сетевой научный журнал ISSN 2518-1092

НАУЧНЫЙ РЕЗУЛЬТАТ

RESEARCH RESULT

Том 4 | № 1
Volume 4 | 2019

НАУЧНЫЙ РЕЗУЛЬТАТ. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

RESEARCH RESULTS. INFORMATION TECHNOLOGY

Сайт журнала:
rrinformation.ru
сетевой научный рецензируемый журнал
online scholarly peer-reviewed journal

НАУЧНЫЙ РЕЗУЛЬТАТ
RESEARCH RESULT

НАУЧНЫЙ РЕЗУЛЬТАТ. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
RESEARCH RESULT. INFORMATION TECHNOLOGIES

Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
Свидетельство о регистрации средства массовой информации Эл. № ФС77-69101 от 14 марта 2017 г.

The journal has been registered at the Federal service for supervision of communications information technology and mass media (Roskomnadzor)
Mass media registration certificate El. № FS 77-69101 of March 14, 2017

Том 4, № 1. 2019

Volume 4, № 1. 2019

СЕТЕВОЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
Издается с 2016 г.
ISSN 2518-1092

ONLINESCHOLARLYPEER-REVIEWEDJOURNAL
First published online: 2016
ISSN 2518-1092

Учредитель: Федеральное государственное автономное образовательное учреждение высшего образования
«Белгородский государственный национальный исследовательский университет»
Издатель: НИУ «БелГУ». Адрес издателя: 308015 г. Белгород, ул. Победы, 85.
Журнал выходит 4 раза в год

Founder: Federal state autonomous educational establishment of higher education
«Belgorod State National Research University»
Publisher: Belgorod State National Research University
Address of publisher: 85 Pobeda St., Belgorod, 308015, Russia
Publication frequency: 4 /year

СОДЕРЖАНИЕ

CONTENTS

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ
COMPUTER SIMULATION HISTORY

УДК 621.396.01 **DOI: 10.18413/2518-1092-2019-4-1-0-1**

Черноморец Д.А.[1]
Болгова Е.В.[1]
Черноморец А.А.[1]
Барсук А.А.[2]

ПРЕДСТАВЛЕНИЕ ИЗОБРАЖЕНИЙ НА ОСНОВЕ БАЗИСА СОБСТВЕННЫХ ВЕКТОРОВ СУБПОЛОСНЫХ МАТРИЦ КОСИНУС-ПРЕОБРАЗОВАНИЯ

[1)] Белгородский государственный национальный исследовательский университет, ул. Победы д. 85, г. Белгород, 308015, Россия
[2)] Общество с ограниченной ответственностью «АйТиДи», ул. Промышленная д. 6, г. Белгород, 308023, Россия

e-mail: Chernomorets@bsu.edu.ru

Аннотация
В работе предложен оригинальный ортонормированный базис, составленный из собственных векторов субполосных матриц косинус-преобразования, соответствующих заданной подобласти области определения косинус-преобразования. Показано разложение цифровых изображений по векторам предложенного базиса. Введено понятие базисных изображений в двумерном базисе собственных векторов субполосных матриц косинус-преобразования. Показаны свойства базисных изображений и коэффициентов разложения изображения Ф по предложенному базису. Приведены результаты вычислительных экспериментов, демонстрирующих особенности распределения значений полученных коэффициентов разложения изображений.
Ключевые слова: изображение; косинус-преобразование; субполосные матрицы; коэффициенты разложения; собственные векторы.

UDC 621.396.01

Chernomorets D.A.[1]
Bolgova E.V.[1]
Chernomorets A.A.[1]
Barsuk A.A.[2]

IMAGES PRESENTATION BASED ON SUBBAND COSINE TRANSFORM MATRIX EIGENVECTORS BASIS

[1)] Belgorod State National Research University, 85 Pobedy St., Belgorod, 308015, Russia
[2)] Limited Company "ITD", 6 Promyshlennaya St., Belgorod, 308023, Russia

e-mail: Chernomorets@bsu.edu.ru

Abstract
We propose an original orthonormal basis composed of the eigenvectors of subband cosine transform matrices corresponding to a given subdomain of the cosine transform definition domain. The decomposition of digital images onto vectors of the proposed basis is shown. The concept of basic images in the two-dimensional basis of eigenvectors of subband cosine transform matrices is introduced. The properties of the basis images and image decomposition coefficients according to the proposed basis are shown. The results of computational experiments that demonstrate the features of the distribution of the values of the obtained image decomposition coefficients are presented.
Keywords: image; cosine transform; subband matrices; decomposition coefficients; eigenvectors.

Распространение, обработка и использование изображений в электронной форме является неотъемлемой частью практически всех современных информационных систем. Во многих случаях целесообразно для анализа изображений применять их субполосный анализ-синтез на основе косинус-преобразования по дискретным данным [1]. В работах [2, 3] показано, что его для его осуществления используется математический аппарат субполосных матриц косинус-преобразования.

Рассмотрим представление изображений на основе базиса собственных векторов субполосных матриц косинус-преобразования. Пусть изображение задано в виде матрицы вещественных значений $\Phi = (f_{ik})$, $i = 1,2,...,N_1$, $k = 1,2,...,N_2$, элементы которой соответствуют яркости отдельных пикселей изображения.

Пусть заданной подобласти пространственных частот [4] $V_{r_1 r_2}$ (ППЧ) области определения косинус-преобразования соответствуют субполосные матрицы косинус-преобразования G_{r_1} и H_{r_2}, размерности $N_1 \times N_1$ и $N_2 \times N_2$ соответственно.

Субполосные матрицы косинус-преобразования G_{r_1} и H_{r_2} являются вещественными, симметричными матрицами, следовательно, их можно представить в виде следующих разложений:

$$G_{r_1} = Q_{r_1} L_{r_1} Q_{r_1}^T, \quad H_{r_2} = U_{r_2} M_{r_2} U_{r_2}^T, \tag{1}$$

где столбцы матриц Q_{r_1} и U_{r_2} являются собственными векторами матриц G_{r_1} и H_{r_2}, на главной диагонали матриц L_{r_1} и M_{r_2} расположены собственные числа матриц G_{r_1} и H_{r_2},

$$Q_{r_1} = (\vec{q}_1^{\,r_1}, \vec{q}_2^{\,r_1}, ..., \vec{q}_{N_1}^{\,r_1}), \quad U_{r_2} = (\vec{u}_1^{\,r_2}, \vec{u}_2^{\,r_2}, ..., \vec{u}_{N_2}^{\,r_2}), \tag{2}$$

$$L_{r_1} = diag(\lambda_1^{r_1}, \lambda_2^{r_1}, ..., \lambda_{N_1}^{r_1}), \quad M_{r_2} = diag(\mu_1^{r_2}, \mu_2^{r_2}, ..., \mu_{N_2}^{r_2}).$$

Рассмотрим матрицу $\Gamma^{r_1 r_2} = (\gamma_{ik}^{r_1 r_2})$, $i = 1,2,...,N_1$, $k = 1,2,...,N_2$,

$$\Gamma^{r_1 r_2} = Q_{r_1}^T \Phi U_{r_2}, \tag{3}$$

элементы $\gamma_{ik}^{r_1 r_2}$, $i = 1,2,...,N_1$, $k = 1,2,...,N_2$, которой представленные в виде

$$\gamma_{ik}^{r_1 r_2} = (\vec{q}_i^{\,r_1})^T \Phi \vec{u}_k^{\,r_2}, \tag{4}$$

можно считать значениями коэффициентов разложения [5] изображения Ф по ортогональным векторам $\vec{q}_i^{\,r_1}$, $i = 1,2,...,N_1$, и $\vec{u}_k^{\,r_2}$, $k = 1,2,...,N_2$, субполосных матриц косинус-преобразования G_{r_1} и H_{r_2}, соответствующих заданной подобласти пространственных частот (ПЧ) $V_{r_1 r_2}$.

Очевидно, что произведение матрицы коэффициентов разложения $\Gamma^{r_1 r_2}$ на матрицы Q_{r_1} и $U_{r_2}^T$, составленные из соответствующих собственных векторов, совпадает с изображением Ф,

$$\Phi = Q_{r_1} \Gamma^{r_1 r_2} U_{r_2}^T. \tag{5}$$

Представим правую часть соотношения (5) в виде произведения элементов соответствующих матриц,

$$Q_{r_1} \Gamma^{r_1 r_2} U_{r_2}^T = (\vec{q}_1^{\,r_1} \vec{q}_2^{\,r_1} ... \vec{q}_{N_1}^{\,r_1}) \begin{pmatrix} \gamma_{11}^{r_1 r_2} \gamma_{12}^{r_1 r_2} ... \gamma_{1N_2}^{r_1 r_2} \\ \gamma_{21}^{r_1 r_2} \gamma_{22}^{r_1 r_2} ... \gamma_{2N_2}^{r_1 r_2} \\ ... \\ \gamma_{N_1 1}^{r_1 r_2} \gamma_{N_1 2}^{r_1 r_2} ... \gamma_{N_1 N_2}^{r_1 r_2} \end{pmatrix} \begin{pmatrix} (\vec{u}_1^{\,r_2})^T \\ (\vec{u}_2^{\,r_2})^T \\ ... \\ (\vec{u}_{N_2}^{\,r_2})^T \end{pmatrix} = (\vec{s}_1 \vec{s}_2 ... \vec{s}_{N_2}) \begin{pmatrix} (\vec{u}_1^{\,r_2})^T \\ (\vec{u}_2^{\,r_2})^T \\ ... \\ (\vec{u}_{N_2}^{\,r_2})^T \end{pmatrix},$$

где

$$\vec{s}_k = \sum_{i=1}^{N_1} \vec{q}_i^{\,r_1} \gamma_{ik}^{r_1 r_2},\ k = 1,2,...,N_2 .$$

Тогда,
$$\Phi = \sum_{i=1}^{N_1} \sum_{k=1}^{N_2} \gamma_{ik}^{r_1 r_2} \vec{q}_i^{\,r_1} (\vec{u}_k^{\,r_2})^T . \quad (6)$$

Следовательно, изображение Ф можно представить (синтезировать) в виде суммы некоторых компонент (изображений) $X_{ik}^{r_1 r_2}$, $i = 1,2,...,N_1$, $k = 1,2,...,N_2$,

$$X_{ik}^{r_1 r_2} = \vec{q}_i^{\,r_1} (\vec{u}_k^{\,r_2})^T,\ i = 1,2,...,N_1,\ k = 1,2,...,N_2 . \quad (7)$$

Изображения $X_{ik}^{r_1 r_2}$, $i = 1,2,...,N_1$, $k = 1,2,...,N_2$, вида (7), которые образованы собственными векторами $\vec{q}_i^{\,r_1}$ и $\vec{u}_k^{\,r_2}$ субполосных матриц косинус-преобразования G_{r_1} и H_{r_2}, соответственно, предлагается называть базисными изображениями в двумерном базисе собственных векторов субполосных матриц косинус-преобразования, соответствующих заданной подобласти ПЧ $V_{r_1 r_2}$.

Исследуем свойства базисных изображений $X_{ik}^{r_1 r_2}$ (7), соответствующих собственным векторам $\vec{q}_i^{\,r_1}$, $i = 1,2,...,N_1$, и $\vec{u}_k^{\,r_2}$, $k = 1,2,...,N_2$, субполосных матриц косинус-преобразования G_{r_1} и H_{r_2}.

Базисные изображения $X_{ik}^{r_1 r_2}$, соответствующие собственным векторам $\vec{q}_i^{\,r_1}$, $i = 1,2,...,N_1$, и $\vec{u}_k^{\,r_2}$, $k = 1,2,...,N_2$, субполосных матриц косинус-преобразования G_{r_1} и H_{r_2}, имеют размерность $N_1 \times N_2$ пикселей.

Можно показать, что норма базисного изображения $X_{ik}^{r_1 r_2}$, $i = 1,2,...,N_1$, $k = 1,2,...,N_2$, равна 1,

$$\left\| X_{ik}^{r_1 r_2} \right\| = 1 . \quad (8)$$

Следовательно, значения коэффициентов разложения $\left\{ \gamma_{ik}^{r_1 r_2} \right\}$, $i = 1,2,...,N_1$, $k = 1,2,...,N_2$, можно использовать для формального описания их значимости с позиций различной степени отображения информации об изображении.

Можно показать, учитывая свойства разложений по ортогональным базисам, что энергия изображения [1] Ф может быть вычислена на основе значений коэффициентов разложения $\gamma_{ik}^{r_1 r_2}$, вида (4), $i = 1,2,...,N_1$, $k = 1,2,...,N_2$, используя следующее соотношение,

$$\|\Phi\|^2 = \sum_{i=1}^{N_1} \sum_{k=1}^{N_2} (\gamma_{ik}^{r_1 r_2})^2 = \left\| \Gamma^{r_1 r_2} \right\|^2 . \quad (9)$$

Значения коэффициентов разложения $\Gamma^{r_1 r_2}$ изображения Ф по собственным векторам субполосных матриц косинус-преобразования, соответствующих ППЧ $V_{r_1 r_2}$, позволяют аппроксимировать значения части энергии $E_{r_1 r_2}$ [1] изображения Ф в данной подобласти ПЧ.

Были выполнены вычислительные эксперименты для исследования величины значений коэффициентов разложения изображений в двумерном базисе собственных векторов субполосных матриц косинус-преобразования.

Рассмотрим изображение $\Phi = (f_{ik})$, $i = 1,2,...,N_1$, $k = 1,2,...,N_2$. С целью повышения наглядности диаграмм, отображающих значения вычисляемых коэффициентов разложения (рисунок), размерность изображения Ф (без потери общности результатов) была выбрана 32×32 пикселей ($N_1 = N_2 = 32$).

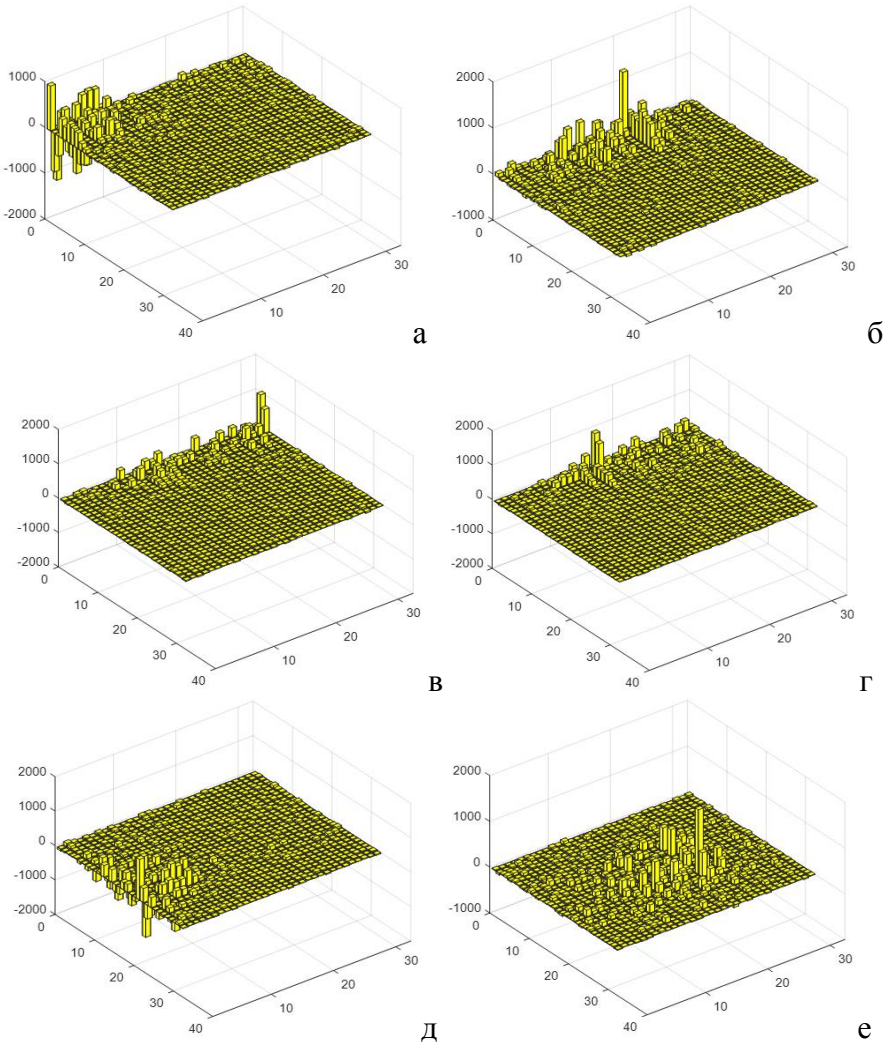


Рис. Диаграммы распределения значений коэффициентов разложения изображения Φ по собственным векторам субполосных матриц косинус-преобразования в соответствующих подобластях ПЧ $V_{r_1 r_2}$:

а – матрица Γ^{11}; б – матрица Γ^{12}; в – матрица Γ^{13}; г – матрица Γ^{14};

д – матрица Γ^{21}; е – матрица Γ^{22}

Fig. 1. Diagrams of the distribution of values of the coefficients of the decomposition of the image on the eigenvectors of subband matrices of the cosine transform in the corresponding subdomain of the $V_{r_1 r_2}$:

a – matrix Γ^{11}; b – matrix Γ^{12}; c – matrix Γ^{13}; d – matrix Γ^{14};

e – matrix Γ^{21}; f – matrix Γ^{22}

Представим область пространственных частот D_π, (область определения косинус-преобразования),

$$D_\pi = \{(u,v) \mid 0 \le u,v < \pi\}, \tag{10}$$

в виде объединения подобластей пространственных частот $V_{r_1 r_2}$, $r_1 = 1,2,...,R_1$, $r_2 = 1,2,...,R_2$, прямоугольной формы. Количество ППЧ выбрано равным $R_1 = R_2 = 4$, что не влияет на общность получаемых результатов.

