

**СИСТЕМНЫЙ АНАЛИЗ
И ПРИКЛАДНАЯ
ИНФОРМАТИКА
№ 2, 2019**

**SYSTEM ANALYSIS
AND APPLIED
INFORMATION SCIENCE
No 2, 2019**



**Международный
Научно-технический журнал**

Издается с декабря 2012 года

Учредитель

Белорусский национальный
технический университет

Главный редактор

Сергей Васильевич Харитончик

Редакционная коллегия

В. Ф. Голиков (зам. главного редактора),
В. А. Богущ, Т. В. Борботько, В. Б. Байбурин (РФ),
Д. Ю. Большаков (РФ), Л. С. Герасимович, Н. Н. Гурский,
Ю. М. Захарик, И. А. Каляев (РФ), Г. О. Кипиани (Грузия),
Э. Г. Лазаревич, В. А. Липницкий, А. А. Лобатый,
В. А. Мищенко, Е. И. Никифорович (Украина),
А. А. Прихожий, И. А. Сатиков, В. В. Старовойтов,
П. П. Урбанович, А. Патрин (Польша),
Ю. Н. Петренко (ответственный секретарь),
Н. Н. Ташатов (Казахстан), А. В. Чигарев, Д. К. Щеглов (РФ)

**International
Science and Technique Journal**

Published since December, 2012

Founder

Belarusian National Technical
University

Editor-in-chief

Sergei V. Kharytonchyk

Editorial board

V. Golikov (deputy editor-in-chief), V. Bogush,
T. Borbotko, V. Baiburin (RF), D. Bolshakov (RF), N. Gurskiy,
L. Gerasimovich, J. Zaharik, I. Kalyaev, G. Kipiani (Georgia),
E. Lazarevich, V. Lipnitsky, A. Lobaty, V. Mishchenko,
E. Nikiforovich (Ukraine), A. Prihozhy, I. Satikov,
V. Starovoytov, P. Urbanovich, A. Patrin (Poland),
Y. Petrenko (executive secretary), N. Tashcatov
(Kazakhstan), A. Chigarev, D. Shcheglov (RF)

Журнал включен в "Перечень научных изданий Республики Беларусь
для опубликования результатов диссертационных исследований".

Журнал включен в международные каталоги и базы данных:

- ❖ Российский индекс научного цитирования (РИНЦ)
- ❖ Научная электронная библиотека eLIBRARY.RU
- ❖ Электронно-библиотечная система (ЭБС) издательства Лань
- ❖ DOAJ <https://doaj.org/toc/2414-0481>
- ❖ Google Scholar
- ❖ Киберленинка

- ❖ EBSCO
- ❖ BASE Search
- ❖ OpenAIRE
- ❖ WorldCat
- ❖ OpenDOAR
- ❖ ROAR

Содержание

Contents

СИСТЕМНЫЙ АНАЛИЗ

Голуб Ю. И., Старовойтов Ф. В.

Исследование локальных оценок контраста цифро-
вых изображений при отсутствии эталона 4

Старовойтов В. В.

Индекс SSIM не является метрикой и плохо оцени-
вает сходство изображений 12

УПРАВЛЕНИЕ ТЕХНИЧЕСКИМИ ОБЪЕКТАМИ

Лях Б. А., Кондратенко В. А., Морозов Д. В.

Структура математической модели многопозицион-
ной системы радиомониторинга сигналов коротко-
волнового диапазона 19

Малкин В. А., Рожков И. В., Санько А. А.

Влияние ветровых возмущений и нелинейностей
сервопривода на контур стабилизации высоты по-
лета беспилотного летательного аппарата 23

SYSTEM ANALYSIS

Golub Y. I., Starovoytov F. V.

Study of local assessments of contrast for digital
images 4

Starovoytov V. V.

The SSIM index is not a metric and it is badly evaluate
the simility of images 12

MANAGEMENT OF TECHNICAL OBJECTS

Liakh B. A., Kondratyonok V. A., Morozov D. V.

Modelling of radio monitoring system of short-wave
radio communication adaptive systems 19

Malkin V. A., Rozhkov I. V., San'ko A. A.

Influence of wind disturbances and nonlinearities of
servo drive on the contour of stabilization of the flight
of height of unmanned aerial vehicle 23

ОБРАБОТКА ИНФОРМАЦИИ И ПРИНЯТИЕ РЕШЕНИЙ**Блинова Е. А., Сущеня А. А.**

Применение нескольких стеганографических методов для осаждения скрытых данных в электронных текстовых документах 32

Кузьмич Л. В., Орнатский Д. П., Квасников В. П.

Моделирование аналогового интерфейса для дистанционных измерений 39

ЗАЩИТА ИНФОРМАЦИИ**Голиков В. Ф., Радюкевич М. Л.**

Формирование общего секрета с помощью искусственных нейронных сетей 49

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ**Попова Ю. Б.**

От LMS к адаптивным обучающим системам 58

DATA PROCESSING AND DECISION-MAKING**Blinova E. A., Suschenia A. A.**

Several steganographic methods using for embedding of hidden data in electronic text documents 32

Kuzmych L. V., Ornatskyi D. P., Kvasnikov V. P.

Simulation of the analogue interface for remote measurements 39

INFORMATION SECURITY**Holikau U. F., Radziukevich M. L.**

Generation a shared secret using artificial neural networks 49

INFORMATION TECHNOLOGIES IN EDUCATION**Popova Y. B.**

From LMS to adaptive training systems 58

Ответственный секретарь редакции

Петренко Ю. Н.

Технический редактор

Лакин В. И.

Адрес редакцииул. Франциска Скорины 25/3, Минск, 220114,
Республика Беларусь
Тел. +375 17 267-66-84
e-mail: CA_PI@bntu.by**Executive secretary of the editorial board**

Y. Petrenko

Technical Editor

V. Lakin

Editorial board address25/3 Franciska Skariny str., Minsk, 220114,
Republic of Belarus
Tel. +375 17 267-66-84
e-mail: CA_PI@bntu.by

Свидетельство о государственной регистрации средства массовой информации № 1540 от 08.06.2012, выданное Министерством информации Республики Беларусь

Подписано в печать 00.00.2019. Формат бумаги 60×84 1/8. Бумага офсетная.

Отпечатано на ризографе. Усл. печ. л. 9,30. Уч.-изд. л. 3,64. Тираж 100 экз. Заказ 960.

Отпечатано в БНТУ. ЛП № 02330/74 от 03.03.2014.

220013, г. Минск, пр. Независимости, 65.

