Учредитель
НОУ ВПО «Российский новый университет»

Издатель
НОУ ВПО «Российский новый университет»

Журнал зарегистрирован
в Министерстве Российской Федерации по делам печати, телерадиовещания
и средств массовых коммуникаций.
Свидетельство о регистрации
№ 77-14812 от 12 марта 2003 г.

Адрес редакции:
105005 Москва, ул. Радио, 22.
Тел. (495) 544-41-67,
тел./факс (495) 544-41-67,
(495) 223-40-70
www.vestnik-rosnou.ru
E-mail: ridrosnou@mail.ru

ISSN 1998-4618

ВЕСТНИК

РОССИЙСКОГО НОВОГО УНИВЕРСИТЕТА

Журнал входит в Перечень ведущих рецензируемых научных журналов и изданий, рекомендованных ВАК для публикации основных результатов диссертационных исследований

Журнал основан в 2003 г.

Выходит 12 раз в год по сериям

Серия
«Сложные системы:
модели, анализ и управление»

Выпуск 2

Статьи публикуются в авторской редакции

ISSN 1998-4618

СОДЕРЖАНИЕ

СЛОЖНЫЕ СИСТЕМЫ: МОДЕЛИ, АНАЛИЗ И УПРАВЛЕНИЕ

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

УПРАВЛЕНИЕ СЛОЖНЫМИ СИСТЕМАМИ

ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Математическое моделирование

УДК 517.55; 517.988

А.С. Крюковский[1]
Ю.И. Скворцова[2]

A.S. Kryukovsky
Yu.I. Skvortsova

КАУСТИЧЕСКАЯ СТРУКТУРА КРАЕВОЙ КАТАСТРОФЫ $K_{4,2}$[3]

CAUSTIC STRUCTURE OF EDGE CATASTROPHE $K_{4,2}$

Изучена каустическая структура краевой катастрофы $\mathbf{K}_{4,2}$, *возникающей при совместной каспоидной пространственной и временной фокусировке электромагнитного излучения волны в плазменном слое с сильной частотной дисперсией.*

Ключевые слова: *краевая катастрофа, каустики, электромагнитная волна, частотная модуляция, дисперсия, плазма.*

The structure of regional catastrophe $\mathbf{K}_{4,2}$, *arising at joint cuspoid space and time focusing of electromagnetic radiation of a wave in a plasma layer with a strong frequency dispersion is investigated.*

Keywords*: edge catastrophe, caustics, electromagnetic wave, frequency modulation, dispersion, plasma.*

Настоящая работа посвящена исследованию каустической структуры краевой катастрофы $\mathbf{K}_{4,2}$, описывающей унимодальную каспоидную фокусировку первичных и вторичных лучевых семейств. Как показано в работах [1–4], волновая катастрофа $\mathbf{K}_{4,2}$ возникает как в задачах стационарной дифракции, когда и первичное, и вторичное излучение имеет особенность каспоидного типа $\mathbf{A}_3$, так и в нестационарных задачах распространения электромагнитных сигналов при совместной фокусировке пространственных и временных лучевых семейств.

Как известно [1–4], универсальная деформация катастрофы $\mathbf{K}_{4,2}$ имеет вид:

$$F_{K_{4,2}} = k_1 z^2 + a x^2 z + k_2 x^4 + \\ + \lambda_1 x + \lambda_2 x^2 + \lambda_3 z + \lambda_4 x z, \qquad (1)$$

где x и z – внутренние переменные, a – функциональный модуль, а λ_1, λ_2, λ_3, λ_4 – коэффициенты

[1] Доктор физико-математических наук, профессор, декан факультета ИСиКТ НОУ ВПО «Российский новый университет».

[2] Заместитель декана факультета ИСиКТ НОУ ВПО «Российский новый университет».

[3] Работа выполнена при поддержке РФФИ (гранты № 15-02-04206-а, № 13-07-00937-а, ОФИ_М № 13-02-12121).

универсальной деформации, причем $z \in [0,+\infty)$, $x \in (-\infty,+\infty)$. В соответствии с необходимыми и достаточными условиями образования катастрофы $\mathbf{K_{4,2}}$ [4–8], на функциональный модуль a накладываются ограничения [9]:

$$a^2 \neq \pm 4 . \qquad (2)$$

Параметры k_1 и k_2 принимают значения +1 или –1.

Равномерная асимптотика, соответствующая рассматриваемой особенности, имеет вид [2]:

$$U(\vec{r},t) = e^{i\theta}\left\{(l_1)_g I^{K_{4,2}}(a;\vec{\lambda}) + \sum_{k=3}^{4}(l_k)_g \frac{\partial I^{K_{4,2}}}{\partial \lambda_k} + \right.$$

$$\left. + (l_1)_E I^{A_3}(\lambda_1,\lambda_2) + \sum_{k=1}^{2}(l_k)_E \frac{\partial I^{A_3}}{\partial \lambda_k}\right\}, \qquad (3)$$

где $I^{K_{4,2}}(a,\vec{\lambda}) =$

$$= \int_0^{+\infty} dz \int_{-\infty}^{+\infty} \exp\left\{ i\left(k_1 z^2 + a x^2 z + k_2 x^4 + \lambda_1 x + \right.\right.$$

$$\left.\left. + \lambda_2 x^2 + \lambda_3 z + \lambda_4 x z\right)\right\} dx \qquad (4)$$

спецфункция (СВК) краевой катастрофы $\mathbf{K_{4,2}}$ (в показателе экспоненты стоит универсальная деформация (1)), а

$$I^{A_3}(\lambda_1,\lambda_2) = \int_{-\infty}^{+\infty} \exp\left\{ i\left(k_2 x^4 + \lambda_2 x^2 + \lambda_1 x\right)\right\} dx \qquad (5)$$

функция Пирси, то есть СВК основной катастрофы $\mathbf{A_3}$. Её универсальная деформация получается как сужение исходной универсальной деформации с помощью подстановки $z = 0$. В формуле (3) θ – фаза бегущей волны, а $(l_j)_g$ и $(l_j)_E$ – геометрооптические (ГО) и краевые коэффициенты асимптотического разложения.

Рассмотрим каустические структуры катастрофы $\mathbf{K_{4,2}}$. Во-первых, отметим, что разложение катастрофы $\mathbf{K_{4,2}}$ на основную особенность и катастрофу сужения имеет вид [2; 6]: $K_{4,2} = (A_3, A_3)$, то есть обе особенности представляют собой каустическое остриё. Только ГО каустическое остриё имеет обрыв. Поэтому каустики (огибающие семейство ГО и краевых лучей) будут иметь форму клювов, причем связывает их прямая – граница свет-тень.

Рассмотрим сначала краевые лучи. Уравнения краевых лучей получаются из дифференцирования сужения ($z = 0$) исходной универсальной деформации (1), имеющей вид:

$$F_{A_3} = k_2 x^4 + \lambda_2 x^2 + \lambda_1 x \qquad (6)$$

по параметру x и приравниванием результата нулю:

$$\lambda_1 = -4k_2 x^3 - 2\lambda_2 x . \qquad (7)$$

Для того чтобы получить каустику (огибающую семейства краевых лучей), необходимо дополнить уравнение (7) нулем второй производной функции (6) по x:

$$12k_2 x^2 + 2\lambda_2 = 0 . \qquad (8)$$

В результате найдем уравнение каустики в параметрической форме:

$$\begin{cases} \lambda_1 = 8k_2 x^3 \\ \lambda_2 = -6k_2 x^2 \end{cases} . \qquad (9)$$

Рассмотрим теперь каустику ГО лучей. Лучевые уравнения получаются дифференцированием универсальной деформации (1) по внутренним переменным x и z:

$$\begin{cases} \lambda_1 = -4k_2 x^3 - 2a x z - 2\lambda_2 x - \lambda_4 z \\ \lambda_3 = -a x^2 - 2k_1 z - \lambda_4 x \end{cases} . \qquad (10)$$

Для того чтобы получить каустику ГО лучей, необходимо дополнить уравнения (10) нулем Гессиана универсальной деформации (1) по внутренним переменным:

$$\det \begin{Vmatrix} \dfrac{\partial^2 F_{K_{4,2}}}{\partial x^2} & \dfrac{\partial^2 F_{K_{4,2}}}{\partial x \partial z} \\ \dfrac{\partial^2 F_{K_{4,2}}}{\partial x \partial z} & \dfrac{\partial^2 F_{K_{4,2}}}{\partial z^2} \end{Vmatrix} = 0 . \qquad (11)$$

Подставляя (1) в (11), получаем:

$$2k_1(12k_2 x^2 + 2az + 2\lambda_2) - (2ax + \lambda_4)^2 = 0 , \qquad (12)$$

откуда находим внутренний параметр z:

$$z = \frac{(2ax + \lambda_4)^2 - 24k_1 k_2 x^2 - 4k_1\lambda_2}{4k_1 a} . \qquad (13)$$

Подставив (13) в (10) и выполнив соответствующие преобразования, найдем, как и в случае каустики краевых лучей, выражения для λ_1 и λ_2:

$$\begin{cases} \lambda_1 = \dfrac{\lambda_3\lambda_4 - 4a^2 x^3 + 16k_1 k_2 x^3 - 3ax^2\lambda_4}{2k_1} \\ \lambda_2 = \dfrac{\lambda_4^2 + 6a^2 x^2 - 24k_1 k_2 x^2 + 2a\lambda_3 + 6ax\lambda_4}{4k_1} \end{cases} . \qquad (14)$$

Для того чтобы получить уравнение границы свет-тень, подставим $z = 0$ в систему (10) и, выполнив преобразования, найдем, что:

$$\lambda_1 = -2x_b\lambda_2 - 4k_2 x_b^3 , \qquad (15)$$

где

$$x_b = x_{b2} = \frac{-\lambda_4 + \sqrt{\lambda_4^2 - 4a\lambda_3}}{2a} \qquad (16)$$

или

$$x_b = x_{b1} = \frac{-\lambda_4 - \sqrt{\lambda_4^2 - 4a\lambda_3}}{2a} . \qquad (17)$$

На рис. 1–9 показаны каустические структуры катастрофы $\mathbf{K}_{4,2}$ в плоскости (λ_1, λ_2) при различных значениях параметров λ_3, λ_4 и функционального модуля a. Толстой линией на рисунках показана каустика ГО лучей. Её аналитическое продолжение, отсекаемое границей свет-тень, показано штриховой линией (пунктиром). Штрихпунктирной линией показана граница свет-тень. Наконец, тонкой линией показана каустика краевых лучей.

Сначала рассмотрим случай, когда параметры λ_3, λ_4 равны нулю. Рис. 1 соответствует случаю $a = 0$.

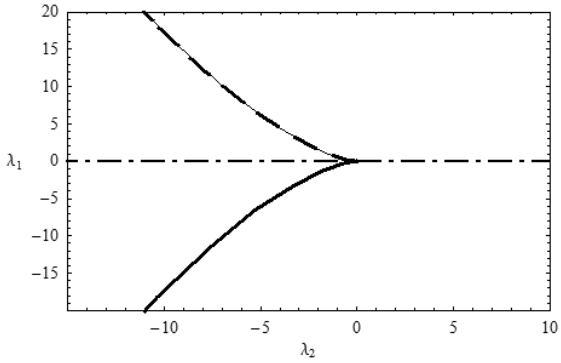


Рис. 1. $a = 0$; $k_1 = k_2 = 1$, $\lambda_3 = \lambda_4 = 0$

Каустика краевых лучей (каустическое остриё) совпадает с каустикой ГО и её продолжением, граница свет-тень является биссектрисой.

При увеличении функционального модуля a каустика ГО лучей (и её продолжение) отрывается от каустики краевых лучей (рис. 2) и стремится при $a \to 2$ к вертикали, что является вырожденным случаем.

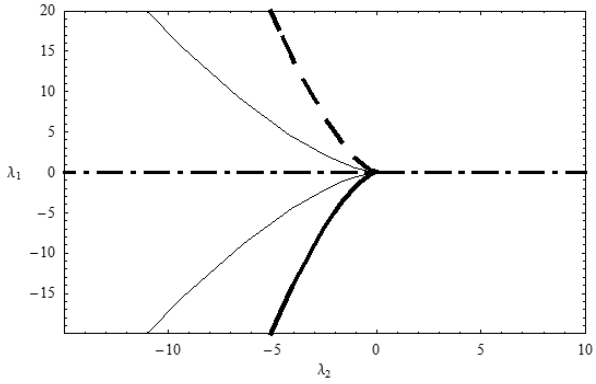


Рис. 2. $a = 1{,}9$; $k_1 = k_2 = 1$, $\lambda_3 = \lambda_4 = 0$

В случае когда функциональный модуль превосходит 2 (рис. 3), остриё ГО лучей отображается относительно острия краевых лучей в правую часть рисунка.

Необходимо отметить, что на рис. 1–3 при всех значениях функционального модуля точка с координатами (0,0) является особой точкой катастрофы $\mathbf{K}_{4,2}$, так как изменение функционального модуля не устраняет особенности.

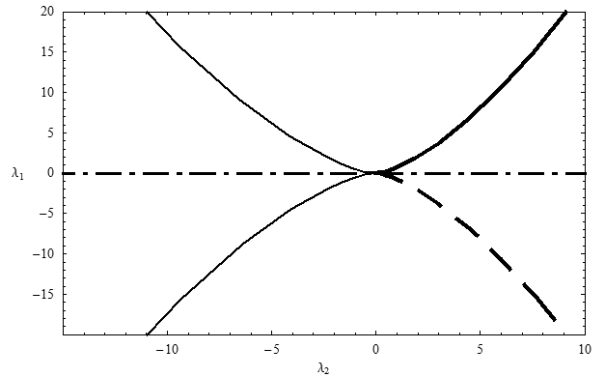


Рис. 3. $a = 2{,}5$; $k_1 = k_2 = 1$, $\lambda_3 = \lambda_4 = 0$

Рассмотрим теперь случаи, когда параметры λ_3 и λ_4 не равны нулю. На рис. 4 показан случай, когда и λ_3, и λ_4 не равны нулю, но разных знаков.

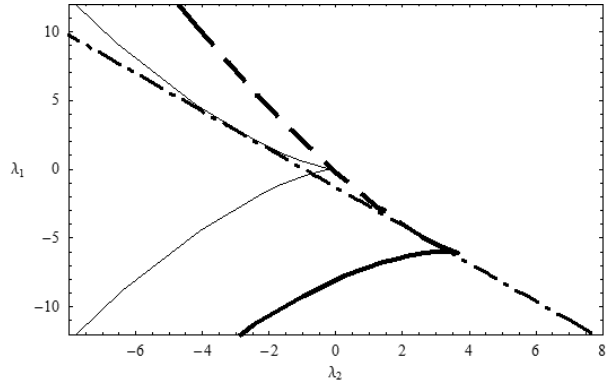


Рис. 4. $a = 0{,}5$; $k_1 = k_2 = 1$, $\lambda_3 = -3$, $\lambda_4 = 4$

Поскольку a меньше 2, оба каустических острия смотрят вправо, в разных точках касаются границы свет-тень и смещены относительно друг друга. Для вычисления x_b использовалась формула (16).

Аналогичная картина возникает, если поменять знак у функционального модуля (рис. 5).

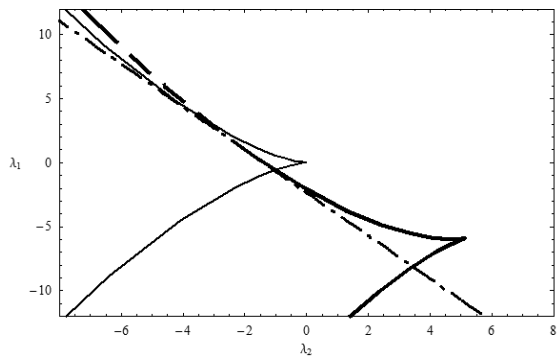


Рис. 5. $a = -0{,}5$; $k_1 = k_2 = 1$, $\lambda_3 = -3$, $\lambda_4 = 4$

Пусть теперь функциональный модуль превышает 2, причем k_2 принимает значение не +1, а –1 (рис. 6).

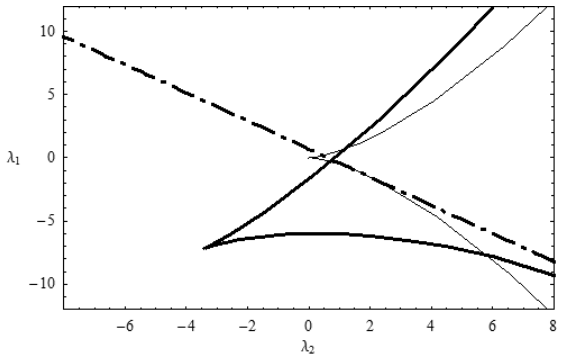


Рис. 6. $a = 2{,}5$; $k_1 = 1$, $k_2 = -1$, $\lambda_3 = -3$, $\lambda_4 = 4$

Видно, что оба каустических острия смотрят влево, причём каустическое остриё краевых лучей отстаёт от каустического острия ГО лучей. Для вычисления x_b по-прежнему использовалась формула (16).

Поменяем знак функционального модуля и знаки у λ_3 и λ_4 (рис. 7).

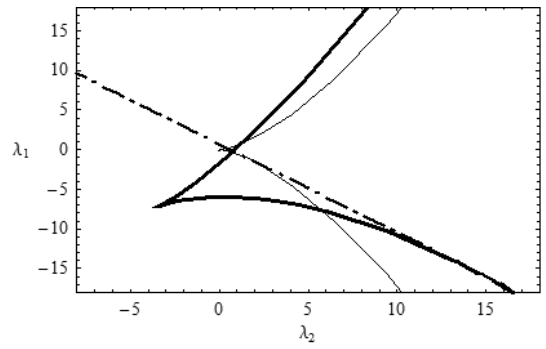


Рис. 7. $a = -2{,}5$; $k_1 = 1$, $k_2 = -1$, $\lambda_3 = 3$, $\lambda_4 = -4$

Видно, что картина качественно не изменилась, но для вычисления x_b теперь уже используется формула (17).

Поменяем знак у k_1 с плюса на минус и сохраним неизменными остальные параметры.

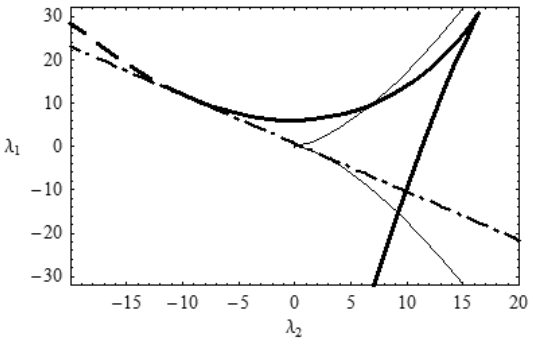


Рис. 8. $a = -2{,}5$; $k_1 = -1$, $k_2 = -1$, $\lambda_3 = 3$, $\lambda_4 = -4$

Теперь каустическое остриё краевых лучей (которое осталось на месте) и каустическое остриё ГО лучей смотрят в разные стороны. Для вычисления x_b используется формула (17).

Наконец, рассмотрим случай, когда граница свет-тень отрезает полностью каустическое остриё ГО лучей, оставляя только каустику с краем (рис. 9).

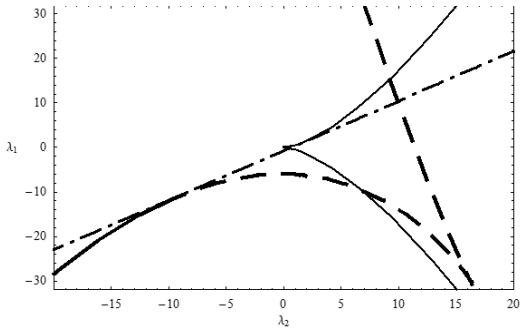


Рис. 9. $a = 2{,}5$; $k_1 = -1$, $k_2 = -1$, $\lambda_3 = -3$, $\lambda_4 = -4$
или $a = -2{,}5$; $k_1 = -1$, $k_2 = -1$, $\lambda_3 = 3$, $\lambda_4 = 4$

Это возможно в двух случаях: когда функциональный модуль положительный, а параметры λ_3, λ_4 отрицательные, либо наоборот – функциональный модуль отрицательный, а параметры λ_3, λ_4 положительные. В первом случае для вычисления x_b используется формула (17), а во втором – формула (16).

Аналогично, как показано в работах [10–12], посвященных информационной системе «Волновые катастрофы в радиофизике, акустике и квантовой механике» (wavecat.rosnou.ru), могут быть исследованы каустические структуры и более сложных краевых особенностей.

Таким образом, в настоящей работе исследована каустическая структура краевой катастрофы $\mathbf{K_{4,2}} = \mathbf{(A_3, A_3)}$, распадающейся две каспоидные катастрофы $\mathbf{A_3}$, соответствующие каустикам семейств краевых и ГО лучей [1; 2; 6]. Катастрофы каспоидного такого типа возникают в задачах распространения и дифракции волн и соответствуют областям фокусировок (см., например, [3; 13; 14]). Краевые катастрофы возникают при совместной пространственной и временной фокусировке электромагнитного излучения волны в плазменном слое с сильной частотной дисперсией [3; 4]. Для описания электромагнитных полей в таких областях разработана волновая теория катастроф [1; 2; 6], опирающаяся как на классические результаты теории катастроф [9], так и на лучевые методы [15–17].

Приведены каустические структуры краевой катастрофы $\mathbf{K_{4,2}}$ при различных коэффициентах универсальной деформации и функционального модуля.

Литература

1. Крюковский А.С., Лукин Д.С. Краевые и угловые катастрофы в равномерной геометрической теории дифракции : учебное пособие. – М. : МФТИ, 1999. – 134 с.

2. Крюковский А.С. Равномерная асимптотическая теория краевых и угловых волновых катастроф. – М. : РосНОУ, 2013. – 368 с.

3. Крюковский А.С., Лукин Д.С., Палкин Е.А., Растягаев Д.В. Теория катастроф в проблемах стационарной и нестационарной дифракции // Труды X школы-семинара по дифракции и распространению волн. 7–15.02.1993. – М. : МФТИ, 1993. – С. 36–111.

4. Крюковский А.С., Скворцова Ю.И. Применение теории катастроф для описания пространственно-временной структуры частотно-модулированного сигнала в плазме // Электромагнитные волны и электронные системы. – 2013. – Т. 18. – № 8. – С. 18–23.

5. Крюковский А.С., Растягаев Д.В. О необходимых и достаточных условиях образования каспоидных катастроф // Распространение и дифракция волн в неоднородных средах : сборник. – М. : МФТИ, 1989. – С. 56–60.

6. Крюковский А.С., Лукин Д.С., Палкин Е.А. Краевые и угловые катастрофы в задачах дифракции и распространения волн. – Казань : Каз. авиационный ин-т, 1988. – 199 с.

7. Крюковский А.С. Необходимые и достаточные условия образования основных волновых катастроф с корангом, равным двум // Распространение и дифракция электромагнитных волн : междувед. сб. – М. : МФТИ, 1993. – С. 4–19.

8. Крюковский А.С. Необходимые и достаточные условия образования краевых катастроф // Проблемы дифракции и распространения волн : межвед. сб. – М. : МФТИ, 1994. – С. 47–54.

9. Арнольд В.И., Варченко А.Н., Гусейн-Заде С.М. Особенности дифференцируемых отображений. – М. : Наука, 1982. – Т. 1. Классификация критических точек, каустик и волновых фронтов. – 304 с.

10. Дорохина Т.В., Крюковский А.С., Лукин Д.С. Информационная система «Волновые катастрофы в радиофизике, акустике и квантовой механике» // Электромагнитные волны и электронные системы. – 2007. – Т. 12. – № 8. – С. 71–75.

11. Дорохина Т.В., Крюковский А.С., Лукин Д.С., Волкова Е.В., Костьо А.О., Павлова М.В. Создание информационной системы волновой теории катастроф и её применение при математическом моделировании // Вестник Российского нового университета. – 2007. – Выпуск 2. – С. 91–107.

12. Дорохина Т.В., Ипатов Е.Б., Крюковский А.С., Лукин Д.С., Палкин Е.А., Растягаев Д.В. Математическое компьютерное моделирование волновых полей типа катастроф // Распространение радиоволн: сборник докладов XXI Всероссийской научной конференции. – Йошкар-Ола, 25–27 мая 2005 г. – Йошкар-Ола : МарГТУ, 2005. – Т. 2. – С. 336–339.

13. Крюковский А.С., Лукин Д.С. Локальная асимптотика быстроосциллирующих интегралов, описывающих волновое поле в областях фокусировки // Дифракция и распространение электромагнитных волн : междувед. сб. – М. : МФТИ, 1984. – С. 39–53.

14. Крюковский А.С., Растягаев Д.В. Исследование устойчивых фокусировок, возникающих при нарушении симметрии волнового фронта // Дифракция и распространение электромагнитных волн : сборник. – М. : МФТИ, 1993. – С. 20–37.

15. Крюковский А.С., Лукин Д.С., Кирьянова К.С. Метод расширенной бихарактеристической системы при моделировании распространения радиоволн в ионосферной плазме // Радиотехника и электроника. – 2012. – Т. 57. – № 9. – С. 1028–1034.

16. Крюковский А.С., Скворцова Ю.И. Описание пространственно-временной структуры частотно-модулированного импульса методами волновой теории катастроф // IV Всероссийские Армандовские чтения [Электронный ресурс]: радиофизические методы в дистанционном зондировании сред : материалы VI Всероссийской научной конференции (Муром, 27–29 мая 2014 г.). – Муром : Изд.-полиграфический центр МИ ВлГУ, 2014. – 296 с. – С. 85–92.

17. Крюковский А.С., Растягаев Д.В., Скворцова Ю.И. Распространение частотно-модулированных пространственно-временных радиоволн в анизотропной ионосфере : труды XXIV Всероссийской научной конференции «Распространение радиоволн» (29 июня – 5 июля 2014 г., Иркутск). – Иркутск : ИСЗФ СО РАН, 2014. – Т. 4. – С. 126–129.

УДК 621.396.91/.96

Д.А. Денисенков[1]
В.Ю. Жуков[2]

ОБНАРУЖЕНИЕ СДВИГА ВЕТРА НА ОСНОВЕ АНАЛИЗА КАРТ ШИРИНЫ СПЕКТРА СИГНАЛА, ПРИНИМАЕМОГО МЕТЕОРОЛОГИЧЕСКИМ РАДИОЛОКАТОРОМ

Разработана аналитическая модель пространственного распределения ширины спектра радиальных скоростей частиц метеообразования при его наблюдении метеорологическим радиолокатором под малыми углами места. Проанализировано несколько характерных вариантов структуры ветра. Представлены способы обнаружения наличия сдвига ветра и определения его параметров.

Ключевые слова: *математическая модель, ширина спектра радиальных скоростей частиц, метеорологический радиолокатор, сдвиг ветра.*

D.A. Denisenkov
V.Yu. Zhukov

THE DETECTION OF WIND SHEAR ON THE BASIS OF THE ANALYSIS MAPS SPECTRUM WIDTH OF THE SIGNAL RECEIVED BY THE WEATHER RADAR

There has been developed a mathematical model of the spatial distribution spectral width of radial velocities particles of the meteorological formations in the time of observing by weather radar at low elevation angles. There has been analyzed some specific options surface of wind patterns. The way of detect the presence of wind shear has been presented for each option and has been determined its parameters.

Keywords: *mathematical model, spectral width of radial velocities particles, weather radar, wind shear.*

Для авиации большой интерес представляет информация о наличии такого опасного явления, как сдвиг ветра в пограничном слое атмосферы высотой до 500 м [1]. Современные метеорологические радиолокаторы предоставляют информацию о наличии данных явлений, но не с требуемым разрешением и не в указанном диапазоне высот [2]. В связи с этим большой интерес представляет исследование информации, которая может быть извлечена из поставляемых ими карт ширины спектра сигнала (рис. 1).

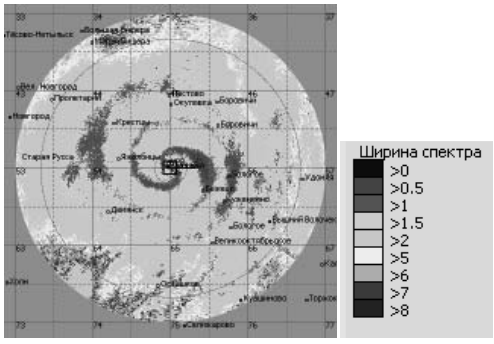


Рис. 1. Карта распределения ширины спектра по поверхности конического разреза

Авторами была выдвинута гипотеза о тесной связи вертикального профиля ветра с особенностями пространственного распределения параметра на указанных картах [3]. Для ее подтверждения была разработана аналитическая модель, с помощью которой получены карты для трех видов изменения ветра с высотой:

[1] Инженер кафедры технологий и средств геофизического обеспечения войск ФГКОУ ВПО «Военно-космическая академия им. А.Ф. Можайского» Министерства обороны Российской Федерации (ВКА им. А.Ф. Можайского).

[2] Кандидат технических наук, старший научный сотрудник 32 отдела ВИНИ ФГКОУ ВПО «Военно-космическая академия им. А.Ф. Можайского» Министерства обороны Российской Федерации (ВКА им. А.Ф. Можайского).

1) два слоя гидрометеоров с различными векторами скорости в каждом из них (рис. 2а);

2) два слоя, в одном из которых скорость ветра равномерно изменяется по величине (рис. 2б);

3) два слоя с равномерным изменением скорости и направления ветра в одном из них (рис. 2в).

Достаточно сравнить рис. 1 и 2в, чтобы убедиться в том, что гипотеза хорошо согласуется с реальными результатами.

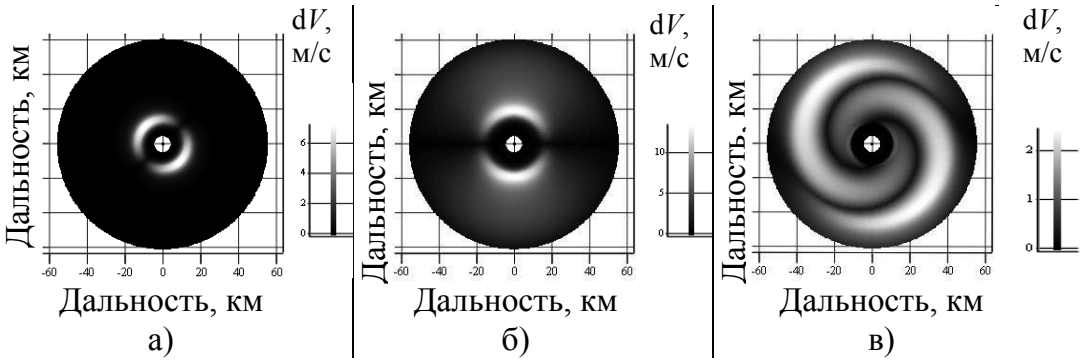


Рис. 2. Карты распределения ширины спектра по поверхности конического разреза

Следующий шаг – решение обратной задачи восстановления профиля ветра на основе анализа полученной карты. Для этого была разработана математическая модель пространственного распределения ширины спектра радиальных скоростей гидрометеоров, на основании которой возможно не только обнаружить сдвиг ветра, но и оценить его количественные характеристики.

В поставленной задаче было принято, что метеоцель состоит из двух смежных слоев с разными отражаемостью, направлением и скоростью ветра в каждом из них. Параметры слоев следующие:

– первый слой: диапазон высот – от 0 до h_1, отражаемость слоя – Z_1, скорость и направление ветра постоянны и равны соответственно V_1 и γ_1, ширина спектра скоростей σ_1;

– второй слой: диапазон высот – от h_1 до бесконечности, отражаемость – Z_2, скорость и направление ветра в общем случае изменяются с высотой в соответствии с функциями $V_2(h)$ и $\gamma_2(h)$, ширина спектра скоростей – σ_2.

Ширина спектра суммарного сигнала $S(w)$, состоящего из двух составляющих $S_1(w)$ и $S_2(w)$, определяется формулой [4]

$$\sigma^2 = \frac{1}{P_1 + P_2}\left[P_1\sigma_1^2 + P_2\sigma_2^2 + \frac{P_1P_2}{P_1 + P_2}\left(F_1 - F_2\right)^2 \right], \quad (1)$$

где F_1 и F_2 – средние частоты, а P_1 и P_2 – мощности сигналов от первого и второго слоев соответственно.

На основе созданной численной модели принимаемого радиолокатором сигнала исследовано пространственное распределение ширины спектра для четырех характерных вариантов структуры приземного ветра.

Первый вариант метеообстановки – «скачок» вектора скорости – два слоя с разной отражаемостью и разным направлением ветра в каждом из них.

В этом случае наибольшего значения ширина спектра достигает при равенстве мощностей отражений от обоих слоев и при азимуте антенны, на котором значение разности $F_1 - F_2$ максимально и соответствует вектору разности скоростей $\vec{V}_1 - \vec{V}_2$ (рис. 3).

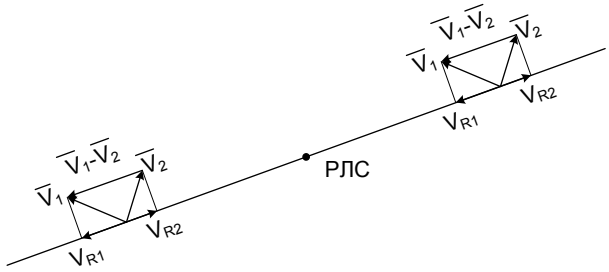


Рис. 3. Формирование максимума ширины спектра сигнала при «скачке» вектора скорости

Величины σ_1 и σ_2 можно оценить по отражениям от соседних элементов разрешения, в которых присутствует только один из слоев. Тогда сдвиг ветра ΔV определяется по формуле

$$\Delta V = V_1 - V_2 = \frac{\lambda}{2}\sqrt{4\tilde{\sigma}^2 - 2\tilde{\sigma}_1^2 - 2\tilde{\sigma}_2^2}, \quad (2)$$

где V_1 – скорость ветра в нижнем слое, V_2 – скорость ветра в верхнем слое, $\tilde{\sigma}$ – оценка величины σ, λ – длина волны.

Второй вариант метеообстановки – «сдвиг ветра без поворота».

Ветер во втором слое меняется с высотой по закону

$$V_2 = V_1 + W\left(h - h_1\right), \quad h \ge h_1. \qquad (3)$$

Аппроксимируем поперечный разрез разрешаемого объема квадратом (рис. 4), равным по площади кругу с радиусом $r = \frac{R\theta}{2}$ (θ – ширина ДН антенны; R – наклонная дальность центра элемента разрешения).

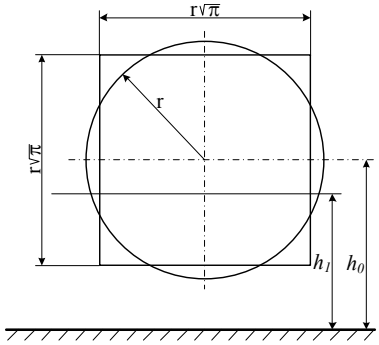


Рис. 4. Аппроксимация элемента разрешения

Средняя частота спектра сигнала, отраженного вторым слоем, вычисляется по формуле:

$$F_2 = \int_{h_1}^{h_0+\frac{r\sqrt{\pi}}{2}} f\left(h\right) p\left(h\right) dh, \qquad (4)$$

где $f(h)$ – доплеровский сдвиг частоты, $p(h)$ – распределение мощности отражений по высоте, принимаемое равномерным, r – радиус поперечного разреза разрешаемого объема, h_0 – высота центра элемента разрешения.

Ширина спектра сигнала, отраженного вторым слоем, вычисляется по формуле:

$$\sigma_2^2 = \int_{h_1}^{h_0+\frac{r\sqrt{\pi}}{2}} \left(f\left(h\right) - F_2\right)^2 p\left(h\right) dh. \qquad (5)$$

После вычисления формул (4), (5) и подстановки результатов в (1) получаем

$$\sigma^2 = \frac{1}{P_1 + P_2}\left[P_1\sigma_1^2 + \frac{W^2A^2}{3\lambda^2}\frac{P_2\left(P_2 + 4P_1\right)}{\left(P_1 + P_2\right)}\right], \qquad (6)$$

где $A = h_0 + \frac{r\sqrt{\pi}}{2} - h_1$.

После ряда математических преобразований приходим к выражению

$$\sigma^2 = \frac{P_1\sigma_1^2}{P_1 + P_2} + \frac{W^2\pi\, r^2}{3\lambda^2}\,\frac{x^2\left(4\varepsilon + \left(1 - 4\varepsilon\right)x\right)}{\left(\varepsilon + \left(1 - \varepsilon\right)x\right)^2}, \qquad (7)$$

где $x = \frac{A}{r\sqrt{\pi}}$, $\varepsilon = \frac{Z_1}{Z_2}$.

Второе слагаемое в формуле (7) имеет максимум только при условии $\varepsilon > 1$ (как правило, выполняемое), который достигается при нахождении x в интервале $0{,}95 \le x < 1$, т.е. в случае, когда разрешаемый объем радиолокатора почти полностью «вышел» из нижнего слоя. Значение максимума невелико и не превышает 120% от той ширины спектра, которая обусловлена сдвигом ветра во втором слое. Следовательно, для оценивания величины W достаточно измерить ширину результирующего спектра на дальности, превышающей на 5% дальность расположения максимума. В этом случае $\varepsilon = 0$, $x = 1$ и из (7) получаем $W = \frac{\sqrt{3}\lambda\sigma}{r\sqrt{\pi}}$.

Третий вариант метеообстановки – «поворот ветра без сдвига».

Направление ветра во втором слое меняется с высотой по закону

$$\gamma_2 = \gamma_1 + \Delta(h - h_1),\ h \ge h_1. \qquad (8)$$

Как было показано в [3], показателем существования рассматриваемой метеообстановки служит появление на карте ширины спектра сигнала характерного распределения минимального значения измеряемого параметра в виде спирали. Следовательно, для оценивания скорости поворота ветра с высотой, надо найти формулу последней, т.е. зависимость дальности точки, в которой наблюдается минимум ширины спектра, от азимута антенны радиолокатора.

Используя принятую ранее аппроксимацию импульсного объема, находим среднюю частоту спектра сигнала, отраженного вторым слоем

$$F_2 = \int_{h_1}^{h_0+\frac{r\sqrt{\pi}}{2}} f\left(h\right) p\left(h\right) dh = \frac{2V_1\cos\left(\alpha\right)}{\Delta\lambda\left(h_0 + \frac{r\sqrt{\pi}}{2} - h_1\right)} \times$$

$$\times\left(\sin\left(\varphi - \gamma_1 - \Delta\left(h_0 + \frac{r\sqrt{\pi}}{2} - h_1\right)\right) - \sin\left(\varphi - \gamma_1\right)\right). \qquad (9)$$

Условием минимума σ^2 будет

$$F_2 = F_1 = \frac{2V_1}{\lambda}\cos\left(\varphi - \gamma_1\right)\cos\left(\alpha\right). \qquad (10)$$

Обозначим

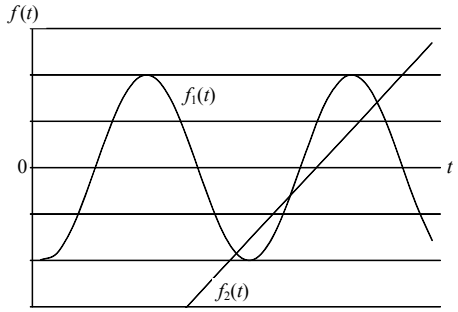
$$t = \Delta\left(h_0 + \frac{r\sqrt{\pi}}{2} - h_1\right), \qquad (11)$$

$$a = \varphi - \gamma_1 \qquad (12)$$

и перепишем (9) с учетом (11) и (12). Получаем

$$\sin\left(a - t\right) = t\cos\left(a\right) + \sin\left(a\right). \qquad (13)$$

Решить данное уравнение возможно только графическим способом [5]. Пример такого решения для $a = 0{,}5$ представлен на рис. 5.



$$f_1(t) = \sin(a - t), \quad f_2(t) = t\cos(a) + \sin(a)$$

Рис. 5. Пример решения уравнения (12)

Четвертый вариант метеообстановки – «сдвиг ветра с поворотом».

Ветер во втором слое меняется с высотой по закону

$$V_2 = \left(V_1 + W(h - h_1)\right)\cos\left(\gamma_1 + \Delta(h - h_1)\right),$$

$$h \geq h_1. \qquad (14)$$

Средняя частота спектра сигнала, отраженного вторым слоем,

$$F_2 = \int_{h_1}^{h_0 + \frac{r\sqrt{\pi}}{2}} f(h)\, p(h)\, dh = \qquad (15)$$

$$= \int_{h_1}^{h_0 + \frac{r\sqrt{\pi}}{2}} \frac{2\left(V_1 + W(h - h_1)\right)}{\lambda\left(h_0 + \frac{r\sqrt{\pi}}{2} - h_1\right)} \cos\left(\varphi - \left(\gamma_1 + \Delta(h - h_1)\right)\right) dh.$$

Используя принятые ранее обозначения, получаем

$$F_2 = \frac{2V_1}{\Delta A\lambda}\left(\sin(a - t) - \sin(a)\right) +$$

$$+ \frac{2W}{\Delta^2 A\lambda}\left(t\sin(a - t) + \cos(a)\cos(a - t)\right). \qquad (16)$$

Минимум наступает при условии $F_2 = F_1$. В итоге приходим к выражению

$$\sin(a - t) + \frac{W}{V_1\Delta} t\sin(a - t) - \frac{W}{V_1\Delta}\cos(a - t) =$$

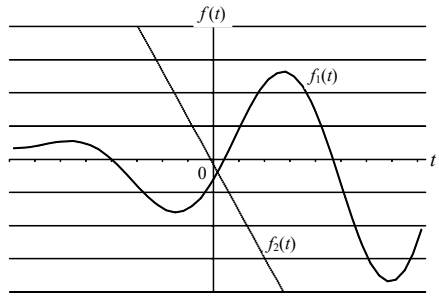
$$= t\cos(a) + \sin(a) - \frac{W}{V_1\Delta}\cos(a)$$

или

$$\left(1 + \frac{W}{V_1\Delta} t\right)\sin(a - t) - \frac{W}{V_1\Delta}\cos(a - t) =$$

$$= t\cos(a) + \sin(a) - \frac{W}{V_1\Delta}\cos(a). \qquad (17)$$

Пример графического решения данного уравнения представлен на рис. 6.



$$f_1(t) = \left(1 + \frac{W}{V_1\Delta} t\right)\sin(a - t) - \frac{W}{V_1\Delta}\cos(a - t),$$

$$f_2(t) = t\cos(a) + \sin(a) - \frac{W}{V_1\Delta}\cos(a)$$

Рис. 6. Пример графического решения уравнения (16)

Заключение

Из приведенных расчетов следует, что получаемые современными метеорологическими радиолокаторами карты ширины спектра принимаемого сигнала несут информацию о распределении вектора скорости ветра по высоте в пограничном слое атмосферы. Характеристики этого распределения могут быть оценены по максимальному значению параметра на указанной карте и по образующейся зависимости его минимального значения от азимута антенны.