Для всех подобластей $V_{r_1r_2}$, $r_1 = 1,2,...,R_1$, $r_2 = 1,2,...,R_2$, были вычислены значения коэффициентов разложения изображения Ф по собственным векторам соответствующих субполосных матриц косинус-преобразования. На рисунке в виде диаграммы представлены значения коэффициентов разложения изображения Ф по собственным векторам соответствующих субполосных матриц косинус-преобразования в отдельных подобластях ПЧ V_{11}, V_{12}, V_{13}, V_{14}, V_{21} и V_{22} области определения косинус-преобразования (на диаграммах по осям координат указаны номера соответствующих собственных векторов).

Результаты вычислительных экспериментов показали, что значительное количество коэффициентов разложения имеет величину близкую к нулю. Визуально данное свойство подтверждается диаграммами, приведенными на рисунке 1. Указанное свойство коэффициентов разложения изображений может быть использовано при решении различных задач анализа и обработки изображений, в частности, в задаче сжатия и скрытного внедрения информации в изображения.

Таким образом, показано, что на основании собственных векторов субполосных матриц косинус-преобразования можно построить ортогональные разложения изображений. При этом пары собственных векторов соответствующих субинтервальных матриц образуют естественный двумерный базис. Исследованы свойства коэффициентов разложения изображений по парам собственных векторов субполосных матриц косинус-преобразования.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-07-00657.

Список литературы

1. Черноморец, А.А. Об анализе данных на основе косинусного преобразования [Текст] / А.А. Черноморец, Е.В. Болгова // Научные ведомости БелГУ. Сер. Экономика. Информатика. – 2015. – № 1(198). – Вып. 33/1. – С. 68-73.

2. Болгова, Е.В. Свойства субинтервальных матриц двумерного косинусного преобразования [Текст] / Е.В. Болгова // Информационные системы и технологии. – 2017. – № 6(104). – С. 19-28.

3. Болгова, Е.В. О собственных числах субинтервальных матриц косинусного преобразования [Текст] / Е.В. Болгова // Научные ведомости БелГУ. Сер. Экономика. Информатика. – 2017 – № 2(251). – Вып. 41. С. 92-101.

4. Болгова, Е.В. О сосредоточенности энергии косинусного преобразования [Текст] / Е.В. Болгова // Научные ведомости БелГУ. Сер. Экономика. Информатика. – 2017. – № 9(258). – Вып. 42. – С. 111-121.

5. Ахмед, Н. Ортогональные преобразования при обработке цифровых сигналов [Текст] / Н. Ахмед, К.Р. Рао. – М.: Связь, 1980. – 248 с.

References

1. Chernomorets, A.A. On the analysis of data based on the cosine transformation [Text] / A.A. Chernomorets, E.V. Bolgova // Scientific bulletins of the Belgorod State University. Economy. Information technologies. – 2015. – № 1(198). – Vol. 33/1. – pp. 68-73.

2. Bolgova, E.V. The properties of subinterval matrices for a two-dimensional cosine transform [Text] / E.V. Bolgova // Information systems and technologies. – 2017. – № 6(104). – p. 19-28.

3. Bolgova, E.V. About the eigenvalues of cosine transform subinterval matrices [Text] / E.V. Bolgova // Scientific bulletins of the Belgorod State University. Economy. Information technologies. – 2017 – No. 2(251). – Vol. 41. P. 92-101.

4. Bolgova, E.V. About cosine transform energy concentration [Text] / E.V. Bolgova // Scientific bulletins of the Belgorod State University. Economy. Information technologies. – 2017. – No. 9(258). – Vol. 42. – p. 111-121.

5. Ahmed, N. Orthogonal transformations in digital signal processing [Text] / N. Ahmed, K.R. Rao. – M.: Svyaz, 1980. – 248 p.

Черноморец Дарья Андреевна, магистрант кафедры математического и программного обеспечения информационных систем
Болгова Евгения Витальевна, старший преподаватель кафедры прикладной информатики и информационных технологий
Черноморец Андрей Алексеевич, доктор технических наук, доцент, профессор кафедры прикладной информатики и информационных технологий
Барсук Алексей Александрович, директор, Общество с ограниченной ответственностью «АйТиДи»

Chernomorets Daria Andreevna, master student, Department of Mathematical and Software Information Systems
Bolgova Evgeniya Vitalievna, Senior Lecturer, Department of Applied Informatics and Information Technologies
Chernomorets Andrey Alekseevich, Doctor of Technical Sciences, Professor of the Department of Applied Informatics and Information Technologies
Barsuk Alexey Alexandrovich, Director, Limited Company "ITD"

СИСТЕМНЫЙ АНАЛИЗ И УПРАВЛЕНИЕ
SYSTEM ANALYSIS AND PROCESSING OF KNOWLEDGE

УДК 004.438 **DOI: 10.18413/2518-1092-2019-4-1-0-2**

Гончаренко Ю.Ю.
Кушнарев А.А.
Исаков С.А.

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДИКИ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

ФГАОУ ВО «Севастопольский государственный университет»,
ул. Университетская 33, г. Севастополь, 299053, Россия

e-mail: iuliay1985@mail.ru, sahsa14.95@yandex.ru, engener1990@mail.ru

Аннотация
Наиболее актуальный и распространенный вид информации, с которым работают практически все организации Российской Федерации – это персональные данные. По причине их распространенности они требуют особой бдительности при их обработке и обеспечении безопасности. Информационные системы обрабатывающие персональные данные могут подвергаться различным атакам из-за определенных уязвимостей. Для обеспечения максимальной защищенности информационной системы персональных данных Федеральная служба по техническому и экспортному контролю разработала специальную методику для определения актуальных угроз информационной системе. Для уменьшения трудозатрат эксперта при оценке каждой угрозы актуальным будет автоматизация данного процесса, что в конечном итоге не только даст выигрыш по времени, но и сократит количество ошибок, связанных с человеческим фактором.
Ключевые слова: персональные данные; актуальные угрозы безопасности; информационная система персональных данных; модель угроз; программная реализация.

UDC 004.438

Goncharenko J.A.
Kushnaryov A.A.
Isakov S.A.

SOFTWARE IMPLEMENTATION OF THE METHOD FOR DETERMINING THE ACTUAL THREATS TO THE PERSONAL DATA SECURITY

FSAEI HE "Sevastopol state University", University street 7, Sevastopol, 299053, Russian

e-mail: iuliay1985@mail.ru, sahsa14.95@yandex.ru, engener1990@mail.ru

Abstract
The most relevant and widespread type of information that almost all organizations of the Russian Federation work with is personal data. Because of their prevalence, they require special vigilance in their processing and security. Information systems processing personal data may be subject to various attacks due to certain vulnerabilities. To ensure maximum protection of the personal data information system, the Federal Service for Technical and Export Control has developed a special methodology for determining the current threats to the information system. In order to reduce the expert's labor in assessing each threat, the automation of this process will be relevant, which in the end will not only give a gain in time, but also reduce the number of errors associated with the human factor.
Keywords: personal data; current security threats; personal data information system; threat model; software implementation.

ВВЕДЕНИЕ

Основным объектом пристального внимания в наше время является информация. Существует множество видов информации, требующие компетентного получения, хранения, обработки и защиты. Информация о личных данных человека всегда имела и будет иметь большой спрос.

Основной проблемой является наличие персональных данных в любой организации, коммерческой или государственной. Утечка таких данных может привести к финансовым убыткам, административным или уголовным последствиям. Наряду с ростом технических возможностей для копирования и распространения информации возросла необходимость своевременного принятия мер по качественной защите персональных данных.

Уровень информационных технологий на данном этапе развития человечества довольно высок. В силу этого, самозащита информационных прав перестала функционировать эффективно. В современных реалиях человек физически не может добиться скрытности от всего изобилия применяемых в отношении него технических и программных средств и методов сбора или хищения данных, поэтому одна из самых актуальных проблем – это проблема защиты персональных данных [1].

Для построения адекватной системы защиты персональных данных на начальном этапе составляется список реальных угроз безопасности. Используя данный перечень актуальных угроз и уровень исходной защищенности, формулируются конкретные организационно-технические требования по защите информационных систем от утечки данных по техническим каналам, от несанкционированного доступа [2]. Также осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

ОСНОВНАЯ ЧАСТЬ

Система безопасности включает в себя защиту информации только для актуальных угроз. В соответствии с пунктом 2 статьи 19ФЗ «О персональных данных» обеспечение безопасности персональных данных достигается, в частности определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных, т.е. разработкой модели угроз [3].

В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» разработанной ФСТЭК, определение уровня исходной защищенности производится на основании анализа технических и эксплуатационных характеристик ИСПДн [4].

Однако данная методика реализована только на материальных носителях, что усложняет расчет и поиск актуальных угроз, что увеличивает время работы экспертов и затраты. Для исправления данного фактора разработана программная реализация методики на языке разметки HTML, то есть получить доступ к данной разработке можно при наличии интернета и веб-браузера.

Hyper Text Markup Language является стандартным языком разметки документов в глобальной сети. Его разработал британский ученый Тим Бернернс-Ли в 1990-х годах. Целью этого языка было упрощение обмена научной и технической документации [5].

HTML-страницы или гипертекстовые документы преобразуются браузером на стороне пользователя, в удобный для чтения вид. Это позволяет просматривать информацию в различных формах, например, изображения, текст, таблицы. При этом данный язык позволяет составить сложную иерархическую структуру из аналогичных документов.

При написании кода на данном языке используются специальные пометки или теги. Тегами обозначается начало и конец элемента, при этом любой документ, написанные с использованием HTML является набором таких элементов. Они могут быть пустыми, вложенными или иметь

собственные атрибуты, которые будут определять какие-либо свойства элемента. Кроме элементов существуют сущности – это специальные символы со знаком амперсанта.

Основной задачей языка является размещение элементов на странице, то есть он предназначен для создания статических веб-страниц. При этом он является самым демократичным языком, благодаря тому, что может подстроиться под каждый из браузеров [6].

На текущем этапе реализована поддержка только одного эксперта, добавление количества экспертов, разработка продукта на мобильную платформу и автоматическая генерация отчетов будет реализована в 2019 г.

При открытии страницы с реализованным расчетом актуальных угроз, эксперту предлагается определить характеристики информационной системы по таким критериям как наличие выхода в глобальную сеть интернет, территориальное размещение, разрешенные действия с данными и дальнейшие критерии, утвержденные методикой (рис. 1). Верный выбор данных свойств позволит программе определить коэффициент исходной защищенности информационной системы.

Во второй таблице эксперт оценивает вероятные угрозы системы по двум критериям: критичность и вероятность реализации.

Расчет исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности
1. По территориальному размещению:	
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом	◉
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)	○
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации	○
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий	○
локальная ИСПДн, развернутая в пределах одного здания	○
2. По наличию соединения с сетями общего пользования:	
ИСПДн, имеющая многоточечный выход в сеть общего пользования	○
ИСПДн, имеющая одноточечный выход в сеть общего пользования	○
ИСПДн, физически отделенная от сети общего пользования	○
3. По встроенным (легальным) операциям с записями баз персональных данных	
чтение, поиск	◉
запись, удаление, сортировка	○
модификация, передача	○
4.По разграничению доступа к персональным данным	
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	○
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	○
5. По наличию соединений с другими базами ПДн иных ИСПДн	
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн)	○
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	○
6. По уровню обобщения (обезличивания) ПДн	
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)	○
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	○
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	○
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	

Рис. 1. Таблица расчета исходной защищенности ИСПДн
Fig. 1. Table of calculation of initial security of ISPD

Предложены наиболее распространенные угрозы утечки информации, такие как акустические, видовые, побочные электромагнитные излучения (ПЭМИН), хищение средств хранения информации, а также преднамеренные и непреднамеренные угрозы. Эксперт определяет для каждой угрозы вероятность реализации, исходя из предложенных четырех вариантов и показатель опасности (предложено 3 варианта ответа) (рис. 2, 3).

После заполнения всех данных эксперту необходимо нажать кнопку «Закончить» после таблиц. Программы рассчитает угрозы по утвержденным методикой баллам и определит наиболее актуальные угрозы информационной системе персональных данных (рис. 4).

Экспертные оценки

Угрозы утечки акустической (речевой) информации	Вероятность реализации	Показатель опасности
Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.	Маловероятно	Низкий
Угрозы утечки видовой информации		
Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.	Маловероятно (Маловероятно, Низкая вероятность, Средняя вероятность, Высокая вероятность)	Низкий
Угрозы утечки информации по каналам ПЭМИН		
Кража ПЭВМ и кража носителей информации. Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПДн.	Маловероятно	Низкий
Кража ключей и атрибутов доступа. Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.	Маловероятно	Низкий
Кражи, модификации, уничтожения информации. Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.	Маловероятно	Низкий
Несанкционированное отключение средств защиты. Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.	Маловероятно	Низкий
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).		
Действия вредоносных программ (вирусов). Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программа с потенциально опасными последствиями или вредоносной программой (вирусом).	Маловероятно	Низкий
Не декларированные возможности системного ПО и ПО для обработки персональных данных. Не декларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.	Маловероятно	Низкий
Установка ПО не связанного с исполнением служебных обязанностей. Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.	Маловероятно	Низкий
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении.		
Утрата ключей и атрибутов доступа. Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают		

Рис. 2. Варианты вероятности реализации угроз
Fig. 2. Variants of the likelihood of threats

Экспертные оценки

Угрозы утечки акустической (речевой) информации	Вероятность реализации	Показатель опасности
Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.	Маловероятно	Низкий
Угрозы утечки видовой информации		
Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.	Маловероятно	Низкий
Угрозы утечки информации по каналам ПЭМИН		
Кража ПЭВМ и кража носителей информации. Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПДн.	Маловероятно	Низкий
Кража ключей и атрибутов доступа. Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.	Маловероятно	Низкий (Низкий, Средний, Высокий)
Кражи, модификации, уничтожения информации. Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.	Маловероятно	
Несанкционированное отключение средств защиты. Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.	Маловероятно	Низкий
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).		
Действия вредоносных программ (вирусов). Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программа с потенциально опасными последствиями или вредоносной программой (вирусом).	Маловероятно	Низкий
Не декларированные возможности системного ПО и ПО для обработки персональных данных. Не декларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.	Маловероятно	Низкий
Установка ПО не связанного с исполнением служебных обязанностей. Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.	Маловероятно	Низкий
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении.		
Утрата ключей и атрибутов доступа. Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают		

Рис. 3. Варианты показателя опасности угроз
Fig. 3. Hazard indicator variants

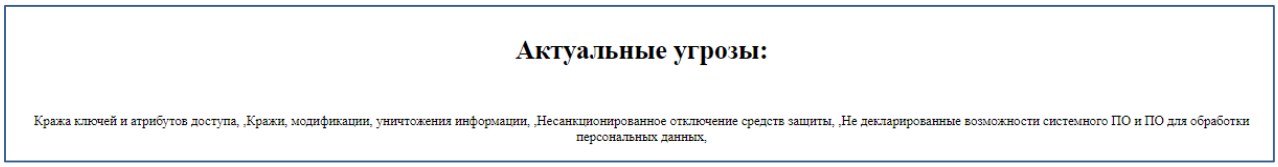


Рис. 4. Результат оценки
Fig. 4. Evaluation result

ЗАКЛЮЧЕНИЕ

Таким образом, данный метод позволит определить актуальные угрозы, имея доступ к сайту с данной формой, однако так как временно существует поддержка только одного эксперта, оценка является субъективной, то есть, возможно, потребуется оценка другого эксперта, для определения общих актуальных угроз.

Список литературы

1. Олег Слепов. Защита персональных данных // ИТ-портал компании «Инфосистемы Джет»: электронный журнал, 2009. №5. URL: http://www.jetinfo.ru/jetinfo_arhiv/zaschita-personalnykh-dannykh/zaschita-personalnykh/2017 (дата обращения: 11.12.2018).

2. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. М.: Горячая линия-телеком, 2001. 148 с.

3. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 10.12.2018).

4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380/ (дата обращения: 12.11.2018).

5. HTML: основы для начинающих. URL: http://fb.ru/article/250376/html-osnovyi-dlya-nachinayuschih/ (дата обращения: 14.12.2018).

6. Что такое HTML. URL: https://blogwork.ru/chto-takoe-html/ (дата обращения: 14.12.2018).

References

1. Oleg Slepov. Protection of personal information. Jet Infosystems IT portal: electronic journal, 2009. №5. URL: http://www.jetinfo.ru/jetinfo_arhiv/zaschita-personalnykh-dannykh/zaschita-personalnykh/2017 (handling date: 11/12/2018).

2. Malyuk A.A., Pazizin S.V., Pogozhin N.S. Introduction to information security in automated systems. Moscow: Goryachaya liniya-telekom, 2001. 148.