© Белорусский национальный технический университет

СИСТЕМНЫЙ АНАЛИЗ

SYSTEM ANALYSIS

УДК 004; 004.93

Ю. И. ГОЛУБ¹, Ф. В. СТАРОВОЙТОВ²

ИССЛЕДОВАНИЕ ЛОКАЛЬНЫХ ОЦЕНОК КОНТРАСТА ЦИФРОВЫХ ИЗОБРАЖЕНИЙ ПРИ ОТСУТСТВИИ ЭТАЛОНА

¹Объединенный институт проблем информатики
Национальной академии наук Беларуси

²Белорусский национальный технический университет

В статье рассматривается понятие контраста цифрового изображения. Исследованы различные количественные оценки контраста цифровых изображений. Выполнены сравнительные экспериментальные исследования разных оценок контраста на двух стандартных базах изображений. Показано, что оценивание контраста посредством вычисления среднего арифметического или среднеквадратического значений множества локальных оценок не всегда совпадает с визуальной оценкой человека. Результаты экспериментов показали, что параметр формы распределения Вейбулла является более точной оценкой множества локальных измерений контраста, вычисленных функциями BEGH, GORD, LOEN и хорошо коррелирует с визуальными оценками контраста.

Ключевые слова: контраст изображения, коэффициент контраста, оценка качества изображения

Введение

Одним из показателей качества изображения является его контраст. Анализ научно-технической литературы показал, что единое определение этого понятия отсутствует [1–2]. Кроме того, есть различные определения коэффициента контраста, определяющего степень и выражаемого безразмерной величиной [3]. Контраст изображения визуальный – это зрительное восприятие разницы между светлыми и темными участками изображения [1].

В 1729 г. французский физик Пьер Бугер, исследуя способность человека различать величины физической яркости (или освещенности предмета), установил, что дифференциальный порог для яркости – т. е. минимальный прирост яркости ΔI , необходимый для того, чтобы вызвать едва заметное различие в ощущении яркости, – примерно пропорционален уровню фоновой яркости I , в силу чего отношение $\Delta I / I$ – величина постоянная.

Через 100 лет, в 1831 г. независимо от Бугера, психофизик Эрнст Вебер в экспериментах на различение весов, длин линий и высоты звукового тона также обнаружил постоянство отношения дифференциального порога к фоновой величине стимула, т. е. определил мини-

мальный контраст, при котором глаз может различать детали сцен и объектов. Он ограничен порогом контрастной чувствительности глаза. В научной литературе такое определение коэффициента контраста называют законом Вебера, он равен

$$K_B = (I_{об} - I_{фон}) / I_{фон}, \quad (1)$$

где $I_{об}$ – яркость объекта, $I_{фон}$ – яркость фона. Однако понятие объекта и фона для произвольного изображения определить затруднительно.

Михельсона уточнил определение коэффициента контраста:

$$K_M = (I_{max} - I_{min}) / (I_{max} + I_{min}), \quad (2)$$

где I_{max} – максимальное и I_{min} – минимальное значения яркости. Недостаток такого определения – равный контраст у темных и светлых изображений при $I_{min} = 0$.

Модифицированный вариант такого вычисления контраста изображения предложен Гордоном [4]. Он предложил вычислять коэффициент контраста Михельсона локально, а вместо I_{min} и I_{max} использовать средние значения яркости в квадратных окрестностях пикселей размером 3×3 и 9×9 .

Кадничанский С. А. в работе [5] показал, что основные классические формулы вычисле-

ния глобального контраста не совпадают с визуальными оценками. Он же для описания контраста 8-битного полутонового цифрового изображения предложил два варианта формул вычисления локального $K_{\text{лок}}$ и глобального контраста $K_{\text{глоб}}$:

$$\begin{aligned} K_{\text{лок}} &= (I_{\text{max}} - I_{\text{min}}) / 255, \\ K_{\text{глоб}} &= 2\sigma / 255, \end{aligned} \quad (3)$$

где I_{max} , I_{min} – максимальное и минимальное значения яркости в окрестностях пикселей, σ – стандартное отклонение.

В качестве альтернативных параметров используют также модули градиентов яркости. Простое рассуждение показывает, что при автоматическом определении контраста глобальные параметры, вычисленные для всего изображения, могут дать значения контраста не совпадающее с визуальной оценкой человека. Например, когда все изображение малоконтрастное, а пара пикселей или маленьких фрагментов имеют максимально противоположные значения, глобальное значение контраста будет максимальным.

Таким образом, следует вычислять локальные оценки контраста в окрестности каждого пикселя или разделив изображение на небольшие фрагменты. В этом случае вычисляется множество локальных оценок и возникает задача вычисления на их базе единой оценки контраста. Чаще всего для этого используют среднее арифметическое или среднеквадратичное значение, однако наши исследования показывают, что это не лучший вариант обобщения множества локальных оценок [6–7]. Поэтому для вычисления единой оценки контраста изображения исследуем параметры других распределений случайных величин. В данной статье были проанализированы параметры распределения Вейбулла, для оценки контраста использовались следующие количественные меры: локальная энтропия, CHAN, CMO, CONT, BEGH [8], EBCM, GCF1, GCF2, GOLF [9], локальный контраст, вычисленный по формуле Гордона GORD [4], GRAD (вычисление контраста через градиент дает нечеткие пики), GRAT, LAPL, LCON, LOCC, LOCM (вычисляет разницу яркости в одном направлении), LOEN, LVAR, MATK [10], NATU, NIQE, NJQA, PB, S3, SFIL, SFRQ, STD, SVD1, SVD2, SVD, SVDM, SVDO, TMQI, часть из них описана в работе [7].

Экспериментальная часть

В экспериментах исследована гипотеза о возможном использовании в качестве новой глобальной оценки контраста параметры распределения Вейбулла, построенного для гистограммы множества локальных оценок. Параметры этого преобразования исследовались при модификации популярной меры сравнения цифрового изображения с эталоном – индекса структурного сходства, называемого в литературе *SSIM*. Результаты исследований описаны в статье [6], где было обосновано применение параметров распределения Вейбулла для оценки качества изображений. Однако мера *SSIM* сравнивает изображение с эталоном и показывает степень отличия от эталона. На практике эталонный образец зачастую не известен. Основной результат работы [6] – доказательство того, что множество локальных оценок можно характеризовать не средним значением, а одним из параметров статистического распределения этих оценок, в частности распределения Вейбулла.

Для тестирования различных мер контраста использовались два множества изображений:

1) база данных CCID2014 [11], содержащая 655 разноконтрастных вариантов 15-ти цветных изображений из базы Kodak [12] размером 768×512 пикселей. Кроме того, база CCID2014 содержит усредненные пользовательские оценки MOS для каждого изображения;

2) множество из 21 стандартного изображения, используемого в исследованиях по обработке изображений. К каждому изображению применялось линейное преобразование. Коэффициент контраста k изменялся от 0,25 до 7,0 с шагом 0,25, яркость каждого пикселя (i, j) изменялась согласно формуле $\text{newIm}(i, j) = k * (\text{Im}(i, j) - 127,5) + 127,5$, в итоге было сформировано 588 изображений с разным контрастом (рис. 1).