Литература

1. Руководство по сдвигам ветра ИКАО.

2. Довиак Р., Зрнич Д. Доплеровские радиолокаторы и метеорологические наблюдения. – Л. : Гидрометеоиздат, 1988. – 512 с.

3. Денисенков Д.А., Жуков В.Ю. Исследование влияния профиля ветра в пограничном слое на пространственное распределение ширины спектра : труды III Всероссийской научной конференции «Проблемы военно-прикладной геофизики и контроля состояния природной среды». – СПб., 2014. – С. 65–71.

4. Жуков В.Ю., Щукин Г.Г. Обоснование метода оценивания доплеровского сдвига частоты эхо-сигнала метеообразований при негауссовой форме их спектра // III Всероссийские Армандовские чтения : материалы IV Всероссийской научной конференции «Сверхширокополосные сигналы в радиолокации, связи и акустике». – Муром, 2013. – С. 174–180.

5. Крюковский А.С. Каустическая и лучевая структуры отраженных радиоволн в линейном плазменном слое // Вестник Российского нового университета. – 2011. – Вып. 4. Управление, вычислительная техника и информатика. – С. 12–22.

УДК 624.04; 539.31

И.С. Клименко[1]
С.В. Холодков[2]

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ КОНЕЧНЫХ ЭЛЕМЕНТОВ И РАСЧЕТА УПРУГОПЛАСТИЧЕСКИХ ТЕЧЕНИЙ ПРИМЕНИТЕЛЬНО К ЗАДАЧЕ УДАРА ТВЕРДОГО ТЕЛА О ДЕФОРМИРУЕМУЮ ПРЕГРАДУ

В настоящей работе приведен сравнительный анализ двух основных методов решения задачи удара твердого тела о деформируемую преграду. Показаны и обсуждены достоинства и ограничения каждого из методов применительно к специфике постановки конкретных задач подобного типа. Продемонстрирована возможность комбинированного использования обсуждаемых методов при решении статических и динамических задач.

Ключевые слова: *математическая модель, твердое тело, деформируемая преграда, сравнительный анализ, достоинства и ограничения методов.*

I.S. Klimenko
S.V. Kholodkov

COMPARATIVE ANALYSIS OF FINITE ELEMENT AND COMPUTATION OF PLASTOELASTIC FLOWS METHODS AS APPLIED TO BLOW TASK

In this paper we present a comparative analysis of the two main methods of solving the problem of the impact of a rigid body about a deformable barrier. The advantages and limitations of each method are showing in relation to the formulation of specificity problems of this type. The possibility of combined using of the discussed methods for solving static and dynamic problems is demonstrated.

Keywords: *mathematical model, solid body, deformable barrier, comparative analysis, advantages and limitations of methods.*

Введение

В работе [1] нами было проведено исследование распределения полей давления и деформаций, возникающих при ударе твердого тела о деформируемую преграду с использованием численного метода расчета упругопластических течений НАМР. Показано, что при выстрелах из травматического оружия может возникать широкий спектр повреждений – от ссадин и кровоподтеков (гематом), размозжения мягких тканей до проникающих ранений. При этом было отмечено, что применение так называемых лагранжевых сеток, которые лежат в основе метода НАМР, ограничено кругом задач с относительно небольшими деформациями среды, следовательно, они неприменимы для рассмотрения ситуаций с пробитием моделируемой области. Тем не менее, с их помощью можно получать косвенные данные об уровне возникающих в этом случае нагрузок и тем самым судить о характере протекания процесса, что как нельзя лучше подходит для рассматриваемой задачи удара.

В настоящей работе мы рассматриваем метод конечных элементов (МКЭ) в качестве альтернативы методу НАМР в случае существенных деформаций. Естественным является проведение сравнительного анализа двух названных методов для выявления достоинств и недостатков каждого из них. При этом мы предполагаем более детально исследовать возможности конечно-разностных методов применительно к задачам такого типа, представляющих значительный интерес в рамках теории пластичности.

Теория пластичности, в отличие от теории

[1] Доктор физико-математических наук, профессор, профессор кафедры информационных систем в экономике и управлении НОУ ВПО «Российский новый университет».

[2] Аспирант НОУ ВПО «Российский новый университет».

упругости, рассматривает тела, которые по своей природе не проявляют свойств упругости либо с самого начала приложения к ним внешнего воздействия (пластическое тело), либо начиная с некоторой стадии такого воздействия (упругопластическое тело) [2]. Существенно, что после снятия с таких тел внешних воздействий они не возвращаются к своей исходной форме, т.е. в них сохраняется остаточная деформация.

Распространенными модельными задачами, отражающими наиболее характерные особенности деформирования и разрушения, являются плоские задачи теории упругости и пластичности, и в частности – задачи удара.

Ограниченность класса задач, к которым могут быть применены известные аналитические методы, обусловила целесообразность использования численных методов. К наиболее распространенным и эффективным методам расчета поставленной задачи удара относятся вариационно-сеточный метод конечных элементов (МКЭ) [3] и метод упругопластических течений НАМР [2], представляющий собой разновидность метода конечных разностей (МКР).

1. Достоинства и ограничения метода упругопластических течений НАМР

При реализации этого метода движение рассматривается в переменных Лагранжа [4] с построением сетки в декартовых координатах. Так как задача имеет только два измерения, то вид области сбоку представляет собой простой прямоугольник однородного поперечного сечения. Область, занятая средой, делится на четырехугольники сеткой *j-k*, которая движется вместе со средой (см. [1]).

Для расчета упругопластических течений необходимо задать уравнение состояния. Уравнение состояния должно описывать упругую, упругопластическую и гидродинамическую стадии движения. Для последних двух режимов движения должны быть сформулированы соответствующие критерии текучести.

Характеристики, представляющие интерес – это новые координаты узлов расчетной сетки. Их можно получить как в виде таблицы, так и в виде изображения деформированной области. Преимущество данного метода в том, что моделируется динамический процесс, а значит, можно исследовать разные ситуации: т.е. можно получить нужные характеристики в любой момент времени.

Одним из основных требований к программе с использованием метода НАМР является возможность вычисления давлений в деформируемой области и на основании этих данных – построение полей давления и деформаций, возникающих при взаимодействии с ударником.

При проведении расчетов начальная скорость ударника была задана равной 100 м/с (0,1 м/мс), что приблизительно соответствует штатной скорости пули травматического пистолета (энергия которой ≈ 85 Дж).

Основным вопросом при разработке и применении травматического оружия является вопрос, связанный с недопустимостью возникновения поражений внутренних органов. В реальных условиях такое поражение происходит при пробитии пулей наружных покровов.

Поэтому второе основное требование, предъявляемое к созданному нами приложению, использующему метод НАМР, состоит в получении наглядных представлений об уровнях нагрузок, действующих в биологических тканях при ударе, и тем самым косвенно судить о характере процесса. Естественно, что в качестве физико-механических свойств деформируемой преграды в программе были заданы параметры биологической ткани тела человека.

Основные параметры, используемые при моделировании, были заданы следующим образом: плотность $\rho = 1000$ кг/м^3, скорость звука $= 1600$ м/с, модуль объемного сжатия $K = \rho c_0^2 = 25,6 \cdot 10^8$Па [6].

Очевидно, что следует найти оптимальное значение размеров ячеек сетки, при которых суммарный объем модели гематомы, являющийся основной мерой интенсивности воздействия при ударе, будет изменяться незначительно с уменьшением размеров сетки.

Для этого были проведены количественные расчеты, а именно: строились расчетные сетки с различными параметрами величин ячеек, для определения зависимости распространения полей сжатий и растяжений, а также зависимости объемов гематомы от выбора параметров расчетной сетки.

На рис. 1 приведен график зависимости объема гематомы от размеров ячеек сетки. Очевидно, что на более крупных сетках оценки объемов оказываются достаточно грубыми, поскольку расчетный объем гематомы существенно зависит от размера ячеек. Было проведено восемь расчетов, и по их результатам была построена оптимальная сетка, наглядно демонстрирующая процессы распространения полей сжатия и растяжений (оптимальный размер ячеек расчетной сетки составил 0,5 мм (0,0005 м) при разбиении расчетной области сеткой 401 на 101) в диапазоне скоростей ударника 102–115 м/с (среднее значение 110 м/с). При уменьшении размеров сет-

ки эти объемы различались незначительно. Это подтверждает сходимость используемого метода НАМР, а значит, подтверждает обоснованность его использования.

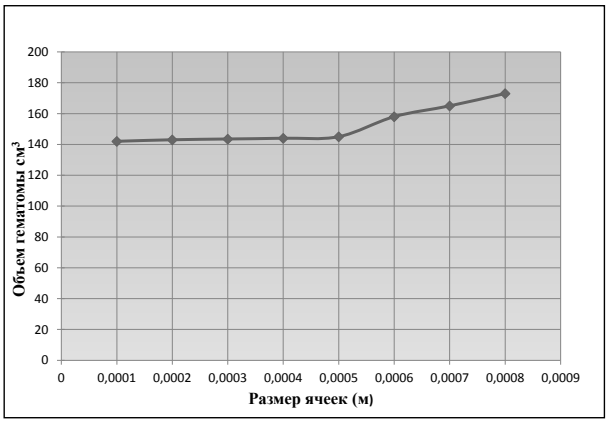


Рис. 1. Зависимость объема гематомы от размера ячеек сетки

Расчеты показывают, что до глубины 1,5 см происходит размозжение тканей, т.е. разрушение их клеточной структуры. На рис. 2 представлено изображение гематомы при достижении ее максимального значения, при котором радиус образовавшейся гематомы равен 3,65 см.

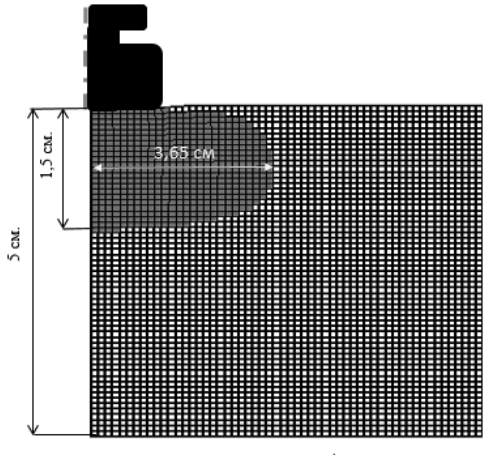


Рис. 2. Изображение гематомы при достижении ее максимального значения

На рис. 3 представлены графики зависимости объемов гематомы и откольной тарелки, полученные на сетке с оптимальным значением величины ячеек расчетной сетки 0,5 мм (0,0005 м) при среднем значении скорости удара 110 м/с.

Как видим, максимальный объем образовавшейся гематомы составил 140 см^3 при эффективном ее диаметре $D_{эфф}$ = 7,3 см (радиус 3,65 см · 2).

Однако отметим, что программа на основе лагранжевого подхода, который используется в методе упругопластических течений, при описании движения во время удара не может использоваться для расчета процесса проникания (пробития) из-за очень больших деформаций сетки. Следовательно, для моделирования задачи пробития твердого тела целесообразно рассмотреть возможности комбинирования разработанного алгоритма метода упругопластического течения с методом конечных элементов.

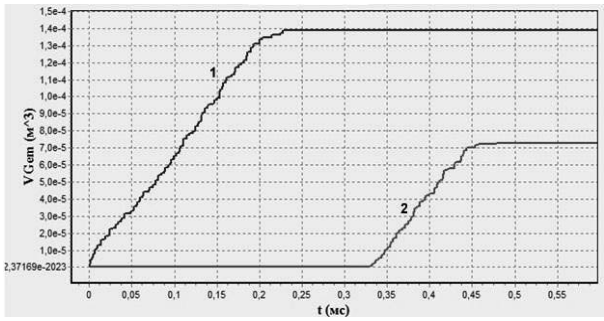


Рис. 3. Объемы гематомы (1) и откольной тарелки (2) при начальной скорости V = 110 м/с

2. Достоинства и ограничения метода конечных элементов

При использовании МКЭ для решения задач напряжённо-деформированного состояния твёрдого тела, оно представляется в виде совокупности конечных элементов (КЭ), связанных между собой в узловых точках [3].

Деформируемое тело (конструкция) разбивается на конечные элементы. Конечные элементы могут иметь различную форму и различные размеры. В результате разбиения создаётся сетка из границ элементов. Пересечения этих границ образуют узлы. Ансамбль из всех конечных элементов и узлов является основой конечно-элементной модели деформируемого тела. Выбор типа, формы и размера конечного элемента (КЭ) зависит от вида напряжённо-деформированного состояния, типа и формы, а также нагрузки исследуемого тела. На рис. 4 представлены основные типы КЭ.

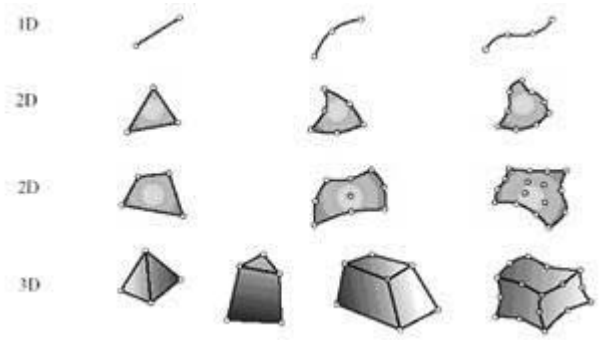


Рис. 4. Типы конечных элементов

Конечные элементы могут описываться одной, двумя или тремя пространственными координатами в зависимости от размерности задачи, для решения которой они предназначены. Соответствующее число внутренних или локальных координат называется собственной размерностью элемента. Плоский (двухмерный) КЭ в виде, например, треугольной или четырёхугольной пластины используется для моделирования плоского напряжённого или плоского деформированного состояния, что вполне подходит для моделирования нашей задачи.

Пример очень мелкого разбиения области на конечные элементы показан на рис. 5.

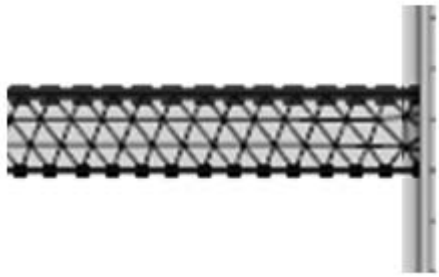


Рис. 5. Пример разбиения области на конечные элементы

Для конечных элементов, используемых в механических расчетах, определяющее соотношение задается с учетом поведения материала, из которого изготовлена конструкция. Например, в качестве такого соотношения во многих случаях используется обобщенный закон Гука, связывающий тензор деформаций и тензор напряжений в точке. На практике применяются три варианта МКЭ: в форме метода перемещений; в форме метода сил; в смешанной форме [3].

В настоящей работе рассматривается вариант МКЭ в форме метода перемещений. Это объясняется тем, что для заданной в такой форме конструкции легче получить основную систему метода перемещений, нежели статически определимую основную систему метода сил.

В алгоритме МКЭ используются общая (глобальная) система координат, привязанная ко всей конечно-элементной модели, и местные (локальные) системы координат, связанные с конкретными конечными элементами, поэтому их называют элементными системами координат. Переход от одной системы координат к другой производится с помощью матриц преобразования. Число степеней свободы одного узла зависит от типа задачи.

В основе математической формулировки МКЭ в форме метода перемещений лежит вариационный принцип Лагранжа, т.е. принцип минимума потенциальной энергии системы. Основными неизвестными здесь являются перемещения узловых точек дискретной схемы, а напряжения определяются путем численного дифференцирования перемещений. При этом напряжённо-деформированное состояние i-го элемента однозначно определяется через вектор-столбец узловых параметров (полиномиальные коэффициенты):

$$\{\alpha^i\} = \begin{Bmatrix} \alpha_1^i \\ \alpha_2^i \\ \vdots \\ \alpha_r^i \end{Bmatrix}. \qquad (1)$$

С его помощью выражается вектор-столбец узловых перемещений:

$$\{q^i\} = [A^i]\{\alpha^i\}. \qquad (2)$$

Здесь r – число узловых неизвестных для i-го конечного элемента, которое равно числу его степеней свободы. Для двухмерного треугольного конечного элемента $r = 6$ (по две степени свободы на каждый из трех узлов).

Связь между смежными конечными элементами вызывает в узловых точках i-го элемента реактивные усилия взаимодействия, и каждый из конечных элементов оказывается загруженным этими усилиями:

$$\{F^i\} = \begin{Bmatrix} F_1^i \\ F_2^i \\ \vdots \\ F_r^i \end{Bmatrix}. \qquad (3)$$

Заданные внешние нагрузки, действующие на каждый конечный i-й элемент, заменяются приложенными в узлах сосредоточенными силами, статистически эквивалентными по своему действию фактической нагрузке. Эти силы включаются в качестве соответствующих добавок в вектор $\{F^i\}$ и учитываются при составлении уравнений равновесия в узлах.

Вектор-столбец узловых нагрузок (вектор усилий) $\{F^i\}$ также однозначно определяет напряжённо-деформированное состояние i-го элемента.

Между векторами $\{F^i\}$ и $\{q^i\}$ существует следующая связь:

$$\{F^i\} = [K^i]\{q^i\}, \qquad (4)$$

где $[K^i]$ – матрица жёсткости, определяющая упругие свойства i-го элемента.

Поскольку не наложено каких-либо ограничений, касающихся формы конечного элемента, выражение для матрицы жёсткости $[K^i]$ можно

применять для конечных элементов произвольной формы. Матрица $[K^i]$ является квадратной, и её порядок будет равняться числу степеней свободы рассматриваемого элемента.

Располагая значением матрицы жёсткости для каждого из конечных элементов, можно составить общую (глобальную) матрицу жёсткости $[K]$ в общей системе координат, которая устанавливает связь между узловыми перемещениями дискретной модели $\{q\}$ и внешней нагрузкой исходной конструкции $\{F\}$:

$$[K]\{q\} = \{F\}. \quad (5)$$

Это основное разрешающее матричное уравнение в общей системе координат [4]. Отметим, что для сложных конструкций возникают определённые трудности при выборе подходящей сетки разбиения из имеющегося разнообразия вариантов.

Критерии устойчивости, сходимости и точности в основном определяются погрешностями операций, проводимых в рамках МКЭ. Наряду с обычными ошибками округления и погрешностью приближенных методов линейной алгебры, применяемых в МКЭ, есть и ошибки, обусловленные самой концепцией метода. В первую очередь речь идет о зависимости результатов расчета от выбора (построения) сетки конечных элементов. Кроме того, следует иметь в виду и трудность оценки точности получаемых результатов. Ошибки дискретизации уменьшаются с увеличением числа конечных элементов и соответственно с уменьшением их размеров, причем они стремятся к нулю, когда размер элемента стремится к нулю. Ошибки аппроксимации не обязательно уменьшаются по мере уменьшения размеров элементов или повышения степени аппроксимации, поэтому могут ухудшать сходимость к точному решению или даже приводить к расходимости с ним.

Заключение

Сравнительный анализ рассмотренных методов позволяет сделать следующие выводы. Если расчетные области имеют правильную форму и позволяют построить разностную сетку, то на первый план выдвигаются преимущества метода конечных разностей (МКР). Однако если геометрические формы оказываются сложными, преимуществом будет обладать метод конечных элементов (МКЭ) в силу своей независимости от геометрии задачи. Достоинства этого метода проявляются в представлении геометрии задачи, построения сетки и определения граничных условий, а также при оценке и интерпретации результатов.

В свою очередь, использование методологии конечных разностей в варианте метода упругопластических течений НАМР позволяет, в отличие от метода конечных элементов (МКЭ), решать динамическую задачу, в частности – исследовать состояние моделируемой области в разные моменты времени.

Таким образом, могут быть сформированы критерии применимости метода НАМР и сделаны выводы о возможности дополнения существующего алгоритма метода упругопластического течения методом конечных элементов для полноценного моделирования задачи пробития твердого тела.

Литература

1. Клименко И.С., Холодков С.В. Распределение полей давления и деформаций, возникающих при ударе твердого тела о деформируемую преграду // Вестник Российского нового университета, 2014. – Вып. 4. – С. 49–54.

2. Уилкинс М.Л. Расчет упругопластических течений / М.Л. Уилкинс // Вычислительные методы в гидродинамике. – М. : Мир, 1967. – 383 с.

3. Зенкевич О.С. Метод конечных элементов в технике. – М. : Мир, 1975. – 541 с.

4. Бахвалов Н.С. Численные методы / Н.С. Бахвалов. – М. : БИНОМ, 2008. – 636 с.

5. Колпаков В.И., Охитин В.Н., Прикладная механика сплошных сред : в 3 т. / науч. ред. В.В. Селиванов // Численные методы в задачах физики взрыва и удара. – М. : Изд-во МГТУ им. Н.Э. Баумана, 2000. – 516 с.

6. Применение ультразвука в медицине. Физические основы / под ред. К. Хилла. – М. : Мир, 1989. – 282 с.

Управление сложными системами

УДК 519.81

И.С. Клименко[1]
М.А. Плуталов[2]
Г.А. Чеботарев[3]

К ВОПРОСУ ОБ ОЦЕНИВАНИИ ОПТИМИЗМА КРИТЕРИЕВ ВЫБОРА СТРАТЕГИЙ В «ИГРЕ С ПРИРОДОЙ»

Проведено исследование причин совпадения результатов выбора стратегий на основе применения различных классических критериев. На большой выборке матриц полезности выявлены аномалии зависимости коэффициентов взаимной корреляции пар критериев от выбора степени оптимизма. Выдвинута и подтверждена гипотеза, объясняющая причину таких аномалий.

Ключевые слова: *стратегия, решение, критерии, альтернатива, матрица, корреляция, оптимизм.*

I.S. Klimenko
M.A. Plutalov
G.A. Chebotarev

TO THE EVALUATION OF OPTIMISM CRITERIONS FOR SELECTION OF STRATEGIES IN THE "GAME WITH NATURE"

The research of coincidence results of strategies selection on the base of various classical criterions is used. On the big extract of utility matrix, the anomaly of cross-correlations coefficients dependence from optimism degree choice is detected. A hypothesis, which explains a cause of such anomaly is proposed and confirmed.

Keywords: *strategy, solution, criteria, alternative, matrix, optimism.*

Введение

В работе [1] нами был проведен сравнительный анализ основных критериев выбора стратегий в условиях статистической неопределенности. Коэффициенты взаимной корреляции пар критериев были получены в результате обобщения результатов анализа 50 матриц псевдослучайных чисел, распределенных по нормальному закону с размерностью 6 × 6 (6 состояний обстановки и 6 альтернативных решений).

В результате ранжирования по степени оптимизма критериев Вальда, Сэвиджа, Лапласа, максимакса и Гурвица [2–7] при дискретных значениях коэффициента оптимизма последнего было установлено отношение нестрогого порядка между указанными критериями, в соответствии с которым может быть построена неоднородная порядковая шкала для априорного выбора ЛПР степени оптимизма стратегии.

При этом было установлено, что для принятых условий критерий Сэвиджа (сформированный на матрице риска) отражает существенно больший оптимизм потенциального ЛПР, чем критерий Вальда. Также было показано, что критерий Лапласа в большей степени, чем остальные, тяготеет по степени своего оптимизма к критерию максимакса. Существенный результат [1] состоит в том, что критерий Гурвица проявляет малую чувствительность к вариациям

[1] Доктор физико-математических наук, профессор, профессор кафедры информационных систем в экономике и управлении НОУ ВПО «Российский новый университет».

[2] Аспирант НОУ ВПО «Российский новый университет».

[3] Аспирант НОУ ВПО «Российский новый университет».

своего коэффициента оптимизма, ограничивая в большинстве случаев выбор решений двумя крайними альтернативами.

Тем не менее, критерий Гурвица позволяет ввести интервальную шкалу оптимизма. Представляется целесообразным «привязать» все рассматриваемые критерии к шкале оптимизма критерия Гурвица, построив зависимость степени взаимной (парной) корреляции каждого из них с критерием Гурвица.

С целью получения точных результатов была разработана программа, позволившая автоматически вычислять коэффициенты взаимной корреляции пар критериев по совпадению результатов выбора решений для выборки из 10 000 таких матриц.

1. Анализ результатов, полученных на большой выборке

В ходе выполнения программы для каждой матрицы фиксировалось относительное число совпадений результатов выбора решений по исследуемому критерию и по критерию Гурвица для каждого значения коэффициента оптимизма последнего (диапазон [0; 1] с шагом 0,1). Тем самым устанавливались значения коэффициентов парной корреляции каждого критерия с критерием Гурвица λ_{nH}. Далее строились графики зависимости значений этих коэффициентов (λ_{VH}, λ_{SH}, λ_{LH}, и λ_{MH}) от значений коэффициента оптимизма α.

На рис. 1 и 2 приведены совмещенные графики для близких по степени оптимизма пар критериев.

Из анализа рис. 1 следует, что при значениях α в интервале [0; 0,5] коэффициент взаимной корреляции λ_{SH} изменяется весьма незначительно (в пределах 5%). Напротив, при значениях α в интервале [0,5; 1] ход графика приобретает

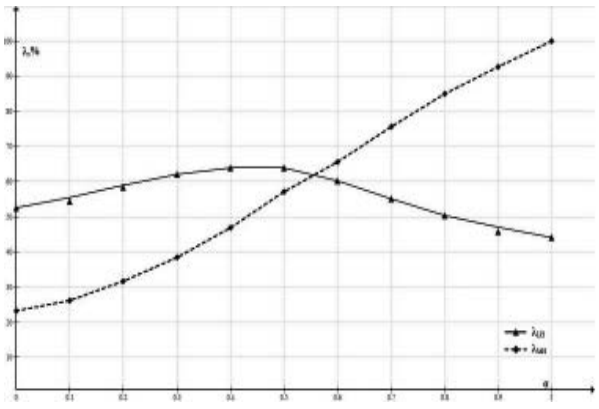


Рис. 2. Графики зависимости коэффициентов взаимной корреляции λ_{LH} и λ_{MH} от коэффициента оптимизма α

направление, характерное для зависимости λ_{VH} от α. При $\alpha = 0{,}6$ графики пересекаются, и далее кривая λ_{SH} качественно сопровождает график λ_{VH}.

Здесь следует обратить внимание на следующий факт: можно было ожидать, что, согласно теоретической интерпретации семантики критерия Вальда (как предельно осторожного критерия), график зависимости λ_{VH} от α при $\alpha = 1$ должен достичь оси абсцисс. Однако этого не происходит: при $\alpha = 0{,}7$ график уходит выше ожидаемого направления, и при $\alpha = 1$ получаем $\lambda_{VH} \approx 0{,}2$.

Из анализа рис. 2 следует, что график зависимости λ_{LH} от α при малых значениях коэффициента оптимизма (в интервале [0; 0,5]) качественно следует за ходом зависимости λ_{MH} от α, но, начиная с $\alpha = 0{,}6$, графики расходятся, и значение коэффициента λ_{MH} устремляется к своему теоретическому значению, равному единице. Однако и здесь мы сталкиваемся с отклонением хода зависимости λ_{MH} (α) от теоретического значения, равного нулю при $\alpha = 0$.

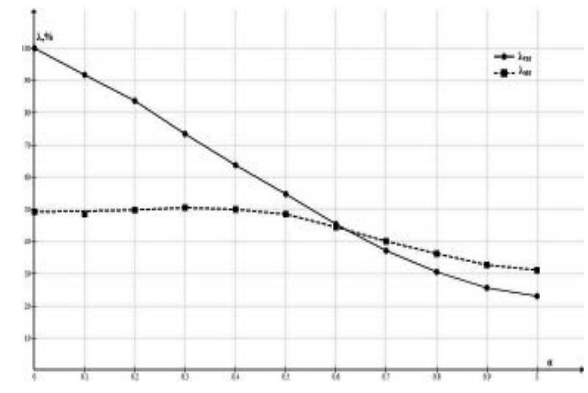


Рис. 1. Графики зависимости коэффициентов взаимной корреляции λ_{VH} и λ_{SH} от коэффициента оптимизма α

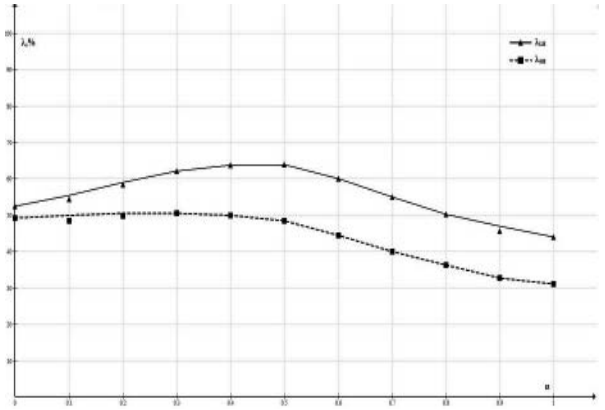


Рис. 3. Графики зависимости коэффициентов взаимной корреляции критериев λ_{LH} и λ_{SH} от коэффициента оптимизма α

Что же касается графика $\lambda_{LH}(\alpha)$, то по своему характеру он оказывается весьма близким к аналогичному графику для $\lambda_{SH}(\alpha)$, что свидетельствует о значительной степени эквивалентности критериев Сэвиджа и Лапласа, притом что степень их парной корреляции с критерием Гурвица достаточно слабо зависит от значения оптимизма последнего (см. рис. 3).

Таким образом, можно сделать вывод о том, что критерий Лапласа, хотя и более оптимистичен, чем критерий Сэвиджа, все же не может быть отнесен к критериям с высокой степенью оптимизма, а характерным для него является относительно небольшой перепад значений λ_{LH} во всем диапазоне α.

2. Анализ причин отклонения статистических зависимостей от характера, предсказываемого теорией

Очевидно, что выяснение причин аномального с точки зрения теории хода графиков для критериев Вальда и максимакса следует проводить на основе анализа структуры конкретных матриц. Основная гипотеза, направленная на объяснение этого феномена, была сгенерирована, исходя из обнаруженного в нашей работе [1] явления полного совпадения результатов выбора решения по всем критериям, наблюдаемого примерно для 10% матриц.

Прежде всего необходимо было убедиться в том, что особенности хода графиков, выявленные для большой выборки матриц, проявляются и на ограниченной выборке из 50 матриц. При этом появляется возможность проанализировать каждую из матриц с целью выявления причин наблюдаемого феномена.

С этой целью на 50 матрицах были рассчитаны вручную коэффициенты парной корреляции

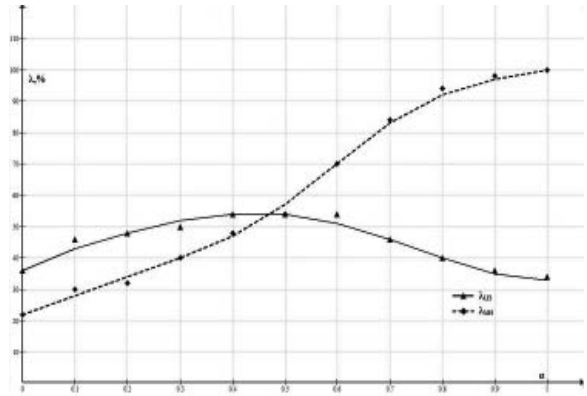


Рис. 5. Графики зависимости коэффициентов взаимной корреляции λ_{LH} и λ_{MH} от коэффициента оптимизма α (ограниченная выборка из 50 матриц)

λ_{VH}, λ_{SH}, λ_{LH}, и λ_{MH} и построены зависимости, аналогичные приведенным на рис. 1 и 2.

На рис. 4 и 5 приведены совмещенные графики для близких по оптимизму пар критериев, полученные на этой выборке.

Нетрудно убедиться, что обсуждаемые закономерности и в этом случае проявляются в полной мере. Подчеркнем, что уклонение графиков, построенных для λ_{VH} и λ_{MH}, от оси абсцисс, и здесь носит очевидный характер. Из сравнения следует также, что графики λ_{SH} и λ_{LH} качественно близки (см. рис. 6), хотя, в отличие от рис. 3, в случае ограниченной выборки имеет место пересечение графиков.

Необходимо отметить, что качественный характер закономерностей для большой (10 000 матриц) и ограниченной (50 матриц) выборки в значительной степени совпадает. Следовательно, можно считать случайную выборку из 50 матриц репрезентативной, по крайней мере, для получения оперативных оценок.

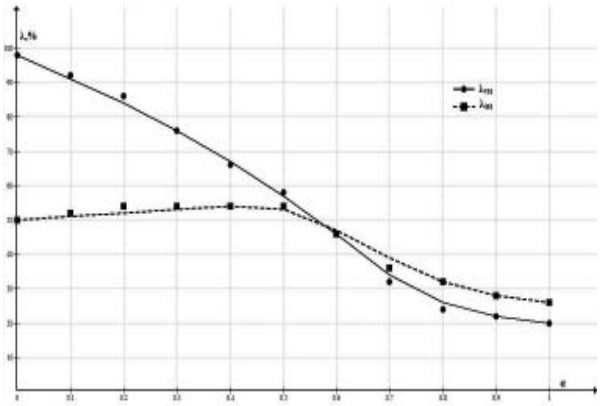


Рис. 4. Графики зависимости коэффициентов взаимной корреляции λ_{VH} и λ_{SH} от коэффициента оптимизма α (ограниченная выборка из 50 матриц)

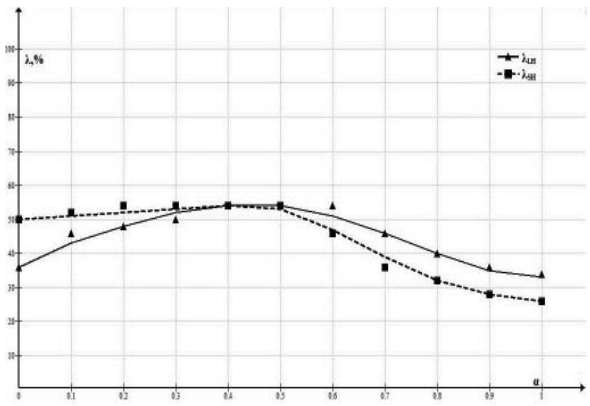


Рис. 6. Графики зависимости коэффициентов взаимной корреляции λ_{LH} и λ_{SH} от коэффициента оптимизма α (ограниченная выборка из 50 матриц)

Как показано в [1], среди этих 50 матриц было обнаружено несколько аномальных в том смысле, что для них результаты выбора альтернатив по критериям Вальда и максимакса совпадают, притом что остальные критерии рекомендуют выбор других альтернатив. Это обстоятельство мы сочли необходимым учесть при проверке выдвинутой гипотезы.

Таким образом, для решающей проверки гипотезы из рассматриваемой выборки были исключены, во-первых, пять матриц, для которых всеми критериями рекомендуется одна и та же альтернатива. Как показано в [1], такие матрицы отражают реальный случай эквивалентности всех критериев при выборе объективно наилучшей альтернативы. Кроме того, во-вторых, из рассмотрения были исключены шесть матриц, для которых характерно аномальное совпадение результатов выбора по взаимоисключающим критериям Вальда и максимакса.

Для новой выборки из 39 матриц вновь вручную были рассчитаны коэффициенты λ_{VH}, λ_{SH}, λ_{LH} и λ_{MH} и построены зависимости, аналогичные прежним (рис. 7 и 8).

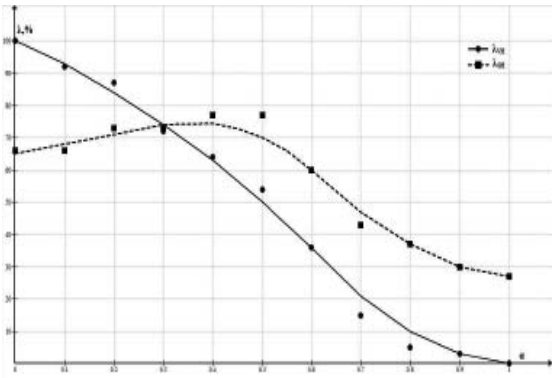


Рис. 7. Графики зависимости коэффициентов взаимной корреляции λ_{VH} и λ_{SH} от коэффициента оптимизма α (ограниченная выборка из 39 матриц)

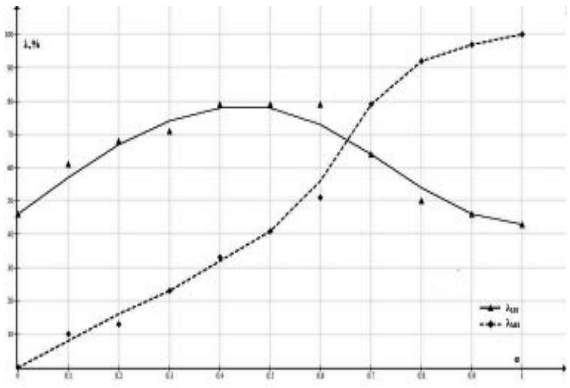


Рис. 8. Графики зависимости коэффициентов взаимной корреляции λ_{LH} и λ_{MH} от коэффициента оптимизма α (ограниченная выборка из 39 матриц)

Нетрудно убедиться, что для такой выборки зависимости коэффициентов корреляции критериев Вальда и максимакса с критерием Гурвица отвечают их семантике: как и ожидалось, при $\alpha = 0$ $\lambda_{VH} = 1$, а $\lambda_{MH} = 0$ и, напротив, при $\alpha = 1$ $\lambda_{VH} = 0$, а $\lambda_{MH} = 1$.

Тем самым получила подтверждение гипотеза относительно причины обнаруженных особенностей зависимостей коэффициентов взаимной корреляции λ_{VH} и λ_{MH} от коэффициента оптимизма критерия Гурвица, которому в настоящей работе была отведена роль базового.

На рис. 9 приведены совмещенные графики зависимости коэффициентов взаимной корреляции λ_{LH} и λ_{SH} от коэффициента α.

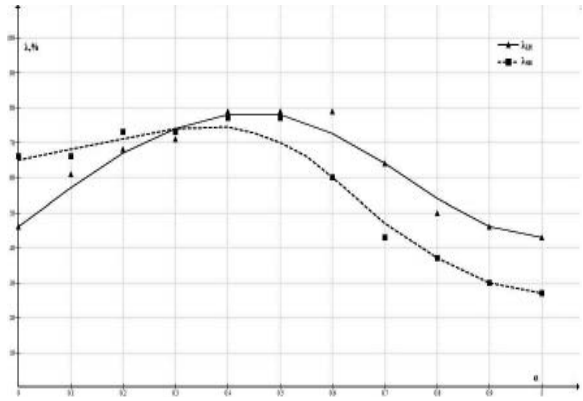


Рис. 9. Графики зависимости коэффициентов взаимной корреляции λ_{LH} и λ_{SH} от коэффициента оптимизма α (ограниченная выборка из 39 матриц)

Сравнение рис. 9 с рис. 6 показывает некоторое их различие, однако общий характер зависимости практически совпадает. Таким образом, в ходе подтверждения гипотезы была также выявлена и подтверждена существенная близость семантики критериев Лапласа (рассчитываемого на матрице эффективности) и Сэвиджа (рассчитываемого на матрице риска).

Заключение

Исследование результатов выбора решений (стратегий) по различным критериям на выборке из 10 000 матриц полезности показало, что теоретическое соотношение степени оптимизма критериев Вальда, Гурвица и максимакса нарушается примерно в 20 процентах случаев.

Для объяснения этого феномена была задействована выборка из 50 известных матриц, что позволило, с одной стороны, убедиться в ее репрезентативности, а с другой – проверить выдвинутую гипотезу относительно природы обнаруженной аномалии.

Установлено, что исключение из рассмотре-

ния матриц двух типов, для которых совпадают результаты выбора по критериям Вальда и максимакса, позволяет обеспечить выполнение теоретического соотношения оптимизма названных критериев.

Обнаружена семантическая близость критерия Лапласа с критерием Сэвиджа, что свидетельствует о необходимости поиска и формирования нового критерия, обладающего более высокой степенью оптимизма по сравнению с этими критериями.

Литература

1. Клименко И.С., Плуталов М.А., Чеботарев Г.А. Сравнительный анализ критериев выбора стратегий в «игре с природой» // Вестник Российского нового университета. – 2015. Сер. Сложные системы: модели, анализ и управление. – Вып. 1. – С. 55–59.

2. Vald, A. Contribution of the theory of statistical estimation and testing hypothesis // Annuals Math. Statist. – 1939. – Vol. 10. – P. 299–326.