3. Federal Law “On Personal Data” dated July 27, 2006 No. 152-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (handling date: 10/12/2018).

4. The method of determining the actual threats to the security of personal data during their processing in the information systems of personal data. FSTEC of Russia, 2008. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380/ (handling date: 12/11./018).

5. HTML: Basics for Beginners. URL: http://fb.ru/article/250376/html-osnovyi-dlya-nachinayuschih/ (handling date: 12/14/2018).

6. What is HTML? URL: https://blogwork.ru/chto-takoe-html/ (handling date: 12/14/2018).

Гончаренко Юлия Юрьевна, доктор технических наук, доцент, профессор кафедры «Информационная безопасность»
Кушнарев Александр Александрович, студент первого курса магистратуры кафедры «Информационная безопасность»
Исаков Сергей Алексеевич, студент четвертого курса кафедры «Информационная безопасность»

Goncharenko Julia, Doctor of Technical Sciences, Professor of "Information security"
Kushnaryov Aleksandr, First-Year Master's Student of the Department "Information security"
Isakov Sergey, Fourth-Year Student of the Department "Information security"

УДК 004.94 **DOI: 10.18413/2518-1092-2019-4-1-0-3**

Литвинова А.А.[1]
Забнин С.А.[2]

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПРОГНОЗИРОВАНИЯ ОБЪЕМОВ ПРОДАЖ ОПТОВОЙ ТОРГОВОЙ КОМПАНИИ С УЧЕТОМ СЕЗОННОСТИ

[1)] ООО «Команда ЛАБС», пер. Гороховский, д. 6/1, стр. 1, г. Москва, 105064, Россия
[2)] ООО «Интерактивные технологии и системы», Пресненская набережная, дом 8с1, г. Москва, 141400, Россия

e-mail: figer91@mail.ru

Аннотация
В работе рассмотрена разработка автоматизированной системы прогнозирования объемов продаж оптовой торговой компании с учетом сезонности. Адаптирован метод поиска похожих подпоследовательностей временного ряда прогнозирования объема продаж с учетом сезонной компоненты под особенности прогнозирования объема продаж конкретного предприятия. Оценена эффективность адаптации метода поиска похожих подпоследовательностей временного ряда для прогнозирования объемов продаж на предприятии.
Ключевые слова: прогнозирование объемов продаж, динамическая транформация временной шкалы, прогнозирование, численные методы, критерии, объем продаж, сезонность.

UDC 004.94

Litviniva A.A.[1]
Zabnin S.A.[2]

AUTOMATED FORECASTING SYSTEM FOR VOLUMES OF SALES WHOLESALE TRADE COMPANY WITH SEASON ACCOUNT

[1)] "Komanda LABS", per. Gorokhovsky, 6/1, p. 1, Moscow, 105064, Russia
[2)] Interactive Technologies and Systems, Presnenskaya naberezhnaya, 8S1, Moscow, 141400, Russia

e-mail: figer91@mail.ru

Abstract
The paper considers the development of an automated system for forecasting sales volumes of a wholesale trading company, considering seasonality. The method of searching for similar subsequences of the time series of forecasting sales volume, considering the seasonal component, has been adapted to the specifics of forecasting sales volumes of a particular enterprise. The effectiveness of adapting the method of searching for similar time series subsequences for forecasting sales volumes at an enterprise has been evaluated.
Keywords: sales forecasting, dynamic transformation of the timeline, forecasting, numerical methods, criteria, sales, seasonality.

ВВЕДЕНИЕ

Одним из основных инструментов достижения коммерческих целей предприятия является план продаж. В силу того, что план продаж – это ожидаемая выручка (объем продаж) за планируемый период, составление плана продаж предшествует процесс прогнозирования, результаты которого и лягут в основу будущего плана. Особенно это важно для скоропортящихся товаров (например, охлажденная рыбная продукция), требующих быстрой реализации на рынке. В таких условиях для составления эффективного плана продаж необходимо иметь прогноз на будущее. Прогноз может быть основан на субъективном опыте эксперта, либо опираться на экономико-статистические методы. Эксперт при составлении оценочного прогноза должен учитывать большое количество внешних факторов среды, которые могут повлиять на объем продаж. Часто в качестве экспертов выступают специалисты, знающие рынок, новые тенденции

движения цен, продукцию конкурентов, а также любую другую информацию о возможных изменениях потребности товара. Однако точность такого прогноза напрямую зависит от компетентности специалиста, его опыта работы в этой области. Найти такого грамотного человека – непростая задача. Кроме того, для небольших предприятий это может обойтись очень дорого. Поэтому использование экономико-статистических методов выглядит наиболее предпочтительным вариантом. Среди этих методов есть группа, опирающаяся на результаты прошлых периодов. А такая статистика имеется на предприятии, выбранном для апробации результатов исследования.

Основными проблемами при прогнозировании объема продаж экономико-статистическими методами являются: обработка большого числа статистических данных; сложность выбора подходящего метода, учитывающего сезонность и особенности спроса на продукт конкретного предприятия; низкая точность прогнозирования при большом количестве сезонных и несезонных колебаний.

Таким образом, разработка автоматизированной системы прогнозирования объемов продаж оптовой торговой компании с учетом сезонности является актуальной.

ОСНОВНАЯ ЧАСТЬ

С учетом вышеизложенного были проведены вычислительные эксперименты с данными предприятия объемов продаж прошлых периодов, которые представляют собой несколько временных рядов длиной в год. На рисунке 1 представлена собранная статистика по выручке за прошедшие годы. С целью сохранения коммерческой тайны они приводятся в нормированном виде. Так как прогноз на данном предприятии чаще всего составляется на месяц, то имеющиеся точки с информацией о сделках были сгруппированы по месяцам.

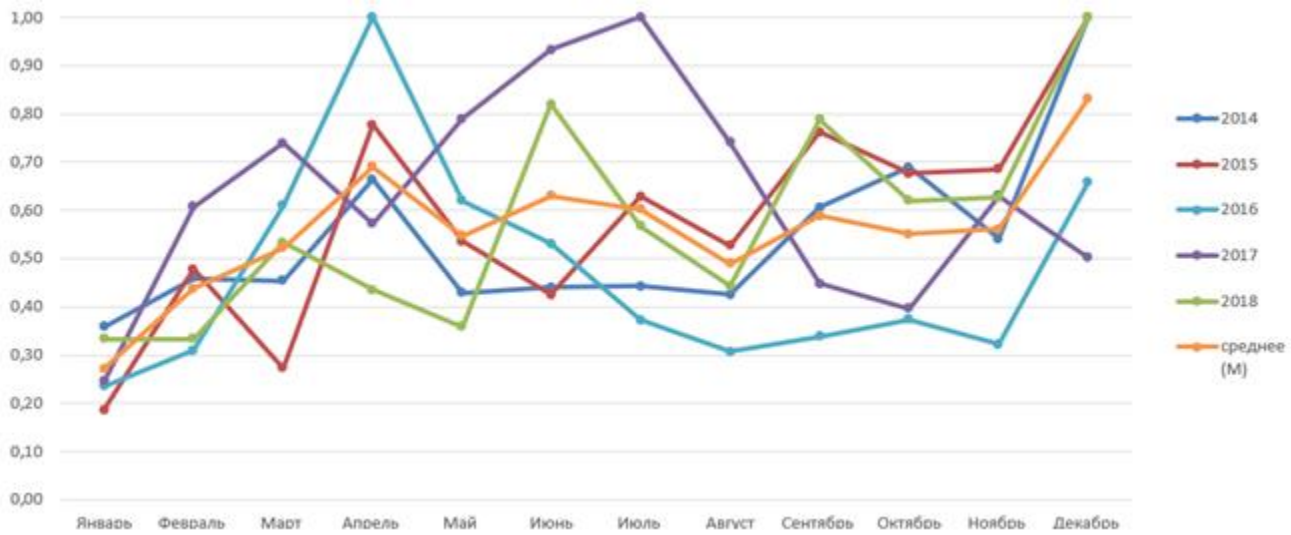


Рис. 1. Статистика объемов продаж по годам
Fig. 1. Statistics of sales by year

Для оценки разброса значений временных рядов на график был добавлен ряд средних значений для каждого месяца.

Из графика видно, что данные носят крайне неоднородный характер, можно отметить лишь только то, что тенденцию каждый год имеют всего несколько отрезков – это январь-февраль, ноябрь-декабрь и август-сентябрь.

Для изучения свойств и закономерностей в данных, были найдены средние значения месяцев в году и средние значение для каждого месяца за все годы. Посчитано среднее отклонение в обои случаях. Среднее отклонение показало, что во втором случае отклонение от среднего

значения имеют меньшую величину, т.е. значение месяца сильнее зависит от значений того же месяца в прошлые годы, чем от значения предыдущего месяца в этом году. Вычисленные коэффициенты сезонности и экспертное мнение специалиста по продажам выявили сезонные месяцы – апрель и декабрь, закономерно наблюдается спад в январе и феврале. Результаты пробных прогнозов представлены на рисунках 2: и 3 методом скользящего среднего и построения линии тренда соответственно.

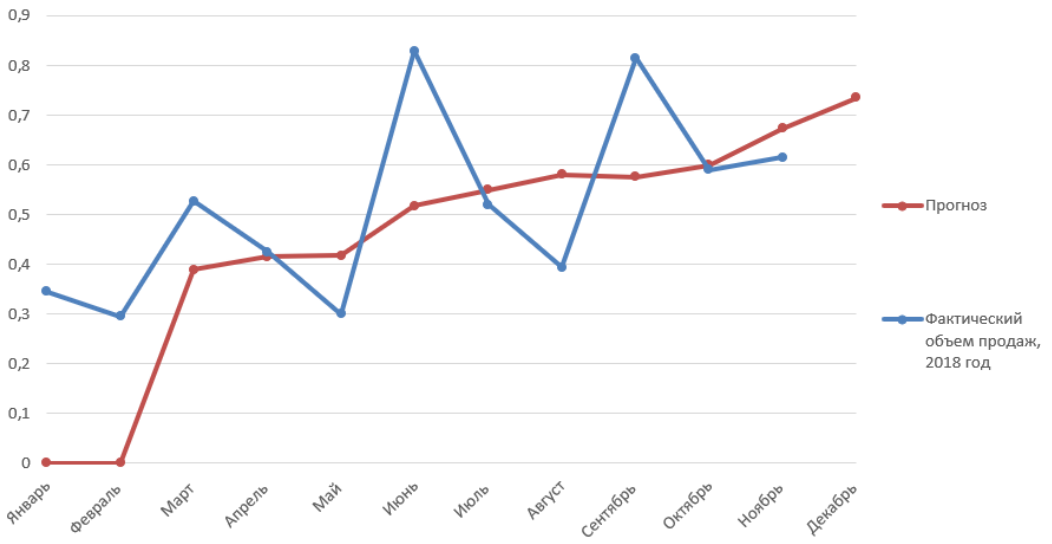


Рис. 1. Прогнозирование методом скользящего среднего
Fig. 2. Moving average prediction

Прогнозирование методом скользящего среднего направлен на то, чтобы сгладить всплески в данных и выявить основную тенденцию. Такой метод, очевидно, не подходит для прогнозирования объема продаж рассматриваемого предприятия.

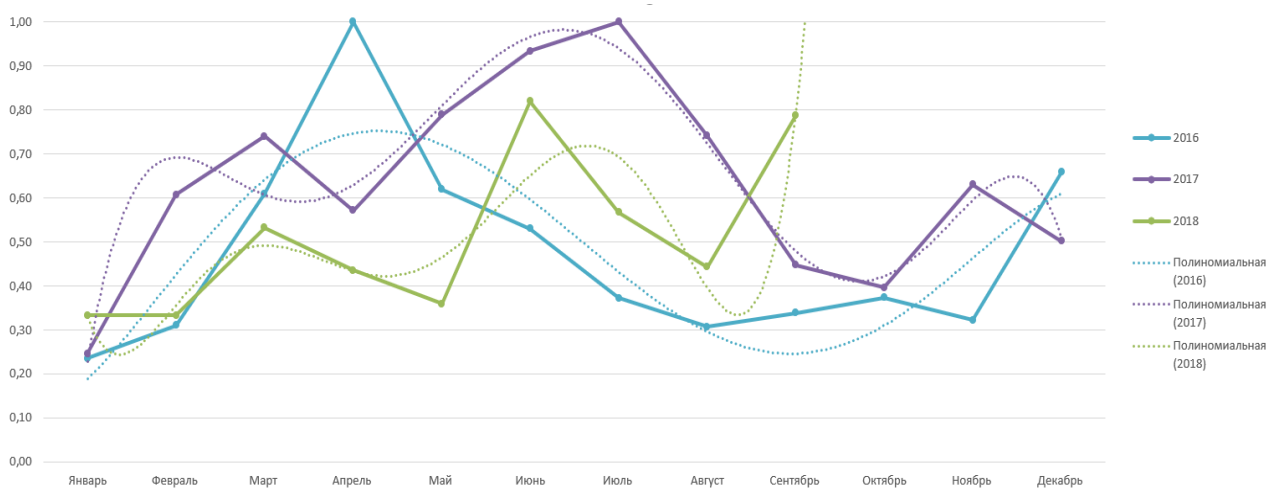


Рис. 2. Линии тренда для 2016, 2017 и 2018 года
Fig. 3. Trend Lines for 2016, 2017 and 2018

Каждая линия тренда является полиномиальной и представляет собой уравнение шестой степени. Например, для 2017 года зависимость выражается следующим образом: $y = 0{,}0009x^6 – 0{,}0252x^5 + 0{,}2784x^4 – 1{,}5051x^3 + 4{,}1269x^2 – 5{,}2668x + 2{,}7194$. Составление такой сложной зависимости само по себе является трудной задачей. Более того, даже составив ее далеко не всегда удается получить точный прогноз, как это видно из графика: например, сезонный пик апреля 2016 года не учитывается.

Для выявления похожих циклов был построен хронологический график объема продаж. Ниже на рисунке 4 приведена одна из частей графика.

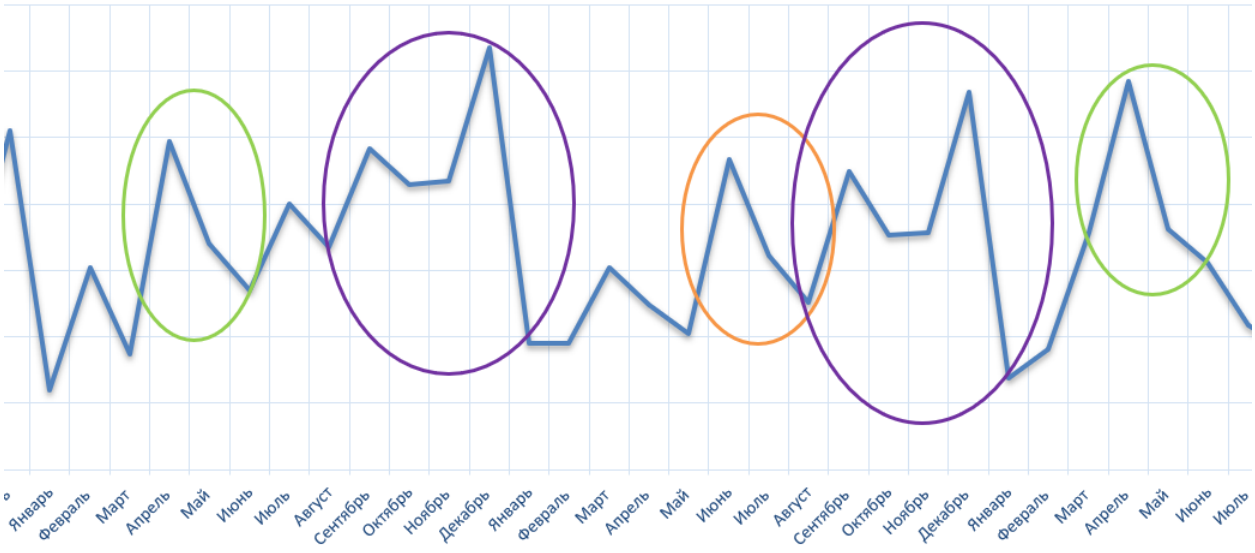


Рис. 3. Хронология объемов продаж
Fig. 4. Chronology of sales

На рисунке 4 имеются переодичность подъемов и спадов, то есть присутствуют факторы цикличности и сезонности.

Таким образом, существует необходимость в разработке нового метода прогнозирования, который будет учитывать сезонность и цикличность на основе статистических данных прошлых периодов.

Далее приведена формализованная постановка задачи, выбран и адаптирован метод для прогнозирования объема продаж, построены алгоритмы, реализующие адаптированный метод.

Основой прогнозирования является метод поиска похожих подпоследовательностей временного ряда, в качестве метрики схожести выбран алгоритм динамической трансформации временной шкалы (DTW алгоритм).

Были выведены и формализованы дополнительные параметры, участвующие в оптимизации процесса прогнозирования: цикличность и сезонность. Проведена адаптация выбранного метода метод поиска похожих подпоследовательностей временного ряда к процессу прогнозирования объема продаж за счет выравнивания начальных точек сравниваемых интервалов.

Для адаптации метода был разработан алгоритм, блок-схема которого изображена на рисунке 5.