Как было отмечено в наших исследованиях ранее [6, 7], выбор изображения с визуально лучшим контрастом – очень сложная задача, с которой практически не справилась ни одна из описанных в литературе оценок качества изображений.

Оценочные меры Кадичанского были исследованы в локальном и глобальном вариантах. Тестирование этих мер на разных изображениях с изменяющимся коэффициентом кон-

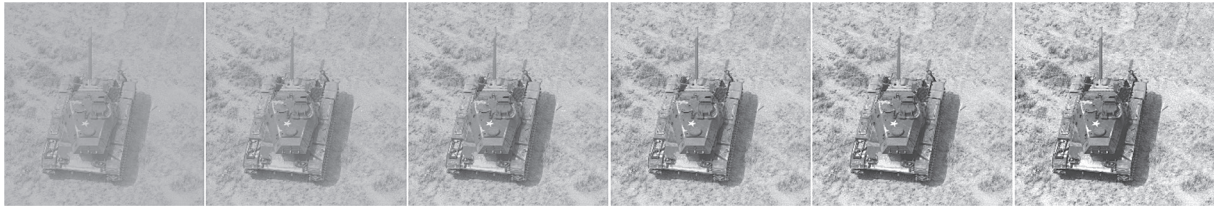


Рис. 1. Примеры изображений с разными значениями коэффициента контраста

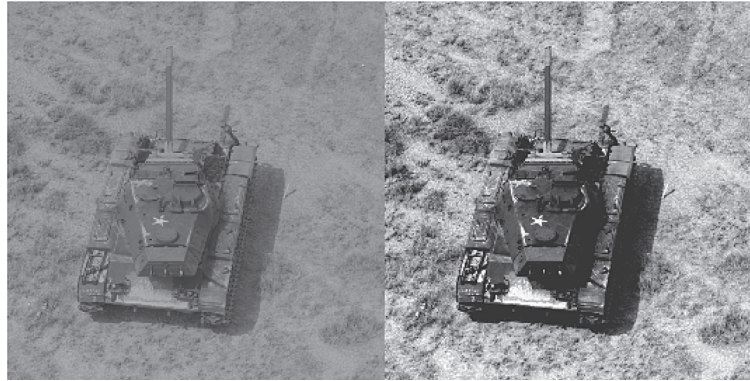


Рис. 2. Слева исходное изображение, справа автоматически выбранное изображение с максимальным контрастом

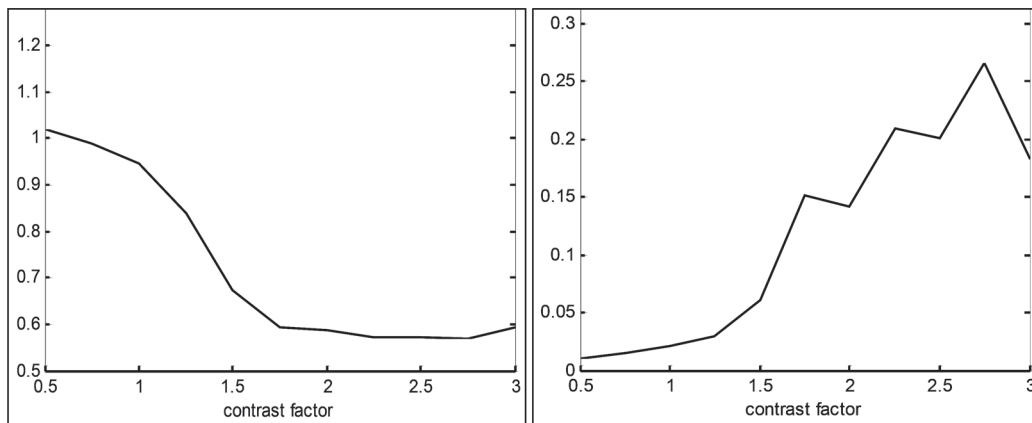


Рис. 3. Параметр формы распределения Вейбулла имеет минимальное значение при максимальном контрасте изображения (слева), а среднее значение локальных контрастов имеет максимальное значение для этого же коэффициента контраста равного 2,75

траста показало, что с их помощью невозможно выбрать наиболее контрастное изображение. Кроме того, эти две меры плохо коррелируют с визуальными оценками контрастности изображений. Поэтому эти меры были отвергнуты как не точные.

Ряд мер контраста, предложенных в литературе, по этим же причинам был забракован. Среди них: меры: GRAD (вычисление контраста через градиент дает нечеткие пики), LOCM (вычисляет разницу яркости в одном направлении), GOLE [9], MATK [10].

Некоторые оценки позволяют относительно корректно определить наиболее контрастные изображения во втором тесте. К ним относятся локальные оценки контраста по фор-

муле Гордона [4] после применения распределения Вейбулла параметр масштаба a , вычисленный для ряда изображений с линейно измененным контрастом, имеет вид неубывающей функции, параметр формы b более информативен. Он имеет пики и минимумы внутри диапазона значений коэффициента контраста для большинства тестовых изображений (см. рис. 2–5 и таблицу).

В таблице представлены сводные результаты определения контраста разных изображений двумя функциями: Гордона (GORD) [4] и Beghdadi (BEGH) [8]. Для обоих вычислялись локальные оценки, затем определялись их среднее значение и параметры их распределения функцией Вейбулла (a и b). Знаком «+»



Рис. 4. Слева исходное изображение, справа лучшее изображение с коэффициентом контраста равным 1,5

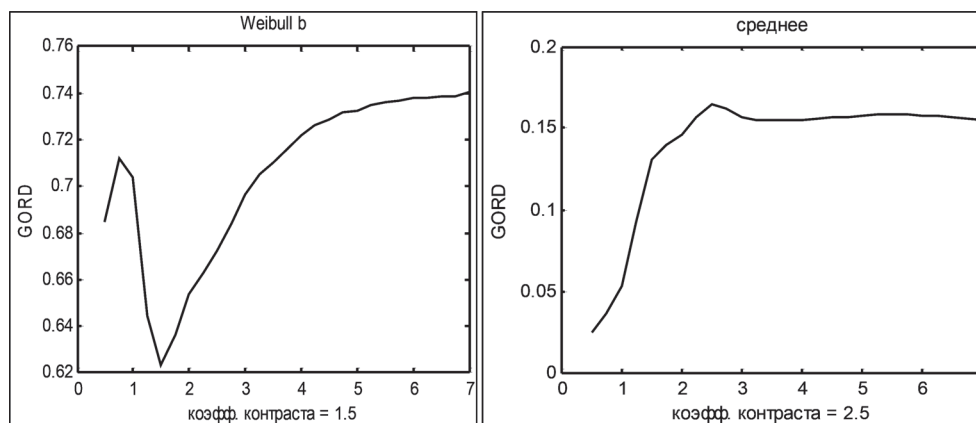


Рис. 5. Параметр формы распределения Вейбулла локальных оценок контраста Гордона при анализе изображений, представленных на рис. 4, указывает на максимальный контраст изображения при коэффициенте изменения контраста равном 1,5, а среднее локальных оценок дает пик при коэффициенте равном 2,5, что неверно