3. Savage, L.J. The foundation of statistics. – N.Y. : Wiley, 1954.

4. Гермейер Ю.Б. Игры с непротивоположными интересами. – М. : Наука, 1978. – 328 с.

5. Бродецкий Г.Л. Системный анализ в логистике. Выбор в условиях неопределенности. – М. : Academia, 2010. – 336 с.

6. Клименко И.С. Теория систем и системный анализ: учебное пособие. – М. : РосНОУ, 2014. – 264 с.

7. Жуковский В.И., Солдатова Н.Г. Гарантированные риски и исходы в «игре с природой» // Проблемы управления. – 2014. – № 1. – С. 14–26.

УДК 681.5.08

А.И. Гладышев[1]

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ СЕГОДНЯ

В статье приводятся показатели развития инфокоммуникационных технологий, формулируются задачи оптимизации криптографической защиты информации в условиях сверхпроводящей и агрессивной информационной среды.

Ключевые слова: *безопасность информации, проблемы обеспечения безопасности информации, защита данных.*

A.I. Gladyshev

PROBLEMS OF ENSURING INFORMATION SECURITY TODAY

The article presents the indicators of ICT development and formulates the optimization problem of cryptographic protection of information in terms of superconducting and aggressive information environment.

Keywords: *information security, problems of ensuring information security, data protection.*

Причина неожиданных и неприятных явлений, как обычно, в том, что количество медленно и подло переходит в качество. Мегацель компьютерной индустрии – «информационная сверхпроводимость» в той самой цифровой вселенной: бесконечная память, бесконечная производительность, бесконечная скорость передачи информации.

Возможности любой информационной системы определяются в трех измерениях: производительность вычислений, память, коммуникативность.

До середины 1990-х годов совершенно отдельной отраслью были суперкомпьютеры и процессоры для них. Но массовость производства (с неизбежной дешевизной) «обычных» микропроцессоров привели к их проникновению в область суперкомпьютеров. С переходом на многоядерную архитектуру микропроцессоры превратились в «суперкомпьютеры на чипе». Если 1 Гфлопс в 1997 году стоил 96,4 тыс. долл. (суперкомпьютер IBM ASCI Red), то в 2008 году этот показатель составляет всего 15 долл. (суперкомпьютер Cray CX-1). Желающие получить представление о том, что такое современные суперкомпьютеры, могут обратиться к рейтингу Top500, который составляется два раза в год (www.top500.org, российский аналог – www.top50.ru).

Память и коммуникативность. Аналогично закон Мура действует и на снижение стоимости памяти как оперативной, так и энергонезависимой. Собственно Гордон Мур говорил вообще о микросхемах: их миниатюризация одинаково влияет и на память, и на производительность, и даже на коммуникативность – ведь везде мы имеем дело с одной и той же микроэлектронной базой. «Информационная сверхпроводимость» наблюдается и в коммуникативности, причем в глобальном диапазоне – от системных шин и локальных сетей до Интернета [3; 5].

Наиболее частая угроза информационной безопасности – кража информации. И здесь злоумышленников прежде всего интересует развитие сверхпроводимости в аспекте «память», в меньшей степени – коммуникативность. Все же переписать информацию на носитель и унести намного быстрее и безопаснее, чем «прокачать». Тут достаточно привести только российскую статистику крупных краж информации с последующим распространением на пиратском рынке.

На каждую крупную базу – сотни и тысячи баз данных клиентов, операций и т.д., которые уносятся сотрудниками фирм при уходе с работы или просто на всякий случай (по данным Ponemon Institute 59% сотрудников хотя бы раз уносили с работы конфиденциальные данные).

[1] Кандидат технических наук, доцент, доцент кафедры ИТиЕНД НОУ ВПО «Российский новый университет».

Воспрепятствовать этому технически очень трудно. На 4-гигабайтную флэшку можно записать абсолютно все, если речь идет не о голливудском фильме, а о «настоящей» информации [1; 2]. И такие случаи остаются либо неизвестными, либо, по понятным причинам, не выносятся за пределы компаний. О том, что становится известным, можно прочитать, например, на сайте отечественной компании InfoWatch.

Об отрицательном влиянии на информационную безопасность другого аспекта – коммуникативности – можно говорить много. Наиболее очевидные угрозы видны на примере Интернета, который стал благодатной средой сразу для целого букета угроз: это и распространение вирусов, и рассылка спама, и хакерские атаки. Причем за последние 5 лет, как отмечают аналитики, эти направления прочно слились и коммерциализовались. Например, создаются вирусы, которые впоследствии выстраивают так называемые зомби-сети для удаленных атак и рассылки спама, и все это ради банальной прибыли – only business. Эпоха романтиков-студентов вроде Роберта Морриса, создающих вирусы из любопытства и желания самоутверждения, канула в Лету.

Второй, менее очевидный побочный эффект – дешевые коммуникации – открыли возможности создания высокопроизводительных систем из любых устройств, разве что не из микрокалькуляторов. При чем здесь суперкомпьютеры и информационная безопасность? [2]. Некоторые задачи взлома систем защиты (подбор ключа или прообраза для хэш-функции) обладают свойством практически абсолютной распараллеливаемости, то есть разбиении задачи на независимые подзадачи, которые могут решаться одновременно на разных вычислительных устройствах. При высокой скорости соединений между вычислительными модулями (будь то системная шина, локальная сеть или Интернет) возникает возможность создания дешевых метакомпьютеров – кластеров, линейно объединяющих производительности отдельных микропроцессоров или компьютеров. Пока мы не говорили о роли аспекта коммуникативности в информационной безопасности. Самое время сказать и о нем, и о синергетическом эффекте одновременного роста производительности, памяти и коммуникативности.

В сверхпроводящей и агрессивной информационной среде оказываются методы криптографической защиты информации, которые попрежнему считаются самым надежным звеном в сложных цепях систем защиты информации [1].

Для большинства криптографических систем математически строго доказывается стойкость. Например, если алгоритм шифрования не имеет врожденных изъянов, то нетрудно подсчитать, сколько ключей потребуется злоумышленнику перебрать, чтобы найти правильный, и сколько на это потребуется времени. В современных шифрах длина ключа составляет 128–256 бит (американский стандарт DES и отечественный ГОСТ 28147-89), и принято считать, что запас прочности здесь огромный [2].

Но те методы защиты информации, которые сегодня считаются надежными, завтра могут оказаться прозрачными для злоумышленников. По мнению авторов статьи, ситуация усугубляется тем, что из-за возможности взаимного дополнения производительности, памяти и коммуникативности возникает эффект «закона Мура в кубе». Имея увеличение характеристик по трем направлениям в соответствии с законом Мура, можно говорить о том, что возможности криптоанализа увеличиваются в 8–10 раз каждые 1,5 года, то есть каждые полтора года прочность криптографического ключа «съедается» на 3-4 двоичных разряда ежегодно. Это наглядно демонстрируют конкурсы, которые проводит среди добровольцев фирма RSA Data Security (США) по взлому распространенных криптосистем (в качестве стимула выступает денежная премия). Так, в 1977 г. авторы криптосистемы RSA опубликовали 129-значное десятичное число, предположив, что на факторизацию (открывающую путь к взлому системы) уйдет несколько миллионов лет, однако решение было найдено уже в 1994 г. В 1999 г. на интернет-кластерах из компьютеров добровольцев были разложены числа в 140 и 155 десятичных разрядов, в 2006 г. – 220. Характерны и итоги конкурса по взлому шифра DES (поиск 56-разрядного ключа): в 1997 г. шифр был взломан за 96 суток (DESCHALL Project: распределенная сеть из компьютеров добровольцев, число узлов до 78 тыс.), в 1999 г. – меньше чем за сутки (специализированный компьютер EFF Deep Crack стоимостью 250 тыс. долл.), в 2006 г. практически тот же результат был показан на специализированном компьютере COPACOBANA, который стоил всего 10 тыс. долл. Создатели стандарта DES (1977 г.) рассчитывали, что запаса прочности хватит на 25 лет, однако уже в 1998 г. была в срочном порядке развернута работа по выработке нового стандарта AES (принят в 2001 г.) [8].

Это все иллюстрирует взаимодополнение в аспекте «производительность – коммуникативность». О балансе «память – производительность» слышал каждый, кто хоть немного инте-

ресовался криптографией. Скромный вычислительный ресурс в ряде задач можно компенсировать огромной памятью. Существуют, например, несколько сайтов, которые предлагают быстрый взлом хэш-образов паролей на основе так называемых радужных таблиц. Если кратко – то, рассчитав и правильно разместив в памяти хэш-образы для большого количества паролей (в первую очередь часто используемых), можно практически мгновенно находить искомый пароль, хотя на «честный» даже на мощном компьютере на это ушло бы несколько часов или дней. Наиболее известный из таких проектов – RainbowCrack.com, который наработал уже более 1 Тб таблиц [7].

Стоит ли сгущать краски и отказаться от прогресса ради безопасности? Конечно, нет. Тем более что сам прогресс неизбежен. Правильным представляется использование современных информационных технологий не только для работы с информацией, но и для ее защиты. Правда, здесь угрозы информационной безопасности можно разделить на те, в которых прогресс создает равные шансы для защиты и нападения и те, в которых прогресс всё же больше играет на руку злоумышленникам [5].

Например, использование сверхъемких устройств хранения информации трудно предотвратить технологически, хотя в корпоративных системах защиты информации можно использовать «теневое копирование» – то есть запись всего, что записывается на внешние носители или передается через Интернет. А вот в задачах криптографии прогресс играет скорее на руку тем, кто зашифровывает информацию, чем тем, кто пытается прочитать ее без знания ключа [3]. Увеличение длины ключа всего на 1 бит, увеличивает объем работы по перебору ключей в два раза. Другое дело, что если речь идет о принятии каких-то стандартов, то их трудно менять слишком часто – вспомним, что стандарт DES поменяли на AES практически «на последней минуте матча».

Эффект «закона Мура в кубе» означает необходимость перехода к существенно большей длине ключа в криптографических системах. Речь может идти даже о возвращении в соответствии с законом диалектики к истокам научной криптографии, когда К. Шенноном было доказано, что идеальную криптостойкость дает система одноразового шифрования. На практике это означает, например, использование ключей длиной в несколько мегабит в режиме сложения по модулю 2 (гаммирования) с защищаемыми данными, при котором достигается одновременно и высокая стойкость шифрования, и предельная скорость шифрования. Это лишь одно решение, которое лежит на поверхности. Проблема защиты информации в условиях «информационной сверхпроводимости» безусловно приведет в практическую плоскость и более сложные решения – например квантовые каналы, по крайней мере теоретически обещающие идеальную криптостойкость [6].

Одним словом, восхищаясь технологическим прогрессом, не стоит забывать о том, что им так же восхищаются и те, кто стоит по другую сторону информационных баррикад [4].

Все вышесказанное относится только к развитию вычислительной техники в рамках существующих технологий (микро-), однако переход к нанокомпьютерам, квантовым устройствам может означать скачкообразное увеличение информационной сверхпроводимости. Нанокомпьютеры обещают сразу на несколько порядков увеличить емкость памяти и производительность микропроцессоров (за счет создания большого числа ядер). Впрочем, в долгосрочной перспективе возможно это уложится в закон Мура. В отличие от нанокомпьютеров, где изменения хотя и серьезные, но все-таки чисто количественные, квантовые компьютеры обещают, например, быстрое решение задачи факторизации больших чисел (разложение на множители больших чисел), что сделает тривиальной задачу взлома асимметричных шифров, на которых держатся, например, все защищенные интернет-технологии. Кстати, один из создателей асимметричного шифра RSA Леонард Адельман еще 15 лет назад увлекся идеей биокомпьютеров (построенных на ДНК) и показал, что они намного быстрее могут решать некоторые задачи, чем обычные компьютеры.

Наконец стоит сказать и об одной технологии уже сегодняшнего дня – виртуализации вычислений. О виртуализации говорят сейчас много, один из модных терминов – «облако вычислений», создание единой среды из разрозненных компьютеров, часть из которых обычно простаивает, в то время как другая работает с перенапряжением. В 2008 г. появилась новость, которая на первый взгляд никакого отношения к защите информации не имеет. Открылся web-сервис Amazon Elastic Computing Cloud (EC2), в рамках которого есть возможность приобретать машинное время такого виртуального компьютера. Ориентировочная стоимость сервиса – 10 центов за один час аренды среднестатистического ПК. Расчеты показывают, что для подбора 56-разрядного ключа потребуется около 2 млн долларов

и 200 часов. Конечно, это пока дорого, но ведь речь идет только о зарождении такого мощного направления, как виртуализация вычислений, способная на несколько порядков удешевить всю ту же стоимость 1 гигафлопса.

Литература

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М. : Радио и связь, 1999.

2. ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. – М., 1995.

3. ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования. – М., 1995.

4. ГОСТ Р 34.10-2001 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М., 2001.

5. Гладышев А.И. Разработка имитационной модели вирусной эпидемии на основе модели биологических вирусов: принципы, основные параметры, описание и зависимости // Вестник Российского нового университета. – 2012. – Выпуск 4. Управление, вычислительная техника и информатика. – С. 17–21.

6. Гладышев А.И., Жуков А.О. Использование в автоматизированной системе контроля полномочий биометрической идентификации // Вестник Российского нового университета. – 2013. – Выпуск 4. Управление, вычислительная техника и информатика. – С. 95–99.

7. Гладышев А.И. Удобство и безопасность компьютерных систем. В чем противоречие? // Вестник Российского нового университета. – 2012. – Выпуск 4. Управление, вычислительная техника и информатика. – С. 89–93.

8. Гладышев А.И., Жуков А.О. Достоинства и недостатки имитационного моделирования с использованием нейронных сетей // Вестник Российского нового университета. – 2013. – Выпуск 4. Управление, вычислительная техника и информатика. – С. 53–56.

УДК 658.5

Л.А. Бурцева[1]
О.В. Золотарев[2]

ИССЛЕДОВАНИЕ И АНАЛИЗ ИНФОРМАЦИОННО-ЛОГИСТИЧЕСКИХ ПРОЦЕССОВ КОМПАНИИ ПО ОПТОВЫМ ПОСТАВКАМ ЧАЯ

В статье был проведен анализ объемов реализации продукции, выраженный в рублях, на примере одной из компаний города Москвы, занимающейся оптовыми продажами чая, для которой была выполнена оценка внутригодовой динамики, определены основные методы сглаживания скачкообразного спада продаж. В ходе данного исследования были рассмотрены и выявлены внутригодовые изменения сезонных колебаний в объемах товарооборота компании. Построены диаграммы, которые служат инструментом анализа процессов с внутригодовой динамикой и применяются при прогнозировании сезонных процессов.

Ключевые слова: *процессный подход, периодические колебания, внутригодовой спрос, скачкообразное снижение прибыли.*

L.A. Burtseva
O.V. Zolotarev

RESEARCH AND ANALYSIS OF INFORMATION AND LOGISTICS PROCESSES OF THE WHOLESALE SUPPLY TEA COMPANY

The article analyses the amount of sales, expressed in roubles, by the example of one of the Moscow companies, engaged in wholesales of tea, which was evaluated intraannual dynamics, basic methods of smoothing abrupt downturn in sales. In the course of this study were reviewed and identified annual changes in seasonal fluctuations in the volume of trade of the company. The charts that serve as a tool of processes analysis of intraannual dynamics and applied in forecasting seasonal processes were built.

Keywords: *process approach, periodic fluctuations, annual demand, abrupt decrease in profit.*

Цель работы – выявление динамики спроса на продукцию, продаваемую компанией.

Под сезонностью обычно понимают периодические изменения спроса в зависимости от различных факторов, чаще всего – от времени года (зима, весна, лето, осень). От сезонных колебаний продаж зависит процесс планирования и прогнозирования продаж. Обычно цикл сезонности составляет один год, однако колебания спроса могут наблюдаться и в течение недели, и в течение одного дня. Но, как правило, такие колебания спроса не рассматривают как сезонные. Такие колебания не требуют специальных мероприятий по их выравниванию, необходимо лишь принимать во внимание эти особенности деятельности организации и учитывать их при планировании продаж.

В сезонности можно выделить два типа, такие, как:

– сезонность производства;

– сезонность потребления.

Если сравнивать эти типы сезонности, то очевидно, что сезонность производства намного сложнее корректировать, нежели сезонность потребления. Сезонность производства связана с климатическими условиями. Однако в настоящее время имеется возможность сглаживать ее путем развития технологий по переработке и хранению продукции, что дает возможность реализовывать продукцию на протяжении всего года.

Сезонность потребления может быть вызвана следующими факторами:

– времена года. Например, в холодное время

[1] Магистрант НОУ ВПО «Российский новый университет».

[2] Кандидат технических наук, доцент, доцент кафедры ИСиКТ НОУ ВПО «Российский новый университет».

года возрастает потребление чая, летом же спрос на горячие напитки снижается;

– праздники. Традиционно на праздники люди дарят подарки, и спрос на подарочный чай возрастает. Пик продаж приходится на декабрь, ведь в России именно Новый год является самым любимым праздником;

– деловая активность. Общая деловая активность может существенно влиять на уровень продаж. Деловая активность – это не только соотношение работающих и отдыхающих в определенный момент людей, но и общий настрой, атмосфера, стремление либо к активной деятельности, либо к спокойной работе.

Общеизвестно, что в течение года традиционно наблюдаются три спада деловой активности: конец декабря – середина января, первая декада мая и летние месяцы.

Рассмотрим бизнес-процесс продажи товара на примере диаграммы деятельности. Каждое состояние на диаграмме деятельности соответствует выполнению некоторой элементарной операции, а переход в следующее состояние срабатывает только при завершении этой операции в предыдущем состоянии.

Графически диаграмма деятельности представляется в форме графа деятельности, вершинами которого являются состояния действия, а дугами – переходы от одного состояния действия к другому (рис. 1).

На диаграмме отслеживается последовательность выполнения действий от поступления заявки от клиента компании до окончательного выполнения заказа. Процесс не требует пересмотра, тем не менее фактор возрастания спроса и снижения продаж имеет место быть. Он в большей степени зависит не от внутреннего состояния компании и выполнения процесса продажи товара, а от внешних факторов повышения и снижения спроса в течение года.

Рассмотрим внутригодовое распределение возрастания спроса и снижения продаж в одной из компаний города Москвы, занимающейся оптовыми продажами чая (таблицы 1, 2).

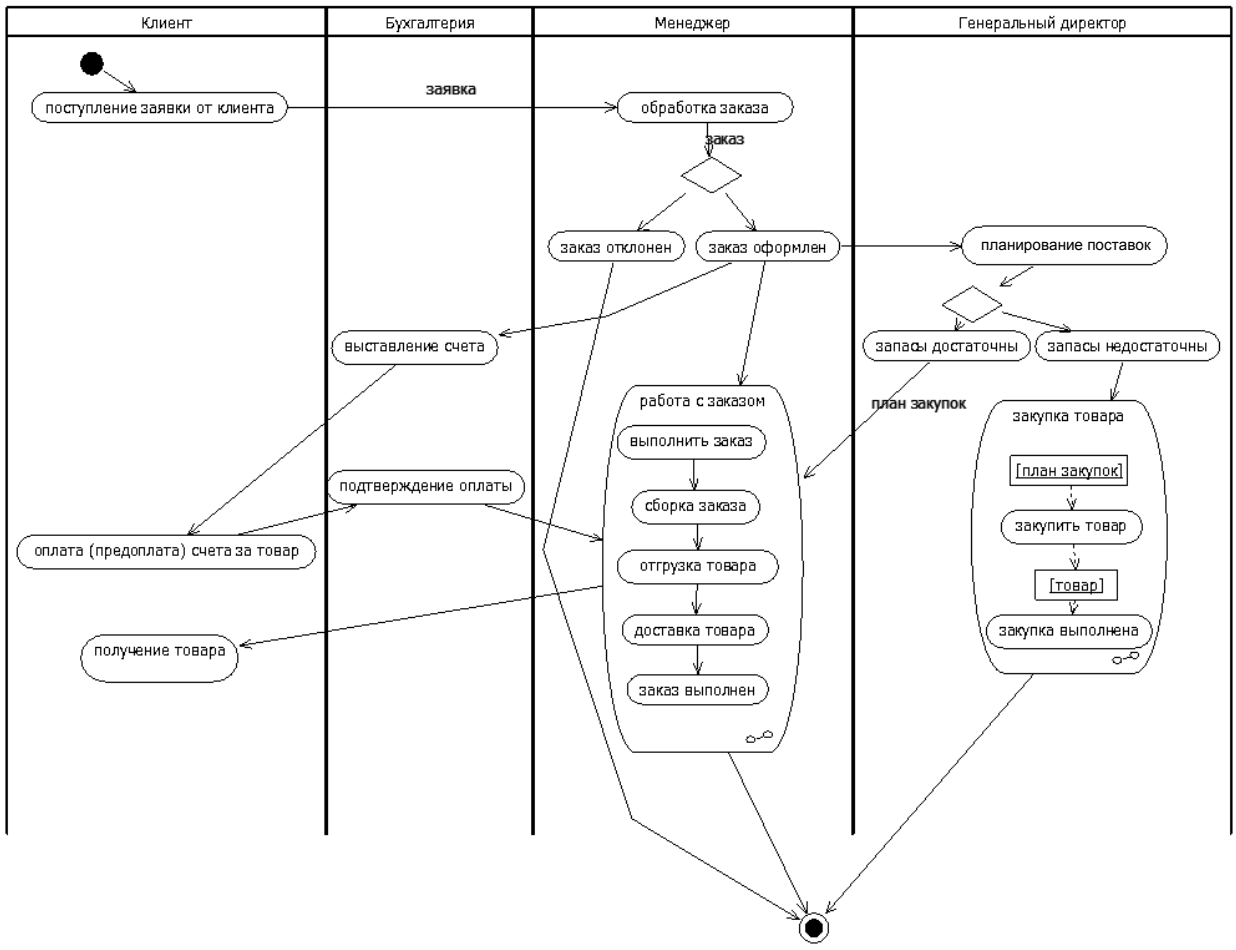


Рис. 1. Activity Diagram, UML. Диаграмма деятельности. Продажа товара

Таблица 1

Внутригодовое распределение возрастания спроса и снижения продаж чая за январь – июнь 2013 года

Виды чая	Валовая прибыль, руб.					
	январь	**февраль**	**март**	**апрель**	**май**	**июнь**
ГЕРМАНИЯ	**751 007,04**	**1031330,12**	**979121,12**	**908649,34**	**444127,76**	**533228,61**
Зеленый	8 577,31	17 727,34	68 931,39	8 938,82	3 374,50	3 694,25
Зеленый ароматизированный	114 828,98	137 095,93	138 271,21	134 390,17	77 112,45	71 210,21
Мате	2 108,79	8 159,63	3 941,62	10 170,56	2 443,81	7 002,25
Ройбос	43 323,58	24 006,15	27 565,29	40 066,12	5 014,66	9 795,01
Травяной	28 481,59	48 615,90	49 504,44	65 925,13	17 915,10	15 142,79
Фруктовый	43 186,97	107 471,15	100 286,66	96 822,41	53 876,10	43 628,45
Черный	221 665,35	329 356,65	291 791,99	262 711,37	190 247,99	222 908,04
Черный ароматизированный	288 834,47	358 897,37	298 828,52	289 624,76	94 143,15	159 847,61
КИТАЙ	**397 516,17**	**530 550,15**	**347 939,14**	**382 498,95**	**284 307,59**	**228 084,25**
Пуэр	73 067,50	91 805,26	61 727,57	79 202,42	73 312,08	27 472,62
Улун	169 611,11	222 598,65	157 609,35	153 162,70	123 265,66	64 463,21
Белый + зеленый	69 181,79	132 449,75	87 964,67	107 422,12	64 023,24	111 312,02
Вязаный	60 883,97	52 998,55	27 146,21	30 914,78	7 559,33	21 409,12
Красный	24 771,80	30 697,94	13 491,34	11 796,93	16 147,28	3 427,28

Таблица 2

Распределение валовой прибыли по отдельным видам чая за январь – июнь 2013 года

Виды чая	Валовая прибыль, руб.					
	июль	**август**	**сентябрь**	**октябрь**	**ноябрь**	**декабрь**
ГЕРМАНИЯ	**553336,91**	**634180,4**	**733055,59**	**885107,54**	**1058761,21**	**1153949,68**
Зеленый	2 639,08	2 191,77	2 550,81	2 112,14	9 541,88	13 292,33
Зеленый ароматизированный	86 056,41	91 002,12	78 706,87	149 236,49	160 982,97	102 212,45
Мате	4 655,30	6 287,00	5 023,06	7 865,32	3 516,20	5 389,95
Ройбос	13 796,40	34 892,89	13 288,58	21 115,04	38 581,25	27 142,18
Травяной	29 311,78	31 796,06	16 539,32	59 189,98	48 439,90	42 495,23
Фруктовый	47 861,62	45 578,10	46 561,05	59 704,85	52 937,29	57 217,63
Черный	207 145,16	218 451,39	232 705,85	371 850,70	447 974,05	378 018,21
Черный ароматизированный	161 871,16	203 981,07	337 680,05	214 033,02	296 787,67	528 181,70
КИТАЙ	**389 313,79**	**404 036,44**	**256 168,45**	**505 535,59**	**465 447,65**	**703 784,11**
Пуэр	88 162,97	107 653,88	46 948,32	94 441,30	106 690,18	172 239,24
Улун	129 119,14	116 516,99	105 017,08	134 607,52	134 872,05	210 038,33
Белый + зеленый	136 497,89	121 038,80	76 700,82	213 332,30	161 719,31	169 229,92
Вязаный	20 338,50	26 697,92	7 918,69	29 012,68	23 503,38	100 837,05
Красный	15 195,29	32 128,85	19 583,54	34 141,79	38 662,73	51 439,57

Визуализируем полученные данные по валовой прибыли построением графиков.

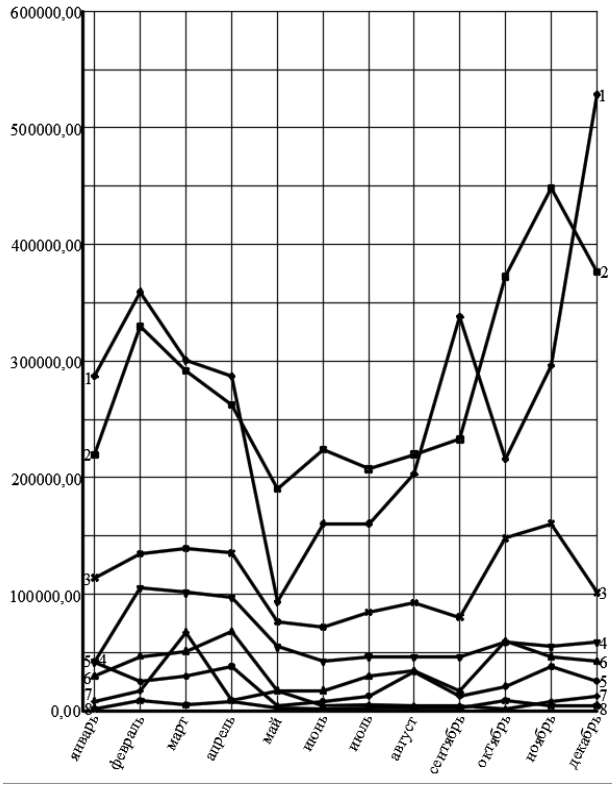


Рис. 2. Внутригодовые колебания спроса
на отдельные виды чая, произведенного в Германии:
1 – черный ароматизированный чай;
2 – черный чай;
3 – зеленый ароматизированный чай;
4 – фруктовый чай; 5 – ройбос;
6 – травяной чай; 7 – зеленый чай; 8 – мате

На графике четко отслеживаются все три фактора сезонности, такие, как времена года, праздники и деловая активность.

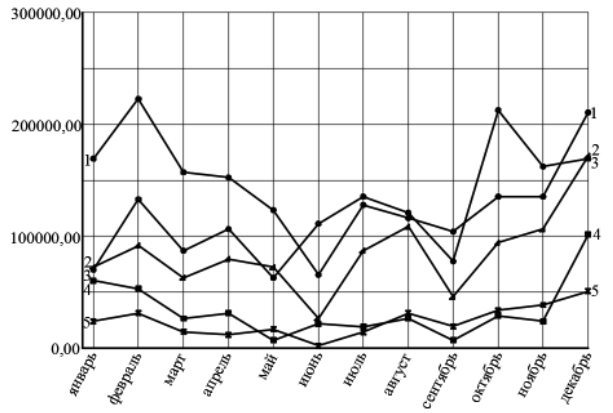


Рис. 3. Внутригодовые колебания спроса
на отдельные виды чая, произведенного в Китае:
1 – улун; 2 – белый + зеленый чай;
3 – пуэр; 4 – вязаный чай; 5 – красный чай

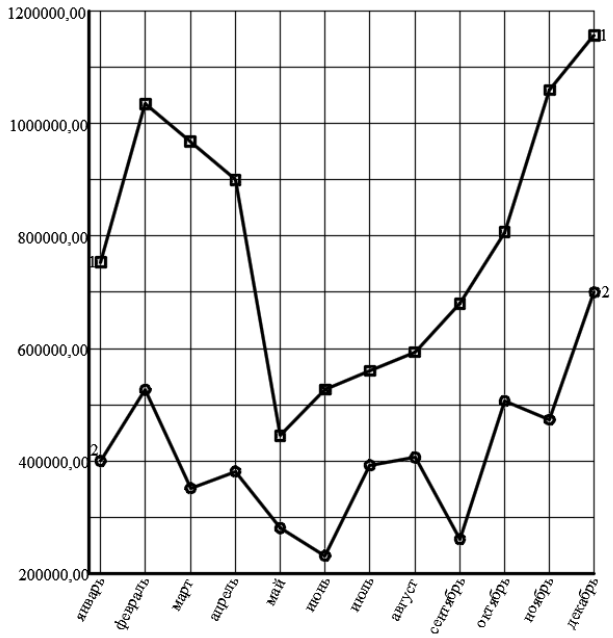


Рис. 4. Сравнение внутригодовых колебаний спроса
на чай, поставляемый из Германии и Китая:
1 – чаи, поставляемые из Германии;
2 – чаи, поставляемые из Китая

При сравнении графиков на рис. 2 и 3 заметны скачки спроса, однако динамика сезонности сохраняется. На декабрь приходится пик активности, весной наблюдается спад продаж.

Поскольку внутригодовая динамика имеет выявленную цикличность, есть возможность прогнозировать периоды спада продаж и проводить мероприятия по их корректировке.

Разработаны методы сглаживания влияния сезонных факторов на валовую прибыль от продаж чая:

– проведение рекламных акций перед периодами снижения продаж;

– назначение скидок на некоторые виды товара, которые в данный период времени не пользуются спросом;

– дополнение ассортимента компании всесезонными товарами;

– использование в деятельности компании креативного маркетинга. Эффективность такой рекламы достаточно высока, потому что творческий подход больше запоминается. Это влечет за собой так называемый вирусный маркетинг, который основан на обмене пользователями понравившейся информацией. Как следствие, люди, не осознавая этого сами, пересылают рекламу продукции компании друг другу;

– вывод на рынок новинок.

Лучшими месяцами знакомства потребителей с новинками будут май и январь – месяцы,

в которые наблюдается спад продаж. Именно в это время выгодно заострить внимание потребителей на интересных предложениях.

Анализ и прогнозирование процесса сезонных колебаний спроса является важной составляющей управленческой деятельности компании.

В ходе данного исследования были рассмотрены и выявлены внутригодовые изменения сезонных колебаний в объемах товарооборота компании. Построены диаграммы, которые служат инструментом анализа процессов с внутригодовой динамикой и применяются при прогнозировании сезонных процессов.

В данной статье на основе процессного подхода рассматриваются периодические колебания продаж отдельных видов чая, возникающие под влиянием внутригодового спроса. Анализируются бизнес-процессы организации, определяется, каким образом сезонный фактор влияет на получение прибыли. Описываются методы урегулирования скачкообразного снижения прибыли в отдельные месяцы года.

Литература

1. Управление закупками и поставками : учебник для высших учебных заведений / Майкл Линдерс. – М. : ЮНИТИ : ЮНИТИ-ДАНА, 2007. – 723 с.

2. Стерлигова А.Н. Управление запасами в цепях поставок. – М. : ИНФРА-М, 2009. – 428 с.

3. Золотарев О.В. Инновационные решения в формировании функциональной структуры предметной области // Вестник Российского нового университета. – 2013. – Выпуск 4.

4. Золотарев О.В. Управление в проектах внедрения распределенных корпоративных информационных систем // Вестник Российского нового университета. – 2012. – Выпуск 4.

УДК 517.929

В.И. Мухин[1]
И.С. Рекунков[2]
М.А. Зайцев[3]

О ВИРТУАЛИЗАЦИИ МАССОВЫХ НАСТРОЕНИЙ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ ПОСРЕДСТВОМ ВНЕДРЕНИЯ КИБЕРСИМУЛЯКРОВ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ СЕТИ

Статья посвящена способам виртуализации массовых настроений в интернет-пространстве путем внедрения киберсимулякров в информационно-коммуникационные сети.

Ключевые слова: *киберсимулякр, интернет-пространство, политическая коммуникация, информационно-коммуникационные сети.*

V.I. Mukhin
I.S. Rekunkov
M.A. Zaytsev

ABOUT VIRTUALIZATION OF MASS SENTIMENTS IN THE INTERNET SPACE BY MEANS OF INTRODUCTION OF CYBERSIMULACRA INTO INFOCOMMUNICATION NETWORKS

This article is devoted to ways of mass sentiments virtualization in Internet space by means of cybersimulacra introduction into information and communication networks.

Keywords: *cybersimulacrum, Internet space, political communication, infocommunication networks.*

Сущность массового настроения в политике

Социально-политическое настроение – это социальный феномен, сущность которого состоит в переживании и наделении со стороны субъекта определенным смыслом его принадлежности к социальной системе. Оно определяется степенью идентификации себя с социальной ролью, а в конечном счете – с социальной системой, т.е. приобретает социально-политическую окраску. «Настроения, в основе которых лежит эмоционально-аффективный сигнал об удовлетворенности осуществления потребности людей, могут приобрести специфическую политическую направленность и охватывать значительные массы» [2].

Виртуализация массовых настроений в интернет-пространстве

Виртуализация массовых настроений в интернет-пространстве «существенно повышает значение коммуникационных инструментов распределения и реализации власти, при этом предоставляет, с одной стороны, новые возможности, формы и механизмы политической коммуникации внутри общества, между обществом и властью», а с другой – «приводит к состоянию межгосударственных или внутригосударственных отношений, характеризуемых совокупностью факторов, способных при определенных условиях привести к возникновению военной угрозы» [1].

В сетевом пространстве функцию репрезентации реальных пользователей выполняют виртуальные аккаунты. На практике они все больше становятся оторванными от реальных пользователей. Указанные обстоятельства позволяют их нишу занять киберсимулякрам.

Киберсимулякр – функционирующая в интернет-пространстве виртуальная личность, симулирующая репрезентацию реально существующего сетевого пользователя.

[1] Доктор военных наук, профессор, профессор кафедры информационных систем и технологий Академии гражданской защиты МЧС России.

[2] Кандидат технических наук, доцент кафедры защиты информации Московского государственного университета информационных технологий, радиотехники и электроники.

[3] Кандидат технических наук, доцент кафедры математики и информатики Московского университета им. С.Ю. Витте.

Функциональное предназначение киберсимулякров – вброс, распространение, интерпретация общественно значимой политической информации.

Применение механизма политической коммуникации для формирования массовых политических настроений

Форма применения механизма политической коммуникации для формирования массовых политических настроений – это организационная деятельность в сетевом пространстве, направленная на [1]:

– разрушение традиционных ценностно-смысловых пространств в национальных сегментах интернет-пространств (включая Рунет);

– внедрение альтернативных идей, ценностей, смыслов в общественное мнение посредством информационно-коммуникационной работы в сети;

– изменение существующих традиционных моделей поведения в желаемом для субъектов информационно-коммуникационной работы направлении;

– дискредитация национальных лидеров, существующих политических режимов, национально-политической элиты, в целом, за счет негативизации информационного освещения их деятельности в сетевом пространстве;

– внедрение моделей протестной активности через сетевые сообщества;

– мобилизация политически активных масс из сетевого пространства для участия в реальных акциях протеста против действующей власти;

– конструирование выгодных для субъектов информационно-коммуникационного воздействия моделей социально-политической реальности, которая замещает объективную реальность, выступая в качестве псевдосреды, принимаемой массами за реальную.

Лидерами в широкомасштабном применении киберсимулякров в сетевых коммуникациях являются США. При этом, «военными силами США для распространения определенных протестных идей, смыслов и ценностей в национальных сегментах стран-мишеней» внедрение моделей протестной активности осуществляется посредством информационно-коммуникационных сетей. Затем активно используются программные комплексы, позволяющие конструировать максимально приближенные к реальным виртуальные личности, создавая им сетевую историю, «прописывая» их в основных поисковых системах и социальных сетях, в результате чего они становятся практически неотличимыми от реально существующих интернет-пользователей [4].

Осуществляя коммуникацию на языке, использующемся в стране-мишени, такие киберсимулякры с высокой степенью эффективности позволяют решать поставленные задачи по дестабилизации существующих политических режимов, влияя на общественное мнение и рост протестных настроений, что основывается, прежде всего, на использовании технологий убеждающей коммуникации от лица вымышленных персонажей, являющихся релевантными по отношению к аудиториям информационно-коммуникационного воздействия [2].

Успешность применения киберсимуклякров для формирования общественного мнения подтверждают события на Украине с ноября 2013 г. по настоящее время.

Способы внедрения киберсимулякров в информационно-коммуникационную сеть

Первый способ – активное влияние на восприятие информации в сети владельцев киберсимулякров на уровне горизонтальных коммуникаций в процессе информационно-коммуникационного взаимодействия с реальными пользователями.

Цель – внедрение массовых настроений в сознание людей.

Второй способ – повышение качества восприятия сообщений реальными пользователями, которые передаются в информационно-коммуникационной сети путем совместной выработки киберсимулякрами смыслов и мнений в процессе их взаимодействия с другими пользователями в Интернете [3; 5].

«Исходя из этого, в современных сетевых коммуникациях непосредственно контент сообщения играет все меньшую роль, а на первый план выходят пользовательские оценки и комментарии, смысловое содержание внутригрупповых дискуссий в сетевых сообществах, поэтому мы можем констатировать, что конечная ценностно-смысловая нагрузка и качественное восприятие исходного сообщения реальными пользователями во многом определяются той сетевой информационно-коммуникационной активностью, которую осуществляют киберсимулякры при взаимодействии с другими пользователями в Интернете, осуществляя при этом совместную выработку коллективных смыслов и мнений» [1].

Третий способ – повышение пользовательской активности потребления информации за счет современных интернет-ресурсов путем использования инструментов социального взаимодействия и социальной оценки сообщений.

Таким образом, «потребление информации

становится не пассивным в форматах традиционного индивидуального получения и осмысления информационного контента (например, чтение книги или газеты, просмотр телепередачи или прослушивание радиорепортажей), а активным, публичным. Большинство современных интернет-ресурсов предполагает использование инструментов социального взаимодействия и социальной оценки сообщений (Like, Retweet и т.д.), что обусловливает существенное значение пользовательской активности в процессе потребления информации для оценки самого сообщения другими пользователями. В результате, значимость сообщения определяется не столько содержанием информации, а той активностью, которую проявляют пользователи в процессе потребления информационного сообщения. Так, чем больше «лайков» и «ретвитов» получило сообщение, тем более значимым оно выглядит в представлении рядового интернет-пользователя. Исходя из этого, «накрутки» «социального веса» сообщения становятся еще одним инструментом влияния на восприятие сетевых пользователей, и ключевую роль здесь играют в первую очередь киберсимулякры, обеспечивающие «продвижение» сообщения и его «видимость в сети» [1].

Литература

1. Володенков С.В. Киберсимулякры как инструмент виртуализации современной массовой политической коммуникации // Информационные войны. – 2014. – № 4. – С 18–21.

2. Ольшанский Д.В. Массовые настроения в политике // Центр стратегического анализа и прогноза. – 1995. – С. 239.

3. Гладышев А.И. Разработка имитационной модели вирусной эпидемии на основе модели биологических вирусов: принципы, основные параметры, описание и зависимости // Вестник Российского нового университета. – 2012. – Выпуск 4. Управление, вычислительная техника и информатика. – С. 17–21.

4. Гладышев А.И., Жуков А.О. Использование в автоматизированной системе контроля полномочий биометрической идентификации // Вестник Российского нового университета. – 2013. – Выпуск 4. Управление, вычислительная техника и информатика. – С. 95–99.

5. Гладышев А.И. Удобство и безопасность компьютерных систем. В чем противоречие? // Вестник Российского нового университета. – 2012. – Выпуск 4. Управление, вычислительная техника и информатика. – С. 89–93.

УДК 681.322.067

И.Ю. Гришин[1]

АНАЛИЗ ПЕРСПЕКТИВНЫХ ПОДХОДОВ К ПРОЕКТИРОВАНИЮ СИСТЕМ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Работа посвящена анализу современных подходов к построению систем безопасности распределенных компьютерных сетей (корпоративных, банковских, учебных заведений и т.п.). Исследованы наиболее распространенные за последние 10 лет подходы, сделаны выводы об их эффективности, осуществлен выбор систем защиты для различных условий применения распределенных сетей.

Ключевые слова: *распределенная компьютерная сеть, система безопасности, корпоративная сеть, анализ эффективности, криптографические методы, операционная система.*

I.Yu. Grishin

ANALYSIS OF PROMISING APPROACHES TO DESIGN OF DISTRIBUTED COMPUTER NETWORKS SECURITY SYSTEMS

This article is devoted to analysis of promising approaches to design of distributed computer networks security systems (corporate, banking, educational institutions, etc.). The most common over the last 10 years approaches are explored, and the conclusions on their effectiveness and selection of protection systems for different applications of distributed networks ade made.