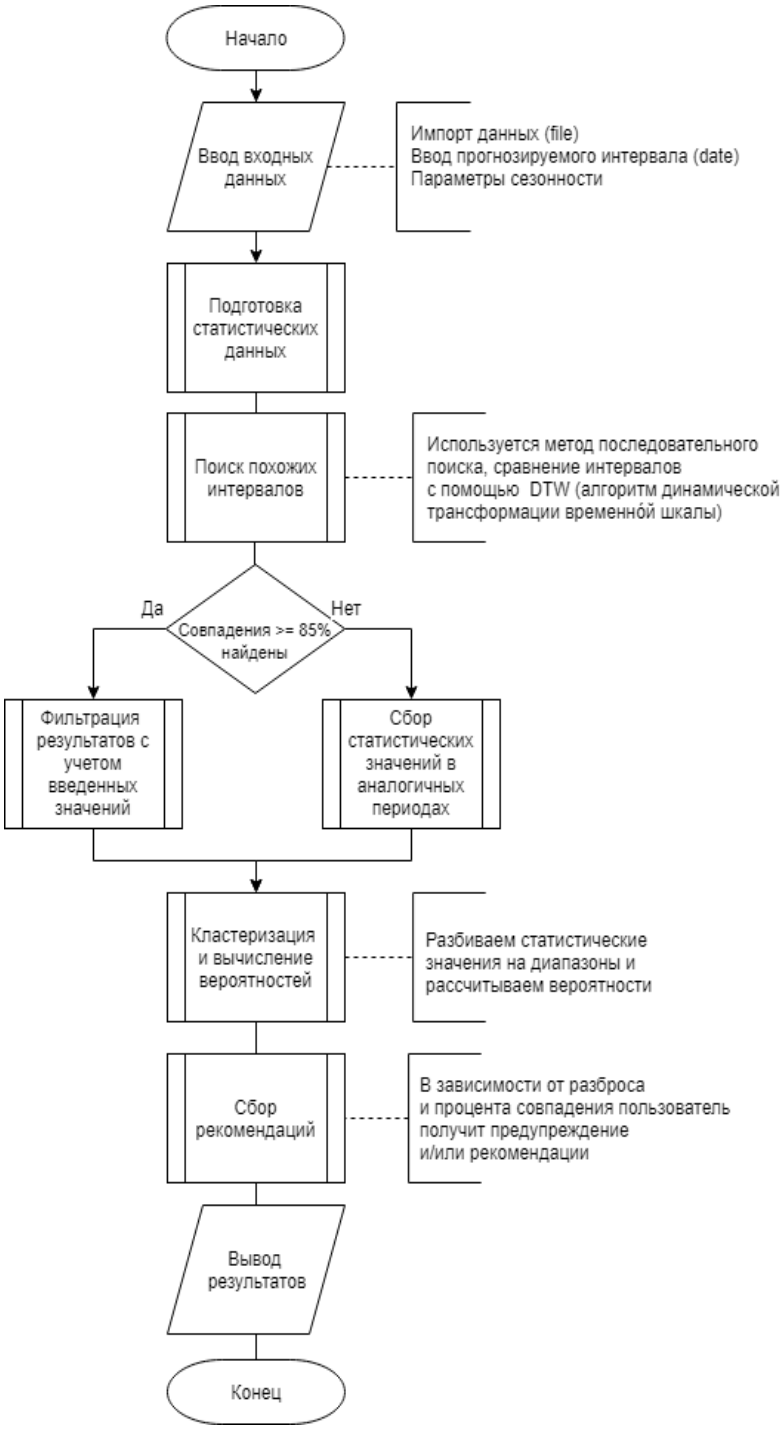


Рис. 5. Общая схема алгоритма прогнозирования объема продаж
Fig. 5. The general scheme of the sales forecasting algorithm

Подготовка статистических данных включает поиск интервалов, основанных на параметрах, введенных пользователем. Затем среди них идет поиск похожих интервалов при помощи алгоритма DTW (динамической трансформации временной шкалы). Часто бывает так, что характерные части временных рядов не только отстоят друг от друга по оси времени, но ещё и растянуты или сжаты. Тогда ни евклидова метрика, ни кросс-корреляция не дают результатов, в то время как алгоритм DTW способен выявить подобие даже на таких частях временного ряда.

На рисунке 6 показаны отличия метрики Евклида и DTW. DTW-алгоритм строит матрицу возможных отображений одной последовательности ряда на другую, с учётом того, что отсчёты рядов могут как сдвигаться, так и изменять уровень. Путь в этой матрице с минимальным значением стоимости – и есть DTW-расстояние.

Классический DTW алгоритм по этим последовательностям строит путь наименьшей стоимости. Главным недостатком этого алгоритма является неспособность различить два идентичных отрезка, расположенных параллельно друг другу. Поэтому необходимо адаптировать классический DTW алгоритм к специфике прогнозирования объемов продаж торгового предприятия, что позволит сравнивать отрезки независимо от их относительного расположения.

Прогнозируемый отрезок накладывается на сравниваемый таким образом, чтобы начальные точки совпадали, после чего происходит измерение расстояния между отрезками.

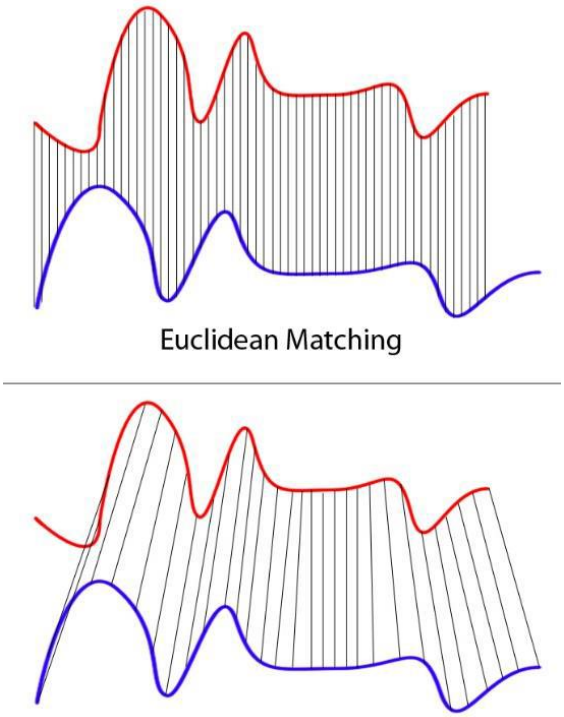


Рис. 6. Сравнение метрик Евклида (над чертой) и DTW (под чертой)
Fig. 6. Comparison of Euclidean metrics (above the line) and DTW (below the line)

Прогнозируемый отрезок накладывается на сравниваемый таким образом, чтобы начальные точки совпадали, после чего происходит измерение расстояния между отрезками. Блок-схема этого алгоритма изображена на рисунке 7.

Рис. 7. Блок-схема алгоритма оптимизированного поиска похожих интервалов
Fig. 7. Block diagram of the optimized search algorithm for similar intervals

В силу того, что ряд может обладать схожими некоторым образом всплесками в силу цикличности и сезонности, мы можем попросить менеджера по продажам указать, в какие временные интервалы спрос увеличивается именно в силу внешнего сезона.

Имея дополнительные параметры, в нашем случае можно оптимизировать работу последовательного метода поиска похожих подпоследовательностей, отличив таким образом случайные всплески от сезонных колебаний.

Если поиск не дает схожих подпоследовательностей в статистических данных, и соответственно, не может построить прогноз, то дальнейшее прогнозирование строится на основе разделения всех статистических значений на несколько диапазонов: оптимистичный прогноз, пессимистичный и средний.

На рисунке 8 отображен интерфейс разработанной системы.

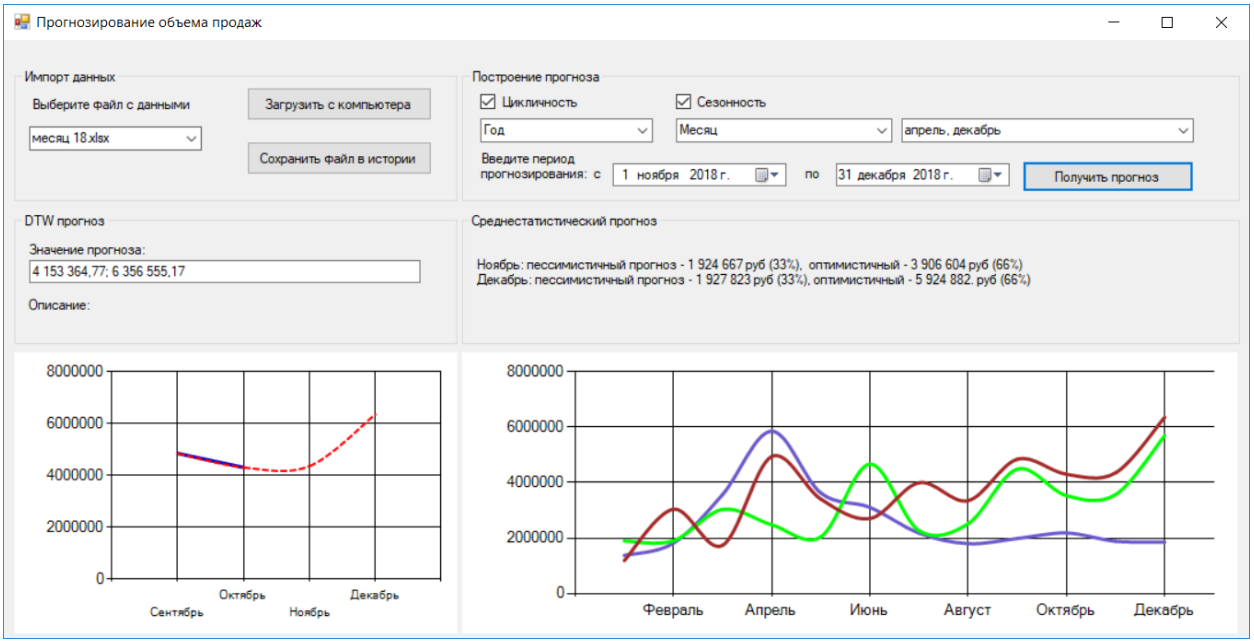


Рис. 8. Интерфейс разработанной программы
Fig. 8. Interface of the developed program

Для численной оценки качества адаптированного метода использовались MARE и среднее отклонение. В таблице представлены соответствующие количественные оценки.

Таблица

Результаты эксперимента

Table

Experimental results

Используемый метод / Критерий оценки	MAPE, %	Среднее отклонение, %
Адаптированный метод поиска похожих подпоследовательностей на основе динамической трансформации шкалы времени	7,79	3,52
Метод, используемый на предприятии	28,38	14,17
Построение полиномиальной линии тренда	13,31	3,99
Линейная регрессия с учетом сезонности	18,43	6,72

Адаптированный метод поиска похожих подпоследовательностей на основе динамической трансформации шкалы времени показывает более точные результаты по сравнению с методом, используемом на предприятии.

ЗАКЛЮЧЕНИЕ

В большинстве случаев профессиональные математические инструменты недоступны для компаний малого бизнеса и не соответствуют затратам, если прогнозирование необходимо для одного временного ряда. Разработанная информационная система и адаптированный метод прогнозирования с использованием алгоритма трансформации временной шкалы реализует простой функционал, необходимый для автоматизации деятельности менеджера по продажам при прогнозировании объема продаж предприятия с учетом сезонности.

Использование разработанной системы позволит снизить временные затраты на прогнозирование, автоматизировать рутинные действия пользователя.

Список литературы

1. Швагер, Джек Д. Технический анализ. Полный курс / Джек Д. Швагер – М.: Альпина Паблишер, 2017. – 880 с.
2. Мэрфи, Джон Дж. Технический анализ фьючерсных рынков. Теория и практика / Джон Дж. Мэрфи – М.: Альпина Паблишер, 2011. – 616 с.
3. Черноморец, А.А. Информационные системы валютного рынка / А.А. Черноморец: Белгородский институт государственного и муниципального управления ОРАГС, 2006 – 173 с.
4. Киселевич, Ю.В. Применение моделей оценки конкурентоспособности при формировании оптимального портфеля ценных бумаг //Материалы международной научно-практической конференции «Конкурентоспособность бизнеса и технологий» / Ю.В. Киселевич – Брянск, 2005
5. Вдовин, В.М. Информационные технологии в финансово-банковской сфере: Практикум / В.М. Вдовин, Л.Е Суркова – Москва: Дашков и К°, 2010. – 248 с.
6. Гахов, Р.П. Компьютерное моделирование экономических процессов: учебное пособие для студентов вузов по специальности 230400.62 "Информационные системы и технологии" [Текст] / Р.П. Гахов, Н.В. Щербинина и др. – Белгород: ИД Белгород, 2014. – 88 с.
7. Рутковская, Д. Нейронные сети, генетические алгоритмы и нечеткие системы / Д. Рутковская, М. Пилиньский, Л. Рутковский – М.: Горячая линия – Телеком, 2006. – 452 с.
8. Иорш, В.И. Управление основными фондами на основе ключевых показателей эффективности [Текст] / В. И. Иорш, В. Д. Стружинский // Горный журнал. – 2010. – №3. – С. 25 – 28.
9. Фаулер, М. Архитектура корпоративных программных приложений / М. Фаулер, Д. Райс, М. Фоммел, Э. Хайет, Р. Ми, Р. Стаффорд – М.: Вильямс, 2007. – 544 с.

References

1. Schwager, Jack D. Technical analysis. Full course / Jack D. Schwager – M.: Alpina лишablisher, 2017. – 880 p.
2. Murphy, John J. Technical analysis of futures markets. Theory and Practice / John J. Murphy – Moscow: Alpina лишablisher, 2011. – 616 p.
3. Chernomorets, A.A. Information systems of the currency market / A.A. Chernomorets: Belgorod Institute of State and Municipal Administration of the ORAGS, 2006 – 173 p.
4. Kiselevich, Yu.V. The use of competitiveness assessment models for the formation of an optimal securities portfolio // Proceedings of the international scientific-practical conference “Business and Technology Competitiveness” / Yu.V. Kiselevich – Bryansk, 2005
5. Vdovin, V.M. Information technologies in the financial and banking sphere: practical work / V.M. Vdovin, L.E. Surkova – Moscow: Dashkov and Co., 2010. – 248 p.
6. Gakhov, R.П. Computer modeling of economic processes: a textbook for university students in the specialty 230400.62 "Information systems and technologies" [Text] / R.П.Gakhov, N.V. Shcherbinina et al. – Belgorod: ID Belgorod, 2014. – 88 p.
7. Rutkovskaya, D. Neural networks, genetic algorithms and fuzzy systems / D. Rutkovskaya, M. Pilinsky, L. Rutkovsky – M.: Hotline – Telecom, 2006. – 452 p.
8. Iorsh, V.I. Management of fixed assets based on key performance indicators [Text] / V.I. Iorsh, V.D. Struzhinsky // Mining Journal. – 2010. – №3. – P. 25 – 28.
9. Fowler, M. Architecture of corporate software applications / M. Fowler, D. Rice, M. Fommel, E. Hyatt, R. Mee, R. Stafford – M.: Williams, 2007. – 544 p.

Литвинова Алина Александровна, старший инженер в ООО «Команда ЛАБС»
Забнин Сергей Александрович, инженер, ООО «ИТИС»

Litvinova Alina Aleksandrovna, senior engineer in Komanda LABS
Zabnin Sergey Aleksandrovich, engineer, Intelligent Technologies and Systems

УДК 681.3 **DOI: 10.18413/2518-1092-2019-4-1-0-4**

Мустаев И.З.[1]
Семивеличенко Е.А.[2]
Иванов В.Ю.[3]
Максимова Н.К.[4]
Мустаев Т.И.[1]

МОДЕЛИРОВАНИЕ СОСТОЯНИЯ НАУКОЕМКОГО ОБЪЕКТА, СУЩЕСТВУЮЩЕГО В УСЛОВИЯХ РАЗВИВАЮЩЕГОСЯ РЫНКА

[1)] Уфимский государственный авиационный технический университет, Уфа, Россия
[2)] ПАО ОДК – УМПО, Уфа, Россия
[3)] СП «ДБА-инжиниринг», Уфа, Россия
[4)] ПАО УМПО, Уфа, Россия

e-mail: fermi_moustaev@mail.ru, umpo@umpo.ru, ivanov.vladimir@mail.ru, maksimova@umpo.ru, tima.mus.1321@gmail.com

Аннотация
Статья посвящена изложению методологии моделирования состояния наукоемкой продукции с большой длительностью жизненного цикла. Неустойчивость характеристик развивающегося рынка входит в противоречие с необходимостью прогнозирования характеристик объекта в течение больших промежутков времени и представляет проблему, препятствующую эффективному использованию известных подходов. Для преодоления этой проблемы был разработан новый инструментарий моделирования, базирующийся на моделировании динамики состояния объекта. Состояние объекта является фундаментальным свойством, которое сохраняется в условиях высокой изменчивости внешней среды. Моделирование состояния осуществляется с использованием комплекса описанных в статье характеристик.
Ключевые слова: наукоемкий продукт; потенциал; жизненный цикл.