Оценки корректного определения визуально оптимального контраста тестовых изображений

№	Название изображения	Мера	Оптим. коэф. контраста через параметр формы b	Среднее	№	Название изображения	Мера	Оптим. коэф. контраста через параметр формы b	Среднее
1	boat	GORD BEGH	1,5 + 1,25 +	— +	12	bridge	GORD BEGH	1,75 + 1,5 +	~ —
2	moon	GORD BEGH	— —	— —	13	lena	GORD BEGH	1,5 + 1,5 +	~ ~
3	clock	GORD BEGH	2,75 ~ 3,25 ~	— —	14	goldhill	GORD BEGH	—	—
4	man	GORD BEGH	1,25 + —	— —	15	baboon	GORD BEGH	1,5 + —	— —
5	finger	GORD BEGH	2,75 + 3,5 +	+ +	16	flowers	GORD BEGH	— ~	— —
6	houses	GORD BEGH	3,25 ~ 3,0 ~	~ —	17	tiffany	GORD BEGH	— —	— —
7	kiel	GORD BEGH	1,25 + —	— —	18	truck	GORD BEGH	2,25 ~ 1,25 +	— +
8	trucks	GORD BEGH	2,5 + —	— —	19	pepper	GORD BEGH	1,25 +	—
9	zelda	GORD BEGH	1,5 + —	— —	20	orchid	GORD BEGH	— 1,5 +	— —
10	airfield	GORD BEGH	1,75 + —	— —	21	cameraman	GORD BEGH	— —	— —
11	tank	GORD BEGH	1,75 + —	— —					



Рис. 6. Оригинальные изображения баз Kodak и CCID2014

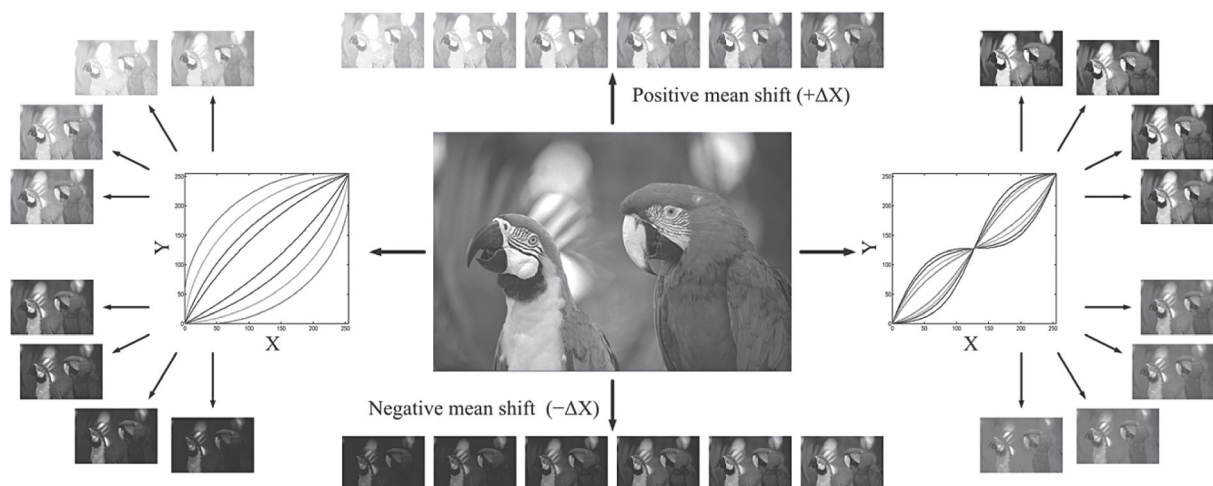


Рис. 7. Схема преобразований изменения контраста исходного изображения

отмечены варианты с визуально корректными результатами, а рядом записаны найденные значения коэффициента контраста. Знак « $\leftarrow$ » означает неверное определение коэффициента контраста, знак « $\sim$ » – удовлетворительное.

На данном этапе выполнены исследования известных оценок контраста цифровых изображений. Показано, что глобальные количественные оценки часто противоречат визуальным оценкам. При использовании локальных оценок контраста в известных мерах чаще всего определяется их среднее арифметическое в качестве единой оценки контраста. Экспериментально показано, что такое среднее значение редко коррелирует с визуальной оценкой контраста.

Исследован вариант модификации ряда оценок контраста посредством применения к ним распределения Вейбулла и анализ двух его параметров на предмет использования в качестве оценки контраста изображения. Согласно выполненным экспериментам лучшие оценки контраста изображений получены с помощью локальных оценок, вычисляемых по функции Гордона, к которым применено распределение Вейбулла. Минимальное значение параметра формы этого распределения чаще всего указывает на визуально наиболее контрастное изображение.

Вторая группа экспериментов была выполнена на базах изображений – Kodak (25 изображений) [12] и CCID2014 (655 изображений) [11]. Исходные изображения Kodak представлены на рис. 6. На рис. 7 представлена схема преобразований изменения контраста исходных изображений. Было протестировано 26 мер качества, опубликованных в научной литературе и используемых для оценки контраста и качества изображений при отсутствии эталона (no-reference measures). Протестирован ряд количественных мер оценки качества изображений при отсутствии эталона, а именно: CHAN, CMO, CONT, EBCM, GCF1, GCF2, GRAT, LAPL, LCON, LOCC, LOEN, LVAR, NATU, NIQE, NJQA, PB, S3, SFIL, SFRQ, STD, SVD1, SVD2, SVD, SVDM, SVDO, TMQI, часть из них описана в работе [6].

Была выполнена оценка каждого тестируемого изображения – построены графики для всех количественных мер качества и визуальной субъективной оценки (MOS – Mean Opinion Score, Средняя экспертная оценка), полученной вместе с базой изображений CCID2014 [11]. Из всех вышеперечисленных количественных мер, лучшие результаты показали функции BEGH, GORD, LOEN.