Keywords: *distributed computer network, security, enterprise network, efficiency analysis, cryptographic techniques, operating system.*

На рубеже веков существенно возрос объем циркулирующих в компьютерных сетях информационных потоков, характеризующих различные стороны деятельности человеческого общества. Отмечается тенденция экспоненциального увеличения объемов информации, необходимой для принятия решений в различных отраслях народного хозяйства, государственном управлении, финансовом и банковском секторах, научных исследованиях, образовании и т.д. Появилось новое понятие – “big data”, отражающее указанные выше тенденции и указывающее на необходимость обработки нетрадиционно больших объемов информации и их передачи в сетях. Способность общества и его институтов собирать, обрабатывать, анализировать, систематизировать и накапливать информацию является важной предпосылкой социального и технологического прогресса, фактором национальной безопасности, одной из основ успешной внутренней и внешней политики.

В этих условиях становится чрезвычайно актуальной проблема защиты информации, циркулирующей в распределенных компьютерных сетях, поскольку возможное несанкционированной уничтожение, копирование или искажение информации затрагивает интересы как государственных органов, так и юридических и физических лиц, может привести к ошибкам в принятии решений и, как следствие, – к тяжелым последствиям в сфере экономики, экологии, промышленности, государственного и муниципального управления.

Базой для совершенствования систем защиты информации в распределенных компью-

[1] Доктор технических наук, профессор, профессор кафедры компьютерных технологий и информационной безопасности ФГБОУ ВПО «Кубанский государственный технологический университет».

терных сетях являются достижения в области информатики и вычислительной техники, телекоммуникаций, микроэлектроники, системного анализа и ряда других наук.

Таким образом, актуальность проблемы повышения эффективности систем защиты информации в распределенных компьютерных сетях целесообразно анализировать в аспектах мирового общественного развития, экономического развития и развития науки, техники и технологий.

Новые информационные технологии, которые активно развиваются в различных сферах деятельности общества, формируют повышенный спрос на создание систем защиты информации, причем этот спрос часто превышает потребности государственных заказчиков.

Значительный вклад в совершенствование различных аспектов подходов к проектированию систем безопасности распределенных компьютерных сетей внесли такие ученые, как В.А. Хорошко, А.А. Молдовян, В.А. Герасименко, М. Хеллман, Ж. Брассар [1–6] и др.

Однако в сфере проектирования систем защиты информации остается целый ряд проблем, решение которых имеет важное научно-техническое и государственное значение. Одной из таких задач является совершенствование подходов к проектированию систем защиты информации в распределенных компьютерных сетях.

Целью настоящей работы является проведение анализа новых, перспективных подходов к проектированию систем безопасности распределенных сетей с целью выработки методологии такого анализа и рекомендаций по применению того или иного подхода.

В ходе проведения анализа необходимо учитывать обстоятельство, что целью создания систем безопасности является защита субъектов, которые участвуют в процессах информационного взаимодействия, от нанесения им существенного материального, морального, иного ущерба в результате воздействия на информационную систему со стороны злоумышленника [7–10].

В результате анализа современных тенденций развития информационных технологий могут быть выделены следующие направления совершенствования систем информационной безопасности [СБ РФ 12]:

– создание специальных защищенных операционных систем, особенно для тонких и нулевых клиентов;

– создание специальных архитектур безопасного администрирования со средствами управления безопасностью и обнаружения атак;

– развитие важнейших прикладных и фундаментальных криптографических методов.

При анализе степени защищенности распределенных компьютерных сетей необходимо учитывать, что большинство распределенных корпоративных сетей используют глобальную сеть Интернет в качестве транспортной системы. Данное обстоятельство существенно усложняет требования к построению безопасности таких сетей.

Существующие в настоящее время отечественные и зарубежные требования исходят из того, что политика безопасности рассматриваемых систем должна опираться на модели разграничения прав доступа – дискреционную и мандатную [13]. При этом в основе дискреционной модели лежат идентификаторы субъекта и объекта, а также право доступа определенного субъекта к конкретному объекту, а модели мандатного доступа – официальный допуск субъектов к информации определенного уровня конфиденциальности безотносительно пары субъект – объект.

Известно [14; 15], что в структуру политики безопасности входит множество возможных операций над объектами, а также множество разрешенных операций подмножества всего множества возможных операций. В результате проецирования основных требований политики безопасности на параметры и топологию компьютерной сети может быть получена архитектура безопасности [16; 17], представляющая план и множество принципов, описывающих службы безопасности системы для удовлетворения требований пользователя, состав элементов системы для реализации этих служб, а также необходимые уровни производительности указанных элементов системы.

В случае решения указанных задач администраторами безопасности возникает угроза ошибок администрирования либо пропуска организации защиты каких-либо функций, что приводит к выводу о необходимости применения средств автоматизации проектирования архитектур безопасности [18]. В основе автоматизированного проектирования лежат модели объекта проектирования и приемов решения проектных задач [19].

В работе [20] архитектура безопасности распределенной сети представляется в виде проекции схемы информационных потоков на семантическую сеть, в которой узлы выполняют те или иные функции защиты, а дуги – связи между ними (рис. 1).

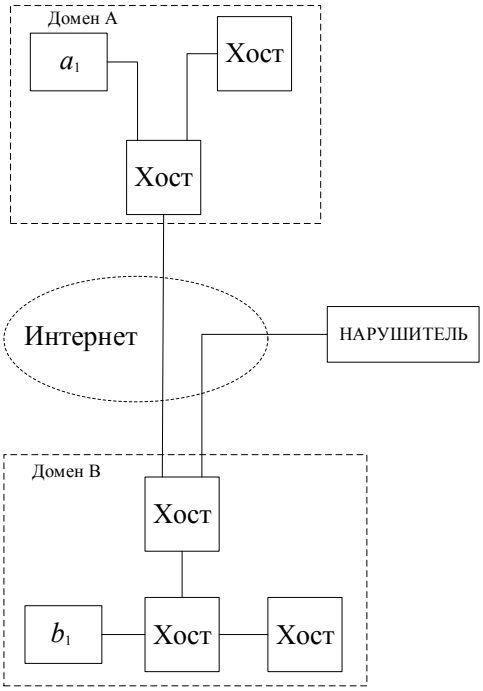


Рис. 1. Архитектура безопасности распределенной сети [20]

Предложена модель, состоящая из функциональных защитных компонент нескольких типов, связанных между собой. Данная модель (высокоуровневый аспект) представлена на рис. 2.

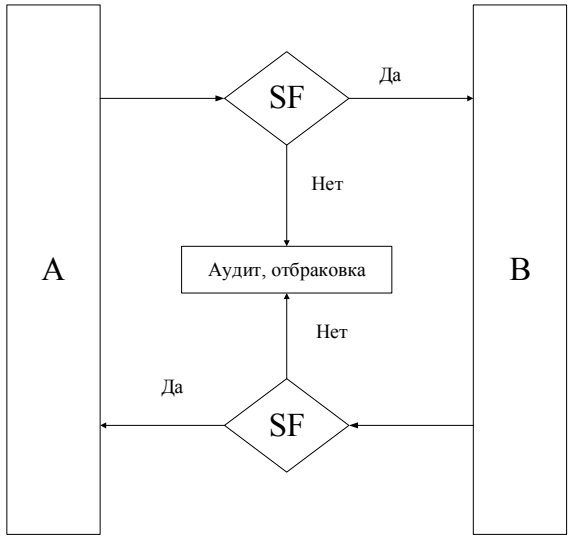


Рис. 2. Высокоуровневая модель архитектуры безопасности [20]

В приведенной на рис. 2 модели разделение функции защиты (SF) на две составляющие обусловлено возможностью передачи данных в двух направлениях. Аргументами функции защиты SF являются часть или вся порция обмена информацией. В случае успешной проверки на безопасность формируется значение функции ИСТИНА, а порция обмена передается к месту назначения, в противном случае формируется значение ЛОЖЬ – и порция обмена отбраковывается с соответствующей записью в контрольном журнале.

Управление доступом, проверка аутентичности, а также проверка целостности могут осуществляться в рассматриваемой модели на границе защищенного сетевого домена либо внутри него, однако в обоих случаях необходимо гарантировать защиту любого пути прохождения порции обмена к месту назначения в защищенном домене.

Для обеспечения аутентичности и целостности целесообразно применять криптографические протоколы с участием отправителя (например, для выработки сеансовых ключей отправитель генерирует свой ключ).

При построении математических моделей, предназначенных для исследования и построения политик безопасности в распределенных сетях, часто опираются на матричную модель [20], в которой присутствуют сеансовая и почтовая матрицы. Сеансовая матрица позволяет описать политику доступа каждой категории пользователей к различным файлам, а почтовая – определяет возможность передачи файлов между пользователями различной категории:

$$\mathbf{M} = \begin{pmatrix} M_{1,1} & M_{1,2} & \cdots & M_{1,n} \\ M_{2,1} & M_{2,2} & \cdots & M_{2,n} \\ \vdots & \vdots & M_{i,j} & \vdots \\ M_{m,1} & M_{m,2} & \cdots & M_{m,n} \end{pmatrix}, \qquad (1)$$

$$\mathbf{MT} = \begin{pmatrix} MT_{1,1} & MT_{1,2} & \cdots & MT_{1,m} \\ MT_{2,1} & MT_{2,2} & \cdots & MT_{2,m} \\ \vdots & \vdots & MT_{i,j} & \vdots \\ MT_{m,1} & MT_{m,2} & \cdots & MT_{m,m} \end{pmatrix}. \qquad (2)$$

При этом элементы указанных матриц определяются следующим образом:

$$M_{i,j} = \begin{cases} r, \text{ чтение;} \\ rw, \text{ редактирование;} \\ 0, \text{ нет доступа.} \end{cases} \qquad (3)$$

$$MT_{i,j} = \begin{cases} 1, & i\text{-й субъект может посылать данные } j\text{-му субъекту,} \\ 0, & i\text{-й субъект не может посылать данные } j\text{-му субъекту.} \end{cases} \qquad (4)$$

Следует учитывать, что множество объектов и субъектов в процессе функционирования изменяется ввиду появления или уничтожения объектов и субъектов, а также изменения их статуса (прав доступа). Поэтому и матрицы доступа также динамически меняются.

В работе [7] предложено развитие рассмотренного подхода. Указанная модель является многоуровневой, объекты могут иметь разные уровни доступа, а субъекты – степени доступа. В основе такой модели лежит теория алгебраических решеток. Для обеспечения более гибкого управления безопасностью могут применяться комбинированные модели (совокупность мандатной и дискреционной моделей), когда в дискреционной модели для контроля за информационным взаимодействием одноуровневых пользователей применяется мандатная модель, к примеру модель Белла – Лападулы [21] (рис. 3).

Рис. 3. Структура модели Белла – Лападулы

Составляющими данной модели являются множества субъектов S, объектов O и уровней защиты L, прав доступа G, а также списки текущего доступа b и запросов Z. Определяющим в задании политики безопасности является множество прав доступа, имеющее вид $G = \{r, a, w, e\}$, где признаки r, a, w, e означают, соответственно, чтение, дополнение, модификацию и исполнение иных действий. Матрица доступа $\mathbf{M} = \|M_{i,j}\|$ в данной модели не должна содержать пустых столбцов, однако ненулевое значение элемента $M_{i,j}$ не является достаточным условием разрешения доступа.

В рассматриваемой модели используются два условия защиты – простое и так называемое *-условие. При этом простое условие обеспечивает исключение прямой утечки охраняемых данных и накладывает ограничения на базовые уровни защищенных объектов, а *-условие предотвращает косвенную утечку данных, например чтение для переписи данных в объект с низшим уровнем защиты. В данной модели описываются разрешения для каждого из одиннадцати возможных видов запросов. Главным достоинством рассматриваемой модели является формализация анализа выполнения политики безопасности, что позволяет осуществлять эти действия с помощью соответствующего программного обеспечения информационной системы.

Рассмотренные модели и методы ложатся в основу методологии проектирования систем безопасности распределенных корпоративных сетей, в которых связанные между собой локальные сети являются важнейшими их составляющими.

Под проектированием архитектуры безопасности обычно понимают средства, реализующие функции защиты с необходимым набором параметров, их место в вычислительной сети и способы связи друг с другом [Cisco].

Предложенная в работе [20] методология включает следующие этапы: задание обобщенной исходной топологии защищаемой системы, локализация информационных потоков, систематизация функций защиты информации и их локализация, введение классов защищенности, построение поэтапного алгоритма проектирования архитектуры безопасности.

В связи с появлением новых угроз информационной безопасности (быстрое распространение ботнетов, постоянное усложнение сетевых атак, тревожащий рост организованной киберпреступности и шпионажа с использованием Интернета, хищение персональных и корпоративных данных, более сложные способы инсайдерских атак, развитие новых форм угроз для мобильных систем) компанией Cisco предложена своя концепция информационной безопасности Cisco Security Framework (CSF), которая определяет концепцию создания системы информационной безопасности, ориентированной на обеспечение доступности сети и сервисов и поддержание непрерывности бизнеса. Угрозы безопасности характеризуются высокой динамикой, и концепция CSF предусматривает способы выявления текущих направлений угроз, а также отслеживания новых и развивающихся угроз за счет следования лучшим практическим рекомендациям и использования комплексных решений. Новая архитектура системы безопасности Cisco использует подходы, определенные в концепции CSF, для определения продуктов и функций, позволяющих надежно обеспечить безопасность во всей сети [концепция Cisco].

Концепция CSF предполагает наличие политик безопасности, разработанных по результатам анализа угроз и рисков и согласованных с бизнес-целями и задачами. Критически важным фактором для достижения успеха бизнеса является создание таких политик безопасности, которые не только не препятствуют, а, напротив, способствуют достижению организацией

поставленных бизнес-целей и плановых показателей. Поэтому разработка политик должна начинаться с четкого определения бизнес-целей и задач. После определения этих целей необходимо выявить возможные угрозы для выделенных целей и задач. Следует иметь в виду, что цели, задачи и возможные угрозы могут сильно меняться в зависимости от организации и среды.

В заключение можно отметить, что проведенный анализ существующих подходов к проектированию систем безопасности распределенных компьютерных сетей позволяет выделить наиболее важные тенденции совершенствования методологии проектирования и применения систем безопасности. Следует, однако, иметь в виду, что методы атак корпоративных сетей также постоянно совершенствуются, и это требует разработки новых подходов к проектированию и применению систем безопасности.

Литература

1. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К. : Юниор, 2003. – 504 с.
2. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. – Петербург, БХВ, 2005. – 288 с.
3. Брассар Ж. Современная криптология / пер. с англ. – М. : Издательско-полиграфическая фирма ПОЛИМЕД, 1999. – 176 с.
4. Герасименко В.А. Защита информации в автоматизированных системах обработки данных : в 2 кн. – М. : Энергоатомиздат, 1994.
5. Hellman, M.E. An overview of public key cryptography // IEEE Communication Magazine. – 2002. – Iss. 50. – P. 42–49.
6. Diffie, W. and Hellman, M.E. New directions in cryptography // IEEE Trans. Inform. Theory. – 1976. – V. 22. – P. 644–654.
7. Чураев Л.А., Просихин В.П. Построение алгоритма проектирования архитектуры безопасности распределенных вычислительных систем // Проблемы информационной безопасности высшей школы. – М. : МИФИ, 2000. – С. 126–127.
8. Аносов В.Д., Зегжда П.Д., Курило А.П. Современные требования к информационной безопасности и актуальные направления разработки средств защиты // Методы и технические средства обеспечения безопасности информации. – СПб., 1995. – С. 12–16.
9. Бронников В.А., Просихин В.П. Телекоммуникации в аспекте национальной безопасности // READ.ME. – 1998. – № 10. – С. 7.
10. Першин А.Ю. Организация защиты вычислительных систем // Компьютер-пресс. – 1992. – № 10. – С. 35–50; № 11. – С. 33–42.
11. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации. – URL: http://www.scrf.gov.ru/documents/6/94.html (дата обращения 06.06.2015).
12. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. – М. : МИФИ, 1997.
13. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. – М., 1992.
14. Клир Д. Системология. Автоматизация решения системных задач / под ред. А.И. Горлина. – М. : Радио и связь, 1990.
15. Щербаков А.Ю. К вопросу о гарантированной реализации политики безопасности в компьютерной системе // Безопасность информационных технологий. – 1997. – № 1. – С. 15–26.
16. CERT. IP Spoofing Attacks and Hijacked Terminal Connections, CA-95:01. // Computer Emergency Response Team. – Carnegie Mellon University, 1995.
17. Held, G., Hundley, K. Cisco Security Architectures // Computing McGraw-Hill, 1999.
18. Kaufman, C.W., Perlman, R., Speciner, M. Network Security. Private Communication in a Public World // Prentice-Hall, Englewood Cliffs. – New Jersey. – 1995.
19. Amoroso, E.G. Fundamentals of computer security technology // Prentice Hall, 1994.
20. Просихин В.П. Методология построения архитектуры безопасности распределенных компьютерных систем: дис. … д-ра техн. наук. – СПб., 2001. – 199 с.
21. Bell, D.T., LaPadula, L.J. Secure Computer System: Unified Exposition and Multics Interpretation // The Mitre Corp., ESD-TR-75-306. Hanscom AFB, Massachusetts, March 1976.
22. Обзор архитектуры безопасности версии 1.0. // Информационный бюллетень Cisco, 2009.

УДК 004.054

А.С. Марковский[1]
А.П. Киреев[2]
М.Д. Санин[3]

МЕТОДИКА ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

Данная статья посвящена проблеме обеспечения аудита информационной безопасности и предлагает комплекс мероприятий, повышающий уровень защищенности систем управления критически важных объектов.

Ключевые слова: *информационная безопасность, аудит, уровень защищенности.*

A.S. Markovsky
A.P. Kireev
M.D. Sanin

THE TECHNIQUE OF CARRYING OUT AUDIT OF INFORMATION SECURITY OF AUTOMATED CONTROL SYSTEMS OF CRITICAL INFRASTRUCTURE

This article is devoted to the problem of ensuring information security audit and offers a range of activities that enhance the security of the control systems of critical infrastructure.

Keywords: *information security, audit, security level.*

Широкое внедрение систем информационных технологий, являющихся одним из компонентов, поддерживающих цели деятельности критически важных объектов (КВО), обеспечивая их эффективное и бесперебойное функционирование, также привело к необходимости реализации решений по обеспечению информационной безопасности (ИБ). Для того чтобы оценить уровень безопасности автоматизированной системы управления (АСУ) КВО и впоследствии построить эффективную систему защиты информации, проводится целый комплекс мероприятий, называемых аудитом ИБ.

В то же время, для того чтобы сделать компетентные выводы относительно уровня защищенности АСУ КВО, аудитору потребуется наличие всех необходимых исходных данных. Их получение осуществляется в ходе информационного и инструментального обследования.

Вместе с тем, в стране отсутствует единая система взглядов на государственное регулирование процессов аудита ИБ. В настоящее время существует ряд частных организаций, предлагающих услуги по проведению аудита ИБ. В то же время, в отсутствие необходимых национальных регуляторов такая деятельность может нанести непоправимый вред. Ранее были рассмотрены [1] наиболее распространенные методики аудита ИБ, проведен их анализ, представлены сравнительные характеристики (табл. 1).

Исходя из проведенного анализа, а также сложившихся условий отсутствия правового и методического обеспечения аудита ИБ, возникла необходимость разработки собственной методики информационного обследования объекта аудита АСУ КВО, учитывающих цели, задачи обследования и уровни ИБ, с одной стороны, и специфику деятельности КВО, особенности функционирований, топологии самих АСУ КВО – с другой.

[1] Кандидат технических наук, старший научный сотрудник Военно-космической академии им. А.Ф. Можайского.

[2] Старший научный сотрудник Военно-космической академии им. А.Ф. Можайского.

[3] Научный сотрудник Военно-космической академии им. А.Ф. Можайского.

Таблица 1

Сравнительные характеристики различных стандартов оценивания ИБ

	Уровни ИБ	Структурированность	Подход
ГОСТ 15408	технический	11 классов, 61 семейство функциональных требований, 7 классов, 26 семейств требований доверия	системный, функциональный
СТО БР ИББС	организационный	3 группы, 32 групповых показателя, 237 частных показателей	процессный
ISO 17799/ 27001	организационный, процедурный	11 разделов, 133 требования	процессный
BSI	организационный, технический	5 групп, 46 объектов контроля	функциональный
NIST	организационный, процедурный, технический	3 класса, 17 семейств, 163 меры контроля	функциональный
COBIT	организационный, процедурный	4 домена, 34 цели контроля, 318 средств контроля	процессный

Взаимная детализация каждой из рассматриваемых деятельностей позволяет определить основные элементы в основной деятельности КВО, контроль которых на основе методики аудита ИБ обеспечит основу для оценки эффективности внедряемых организационных и технических мероприятий по защите информации.

Методика информационного обследования объекта аудита АСУ КВО состоит из следующих основных этапов (рис. 1).

Рис. 1. Методика информационного обследования объекта аудита АСУ КВО

Этап определения уровней ИБ и критичных ресурсов объекта аудита

Для этого на основе процессного подхода [2] построена обобщенная модель взаимосвязи деятельности по обеспечению ИБ и основной деятельности КВО (рис. 2). Определение уровней ИБ $Y = \{y_1, y_2, y_3\}$ основывается на целях аудита и требованиях руководства, что, в свою очередь, позволит нам сформировать методику сбора и обработки информации об объекте аудита.

Объект аудита может быть представлен в виде множества взаимосвязанных ресурсов $X = \{x_i\}$,

формально представленных в виде $x_i \in X$, где X – множество ресурсов АС, $i \in 1\ldots n$, а n – общее количество ресурсов.

В соответствии со стандартом ISO 17799-2005 [4], ресурсы организации с точки зрения ИБ можно разделить на информационные, физические, программные, сервисные, кадровые и нематериальные. Анализ критичности ресурсов должен выявить ресурсы, наиболее критичные с точки зрения ИБ.

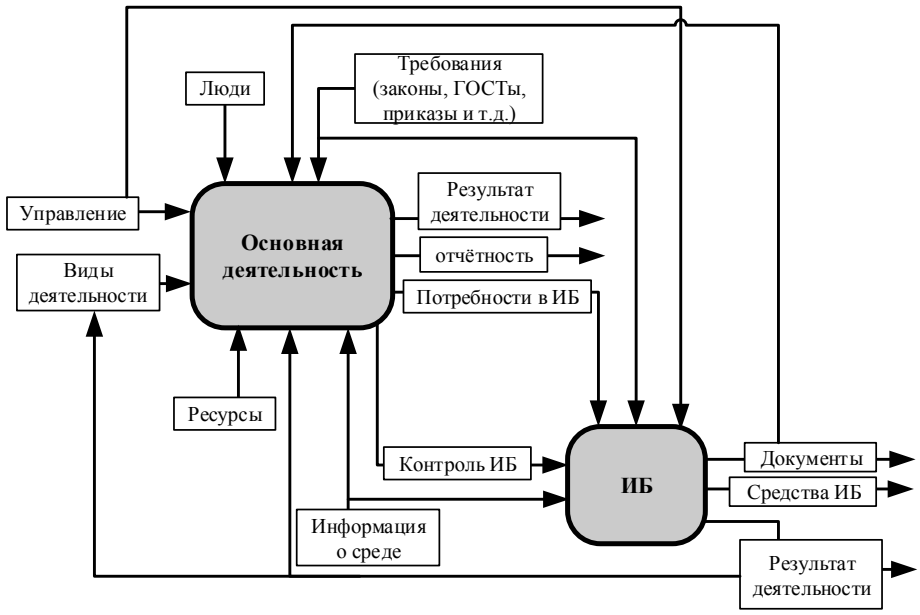


Рис. 2. Модель взаимосвязи деятельности по обеспечению ИБ и основной деятельности КВО

С помощью построенной модели стало возможным провести детализацию каждой деятельности КВО (рис.2), что, в свою очередь, позволило определить критичные ресурсы объекта аудита $X^j = \{x_i^j\}$, $i \in 1\ldots n$, $j \in 1\ldots l$, l – общее количество критичных ресурсов.

Из-за большого количества разнообразных ресурсов в ряде случаев удобнее их сгруппировать по функциональному назначению, принадлежности или местоположению. Серверы и рабочие станции рассматриваются в комплексе с установленным на них программным обеспечением (ПО), реализуемыми сервисами, хранящейся информацией в файлах и базах данных – соответственно как серверные ресурсы и автоматизированные рабочие места (АРМ). Также в качестве комбинированных ресурсов рассматриваются АСУ с используемым аппаратным и программным обеспечением (ПО), прикладными системами, файлами и базами данных. Одна АСУ может включать в свой состав несколько физических (серверы, АРМ), программных (прикладное ПО) или информационных ресурсов (базы данных, файлы).

Все ресурсы объекта аудита ИБ предлагается разбить в соответствии со следующей **иерархией уровней** [3].

1. Нормативно-документационный уровень.
2. Организационно-управленческий уровень.
3. Уровень прикладных систем.
4. Уровень систем управления базами данных (СУБД).
5. Уровень операционных систем и общесистемного ПО.
6. Уровень сетевых сервисов и приложений.
7. Сетевой уровень.
8. Физический уровень.

Этап определения соответствия ресурсов объекта аудита $X = \{x_i\}$ областям контроля $Q = \{q_1 \ldots q_{10}\}$

Для контроля состояния ресурсов объекта аудита можно выделить области контроля информационной безопасности (ИБ). Области контроля охватывают группы взаимосвязанных вопросов в области ИБ. Исходя из имеющейся практики стандартизации, они не обязательно должны соответствовать одному из иерархических уровней ресурсов объекта аудита. Часть ресурсов разных уровней может входить в одну область контроля.

Выделяются следующие ***области контроля*** [4].

1. Нормативно-документационное обеспечение ИБ.

2. Организационно-управленческое обеспечение ИБ.

3. Организация физической защиты элементов инфраструктуры АСУ.

4. Инвентаризация и классификация (категорирование) ресурсов.

5. Защита периметра АСУ и организация доступа пользователей в сети структурных подразделений.

6. Безопасность сетевой инфраструктуры.

7. Администрирование безопасности информации внутри АСУ.

8. Контроль доступа к информации.

9. Обеспечение безопасного функционирования АСУ.

10. Разработка, внедрение и сопровождение АСУ.

В рамках каждой области контроля разрабатывается контрольный список требований и рекомендаций, которые проверяются в ходе проведения аудита. В составе контрольных списков могут быть вопросы двух типов:

– вопросы-требования, имеющие определенный вес, ответы на которые и напрямую влияющие на оценивание показателей уровня ИБ в зависимости от степени соответствия требованию (соответствует, не соответствует, частично соответствует);

– вопросы информационного характера, необходимые для дальнейшей работы аудитора по сбору свидетельств аудита и косвенно влияющие на оценивание показателей уровня ИБ.

Для проверки состояния информационной безопасности ресурсов объекта аудита последние необходимо охватить в проверяемых вопросах контрольных списков по областям контроля.

Можно предложить следующую обобщенную матрицу соответствия иерархического уровня проверяемых ресурсов областям контроля (табл. 2).

Таблица 2

Матрица соответствия иерархического уровня проверяемых ресурсов областям контроля

Уровень ресурса (*X*) / **Область контроля (*Q*)**	**Нормативно-документационный уровень**	**Организационно-управленческий уровень**	**Уровень прикладных систем**	**Уровень систем управления базами данных**	**Уровень операционных систем и общесистемного ПО**	**Уровень сетевых сервисов и приложений**	**Сетевой уровень**	**Физический уровень**
1. Нормативно-документационное обеспечение ИБ	+							
2. Организационно-управленческое обеспечение ИБ	+	+						
3. Организация физической защиты элементов инфраструктуры АСУ		+					+	+
4. Инвентаризация и классификация (категорирование) ресурсов	+	+	+	+	+	+	+	+
5. Защита периметра АСУ и организация доступа пользователей во внешние сети	+					+	+	
6. Безопасность сетевой инфраструктуры						+	+	+
7. Администрирование безопасности информации внутри корпоративной сети			+	+	+	+		
8. Контроль доступа к информации	+	+	+	+	+	+	+	+
9. Обеспечение безопасного функционирования АСУ		+	+		+	+	+	+
10. Разработка, внедрение и сопровождение автоматизированных систем управления	+	+	+					+

На этапе сбора информации о состоянии ИБ объекта аудита АСУ КВО продолжается более подробный сбор и анализ информации. Методика сбора информации основывается на ряде требований (рис. 3).

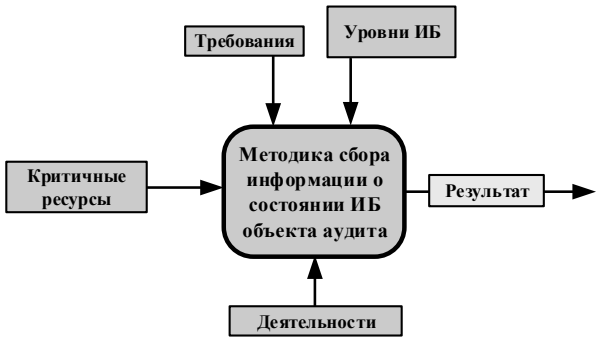


Рис. 3. Формирование методики сбора информации о состоянии ИБ объекта аудита АСУ КВО

В частности, сбор информации включает в себя этапы:

– изучения документации;

– проведения интервьюирования руководителей и специалистов предприятия;

– инструментального обследования;

– наблюдения за работой;

– проверки настроек и конфигураций ИС и др.

Сбор информации, как правило, начинается с изучения существующей документированной информации об объекте аудита, созданной при проектировании, эксплуатации и поддержке функционирования системы.

Интервьюирование персонала проводится с целью получения исходной информации об АСУ, отсутствующей в документированном виде, подтверждения актуальности документированной информации и определения уровня осведомленности сотрудников в части требований по обеспечению ИБ.

Наблюдение за реальными процессами, связанными с обеспечением информационной безопасности, могут касаться следующих вопросов:

– процедура регистрации/исключения пользователей, генерации и смены паролей;

– процедура анализа журналов аудита и реагирования на подозрительную активность;

– порядок изменения конфигурации и обновления системного ПО сетевых устройств и серверов;

– порядок обработки заявок на предоставление дополнительных прав доступа;

– порядок работы с наложенными средствами защиты (межсетевые экраны, системы обнаружения вторжений, антивирусы и т.д.);

– анализ действий, предпринятых при обработке произошедших инцидентов;

– анализ действий, предпринятых при аварийных ситуациях;

– порядок доступа в серверные помещения;

– другие аспекты деятельности по обеспечению ИБ.

При проведении анализа конфигурации типовых рабочих мест, сетевых устройств и ключевых серверов их перечень определяется по согласованию с должностным лицом, ответственным за ИБ на проверяемом предприятии.

Целью такого анализа является оценка соответствия реальной конфигурации тому, что декларируется эксплуатационной документацией, требованиями политики безопасности и персоналом заказчика.

Анализу подлежат параметры аутентификации и контроля доступа, механизмы авторизации, доступа и управления, параметры аудита, меры защиты маршрутной информации, меры защиты от внешних атак АСУ КВО.

Этап оценки, согласования и корректировки результатов реализуется на основании всей полученной информации (в том числе – на основе инструментального обследования).

В процессе анализа и формирования результатов могут возникнуть противоречия между различными источниками информации. Поэтому в случае необходимости проводится повторное уточняющее обследование по конкретному вопросу.

После формирования результатов необходимо воспользоваться методиками оценки соответствия ИБ АСУ КВО требованиям нормативных документов и методикой сравнительной оценки объектов аудита с учетом системы показателей и критериев оценивания.

Литература

1. Марковский А.С. Анализ существующих методик аудита информационной безопасности : научно-технический сборник ОАО «Концерн “Системпром”», 2014.

2. Ерохин С.С., Мещеряков Р.В., Бондарчук С.С. Модели и методы оценки защищенности информации и информационной безопасности объекта. Безопасность информационных технологий // Министерство образования и науки РФ. Московский инженерно-физический институт. – 2007. – № 4. – С. 39–46.

3. Березин А.С., Петренко С.А. Построение корпоративных защищенных виртуальных частных сетей // Конфидент. Защита Информации. – 2001. – № 1.

4. Information technology – Code of practice for Information security management. International Standard ISO/IEC 17799:2005.

5. Нечай А.А. Специфика проявления уязвимостей в автоматизированных системах управления критически важными объектами / А.А. Нечай, П.Е. Котиков // Современные тенденции в образовании и науке : сборник научных трудов по материалам Международной научно-практической конференции : в 14 ч. – Тамбов, 2014. – С. 96–97.

6. Уланов А.В. Повышение оперативности принятия решения в автоматизированных системах / А.В. Уланов, А.А. Нечай, П.Е. Котиков // Наука и современность. – 2014. – № 2 (2). – С. 95–101.

7. Нечай А.А. Контроль сохранности информации / А.А. Нечай, П.Е. Котиков // Научный вестник. – 2014. – № 2 (2). – С. 85–91.

8. Нечай А.А. Применение перепрограммируемых структур в современных информационных решениях / А.А. Нечай, П.Е. Котиков // Научный вестник. – 2014. – № 2 (2). – С. 92–101.

9. Лопатин В.А. Оценка надежности и оперативности распределенной обработки информации / В.А. Лопатин, А.А. Нечай // Экономика и социум. – 2015. – № 1–3 (14). – С. 949–951.

10. Лопатин В.А. Некоторые обобщения в теории множеств, отношений и графов, их применение в информационных технологиях / В.А. Лопатин, А.А. Нечай // Экономика и социум. – 2015. – № 1–3 (14). – С. 958–960.

11. Котиков П.Е. Репликация данных между серверами баз данных в среде геоинформационных систем / П.Е. Котиков, А.А. Нечай // Вестник Российского нового университета. Сер. Сложные системы: модели, анализ и управление. – 2015. – Выпуск 1. – С. 90–93.

12. Нечай А.А. Методика комплексной защиты данных передаваемых и хранимых на различных носителях информации / А.А. Нечай, П.Е. Котиков // Вестник Российского нового университета. Сер. Сложные системы: модели, анализ и управление. – 2015. – Выпуск 1. – С. 94–97.

13. Нечай А.А. Выявление недекларированных возможностей аппаратно-программного обеспечения / А.А. Нечай // Экономика и социум. – 2014. – № 1–2 (10). – С. 457–460.

14. Нечай А.А. Подходы к выявлению конфиденциальной информации / А.А. Нечай, С.А. Краснов, И.В. Першина // Экономика и социум. – 2015. – № 1–4 (14). – С. 26–31.

15. Першина И.В. Программные методы сокрытия информации / И.В. Першина, А.А. Нечай // Экономика и социум. – 2015. – № 1–4 (14). – С. 195–198.

УДК 004.414.2=161.1

Э.И. Митряев[1]

E.I. Mitryaev

АНАЛИТИЧЕСКИЙ МЕТОД ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО КРИТЕРИЮ ДОСТУПНОСТИ ИНФОРМАЦИИ ДЛЯ РЕШЕНИЯ ЗАДАЧ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

ANALYTICAL METHOD OF THE ASSESSMENT OF INFORMATION SECURITY BY CRITERION OF AVAILABILITY OF INFORMATION TO THE SOLUTION OF PROBLEMS OF CREATION OF THE PROTECTED DISTRIBUTED INFORMATION SYSTEMS

В статье рассматривается проблема построения устойчиво функционирующей территориально распределенной информационной системы при условии воздействия на нее потенциально возможных деструктивных факторов техногенного и антропогенного характера. Для решения практических задач инженерного проектирования предлагается аналитическая модель, построенная на основе применения математической теории графов. В статье излагается аналитическая методика и приводится пример ее использования для решения конкретной задачи.

Ключевые слова: *распределенная информационная система, защита информации, информационная безопасность, уязвимость информационной системы, доступность информации, связность каналов связи, граф структуры информационной системы, пропускная способность канала связи.*

In the article is considered the problem of creation of steadily functioning territorially distributed information system on condition of impact on it of potentially possible destructive factors of technogenic and anthropogenous character. For the solution of practical problems of engineering design is offered the analytical model constructed on the basis of application of the mathematical theory of counts. In the article is given the analytical technique is stated and the example of its use for the solution of a specific objective.

Keywords: *distributed information system, information protection, information security, vulnerability of information system, availability of information, connectivity of communication channels, columns of structure of information system, communication channel capacity.*

Современная тенденция развития информационных технологий определяется переходом в сторону создания распределенных информационных систем и сетей. При этом, основной характеристикой этих систем является территориальная распределенность компонентов системы и наличие интенсивного обмена информацией между ними.

Масштабы применения и приложения информационных технологий стали такими, что наряду с проблемами производительности, надежности и устойчивости функционирования информационных систем остро встает проблема обеспечения информационной безопасности по критерию доступности циркулирующей в системах информации.

Понятие «информационная безопасность» было нормативно закреплено в качестве самостоятельной составляющей безопасности Российской Федерации в 1992 году. За прошедшее время было многое сделано для наполнения этого термина конкретным содержанием, определе-

[1] Доктор технических наук, профессор, профессор кафедры информационной безопасности факультета информационных систем и компьютерных технологий НОУ ВПО «Российский новый университет».

ния наиболее важных направлений деятельности государства в этой области.

На сегодняшний день сформулированы базовые принципы информационной безопасности, среди которых наибольшее актуальное звучание принимает обеспечение доступности информации для всех авторизованных пользователей.

Широкое внедрение в повседневную практику компьютерных сетей, их открытость, масштабность делают проблему защиты информации исключительно сложной. При анализе данной проблемы выделяют две базовые подзадачи:

1) обеспечение безопасности обработки и хранения информации в каждом из компьютеров, входящих в сеть;

2) защита информации, передаваемой между компьютерами сети.

В Федеральном законе Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [1] дается следующее определение защиты информации как принятие правовых, организационных и технических мер, направленных, в частности, на реализацию права на доступ к информации, которое можно также трактовать и как обеспечение доступности информации.

В ГОСТ Р50922-2006 [2] дано следующее определение доступности информации: «Доступность информации (ресурсов информационной системы) – это состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно».

Таким образом, доступность информации есть свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующаяся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Исходя из большого разнообразия условий, при которых может возникнуть необходимость защиты информации, общая целевая установка заключается в разработке стратегий защиты информации, включающих рациональное обеспечение требуемой защиты и надлежащего использования информационных ресурсов в любых условиях, даже в случае, если эти ресурсы будут подвергнуты деструктивному воздействию как извне, так и изнутри.

1. Особенности современных информационных систем как объектов защиты

Большинство современных информационных систем (ИС) обработки информации в общем случае представляет собой территориально распределенные системы, интенсивно взаимодействующие (синхронизирующиеся) между собой по данным (ресурсам) и управлению (событиям) локальных вычислительных сетей (ЛВС) и отдельных ЭВМ.

В распределенных ИС (РИС) возможны все традиционные для локально расположенных (централизованных) вычислительных систем способы несанкционированного вмешательства в их работу и доступа к информации.

В силу территориально распределенных компонентов системы и наличия интенсивного обмена информацией между ними, для РИС характерны новые специфические угрозы работе системы и нарушению доступности информации, в том числе:

– физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);

– отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

– действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.).

2. Синтез распределенной информационной системы с гарантией информационной безопасности по критерию доступности информации

Проблема искусственных преднамеренных (умышленных) нарушений функционирования РИС различного назначения в настоящее время является одной из наиболее актуальных в связи с резко обострившейся геополитической обстановкой в мире. Наиболее справедливо это утверждение для стран с сильно развитой информационной инфраструктурой.

Создание информационной системы всегда связано с проблемой обеспечения ее информационной безопасности. Создание защищенной информационной системы заключается в выполнении совокупности мероприятий, направленных на разработку и/или практическое применение

таких информационных технологий, которые бы реализовали функции по защите информации в соответствии с требованиями стандартов и нормативных документов как во вновь создаваемых, так и в действующих системах.

Основные принципы и положения по созданию и функционированию защищенных систем изложены в нормативных документах. Согласно данным документам, информационная технология проектирования защищенной ИС в унифицированном исполнении включает в себя проведение следующих основных работ.

I. Анализ средств защиты

1. Представление организационно-структурного построения ИС в виде упорядоченного графа: узлы – типовые структурные компоненты, дуги – взаимосвязи между компонентами.

2. Представление технологии обработки защищаемой информации в виде строго определенной схемы.

3. Определение параметров защищаемой информации и условий ее обработки.

II. Оценки уязвимости информации

1. Определение значений вероятностей нарушения защищаемой информации в тех условиях, в которых она будет обрабатываться.

2. Оценки размеров возможного ущерба при нарушениях защищенности информации.

Учитывая активность, непрерывность, скрытность, количество и разнообразие потенциальных угроз информационной системе, проблему защиты информации относят к числу слабо формализуемых задач, т.е. задач, неразрешимых строго математически. В то же время, для решения проблемы проектирования защищенной ИС необходимы количественные оценки планируемых показателей информационной безопасности уже на этапе ее проектирования. На сегодня, для оценки различных показателей функционирования сложных систем в теории разработаны и доведены до практического применения различные аналитические методы.

3. Аналитический метод оценки показателя доступности информации

Распределенная информационная система (РИС) представляет собой многоуровневую иерархическую структуру, включающую множество узлов, связанных между собой определенным образом. Такой конструкции присуще свойство уязвимости, определяющейся тем, что за счет многочисленных узлов и связей между ними (учитывая, что нормальное функционирование нескольких узлов иерархической сети возможно только при нормальном функционировании одного основного узла, называемого управляющим) нередко проявляется «каскадный эффект», когда сбой в одном месте провоцирует перегрузки и выход из строя других элементов.