UDC 681.3

Mustaev I.Z.[1]
Semivelichenko E.A.[2]
Ivanov V.Yu.[3]
Maksimova N.K.[4]
Mustaev T.I.[1]

THE MODELING OF A HIGH-PROJECT OBJECT STATE EXISTING IN THE CONDITIONS OF A DEVELOPING MARKET

[1)] Ufa State Aviation Technical University, Ufa, Russia
[2)] PAO ODK – UMPO, Ufa, Russia
[3)] JV «DBA-engineering», Ufa, Russia
[4)] PAO UMPO, Ufa, Russia

e-mail: fermi_moustaev@mail.ru, umpo@umpo.ru, ivanov.vladimir@mail.ru, maksimova@umpo.ru, tima.mus.1321@gmail.com

Abstract
The methodology of modeling the state of high-tech products with a long life cycle is described. The instability of the characteristics of the developing market is in contradiction with the need to predict the characteristics of the object for large periods of time. It is the problem that prevents the effective use of known approaches. To overcome this problem, a new modeling tool based on modeling the dynamics of the object state was developed. The state of the object is a fundamental property that is preserved in conditions of the high variability of the environment. The set of characteristics described in the article are used.
Keywords: high-tech product; potential, life cycle.

Совокупная длительность этапов проектирования, производства и эксплуатации инновационной наукоемкой продукции, например, авиационной техники, характеризуется большими длительностями. Так, жизненный цикл авиационного двигателя достигает 40…50 лет. В России создание такой продукции сталкивается с рядом проблем, характерных для развивающихся рынков развивающихся стран. Они вызваны необходимостью ведения бизнеса в условиях технологического отставания в смежных отраслях, поддерживающих основное конкурентоспособное производство. К ним добавляются проблемы утечки мозгов, ограниченности финансового и человеческого капиталов. Необходимо также отметить повышенную неустойчивость и уязвимость бизнеса, обусловленную воздействием глобальных и локальных кризисов. За последние 20 лет можно констатировать дефолт 1998 года, кризисы 2008 и 2013 годов, т.е. один кризис в 6…7 лет. Отмеченное в совокупности существенно и неопределенным образом изменяет характеристики у предприятий, поддерживающих жизненный цикл объекта, что должно приниматься во внимание при составлении прогнозов. Следует также подчеркнуть, что за время жизни объект меняет форму, развиваясь от идеи до конкретной продукции, причем предприятия, обеспечивающие его существование (предприятия жизненного цикла), различаются по типам и формам собственности, размерам, финансово-экономическим показателям, территориальной принадлежности и т.д.

На большие горизонты времени сориентированы известные методы, опирающиеся на прогнозирование технологических, экономических, конкурентных, международных, рыночных и политических факторов (Иващенко Н. П., 2013). Однако, результаты прогнозирования, часто оказываются неверными, причем их эффективность, понимаемая как реализуемость прогнозов, варьируется в пределах от 30% до 90%. (Комков Н. И., 2015). Прогнозирование состояния объекта, существующего в условиях высокой неопределенности развивающихся рынков, остается не решенной проблемой. Это предполагает как развитие существующих подходов и моделей, так и формирование новых. В работе излагаются элементы новой методологии моделирования состояния объекта комплексной природы. Особенностью является робастность результирующих моделей, проявляющаяся как устойчивость к изменению частоты регистрации информации и к случайным вариациям внешних и внутренних факторов. Важным является то, что это позволяет использовать модели при прогнозировании состояния объекта, согласованного с результатами деятельности предприятий, поддерживающих его жизненный цикл. Дополнительно появляется возможность управления состоянием объекта на горизонте жизненного цикла через управление указанными предприятиями.

В основе методологии лежат интегральные характеристика и свойство объекта, названное накопленным потенциалами и, соответственно, накопленным состоянием (Мустаев, 2013, 2017). Содержание понятия можно пояснить на следующих примерах. Зафиксируем текущий момент времени t. Предположим, что в прошлом, в момент $(t-\tau)$ был выполнен единственный платеж величиной $q(t-\tau)=q_0$. Для того, чтобы платеж, будучи инвестированным в рыночные инструменты в прошлом в момент времени $t-\tau$, привел к текущей величине актива, т.е. к q_0 в момент времени t, он должен быть равен:

$$X_q^a(t,\alpha,\sigma)=q(t-\tau)\cdot\psi(\tau,\alpha,\sigma)=q_0\cdot\psi(\tau,\alpha,\sigma). \quad (1)$$

Здесь, ψ – социотехническая функция системы, включающей объект в качестве объекта управления, α – величина доходности, сложившаяся на отрезке времени $(t-\tau,t)$, σ – риск. Величина X_q^a названа *накопленным потенциалом* и имеет смысл текущей рыночной оценки платежа, совершенного в прошлом. Накопленный потенциал потока прошлых платежей, определяется по формуле:

$$X_q^a(p,t)=\int_{\tau=0}^{\infty} q(t-\tau)\psi(\tau,p)\,d\tau=\hat{A}q, \quad (2)$$

В (2) комплексная переменная p сформирована из двух функций λ и $p = \lambda(\alpha) + j\nu(\sigma)$. Функция λ названа функцией прибыльности, – функцией неопределенности. Формула (2) используется для определения накопленного потенциала переменной состояния любого типа, а не только денежных потоков. В совокупности накопленные потенциалы переменных состояния характеризуют накопленный потенциал объекта. Состояние, в котором находится объект, определяется как *накопленное состояние*. Таким образом, накопленному состоянию объекта ставится в соответствие его накопленный потенциал. К функции , названной социофизической функцией, предъявляются требования, подобные требованиям, предъявляемые при рыночной оценке потоков и активов.

Объект находится в одном из состояний, число которых конечно или бесконечно. На различных этапах существования объекта ему присущи различные состояния, которые в совокупности объединяются в понятие жизненного цикла объекта. Использование предлагаемого подхода применительно к предприятию предполагает, что оно развивается, также изменяя свои состояния. Ниже приводится результат анализа управляемости процессов для различных учетных единиц современного предприятия. В качестве искомых используются: предприятие в целом; отдельные производственные процессы, рассматриваемые с системных позиций, т.е. как подсистемы управления с предприятием в одном из аспектов своей деятельности в качестве объекта управления; структурные единицы (цеха). Такой выбор учетных единиц позволяет ответить на вопросы, связанные с оценкой возможности сопоставления эффективности различных учетных единиц и проведения аналогичного сопоставления на основе вычисления потенциалов. Оценка предприятия в целом осуществляется на основе сопоставления информации о динамике выручки и основных показателей внешней отчетности предприятия – валюты баланса, стоимости оборотных и внеоборотных активов. Количественную и качественную оценку неопределенности можно получить из попарного сопоставления указанных величин на рассматриваемом промежутке времени. Это сопоставление также позволяет ответить на вопрос о степени неопределенности при принятии управленческих решений. В частности, рассматривая одну из величин (x) в качестве управляющей, а другую (y) в качестве реакции на это управление, график $y = f(x)$ будет иллюстрировать качественную картину принятия решений, связанных с регулированием величины (y) через воздействие на величину (x). На Рис. 1(а, б) приведены графики по различным парам данных на 14-летнем период 2004-2017гг. Анализ графиков показывает, что уровень неопределенности превышает 50%, в ряде случае она достигает 90%. Все данные на этом и других графиках приведены в относительных величинах.

(а) (б) (в)

Рис. 1. Характеристика управляемости предприятия на горизонте 14 лет. Сопоставление по парам «выручка квартальная – валюта баланса», «выручка квартальная – внеоборотные активы, «накопленные потенциалы выручки и активов»

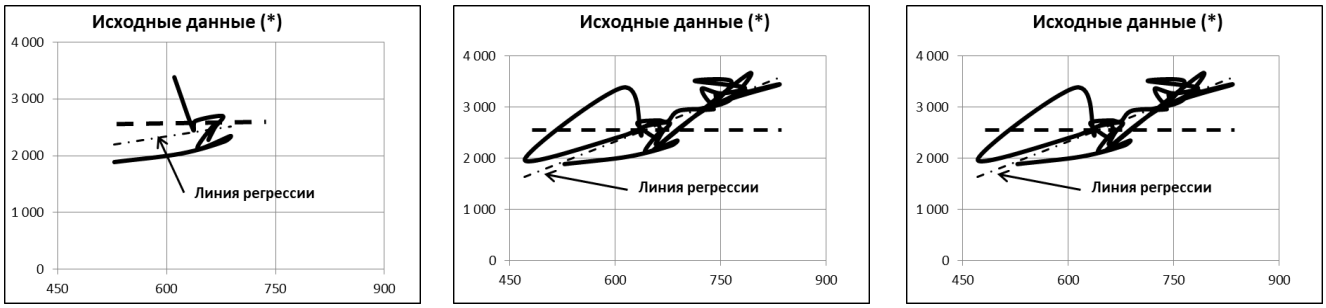
Fig. 1. Characteristics of the enterprise manageability for 14 years. The comparison in pairs "quarterly revenue and balance sheet total", "quarterly revenue and non-current assets" and "accumulated potentials of revenue and assets"

Иллюстрация характера производственных процессов предприятия, т.е. характеризацию внутренних процессов предприятия, проведена на примере показателей производства одной из сборочных единиц. Для этого проанализирована динамика зависимости товарного выпуска основного производства и динамика фактической себестоимости основного производства на различных промежутках времени – годовом, двухлетнем и трехлетнем. Анализ данных показывает, что вариация показателя выпуска относительно средней величины достигает 25%, вариация показателя себестоимости относительно линии регрессии достигает 30% величины. Годовой, двухлетний и трехлетний промежутки времени были выбраны как характерные для экономического анализа деятельности промышленного предприятия. Сопоставление величин производства и себестоимости позволяет характеризовать характер изменения эффективности производства при изменении плана выпуска, т.е. охарактеризовать эффект масштаба. Ожидаемая величина должна иллюстрировать нейтральную или положительную величину эффекта, когда увеличение масштаба производства не сказывается на изменении себестоимости выпуска или приводит к уменьшению себестоимости. Для этого были сопоставлены указанные величины на одном графике; вдоль оси абсцисс откладывалась величина выпуска, а по оси ординат – величина себестоимости. Результаты сопоставления приведены на Рис. 2. Анализ данных свидетельствует о том, что с увеличением товарного выпуска увеличивается себестоимость производства. Сказанное может иллюстрироваться линиями регрессии, приведенными на графиках. Указанные линии регрессии описываются линейным уравнением вида

$$y = kx + b. \qquad (3)$$

Существенной величиной, характеризующей в данном случае тенденцию изменения себестоимости, т.е. характеризующей эффект масштаба, является коэффициент k. Положительная величина коэффициента k будет свидетельствовать об увеличении себестоимости при увеличении производства изделия, т.е. об отрицательном эффекте масштаба производства. Наоборот, отрицательная величина будет свидетельствовать об уменьшении себестоимости при увеличении производства изделий, т.е. о положительном эффекте масштаба производства. Действительные значения коэффициента k при сопоставление однолетних и трехлетних данных свидетельствует о возможно более, чем двукратном изменении коэффициента k: $K = \frac{k_{2015-2017}}{k_{2015}} = \frac{5{,}4}{2{,}0} = 2{,}7$. С другой стороны, положительная величина коэффициента может свидетельствовать о необходимости технологического перевооружения в связи с достигнутыми предельными значениями эффективности производства. Однако, такой вывод не может быть сделан однозначно на основании исходных данных, поскольку величина неопределенности превышает 100%. Иными словами, коэффициент k, определяемый по исходным данным является незначимым и определяется с невысокой достоверностью.

Другая интерпретация данных может свидетельствовать о неизменной в целом величине себестоимости производства товарной продукции. Это иллюстрируется горизонтальными штриховыми линиями, нанесенными на графики на Рис. 2. Приведенные примеры свидетельствуют о высокой степени неопределенности в исходных данных, препятствующей адекватному определению реальных тенденций в себестоимости продукции. Следует подчеркнуть, что это затрудняет своевременное обнаружение возможных негативных тенденций в целом по предприятию и может приводить к принятию управленческих решений, приводящих к отрицательным результатам – снижению эффективности, запасов устойчивости и др.



(а) (б) (в)

Рис. 2. Характеристика управляемости производственных процессов предприятия. Сопоставление по паре «товарный выпуск по цехам основного производства – фактическая себестоимость основного производства» в 2015г. (а); в промежуток времени 2015-2016гг. (б); в промежуток времени 2015-2017гг. (в). По оси ординат отложены величины себестоимости, по оси абсцисс – товарного выпуска

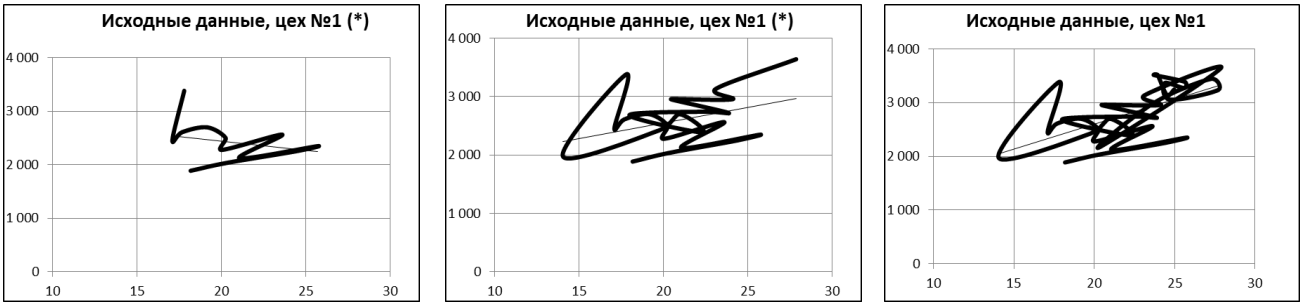
Fig. 2. Characteristics of the controllability of the production processes in the enterprise. The comparison in the pair "commodity output for the main production workshops and – the actual cost of main production" in 2015 (a); in the period of 2015-2016 (b); in the period of 2015-2017 (c). The ordinate axis shows the prime cost value, the abscissa axis – the commodity output

Иллюстрация характера производственных процессов структурных подразделений предприятия, проведена на примере показателей производства выбранной сборочной единицы по цехам. Для этого проанализирована динамика зависимости товарного выпуска по цехам основного производства и динамику фактической себестоимости, складывающейся на различных промежутках времени – годовом, двухлетнем и трехлетнем. Как и выше, годовой, двухлетний и трехлетний промежутки времени были выбраны как характерные для экономического анализа деятельности промышленного предприятия. Анализ данных показывает, что в течение 3-х лет наблюдается смена тенденции изменения выпуска продукции при сохранении тенденции увеличения себестоимости. Предполагается, что линии регрессии описываются линейным уравнением вида:

$$y = l \cdot t + b. \qquad (4)$$

Существенной величиной, характеризующей в данном случае тенденцию изменения себестоимости, т.е. характеризующей эффект масштаба, является коэффициент l. Положительная величина коэффициента l свидетельствует об увеличении себестоимости или товарного выпуска с течением времени. Наоборот, отрицательная величина свидетельствует об уменьшении себестоимости или объема выпуска с течением времени. Фактические значения коэффициента l показывают, что за 3 года наблюдается смена тенденций как в динамике выпуска продукции цехом, так и в динамике себестоимости продукции основного производства. Изменение тенденций не формализуется как безусловно установленное, поскольку значительных значений достигает вариация величин в каждый из промежутков времени. Сопоставление данных в указанные промежутки времени демонстрируется графиками, представленными на Рис. 3. По оси ординат отложены значения фактической себестоимости помесячно на годовом, двухлетнем и трехлетнем промежутках времени. По оси абсцисс отложены значения товарного выпуска этого цеха, регистрируемые помесячно на годовом, двухлетнем и трехлетнем промежутках времени соответственно. Такое представление данных позволяет провести сопоставление эффектов масштаба на уровне предприятия с аналогичным эффектом на уровне цеха. Значения коэффициента k в случае принятия гипотезы о линейной регрессии переменных при сопоставление однолетних и трехлетних данных свидетельствует о возможно более, чем

двукратном изменении коэффициента l: $K = \frac{l_{2015-2017}}{l_{2015}} = \frac{92.8}{-35.2} = -2{,}6$. Приращение коэффициента составило $\Delta l = 92{,}8 - (-35{,}2) = 128$ единиц. Знак $" - "$ свидетельствует о качественном изменении исследуемых тенденций с отрицательных величин до положительных. Недостатком проведенного анализа является незначительная достоверность результатов, вызванная высокой неопределенностью в поведении кривых. Необходимо также отметить невозможность прямого сопоставления коэффициентов k для предприятия и его подразделений.



(а) (б) (в)

Рис. 3. Товарный выпуск цеха в 2015г.(а); в период 2015-2016гг.(б); в период 2015-2017гг.(в). По оси ординат отложена фактическая себестоимость основного производства помесячно, денежные единицы (*). По оси абсцисс отложен товарный выпуск по цехам, помесячно, н/ч

Fig. 3. Commodity production of workshop in 2015 (a); in the period of 2015-2016 (b); in the period of 2015-2017 (c). The ordinate axis shows the actual monthly prime cost of main production, monetary units (*). The abscissa axis shows the monthly commodity output of the workshops

Можно сделать общий вывод о том, что анализ исходных данных не позволяет достоверно определить характер изменения эффективности производства, как на уровне предприятия, так и на уровне его структурных подразделений.