На рис. 8 представлены графики изменений средних значений для лучших количественных

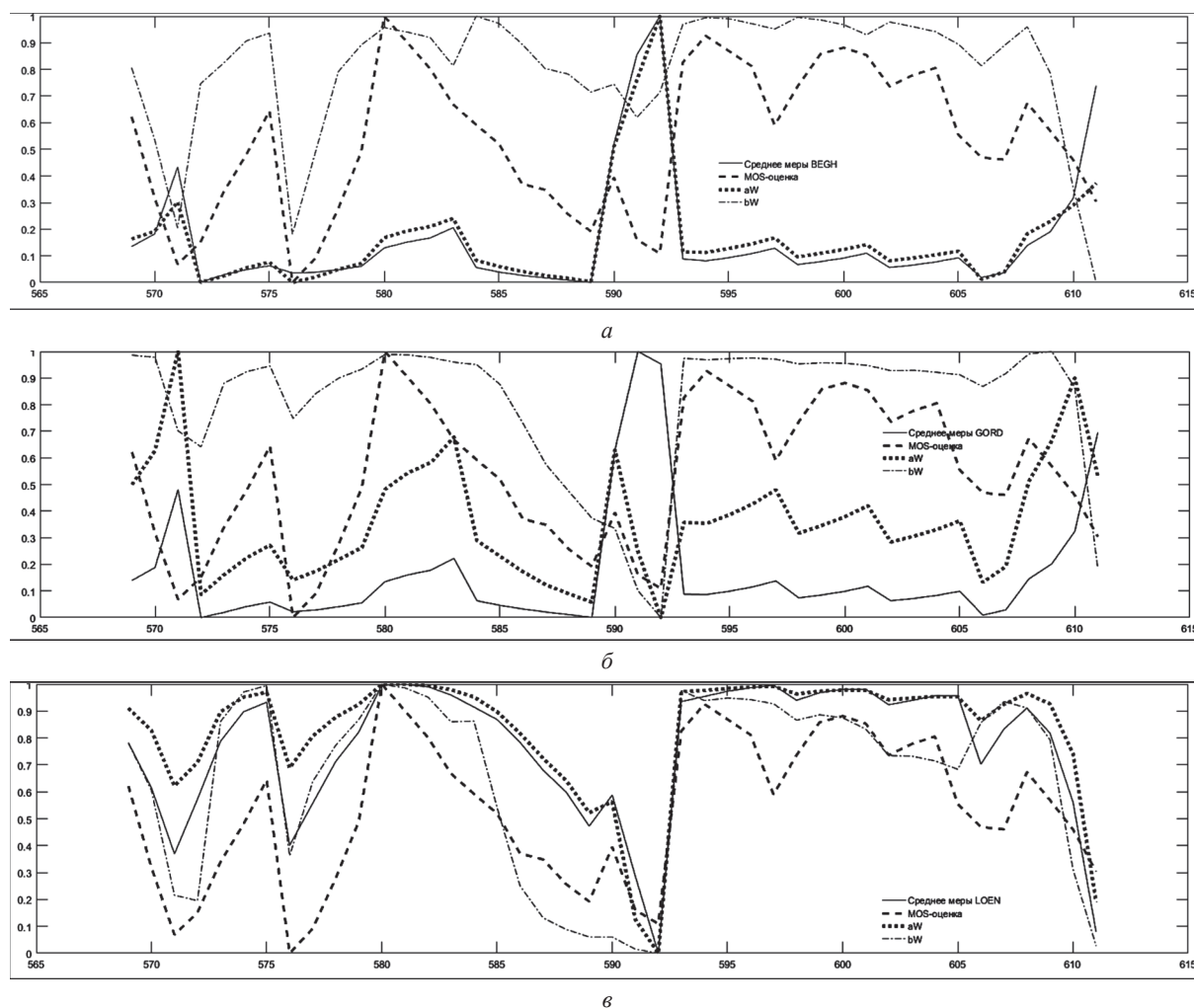


Рис. 8. Графики изменений визуальной оценки качества (MOS-оценки) и количественных мер качества: *а* – BEGH; *б* – GORD; *в* – LOEN

мер BEGH, GORD, LOEN, параметров распределения Вейбулла (aW – параметр масштаба, bW – параметр формы) и субъективных оценок (MOS) для 43 изображений вариантов изображения «Попугай» с разным контрастом.

Все оценки (MOS-оценки, BEGH, GORD, LOEN) на графиках нормализованы в диапазоне $[0, 1]$. Анализ подобных графиков показал, что субъективные оценки экспертов (MOS-оценки) больше всего коррелируют с параметром формы b распределения Вейбулла.

Заключение

В результате анализа литературных источников отобран ряд мер, позволяющих оценить контраст цифровых изображений. Они были запрограммированы и протестированы двумя

типами экспериментов на предмет способности определять лучшее значение контраста при его линейном изменении и корреляции с экспертными оценками контрастности изображений, представленных в специализированной базе изображений CCID2014. Отобраны три лучшие меры контраста цифровых изображений: BEGH, GORD, LOEN.

Экспериментально показано, что модификация известных подходов посредством использования параметра формы распределения Вейбулла вместо среднего значения локальных оценок точнее описывает контраст изображения и лучше коррелирует с визуальными оценками качества изображения.

Исследования выполнены в рамках проекта БРФФИ Ф18МС-028.

ЛИТЕРАТУРА

1. Краткий фотографический словарь. Под общей редакцией А. А. Лапури и В. И. Шеберстова. – М.: Искусство. – 1956.

2. **Артюшин Л. Ф.** Контраст фотографического изображения // Фотокинетика: Энциклопедия / Гл.ред. Е. А. Иофис. М.: Советская энциклопедия, 1981. – С. 148–150.
3. **Каценеленбоген Э. Д.** Контрастности коэффициент // Фотокинетика: Энциклопедия / Гл. ред. Е. А. Иофис. – М.: Советская энциклопедия, 1981. – С. 150.
4. **Gordon R., Rangayyan R. M.** Feature enhancement of film mammograms using fixed and adaptive neighborhoods // Applied Optics, 1984. – 23(4). – P. 560–564.
5. **Кадничанский С. А.** Оценка контраста цифровых аэрофото- и космических снимков // Геодезия и картография. – 2018. – № 3. – С. 46–51.
6. **Старовойтов В. В.** Уточнение индекса структурного сходства изображений SSIM // Информатика. – 2018. – Т. 15. – № 3. – С. 7–16.
7. **Старовойтов В. В., Старовойтов Ф. В.** Сравнительный анализ безэталонных мер оценки качества цифровых изображений // Системный анализ и прикладная информатика. – 2017. – Т. 13. – № 1. – С. 24–31.
8. **Beghdadi, A., Le Negrata, A.** Contrast enhancement technique based on local detection of edges // Computer Vision, Graphics, and Image Processing, 1989. – Vol. 46. – N. 2. – P. 162–174.
9. **Golestaneh, S. A., & Chandler, D. M.** No-reference quality assessment of JPEG images via a quality relevance map // IEEE Signal Processing Letters. – 2014. – Vol. 21. – N. 2. – P. 155–158.
10. **Matkovic K. et al.** Global Contrast Factor – a New Approach to Image Contrast // Computational Aesthetics, 2005. – P. 159–168.
11. **Gu K., Zhai G., et.al.** Subjective and objective quality assessment for images with contrast change // Proc. IEEE Int. Conf. on Image Processing, Melbourne, VIC, Australia, Sep. 2013. – P. 383–387.
12. **Kodak Lossless True Color Image Suite.** [Online]. Available: <http://r0k.us/graphics/kodak/>.

