в вузе.

Ключевые слова — образовательное учреждение, внешние риски, внутренние риски, оценка рисков, управление рисками.

Список лит.: 4 назв.

UDK 378.4

Risk Management Model at Educational Institutions

Kostyukova T. P., Lysenko I. A. IUS, 2011. N 2. P. 73–76.

In the article we present an approach of risk management at the educational institutions. We provide the classification of external and internal risks. A risk management model is proposed that ensures the impact of risks, and increase efficiency and quality of decision-making process at the educational institutions.

Keywords — Educational of Establishmen, External risks, Internal risks, the Estimation of Risks, Risk Management.

Refs: 4 titles.

УДК 330.101.5

Логико-вероятностная модель операционного риска банка

Карасева Е. И., Степанов А. Г. Информационно-управляющие системы, 2011. № 2. С. 77–83.

Предложены структурная, логическая и вероятностная модели операционного риска банка с внутренними, внешними и повторными инициирующими событиями для вычисления резервирования под операционный риск. Изложены результаты исследований логико-вероятностной модели операционного риска банка и анализа вкладов инициирующих и повторных событий в риск.

Ключевые слова — операционный риск, структурная, логическая, вероятностная модели риска, внешние, внутренние и повторные инициирующие события, резервирование капитала, управление, анализ.

Список лит.: 10 назв.

UDK 330.101.5

LP Operational Risk Model in Banking

Karaseva E. I., Stepanov A. G. IUS, 2011. N 2. P. 77–83.

Structural, logical and probabilistic models of operational risk in banking with outside initiating events, inside initiating events and repeated initiating events for calculation of reservation fund under operational risk are presented. Research results for LP-model of operational risk in banking and analysis of contributions of initiating and repeated events in risk are discussed.

Keywords — Operational Risk, Structural, Logical, Probabilistic Model Risks, Outside Initiating Event, Inside Initiating Event, Repeated Initiating Event, Reservation Fund, Management, Analysis, Banking.

Refs: 10 titles.

УДК 551.52

Высотно-стратифицированный трехволновый метод измерения параметров солнечной радиации в береговых зонах в видимой области света

Агаев Ф. Г., Ибрагимов Э. А. Информационно-управляющие системы, 2011. № 2. С. 84–85.

Рассмотрен высотно-стратифицированный трехточечный трехволновый метод для измерения дискретных значений солнечной постоянной по результатам фотометрических измерений на береговой зоне. Даны необходимые формулы для проведения вычислений.

Ключевые слова — солнечная радиация, трехволновый метод, видимая область солнечного спектра.

Список лит.: 2 назв.

UDK 551.52

Height Stratified Three-Wavelength Method for Measuring Solar Radiation Parameters in Coastal Zones in Visible Spectral Band

Agaev F. G., Ibrahimov E. A. IUS, 2011. N 2. P. 84–85.

A height stratified three-wavelength method for calculation of discreet values of solar constants by the results of photometric measurements carried out in coastal zone in visible band is suggested. The mathematical grounds of the suggested method is given.

Keywords — Solar Radiation, Three-Wavelength Method, Visible Band of Solar Spectrum.

Refs: 2 titles.

УДК 681.326.3

Математические и имитационные модели сигналов для отладки алгоритмов обработки информации в бортовых автоматизированных системах контроля

Кублановский В. Б. Информационно-управляющие системы, 2011. № 2. С. 86–88.

Предлагаются математические и имитационные модели входных информационных и мешающих сигналов, наблюдаемых в автоматизированных системах контроля бортовой аппаратуры летательных аппаратов. Модели основаны на экспериментальных данных, предназначены для отладки аппаратуры и программного обеспечения автоматизированных бортовых систем контроля, работающих в условиях жестко ограниченных временных и аппаратных ресурсов.

Ключевые слова — математическая модель, имитационная модель, информационный параметр, алгоритм обработки, система контроля.

Список лит.: 5 назв.

UDK 681.326.3

Mathematical and Simulation Models of Signals for Information Processing Algorithms Adjustment in On-Board Automated Control Systems

Kublanovsky V. B. IUS, 2011. N 2. P. 86–88.

In this paper, mathematical and simulation models of input information and disturbing signals of automated control systems in aircraft on-board equipment are offered. The models are based on experimental data and intended for adjustment of hardware and software of automated on-board control systems, working under strictly time- and hardware resource limited conditions.

Keywords — Mathematical Model, Simulation Model, Information Parameter, Processing Algorithm, Control System.

Refs: 5 titles.

ISSN 1684-8853

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