Проектирование новых РИС и развитие уже существующих связано с проблематикой принятия решений по использованию имеющихся сетевых структур:

– управлению потоками;

– распределению ресурсов между узлами.

Перечисленные проблемы тесно связаны с задачей определения связности и доступности информации в существующей или проектируемой ИС в условиях потенциально возможных деструктивных факторов техногенного или антропогенного характера.

Под связностью информационной системы понимается топологический вид сети межмашинных связей и надежностные характеристики компонентов этой сети.

С учетом показателя связности, доступность информации будем характеризовать способностью информационной системы в любой момент времени функционирования использовать суммарную производительность всех исправных ЭВМ для решения задач обработки и передачи информации. Кроме того, на значение показателя доступности информации сети сильно влияет минимальная пропускная способность (число каналов связи) на информационном направлении, ниже которой связь считается отказавшей.

Данной проблеме ИС посвящен ряд работ (Винокуров Д.Е. [3], Додонов А.Г. [4], Дудник Б.Я. [5], Кривулец В.Г. [6], Мельников Ю.Е. [7],. Сарыпбеков Ж.С. [8], Хорошевский В.Г [9] и др.).

В настоящее время актуальной является задача разработки аналитических моделей и методов, использующих полученные по аналогичным проблемам оценки показателей надежности и живучести РИС, результаты для оценки информационной безопасности РИС по критерию доступности информации, позволяющих решать задачи расчета ИБ РИС большой размерности и сложной структуры.

На макроуровне РИС выглядит как ансамбль ЭВМ, между которыми есть линии связи (каналы связи).

Эти элементы составляют макроструктуру (или структуру) РИС. Структура РИС описывается однородным графом $G = \{N; M\}$.

N – множество вершин (множество ЭВМ или системных устройств);

M – множество ребер (линии, каналы, связи).

Мощность N равна числу ЭВМ в РИС.

Структура РИС характеризуется:

1) связностью требуемого числа работоспособных ЭВМ в системе при ненадежных линиях связи;

2) способностью к реализации обменов информацией между любыми ЭВМ ИС в течение заданного времени (иначе – задержками при передаче информации между ЭВМ, которые не превышают установленной нормы).

В рамках формальной теории графов, структуру ИС можно представить в виде вектор-функции доступности информации:

$$L(\mathrm{G}, Q) = \{L_r(\mathrm{G}, Q)\}, \qquad (1)$$

где $L_r(\mathrm{G}, Q)$ – вероятность существования подсистемы ранга r.

Подсистема ранга r – подмножество работоспособных ЭВМ, связность которых устанавливается через работоспособность линии связи.

G – структура РИС (граф).

Q – пропускная способность (трафик) каналов связи между ЭВМ.

Пропускная способность – один из важнейших с точки зрения пользователей факторов. Она оценивается количеством данных, которые сеть в пределе может передать от одного подсоединенного к ней устройства к другому.

Пропускная способность канала связи определяется максимальной скоростью передачи информации по каналу связи в единицу времени и выражается формулой:

$$q = V/\, t,$$

q – пропускная способность канала (в битах в секунду или подобных единицах);

($q \in Q$)

t – время передачи.

Доступность информации при передаче информации между ЭВМ РИС определяется расстоянием (в смысле графов – у нас это время передачи информации (трафик) между вершинами структуры графа G, сопоставленными взаимодействующими ЭВМ.

Для оценки доступности информации в ИС используем диаметр "d" и средний диаметр "d_c" структуры.

Диаметр "d" определим как максимальное расстояние, определенное на множестве кратчайших путей между парами вершин структуры РИС.

$$d = \max\ \{d_{ij}\}.$$

Средний диаметр: $d_c = (N-1)^{-1} \sum_{i=1}^{n} ln$

d_{ij} – расстояние – минимальное число ребер, образующих путь из вершины i в вершину j,

$i, j \in N$,

n – число вершин, находящихся на расстоянии l от любой выделенной вершины (однородного) графа G.

Получение аналитических выражений для координат вектор-функции доступности информации (1) является сложной задачей, разрешимой лишь для частных случаев.

Для решения данной задачи используем представление однородного графа G РИС в виде матрицы смежности порядка ($m \times n$), где $n \in N$ – число вершин однородного графа G (число ЭВМ РИС) , $m \in M$ – число ребер (число каналов связи между смежными ЭВМ РИС).

Используя матричное представление графа ИС значения пропускной способности каналов связи в качестве весовых характеристик ребер графа РИС, можно решать различные практические задачи проектирования РИС по критерию доступности информации.

В качестве примера рассмотрим следующую задачу.

В силу большой пространственной протяженности линий связи через неконтролируемую территорию практически всегда имеется возможность подключения к ним либо вмешательства в процесс передачи данных со стороны злоумышленников. При этом меняется объем (трафик) передаваемой информации – что может служить показателем данной угрозы.

Современные топологии и протоколы требуют, чтобы сообщения были доступны большому числу узлов при передаче данных сообщений по назначению. Это гораздо дешевле и легче, чем иметь прямой физический путь каждой пары машин.

Для повышения пропускной способности РИС, с учетом деструктивных факторов на каналы связи, можно их проектировать с использованием различной физической реализации каналов связи (кабельные, волоконно-оптические, широкополосные радиоканалы) по критерию доступности информации.

Математически данная задача формулируется следующим образом.

Между абонентами X_1, X_2, X_3 РИС и территориально удаленными абонентами Y_1, Y_2, Y_3 этой же РИС может быть установлена связь по телефонным или широкополосным радиоканалам.

Матрицами A и B задано время, которое необходимо затратить при использовании телефонного или широкополосного радиоканала для связи абонента X_i с абонентом Y_j.

$$\mathrm{A} = \begin{array}{c} \\ X_1 \\ X_2 \\ X_3 \end{array} \begin{array}{c} \begin{array}{ccc} Y_1 & Y_2 & Y_3 \end{array} \\ \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \end{array}$$

Элементы a_{ij} матрицы А – это пропускная способность телефонных каналов связи.

$$\mathrm{B} = \begin{array}{c} \\ X_1 \\ X_2 \\ X_3 \end{array} \begin{array}{c} \begin{array}{ccc} Y_1 & Y_2 & Y_3 \end{array} \\ \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} \end{array}$$

Элементы b_{ij} матрицы В – это пропускная способность широкополосных радиоканалов.

Для выбора каналов связи проектируемой сети по критерию доступности информации надо построить матрицу $\mathrm{C} = (c_{ij})$, где $c_{ij} = \min \{a_{ij}; b_{ij}\}$

Решение данной задачи в матричном представлении графа РИС успешно реализуется на ЭВМ.

Литература

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями).

2. ГОСТ Р50922-2006 Защита информации. Основные термины и определения.

3. Винокуров Д.Е. Исследование живучести информационных сетей / Ю.Ю. Громов, Д.Е. Винокуров, Т.Г. Самхарадзе, И.И. Пасечников // Инженерная физика. – М. : Научтехлитиздат, 2006. – № 3. – С. 123–139.

4. Додонов А.Г. Введение в теорию живучести вычислительных систем / А.Г. Додонов, М.Г. Кузнецова, Е.С. Горбачик. – Киев : Наук. думка, 1990. – 184 с.

5. Надежность и живучесть систем связи / под ред. Б.Я. Дудника. – М. : Радио и связь, 1984. – 243 с.

6. Кривулец В.Г. Что такое теория связности и живучести транспортных сетей? / В.Г. Кривулец, В.П. Полесский. – М. : Инофрмационные процессы, 2001. – Т. 1. – № 2. – С. 199–203.

7. Мельников Ю.Е. Модель комплексной оценки и обеспечения живучести распределенных информационно-вычислительных систем / Ю.Е. Мельников, Ж.С. Сарыпбеков : материалы II Всесоюзной науч.-техн. конф. – М., 1988.

8. Сарыпбеков Ж.С. Многокритериальная оценка живучести РВС / Ж.С. Сарыпбеков, Б.А. Ченсизбаев // Однородные вычислительные системы, структуры и среды : тез. докл. V Всесоюзн. науч.-техн. конф. – М., 1991. – Ч. III. – С. 219–220.

9. Хорошевский В.Г. Инженерный анализ функционирования вычислительных машин и систем / В.Г. Хорошевский. – М. : Радио и связь, 1987. – 155 с.

УДК 338.242.2

К.М. Лауфер[1]
З.А. Отарашвили[2]

АЛГОРИТМ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПОСТРОЕНИЯ ОПТИМАЛЬНОЙ АССОРТИМЕНТНОЙ ПОЛИТИКИ ПРЕДПРИЯТИЯ

В работе исследуется вопрос перехода от экстенсивной к интенсивной финансовой политике предприятия на основе проведения ассортиментного анализа. Приведен алгоритм правильного выбора очередности выпуска продукции. Проведены аналитические исследования кривых выигрыша для различных случаев. Приведены примеры расчёта.

Ключевые слова: *ассортиментная политика, продуктовый анализ, маржинальная рентабельность.*

K.M. Laufer
Z.A. Otarashvili

ALGORITHM AND INFORMATION TECHNOLOGIES FOR CONSTRUCTING OPTIMAL ASSORTMENT POLICY OF AN ENTERPRISE

In this paper the transition from extensive to intensive financial policy based on the analysis of assortment of enterprise is investigated. An algorithm for the correct selection of priority output is quoted. An analytical study of curves winnings for different occasions is carried out, and examples of its calculation are quoted as well.

Keywords: *assortment policy, food analysis, marginal profitability.*

В условиях финансового кризиса, дороговизны заемных ресурсов, риска оказаться в кредитной ловушке с перспективой потери бизнеса для коммерческого предприятия особенно актуальным становится поиск альтернативных источников финансирования.

При определенных условиях предприятие может изыскать дополнительные необходимые финансовые ресурсы за счет собственных средств.

Варианты выбора очередности финансирования проекта

Проанализируем возможные варианты выбора проектов. Ограниченность средств предполагает приоритеты в финансировании и ранжирование проектов по определенному критерию, в данном случае – по эффективности проекта. Существует немало известных способов определения эффективности и выбора проектов из ряда предлагаемых на основе критериев внутренней доходности (IRR) и других показателей.

Предлагается рассмотреть метод выбора очередности финансирования на основе маржинальной рентабельности.

Пусть имеется n проектов [3]. Возможное число размещений из n проектов по n определяется перестановкой из n элементов и рассчитывается по формуле $A_n^n = n!$. Предположим, число проектов равно пяти, тогда количество перестановок (число) будет равно $5! = 120$. Ста двадцатью различными способами (по очередности финансирования) можно расставить пять проектов.

Рассмотрим графики очередности финансирования проектов (рис. 1). При принятом критерии (в нашем случае эффективность) на графике найдется один лучший вариант (1), один – худший (2) (проектов с равной, максимальной или минимальной эффективностью может быть несколько, но это не меняет сути). Остальные 118 вариантов будут располагаться между ними (3).

[1] Кандидат философских наук, доцент, доцент кафедры экономики и менеджмента МГМУ им. А.И. Сеченова.

[2] Университет Иннополис, г. Иннополис, Республика Татарстан.

Самым худшим выбором является выбор, обратный лучшему, то есть соответствующий критерию наименьшей эффективности. При этом проекты ранжируются по возрастанию маржинальной рентабельности. Последние и первые проекты меняются местами.

Чтобы представить всю серьезность рассматриваемой задачи, скажем, что уже для 10 проектов теоретически существует 3 628 800 различных вариантов выбора. Один (или несколько) лучше остальных, с точки зрения максимальной финансовой отдачи.

Рис. 1. Зависимость маржинальной прибыли от суммарных переменных затрат по проектам

Маржинальная рентабельность портфеля в целом или средняя маржинальная рентабельность по портфелю есть отношение суммарной маржинальной прибыли к суммарным затратам. Очевидно, в портфеле есть проекты с большей и меньшей маржинальной рентабельностью, чем средняя. При возникновении ограничений на финансы возникает необходимость приостановки финансирования портфеля проектов на недостающую сумму. Нужен простой, надежный механизм гарантирующий сохранение финансирования наиболее выгодным проектам (с точки зрения максимальной финансовой отдачи).

Маржинальная рентабельность есть отношение маржинальной прибыли к переменным затратам. Геометрически – это тангенс угла наклона отрезка, характеризующего данный проект к горизонтальной оси. Принцип убывания маржинальной рентабельности означает, что тангенс угла наклона каждого последующего отрезка меньше предыдущего. Соответственно, получается ограниченная сверху выпуклая вверх параметрическая кривая. То есть, площадь под этой кривой является максимально возможной из всех возможных вариантов их расположения. На рис. 1 – это кривая 1.

В общем виде оптимальная кривая носит степенной характер. Показатель степени положительный и меньше единицы:

$$y = x^p,\ 0 < p < 1, \tag{1}$$

где $p = \frac{n}{m}$, n и m – натуральные числа, $n < m$.

Функция монотонно возрастает, не имеет экстремумов, выпукла вверх.

Функция, позволяющая находить выигрыш между оптимальным и средним способами реализации проектов находится по следующей формуле:

$$y = Ax^p - Bx, \tag{2}$$

где A и B – масштабные множители.

$$y = Bx \tag{3}$$

прямая среднего распределения проектов.

Дифференцирование уравнений (2) и (3) и их последующее решение дает возможность определить максимальную разницу в результате.

Максимум достигается при

$$x = \sqrt[m-n]{\left(\frac{An}{Bm}\right)^m} \tag{4}$$

$$y = A\left(\frac{An}{Bm}\right)^{\frac{n}{m-n}} - B\left(\frac{An}{Bm}\right)^{\frac{m}{m-n}} =$$

$$= A\left(\frac{An}{Bm}\right)^{\frac{n}{m-n}}\left[1 - \frac{B}{A}\left(\frac{An}{Bm}\right)\right]. \tag{5}$$

Пример практических расчетов по разности выигрыша между наилучшим и средним вариантами выбора проектов приведён на рис. 4.

Производная уравнения (2) отрицательна, кривая выпукла вверх.

Для случая $n = 1, m = 2,\ p = \frac{1}{2}$ выигрыш между оптимальной и средней кривыми будет иметь следующий вид:

$$y = A\sqrt{x} - Bx, \tag{6}$$

где A и B – масштабные множители.

На рис. 2 это область между кривой и прямой линиями.

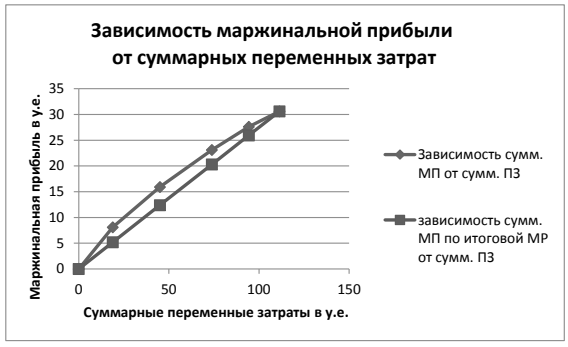


Рис. 2. Зависимость максимальной и средней маржинальной прибыли от суммарных переменных затрат

Максимум достигается при

$$x = \frac{A^2}{4B^2},\ y = \frac{A^2}{4B}. \quad (7)$$

Для полноты рассмотрим еще один случай, а именно: разницу между наилучшим и наихудшим распределением проектов (кривые 1 и 2 на рис. 1).

В общем виде функция кривой 2 носит степенной характер, степень больше единицы (функция кривой 2 является обратной к функции кривой 1). Функция кривой 2 имеет следующий вид:

$$y = Bx^{\frac{m}{n}}. \quad (8)$$

Тогда функция разности между прямой и обратной функциями будет иметь вид:

$$y = Ax^{\frac{n}{m}} - Bx^{\frac{m}{n}}. \quad (9)$$

Дифференцирование уравнений (8) и (9) дает возможность определить координаты точки максимума:

$$x = \sqrt[\frac{mn}{m^2-n^2}]{\frac{An^2}{Bm^2}}, \quad (10)$$

$$y = A\left(\frac{An^2}{Bm^2}\right)^{\frac{m^2-n^2}{n^2}}\left[1-\frac{B}{A}\left(\frac{An^2}{Bm^2}\right)^{\frac{\left(m^2-n^2\right)^2}{m^2n^2}}\right]. \quad (11)$$

Результаты практических расчетов по фактическим опытным данным по разности выигрыша между наилучшим и средним и наилучшим и наихудшим вариантами выбора очередности финансирования проектов приведены на рис. 3 и 4, соответственно.

Производная уравнения (9) отрицательна, кривая выпукла вверх.

Алгоритм выбора выгодного ассортимента

Шаг 0. (Подготовительный). Составляется таблица, куда заносятся результаты всех последующих шагов.

Пример построения таблицы – по алгоритму (см. табл. 1). В таблицу уже внесены данные пяти проектов.

Шаг 1. Формируется перечень бизнес-проектов. Графа 1.

Шаг 2. Для каждого бизнес-проекта рассчитывается ожидаемая выручка в течение заранее заданного срока. Графа 2.

Шаг 3. Определяется процент маржинальной прибыли в выручке. Графа 3.

Шаг 4. Рассчитывается величина маржинальной прибыли для каждого бизнес-проекта (результат шага 2 умножается на результат шага 3). Графа 4.

Шаг 5. Для каждого бизнес-проекта рассчитываются переменные затраты (результат шага 2 – соответствующий результат шага 4). Графа 5.

Шаг 6. Рассчитывается маржинальная рентабельность для каждого бизнес-проекта (результат шага 4 делится на соответствующий результат шага 5). Графа 6.

Шаг 7. Ранжируются бизнес-проекты по данным шага 6. Графа 7.

Шаг 8. Расставляются в таблице бизнес-проекты согласно данным о ранжировании (графа 7) в порядке возрастания номеров.

Шаг 9. (Оптимальное распределение). Рассчитываются суммарные значения маржинальной прибыли (данные графы 4 после ранжирования выписываются для бизнес-проектов накопительным итогом). Графа 8.

Шаг 10. Рассчитываются суммарные значения переменных затрат (данные шага 5 выписываются для бизнес-проектов накопительным итогом). Графа 9.

Шаг 11. Рассчитывается средняя по всем проектам маржинальная рентабельность (данные графы 8 делятся на соответствующие данные графы 9). Графа 10.

Значение средней по всем финансируемым проектам маржинальной рентабельности есть последнее значение в графе 10.

Шаг 12. Значение средней по всем финансируемым проектам маржинальной рентабельности (последнее значение в графе 10) заносится во вспомогательную графу 11. Графа 11.

Шаг 13. (Неоптимальное распределение). Рассчитывается маржинальная прибыль для всего портфеля по средней маржинальной рентабельности (значение средней маржинальной рентабельности из графы 11 умножается на значения переменных затрат нарастающим итогом из графы 9, данные шага 10). Графа 12.

Шаг 14. Находится выигрыш маржинальной прибыли в зависимости от выбранной стратегии. Например, между лучшим и средним распределением проектов (рис. 3) при наличии дефицита финансирования. Из данных шага 9 (графа 8) вычитаются соответствующие значения данных шага 13 (графа 12). Расчеты выигрыша между лучшей и худшей стратегиями, между средней и худшей стратегиями показаны на рис. 4 и 5, соответственно.

Шаг 15. В графу 14 вносятся данные маркетологов о приросте выручки по рассматриваемым проектам. Графа 14.

Шаг 16. Строится параметрическая зависимость между изменением маржинальной рентабельности от проекта (данные графы 5 после

Таблица 1

Таблица для расчета выгодного ассортимента

Проекты	Выручка (тыс. у.е.)	МП, %	МП, тыс. у.е. (2*3)/100	ПЗ, тыс. у.е. (2-4)	МР, % (4/5)*100	Ранг	МП нарастающим итогом (тыс. у.е.)	ПЗ нарастающим итогом (тыс. у.е.)	МР нарастающим итогом (8/9) *100%	Итоговая средняя МР, %	МП средняя нарастающим итогом (тыс. у.е.) (9*11)	Выигрыш МП между лучшим и средним выборами проектов (тыс. у.е.) 8–12	Прогноз роста выручки (тыс. у.е.)
Проект 1	27	30	8	19	43	1	8	19	43	27	5	3	40
Проект 2	34	23	8	26	30	2	16	45	35	27	12	4	35
Проект 3	36	20	7	29	25	3	23	74	31	27	20	3	40
Проект 4	25	18	5	21	22	4	28	94	29	27	26	2	50
Проект 5	20	15	3	17	18	5	31	111	27	27	31	0	15

Проект – мероприятия по выпуску конкретного ассортимента продукции;
У.е. – условные денежные единицы;
МП – маржинальная прибыль;
ПЗ – переменные затраты;
МР – маржинальная рентабельность

Рис. 3. Выигрыш лучшей ассортиментной стратегии по сравнению со средней

Рис. 4. Выигрыш лучшей ассортиментной стратегии по сравнению с худшей

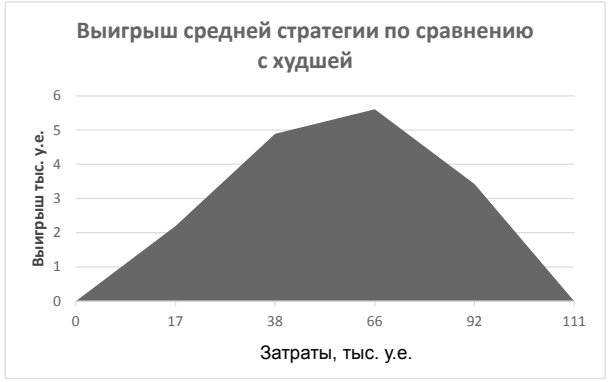


Рис 5. Выигрыш средней ассортиментной стратегии по сравнению с худшей

ранжирования). По левой (основной) вертикальной оси откладываются проценты, по основной горизонтальной оси откладываются наименования проектов после ранжирования. По второй (вспомогательной, правой) вертикальной оси откладываются данные соответствующих значений маржинальной прибыли, выручки и планируемой выручки по данным маркетологов (данные из соответствующих граф 2, 4, 14), рис. 6.

Как видно из табл. 1 и рис. 6, самыми выгодными проектами с точки зрения максимальной выручки являются 3 и 2. С точки зрения максимальной выручки (прогнозируемой) на будущий

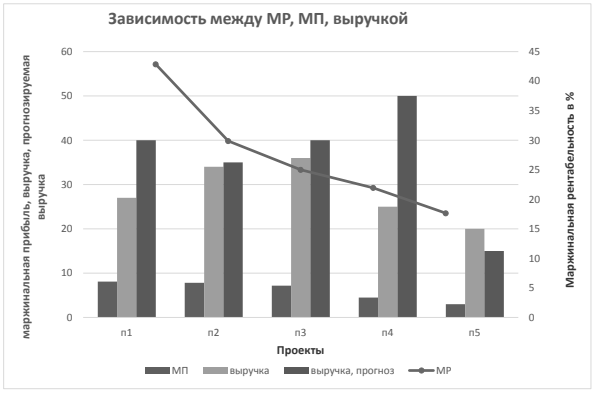


Рис. 6. Параметрическая зависимость между изменением маржинальной рентабельности от проекта

период лучшим является проект 4. С точки зрения максимальной маржинальной рентабельности (отдача по маржинальной прибыли на единицу вложения переменных затрат) лучшим является проект 1.

Предложенный алгоритм позволяет увеличить финансовые результаты без привлечения внешних заимствований. Для этого руководителю необходимо перебросить финасовые и материальные ресурсы с проектов 3, 4 и 5 в проекты 1 и 2 – до уровня достижения пределов продаж. Если после такого перераспределения средства еще останутся, то их следует вложить в следующий по маржинальной рентабельности проект. И так далее, пока не будут вложены все ресурсы.

Когда нет ограничений на затраты, результат финансирования одинаков по всем 120-ти вариантам выбора очередности запуска пяти проектов в производство.

Разница возникает при наличии дефицита финансирования. Если в наличии не 90 тыс. условных единиц, а 75 (дефицит бюджета 16,7%), то выбор проектов по способам 1 и 3 дают 40 тыс. у.е. маржинальной прибыли, а способ 2 – только 27 тыс. у.е., т.е. на 33,5% меньше (рис. 1).

Если дефицит составляет 50%, то способ 1 дает маржинальную прибыль 30 тыс. у.е., способ 3 – 20 тыс. у.е., а способ 2 – 12 тыс. у.е. Разница составляет 33% и 60%, соответственно (рис. 1).

Рентабельность и прибыль проекта зависят от способа разнесения постоянных затрат по всем проектам (например, пропорционально объему продаж или фонду заработной платы). Постоянные затраты меняются слабо от изменений объемов выпуска, поэтому сокращение по одному проекту приводит к росту затрат по другим проектам. В способе разнесения постоянных затрат заложена скрытая опасность, по формальным признакам в аутсайдерах может оказаться эффективный проект. При дефиците финансирования он будет закрыт [4]. Предложенный метод позволяет при наличии дефицита финансирования избежать закрытия проекта с большей маржинальной рентабельностью.

Литература

1. Отарашвили З.А., Печенов Ю.А. Повышение эффективности формирования и реализации ассортиментной политики как основа экономической безопасности компании // Спецтехника и связь. – 2012. – № 3. – С. 55–59.

2. Ириков В.А., Михеев В.А., Отарашвили З.А, Сушков Д.В. Разработка программы инновационного развития предприятия: методика, практика, рекомендации по внедрению / под ред. В.А. Ирикова. – М. : Логос: МЗ-Пресс, 2013. – 112 с.

3. Отарашвили З.А. Статическая и динамическая модели оценки бюджетной эффективности развития // Управление инновациями – 2011: материалы Международной научно-практической конференции / под ред. Р.М. Нижегородцева. – М. : Ленанд, 2011. – С. 409–411.

4. Тумбинская М.В. Организационное обеспечение процесса управления IT-инфраструктурой в системе защиты информации на предприятии // Национальные интересы: приоритеты и безопасность. – 2015. – № 1 (286). – С. 31–41.

Информатика и вычислительная техника

УДК 519.8

В.М. Сафонов[1]

МОДЕЛИ ОГРАНИЧЕННЫХ СЛУЧАЙНЫХ ВЕЛИЧИН В ЗАДАЧАХ ИДЕНТИФИКАЦИИ КЛАВИАТУРНОГО ПОЧЕРКА

Предлагается универсальная модель для аппроксимации законов распределений ограниченных случайных величин, используемая в исследовании для описания временных параметров клавиатурного почерка.

В статье предложено описание элементов клавиатурного почерка (продолжительность нажатия клавиши, период времени между нажатиями клавиш, период времени между отпусканием и нажатием следующей клавиши и т.д.), которые являются случайными величинами. Поскольку данные величины являются ограниченными, обоснована их аппроксимация бета-распределениями. Особенностью данного распределения является то, что оно описывает непрерывные случайные величины на ограниченном интервале.

Ключевые слова: *клавиатурный почерк, ограниченные случайные величины, закон распределения случайной величины, бета-распределение.*

V.M. Safonov

MODELS OF BOUNDED RANDOM VARIABLES IN PROBLEMS OF IDENTIFICATION OF HANDWRITING KEYBOARD

A universal model for the approximation of laws of distributions bounded random variables used in the study to describe the timing of keyboard handwriting is proposed

The article describes the elements of handwriting keyboard (pressing duration, time between keystrokes, time between releasing and pressing the next key, etc.), which are random variables. Since these values are limited, their approximation by beta distributions are justified. The peculiarity of this distribution is that it describes the continuous random variables in a limited range.

Keywords: *handwriting keyboard, limited random variables, law of random variable, beta distribution.*

Введение

В настоящее время актуальны задачи совершенствования систем аутентификации пользователей информационных систем (ИС), а также повышения результативности расследования компьютерных инцидентов. Одним из способов их решения является идентификация клавиатурного почерка (КП) пользователя ИС. Клавиатурный почерк – это поведенческие закономерности ввода конкретным оператором текста. КП фиксируется значениями биометрических характеристик. Такими характеристиками являются: продолжительность нажатия клавиши, период времени между нажатиями клавиш, период времени между отпусканием и нажатием следующей клавиши, среднее значение продолжительности нажатия клавиши, среднее квадратическое отклонение продолжительности нажатия клавиш и т.п. Совокупность значений этих характери-

[1] Адъюнкт кафедры математического и программного обеспечения Военно-космической академии им. А.Ф. Можайского.

стик, полученная при вводе текста оператором, является реализацией случайного вектора, а его распределение зависит от индивидуальных особенностей личности.

Как правило, большинство элементов рассматриваемого случайного вектора являются независимыми, а следовательно плотность распределения случайного вектора может быть представлена произведением плотностей распределения отдельных его элементов. Для описания закона распределения такого случайного вектора необходимо использовать законы распределения элементов вектора, которые могут быть получены на основе обработки зарегистрированных характеристик клавиатурного почерка. Носители распределения указанных характеристик принципиально ограничены, поэтому представляется целесообразным искать аппроксимирующие распределения в классе распределений ограниченных случайных величин (СВел).

Анализ форм кривых бета-распределения привел к выводу о том, что именно с его помощью удобно аппроксимировать большинство законов распределения (ЗакРас) ограниченных СВел.

Плотность $\phi_{\hat{x}}(x)$ и функция $F_{\hat{x}}(x)$ четырёхпараметрического бета-распределения определяются следующими выражениями [1]:

$$\phi_{\hat{x}}(x)=\phi_{\hat{x}}^{[B]}(x;a,b,\alpha,\beta)=$$

$$=\frac{(x-a)^{\alpha}(b-x)^{\beta}}{B(\alpha+1,\beta+1)(b-a)^{\alpha+\beta+1}}\Pi(x;a,b), \quad (1)$$

$$F_{\hat{x}}(x)=F_{\hat{x}}^{[B]}(x;a,b,\alpha,\beta)=\int_{-\infty}^{x}\phi_{\hat{x}}^{[B]}(x';a,b,\alpha,\beta)dx'=$$

$$=\int_{-\infty}^{x}\frac{(x'-a)^{\alpha}(b-x')^{\beta}\,dx'}{B(\alpha+1,\beta+1)(b-a)^{\alpha+\beta+1}}, \quad (2)$$

где $\hat{x}$ – случайная величина ($\wedge$ – символ случайного объекта); $a < b$; $a, b \in (-\infty, \infty)$ – параметры положения распределения (минимальное и максимальное значения СВел); $\alpha \geq -1$, $\beta \geq -1$ – параметры формы распределения; $B(\alpha+1,\beta+1)=$

$=\int_0^1 v^{\alpha}(1-v)^{\beta}\,dv=\frac{\Gamma(\alpha+1)\Gamma(\beta+1)}{\Gamma(\alpha+\beta+2)}$ – интеграл Эйлера первого рода; $\Gamma(z)=\int_0^{\infty}t^{z-1}e^{-t}dt$ – интеграл Эйлера второго рода (гамма-функция) при z, являющимся натуральным числом $\Gamma(z)=(z-1)!$;

$\Pi(x;a,b)=\begin{cases}0, \text{ при } x<a \text{ или } x\geq b\\ 1, \text{ при } a\leq x<b\end{cases}$ – селектор интервала.

При $a = 0$; $b = 1 \Rightarrow b - a = 1 \Rightarrow$

$$\Rightarrow \phi_{\hat{x}_0}(x)=\phi_{\hat{x}}^{[B]}(x;0,1,\alpha,\beta)=$$

$$=\frac{x^{\alpha}(1-x)^{\beta}}{B(\alpha+1,\beta+1)}\Pi(x;0,1), \quad (3)$$

$$F_{\hat{x}_0}(x)=F_{\hat{x}}^{[B]}(x;0,1,\alpha,\beta)=$$

$$=\int_{-\infty}^{x}\phi_{\hat{x}}^{[B]}(x';0,1,\alpha,\beta)dx'\cdot\Pi(x;0,1)+\Delta(x-1)= \quad (4)$$

$$=\int_0^x\frac{x'^{\alpha}(1-x')^{\beta}\,dx'}{B(\alpha+1,\beta+1)}\cdot\Pi(x;0,1)+\Delta(x-1),$$

где $\hat{x}_0$ – нормированная по величине $(b - a)$ размаха выборки СВел $\hat{x}$;

$\Delta(x-d)=\begin{cases}0, \text{ при } x<d\\ 1, \text{ при } x\geq d\end{cases}$ – селектор луча.

Бета-распределение с плотностью (3) и функцией (4) называется каноническим [2]. Примеры графиков его плотностей для различных значений α и β приведены на рис. 1.

Приведенные графики плотностей распределений показывают широкие возможности предлагаемой модели по аппроксимации ЗакРас, наблюдаемых в природе СВел. Как видно из приведенных примеров, универсальность бета-распределения позволяет аппроксимировать ЗакРас практически всех наблюдаемых в природе СВел, которые являются ограниченными в силу закономерностей процесса их измерения исследователем. Таким образом, в автоматизированных системах, использующих законы распределения, возможно описывать законы распределения только моделью бета-распределения.

Параметры ЗакРас бета-распределения легко определяются на основе следующих выражений [3]:

$$\tilde{\alpha}=\tilde{M}[\hat{x}_0]\left[\frac{\tilde{M}[\hat{x}_0](1-\tilde{M}[\hat{x}_0])}{\tilde{M}[\hat{x}_0^2]-\tilde{M}^2[\hat{x}_0]}-1\right]-1, \quad (5)$$

$$\tilde{\beta}=(1-\tilde{M}[\hat{x}_0])\left[\frac{\tilde{M}[\hat{x}_0](1-\tilde{M}[\hat{x}_0])}{\tilde{M}[\hat{x}_0^2]-\tilde{M}^2[\hat{x}_0]}-1\right]-1, \quad (6)$$

где $\tilde{M}[\hat{x}_0]$; $\tilde{M}[\hat{x}_0^2]$ – оценки первого и второго начальных моментов распределения СВел $\hat{x}_0$, связанной с СВел $\hat{x}$ следующим соотношением:

$$\hat{x}=(b-a)\hat{x}_0+a. \quad (7)$$

Отметим, что СВел $\hat{x}_0$ подчинена каноническому бета-распределению на интервале $[0,1)$. В программах Mathcad, Microsoft Excel приведены встроенные плотности и функции распределе-

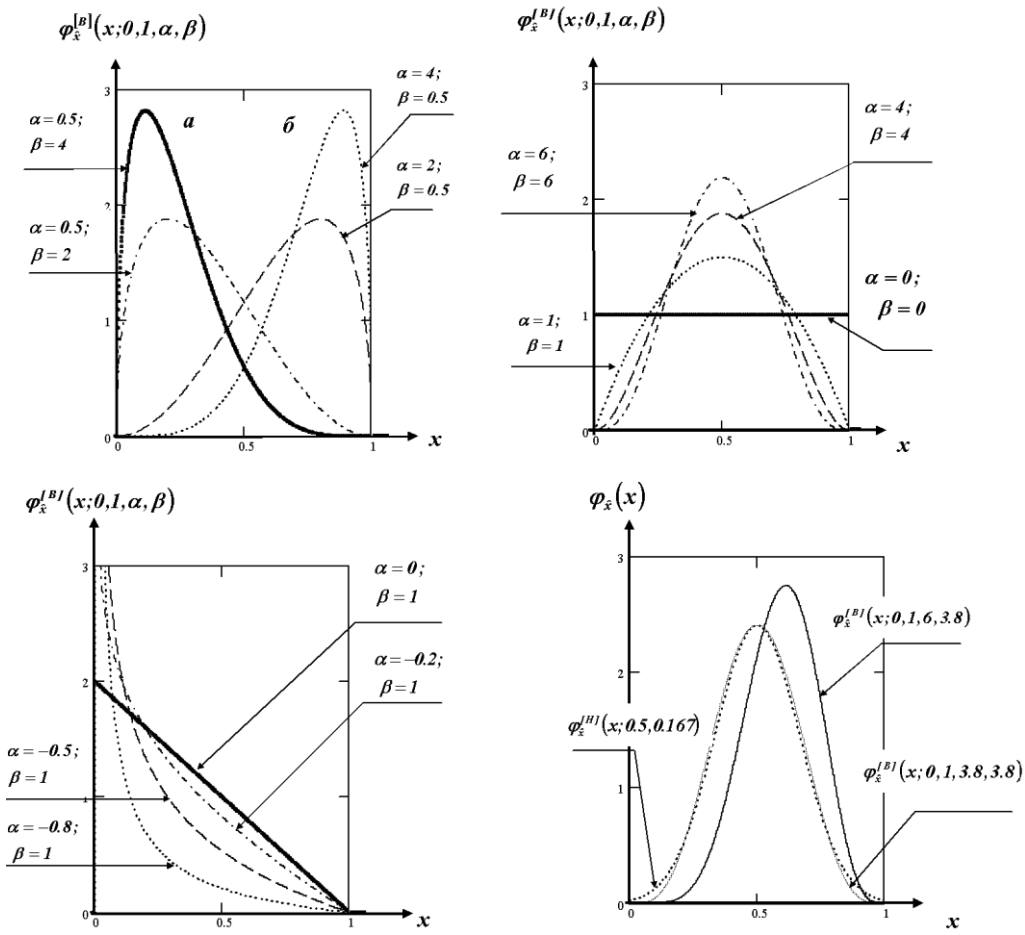


Рис. 1. Семейства кривых канонического бета-распределения, определяемых сочетаниями параметров форм α и β

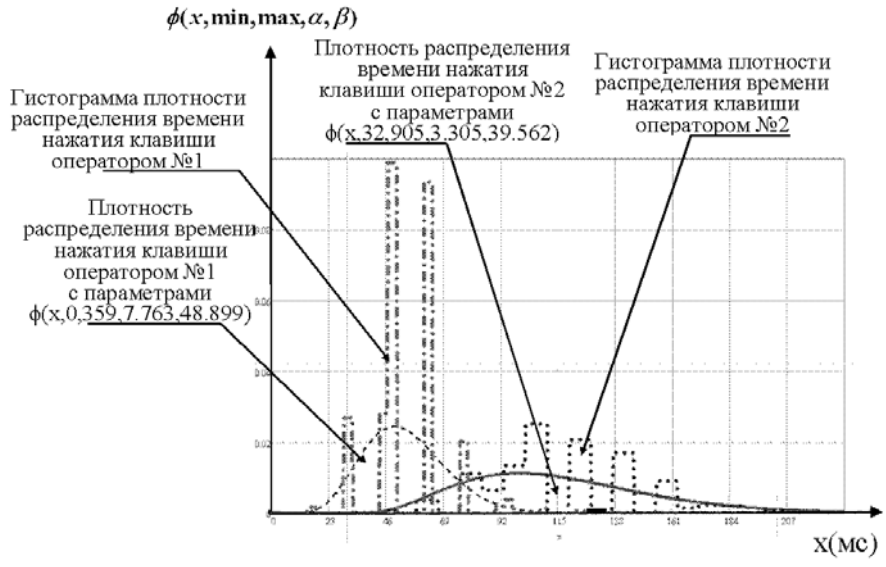


Рис. 2. Гистограммы плотностей распределения и аппроксимации бета-распределением случайных продолжительностей нажатия клавиш (для двух операторов)

ния именно канонического бета-распределения. Следует учитывать, что коэффициенты (α_1, β_1) форм в данных программах связаны с коэффициентами (α, β) форм (в данной статье) следующими соотношениями:

$$\alpha_1 = \alpha + 1, \quad \beta_1 = \beta + 1. \qquad (8)$$

Выражение, связывающее плотности произвольно бета-распределенной СВел $\hat{x}$ и связанной с ней канонической СВел $\hat{x}_0$, имеет вид

$$\varphi_{\hat{x}}(x; a, b, \alpha, \beta) = \frac{1}{b-a}\varphi_{\hat{x}_0}\left(\frac{x-a}{b-a}; 0, 1, \alpha, \beta\right) =$$

$$= \frac{1}{b-a}\varphi_{\hat{x}_0}^{[Mathcad]}\left(\frac{x-a}{b-a}; \alpha+1, \beta+1\right). \qquad (9)$$

На рис. 2 приведены графики гистограмм плотностей распределений СВел продолжительностей нажатия клавиш для двух различных операторов. Там же приведены графики аппроксимаций бета-распределениями. Эффект «отдельно стоящих столбов гистограмм» вызван дискретностью сообщений таймера. Поскольку продолжительность нажатия клавиши является непрерывной СВел, применение бета-распределения будет более адекватно описывать данную СВел.

Заметим, что при накоплении статистики в течение длительного срока нет необходимости хранить всю выборку. Целесообразно хранить текущие параметры бета-распределения и объём выборки [4]. Так при появлении нового члена x_{m+1} исходной выборки несложно откорректировать параметры (a, b, α, β) бета-распределения по следующей схеме. Определяются значения $\tilde{M}[\hat{x}_0]; \tilde{M}[\hat{x}_0^2]$, соответствующие объему выборки m. Уточняются параметры положения

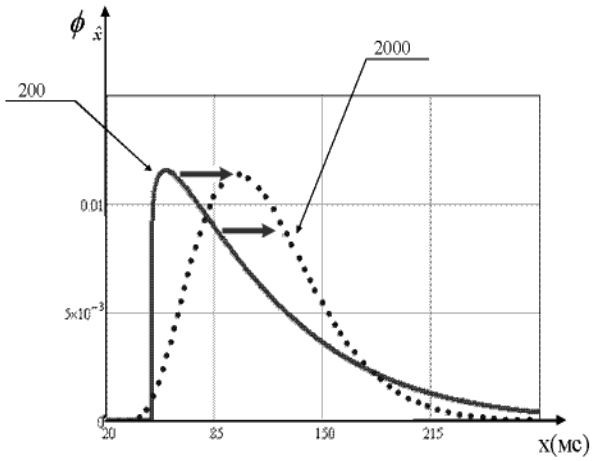


Рис. 3. Уточнение плотностей распределения СВел при продолжительности нажатия клавиши при фиксации 200 и 2000 нажатий

распределения по тому, попадает ли x_{m+1} в интервал [a, b]. Затем уточняются оценки упомянутых математических ожиданий для объема выборки $m + 1$. Далее с использованием выражений (5)–(6) определяются оценки (α, β), соответствующие объему выборки $m + 1$.