REFERENCES

1. **Kratkij fotograficheskij slovar'.** Pod obshhej redakciej A. A. Lapauri i V. I. Sheberstova. – М.: Iskustvo. – 1956.
2. **Artjushin L. F.** Kontrast fotograficheskogo izobrazhenija // Fotokinetika: Jenciklopedija / Gl. red. E. A. Iofis. – М.: Sovetskaja jenciklopedija, 1981. – S.148–150.
3. **Kacenelenbogen Je. D.** Kontrastnosti koeficient // Fotokinetika: Jenciklopedija / Gl. red. E. A. Iofis. – М.: Sovetskaja jenciklopedija, 1981. – S. 150.
4. **Gordon R., Rangayyan R. M.** Feature enhancement of film mammograms using fixed and adaptive neighborhoods // Applied Optics, 1984. – 23(4). – P. 560–564.
5. **Kadnichanskij S. A.** Ocenka kontrasta cifrovych ajerofoto- i kosmicheskikh snimkov // Geodezija i kartografija. – 2018. – № 3. – S. 46–51.
6. **Starovojtov V. V.** Utochnenie indeksa strukturnogo shodstva izobrazhenij SSIM // Informatika. – 2018. – V. 15. – № 3. – S. 7–16.
7. **Starovojtov, V. V., Starovojtov F. V.** Sravnitel'nyj analiz bezjetalonnih mer ocenki kachestva cifrovych izobrazhenij // Sistemnyj analiz i prikladnaja informatika. – 2017. – V. 13. – № 1. – S. 24–31.
8. **Beghdadi, A., Le Negrata, A.** Contrast enhancement technique based on local detection of edges // Computer Vision, Graphics, and Image Processing, 1989. – V. 46. – N. 2. – P. 162–174.
9. **Kodak Lossless True Color Image Suite.** [Online]. Available: <http://r0k.us/graphics/kodak/>.
10. **Gu K., Zhai G., et.al.** Subjective and objective quality assessment for images with contrast change // Proc. IEEE Int. Conf. on Image Processing, Melbourne, VIC, Australia, Sep. 2013. – P. 383–387.
11. **Golestaneh, S. A., Chandler, D. M.** No-reference quality assessment of JPEG images via a quality relevance map // IEEE Signal Processing Letters. – 2014. – V. 21. – N. 2. – P. 155–158.
12. **Matkovic K. et al.** Global Contrast Factor – a New Approach to Image Contrast // Computational Aesthetics, 2005. – P. 159–168.

Поступила
01.06.2019

После доработки
22.06.2019

Принята к печати
01.07.2019

GOLUB Y. I.¹, STAROVOITOV F. V.²

STUDY OF LOCAL ASSESSMENTS OF CONTRAST FOR DIGITAL IMAGES

¹United Institute of Informatics Problems of the National Academy of Sciences of Belarus,

²Belarusian National Technical University

The article study notion of the digital image contrast. Various quantitative estimates of the contrast of digital images are investigated. Comparative experimental studies of different contrast estimates were performed on two standard image data-bases. It is shown that the evaluation of contrast by calculating the arithmetic average or MSE values of a set of local estimates does not always coincide with the visual contrast assessment. Experimental results showed that the Weibull distribution shape parameter is a more accurate estimate of the set of local contrast estimates calculated by the BEGH, GORD, LOEN functions and correlates well with the visual contrast estimates.

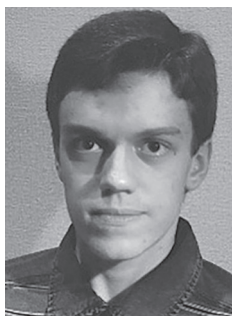


Голуб Юлия Игоревна – кандидат технических наук, доцент, старший научный сотрудник государственного научного учреждения «Объединенный институт проблем информатики Национальной академии наук Беларуси».

email: 6423506@gmail.com.

Yuliya I. Golub – PhD, Associate Professor, Senior Research Fellow at the United Institute of Informatics Problems of the National Academy of Sciences of Belarus.

Email: 6423506@gmail.com.



Старовойтов Федор Валерьевич – аспирант Белорусского национального технического университета.

Fedor V. Starovoitov is a PhD student of the Belarusian National Technical University.

УДК 004; 004.93

В. В. СТАРОВОЙТОВ

ИНДЕКС SSIM НЕ ЯВЛЯЕТСЯ МЕТРИКОЙ И ПЛОХО ОЦЕНИВАЕТ СХОДСТВО ИЗОБРАЖЕНИЙ

Объединенный институт проблем информатики НАН Беларуси

В статье исследованы некоторые свойства очень популярного показателя структурного сходства изображений, называемого индексом SSIM. Согласно сайту <https://scholar.google.com> на статью [3], где он был впервые описан, за 14 лет сделано более 20000 ссылок. Этот показатель активно используется международным сообществом в научных исследованиях. Он приобрел статус неофициального международного стандарта для оценки качества изображения при наличии эталона, часто называемого метрикой качества изображений. В настоящей статье развенчиваются некоторые мифы, возникшие вокруг этого индекса. Доказана теорема утверждающая, что индекс SSIM и любые его линейные преобразования не являются метрическими функциями. Во многих публикациях и в пакете прикладных программ Матлаб в описании функции `ssim`, сказано, что индекс SSIM используется для измерения качества изображений. Однако этот индекс, а также любая функция сравнения с эталонным изображением (типа *full-reference*) в принципе не могут оценить качество анализируемых изображений. Они оценивают только некоторую степень сходства между изображением и его искаженной копией. В статье также показано, что индекс SSIM не всегда может корректно определить сходство изображений одной и той же сцены, в то время как коэффициент линейной корреляции Пирсона делает это намного быстрее и точнее.

Ключевые слова: оценка качества изображения, индекс SSIM, коэффициент корреляции Пирсона

Введение

За последние десятилетия были разработаны сотни алгоритмов для сравнения изображений [1]. Часть из них ориентирована на оценку качества изображения (IQA). Факторы, влияющие на качество, включают в себя равномерность освещения и яркости, разрешение и геометрию, контрастность и резкость, точность цветопередачи и цветовую дискриминацию наблюдаемого изображения. Алгоритмы были разделены на три группы: полный эталонный (FR), сокращенный эталонный (RR), без эталонный (NR) или слепой [2,3]. Одной из самых популярных FR-мер является структурный индекс сходства изображений SSIM [4]. Он используется во многих приложениях и имеет множество клонов, таких как FSSIM, MS-SSIM, HWSSIM, PSSIM, CW-SSIM и других [5,6]. Все они оценивают яркость, контраст и структуру двух сравниваемых изображений в наборе соответствующих окон. На последнем этапе среднее арифметическое локальных оценок принимается как глобальное значение показателя качества изображения на основе SSIM.