Использование потенциалов помогает выявить тенденции, складывающиеся на предприятии. В частности, на **Ошибка! Источник ссылки не найден.**1(в) показано соотношение накопленных потенциалов предприятия. Угол наклона прямой, касательной к линии потенциалов в точке, соответствующей текущим значениям потенциалов, иллюстрирует уровень технологического уклада исследуемого объекта в анализируемый момент времени. Интерпретация графика заключается в том, что тангенс угла наклона касательной к кривой потенциалов демонстрирует конкурентоспособность продукта в соответствующий промежуток времени жизненного цикла. Следует подчеркнуть, что плавность линий потенциалов позволяет использовать их при прогнозировании состояния на большие промежутки времени так, как это показано на рисунке. При этом требуется отметить, что производство разнотипной продукции на предприятии приводит к необходимости вычислений потенциалов используемых ресурсов и потенциалов результатов раздельно для каждого типа продукции. Вогнутость кривой свидетельствует об инновационном развитии предприятия. Напротив, ее выпуклость свидетельствует о процессах деградации конкурентоспособности предприятия и соответствующей наукоемкой продукции. Прямая линия зависимости потенциалов свидетельствует о стабилизации технологического уклада предприятия. Для приведенного случая можно констатировать практически постоянную величину уровня технологического уклада в течение длительного промежутка времени – более 7 лет, несмотря на изменяющиеся по разным причинам показатели деятельности предприятия. Это позволяет осуществить прогноз на будущее с высокой достоверностью. Между тем, необходимо отметить существенное отличие использования предлагаемой методологии от известных. В соответствии с методологией потенциалов, прогнозированию подвергается состояние исследуемого объекта, а не отдельные переменные или процессы.

Список литературы

1. Бейли Р., Майерс С. Принципы корпоративных финансов. М.: Олимп-бизнес, 1997. – 1086 с.
2. Иващенко Н. П. Методические основы и организация научно-технологического прогнозирования в развитых странах / ред. Н. П. Иващенко. М.: МАКС Пресс, 2013.– 296с.
3. Комков Н.И., Бондарева Н.Н., Романцов В.С., Диденко Н.И., Скрипнюк Д.Ф. Методические и организационные основы управления развитием компаний. Санкт-Петербургский политехнический университет Петра Великого; Институт народнохозяйственного прогнозирования. Москва, 2015. – 520 с.
4. Мустаев И. З. Экономические модели инноватики. Уфа: РИК УГАТУ. 2012. – 201 с.
5. Мустаев И. З. Социотехнические модели инноватики. Уфа: РИК УГАТУ. 2017. – 173 с.
6. Шарп У., Александер Г., Бейли Дж. (2001). Инвестиции. М.: ИНФРА-М, 2001. – 1028 с.

References

1. Bailey R., Myers S. Principles of Corporate Finance. M.: Olymp-business, 1997 – 1086pp. (in Russian)
2. Ivashchenko N. P. Methodical foundations and organization of scientific and technological forecasting in developed countries / ed. N. P. Ivaschenko. M.: MAX Press, 2013.– 296pp. (in Russian)
3. Komkov N.I., Bondareva N.N., Romantsov V.S., Didenko N.I., Skrypnyuk D.F. Methodological and organizational framework for managing the development of companies. Peter the Great St. Petersburg Polytechnic University; The Institute of Economic Forecasting of the Russian Academy of Sciences. Moscow, 2015 – 520pp. (in Russian)
4. Mustaev I. Z. Economic models of innovation. Ufa: RIK USATU. 2012, – 201pp. (in Russian)
5. Mustaev I. Z. Sociotechnical models of innovation. Ufa: RIK USATU. 2017, – 173pp. (in Russian)
6. Sharp W., Alexander G., Bailey J. (2001). Investments. M.: INFRA-M, 2001, – 1028pp. (in Russian)

Мустаев Ирек Закиевич, доктор экономических наук, профессор, заведующий кафедрой управления инновациями
Иванов Владимир Юрьевич, кандидат технических наук, зам. директора СП «ДБА-инжиниринг»
Семивеличенко Евгений Александрович, кандидат юридических наук, управляющий директор ПАО ОДК – УМПО
Максимова Наталья Константиновна, начальник департамента программно-проектного управления, ПАО УМПО
Мустаев Тимур Ирекович, магистрант Уфимского государственного авиационного технического университета

Mustaev Irek Zakievich, Doctor of Economic Sciences, Professor, Head of Innovation Management Department
Ivanov Vladimir Yuryevich, Candidate of Technical Sciences, Deputy Director of JV «DBA-engineering»
Semivelichenko Evgeny Aleksandrovich, Candidate of Law, Managing Director of PAO ODK – UMPO
Maksimova Natalya Konstantinovna, Head of Program and Project Management Department, PAO UMPO
Mustaev Timur Irekovich, Ufa State Aviation Technical University, Master

УДК 004.67 **DOI: 10.18413/2518-1092-2019-4-1-0-5**

Маслова М.А.

АНАЛИЗ И ОПРЕДЕЛЕНИЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Севастопольский государственный университет: ул. Университетская д. 33 г. Севастополь, 299053, Россия

e-mail: info@sevsu.ru

Аннотация
Любая информация требует эффективной системы защиты и является обеспечением устойчивого развития и функционирования объекта. Затраты необходимые для защиты информации не всегда оправданы. Поэтому важным условием обеспечения информационной безопасности является задача нахождения соответствующего уровня защиты при допустимых затратах. Значение выявления рисков в различных областях имеет ключевое значение для развития и стабильности предприятий, что дает возможность понять и оценить возможные опасные события, выявить их причины и последствия, вероятности возникновения и принятия решений, что является одной из сложных задач. Для этого необходимо провести анализ рисков информационной безопасности, с помощью которого можно будет оценить существующий уровень защищенности ресурсов любой организации. Существуют различные подходы, методы и средства оценки рисков информационной безопасности, приводящие к конечному результату, как с плюсами, так и с недостатками управления. Проведем оценку и анализ этих методов и выделим более приемлемые, эффективные и менее затратные.
Ключевые слова: информационные риски; информационная безопасность; угроза; ущерб; уязвимость; качественный метод; количественный метод; оценка уровня риска.

UDC 004.67

Maslova M.A.

ANALYSIS AND DEFINITION OF INFORMATION SECURITY RISKS

Sevastopol state University, 33 Universitetskaya St, Sevastopol, 299053, Russia

e-mail: info@sevsu.ru

Abstract
Any information requires an effective system of protection and is to ensure the sustainable development and functioning of the object. The costs necessary to protect the information are not always justified. Therefore, an important condition for information security is the task of finding the appropriate level of protection at an acceptable cost. The importance of identifying risks in different areas is crucial for the development and stability of enterprises, which makes it possible to understand and assess possible dangerous events, to identify their causes and consequences, the probability of occurrence and decision-making, which is one of the challenges. To do this, it is necessary to conduct an analysis of information security risks, with which it will be possible to assess the existing level of security of resources of any organization. There are various approaches, methods and tools for assessing information security risks, leading to the end result, both with advantages and disadvantages of management. We will evaluate and analyze these methods and identify more acceptable, effective and less costly.
Keywords: information risks; information security; threat; damage; vulnerability; qualitative method; quantitative method; risk assessment.

ВВЕДЕНИЕ

Происхождение термина «риск» берет свое начало с французского языка слова risqué или итальянского risico и обозначает возможность или вероятность наступления данного события с определенными последствиями с конечными конкретными решениями или действиями, где рассматривается не только отрицательный тип эффекта, но и положительный. В СССР риск-менеджмент начал развиваться после второй мировой войны и только в направлении страхования, который считался дорогим и неполным инструментом защиты от воздействия риска. Свое начало по работе с рисками считается статья аспиранта Чикагского университета Гарри Марковица «Диверсификация вложений» («Portfolio Selection»), в которой была представлена математически обоснованная стратегия диверсификации инвестиционного портфеля, что помогало грамотно распределить вложения и минимизировать отклонения доходности от ожидаемого показателя. В 1990 году Г.Марковицу была присуждена Нобелевская премия за то, что он вложил фундаментальные основы в развитии и изучении понятия риска.

Изначально работа с рисками применялась только к финансовой сфере, а вот уже во второй половине двадцатого века появились все ныне общеизвестные и применяемые на данный момент методы определения рисков в различных областях науки. Хотя до сих пор многие предприятия изначально не разрабатывают собственную концепцию рисков при «зарождении» предприятия и только столкнувшись с трудностями, приходят к этому [4, 8].

ОСНОВНАЯ ЧАСТЬ

Так как суть любого явления, процесса или объекта является деятельность, которая ведет к формированию результатов и различаются как: косвенные, прямые, конструктивные, деструктивные, псевдослучайные, объективные и субъективные виды результатов и т.д. Тогда объективный результат есть следствие определенного выполнения процесса, который непосредственно связан с его сутью, а субъективный результат есть выполнение процесса с недостаточным уровнем определенности и полноты информации. Преобладающее количество существующих рисков встречающихся на практике связанно именно с субъективными результатами осуществления и выполнения процесса. Поэтому можно сказать, что практически все риски есть субъективный результат выполнения процесса, и они имеют недостаток как количественной, так и качественной информации об определенном рассматриваемом процессе.

На данном этапе развития области рисков в информационных технологиях существует множество типизации рисков. Информационные риски, которые возникают в рассматриваемых процессах и проектах, отличаются между собой, как по совокупности внутренних и внешних факторов, так и по времени и месту их возникновения. При этом они влияют на их уровень, на способ анализа и методы первичного и последующего описания. Т.к. все виды рисков взаимосвязаны, следовательно, они оказывают влияние на осуществляемую деятельность, как по отдельности, так и в совокупности между собой. Необходимо классифицировать множество рисков по критериям и признакам, с помощью которых их можно объединить в общие понятия, такие как: характер, время и факторы возникновения, последствия и т.д. [8]

В свою очередь риски по характеру подразделяются на внешние и внутренние; по времени возникновения на прошлые или ретроспективные и будущие или перспективные; по фактору возникновения такие, как проектные, операционные риски, процессные, организационные; по последствиям на чистые и спекулятивные.

Так же выделяется подклассификация рисков по степени последствий возникновения рисков и состоит из: допустимого риска, критического риска и катастрофического риска. Эта классификации является важной при принятии решений по осуществлению какой-либо деятельности, связанной с рисками.

Важным этапом является идентификация риска – это одна из стадий анализа рисков позволяющая выявить, оценить и понять предпосылки, которые ведут к появлению риска и

которую необходимо проводить перед осуществлением классификации рисков. От ее правильности проведения и будет зависеть результат выбранного метода для устранения ущерба.

Информационный риск является опасное для объекта или субъекта информатизации событие, при реализации которого возможно нанести ущерб, как для информационной сферы, так и для информационного обслуживаемого объекта в целом. Информационные риски, связанные с информационной безопасностью (ИБ) с помощью современных методик анализа и управления рисками.

Определение рисков в сфере ИБ – это вероятность того, что предприятие или организация могут понести убытки из-за нарушения безопасности информационной системы (ИС). При этом часто понятие риска рассматривается с понятием угрозы, где угроза ИБ – это потенциально возможное происшествие, которое может быть совершенно преднамеренно или случайно, но при этом оказывает нежелательное воздействие как на компьютерную систему, так и на информацию, которая находится и обрабатывается и в ней. Основное отличие риска от угрозы состоит в том, что риск имеет как количественную оценку возможных потерь, так и оценки вероятности реализации угрозы.

Если рассматривать обеспечение ИБ к ИС для каких-либо проектов требующих финансовых затрат на их реализацию необходимо четко сформулировать задачу и поставить конкретную цель которую необходимо достичь. Существуют различные способы обоснований проектов подсистем обеспечения безопасности, но на практике свою реализацию получили в основном два подхода: первый заключается в проверке соответствия уровня защищенности ИС требованиям стандартов в данной области, второй – в построении системы обеспечения ИБ, которая производит как оценку, так и управление рисками.

Для того, чтобы риск описывать, необходимо определить актив (ресурс) – это элемент ИС, который имеет ценность и подлежит защите, и тогда риски можно идентифицировать по угрозе (с помощью которой вызван данный риск), ресурсу (для которого реализована данная угроза) и уязвимости (благодаря которой может быть реализована данная угроза в отношении данного ресурса). Т.е. при оценке риска, обязательно необходимо оценить: с какой частотой происходит нежелательное событие, какая вероятность данному ресурсу нанести вред, а также, сколько будет составлять потери от нанесенного ущерба [4]. Проведение оценки рисков есть очень длительной и трудоемкой задачей, при этом нет стандартных общепринятых подходов и методик для оценки рисков в конкретной ситуации. В основном факторы риска, такие как угроза, уязвимость, ущерб рассматриваются и анализируются с помощью эвристических подходов и методов за счет проведения экспертизы разными экспертами, за счет этого результаты могут отличаться друг от друга [7] и при этом возникать следующие проблемы:

- информация о риске очень часто не полная и имеет неоднозначные свойства;
- для достижения улучшения оценок необходимо назначать не менее двух специалистов в данной области;
- существует определенная сложность построения модели ИС и оценки ее уязвимости;
- сложность объединить элементы в одну систему из различных источников;
- требуется длительное время на оценку рисков, при этом потеря актуальности результатов наступает очень быстро.

Т.е. необходимо перебрать множество методов оценки риска ИБ, который будет обеспечивать наилучший результат с максимальной вероятностью оценки [3].

Сейчас на практике применяется множество разнообразных методик для анализа информационных рисков. Отличие существующих методик состоит в том, как они оцениваются: количественно, качественно или с помощью шкал оценки уровня риска. Рассмотрим данные методики.

Для оценки уровня риска организациями используется шкалы оценки, который в большей степени несут в себе описательный характер и делятся на: от 0 до 1 и разбивки на уровни: «очень низкий», «низкий», «средний», «высокий», «очень высокий» (таблица) [2].

Таблица

Уровни шкалы для оценки факторов риска

Table

Scale levels in risk assessment

Уровни шкалы		Угрозы	Ущерб	Уязвимости (У)
Очень низкий	от 0 до 0,2	Событие практически никогда не происходит	Незначительные потери материальных средств и ресурсов	У, которой можно пренебречь
Низкий	от 0,2 до 0,4	Событие случается редко	Более заметные потери материальных активов	Незначительная У, которую можно легко устранить
Средний	от 0,4 до 0,6	Событие вполне возможно при определенном стечении обстоятельств	Достаточные потери материальных активов или ресурсов	Умеренная У
Высокий	от 0,6 до 0,8	Скорее всего, событие произойдет при организации атаки	Значительный урон репутации и интересам, что может представлять угрозу для продолжения деятельности	Серьезная У, ликвидация возможна, но связана со значительными затратами
Очень высокий	от 0,8 до 1	Событие, вероятнее всего, произойдет при организации атаки	Разрушительные последствия и невозможность ведения деятельности	Критическая У, малая доля возможности ее устранения

Каждая организация разрабатывает шкалу оценки самостоятельно, поэтому могут встречаться различные градации в виде присвоения данным последствиям цифровых значений, которые могут быть как линейными, так и нелинейными, при этом смысл оценки остается прежним.

Если необходимо получить комбинации вероятности и воздействий, то используя шкалу уровней воздействия, строится матрица вероятностей, которая дает возможность присвоения ранга рискам: низкий, средний или высокий [9].

Количественный метод – включает в себя количественную оценку рисков, которая используется для исследуемых угроз. При этом связанные с ними риски можно будет сопоставить с конечными количественными значениями (в денежном эквиваленте, человекоресурсах или процентах и т.д.) и позволит получить результат в виде конкретных значений объектов оценки риска при реализации угроз ИБ [1, 5].

При количественном анализе риска используются различные методы оценки: аналитический метод; метод анализа целесообразности затрат; метод экспертных оценок; статистический метод; метод использования аналогов.

Количественная оценка рисков производиться с помощью различных факторов: необходимо определить ценность информационного актива; произвести количественную оценку потенциального ущерба от реализации каждой угрозы для каждого рассматриваемого информационного актива; определить вероятность реализации каждой из угроз ИБ; определить потенциальный ущерб для каждой угрозы и актива за определенный установленный период времени. Далее для каждой угрозы провести полученный анализ ущерба. После проведения

количественной оценки принимается решение, что делать с риском: принять, снизить или перенести [10].

Качественный метод не использует в своей оценке денежных измерений, а используется присвоение показателя по шкалам (пятибалльная шкала от 0 до 5 или десятибалльная от 0 до 10 или трехбалльная: низкая, средняя, высокая). Данный метод проводится сотрудниками (компетентными в области проведения оценки рисков и угроз) с помощью различных методов: анкетирование, тренинги, личные встречи, групповые встречи, опросы, интервьюирование и после сбора информации уже проводиться качественная оценка рисков, в которой необходимо определить:

- ценность информационных активов;
- вероятность реализации угрозы для информационного актива;
- возможность достижение положительного результата реализации угрозы в зависимости от данного состояния ИБ и внедренных средств защиты и мер;
- по каждой угрозе провести анализ конечных результатов и уровень риска.

Конечным результатом проведения качественной оценки должен быть конкретный результат для снижения рисков до минимального или приемлемого уровня, а также составлен список мер безопасности и определенный набор правил и действий [6].