На рис. 3 приведены графики аппроксимаций бета-распределением при различных объемах выборки при ее накоплении.

На рис. 4 приведены совмещенные двумерные плотности распределения случайных векторов $\langle \hat{x}, \hat{y} \rangle$ разных операторов, где СВел $\hat{x}$ – это продолжительность нажатия клавиши, а $\hat{y}$ – это период времени между нажатиями клавиш. Поскольку коэффициент корреляции между $\hat{x}$ и $\hat{y}$ близок к нулю, следовательно, эти СВел можно считать независимыми, поэтому аппроксимация двумерного бета-распределения для оператора № 1 будет иметь вид

$$\varphi_{\langle \hat{x}, \hat{y} \rangle}(x, y) = \varphi_{\hat{x}}\left(\frac{x-a}{b-a}; 0, 1, \alpha, \beta\right) \times$$

$$\times \varphi_{\hat{y}}\left(\frac{y-a}{b-a}; 0, 1, \alpha, \beta\right). \qquad (10)$$

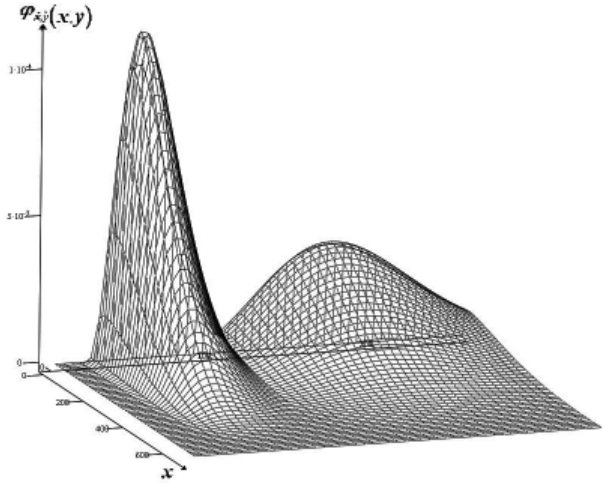


Рис. 4. Графики двумерных ЗакРас случайного вектора $\langle \hat{x}, \hat{y} \rangle$ различных операторов

Области расположения двумерного признака для приведенного случая различаются существенно, что позволяет легко идентифицировать этих операторов с использованием методов теории статистического принятия решения. Однако на практике, в условиях большого числа операторов, решение задачи идентификации пользователя по клавиатурному почерку сопряжено с большими трудностями. Но описание решения этой задачи не является целью данной статьи.

Заключение

На основании вышесказанного можно сделать следующие выводы.

1. Универсальность бета-распределения позволяет аппроксимировать законы распределения практически всех наблюдаемых в природе случайных величин.

2. В системах идентификации клавиатурного почерка успешно апробирована технология аппроксимации законов распределения четырёхпараметрического бета-распределения.

3. Использование программного модуля идентификации параметров закона распределения случайных величин в классе бета-распределений позволит унифицировать задачу аппроксимации закона распределения в программных средствах, а в случае адаптации закона к изменяющейся исходной выборке значительно сократит необходимый объем памяти для ее хранения.

Литература

1. Айвазян С.А. и др. Прикладная статистика: основы моделирования и первичная обработка данных : справочное пособие. – М. : Финансы и статистика, 1983. – 471 с.

2. Петухов Г.Б., Девяткин А.М., Якунин В.И. Идентифицирование законов распределений ограниченных случайных величин. – СПб. : ВКА, 2005. – 30 с.

3. Петухов Г.Б., Якунин В.И. Моделирование случайных ситуационных характеристик на авиационных тренажёрах / Г.Б. Петухов, В.И. Якунин // Изв. ВУЗов. Приборостроение. – 2007. – № 3 – С. 7–11.

4. Маков А.Б., Суворов С.С., Кулешов Ю.В. Динамико-стохастический подход в задачах адаптации методов прогнозирования опасных явлений / А.Б. Маков, С.С. Суворов, Ю.В. Кулешов // Вестник Санкт-Петербургского университета. – СПб. : СПБГУ, 2008. – Сер. № 7. – № 4.

УДК 004.65

П.Е. Котиков[1]
А.А. Нечай[2]

РЕШЕНИЕ ПРОБЛЕМЫ УПРАВЛЕНИЯ ПАРАЛЛЕЛЬНЫМ ВЫПОЛНЕНИЕМ ТРАНЗАКЦИЙ В РАСПРЕДЕЛЕННЫХ БАЗАХ ДАННЫХ ДЛЯ УСТРАНЕНИЯ ОПАСНОЙ ПРОТИВОРЕЧИВОСТИ

Данная статья посвящена проблеме организации распределенных запросов и транзакций в распределенных гетерогенных базах данных геоинформационных систем. Показаны некоторые сложности управления параллельным выполнением и возможные решения.

Ключевые слова: *геоинформационная система, гетерогенные базы данных, транзакция.*

P.E. Kotikov
A.A. Nechay

SOLUTION TO THE PROBLEM OF CONCURRENCY CONTROL IN DISTRIBUTED DATABASE TRANSACTIONS TO ELIMINATE DANGEROUS INCONSISTENCY

This article deals with the problem of distributed queries and distributed transactions across heterogeneous databases of geographic information systems. Some complexities of concurrency management and their possible solutions are presented.

Keywords: *geographic information system, heterogeneous database, transaction.*

Одной из наиболее ценных возможностей при применении гетерогенных распределенных баз данных (БД) является возможность выполнения распределенных запросов [1; 4]. Такую возможность – выполнять распределенный запрос – предоставляет только полностью распределенная база данных, поскольку здесь возможно:

1) разбить базу данных на несколько фрагментов;

2) ссылаться на один или более таких фрагментов из одного запроса, используя прозрачность фрагментации;

3) обеспечить возможность в одном запросе обращаться к физически разделенной таблице.

Во всех случаях прозрачность транзакций остается свойством системы управления распределенной базы данных, которое гарантирует, что все транзакции БД будут обеспечивать целостность и непротиворечивость базы данных. В случае распределенной базы данных геоинформационной системы, транзакции БД могут обновлять данные, хранящиеся на различных компьютерах, объединенных в сеть. Свойство прозрачности транзакций будет гарантировать, что транзакция будет завершена только в том случае, если на всех сайтах базы данных, вовлеченных в транзакцию, будут завершены все части транзакции. В системах распределенных баз данных для управления транзакциями и обеспечения целостности и непротиворечивости базы данных, как правило, используется сложный механизм распределенных транзакций и распределенных запросов. Также сложным становится само управление параллельным выполнением в распределенной среде. Несмотря на известность этого факта, на практике он не привлекает должного внимания, вплоть до возникновения проблем при проектировании [2; 4].

Вне зависимости от того, является ли транзакция распределенной или нет, она формируется на базе одного или нескольких запросов. Основное отличие нераспределенных транзакций от распределенных состоит только в том, что последние могут обновлять или запрашивать данные на нескольких удаленных сайтах сети. Распределенная транзакция (distributed transaction) позволяет ссылаться на несколько различных локальных или удаленных сайтов. При этом каждый простой запрос может ссылаться только на один удаленный сайт, а транзак-

[1] Кандидат технических наук, доцент Военно-космической академии им. А.Ф. Можайского.

[2] Преподаватель Военно-космической академии им. А.Ф. Можайского.

ция в целом может ссылаться на несколько сайтов, поскольку каждый запрос сам по себе может ссылаться на различные сайты. Распределенный запрос (distributed request) позволяет получать данные от нескольких удаленных сайтов. Поскольку каждый запрос может получать доступ к данным, расположенным более чем на одном сайте, транзакция может получать доступ к нескольким сайтам [3].

Размещение и разбиение данных должно быть прозрачно для конечного пользователя. Свойство прозрачности транзакций гарантирует, что все транзакции можно рассматривать как централизованные, а также обеспечивает их сериализуемость, т.е. одновременное выполнение транзакций. Это значит, что независимо от того, являются они распределенными или нет, база данных будет переходить из одного устойчивого состояния в другое.

Исключительно важным становится механизм управления параллельным выполнением из-за возможной противоречивости [5]. Управление параллельным выполнением становится особенно значимым в среде распределенной базы данных, поскольку многоместные (на нескольких сайтах) и многопроцессорные операции с большей вероятностью могут привести к противоречивости данных и тупикам, чем одноместные (выполняющиеся на одном сайте) системы [6]. Компонент TP (процессор транзакций) системы управления распределенной БД должен гарантировать, что все части транзакции на всех сайтах будут завершены до того, как последний оператор COMMIT завершит всю транзакцию в целом. Предположим, что каждая операция транзакции подтверждалась локальным процессором данных (DP), но один из DP не смог записать результаты транзакции. Это может привести к противоречивому состоянию БД и неизбежным проблемам с целостностью, поскольку невозможно отменить уже записанные данные.

Решение проблемы состоит в использовании протокола двухфазного подтверждения транзакции (two-phase commit protocol) [3; 5]. Централизованной базе данных необходим только один процессор данных (DP). Все операции с базой данных проводятся на одном сайте, и последовательность операций сразу становится известна. Распределенные базы данных позволяют транзакциям осуществлять доступ к данным на нескольких сайтах. В этих случаях завершающий оператор COMMIT не должен выполняться до тех пор, пока каждый сайт не завершит свою часть транзакции. Протокол двухфазного подтверждения транзакции требует, чтобы каждая запись в журнале транзакций процессора данных выполнялась до фактического обновления фрагмента. В этом и есть его главная роль. Протокол двухфазного подтверждения транзакции требует применения протокола «выполнить-отменить-повторить» и протокола упреждающей записи. Протокол DO-UNDO-REDO используется процессором данных для отката транзакций назад (roll back) или отката транзакций вперед (roll forward) на основе записей. Чтобы гарантировать, что операции DO-UNDO-REDO смогут обеспечить корректное выполнение операций при крахе системы, используется протокол упреждающей записи. Протокол упреждающей записи (write-ahead protocol) принуждает фиксировать в журнале запись данных для постоянного хранения перед фактическим выполнением этой операции. Протокол двухфазного подтверждения транзакции определяет операции между двумя типами узлов: узел-координатор (coordinator) и один или более подчиненных узлов-субординаторов (subordinates), или когорт (cohort). Протокол реализуется в две фазы.

Фаза 1. Подготовка

1. Координатор посылает сообщение PREPARE TO COMMIT (подготовка к завершению) всем субординаторам.

2. Субординаторы получают сообщение, записывают информацию в журнал транзакций в соответствии с протоколом упреждающей записи и посылают координатору уведомление YES/PREPARED TO COMMIT (да/завершение подготовлено) или NO/NOT PREPARED (нет/завершение не готово).

3. Координатор убеждается, что все узлы готовы к завершению, или в противном случае отменяет действие.

Если все узлы сообщили, что они готовы к завершению (PREPARED TO COMMIT), транзакция переходит в фазу 2. Если один или более узлов отвечают, что они не готовы (NO или NOT PREPARED), координатор распространяет среди всех субординаторов сообщение ABORT (прекращение).

Фаза 2. Последний оператор COMMIT

1. Координатор оповещает всех субординаторов, рассылая сообщение COMMIT, и ожидает ответа.

2. Каждый субординатор, получив сообщение COMMIT, обновляет базу данных в соответствии с протоколом DO.

3. Субординаторы отвечают координатору сообщением COMMITED (завершено) или NOT COMMITED (не завершено).

Если один или более субординаторов не вы-

полнили операцию завершения, координатор рассылает сообщение ABORT и тем самым инициирует операцию UNDO (отмену всех изменений).

Цель протокола двухфазного подтверждения транзакции состоит в обеспечении корректного завершения всеми узлами своих частей транзакции; в противном случае транзакция отменяется. Если один или более узлов не выполняют операцию завершения, то необходимая информация по восстановлению БД будет находиться в журнале транзакций, и база данных может быть восстановлена с помощью протокола DO-UNDO-REDO.

Таким образом, реализация возможности организации распределенных запросов к распределенным базам данных ГИС связана не только с безусловным выполнением требований прозрачности, но и с необходимостью решения проблемы управления параллельным выполнением транзакций в распределенной среде.

Возможным решением является использование протокола двухфазного подтверждения транзакций.

Литература

1. Колбина О.Н Современные и теоретические аспекты управления распределёнными базами данных / О.Н. Колбина, Е.П. Истомин // Информационные технологиии системы: управление, экономика, транспорт, право : сборник научных трудов. – СПб. : ООО «Андреевский издательный дом», 2011. – Вып. 1(9).

2. Колбина О.И Применение распределённых баз данных в геоинформационных системах прогнозирования георисков / Е.П. Истомин, О.Н. Колбина, Е.М. Зоринова // Сборник трудов Международной научно-практической конференции «Инфогео-2013». – СПб. : ООО «Андреевский издательский дом», 2013.

3. Миков А.И., Замятина Е.Б. Распределенные системы и алгоритмы / А.И. Миков, Е.Б. Замятина. – М. : ИНТУИТ, 2008. – 287 с.

4. Разработка и развитие методов, моделей и систем геоинформационного управления пространственно-распределенными объектами: отчет о НИР / Е.П. Истомин, А.Г. Соколов, О.Н. Колбина. – СПб. : Российский государственный гидрометеорологический университет, 2013. – 102 с.

5. Роб П., Коронел К. Системы баз данных: проектирование, реализация и управление. – 5-е изд., перераб. и доп. / пер. с англ. – СПб. : БХВ-Петербург, 2004. – 1040 с.

6. Лохвицкий В.А. Подход к построению системы автоматизированной интеграции информации в базу данных для её своевременной актуализации / В.А. Лохвицкий, С.В. Калиниченко, А.А. Нечай // Мир современной науки. – 2014. – № 2 (24). – С. 8–12.

7. Нечай А.А. Выявление недекларированных возможностей аппаратно-программного обеспечения / А.А. Нечай // Экономика и социум. – 2014. – № 1–2 (10). – С. 457–460.

8. Нечай А.А. Специфика проявления уязвимостей в автоматизированных системах управления критически важными объектами / А.А. Нечай, П.Е. Котиков // Современные тенденции в образовании и науке : сборник научных трудов по материалам Международной научно-практической конференции: в 14 частях. – Тамбов, 2014. – С. 96–97.

9. Клименко И.С. К исследованию феномена информации / И.С. Клименко, Л.В. Шарапова // Вестник Российского нового университета. – 2014. – Вып. 4. – С. 141–148.

УДК 004.056

А.А. Нечай[1]
П.Е. Котиков[2]

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СОВРЕМЕННЫХ АВТОМАТИЧЕСКИХ ТЕЛЕФОННЫХ СТАНЦИЯХ

Статья посвящена актуальному вопросу, обозначенному в заголовке. Представлен анализ влияния применения достижений цифровой техники в АТС на защищенность информации. Наиболее подробно освещены варианты сценариев информационных атак. Ценным является также рассмотрение конкретных технологий информационного воздействия.

Ключевые слова: *АТС (автоматическая телефонная станция), информация, цифровая обработка, защищенность информации, цифровая схема.*

A.A. Nechai
P.E. Kotikov

ACTUAL PROBLEMS OF INFORMATION PROTECTION IN MODERN AUTOMATIC TELEPHONE STATIONS

The article is devoted to the topical issue, marked in the headline. The analysis of effect of applications of digital technology in automatic telephone-exchange on secure information is presented. The scenarios of information attaks are highlighted in details. Valuable is also the consideration of specific technologies of informational influence.

Keywords: *ATE (automatic telephone-exchange), information, digital processing, information security, digital circuit.*

Успехи микропроцессорных технологий привели к массовому переходу автоматических телефонных станций (АТС) на цифровую обработку вызовов. Более того, непосредственно в настоящий момент наблюдается еще один качественный переход в области ведомственной телефонии – от «традиционных» цифровых АТС к IP-телефонии. При этом пропорции всех трех технологий (аналоговая, цифровая, IP-телефония) практически сравнялись.

Цифровая схема передачи сообщений (как управляющих, так и голосовых) на практике не только не устраняет характерные для традиционных схем угрозы, но и порождает целые классы новых угроз нарушения конфиденциальности. Пожалуй, единственным преимуществом цифровой (в том числе IP-) обработки голоса в этом аспекте является потенциальная готовность схемы к прозрачному внедрению программных средств криптографической защиты речевой информации. Однако этот процесс в отношении УАТС общего (неспециального) назначения только начинает свое развитие.

Существует множество механизмов осуществления атак на АТС. При этом задачи, преследуемые нарушителями, могут сильно отличаться, а именно:

– получение коммерческого эффекта от воровства услуг телефонных переговоров;

– осуществление скрытого съема информации, содержащей коммерческую или государственную тайну;

– выведение оборудования телефонной сети из строя.

Наибольшую опасность может представлять несанкционированный доступ злоумышленников к программным портам АТС через внешние каналы телефонной связи. Для осуществления указанных действий в программное обеспечение телефонных станций встраиваются скрытые мо-

[1] Преподаватель Военно-космической академии им. А.Ф. Можайского.

[2] Кандидат технических наук, доцент Военно-космической академии им. А.Ф. Можайского.

дули («закладки»). Командами запуска «закладок» могут являться специальные сообщения, скрытно передаваемые по служебным или пользовательским каналам. В результате реализации указанных действий злоумышленник получает полный контроль над АТС, включая возможность дистанционного съема информации и полного вывода оборудования из строя. В мировой и отечественной практике существует множество реальных фактов обнаружения «закладок» в коммутационном оборудовании зарубежного производства (информация о некоторых из них приведена в СМИ).

Закладки, реализующие упомянутые функции, весьма сложно выявить. Гарантию того, что в коммутационных станциях отсутствуют недекларированные возможности, может дать экспертиза их принципиальных схем и исходных текстов ПО, которая проводится только при сертификации изделий.

Выделим и опишем следующие типовые угрозы цифровых и IP- АТС информатизации:

1. Подключение в пределах коммутационной матрицы

Цифровая обработка сигналов дает возможность копирования («ответвления») голосового трафика в пределах коммутационной матрицы без каких бы то ни было демаскирующих признаков. Факт копирования невозможно отследить, он не вызывает ни изменений в амплитуде передаваемого сигнала, ни искажений, связанных с задержкой передачи. Это является качественным отличием цифровых систем телефонии от систем предыдущего поколения.

Практически все крупные разработчики оборудования для УАТС реализовали в программном обеспечении те или иные возможности копирования речевого трафика при наличии у прослушивающей стороны соответствующих полномочий, определенных администратором телефонной станции. В некоторых случаях это полноценная трехсторонняя конференцсвязь с отключенным входящим голосовым каналом от прослушивающей стороны, в других – ответвление потока по специальной схеме при наборе определенного номера. Некоторые исследователи в области информационной безопасности отдельно выделяют так называемый полицейский режим – возможность выполнения тех же операций извне при наборе из городской телефонной сети определенного номера, принадлежащего номерному полю УАТС, и кода допуска. Рассмотрим реализацию данных технологий в некоторых широко распространенных моделях телефонных станций.

Цифровые учрежденческие АТС модели AVAYA Definity реализуют возможность скрытого копирования речевой информации в рамках возможности “Service Observing” (контроль вызова), позиционируемой как средство для контроля со стороны менеджеров за ходом работы телефонных операторов, в первую очередь – в центрах обработки вызовов. Активация функции возможна как в варианте с подачей в речевой канал каждые 12 секунд предупредительного сигнала о факте прослушивания третьей стороной, так и без него. Настройка полномочий на прослушивание выполняется с консоли администратора по групповому принципу: каждой абонентской линии соотносится класс приоритетов “COR”, а в матричной форме для каждой пары классов определяется разрешение или запрет прослушивания. Активация прослушивания выполняется набором кода доступа к сервису, а затем номера абонента, и может быть назначена на одну из функциональных клавиш прослушивающего аппарата. Кроме того, при определенной настройке возможен доступ к функции с внешних линий, например с городской телефонной сети.

Сервер IP-телефонии CallManager от компании Cisco Systems Inc. также предоставляет возможность включения в разговор третьего абонента, обладающего достаточными полномочиями (как с предупредительным сигналом, так и без него). Функция именуется “Barge In” и имеет две различные схемы технической реализации:

1). Схема на основе программно-аппаратных средств, штатно встроенных во все IP-аппараты компании с двумя линиями. Прослушиваемый IP-аппарат при поступлении запроса на конференцсвязь (в том числе одностороннюю – прослушивание) самостоятельно выполняет ответвление и микширование двух голосовых потоков (первичного – в направлении абонента и вторичного – в направлении прослушивающего устройства) аппаратными средствами второй линии. При этом при соответствующей настройке предупредительных сигналов в первичный голосовой поток не добавляется, более того, на дисплее прослушиваемого IP-аппарата не появляется никаких информационных признаков о факте подключения. Данная схема ограничена только одним подключением прослушивания и только широкополосным (64 кбит/с) кодеком G.711, однако не вносит никаких демаскирующих искажений в голосовой поток.

2). Схема на основе выделенных программно-аппаратных средств конференц-связи сервера

IP-телефонии. При поступлении запроса сервер IP-телефонии замыкает голосовой трафик в обоих направлениях (проходивший до этого момента напрямую между IP-устройствами) на устройство конференцсвязи и с его помощью выполняет микширование и ответвление данных (в этом случае уже на неограниченное количество прослушивающих устройств и вне зависимости от используемого абонентами кодека). Недостатком схемы по сравнению с первым вариантом является слышимое искажение («провал голоса») в момент переключения потоков.

Настройка привилегий на прослушивание выполняется отдельно для каждой прослушиваемой линии (непосредственно указывается набор линий, имеющих право на подключение, в т.ч. незаметное, к разговору).

Таким образом, получение злоумышленником тем или иным образом привилегий администратора цифровой УАТС (например, посредством успешной атаки на его персональный компьютер) предоставляет ему практически неограниченные возможности по незаметному прослушиванию ведущих телефонных переговоров.

2. Прослушивание разговоров в помещении с помощью автоответа

Цифровые и IP-аппараты, как сложные компьютерные устройства, привнесли еще один класс угроз утечки речевой информации, связанный с возможностью удаленного (в том числе при некоторых условиях – несанкционированного) включения микрофона и передачи разговоров, ведущихся в помещении по цифровому каналу. В качестве первого рассмотрим вариант, не связанный с недокументированными возможностями самих аппаратов, – широко распространенную опцию «Автоответ». При ее активации вызываемый аппарат при поступлении вызова подает один (часто – укороченный) сигнал вызова, а затем автоматически включает микрофон и громкоговоритель, с тем чтобы абоненты имели возможность общаться между собой по громкой связи либо с использованием гарнитуры.

3. Наличие недокументированных возможностей

Недокументированные возможности самих аппаратов (в особенности IP-) являются еще одной угрозой для конфиденциальности речевой информации в защищаемых помещениях. Программное обеспечение IP-телефонов представляет собой сложный программный комплекс, в том числе реализующий стек протоколов TCP/IP, и может содержать:

– недокументированные возможности, внесенные разработчиками в целях тестирования или на определенных этапах разработки новых функциональных возможностей аппаратов;

– ошибки в реализации, например приводящие к уязвимостям класса «переполнение буфера» и позволяющие получить полный контроль над программным обеспечением аппарата до его перезагрузки.

Примером угрозы первой группы является имевшаяся в одной из версиЙ ПО возможность отправки на IP-телефоны наиболее популярных моделей 7940 и 7960 компании Cisco Systems Inc. управляющего XML-сообщения CiscoIPPhone-Execute, которое среди прочих возможностей (набор номера, эмуляция нажатия клавиш и т.п.) могло включать микрофон аппарата и передавать весь голосовой трафик на указанный в XML-сообщении IP-адрес.

4. Прослушивание IP-трафика при передаче по сети

Различные варианты реализаций угроз прослушивания трафика традиционны для компьютерных сетей, использующих в своей структуре широковещательные сегменты (Ethernet, в том числе коммутируемый, радио-Ethernet и т.п.), и создают еще один уровень возможных атак на системы IP-телефонии. При отсутствии шифрования трафика на сетевом или более высоких уровнях модели OSI существует несколько вариантов нарушения конфиденциальности передаваемых сообщений.

В условиях отсутствия у злоумышленника административных прав на активное сетевое оборудование наиболее эффективной в коммутируемых Ethernet-сетях является атака “ARP spoofing”, выполняющая изменение таблицы маршрутизации на канальном (MAC) уровне с помощью специально сформированных ARP-пакетов. Также к раскрытию определенной части передаваемой информации может привести перевод коммутатора в режим концентратора с помощью большого количества фальшивых пакетов (MAC storm), хотя этот способ и обладает значительными демаскирующими признаками, выражающимися в резком снижении качества работы сети.

При получении злоумышленником административных прав на коммутирующем или маршрутизирующем оборудовании (например, в результате атаки на компьютер администратора или при перехвате его пароля, передававшегося в открытом виде) у него появляются гораздо более мощные средства перехвата IP-трафика. Они включают:

• возможность активации на коммутаторах зеркальных (SPAN) портов, получающих точную

копию передаваемого по определенным портам трафика;

• использование иных технологий «ответвления» трафика от производителей сетевого оборудования, например:

– протокола ERSPAN (Encapsulated Remote SPAN), инкапсулирующего каждый перехватываемый пакет в пакет протокола GRE, что позволяет передавать его по IP-сетям без каких-либо ограничений дальности;

– опции IP Traffic Export, реализующей «ответвление» трафика при его маршрутизации на 3-ем уровне модели OSI;

– (оба протокола поддерживают возможность тонкой настройки фильтрации перехватываемых пакетов, что позволяет копировать трафик только от определенных групп IP-устройств).

Беспроводные сети при отсутствии стойких алгоритмов шифрования также являются потенциальным источником раскрытия передаваемого по ним голосового трафика.

5. Подмена сообщений в управляющем канале IP-телефонии

Методика централизованного управления IP-телефонными вызовами (реализуемая в УАТС) содержит еще один возможный путь прозрачного для абонентов перехвата их разговоров. В момент установления IP-соединения первоначальный обмен информацией, содержащей номера абонентов, их имена, технические возможности аппаратов и т.п., в том числе IP-адреса оконечных устройств, идет между серверами IP-телефонии. На этом этапе возможна подмена (средствами атак сетевого уровня) информации об одном или обоих IP-адресах с целью внедрения компьютера злоумышленника в цепочку передачи голосового трафика по принципу прозрачного прокси-сервера.

Подобный класс атак остается совершенно незаметным на прикладном уровне, так как пользователю обычно не видны сетевые координаты удаленного абонента, а стек протоколов не способен обнаружить факт подмены, и может быть выявлен только с помощью специализированного мониторинга сетевого трафика.

В целом предпосылкой для появления возможности подобных атак является то, что в современных протоколах IP-телефонии (H.323, SCCP и др.) оконечное оборудование при приеме и передаче голосового потока является ведомым относительно сервера УАТС и полностью полагается на информацию, сообщенную ему в управляющем канале (например, не проверяет соответствие IP-адресов отправителя и получателя голосового потока в рамках одного и того же разговора). Проблема обеспечения защиты от внедрения в голосовой поток прокси-сервера поднимает вопрос об обеспечении целостности передаваемых в управляющем канале данных стойкими криптографическими методами.

Выводы

1. Смена технологий в области телефонии для объектов информатизации от аналоговых к цифровым, а затем и к IP-устройствам породила ряд новых угроз конфиденциальности речевой информации, как передаваемой средствами УАТС, так и циркулирующей в помещениях с установленным оконечным телефонным оборудованием. Это требует разработки и внедрения новых методов, средств и методик контроля над режимом функционирования УАТС и их распределенных компонентов, а также приемов мониторинга несанкционированных воздействий и аномалий в компьютерных сетях, передающих трафик IP-телефонии. Анализ полученных результатов подтверждает актуальность разработки программно-аппаратного комплекса автоматического контроля настроек УАТС и ТА (абонентских линий) КВО информатизации.

2. Необходимо отметить, что абсолютно надежных систем защиты не существует. Кроме того, любая система защиты увеличивает время доступа к информации, поэтому построение защищенных КС не ставит целью надежно защититься от всех классов угроз.

3. Уровень системы защиты – это компромисс между понесенными убытками от потери конфиденциальности информации, с одной стороны, и убытками от усложнения, удорожания КС и увеличения времени доступа к ресурсам от введения систем защиты, с другой стороны.

Литература

1. Петренко А.С., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. – М. : ДМК Пресс, 2005. – С. 384.

2. Мамаев М.А., Петренко С.А. Технологии защиты информации в Интернете. Специальный справочник. – СПб. : Питер, 2002. – С. 848.

3. Лохвицкий В.А. Подход к построению системы автоматизированной интеграции информации в базу данных для её своевременной актуализации / В.А. Лохвицкий, С.В. Калиниченко, А.А. Нечай // Мир современной науки. – 2014. – № 2 (24). – С. 8–12.

4. Нечай А.А. Выявление недекларированных возможностей аппаратно-программного обеспечения / А.А. Нечай // Экономика и социум. – Саратов, 2014. – № 1–2 (10). – С. 457–460.

5. Нечай А.А. Специфика проявления уязвимостей в автоматизированных системах управления критически важными объектами / А.А. Нечай, П.Е. Котиков // Современные тенденции в образовании и науке : сборник научных трудов по материалам Международной научно-практической конференции : в 14 частях. – Тамбов, 2014. – С. 96–97.

6. Скородумов Б.И. Современные проблемы отечественного профессионального стандарта информационной безопасности / Б.И. Скородумов // Вестник Российского нового университета. – 2014. – № 4. – С. 156–158.

УДК 004.738.5

А.С. Дудкин[1]
А.Ф. Шинкаренко[2]

МОДЕЛИРОВАНИЕ ИНФОТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ НА ОСНОВЕ УЧЕТА ВАЖНОСТИ ЕЕ УЗЛОВ В УСЛОВИЯХ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ

В статье изложена проблема оценивания важности узлов инфотелекоммуникационной сети. Рассмотрена и описана модель инфотелекоммуникационной сети и параметры узлов сети, влияющие на их важность. Определен подход к расчету коэффициента важности узлов сети.

Ключевые слова: *инфотелекоммуникационная сеть, граф сети, коэффициент важности, деструктивные воздействия.*

A.S. Dudkin
A.F. Shinkarenko

INFOTELECOMMUNICATION NETWORK MODELING ON THE BASIS OF IMPORTANCE OF ITS NODES IN TERMS OF DESTRUCTIVE IMPACTS

The problem of estimating the importance of infotelecommunication network's nodes is set out in the article. The model of infotelecommunication network and the parameters and importance of its nodes are discussed and descripted, as well as the indicators of importance that are necessary to calculate the importance of network nodes are defined.

Keywords: *infotelecommunication network, network graph, indicators of importance, destructive influences.*

В настоящее время одно из приоритетных направлений развития Вооруженных сил Российской Федерации – это создание единого информационного пространства [1]. Важной проблемой совершенствования технологий информационной безопасности автоматизированных систем являются оценка информационной обстановки и поддержка принятия решения о защите информационных объектов и ресурсов. В настоящее время практически все объекты, имеющие экономическую или военную значимость, функционируют под управлением информационно-технических систем. В условиях значительного возрастания числа важных информационно-технических объектов, по которым планируется проведение удаленных воздействий, их распределенности и разнотипности, задача планирования их защиты существенно осложняется. Для защиты от проведения удаленных воздействий большое значение имеют оперативность и обоснованность принятия решений. В условиях ограниченных возможностей по обеспечению информационной безопасности, а также дефицита времени проблема отнесения информационно-технических объектов к категории важных является, с одной стороны, нетривиальной, а с другой – значительной по своему влиянию на эффективность проведения мероприятий информационной безопасности. Для каждого информационно-технического объекта на основе анализа его свойств требуется принять решение о применении тех или иных способов и средств защиты от информационно-технических воздействий.

Важность подобных объектов определяется многими факторами и является одним из основных показателей, характеризующих возможность достижения конечной цели (решения задачи) применения средств информационной безопасности.

При анализе сложных инфотелекоммуникационных сетей (ИТКС) целесообразно использовать их моделирование с применением графов. Пусть G (V, E) – граф сети, где $V = \{v_i\}$, $i = \overline{1, N}$ – множество вершин; N – количество вершин, а

[1] Кандидат технических наук, преподаватель кафедры информационно-вычислительных систем и сетей ВКА им. А.Ф. Можайского.

[2] Адъюнкт кафедры информационно-вычислительных систем и сетей ВКА им. А.Ф. Можайского.

$E = \{e_i\}$, $i = \overline{1, L}$ – множество ребер; L – количество ребер.

Исследования [2] показывают, что при случайном удалении узлов из произвольного графа существует определенное критическое значение, измеряемое отношением числа удаленных узлов к общему числу узлов в сети, выше которого сеть распадается на отдельные кластеры. Под кластером понимается область ИТКС, в которой внутренние связи (связи данной области) многочисленнее и насыщеннее, чем связи с внешними соседями. Для глобальных сетей, подобных сети Интернет, такого критического числа не существует. Численные эксперименты [3] показывают, что при изъятии из сети даже 80% узлов оставшиеся узлы все еще продолжают поддерживать связанный кластер. Следовательно, такие сети очень устойчивы к случайным повреждениям или внешним случайным воздействиям. Такая устойчивость объясняется слишком взаимосвязанной топологической структурой этих сетей. Но у таких сетей существует особенность, которая позволяет при точечном удалении узлов из сети нанести существенный ущерб всей структуре ИТКС (рис. 1).

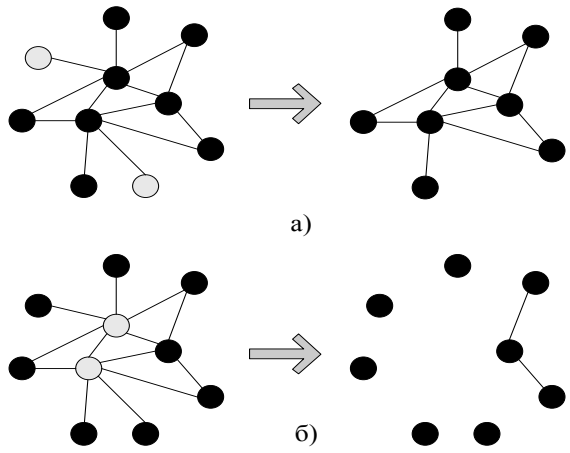


Рис. 1. Граф сети при различном удалении узлов:
а – граф сети при случайном удалении узлов (связность сети продолжается);
б – граф сети при точечном удалении узлов (связность сети разрушается)

В связи с вышеизложенным остро встает вопрос о поиске таких узлов сети, после удаления которых возможно нанесение максимального ущерба всей топологической структуре сети. Это приводит к необходимости обоснования показателей важности сетевых информационно-технических объектов. В результате анализа свойств сложных сетей [2–5] выделяют следующие параметры узлов сети:

– входную и выходную степени K_i узла i – количество ребер графа, которые входят (выходят) из узла i;

– центральность T_i узла i – отношение количества связей узла i к общему числу связей;

– «близость» узла – характеристику средней близости к данному узлу всех остальных узлов сети. Формальное определение этого параметра будет рассмотрено ниже.

«Близость» C_i узла i есть величина

$$C_i = \frac{\sum_j d_{ij}}{N}, \qquad (1)$$

где N – общее число узлов в сети;

d_{ij} – число связей по кратчайшему маршруту между узлами i и j.

Загруженность B_i узла i – доля суммарного числа кратчайших путей между всеми узлами, которые проходят через узел i, к общему числу кратчайших путей сети:

$$B_i = \sigma_{st} / \sum_{st} \sigma_{st}(i), \qquad (2)$$

где $\sigma_{st}(i)$ – число кратчайших путей из узла s в узел t через узел i;

σ_{st} – общее число кратчайших путей между всеми парами s и t.

Рассмотрим свойство «важности» информационно-технического объекта как показатель, учитывающий:

– значения описанных выше параметров соответствующего узла графа, характеризующих интенсивность сетевого трафика, проходящего через этот узел;

– величину потенциальных временных и ресурсных затрат на реализацию деструктивного воздействия на данный информационно-технический объект.

Первый из перечисленных факторов оценим показателем значимости S_i, рассчитываемым через взвешенную сумму рассмотренных выше параметров сети:

$$S_i = \alpha_t T_i + \alpha_c C_i + \alpha_b B_i, \qquad (3)$$

где α_t – вес параметра центральности T_i узла i;

α_c – вес параметра «близости» C_i узла i;

α_b – вес параметра загруженности B_i узла i, причем $\alpha_t + \alpha_c + \alpha_b = 1$.

Представленные коэффициенты значимости могут быть найдены на основе метода экспертных оценок [6]. Значения коэффициентов могут изменяться в зависимости от особенностей сети.

Другим вариантом показателя значимости S_i узла i графа G может быть величина, интерпретируемая как площадь треугольника, образованная тремя отрезками, расположенными на осях, выходящих из общей точки под равными углами

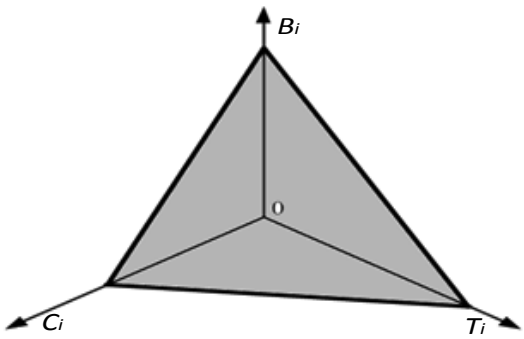


Рис. 2. Расчет показателя значимости S_i узла i

(рис. 2), причем величина каждого из отрезков равна, соответственно, значениям параметров T_i, C_i, B_i в выражении (3). Значение этой площади P легко находится из выражения

$$P = \frac{\sqrt{3}}{4}\left(T_i \times C_i + T_i \times B_i + B_i \times C_i\right). \qquad (4)$$

Определяя показатель значимости S_i узла i, нормированной в диапазоне от 0 до 1, величину P площади треугольника, получим следующее выражение:

$$S_i = \frac{1}{3}\left(T_i \times C_i + T_i \times B_i + B_i \times C_i\right). \qquad (5)$$

Преимуществом определения показателя значимости узла с помощью выражения (5) перед его определением через выражение (3) является отсутствие необходимости применения весьма субъективного метода экспертных оценок.

Второй фактор, являющийся по сути ресурсно-временной «стоимостью» воздействия на i-й узел, будем оценивать показателем стоимости воздействия

$$Z_i = \{z_i \mid \ \tau_i \in \tau_i^{\text{доп}}\}, \qquad (6)$$

где z_i – затраты на проведение удаленного деструктивного воздействия на i-й узел;

τ_i – время, необходимое для проведения удалённого деструктивного воздействия на i-й узел (информационно-технический объект);

$\tau_i^{\text{доп}}$ – допустимое (приемлемое) время проведения воздействия на i-й узел.

Тогда коэффициент W_i важности i-го узла определим как

$$W_i = \{S_i \mid \ Z_i \in Z_i^{\text{доп}}\}, \qquad (7)$$

где $Z_i^{\text{доп}}$ – допустимая (приемлемая) стоимость воздействия на i-й узел.

Предложенный коэффициент важности узла сети обобщает в себе качества:

– результативности воздействия, рассматриваемой как мера ущерба, причиняемого сетевой структуре, который заключается в блокировании некоторого подмножества узлов сети;

– оперативности воздействия как допустимого времени на его проведение;

– ресурсоемкости воздействия как оцениваемых по критерию пригодности затрат на проведение воздействия.

При планировании сценариев защиты от целенаправленных удаленных воздействий на узлы ИТКС эффективность применения и возможный ущерб от последствий в сравнении со случайным и беспорядочным удалением (блокированием) существенно выше.

Описанная модель может служить как для оценивания возможных угроз информационной безопасности распределенных сетевых ресурсов, так и для обоснования облика системы информационной безопасности критически важных объектов.

Предлагаемый показатель – коэффициент важности узла сети – является обобщенным показателем, учитывающим результативность, оперативность и ресурсоемкость потенциального воздействия на узлы сети.

Литература

1. Гладышев А.И. Вопросы создания единого информационного пространства в космотехносфере // Вестник Российского нового университета. – 2014. – Вып. 4. – С. 137–140.

2. Евин И.А. Введение в теорию сложных сетей // Компьютерные исследования и моделирование. – 2010. – Т. 2. – № 2. – С. 121–141.

3. Bellmore, M. Optimal defense of multicommodity networks / M. Bellmore and H.D. Ratliff // Management Science. – 1971. – Vol. 18. – № 4. – P. 174–185.

4. Dorogovtsev, S.N. Lectures on Complex Networks // Oxford University Press. – 2010. – № 75. – P. 54–62.

5. Dorogovtsev, S.N., Mendes, J.F.F. Evolution of Networks: From Biological Nets to the Internet and WWW // Oxford University Press. – 2003. – № 32. – P. 112–118.

6. Басыров А.Г., Шинкаренко А.Ф., Ситало Е.А. Подход к оцениванию важности информационно-технических объектов : труды Военно-космической академии им. А.Ф. Можайского. – СПб. : ВКА им. А.Ф. Можайского, 2014. – Вып. 642. – С. 64–71.

УДК 004.75

А.Г. Басыров[1]
В.В. Широбоков[2]

ПОДХОД К РАСПРЕДЕЛЕННОЙ ОБРАБОТКЕ ИНФОРМАЦИИ В МОБИЛЬНОЙ НЕОДНОРОДНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Рассмотрена проблема организации распределенных вычислений в мобильных неоднородных вычислительных сетях с изменяющейся пропускной способностью каналов связи при ограничениях на объем памяти и энергоресурс автономных источников питания.