Индекс SSIM был разработан как улучшение традиционных методов оценки сигналов, таких как среднеквадратическая ошибка (MSE) и отношение сигнал / шум (PSNR). Статья [4], где был введен индекс SSIM, цитировалась более 22000 раз, согласно Google Scholar. В работе [7] авторы описали результаты статистического исследования этого индекса. В статье [8] показано, что локальные оценки индекса SSIM имеют четкую аналитическую зависимость с локальными среднеквадратичными оценками MSE. В [9] приведена аналитическая зависимость пикового отношения сигнала к шуму (PSNR) и индекса SSIM. Там же экспериментально показана близость этих оценок в случае сравнения эталонных изображений с их копиями, подвергнутыми гауссовому размытию, сжатию алгоритмами JPEG и JPEG2000. В работе [10] аналитически и экспериментально показано, что для медицинских изображений с фрагментами больших или малых значений средней яркости локальные SSIM-оценки не стабильны, это особенно заметно при сжатии изображений алгоритмом JPEG2000. Тем не ме-

нее, во многих исследованиях индекс SSIM используется как неофициальный стандарт для оценки качества искаженного изображения при наличии эталонного изображения и его часто называют метрикой качества изображений.

Настоящая статья продолжает исследования индекса SSIM, начатые в работе [11].

Определение индекса структурного сходства

Индекс основан на локальных оценках $ssim$ между двумя окнами x и y размером $N \times N$ пикселей, рассчитанных вокруг соответствующих пикселей на изображениях A и B согласно формуле [4]:

$$ssim(x, y) = \frac{(2\mu_x\mu_y + \tilde{n}_1)(2\sigma_{xy} + \tilde{n}_2)}{(\mu_x^2 + \mu_y^2 + \tilde{n}_1)(\sigma_x^2 + \sigma_y^2 + \tilde{n}_2)}, \quad (1)$$

где μ_x – среднее значение в окне x ; μ_y – среднее значение в окне y ; σ_x^2 – дисперсия в окне x ; σ_y^2 – дисперсия в окне y ; σ_{xy} – ковариация окон x и y ; константы $c_1 = (k_1L)^2$ и $c_2 = (k_2L)^2$, $L = 255$, определяют динамический диапазон яркости; $k_1 = 0,01$, $k_2 = 0,03$ – экспериментально определенные константы.

Глобальный индекс SSIM для изображений A и B рассчитывается как среднее арифметическое локальных оценок по формуле:

$$SSIM(A, B) = \frac{1}{M} \sum_{x,y} ssim(x, y), \quad (2)$$

где A и B – два изображения одинакового размера, M – количество окон.

Каждая локальная оценка $ssim(x, y)$ рассчитывается в окрестности пикселя с координатами (x, y) для каждого пикселя. Значения индекса SSIM лежат в диапазоне от -1 до $+1$. Значение 1 достигается, когда сравниваемые изображения полностью идентичны.

Индекс SSIM не может оценить качество изображения: если взять изображение очень низкого качества в качестве эталонного и сравнить его с самим собой, тогда получим $SSIM = 1$. Это означает наилучшее качество исследуемого изображения. Если сравнить некачественное изображение с его слегка искаженной копией, оценка будет близка к единице. Полученные максимальные оценки не являются корректными оценками качества изображений, то есть индекс SSIM не оценивает качество изображений, а только их сходство.

Является ли SSIM метрической функцией?

В литературе индекс SSIM часто называют метрикой, но он является метрикой в математическом смысле. Более того, можно доказать следующую теорему.

Теорема 1. Любая функция, полученная линейным преобразованием индекса SSIM, не является метрикой.

Доказательство. Функция f является метрикой, если для нее выполняются четыре аксиомы:

- 1) $f(x, y) \geq 0$,
- 2) $f(x, y) = 0$ iff $x = y$,
- 3) $f(x, y) = f(y, x)$,
- 4) $f(x, z) \leq f(x, y) + f(y, z)$.

Линейное преобразование функции SSIM может быть описано следующим образом:

$$\text{NewSSIM} = \alpha \text{ SSIM} + \beta,$$

где α и β – константы.

Из второй аксиомы и определения индекса SSIM получаем $\max(SSIM) = 1$, откуда следует $\alpha + \beta = 0$ или $\alpha = -\beta$. Это определяет единственный вариант линейного преобразования индекса SSIM в функцию, которая потенциально может быть метрикой (первые три аксиомы выполняются):

$$\text{NewSSIM} = -\beta \text{ SSIM} + \beta,$$

или

$$\text{NewSSIM} = \beta(1 - \text{SSIM}), \quad (3)$$

где $\beta > 0$ соответственно первой аксиоме и $\min(SSIM) = -1$.

Выполнение третьей аксиомы для функции NewSSIM следует из формул (1–2). Следовательно, первые три метрических аксиомы верны как для индекса SSIM, так и для функции NewSSIM.

Что можно сказать о выполнении четвертой аксиомы? Рассмотрим очень похожие изображения одной и той же сцены из базы данных TID2013 [12]. Возьмем изображение $A = \text{'Im01-01-1'}$, изображение B равное A с одним измененным значением пикселя (вместо $A(1, 1, 1) = 73$ используем $B(1, 1, 1) = 74$) и построим изображение $C = (A + A_2) / 2$, где $A_2 = \text{'Im11-01-2'}$ – изображение из той же базы данных.