Рассмотрев методы анализа информационных рисков можно сделать вывод, что с помощью всех методов можно определить перечень актуальных угроз, выбрать эффективные контрмеры и средства защиты. Главное определиться, что надо получить в результате – оценку в денежном эквиваленте и затратить на это больше времени, но получить конкретные цифры по затратам и возможному ущербу, использовав количественный метод оценки рисков. Либо выбрать более простой и быстрый путь – получив субъективный ответ на затраты и выгоды от внедрения средств защиты информации и ущерб, использовав качественный метод или метод шкалы оценки уровня риска [9, 11].

Следовательно, управление ИБ все в большей степени становиться не только необходимым, но и обязательным элементом в функционировании и управлении любого предприятия, организации. При этом ИБ имеет значение не только для сбора, обработки и хранения информации, но и для контроля: своевременного выявления угроз ИБ, уязвимостей информационной системы и меры по их устранению и предупреждению, используя существующие методы оценки уровней рисков и внедрения новых, использовав основные законы международных стандартов управления ИБ, законов ФСТЭК РФ.

ЗАКЛЮЧЕНИЕ

В данной статье было рассмотрено: общая характеристика рисков; информационные риски, связанные с информационной безопасностью; оценка рисков с помощью существующих методик. Из этого выяснили, что в ходе оценки риска можно оценить, как частоту возникновения нежелательных событий и вероятность того, что какое-то данное событие может нанести вред ресурсу, так и самое главное – стоимость данного ущерба. При оценке рисков ИБ можно выделить недостатки: оценка носит практически всегда формальный характер; оценивается без расследования на случайной, а не постоянной основе. Это влияет на то, что существующие важные данные остаются неучтенными и осведомленность лиц, которые принимают, какое-либо решение по ликвидации рисков во многих организациях будет недостаточной. Необходимо так же помнить, что главный риск – это человек, который предоставляет для ИБ наибольшую опасность в преднамеренной или не преднамеренной человеческой ошибке. Так как отсутствуют общепринятые подходы и методики для оценки рисков и в каждом конкретном случае необходимо тщательно просчитывать и продумывать все факторы риска, проводить анализ и расчет, что

является очень трудоемкой задачей, кроме того еще и существует вероятность получить ошибочный результат. Можно сделать вывод, что из всех приведенных методов оценки рисков необходимо применять совокупность методов анализа, обработки информации и только после этого оценивать риски ИБ, и осуществлять управление ИБ. Так же необходимо уменьшать «ручной труд», использовать существующие современные методологии оценки рисков, и все более переходить к оценке рисков с помощью интеллектуального анализа данных нейронных сетей [12].

Список литературы

1. Билозерова А.А., Микова С.Ю., Нестеренко М.А. Оценка рисков ИБ при использовании ERP-систем // М.: Молодой учены. 2016. №15. С. 152-155.
2. Булдакова Т.И., Миков Д.А. Реализация методики оценки рисков информационной безопасности в среде Matlab // М.: Вопросы кибербезопасности. 2015. №4(12). С. 53-61.
3. Вопросы управления информационной безопасностью / Курило А.П., Милославска Н.Г., Сенаторов М.Ю., Толстой А.И. М.: Горячая линия – Телеком, 2015. 234 с.
4. Герасименко В.А., Малюк А.А. Основы защиты информации. М.: Инкомбук, 1997.
5. Львова А.В. Методы анализа и управления рисками безопасности защищено информационной системы: Автореф. Дис. Канд. Тех. Наук. М., 2009. 198 с.
6. Методика определения угроз безопасности информации в информационных системах, 2015г. URL: https://fstec.ru/component/attachments/download/812 (дата обращения 07.01.2019).
7. Сибикина И.В. Анализ рисков информационной безопасности с использованием системы нечеткого вывода // Научный вестник НГТУ Science Bulletin of the NSTU том 65, 2016. № 4. С. 121–134
8. Хоффман Л.Дж. Современные методы защиты информации. М: Советское радио, 1980.
9. International Standard ISO/IEC 27000, 2009 y. URL: http://pqm-online.com/assets/files/lib/std/iso_iec_27000-2009.pdf (дата обращения 15.11.18)
10. Information security risks assessment: a case study / Samuel C.A., Bonaventure N, Olasunkanmi A., RobinLlal Khoshi, Samarappulige I.M. // P 13 [Электронный ресурс]: file:///D:/англоязычные%20стаатьи/1812_04659.pdf
11. Information security risk management: an intelligence-driven approach // Jeb Webb, Sean Maynard, Atif Ahmad, Graeme Shanks. Australasian Journal of Information Systems. Volume 18 Number 3, 2014
12. Reversible Recurrent Neural Networks // Matthew MacKay, Paul Vicol, Jimmy Ba, Roger Grosse, University of Toronto, Vector Institute [Электронный ресурс]: https://arxiv.org/pdf/1810.10999.pdf

References

1. Bilozerova A.A., Mikova S.Yu.. Nesterenko M.A. Risk assessment of is when using ERP-systems // M.: Molodoy ucheny 2016. №15. p. 152-155.
2. Buldakova T.I., Mikov D.A. Implementation of information security risk assessment methodology in Matlab environment M.: Voprosy kiberbezopasnosti // Voprosy kiberbezopasnosti 2015. №4(12). p. 53-61.
3. Information security management issues Kurilo A.P., Miloslavska N.G., Senatorov M.Yu., Tolstoy A.I. Goryachaya liniya – Telekom, 2015. 234 p.
4. Gerasimenko V.A., Malyuk A.A. Framework for the protection of information by information protection M.: Inkombuk. 1997.
5. Lvova A.V. Methods of analysis and management of security risks protected information system: Avtoref. Dis. Kand. Tekh. Nauk. M.: 2009. 198 p.
6. Methodology for determining information security threats in information systems, 2015 y. URL: https://fstec.ru/component/attachments/download/812 (data obrashcheniyaya 07.01.2019).
7. Sibikina I.V. Information security risk analysis using fuzzy inference system // Nauchnyy vestnik NGT Science Bulletin of the NSTU tome 65, 2016. № 4. p. 121–134.
8. Khoffman L.Dzh. Modern methods of information security. M: Sovetskoye radio. 1980.

9. International Standard ISO/IEC 27000, 2009 y. URL: http://pqm-online.com/assets/files/lib/std/iso_iec_27000-2009.pdf (data obrashcheniyaya 15.11.18)

10.Information security risks assessment: a case study / Samuel C.A., Bonaventure N, Olasunkanmi A., RobinLlal Khoshi, Samarappulige I.M. // P 13 [Electronic resource]: file:///D:/англоязычные%20стаатьи/1812_04659.pdf

11.Information security risk management: an intelligence-driven approach // Jeb Webb, Sean Maynard, Atif Ahmad, Graeme Shanks. Australasian Journal of Information Systems. Volume 18 Number 3, 2014.

12.Reversible Recurrent Neural Networks // Matthew MacKay, Paul Vicol, Jimmy Ba, Roger Grosse, University of Toronto, Vector Institute [Electronic resource]: https://arxiv.org/pdf/1810.10999.pdf

Маслова Мария Александровна, старший преподаватель, аспирант Севастопольского государственного университета
Maslova Maria Aleksandrovna, senior lecturer, postgraduate, Sevastopol state University

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ
INFORMATION TECHNOLOGIES AND TELECOMMUNICATION

УДК 004.75 **DOI: 10.18413/2518-1092-2019-4-1-0-6**

Кузнецов Д.А.[1]
Никольский П.Г.[1]
Рачков Д.С.[1]
Кузнецов А.В.[1]
Хахамов А.П.[2]

КЛАССИФИКАЦИЯ МЕТОДОВ ОБНАРУЖЕНИЯ И РАСПОЗНАВАНИЯ ЛИЦА НА ИЗОБРАЖЕНИИ

[1)] Федеральное государственное казённое военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации», ул. Приборостроительная, д. 35, г. Орёл, 302034, Россия
[2)] ФГБОУ ВО «ОГУ имени И.С. Тургенева», ул. Комсомольская, д. 95, г. Орел, 302026, Россия

e-mail: wvxp@mail.ru, pavlusha.golova@gmail.com, rachkov@mail.ru, kvaa77@mail.ru, Anton1233333@yandex.ru

Аннотация
Концепция интеллектуального зала совещаний подразумевает реализацию подсистемы контроля и управления доступом. В число функций, выполняемых этой подсистемой, входят идентификация и аутентификация пользователей. Одним из способов осуществления этих процедур является проведение обнаружения и распознавания лиц на изображениях, полученных с помощью установленных видеокамер. Другой сферой применения методов обнаружения и распознавания лиц является сенсорная плоскость интеллектуального зала совещаний, где указанные методы используются для идентификации участников, а также их автоматического учета. Задача обнаружения лица является первым шагом в процессе решения задачи распознавания лица. Следующим этапом процесса идентификации пользователя после обнаружения лица является непосредственно его распознавание. Оно производится путем сравнения вычисленных признаков с заложенными в базу данных эталонами. Многообразие различных алгоритмов обнаружения и распознавания лица обуславливает необходимость выбора оптимальных методов с точки зрения скорости обнаружения, точности распознавания и простоты реализации.
Ключевые слова: интеллектуальное пространство; зал; обнаружение лица; аутентификация; автоматизация; распознавание; контроль доступа.

UDC 004.75

Kuznetsov D.A.[1]
Nikolsky P.G.[1]
Rachkov D.S.[1]
Kuznetsov A.V.[1]
Khakhamov A.P.[2]

CLASSIFICATION OF DETECTION AND RECOGNITION METHODS OF THE PERSON ON THE IMAGE

[1)] Federal state military educational institution of higher professional education "Academy of the Federal security service of the Russian Federation", 35 Priborostroitelnaya St, Orel, 302034, Russia
[2)] Federal state budgetary institution of higher education "Orel state University" named after I.S. Turgenev, 95 Komsomolskaya St, Orel, 302026, Russia

e-mail: wvxp@mail.ru, pavlusha.golova@gmail.com, rachkov@mail.ru, kvaa77@mail.ru, Anton1233333@yandex.ru

Annotation
The concept of the intellectual hall of meetings means implementation of a subsystem of control and access control. The number of the functions which are carried out by this subsystem includes identification and authentication of users. One of ways of implementation of these procedures is carrying out detection and facial recognition on the images received by means of the installed video cameras. Other scope of methods of detection and facial recognition is the touch plane of the intellectual hall of meetings where the specified methods are used for identification of participants and also their automatic accounting. The problem of detection of the person is the first step in the course of a solution of a problem of recognition of the person. The following process step of user identification after detection of the person is directly its recognition. It is made by comparison of the calculated signs with the standards put in the database. The variety of different algorithms of detection and recognition of the person causes need of the choice of optimum methods in terms of the speed of detection, accuracy of recognition and simplicity of implementation.
Keywords: intellectual space; room; detection of the person; authentication; automation; recognition; access control.

ВВЕДЕНИЕ

Реализация подсистемы контроля и управления доступом в концепции интеллектуального зала совещаний [1] предусматривает многофакторную аутентификацию пользователей, одной из составляющих которой является идентификация человека по лицу. Важную роль играет применение методов обнаружения и распознавания лиц в сенсорной плоскости системы сопровождения совещания для идентификации участников совещания. В связи с этим стоит задача выбора оптимальных с точки зрения точности и простоты реализации методов обнаружения и распознавания лица на изображении.

ОСНОВНАЯ ЧАСТЬ

Методы обнаружения и распознавания лица на изображении

Задача обнаружения лица является первым шагом в процессе решения задачи распознавания лица. Также информация о присутствии и количестве лиц на изображении необходима для автоматического учета участников совещания. Многообразие методов обнаружения лица представлено на рисунке 1.

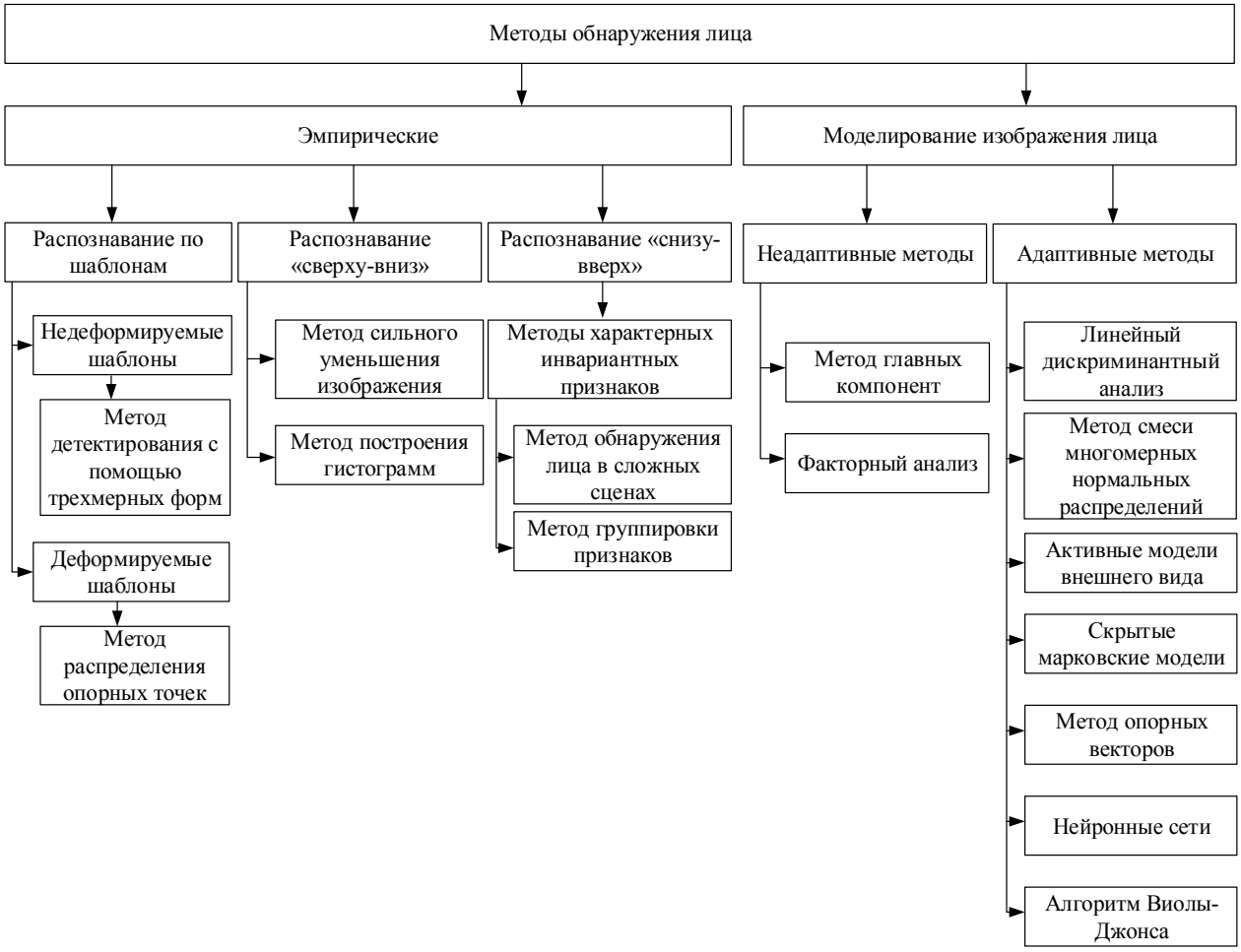


Рис. 1. Классификация методов обнаружения лица
Fig. 1. Classification of face detection methods

Вторым этапом процесса идентификации пользователя после обнаружения лица является непосредственно его распознавание. Оно производится путем сравнения вычисленных признаков с заложенными в базу данных эталонами. Основным отличием всех методов распознавания лица будет вычисление признаков и сравнение между собой (рис.2).