Ключевые слова: *распределенная обработка, мобильная вычислительная система, неоднородная вычислительная сеть.*

A.G. Basyrov
V.V. Shirobokov

APPROACH TO THE DISTRIBUTION OF INFORMATION PROCESSING IN HETEROGENEOUS COMPUTING MOBILE NETWORK

The problem of distributed computing in heterogeneous mobile computing systems with variable bandwidth communication channels by the restrictions on the amount of memory and energy independent power supply is considered.

Keywords: *distributed processing, mobile computer system, heterogeneous computer network.*

На современном этапе развития сетевых технологий большое распространение получили мобильные вычислительные сети. Отличительные свойства данных сетей состоят в том, что они имеют большое число различающихся по производительности элементов (вычислительных устройств), обменивающихся данными по ненадежным каналам с переменной пропускной способностью, объединены в общий ресурс, характеризуются сложной зависимостью производительности от режимов энергопотребления и характеристик каналов связи, а также изменением структуры в процессе функционирования. В данных сетях имеет место зависимость взаимного положения узлов на скорость обработки данных.

Примером подобных сетей могут служить мобильная сеть переносных компьютеров, распределенная вычислительная система, состоящая из бортовых компьютеров группировки микроспутников и т.д.

Расширение масштабов использования мобильных неоднородных вычислительных сетей влечет необходимость повышения автономности их функционирования [1; 2]. Перенос решения ряда задач со стационарных на мобильные вычислительные средства приводит к необходимости увеличения производительности отдельного мобильного компьютера и совершенствование подходов к построению и организации функционирования мобильной вычислительной сети в целом. Наращивание производительности вычислительного устройства мобильного компьютера вступает в противоречие с ограничениями по массе, энергозатратам, требованиям по надежности. При этом наращиваемые ресурсы мобильного компьютера не будут использованы в полной мере, а будут востребованы лишь на относительно коротких интервалах его функционирования.

Решением данного противоречия является подход, в основу которого положена технология предоставления информационно-вычисли-

[1] Доктор технических наук, профессор, начальник кафедры информационно-вычислительных систем и сетей Военно-космической академии им. А.Ф. Можайского.

[2] Адъюнкт кафедры информационно-вычислительных систем и сетей Военно-космической академии им. А.Ф. Можайского.

тельных ресурсов на основе модели «клиент-сервер» с конфигурацией «тонкий клиент». Данный подход позволяет минимизировать требования к аппаратно-программным ресурсам компьютера-клиента, перенося часть информационно-вычислительной нагрузки на центры обработки данных (серверы).

При организации распределенной обработки информации в мобильной неоднородной вычислительной сети возникает задача оптимального распределения вычислительной нагрузки между клиентом (α) и сервером (β) высокой производительности при ограниченном энергоресурсе бортовых источников питания. Это приводит к необходимости создания модели распределенной обработки информации в мобильной неоднородной вычислительной сети (рис. 1), учитывающей: состав и характеристики специального программного обеспечения (ПО) Ψ, входные данные $V_{вх}$, поступающие на обработку, динамически изменяющееся расстояние d между клиентом и сервером. Распределение вычислительной нагрузки между α и β заключается в разделении последовательности задач ПО Ψ на два непересекающихся подмножества: задач, выполняемых на α, и задач, выполняемых на β. Для этого выбирается целое число $1 \le k \le n$, такое, что задачи с номерами 1, 2, …, k будут выполняться на α, а задачи с номерами $k + 1$, $k + 2$,…, N будут выполняться на β. При этом формируются целевые показатели обработки информации – время T выполнения целевой задачи и энергоресурсы E, затраченные на ее выполнение:

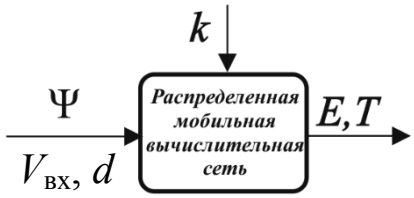


Рис. 1. Абстрактная модель распределенного выполнения целевой задачи

Для выполнения возложенных на клиента задач предназначается ПО $\Psi = \{\psi_1, \psi_2, \ldots, \psi_n\}$, включающее n-подзадач (рис. 2). Каждая подзадача включает $\psi_i = \{S_i, P_i\}$ набор инструкций, состоящий из S_i инструкций данного кода, выполняющихся только последовательно друг за другом на одном ядре вычислительного устройства, и P_i программно-независимыми друг от друга инструкций, которые могут выполняться одновременно на нескольких ядрах процессора мобильной вычислительной системы (МВС).

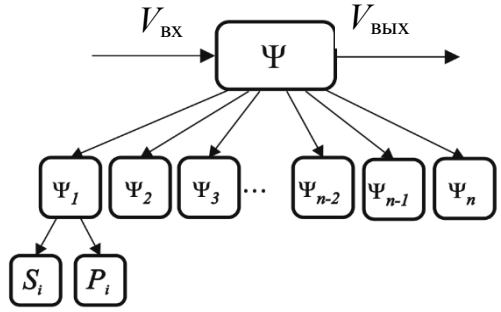


Рис. 2. Структура целевой задачи

Входными данными (рис. 3) для ПО Ψ является информация $V_{вх}$ объемом v_1, поступающая с входных устройств, установленных на клиенте в соответствии с его предназначением, а выходными данными $V_{вых}$ объемом v_{n+1} является результат выполнения программы Ψ, который затем передается потребителям. При этом должно выполняться условие:

$$\left(\sum_{i=1}^{k} v_i + p_\alpha\right) \le W_\alpha \bigcap \left(\sum_{i=k^*+1}^{n} v_i + p_\beta\right) \le W_\beta, \quad (1)$$

где W_α, W_β – объем памяти на α или β, соответственно;

p_α, p_β – объем памяти, занимаемой программами на α или β, соответственно.

Объем памяти программ p_α, p_β определяется по формулам:

$$p_\alpha = \sum_{i=1}^{k} p_i, \quad (2)$$

$$p_\beta = \sum_{i=k+1}^{n} p_i, \quad (3)$$

где p_i – объем памяти, занимаемый программой для выполнения i-й подзадачи на α или β, который может быть найден по формуле:

$$p_i = (S_i + P_i)\, y, \quad (4)$$

где y – размер одной инструкции (байт);

S_i и P_i – количество инструкций программного кода, составляющих подзадачу ψ_i.

При расчете объема памяти, занимаемой программой для выполнения последовательности подзадач на МВС α или β, должно выполняться условие (1).

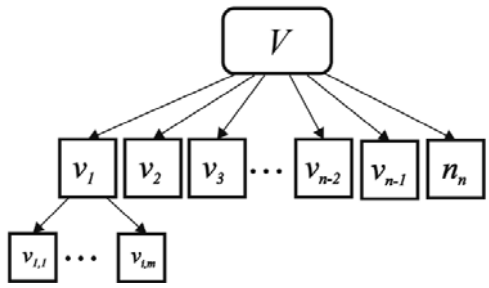


Рис. 3. Входные данные для выполнения подзадачи

Общая схема выполнения программы на МВС клиента представлена на рис. 4.

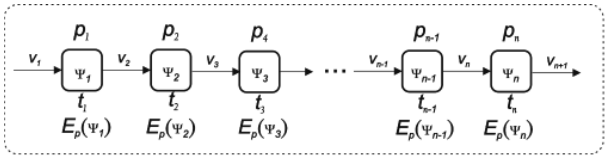


Рис. 4. Схема выполнения задачи на клиенте

Сложные алгоритмы обработки входных данных требуют наличия высокопроизводительной МВС и приемлемого бортового энергоресурса для обеспечения вычислительного процесса. Ограничение по масса-габаритным характеристикам клиента не позволяет устанавливать на него высокопроизводительную МВС и мощную систему бортового энергообеспечения. Кроме того, при выполнении сложных вычислительных алгоритмов на МВС клиента уменьшается ресурс системы бортового энергообеспечения, который в основном и определяет срок его активного существования. Для большинства клиентов мобильной вычислительной сети после истечения гарантийного срока активного существования характеристики системы энергопитания значительно ухудшаются, и клиент используется с ограничениями по целевому назначению.

Перенос обработки части подзадач с компьютера α на компьютер β позволит уменьшить нагрузку на систему электроснабжения компьютера α. Перенос осуществляется по технологии предоставления информационно-вычислительных ресурсов на основе модели «клиент-сервер» с конфигурацией «тонкий клиент» (рис. 5).

Рис. 5. Модель «клиент-сервер»
с конфигурацией «тонкий клиент»

Перенос части вычислений с компьютера α на компьютер β разделяет выполнение программы на две части. Первая часть подзадач ψ_i, $i \in (1, \ldots, k)$ выполняется на α до момента окончания выполнения k-й подзадачи, затем результат выполнения k-й подзадачи передается по каналу связи на β и продолжается обработка подзадач ψ_i, $i = k + 1, \ldots, n$. После обработки данных в МВС β результат передается потребителю.

Схема распределенной обработки программы в компьютерах α и β представлена на рис. 6, где p_i – объем памяти, занимаемый программой для выполнения i-й подзадачи клиента, t_i – длительность монопольного решения i-й подзадачи при входных данных v_i, $E_p(\psi_i)$ – потребляемая процессором компьютера мощность при выполнении i-й подзадачи.

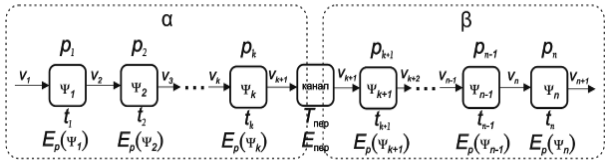


Рис. 6. Схема выполнения задачи
в клиент-серверной системе

Цель организации распределенной обработки информации между клиентом и сервером заключается в минимизации времени выполнения целевых задач при ограничениях на объем памяти каждого компьютера и на энергоресурс автономных источников питания.

Формально постановку задачи с учетом (1) можно представить как необходимость поиска оптимального значения k^* при условии:

$$\begin{cases} k^* = \arg\min T\left(k, d, V, \Psi, L\right) \\ \left(\sum_{i=1}^{k^*} v_i + p_\alpha\right) \le W_\alpha \\ \left(\sum_{i=k^*+1}^{n} v_i + p_\beta\right) \le W_\beta \\ E\left(k^*, d, T, P_{pow}, P_{\text{ппа}}\right) \le E_{\text{тр}} \end{cases}, \qquad (5)$$

где k – наибольший номер задачи, выполняемой на α;

T – время решения целевой задачи;

d – расстояние между α и β;

V – массив входных данных для выполнения каждой подзадачи;

Ψ – специальное программное обеспечение;

L – количество инструкций, выполняемых процессором в единицу времени;

W_α, W_β – объем памяти на α или β, соответственно;

P_{pow} – потребляемая мощность процессором;

$P_{\text{ппа}}$ – потребляемая мощность приемо-передающей аппаратурой.

Так как временные и энергетические ресурсы складываются из затрат на обработку информации и на ее передачу между клиентом и сервером, для решения поставленной задачи необходимо найти:

– время выполнения целевой задачи и затраченного суммарного количества энергии на ее выполнение;

– пропускную способность канала связи;

– количество потребляемой энергии бортовой вычислительной системой при выполнении набора инструкций;

– количество потребляемой энергии при передаче данных.

Общее время выполнения задачи в системе, основанной на модели «тонкий клиент», определяется по формуле:

$$T = T_{\alpha} + T_{\beta} + T_{\text{пер}}, \quad (6)$$

где T_{α} – время выполнения последовательности подзадач на α;

T_{β} – время выполнения последовательности подзадач на β;

$T_{\text{пер}}$ – время передачи данных по каналу связи между α и β.

Время выполнения одной последовательности подзадач на α определяется по формуле:

$$T_{\alpha} = \sum_{i=1}^{k} t_i(\psi_i), \quad (7)$$

где $t_i(\psi_i)$ – длительность монопольного решения i-й подзадачи ψ_i на α.

Время выполнения одной последовательности подзадач на β определяется по формуле:

$$T_{\beta} = \sum_{i=k+1}^{n} t_i(\psi_i), \quad (8)$$

где $t_i(\psi_i)$ – длительность монопольного решения i-й подзадачи ψ_i на β.

Зависимость меры пропускной способности канала от помех выражена в теореме Шеннона следующим образом [2]:

$$C = \frac{P_{\text{пер}} G S_{\text{эф}} \eta_{\text{пр}} \eta_{\text{пер}} L \log_2\left(1 + \frac{P_{\text{с}}}{P_{\text{ш}}}\right)}{d^2 4\pi w \left(\frac{P_{\text{с}}}{P_{\text{ш}}}\right)}, \quad (9)$$

где d – расстояние между α и β;

G – коэффициент направленности передающей антенны;

$P_{\text{пер}}$ – мощность передатчика;

$S_{\text{эф}}$ – эффективная площадь антенны;

w – коэффициент пропорциональности мощности шумов к ширине полосы пропускания;

$P_{\text{с}}/P_{\text{ш}}$ – отношение мощности сигнала к мощности помех;

$\eta_{\text{пр}}$, $\eta_{\text{пер}}$ – коэффициенты полезного действия приемного и передающего антенно-фидерных трактов;

L – потери, вызванные затуханием энергии сигнала в свободном пространстве, ионизацией слоев атмосферы, шумом в приёмных трактах линий связи, неточностью наведения антенн, вращением плоскости поляризации и другими факторами.

Пропускная способность канала будет снижаться пропорционально информационной нагрузке абонентов. При этом возможны два варианта временного разделения абонентов:

– фиксированное разделение пропорционально количеству абонентов q, информационной нагрузке отдельных абонентов;

– случайный множественный доступ абонентов.

При расчете пропускной способности канала связи следует учитывать невысокую мощность установленных на клиенте приемо-передающего оборудования, обусловленную ограничениями, вносимыми системой электропитания и массогабаритными характеристиками клиентов.

При фиксированном разделении интенсивности информационного трафика в канале на q абонентов эффективная пропускная способность канала, выделяемая каждому абоненту, составит

$$C_q = \frac{C}{q}. \quad (10)$$

Суммарный энергоресурс, затраченный на выполнение ПО Ψ, с учетом энергии $E_{\text{пер}}(v_{k+1})$, затраченной на передач**у** выходных данных v_{k+1} k-й подзадачи по каналу связи, определяется следующим выражением:

$$E = \sum_{i=1}^{k} E_p(\psi_i) + E_{\text{пер}}(v_{k+1}) + \sum_{i=k+1}^{n} E_p(\psi_i). \quad (11)$$

Время выполнения одной i-й подзадачи на одноядерном процессоре ($z = 1$) в МВС при входных данных v_i и условии $\langle v_{i,j}, \psi_i \rangle$ составит

$$t_i(\psi_i) = \frac{S_i + P_i}{L}, \quad (12)$$

где $i \in \{1, \ldots, n\}$, S_i и P_i – количество инструкций программного кода, составляющих подзадачу ψ_i, L – количество инструкций, выполняемых процессором в единицу времени.

Количество инструкций, выполняемых за такт, зависит от микроархитектуры процессора, напряжения питания, а также от технологии производства, определяющей минимальные размеры используемых транзисторов, их быстродействие и время задержки передачи сигнала в межуровневых соединениях.

В случае использования многоядерного процессора, число ядер которого равно z, время выполнения одной i-й подзадачи окажется меньше за счет параллельного выполнения ψ_i команд на разных ядрах процессора и составит

$$t_i(\psi_i) = \frac{S_i}{L} + \frac{P_i}{zL}, \quad (13)$$

где z – количество ядер в многоядерном процессоре БВС, S_i – число инструкций этого кода, выполняющихся только последовательно друг за другом, P_i – количество инструкций, являющихся программно независимыми друг от друга и способных выполняться одновременно на всех ядрах процессора.

Зависимость потребляемой процессором мощности от его тактовой частоты можно представить следующей формулой [5]:

$$P_{pow} = CU^2 f, \quad (14)$$

где f – тактовая частота процессора;

U – напряжение питания процессора;

C – динамическая емкость, определяемая микроархитектурой процессора, количеством транзисторов в микросхеме и их активностью переключения.

Учитывая, что тактовая частота обусловлена напряжением питания процессора, потребляемая мощность нелинейным образом зависит от частоты процессора. Соответственно получаем нелинейную связь между производительностью процессора и потребляемой им мощностью.

Следовательно, количество энергии, затраченной на выполнение набора инструкций ψ_i в i-й подзадаче, определяется по формуле (15):

$$E_p(\psi_i) = P_{pow} t_i(\psi_i), \quad (15)$$

где P_{pow} – потребляемая процессором мощность МВС.

Время передачи данных по каналу связи между α и β определяется по формуле:

$$T_{\text{пер}} = \frac{V_{\alpha\beta}}{C} + \frac{d}{c}, \quad (16)$$

где $V_{\alpha\beta}$ – объем трафика;

C – пропускная способность канала связи между α и β;

d – расстояние между α и β;

c – константа, c = 299 792 458 м/с.

Энергия, затраченная для передачи данных по каналу связи между α и β, определяется по формуле:

$$E_{\text{пер}} = T_{\text{пер}} P_{\text{ппа}}, \quad (17)$$

где $P_{\text{ппа}}$ – потребляемая мощность приемо-передающей аппаратуры.

Таким образом, с учетом выражений (6), (11), время распределенной обработки целевой задачи в мобильной неоднородной вычислительной сети может быть представлено в виде:

$$T = \frac{1}{L}\left(\sum_{i=1}^{k}\left(S_i + \frac{P_i}{z}\right) + \sum_{i=k+1}^{n}\left(S_i + \frac{P_i}{z}\right)\right) + \frac{V_{\alpha\beta}}{C} + \frac{d}{c}, \quad (18)$$

а затраты энергоресурса:

$$E = \frac{P_{pow}}{L}\left(\sum_{i=1}^{k}\left(S_i + \frac{P_i}{z}\right) + \sum_{i=k+1}^{n}\left(S_i + \frac{P_i}{z}\right)\right) + P_{\text{пер}}\left(\frac{V_{\alpha\beta}}{C} + \frac{d}{c}\right). \quad (19)$$

В предложенном подходе распределенной обработки информации в мобильной неоднородной вычислительной сети учитывается время выполнения набора инструкций, затраты энергоресурса источников питания компьютера-клиента и сервера, требуемый объем памяти МВС с учетом пропускной способности канала связи и расстояния между клиентом и сервером.

Современные сетевые технологии способны обеспечить высокоскоростной обмен информацией по каналам связи в мобильной вычислительной сети, а технологии программирования и построения распределенных вычислительных сервисов позволяют организовать управляемую, масштабируемую высокопроизводительную систему.

Применение предложенного подхода обеспечивает организацию вычислительного процесса с предоставлением вычислительных ресурсов сервера «по запросу» клиента.

Литература

1. Гладышев А.И. Вопросы создания единого информационного пространства в космотехносфере // Вестник Российского нового университета. – 2014. – Вып. 4. – С. 137–140.

2. Фатеев В.Ф. Инфраструктура малых космических аппаратов. – М. : Радиотехника, 2011. – 432 с.

3. Невзоров Ю.В., Козак О.И., Васильев О.В. Факторы, влияющие на скорость передачи информации по космической радиолинии: развитие систем СВЧ радиосвязи // Электросвязь : научно-технический журнал по проводной и радиосвязи, телевидению, радиовещанию. – 2012. – № 8. – С. 29–31. – ISSN 0013-5771.

4. Пахомов С. Эра многоядерных энергоэффективных процессоров. – URL: http://compress.ru/Article.aspx?id=16962 (дата обращения 01.05.2015).

УДК 004.056

А.А. Костырин[1]

КИБЕРБЕЗОПАСНОСТЬ СЕТЕЙ СВЯЗИ И РАЗРАБОТКА СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Статья посвящена актуальному вопросу. Дается характеристика угроз киберсреды, их перечень и виды. Также ценным в этой статье является описание стадий создания системы защиты информации.

Ключевые слова: *кибербезопасность, киберсреда, угрозы безопасности, уровни безопасности, защита информации.*

A.A. Kostyrin

CYBERSECURITY OF COMMUNICATION NETWORKS AND DEVELOPMENT OF DATA PROTECTION SYSTEMS

The article is devoted to topical issues. The characteristic of cyberthreats and types of their list are given. Just valuable in this article is to describe the steps of creating a system of information protection.

Keywords: *cybersecurity, cyberenvironment, threats to security, levels of security, information security.*

В настоящее время сравнительно легко можно получать информацию, общаться, наблюдать и управлять системами IT на значительных расстояниях. Современные сети играют ключевую роль во многих инфраструктурах государственной важности: электронной торговле, передаче данных и голоса, коммунальных услуг, финансовой, здравоохранения, транспорта и обороны.

Однако широкий доступ и слабая связь взаимосвязанных систем IT может стать первичным источником широко распространенной уязвимости. Для систем, объединенных в сеть, возрастают угрозы, такие, как: взлом в виде «отказ в обслуживании», кража финансовых и личных сведений, сбои в работе сети, нарушение речевой связи и дистанционной передачи данных.

Угрозы для автоматизированных систем быстро возрастают. Вирусы, черви, троянские кони, кража идентичности, спам и кибератаки находятся на подъеме. Необходимо понимание кибербезопасности для построения фундамента тех знаний, которые помогут обезопасить сети завтрашнего дня.

В современных сетях границы между внутренними и внешними сетями становятся более размытыми. Предполагается, что между этими уровнями обеспечена безопасность. Уровневый подход к проблеме безопасности дает возможность создания множества уровней защиты, направленных против угроз.

[1] Преподаватель Военно-космической академии им. А.Ф. Можайского.

Технологии кибербезопасности могут использоваться для гарантирования готовности систем, целостности, аутентичности, конфиденциальности и строгого выполнения обязательств. Технологии кибербезопасности могут использоваться для гарантий соблюдения личной тайны пользователя. Технологии кибербезопасности могут использоваться для установления достоверности пользователя.

Технологии, такие, как беспроводные сети и передача голоса по Интернету, расширяют область влияния и масштаб Интернета. В связи с этим, киберсреда включает пользователей, Интернет, компьютерные устройства, которые подключены к нему, все приложения, услуги и системы, которые могут напрямую или опосредованно подключаться к Интернету, и среду сетей последующих поколений, доступных для общего и частного применения. При использовании технологий Интернета даже настольный телефон может является частью киберсреды.

Даже изолированные устройства также могут являться частью киберсреды, если они могут пользоваться информацией совместно с компьютерными устройствами, подключаемыми с помощью сменных носителей. И, следовательно, на них могут оказывать воздействие разнообразные вредоносные программы – вирусы, черви, троянские программы, перехватчики и подобные им программы. В целях противодействия возможным атакам рекомендуется применять специальные меры борьбы с ними, например анти-

вирусные программы и иные новые разработки специалистов в области защиты киберсреды.

В киберпространство входит программное обеспечение, которое работает в компьютерных устройствах, информация, которая сохраняется (и передается) в этих устройствах, или информация, которая создается этими устройствами. Оборудование и здания, в которых расположены эти устройства, также являются частью киберпространства. Такие элементы должны приниматься в расчет для обеспечения безопасности.

Кибербезопасность подразумевает:

– совокупность политик и действий, которые должны быть предприняты для защиты соединенных сетей (включая компьютеры, устройства, аппаратные средства, хранящуюся информацию и передаваемую информацию) от несанкционированного доступа, изменения, кражи, разрушения и других угроз;

– текущую оценку и мониторинг вышеуказанных политик и действий для гарантии непрерывного качества безопасности перед лицом изменяющейся природы угроз.

К элементам, составляющим киберсреду, следует относить не только базовые станции, коммутаторы и абонентские терминалы. В ее состав входят также и периферийные устройства, такие, как принтеры, сканеры, факсимильные аппараты, которые сегодня в большинстве случаев являются сетевыми.

Любой элемент киберсреды может рассматриваться, как риск для безопасности, который в общем случае воспринимается как комбинированная оценка угрозы. В анализ угрозы входит задача описания типа возможных взломов, методы осуществления попытки нарушения защиты и последствия в случае успешных взломов. Оценка рисков вместе с анализом угрозы позволяют организации просчитать потенциальный риск для своей сети.

Попытки нарушения защиты могут исходить из киберсреды, такие, как взломы, посредством червей или других вредоносных программ, могут быть прямые попытки нарушения защиты важной инфраструктуры, такой, как кабели электросвязи, или взломы, вызванные действиями доверенного, хорошо осведомленного человека. Сочетание этих попыток нарушения защиты также возможно. Риски обычно характеризуются как высокие, средние и низкие. Уровень риска изменяется среди разных компонентов киберсреды.

Кибербезопасность заключается в управлении рисками. Для управления рисками могут использоваться разные технологии:

– разработка стратегии защиты, определяющая меры противодействия, которые могут быть предприняты при возможных попытках нарушения защиты;

– обнаружение, в которое входит идентификация взлома в момент его развития и впоследствии;

– формулировка отклика на попытку нарушения защиты, в которой определяется совокупность мер противодействия этой попытке для того, чтобы ее остановить или снизить ее влияние;

– формулировка стратегии восстановления, которая дает возможность сети возобновить работу с известного состояния.

Согласно Рекомендации МСЭ-Т X.800 (ITU-T X.800), в перечень угроз для системы передачи данных включены следующие:

– уничтожение информации и/или других ресурсов;

– искажение или изменение информации;

– кража, перемещение или потеря информации и/или других ресурсов;

– раскрытие информации;

– прерывание обслуживания.

В соответствии с ITU-T X.800, угрозы могут классифицироваться как случайные или преднамеренные, и они могут быть активными и пассивными. Случайными угрозами являются такие угрозы, которые возникают без предварительного умысла. Примерами реализованных случайных угроз являются: эксплуатация неисправного оборудования, неквалифицированный ремонт компьютерной и иной цифровой техники, неправильное срабатывание системы, грубые просчеты в работе и ошибки в программном обеспечении.

Преднамеренные угрозы могут классифицироваться от непредусмотренной экспертизы, использующей легкодоступные инструменты мониторинга, до сложных попыток нарушения защиты, использующих специальные системные знания. Преднамеренная угроза, если она реализована, может быть воспринята, как «попытка нарушения защиты».

Пассивными угрозами являются такие, которые, если они реализованы, не приводят к какому-либо изменению информации, заключенной в системе, и при которых не изменяется ни работа, ни состояние системы. Использование пассивного подслушивающего оборудования для наблюдения за информацией, передаваемой по подключенной линии, является реализацией пассивной угрозы.

Активные угрозы для системы включают в себя изменение информации, содержащейся в

системе, или изменения в состоянии или работе этой системы. Злонамеренное изменение таблиц маршрутизации системы несанкционированным пользователем является примером активной угрозы.

Таким образом, до начала разработки системы безопасности нужно идентифицировать конкретные угрозы, против которых понадобится защита. Этот анализ известен как оценка угроз.

В оценку угроз включены:

– идентификация уязвимых мест системы;

– анализ вероятности угроз, нацеленных на использование этих уязвимых мест;

– оценка последствий, если каждая угроза будет успешно выполнена;

– оценка стоимости каждой попытки нарушения защиты;

– расчет стоимости потенциальных мер противодействия;

– выбор механизмов безопасности, которые оправданны (возможно с помощью использования анализа стоимостной выгоды).

В ITU-T X.805 фактором безопасности является совокупность мер безопасности, разработанных для определенного аспекта безопасности сетей. В ITU-T X.805 определяются восемь факторов, которые защищают от всех основных угроз безопасности. Эти факторы не ограничиваются сетями, а также распространяются на приложения и информацию конечного пользователя.

Факторами безопасности являются:

– контроль доступа;

– аутентификация;

– неотказуемость;

– конфиденциальность данных;

– безопасность связи;

– целостность данных;

– готовность;

– секретность.

Для того чтобы обеспечить решение вопроса сквозной безопасности связи, факторы безопасности должны применяться к иерархии сетевого оборудования и группировкам средств, которые рассматриваются как уровни безопасности.

Различают три уровня безопасности:

1) уровень безопасности инфраструктуры;

2) уровень безопасности услуг;

3) уровень безопасности приложений.

Уровни безопасности устанавливают, где в продуктах и решениях принимается во внимание обеспечение безопасности путем предоставления последовательной структуры безопасности сетей. Например, сначала обращаются к уязвимым местам с точки зрения безопасности для уровня инфраструктуры, затем – для уровня услуг и для уровня приложений. Факторы безопасности применяются к уровням безопасности для того, чтобы уменьшить количество уязвимых мест, присутствующих в каждом уровне.

В ITU-T X.805 определены три плоскости безопасности для представления трех типов защищенных действий, которые происходят в сети:

1) плоскость управления;

2) плоскость контроля;

3) плоскость конечного пользователя.

Эти плоскости безопасности предназначены для конкретных нужд безопасности, связанных с деятельностью управления сетью, контроля сети или деятельностью по передаче сигналов и деятельностью конечного пользователя, соответственно. В ITU-T X.805 предлагается разрабатывать сети таким образом, чтобы события на одной плоскости безопасности хранились изолированно от других плоскостей безопасности.

Концепция плоскостей безопасности позволяет установить различия в конкретных вопросах безопасности, связанных с этими видами деятельности, и дает возможность обращаться к ним независимым образом.

Разработка систем защиты информации производится подразделением организации или специализированными организациями, имеющими лицензии ФСТЭК (Гостехкомиссии) России. При этом разрабатываются методическое руководство и конкретные требования по защите информации, аналитическое обоснование необходимости создания системы защиты информации (СЗИ), согласовывается выбор основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС), технических и программных средств защиты информации (ЗИ), организуются работы по выявлению возможных каналов утечки информации и нарушения целостности защищаемой информации, аттестация объекта информатизации.

Стадии создания системы защиты информации

1. Предпроектная стадия, включающая предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания СЗИ и технического (частного технического) задания на ее создание.

2. Стадия ввода в действие СЗИ, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также аттестацию объекта информатизации на соответствие требованиям безопасности информации.

3. Стадия проектирования (разработки проектов), включающая разработку СЗИ в составе объекта информатизации.

По результатам предпроектного обследования разрабатывается аналитическое обоснование необходимости создания СЗИ и задаются конкретные требования по защите информации, включаемые в техническое (частное техническое) задание на разработку СЗИ.

Работы, выполняемые на предпроектной стадии, следующие.

1. Устанавливается необходимость обработки (обсуждения) информации на данном объекте информатизации.

2. Определяется перечень сведений конфиденциального характера, подлежащих защите.

3. Определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования объекта.

4. Определяются условия расположения объекта информатизации.

5. Определяются конфигурация и топология ОТСС в целом и их отдельных компонентов, физические, функциональные и технологические связи ОТСС с другими системами различного уровня и назначения.

6. Определяются конкретные технические средства и системы, предполагаемые к использованию в разрабатываемой автоматизированной системе (АС), условия их расположения, их программные средства.

7. Определяются режимы обработки информации в АС в целом и в отдельных компонентах.

8. Определяется класс защищенности АС.

9. Определяется степень участия персонала в информации, характер их взаимодействия между собой и со службой безопасности.

10. Определяются мероприятия по обеспечению конфиденциальности информации на этапе проектирования объекта информатизации.

Аналитическое обоснование подписывается руководителем организации, проводившей предпроектное обследование, согласовывается с должностным лицом, обеспечивающим научно-техническое руководство создания объекта информатизации, руководителем службы безопасности и утверждается руководителем организации-заказчика.

Аналитическое обоснование необходимости создания СЗИ включает в себя следующее:

1) информационная характеристика и организационная структура объекта информатизации;

2) характеристика комплекса ОТСС и ВТСС, программного обеспечения, режимов работы, технологического процесса обработки информации;

3) возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;

4) перечень предлагаемых к использованию сертифицированных средств защиты информации;

5) обоснование необходимости привлечения специализированных организаций;

6) оценка материальных, трудовых и финансовых затрат на разработку и внедрение СЗИ;

7) ориентировочные сроки разработки и внедрения СЗИ;

8) перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования объекта информатизации.

Техническое задание на проектирование объекта информатизации оформляется отдельным документом, согласовывается с проектной организацией, службой (специалистом) безопасности организации-заказчика и утверждается заказчиком.

Содержание технического задания должно содержать следующее.

1. Обоснование разработки.

2. Исходные данные создаваемого (модернизируемого) объекта информатизации в техническом, программном, информационном и организационном аспектах.

3. Класс защищенности АС.

4. Ссылка на нормативные документы, на основании которых будет разрабатываться СЗИ.

5. Требования к СЗИ на основе нормативно-методических документов и установленного класса защищенности АС.

6. Перечень предполагаемых к использованию сертифицированных средств защиты информации.

7. Обоснование проведения разработок собственных средств защиты информации, невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации.

8. Состав, содержание и сроки проведения работ по этапам разработки и внедрения.

9. Перечень подрядных организаций-исполнителей видов работ.

10. Перечень предъявляемой заказчику научно-технической продукции и документации.

Мероприятия по защите информации от утечки по техническим каналам относятся к основным элементам проектных решений, которые включаются в соответствующие разделы проекта и разрабатываются одновременно с ними.

При вводе в эксплуатацию выполняются необходимые мероприятия, такие, как опытная экс-

плуатация средств защиты информации с другими техническими и программными средствами для проверки их работоспособности в комплексе и отработки технологического процесса обработки (передачи) информации, приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации, аттестация объекта информатизации по требованиям безопасности информации.

При этом разрабатываются следующие документы.

1. Приемо-сдаточный акт, подписываемый разработчиком (поставщиком) и заказчиком.

2. Акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний.

3. Протоколы аттестационных испытаний и заключение по их результатам.

4. Аттестат соответствия объекта информатизации требованиям по безопасности информации.

5. Приказ (указание, решение) о назначении лиц, ответственных за эксплуатацию объекта информатизации.

6. Приказ (указание, решение) о разрешении обработки в АС конфиденциальной информации.

Контроль состояния защиты конфиденциальной информации проводится службой безопасности организации не реже чем один раз в год и федеральными и отраслевыми органами контроля не реже одного раза в два года. При проведении аттестации объектов информатизации и периодическом контроле состояния защиты конфиденциальной информации организациями могут, при необходимости, использоваться «Временные методики оценки защищенности конфиденциальной информации». При необходимости, по решению руководителя организации, могут быть проведены работы по поиску электронных устройств съема информации («закладочных устройств»), возможно, внедренных в технические средства, осуществляемые организациями, имеющими соответствующие лицензии или ФСБ России (ФАПСИ).

Литература

1. Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации. – М. : Гостехкомиссия России, 2002.

2. Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации. – М. : Гостехкомиссия России, 2002.

3. Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. – М. : Гостехкомиссия России, 2002.

4. Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах. – М. : Гостехкомиссия России, 2002.

5. Международный союз электросвязи. Серия X. Сети передачи данных, взаимосвязь открытых систем и безопасность. – Швейцария, Женева, 2010.

6. Специальные требования и рекомендации по технической защите конфиденциальной информации. – М., 2001. – С. 9.

7. Лохвицкий В.А. Подход к построению системы автоматизированной интеграции информации в базу данных для её своевременной актуализации / В.А. Лохвицкий, С.В. Калиниченко, А.А. Нечай // Мир современной науки. – 2014. – № 2 (24). – С. 8–12.

8. Нечай А.А. Выявление недекларированных возможностей аппаратно-программного обеспечения / А.А. Нечай // Экономика и социум. – 2014. – № 1–2 (10). – С. 457–460.

9. Нечай А.А. Специфика проявления уязвимостей в автоматизированных системах управления критически важными объектами / А.А. Нечай, П.Е. Котиков // Современные тенденции в образовании и науке : сборник научных трудов по материалам Международной научно-практической конференции : в 14 ч. – Тамбов, 2014. – С. 96–97.

10. Нечай А.А. Выбор и обоснование показателей эффективности решения задачи распределения объектов по средствам поражения / А.А. Нечай, С.В. Матвеев, В.М. Сафонов // Мир современной науки. – 2014. – № 2 (24). – С. 13–16.

11. Скородумов Б.И. Современные проблемы отечественного профессионального стандарта информационной безопасности / Б.И. Скородумов // Вестник Российского нового университета. – 2014. – Вып. 4. – С. 156–158.

УДК 004.65

К.А. Эсаулов[1]
В.С. Забузов[2]
Д.И. Казанцев[3]

ПОВЫШЕНИЕ ДОСТУПНОСТИ СЕРВИСОВ ПУТЕМ СОЗДАНИЯ РЕКОНФИГУРИРУЕМОЙ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ВИРТУАЛИЗАЦИИ

В статье рассматриваются вопросы повышения доступности сервисов в инфотелекоммуникационных системах. Предложен подход повышения доступности сервисов путем перераспределения ресурсов с использованием технологий виртуализации.

Ключевые слова: *доступность сервисов, виртуализация, готовность.*

K.A. Esaulov
V.S. Zabuzov
D.I. Kazantsev

IMPROVING AVAILABLE SERVICES THROUGH THE CREATION OF RECONFIGURABLE SYSTEMS USING VIRTUALIZATION

The article examines the increasing availability of services in info-Telecom systems. The approach that improve service availability by reallocating resources using virtualization technologies is proposed.

Keywords: *availability of services, virtualization, availability.*

Использование информационно-вычислительных систем для решения различных прикладных задач предусматривает предоставление пользователям информационных сервисов. В зависимости от рода деятельности организации набор сервисов и требования к их качеству могут быть различными.

Важнейшим показателем качества информационного сервиса является его доступность. Под доступностью информационного сервиса понимается вероятность получения пользователем сервиса за заданное время. Доступность зависит от таких факторов, как надежность аппаратных и программных средств, производительности вычислительных ресурсов и пропускной способности каналов связи, информационной защищенности системы.

С увеличением количества пользователей информационно-вычислительной системы увеличивается интенсивность поступления в систему задач, а следовательно и интенсивность обращения к информационным сервисам, что может привести к снижению доступности этих сервисов.

Инфраструктура, обеспечивающая работу сервисов, представляет собой оборудование, а также общее и специализированное программное обеспечение. Доступность сервиса будет напрямую зависеть от надежности, отказоустойчивости и защищённости его инфраструктуры. Поэтому для повышения доступности информационного сервиса требуется в первую очередь добиться надежного функционирования аппаратной и программной составляющей.

Повышение характеристик надежности [1] возможно путем применения дублирования аппаратно-программных средств. При использовании облачных технологий и средств виртуализации возможна реализация дублирования как программной, так и аппаратной составляющих без существенного изменения аппаратной инфраструктуры всей информационно-вычислительной системы.

[1] Кандидат технических наук, старший преподаватель Военно-космической академии им. А.Ф. Можайского.

[2] Кандидат технических наук, старший преподаватель Военно-космической академии им. А.Ф. Можайского.

[3] Военно-космическая академия им. А.Ф. Можайского.

Типовая структура информационно-телекоммуникационной системы (ИТКС) представлена на рис. 1.

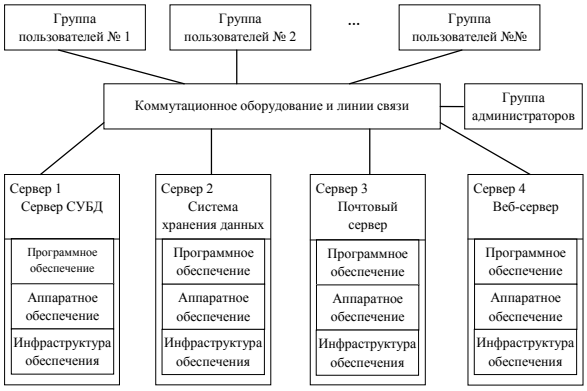


Рис. 1. Типовая структура инфотелекоммуникационной системы

При реализации функций серверов баз данных, хранилища информации, почтового сервера или Web-сервера необходимо учитывать ряд требований к аппаратной платформе, что и определяет гетерогенный характер структуры ИТКС. Задачи, решаемые сервером – хранилищем данных, предъявляют высокие требования к объемам внешних запоминающих устройств, в то время как Web-сервер более критичен к производительности процессора и пропускной способности каналов связи. Качество функционирования любого из представленных на рис. 1 серверов определяется количеством обращений пользователей, объемом решаемых задач, состоянием аппаратного и программного обеспечения. В таблицах 1, 2, 3, 4 представлены технические требования к аппаратным платформам серверов.

Таблица 1

Технические требования для функционирования сервера СУБД

№	Наименование требований	Процессор	ОЗУ	HDD	Тип жесткого диска	Сетевой адаптер
1.	Минимальные требования	1 ядро, 1 ГГц	1 Гб	50 Гб	SATA	100 Мб/сек
2.	Рекомендованные требования	4 ядра, 3 ГГц	128 Гб	2x300 Гб (Raid 1)	SCSI, SAS, FC	1000 Мб/сек

Таблица 2

Технические требования для функционирования системы хранения данных

№	Наименование требований	Процессор	ОЗУ	HDD	Тип жесткого диска	Сетевой адаптер
1.	Минимальные требования	1 ядро, 1 ГГц	0,5 Гб	500 Гб	SATA	100 Мб/сек
2.	Рекомендованные требования	4 ядра, 3 ГГц	4–12 Гб	4x4000 Гб, 4x300 Гб, RAID-1, RAID-10)	SCSI, SAS, FC	1/10G Ethernet, FiberChannel, Infiniband

Таблица 3

Технические требования для функционирования почтового сервера

№	Наименование требований	Процессор	ОЗУ	HDD	Тип жесткого диска	Сетевой адаптер
1.	Минимальные требования	1 ГГц	0,5 Гб	40 Гб	SATA	100 Мб/сек
2.	Рекомендованные требования	4 ядра по 3 ГГц	16 Гб	2x300 Гб (Raid 1)	SCSI, SAS, FC	1000 Мб/сек

Таблица 4

Технические требования для функционирования веб-сервера

№	Наименование требований	Процессор	ОЗУ	HDD	Тип жесткого диска	Сетевой адаптер
1.	Минимальные требования	1 ГГц	0,5 Гб	40 Гб	SATA	100 Мб/сек
2.	Рекомендованные требования	4 ядра по 3 ГГц	6–24 Гб	2x300 Гб (Raid 1)	SCSI, SAS, FC	1000 Мб/сек

На одном сервере могут быть размещены несколько виртуальных машин, отвечающих за работу различных сервисов. Тот же набор виртуальных машин может параллельно функционировать и на других серверах (рис. 2). Таким образом, не изменяя аппаратного состава ИТКС, можно добиться дублирования сервисов, повысить их надежность и тем самым повысить доступность.

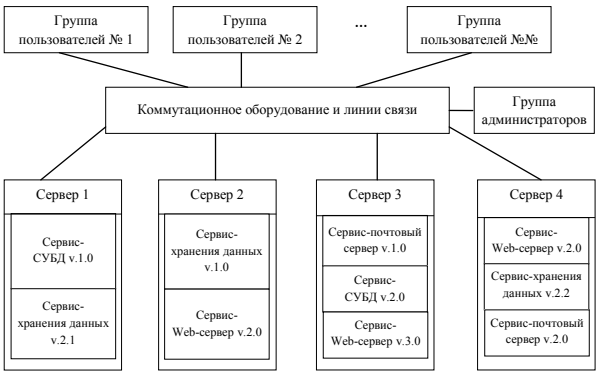


Рис. 2. Пример распределения сервисов с использованием виртуальных машин

Такой подход имеет ряд достоинств и недостатков.

К достоинствам следует отнести:

1. Повышение доступности за счет распараллеливания обращений пользователей, что приводит к снижению загрузки сервиса.

2. Повышения надежности ИТКС в целом за счет применения резервирования сервисов.

3. Улучшение системы технического обслуживания, так как резервирование сервисов позволяет проводить восстановительные мероприятия на сервере и при этом сервис остается доступным для пользователей.

4. Оптимизация использования аппаратных возможностей серверов за счет использования излишков ресурсов.

5. Уменьшение затрат времени администраторов на восстановление после сбоя за счет наличия актуальной копии сервиса на другой виртуальной машине.

Применение виртуальных машин связано с необходимостью решения дополнительных задач администрирования и перераспределения аппаратных ресурсов. Поэтому данный подход кроме перечисленных достоинств имеет ряд недостатков, к которым можно отнести:

1. Снижение производительности ИТКС из-за необходимости обеспечивать работу системы виртуальных машин, синхронизацию данных, перераспределения дискового пространства.

2. Усложнение процесса администрирования работы ИТКС из-за необходимости настройки виртуальных машин.

3. Повышение стоимости ИТКС из-за необходимости приобретения дополнительного программного обеспечения, а также обучения обслуживающего персонала.

4. Появляются дополнительные риски информационной безопасности [2] обрабатываемой информации из-за использования технологий виртуализации.

Таким образом, общая постановка задачи может быть представлена как распределение ресурсов инфотелекоммуникационной системы между виртуальными машинами, имеющая оптимизационный характер. Основным ограничением является объем аппаратных средств ИТКС. Повышения готовности информационно-вычислительных систем можно добиться двойным резервированием – резервирование большой кратности не даст значительного прироста надежности [3]. Минимальное значение виртуальных машин, обеспечивающих функционирование сервисов, должно быть не менее двух.

Обеспечение заданной доступности сервиса может быть достигнуто за счет распределения вычислений на дополнительно созданные копии виртуальных машин и реконфигурирование технических характеристик виртуальных машин.

Для оценки повышения надежности функционирования ИТКС следует использовать коэффициент готовности. Коэффициент готовности представляет собой отношение времени исправной работы к сумме времен исправной работы и вынужденных простоев системы, взятых за один и тот же календарный срок:

$$K_Г = \frac{T_И}{T_И + T_П},$$

где $T_И = \sum_{i=1}^{m} T_{Иi}$ – суммарное время исправной работы системы;

$T_П = \sum_{i=1}^{n} T_{Пi}$ – суммарное время вынужденного простоя.

Число копий и параметры реконфигурации будут зависеть от востребованности сервиса и информационного ресурса, то есть от количества обращений и времени ожидания запроса.

Исходными данными для принятия решения могут послужить результаты мониторинга состояния сервисов и информационных ресурсов ИТКС.

Кроме того, после определения необходимого числа виртуальных машин необходимо решить задачу перераспределения ресурсов ИТКС с учетом гетерогенности ее характера.

На рис. 3 приведен качественный график, на котором представлена зависимость изменения времени обслуживания запроса от интенсивности их поступления в системы без виртуализации и с виртуализацией.

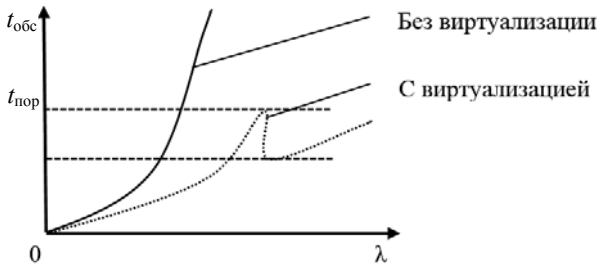


Рис. 3. Качественный график изменения времени обслуживания запроса от интенсивности их поступления в систему

Использование виртуальных машин позволит повысить готовность сервисов ИТКС. Требуемая доступность может быть не всегда достигнута из-за ограничений на количество аппаратных средств ИТКС (ограничение ресурсоемкости аппаратных средств ИТКС). Указанная проблема может быть преодолена за счет приобретения дополнительного оборудования в рамках развития и модернизации информационно-вычислительной системы.

Литература

1. Басыров А.Г., Гончаренко В.А., Забузов В.С., Кремез Г.В, Эсаулов К.А. Повышение устойчивости функционирования бортовых вычислительных систем по результатам космических экспериментов // Известия высших учебных заведений. Приборостроение. – 2009. – Т. 52. – № 4. – С. 70–74.

2. Захаров И.В., Забузов В.С., Фомин С.И., Эсаулов К.А. Способ априорной оценки возможности идентификации пользователей веб-ресурсов на основе энтропийного подхода // Современные проблемы науки и образования. – 2014. – № 1. – URL: www.science-education.ru/115-12004 (дата обращения: 10.02.2014).

3. Аверьянов А.В., Барановский А.М., Эсаулов К.А. Определение пределов аппаратной избыточности информационно-управляющих систем // Известия высших учебных заведений. Приборостроение. – 2014. – Т. 57. – № 3. – С. 23–26.

4. Забузов В.С., Казанцев Д.И., Белая Т.И., Швецов А.С. Способ организации контроля качества обслуживания в инфотелекоммуникационной сети на примере ВКА им. А.Ф. Можайского // Научный обозреватель. – 2014. – № 12. – С. 56–57.

5. Лохвицкий В.А. Подход к построению системы автоматизированной интеграции информации в базу данных для её своевременной актуализации / В.А. Лохвицкий, С.В. Калиниченко, А.А. Нечай // Мир современной науки. – 2014. – № 2 (24). – С. 8–12.

6. Нечай А.А. Выявление недекларированных возможностей аппаратно-программного обеспечения / А.А. Нечай // Экономика и социум. – 2014. – № 1-2 (10). – С. 457–460.

7. Нечай А.А. Специфика проявления уязвимостей в автоматизированных системах управления критически важными объектами / А.А. Нечай, П.Е. Котиков // Современные тенденции в образовании и науке : сборник научных трудов по материалам Международной научно-практической конференции : в 14 ч. – Тамбов, 2014. – С. 96–97.

8. Нечай А.А. Выбор и обоснование показателей эффективности решения задачи распределения объектов по средствам поражения / А.А. Нечай, С.В. Матвеев, В.М. Сафонов // Мир современной науки. – 2014. – № 2 (24). – С. 13–16.

9. Вепрев С.Б. Скрытый метод выявления утечек инсайдерской информации / С.Б. Вепрев, П.И. Гончаров // Вестник Российского нового университета. – 2014. – Вып. 4. – С. 152–155.

УДК 656.02+351.811.12

Е.А. Соснин[1]

ПОСТАНОВКА ЗАДАЧИ РАЗРАБОТКИ ЭФФЕКТИВНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТРАФИКОМ ДОРОЖНО-УЛИЧНОЙ ТРАНСПОРТНОЙ СИСТЕМЫ МЕГАПОЛИСА

В данной статье рассматриваются текущие проблемы транспортной системы г. Москвы, а также мировой опыт в создании интеллектуальной транспортной системы.

Ключевые слова: *интеллектуальная транспортная система, улично-дорожная сеть.*

E.A. Sosnin

STATEMENT OF THE PROBLEM THE DEVELOPMENT OF AN EFFECTIVE CONTROL SYSTEM TRAFFIC ROAD STREET TRANSPORT SYSTEM OF THE METROPOLIS

This article discusses the current problems of the transport system of Moscow, as well as international experience in the creation of intellectual transport system.

Keywords: *intellectual transport system, road network.*

За последние годы в Москве резко возросла интенсивность транспортного движения. С подобными проблемами сталкиваются практически все крупные города мира, и без применения компьютерных средств управления транспортными потоками эту проблему решить практически невозможно.

Мозговой центр подобной системы должен решать следующие задачи:

– уметь оценивать интенсивность потоков транспорта в различных районах города;

– управлять длительностью сигналов светофоров для создания «зеленых волн», с помощью которых «стада» автомобилей, не останавливаясь лишний раз на перекрестках, двигаются в нужных им направлениях;

– оценив интенсивность потока транспорта, управлять его скоростью и, возможно, направлением с помощью интеллектуальных знаков – указателей или прямых директив водителям на световых табло;

– управлять движением потоков транспорта с учетом времени суток;

– уметь понимать команды человека-оператора и передавать их на дорожные контроллеры перекрестков;

– уметь принимать команды полицейских постовых с улиц для оперативного управления движением транспорта с уличного перекрестка;

– работать с беспрецедентной надежностью, так как система должна функционировать круглосуточно, без перерывов.

За последние три года в Москве принят ряд мер по усовершенствованию системы управления и повышению эффективности и престижности общественного транспорта:

– введение выделенных полос с применением аппаратного комплекса фото- и видеофиксации административных правонарушений;

– ввод зон платных парковок.

В центре ГУП «Мосгортранс» развернут программный комплекс для проведения мониторинга передвижения автобусов, следующих по городским маршрутам, с выводом информации о прогнозируемом прибытии автобуса на остановочный пункт. Данный программный комплекс, на мой взгляд, используется не в полном объеме, так как обеспечивает только информационную составляющую функции мониторинга за транспортом, вышедшим на маршрут. Достигнуть более высокого функционала работы комплекса можно было бы в случае организации доступа к местам транспортных инцидентов из центра управления движением г. Москвы для принятия

[1] Аспирант НОУ ВПО «Российский новый университет».

оперативных мер по устранению затруднений в движении маршрутных автобусов. Технически реализовать это можно с помощью средств автоматического регулирования дорожного движения для оперативной передачи информации в соответствующие структуры ГИБДД, ЦООД, ГБУ

На сегодняшний день для достижения поставленных выше целей необходимо объединение всех аппаратных комплексов в одном центре. Необходимо также создание, а в некоторых случаях и разработка алгоритмов управления транспортными потоками. Для принятия правильного решения в управлении транспортными потоками важны доли секунды, и времени для передачи необходимых команд при условиях несовершенной интеграции взаимодействия структур просто нет. В противном случае любые нововведения не несут в себе результатов достижения поставленных целей.

В г. Москве, как и в других мегаполисах, существуют проблемные места в транспортной системе города, и главной проблемой является пропускная способность улично-дорожной сети. Зачастую увеличить пропускную способность невозможно с помощью реконструкций улично-дорожной сети. Такая ситуация складывается особенно в центральной части города. В этом случае правительство Москвы пошло по пути Запада, а именно – создания платного парковочного пространства в центре города с целью обеспечить, тем самым, повышение трафика транспортной сети в часы пик.

С помощью данного организационного решения высоких показателей трафика транспортной сети добиться не удалось по ряду причин, а именно:

– высокого транзитного трафика;

– довольно высокой заселенности центральной части города;

– большого количества людей в центральной части города в силу расположения там административных зданий и рабочих мест.

Формально данную ситуацию можно сформулировать следующим образом.

У участников движения, которые совершают каждодневные поездки в утренние часы из пункта А в пункт В, а в вечернее время – из пункта В в пункт А, существует один и тот же традиционный маршрут, по которому, невзирая на его загруженность, участник движения будет следовать именно этим маршрутом. Часто даже при наличии путей объезда, позволяющих оптимизировать время в пути, водитель этой возможности не использует по ряду причин: отсутствие навигации или просто незнание данного объездного маршрута.

На этот случай Правительство г. Москвы активно внедряет информационные табло, информирующие участников движения о загруженности того или иного участка транспортной сети. К сожалению, эффективность данных табло ничтожно низкая, так как данные табло используются только на 15% их возможности. Причин этому несколько, в том числе:

– неудачное расположение данных табло;

– отсутствие данных табло в центральной части города.

Ключевой причиной низкой эффективности данных устройств является качество информации, которую они сообщают участникам движения, а скорей всего ресурс, через который они это делают (комплекс «Яндекс пробки»).

Технология работы данного ресурса в рамках мегаполиса несовершенна по причине неактуальности и недостоверности предоставления информации ее пользователям – участникам движения. Зачастую при построении маршрута данный ресурс предоставляет ее пользователю искаженную информацию о дорожной ситуации, что приводит к увеличению заторов и времени в пути. В данном случае можно предложить, а точней скопировать, технологию австрийских инженеров, разработавших проект «Зеленая улица». Этот проект предусматривает установку светофорных объектов, меняющих свой режим работы в соответствии с увеличением или снижением интенсивности трафика.

Однако одними светофорами в рассматриваемой здесь ситуации не обойдешься. Из австрийской технологии «Зеленая улица» нам необходима ее основа – это системы оценки плотности и интенсивности загруженности транспортного канала. Основываясь на полученных данных с контроллеров, установленных на улично-дорожной сети города Москвы, можно будет предоставлять водителям актуальную информацию о загруженности трассы и об актуальном прогнозировании увеличения интенсивности трафика транспортного потока. Данная информация может быть доступна участникам движения через мобильные приложения и через те самые информационные табло, с которых участник движения сможет получать актуальную информацию. Посредством данных контроллеров также можно получать предварительную информацию о ДТП и о наличии попавших в аварию автомобилей, создающих препятствия в движении. После получения подобной информации в центре управления дорожным движением ее подтверждают или опро-

вергают и при необходимости передают оперативным службам.

При наличии подобной системы можно прогнозировать эксплуатационным службам производство работ по содержанию улично-дорожной сети менять дислокацию и места производства работ в зависимости от нарастания уровня загруженности трассы, а также проводить анализ дорожно-транспортных происшествий с привязкой к конкретному адресу. Конечно, ключевой ролью данной системы будет являться навигация участников движения. Для повышения экономических показателей данное решение можно внедрять совместно с проектом «Умные светофорные объекты».

Проводить параллель между Западом и Россией в вопросе интеллектуальной транспортной системы трудно в силу различного рода факторов и обстоятельств. Одним из данных факторов является то, что в Европе этим вопросом занимаются целые отрасли не в рамках отдельного мегаполиса, а в рамках континента. Безусловно, не стоит забывать и тот момент, что данным вопросом в Европе озабочены уже порядка 15 лет. К немаловажным факторам относится и уровень жизни, развитость и престижность общественного транспорта в рамках мегаполиса, а также и в рамках страны. К примеру, в европейских государствах создание пространств платных парковок прошло немного по другому сценарию, и многие государства были готовы к данному решению, подойдя к нему:

– с развитой системой общественного транспорта;

– с высокими тарифами на парковочные места в центральных частях города;

– с высокой стоимостью ГСМ;

– с высокими налогами на владение автомобильным транспортом.

Не последнее место занимает здесь и экономическая составляющая передвижения на автотранспорте. В Европе это дорогое удовольствие и, если можно так сказать, не по своей воле граждане пересели на общественный транспорт. Во многих европейских государствах развит велотранспорт и мототранспорт в силу климатических особенностей государств.

И если на сегодняшний день в России, а именно в мегаполисах, пытаются создать и создают эффективную транспортную систему, то далеко не на первом месте стоит задача снижения количества единиц личного транспорта. В Европе же при создании эффективной транспортной системы больший акцент сделан на использовании общественного транспорта.

В России транспортная проблема больше похожа на проблему Японии. Но сходство ее лишь в том, что, в силу географических особенностей государства, правительству приходится разрабатывать интеллектуальную комплексную систему не только для общественного транспорта, но и для личного. Но и здесь сравнение с Россией будет неправильным. В Японии проблемой транспорта занимаются порядка 40 лет, и на сегодняшний день в этой стране есть четко сформулированные задачи научными концернами, занимающимися постоянным усовершенствованием действующей интеллектуальной системы. К примеру, к 2018 году все автомобильные концерны Японии, производящие автомобили, обязаны установить интеллектуальные модули в свои машины, которые в процессе эксплуатации участником движения будут принимать актуальную информацию в режиме онлайн о наличии ДТП, о заторах на тех или иных участках улично-дорожной сети, а также строить маршрут в автоматическом режиме и корректировать его во время следования.

Для технического решения данной транспортной проблемы можно использовать методы анализа и проектирования сложных информационных систем. Целью такого формализованного подхода к данной проблеме является построение оптимального алгоритма управления транспортными потоками по классическому критерию минимакса. В данной задаче этот критерий звучит следующим образом: минимальное время доведения информации до технических средств регулирования транспортным потоком при обеспечении максимально возможного трафика дорожно-уличного движения.

Литература

1. www.wikipedia.org

2. Эндрю Доуни. Самые ужасные пробки в мире. – 2008. – 21 апреля.

3. Заторы: национальный вопрос. – 2008. – 29 августа.

СВЕДЕНИЯ ОБ АВТОРАХ

Басыров Александр Геннадьевич – доктор технических наук, профессор, начальник кафедры «Информационно-вычислительных систем и сетей» Военно-космической академии им. А.Ф. Можайского, тел.: 8-911-248-57-80, e-mail: alexanderbas@mail.ru

Бурцева Людмила Александровна – магистрант НОУ ВПО «Российский новый университет», тел.: 8-926-582-66-83, e-mail: lyudmaksimova@yandex.ru

Гладышев Анатолий Иванович – кандидат технических наук, доцент, доцент кафедры ИТиЕНД, НОУ ВПО «Российский новый университет», тел.: 8-926-221-3026, e-mail: tolyagladyshev@yandex.ru

Гришин Игорь Юрьевич – доктор технических наук, профессор, профессор кафедры компьютерных технологий и информационной безопасности ФГБОУ ВПО «Кубанский государственный технологический университет», тел.: +7-978-805-50-07, e-mail: igugri@gmail.com

Денисенков Дмитрий Анатольевич – инженер кафедры технологий и средств геофизического обеспечения войск. ФГКОУ ВПО «Военно-космическая академия им. А.Ф. Можайского» Министерства обороны Российской Федерации (ВКА им. А.Ф. Можайского), e-mail: dimasden@yandex.ru, vka@mil.ru

Дудкин Андрей Сергеевич – кандидат технических наук, преподаватель кафедры информационно-вычислительных систем и сетей ВКА им. А.Ф. Можайского, тел.: 8-911-964-16-33, e-mail: Andrew-ll@mail.ru

Жуков Владимир Юрьевич – кандидат технических наук, старший научный сотрудник 32 отдела ВИНИ. ФГКОУ ВПО «Военно-космическая академия им. А.Ф. Можайского» Министерства обороны Российской Федерации (ВКА им. А.Ф. Можайского), e-mail: vuzhukov2002@list.ru, vka@mil.ru

Забузов Вячеслав Сергеевич – кандидат технических наук, старший преподаватель Военно-космической академии им. А.Ф. Можайского, e-mail: zzvvss80@mail.ru

Зайцев М.А. – кандидат технических наук, доцент кафедры математики и информатики Московского университета им. С.Ю. Витте, тел: 8-916-279-94-34.

Золотарев Олег Васильевич – кандидат технических наук, доцент, доцент НОУ ВПО «Российский новый университет», тел.: 8-903-262-44-05, e-mail: ol-zolot@yandex.ru

Казанцев Денис Иванович – Военно-космическая академия им. А.Ф. Можайского, e-mail: zilan.ka@yandex.ru

Киреев Андрей Павлович – старший научный сотрудник Военно-космической академии им. А.Ф. Можайского, e-mail: Kireeff@yandex.ru

Клименко Игорь Семенович – доктор физико-математических наук, профессор, профессор кафедры информационных систем в экономике и управлении НОУ ВПО «Российский новый университет», тел.: +7(916)166-35-82, e-mail: igor.k41@yandex.ru

Костырин Александр Александрович – преподаватель Военно-космической академии им. А.Ф. Можайского, e-mail: kosta-78@list.ru

Котиков Павел Евгеньевич – кандидат технических наук, доцент Военно-космической академии им. А.Ф. Можайского, e-mail: kotikovpe@rambler.ru

Крюковский Андрей Сергеевич – доктор физико-математических наук, профессор, декан факультета ИСиКТ НОУ ВПО «Российский новый университет», e-mail: kryukovsky@rambler.ru

Лауфер Константин Маркович – кандидат философских наук, доцент, доцент кафедры экономики и менеджмента МГМУ им. А.И. Сеченова, тел.: 8-926-953-73-31, 8-926-656-25-05, e-mail: klaufer@yandex.ru.

Марковский Алексей Сергеевич – кандидат технических наук, старший научный сотрудник Военно-космической академии им. А.Ф. Можайского, e-mail: leexx26@list.ru

Митряев Э.И. – доктор технических наук, профессор, профессор кафедры информационной безопасности факультета информационных систем и компьютерных технологий НОУ ВПО «Российский новый университет».

Мухин Владимир Иванович – доктор военных наук, профессор, профессор кафедры информационных систем и технологий Академии гражданской защиты МЧС России, тел.: 8-916-783-58-96.

Нечай Александр Анатольевич – преподаватель Военно-космической академии им. А.Ф. Можайского, e-mail: webexpromt@mail.ru

Отарашвили Зураб Автандилович – университет Иннополис, г. Иннополис, Республика Татарстан, e-mail: z.otarashvili@innopolis.ru

Плуталов Максим Александрович – аспирант НОУ ВПО «Российский новый университет», тел.: +7(916)353-84-46, e-mail: maxplutalov@gmail.com

Рекунков Иван Сергеевич – кандидат технических наук, доцент кафедры защиты информации Московского государственного университета информационных технологий, радиотехники и электроники, тел.: 8-985-779-56-43.

Санин Михаил Дмитриевич – научный сотрудник Военно-космической академии им. А.Ф. Можайского, e-mail: sanin.mih@yandex.ru

Сафонов Вадим Максимович – адъюнкт кафедры математического и программного обеспечения Военно-космической академии им. А.Ф. Можайского, тел.: +7-911-161-47-96, e-mail: safonov-vm@mail.ru

Скворцова Юлия Игоревна – заместитель декана факультета ИСиКТ НОУ ВПО «Российский новый университет», e-mail: Julia_bova@mail.ru

Соснин Евгений Александрович – аспирант НОУ ВПО «Российский новый университет», тел.: +7-962-957-13-74, e-mail: tapok_07@inbox.ru

Холодков Сергей Викторович – аспирант НОУ ВПО «Российский новый университет», e-mail: igor.k41@yandex.ru

Чеботарев Григорий Андреевич – аспирант НОУ ВПО «Российский новый университет», тел.: +7(926)380-58-45, e-mail: chebotarevg@mail.ru

Шинкаренко Антон Федорович – адъюнкт кафедры информационно-вычислительных систем и сетей ВКА им. А.Ф. Можайского, тел.: 8-981-859-68-71, e-mail: Tonio87@rambler.ru

Широбоков Владислав Владимирович – адъюнкт кафедры «Информационно-вычислительных систем и сетей» Военно-космической академии им. А.Ф. Можайского, тел.: 8-981-761-28-41, e-mail: vladislavbars@gmail.com

Эсаулов Константин Андреевич – кандидат технических наук, старший преподаватель Военно-космической академии им. А.Ф. Можайского, e-mail: home5263@yandex.ru

УКАЗАТЕЛЬ СТАТЕЙ, ОПУБЛИКОВАННЫХ В ЖУРНАЛЕ

«Вестник Российского нового университета» в 2014 году

ВЫПУСК 1 Психологические науки Педагогические науки Филологические науки	
Психологические науки	
В.С. Агапов, Л.Н. Кулешова, В.В. Саванович	*Особенности рефлексивного Я современного менеджера*
Л.С. Подымова, М.С. Фиронова	*Проблема социализации личности и развития инновационности в условиях социальных изменений*
М.А. Хмелькова	*Влияние уровня развития познавательной сферы дошкольника на освоение им образовательной программы ДОУ*
В.П. Каширин	*Методологические основания психологии*
Ю.М. Караяни	*Психологический аспект в медицинском подходе к реабилитации инвалидов*
Л.Н. Кулешова	*Антропологический подход к проблемам воспитания личности*
Е.В. Звонова	*Символизация и метакогнитивное опосредование: продолжение культурно-исторической традиции*
Н.Н. Азарнов, А.Н. Азарнова	*Способы предупреждения межличностных конфликтов в производственных организациях*
В.Н. Чернышова	*Этнопсихологические аспекты превенции межэтнических конфликтов в образовательной студенческой среде*
Л.В. Тарабакина, Т.Л. Шабанова	*Смысл тревоги в деятельности учителя*
Е.Ю. Шогорева	*Системно-антропологический подход к проблеме самореализации обучаемых в военном вузе*
А.И. Сысоева	*Устойчивость групповой сплоченности и ее связь со стилем эмоциональной регуляции*
С.В. Феоктистова, И.В. Кулева	*Связь особенностей темперамента и механизмов психологической защиты личности в конфликте*
Ю.В. Колесова	*Психологические аспекты имидж-консультирования*
А.М. Боровик	*Содержательные, процессуальные и результативные аспекты психологической адаптированности воспитанников кадетской школы-интерната*

Педагогические науки	
К.В. Бакланов	*Использование мультимедийных презентацийв процессе адаптации студентов-первокурсниковк обучению в вузе*
С.С. Будущева	*Проблемы формирования грамматической иноязычной компетенции у студентов неязыковых направлений подготовки*
М.В. Гирская	*Психолого-педагогические основы подготовки специалистов по правовому обеспечению национальной безопасности в военных вузах*
Т.А. Головятенко	*Субъектные функции образования в развитии творческих способностей будущего специалиста*
Г.С. Исакова	*Модель процесса формирования организационной культуры студентов колледжа*
О.Ю. Сударева	*Психолого-педагогическая подготовка врачей-специалистов к профессиональному общению в ходе научно-практических конференций и лекториев*
С.В. Тенитилов	*Влияние педагогического идеала на адаптацию преподавателя в системе дистанционного обучения*
Г.А. Шабанов	*Критериальные признаки отличия педагогического творчества от псевдотворчества в деятельности преподавателей вузов*
С.В. Шевцова	*Компоненты педагогической системы профессиональной подготовки курсантов*
Е.И. Юдина	*Теоретико-практические аспекты применения метода проектов в образовательном процессе вуза*
О.В. Иванова, И.Н. Мороз	*Особенности обучения иностранному языку в курсе магистерской подготовки неязыкового профиля*
М.Ю. Антропова	*Тьюторство в процессе повышения квалификации педагогических кадров по русскому языку как неродному*
Филологические науки	
М.Н. Алексеева, Л.М. Андросова	*Использование метода актуального членения для исследования сверхфразовых единств в связном тексте*
Р.Х. Анопочкина	*Пути формирования коммуникативной компетенции студентов продвинутого этапа обучения*
Т.А. Голикова	*Коммуникативный тренинг: психолингвистическое экспериментальное исследование*
Н.Л. Грейдина	*К основам разработки прагмакоммуникативно-функционального подхода в процессе обучения русскому языку как близкородственному (на примере болгарской аудитории)*

А.А. Кашликова	*Оценка финансовой устойчивости и ликвидности баланса ОАО «Аэрофлот»*
Е.А. Дудко	*Управление дебиторской и кредиторской задолженностью компании*
О.С. Нуянзина	*Исследование концепции "Value Based Management" и ее влияние на рост финансовых показателей компании*
Малый и средний бизнес в современных условиях	
Т.А. Шпилькина	*Оценка проблем развития малого и среднего бизнеса в РФ в современных условиях*
О.Н. Левшина	*Конкурентная функциональная дифференциация в бизнесе*
О.В. Глинкина	*Антикризисная стратегия компании: опыт разработки и реализации*
М.В. Волошина, О.В. Мигеева	*Оценка коммерческих рисков предприятий в процессе анализа кредитоспособности*
Л.В. Курмаева	*Развитие форм финансового обеспечения деятельности муниципальных учреждений*
Ю.А. Кувшинова	*Концепция финансирования негосударственного образовательного учреждения*
В.К. Алексанян	*Адаптация модели размещения государственного заказа для сектора образовательных услуг (по данным конкурсов Московского правительства)*
Ж.Б. Орманова	*Управление маркетингом: определение места обучающего компонента в границах позиционно-деятельностного поведения организации*
М.М. Новикова	*Развитие персонала организации как механизм повышения конкурентоспособности специалиста*
Л.И. Еременская, О.В. Степнова	*Бренд как интеллектуальная собственность, влияющая на сознание*
Мировая экономика	
Г.Г. Андреев, О.И. Карлова	*Теория и практика международной торговли: из опыта России*
И.А. Квасов, Е.Г. Бутурлакина	*Рейтинг инвестиционной привлекательности регионов стран Таможенного союза*
А.А. Поливалов	*Анализ развития рынка долговых инвестиционных инструментов РФ в период нестабильности мировой экономики*
Т.М. Регент, А.В. Королёва	*Международная миграция как источник стратегии экономического роста Филиппин*

Рекреация и туризм	
Н.В. Вдовина	*Сочетание современных инновационных решений в туризме с русскими традициями*
М.Н. Войт	*Методика комплексной оценки качества обслуживания туристов в речном круизе*
К.Ш. Загаштокова	*Исследование особенностей организации обслуживания гостей во время их пребывания в отеле*
Т.И. Зворыкина, С.В. Михайленко	*Экономические аспекты организации и проведения капитального ремонта многоквартирных домов в различные периоды времени*
Т.И. Зворыкина, И.О. Яшина	*Основные направления развития потребительского рынка крупного города*
Т.А. Котова	*Корпоративная культура как фактор повышения конкурентоспособности организации*
С.М. Кочетков	*Анализ инвестиционного климата в туризме на примере Орловской области*
Д.Д. Макарова	*Обзор научно-исследовательских работ по тематике туристской дестинации*
А.В. Мешков	*Анализ состояния и перспектив развития сферы туристских перевозок в России*
М.М. Морозов	*Риски страхования туроператоров*
М.А. Морозов, Д.Ю. Дудецкий	*Механизм развития конкурентных преимуществ туристской дестинации*
Н.С. Морозова, С.И. Дружинина	*Эффективность туризма: виды и методы оценки*
Е.А. Перепелица	*Исследование влияния рекламы на потребности туристов*
М.В. Романова	*Исследование особенностей директ-маркетинга в туризме*
М.С. Солонцева	*История и перспективы развития усадьбы и усадебного туризма*
О.В. Федоткина	*Исследование современных подходов к разработке брендов туристских дестинаций*
З.П. Филькова	*Особенности ресурсной базы детского туризма в Российской Федерации*

ВЫПУСК 4 Управление, вычислительная техника и информатика	
Математическое моделирование физических процессов	
Е.Б. Ипатов, С.П. Кузнецов, И.В. Мешков, А.В. Шелагин	*Численное моделирование полных сечений рассеяния очень холодных нейтронов на сплошном бесконечном круговом цилиндре*
А.С. Крюковский, С.В. Рогачев	*Архитектура программного комплекса расчета специальных функций волновых катастроф*
Е.А. Палкин, Я.М. Черняк	*Асимптотическая оценка затухания волнового поля в зоне каустической тени с учетом вариаций показателя преломления*
Е.А. Палкин, А.Е. Сергеев	*Особенности фокусировки поверхностных акустических волн на сфере*
П.С. Крюков, В.Т. Поляков	*Анализ состояния ионосферы и процессов в ее отражающих слоях по данным приема сигнала биений несущих вещательных КВ-станций*
П.С. Крюков, В.Т. Поляков	*Метод биений в доплеровских ионосферных наблюдениях*
В.Т. Поляков	*О стабильности частоты настройки телекоммуникационных приемников*
П.С. Крюков, В.Т. Поляков	*Удалённый мониторинг прохождения радиоволн КВ-диапазона*
И.С. Клименко, С.В. Холодков	*Распределение полей давления и деформаций, возникающих при ударе твердого тела о деформируемую преграду*
Математическое моделирование в экономике и управлении	
Л.В. Лабунец, Н.Л. Лебедева, М.Ю. Чижов	*Нечетко-множественная кластеризация поступлений в московский бюджет от рынка наружной рекламы*
Л.В. Лабунец, Е.Л. Лабунец, Н.Л. Лебедева	*Экспертная модель скоринга биржевых активов*
Л.В. Лабунец, Е.Л. Лабунец, Н.Л. Лебедева	*Байесовская модель скоринга биржевых активов*

О.В. Золотарёв, Е.Б. Козеренко, М.М. Шарнин	*Принципы построения моделей бизнес-процессов предметной области на основе обработки текстов естественного языка*
О.В. Золотарёв	*Процессный подход к управлению в проектах внедрения корпоративных информационных систем*
А.В. Бобряков, Е.А. Тихонова, М.В. Раскатова, Д.А. Щербаков	*Подходы к реализации программно-технических средств уровня подведомственных бюджетных учреждений в информационной системе мониторинга финансово-хозяйственной деятельности*
А.В. Бобряков, А.И. Гаврилов, А.Г. Стефанцов, Е.А. Тихонова, М.В. Раскатова	*Разработка информационно-статистической базы учета объемов государственных заданий и проведения расчетов финансового обеспечения оказания государственных услуг*
И.Н. Камышная	*Реинжиниринг бизнес-процессов на примере Западно-Сибирской транспортной прокуратуры*
А.К. Белайчук, А.А. Кастанова	*Современные средства моделирования бизнес-процессов в дипломном проектировании*
К.М. Лауфер, З.А. Отарашвили	*Алгоритм реализации проекта на основе метода уступок и компромиссов*
О.Л. Трефилова, М.В. Раскатова, О.Г. Скуратовская	*Применение методов реинжиниринга бизнес-процессов на крупном предприятии*
Информационные и телекоммуникационные системы	
В.Е. Анциперов, И.В. Забросаев, В.А. Зернов	*Использование аналитических спектров для задач детектирования сердечного ритма человека*
А.И. Гладышев	*Вопросы создания единого информационного пространства в космотехносфере*
И.С. Клименко, Л.В. Шарапова	*К исследованию феномена информации*
А.И. Гладышев, А.О. Жуков	*Методика использования искусственных нейронных сетей с целью идентификации параметров движения летательных аппаратов*
Информационная безопасность	
С.Б. Вепрев, П.И. Гончаров	*Скрытый метод выявления утечек инсайдерской информации*
Б.И. Скородумов	*Современные проблемы отечественного профессионального стандарта информационной безопасности*

ПРАВИЛА ПРЕДСТАВЛЕНИЯ АВТОРСКИХ РУКОПИСЕЙ
в журнал «Вестник Российского нового университета»

Журнал входит в Перечень ведущих рецензируемых научных журналов и изданий, рекомендованных ВАК для публикации основных результатов диссертационных исследований. Журнал выходит 12 раз в год по сериям (4 выпуска в каждой серии):

- Человек в современном мире.
- Человек и общество.
- Сложные системы: модели, анализ и управление.

К публикации принимаются материалы, соответствующие тематике серий журнала, получившие положительное заключение рецензента.

Статья должна отвечать профилю журнала и его рубрикам, быть оригинальной, нигде ранее не опубликованной, не нарушающей авторских прав третьих лиц.

Сроки публикации статьи зависят от серии, в которую входит статья, принятая к публикации в журнале.

1. Статья должна содержать:

– УДК (см., например, здесь: http://naukapro.ru/metod. htm);
– сопроводительное письмо (отзыв заведующего кафедрой о представленной работе, рекомендации руководителя организации, учреждения);
– название на *русском* и *английском* языках (располагается под фамилией автора);
– фамилии и инициалы авторов на *русском* и *английском* языках (например: И.И. Иванов, I.I. Ivanov – сначала инициалы, затем – фамилия);
– аннотацию (300–500 печ. знаков с пробелами) на *русском* и *английском* языках;
– ключевые слова (не более 7 слов или словосочетаний) на *русском* и *английском* языках;
– список литературы на русском языке («Литература»). Списки литературы оформляются в соответствии с библиографическими требованиями (ГОСТ Р 7.0.5 – 2008 «Библиографическая ссылка. Общие требования и правила составления») в едином формате, установленном РУНЭБ;
– краткие сведения об авторах, включающие фамилию, имя, отчество (полностью), ученую степень, ученое звание (полностью с расшифровкой, например: кандидат психологических наук), должность и место работы, контактный телефон, адрес электронной почты. Все эти данные помещаются на отдельной странице.

2. Статья представляется в электронном варианте на **CD-диске** в виде файла формата *MS Word* (*.*doc*) и одного экземпляра распечатки. Название файла должно состоять из фамилии автора и названия статьи. Набор текста осуществляется шрифтом *Times New Roman* кеглем 14. Интервал между строками – 1,5. Выравнивание текста – по ширине; ссылки на формулы даются в круглых скобках. Объем текста не должен превышать 1 авторского листа (40 тыс. печ. знаков с пробелами), включая библиографический список, названия таблиц и подрисуночные подписи. Статья должна иметь сквозную нумерацию и на последней странице авторского экземпляра содержать подписи всех авторов.

– В тексте допускаются выделения шрифтами: **полужирный прямой**, ***полужирный курсив***, *светлый курсив*. Примеры рекомендуется выделять *курсивом;* заголовки, подзаголовки, новые термины и понятия – **полужирным** шрифтом.

Не рекомендуется использовать:
такие выделения, как ПРОПИСНЫЕ БУКВЫ, р а з р я д к а через пробел и подчеркивание; подстрочные ссылки.

3. Рисунки могут быть включены в файл текста и иметь сквозную нумерацию. Кроме этого они ***обязательно*** должны быть ***представлены отдельным файлом*** в формате (*.tif), (*.psd), (*.jpg) с разрешением не менее 300 dpi, в черно-белом изображении. Подрисуночные подписи следует набирать сразу же после ссылки на рисунок. То же самое относится и к таблицам. Текст таблиц не должен выходить за пределы ячеек. Таблицы должны быть представлены в формате *MS Word*.

Не принимаются к рассмотрению нечитаемые сканированные рисунки.

4. При наборе формул следует использовать программу ***Mach Type***; для набора символов – шрифт *Euclid Symbol*.

При наборе графиков использовать шрифты ***Times New Roman***, ***Arial***.

Графики, выполненные в программе Excel, присылаются отдельным файлом вместе с табличными данными.

Не принимаются сканированные графики, формулы, таблицы.

5. Список литературы приводится в конце статьи в порядке цитирования (упоминания) источников в тексте. Ссылки на литературные источники в тексте даются путем указания в квадратных скобках порядкового номера цитируемого источника и страницы, например [2, с. 37], [3–7].

Не принимается список литературы в виде подстрочных ссылок, вынесенных в сноску.

6. Примечания к тексту оформляются в форме постраничных сносок (не более двух строк).

7. Статьи публикуются в авторской редакции. Авторы статей целиком несут ответственность за полноту и достоверность цитируемой в них литературы, приведенных фактов, статистических данных, имен собственных, географических названий и прочих сведений, а также за использование материалов, не предназначенных для открытой печати.

8. Плата с аспирантов за опубликование рукописей не взимается.

Прочие условия публикации

Редакция оставляет за собой право тематического отбора, грамматического и стилевого редактирования поступивших материалов. Мнения авторов, изложенные в статьях, могут не совпадать с мнением редакции. Поступившие в редакцию рукописи не возвращаются.

Авторы несут ответственность за содержание статей, за сам факт их публикации, а также за ущерб, причиненный третьим лицам, если выяснится, что в процессе публикации статьи были нарушены чьи-либо права или общепринятые нормы научной этики.

Автору может быть отказано в публикации, если:

– его статья не оформлена в соответствии с данными правилами;

– автор отказался от доработки статьи согласно требованиям рецензента и редакционной коллегии;

– автор не устранил в срок указанные рецензентом ошибки и недостатки;

– текст статьи содержит более 10% заимствований.

Окончательное решение о публикации материалов принимает редакционная коллегия.

Электронная почта Редакционно-издательского дома (РИД) НОУ ВПО «Российский новый университет» **ridrosnou@mail.ru**

Вестник Российского нового университета

Серия
«Сложные системы: модели, анализ и управление»

Выпуск 2

Ответственная за выпуск

А.В. Голева

Дизайн *Е.М. Матюхиной*
Компьютерная верстка *С.Н. Шевченко*

Подписано в печать 16.10.2015 г. Формат 60x84/8. Печать офсетная.

Усл. печ. л. 13,0. Тираж 200 экз. Заказ № 22.

Российский новый университет.
105005, г. Москва, ул. Радио, д. 22.

Отпечатано
в ИП Шуруева Марина Алексеевна.
142600, Московская обл., г. Орехово-Зуево,
ул. Стачки 1885 года, д. 6.
e-mail: info@orehovoprint.ru.

ДЛЯ ЗАМЕТОК