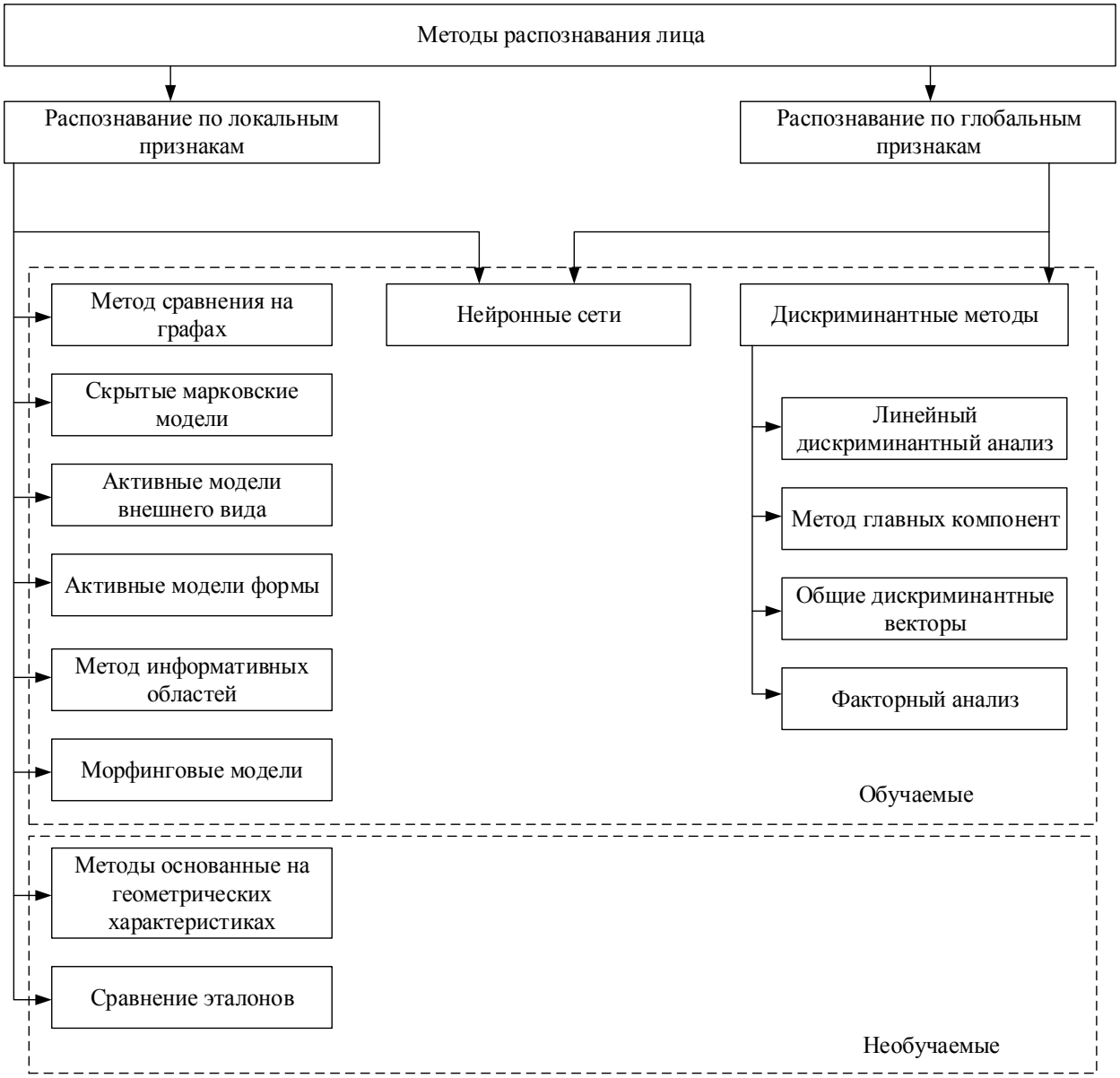


Рис. 2. Классификация методов распознавания лица
Fig. 2. Classification of facial recognition methods

Краткая характеристика методов из предложенной классификации представлена в таблице.

Таблица

Методы обнаружения и распознавания лица на изображении

Table

Methods of person detection and recognition on the image

№ п/п	Название метода	Особенности применения	Область применения	Источник
1	Метод детектирования с помощью трехмерных форм	Использует шаблон в виде пар отношений яркостей в двух областях. Все изображение сравнивается с заданным шаблоном с различным масштабом	Обнаружение лиц	[2]

№ п/п	Название метода	Особенности применения	Область применения	Источник
2	Метод распределения опорных точек	Выделяет форму переменных объектов в пределах учебного набора. Использует корреляцию для нахождения лица	Разработка эффективных систем классификации	[3]
3	Метод сильного уменьшения изображения	Подвергает изображения сильному уменьшению для сглаживания помех и уменьшения вычислительных операций. Обнаруживает область равномерного распределения яркости, после чего проверяет наличие резко отличающихся по яркости областей внутри	Обнаружение лиц	[4]
4	Метод построения гистограмм	Строит горизонтальную и вертикальную гистограммы изображения для определения областей с наличием лица	Обнаружение лиц	[5]
5	Метод обнаружения лица в сложных сценах	Ищет правильные геометрические расположения черт лица с помощью гауссовского производного фильтра с множеством различных масштабов и ориентаций	Обнаружение лиц	[6]
6	Метод группировки признаков	Использует вторую производную гауссовского фильтра для необходимых областей. С помощью порогового фильтра происходит группировка краев вокруг каждой области, а затем оценка с помощью байесовской сети для комбинирования признаков	Обнаружение лиц	[3]
7	Метод главных компонент	Производит сжатие информации с целью сохранения наиболее важной информации	Обнаружение и распознавание лиц	[7]
8	Факторный анализ	Получает модель изображения лица с некоторым числом параметров, с помощью которой производится оценка близости тестового изображения к изображению лица	Обнаружение и распознавание лиц	[8]
9	Линейный дискриминантный анализ	Выбирает проекцию пространства изображений на пространство признаков так, чтобы минимизировать внутриклассовое и максимизировать межклассовое расстояние в пространстве признаков	Обнаружение и распознавание лиц	[9]
10	Метод смеси многомерных нормальных распределений	Строится модель из нескольких кластеров изображений лиц и «не-лиц». Расстояния до этих кластеров передаются нейронной сети для вынесения решения о наличии лица	Обнаружение и распознавание лиц	[10]

№ п/п	Название метода	Особенности применения	Область применения	Источник
11	Активные модели внешнего вида	Задает изменения формы лица и его характерных черт. Для обнаружения лица находятся параметры, которые задают изображение наиболее близкое к наблюдаемому. Степень близости внешнего вида модели к наблюдаемому изображению дает возможность оценить, есть ли лицо на изображении	Анализ рентгеновских снимков и обнаружение и распознавание лиц	[11]
12	Скрытые марковские модели	Преобразует изображение в сигнал. Вероятность появления лица на изображении оценивается как вероятность генерации сигнала, соответствующего вектору признаков	Обнаружение и распознавание лиц	[12]
13	Метод опорных векторов	Производит поиск гиперплоскости в признаковом пространстве, отделяющий класс изображений лиц от изображений «не-лиц». Далее происходит линейное разделение классов с помощью проецирования векторов-признаков	Обнаружение и распознавание лиц	[13]
14	Нейронные сети	Получение классификатора, моделирующего сложную функцию распределения изображений лиц	Обнаружение и распознавание лиц	[14]
15	Алгоритм Виолы-Джонса	Изображение сканируется окном поиска, а затем применяется классификатор по каждому положению с помощью признаков Хаара [15]	Поиск изображений в реальном времени	[15]
16	Метод сравнения на графах	Эластичное сопоставление графов, описывающих изображения лиц. Лица представляются в виде графов со взвешенными вершинами ребрами.	Обнаружение и распознавание лиц	[2]
17	Активные модели формы	Распознавание производится на основе сравнения контуров лица, извлекаемых для линий головы, ушей, губ, носа, бровей и глаз. Контуры представлены ключевыми позициями, между которыми положения точек вычисляются интерполированием	Обнаружение и распознавание лиц	[16]
18	Метод информативных областей	Определение информативных областей изображения, используемых для вычисления признаков. По обучающим наборам сохраняются позиции и признаки лиц с соответствующими метками классов. При сравнении решение принимается по наиболее совпадающему признаку	Обнаружение и распознавание лиц	[17]

№ п/п	Название метода	Особенности применения	Область применения	Источник
19	Морфинговые модели	Для каждого класса объектов (лица или другого необходимого объекта) строится морфинговая модель, позволяющая сравнить новое изображение из этого класса объектов.	Распознавание лиц, верификация объектов	[18]
20	Методы основанные на геометрических характеристиках	Выделение набора ключевых точек (областей) лица и последующее выделение набора признаков	Криминалистика	[19]
21	Сравнение эталонов	Выделение областей лица на изображении и сравнение этих областей двух различных изображений методом попиксельного сравнения	Обнаружение и распознавание лиц	[2]
22	Общие дискриминантные векторы	Каждое изображение является точкой в пространстве некоторой размерности. У каждого человека в выборке есть несколько фотографий. Строится разбиение этого пространства на области, принадлежащие разным людям	Обнаружение и распознавание лиц	[20]

ЗАКЛЮЧЕНИЕ

На сегодняшний день существует множество эффективных алгоритмов обнаружения и распознавания лиц на изображениях. Предложенная классификация методов обнаружения и распознавания лиц отражает основные особенности и принципы работы каждого метода, что позволит более точно определить необходимость использования того или иного метода при реализации конкретных задач. Подсистема контроля и управления доступом в концепции интеллектуального зала совещаний подразумевает многофакторную аутентификацию пользователей, одной из составляющих которой является идентификация человека по лицу. В соответствии с предложенной классификацией в данной подсистеме принято решение использовать метод Виолы-Джонса для обнаружения лица, а также метод активных моделей внешнего вида для распознавания лица.

Работа выполнена при финансовой поддержке фонда РФФИ (проект № 18-07-00380).

Список литературы

1. Кузнецов Д.А. Предпосылки создания интеллектуального зала совещаний / Кузнецов Д.А., Офицеров А.И., Кузнецов А.В., Чистяков С.В., Басов О.О. // Научный результат. Информационные технологии. 2018. Том 3. Вып. 2. С. 44-50.

2. Тропченко А.Ю. Методы вторичной обработки и распознавания изображений / Тропченко А.Ю., Тропченко А.А. // Университет ИТМО, 2015. С. 215.

3. Татаренков Д.А. Анализ методов обнаружения лиц на изображении / Татаренков Д.А. // Молодой ученый. 2015. С. 270-276.

4. Рахманкулов В.З. Обработка и распознавание изображений промышленных деталей // Рахманкулов В.З., Ахрем А.А., Герасимов В.В., Лебедев В.В. // Труды ИСА РАН. 2005. С. 99-129.

5. Валюх А.А. Алгоритм поиска изображений на основе гистограмм. / Валюх А.А., Тонкошкур Ю.О. // [Электронный ресурс]. – Режим доступа: http://ea.donntu.org:8080/bitstream/123456789/12866/1/Валюх%20A.A..pdf (дата обращения: 10.01.2019)

6. Алкилар-Гонзалез П.М. Автоматизированное обнаружение объектов на зашумленном изображении / Алкилар-Гонзалез П.М., Карнаухов В.Н., Кобер В.И. // Информационные процессы. 2014. Том 14. Вып 1. С. 1-8.

7. Померанцев А. Метод главных компонент / Померанцев А. // Российское хемометрическое общество. [Электронный ресурс]. -Режим доступа: http://rcs.chemometrics.ru/Tutorials/pca (дата обращения: 10.01.2019).

8. Харман Г. Современный факторный анализ / Харман Г. // М.: Статистика. 1972. С. 489.

9. Тимошенко Д.М. Методы автоматической идентификации личности по изображениям лиц, полученным в неконтролируемых условиях / Тимошенко Д.М. // Автореферат дис.кан.наук. Петрозаводск. 2014. С. 16.

10. Воронцов К.В. Лекции по статистическим алгоритмам классификации / Воронцов К.В. // ФУПМ МФТИ. 2005.

11. Кутес Т.Ф. Активные модели внешнего вида / Ф. Кутес, Г.Дж. Эдвардс, К.Дж. Тейлор // Конференция IEEE по анализу образов и компьютерной разведке. 2001. С. 681-685.

12. Двойной И.Р. Сравнительный анализ структур скрытых марковских моделей, используемых в задаче установления личности человека по изображению лица / Двойной И.Р., Сальников. И.И. // [Электронный ресурс] Современные проблемы науки и образования. 2013. URL: www.scienceeducation.ru/113-10751 (дата обращения: 10.01.2019).

13. Иванов Ю.С. Алгоритмы распознавания подвижных объектов для интеллектуальных систем охранного видеонаблюдения / Иванов Ю.С. // Автореферат дис. кан. наук. Комсомольск-на-Амуре. 2014. С. 159.

14. Бураков М.В. Нейронные сети и нейроконтроллеры / Бураков М.В. // Учебное пособие. СПб.: ГУАП. 2013. С. 284.

15. Виола Р. Быстрое обнаружение объекта, используя усиленный каскад простых признаков / Р. Виола, М.Д. Джонс // Конференция по компьютерному зрению и распознаванию образов. 2001.

16. Кутес Т.Ф. Сравнение активных моделей формы с активными моделями внешнего вида / Т.Ф. Кутес, Г.Дж. Эдвардс, К.Дж. Тейлор // Конференция: британские слушания по компьютерному зрению. 1999. С. 10.

17. Мурашов Д.М. Метод локализации информативных областей с текстурой специального вида / Мурашов Д.М., Мурашов Ф.Д. // «Машинное обучение и анализ данных. 2018. С. 122-135.

18. Зенин А.В. Анализ методов распознавания образов / Зенин А.В. // Молодой ученый. 2017. С. 125-130.

19. Якименко Ю.И. Методы автоматической идентификации лиц / Якименко Ю.И., Дзюба В.Г. // Четвертая международная студенческая конференция «Свет молодым-молодым свету». 2004. С. 85-90.

20. Ким. Дж. Факторный дискриминантный и кластерный анализ / Ким. Дж., Мьюллер Ч.У., Клекка У.Р. // Финансы и статистика. 1989. С. 215.

References

1. Kuznetsov D. A. Prerequisites of creation of the intellectual hall Meetings / Kuznetsov D.A., Ofitserov A.I., Kuznetsov A.V., Chistyakov S.V., Basov O.O. //Scientific result. Information technologies. 2018. Volume 3. Issue 2. P. 44-50.

2. Tropchenko A.Yu. Methods of secondary processing and images recognition / Tropchenko A.Yu., Tropchenko A.A. // ITMO university, 2015. P. 215.

3. Tatarenkov D.A. The analysis of methods of detection of persons on Image / Tatarenkov D.A. // Young scientist. 2015. P. 270-276.

4. Rakhmankulov V.Z. Processing and recognition of images of industrial details // Rakhmankulov V.Z., Akhr A.A., Gerasimov V.V., Lebedev V.V.//Works IZA RAHN. 2005. P. 99-129.

5. Valyukh A.A. An algorithm of search of images on the basis of histograms. / Valyukh A.A., Tonkoshkur Yu.O. // [Electronic resource]. – the access Mode: http://ea.donntu.org:8080/bitstream/123456789/12866/1/Валюх%20A.A..pdf (date of the address: 10.01.2019).

6. Alkilar-Gonzalez P.M. The automated detection of objects on the noisy image. / Alkilar-Gonzalez P.M., Karnaukhov V.N., Kober V.I. // Information processes. 2014. Volume 14. Vyp 1. P. 1-8.

7. Pomerantsev A. Method main component. / Pomerantsev A. // Russian hemometrichesky society. [Electronic resource]. – the access Mode: http://rcs.chemometrics.ru/Tutorials/pca (date of the address: 10.01.2019).

8. Harman G. Modern factorial analysis / Harman G. // M.: Statistics. 1972. P. 489.

9. Tymoshenko D.M. Methods of automatic identification of the personality according to the images of persons received in uncontrollable conditions / Tymoshenko D.M.//Abstract thesis. cand. of sciences. Petrozavodsk. 2014. P. 16.

10. Vorontsov K.V. Lectures on statistical algorithms of classification / Vorontsov K.V. // FUPM MIPT. 2005.

11. T.F. cutis. Active models of appearance / F. Kutes, G. J. Edwards, K. J. Taylor // IEEE Conference on the analysis of images and computer vision. 2001. P. 681-685.

12. Double I.R. The comparative analysis of structures of the hidden Markov models used in a problem of identification of the person of the image of the person / Double I.R., Sealing glands. I.I. // [Electronic resource] Modern problems of science and education. 2013. URL: www.scienceeducation.ru/113-10751 (date of the address: 10.01.2019).

13. Ivanov Yu.S. Algorithms of recognition of mobile objects for the intellectual systems of security video surveillance. / Ivanov Yu.S. // Abstract yew. canal of sciences. Komsomolsk-on-Amur. 2014. P. 159.

14. Burakov M.V. Neural networks and Neurocontrollers / Beets M. B. // Manual. SPb.: GUAP. 2013. P. 284.

15. Viol of River. Fast detection of an object, using the strengthened cascade of simple signs. / P. Viola, M.D. Jones // Conference on computer sight and recognition of images. 2001.

16. T.F. cutis. Comparison of active models of a form with active models of appearance / T.F. Kutes, G.J. Edwards, K. J. Taylor // Conference: the British hearings on computer sight. 1999. P. 10.

17. Murashov D.M. A method of localization of informative areas with texture of a special look / Murashov D.M., Murashov F.D. // Machine learning and analysis of data. 2018. Page 122-135.

18. Zenin A.V. Analysis of methods of recognition of images. / Zenin A.V. // Young scientist. 2017. P. 125-130.

19. Yakimenko Yu.I. Methods of automatic identification of persons. / Yakimenko Yu.I., Dzyuba V.G. // the Fourth international student's conference "Light to Young People Young People to Light". 2004. Page 85-90.

20. Kim. J. Factorial discriminant and cluster analysis. / Kim. J., Myyuller Ch.U., Klekka U.R. // Finance and statistics. 1989. P. 215.

Кузнецов Денис Андреевич, студент Академии Федеральной службы охраны Российской Федерации
Никольский Павел Геннадьевич, студент Академии Федеральной службы охраны Российской Федерации
Рачков Даниил Сергеевич, студент Академии Федеральной службы охраны Российской Федерации
Кузнецов Андрей Викторович, кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации
Хахамов Антон Павлович, студент кафедры «Электроника, вычислительная техника и информационная безопасность»

Kuznetsov Denis Andreevich, student Academy of the Federal security service of the Russian Federation
Nikolsky Pavel Gennadyevich, student Academy of the Federal security service of the Russian Federation
Rachkov Daniil Sergeevich, student Academy of the Federal security service of the Russian Federation
Kuznetsov Andrey Viktorovich, candidate of technical sciences, Academy of the Federal security service of the Russian Federation
Khakhamov Anton Pavlovich, student Department of Electronics, computer engineering and information security