Для этих изображений должно выполняться следующее неравенство:

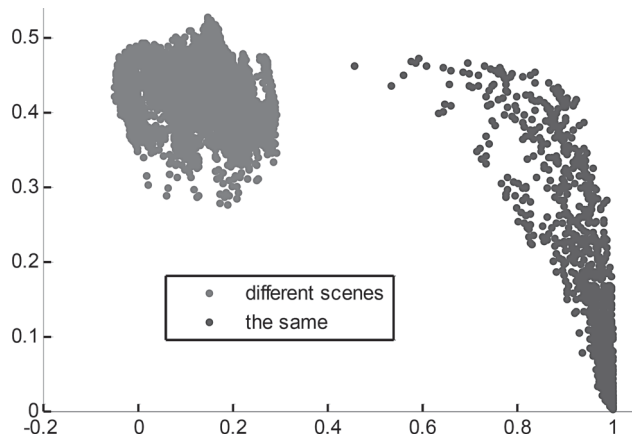
Рис. 1. Изображения A , B и C , использованные в доказательстве теоремы

Рис. 2. Сравнение значений меры NewSSIM и коэффициентов корреляции Пирсона для изображений разных сцен (облако слева) и одинаковых сцен (синие точки справа)

$$\text{NewSSIM}(A, C) \leq \text{NewSSIM}(A, B) + \text{NewSSIM}(B, C)$$

или

$$(1 - \text{SSIM}(A, C)) \leq (1 - \text{SSIM}(A, B)) + (1 - \text{SSIM}(B, C))$$

или

$$-\text{SSIM}(A, C) \leq 1 - \text{SSIM}(A, B) - \text{SSIM}(B, C). \quad (4)$$

Вычислив три значения индекса SSIM для изображений, описанных в уравнении (4), имеем

$$\begin{aligned} -0,97211954683029 &\leq \\ 1 - 0,999999989608151 - 0,972119652499616 &= \\ -0,972119642107767. \end{aligned}$$

Таким образом неравенство треугольника не выполняется для данных изображений. Этот контрпример доказывает **Теорему 1**.

Коэффициенты линейной корреляции Пирсона для пар изображений (A, B) , (A, C) , (B, C) равны 0,9999999994973, 0,9928707064627, 0,9928707094216, соответственно. Можно отметить, что коэффициенты корреляции немного выше, чем соответствующие значения индексов SSIM.

Корреляция или индекс SSIM – что лучше для оценки сходства изображений?

Мы исследовали какой параметр (линейной корреляции Пирсона или индекс SSIM) точнее оценивает сходство изображений. Для экспериментов использовали изображения из двух общедоступных баз данных TID2013 [12] и CCID2014 [13]. Использовался ПК с процессорами Intel(R), Core(TM), процессором i5-4440 с тактовой частотой 3,10 ГГц и 8,00 ГБ Ram, а также пакет Matlab 2014a. Сравнивались два набора из нескольких тысяч пар изображений одинаковых сцен и разных. Для них вычислялись значения индексов SIM и NewSSIM с параметром $\beta = 1$ в уравнении (3), а также коэффициенты корреляции Пирсона. Использовались стандартные функции Matlab corr и ssim.

Из рис. 2 видно, что диапазон значений меры NewSSIM (вертикальная ось) для пар изображений одинаковых сцен пересекается с диапазоном значений NewSSIM, вычисленных для изображений разных сцен. Используя эту меру, невозможно корректно определить сходство анализируемых изображений. Однако, используя коэффициент корреляции (горизонтальная ось), это легко сделать с помощью

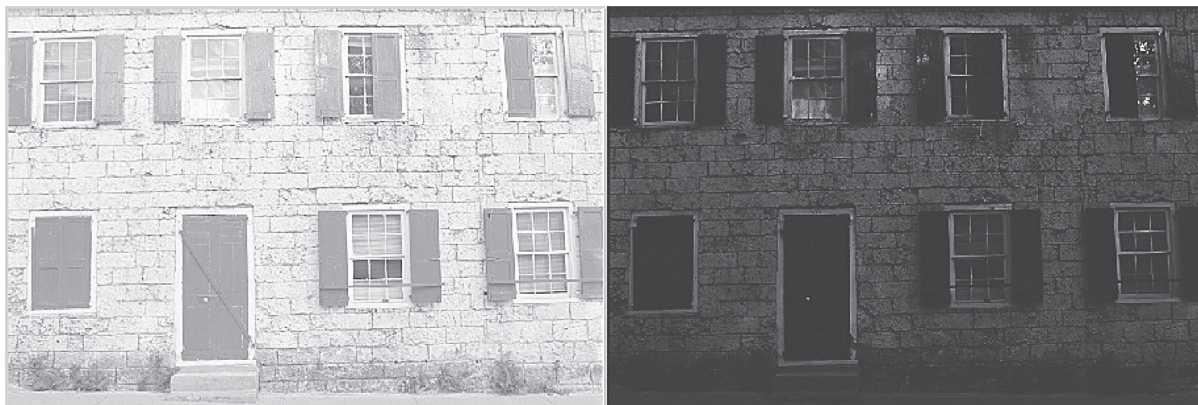


Рис. 3. Изображения img005 (слева) и img045 (справа) из базы данных CCID2014 с характеристиками: SSIM = 0,1754, NewSSIM = 0,4123 и corr = 0,7417



Рис. 4. Изображения img177 (слева) и img187 (справа) из базы данных CCID2014 с характеристиками: SSIM = 0,3886, NewSSIM = 0,3057 и corr = 0,1472

глобального порога в 0,4. Примеры сравнения изображений одной сцены и разных сцен приведены на рис. 3, 4. На рис. 3 приведен пример сравнения двух разноконтрастных изображения одной сцены. Значение индекса SSIM равно $SSIM = 0,1754$, а коэффициента корреляции равно 0,7417. На рис. 4 сравниваются два светлых изображения разных сцен. В этом случае значение индекса SSIM равно 0,3886, а коэффициента корреляции равно 0,1472. Во втором примере значение индекса SSIM гораздо ближе к единице, что означает большее сходство сравниваемых изображений, что не верно. При этом коэффициент корреляции гораздо корректнее оценивает сходство данных изображений.

Можно сделать вывод, что индексы NewSSIM и SSIM могут правильно распознавать только визуально очень близкие изображения и применимы только для оценки сходства изображений одной и той же сцены.

Для цветных изображений из базы данных TID2013 размером 768×512 пикселей истекшее время вычисления корреляции равнялось

0,030 с в Matlab (версия R2014). Время вычисления индекса SSIM на нашем компьютере составило 3,81 с, то есть примерно в 125 раз дольше.

Заключение

В статье исследованы некоторые свойства популярного индекса структурного подобия изображений под названием SSIM. В англоязычной научной литературе он считается неофициальным стандартом для оценки качества изображений при наличии эталона и часто называется метрикой качества. В данной статье продемонстрировано, что 1) индекс SSIM не может точно оценить качество изображения, а только сходство двух изображений; 2) он не является метрической функцией; 3) он не всегда правильно оценивает сходство изображенных сцен, однако коэффициент корреляции Пирсона делает это точнее и быстрее.

Работа частично выполнена в рамках проекта БРФФИ Ф18МС-028.

REFERENCES

1. Pedersen, M., Hardeberg, J. Y. Full-reference image quality metrics: Classification and evaluation // Foundations and Trends® in Computer Graphics and Vision, 2012), V. 7, № 1. – pp. 1–80.
2. Lin W., Kuo C. C. J. Perceptual visual quality metrics: A survey // Journal of Visual Communication and Image Representation. – 2011. – Т. 22. – №. 4. – pp. 297–312.
3. Wang, Z., Bovik, A. C. Modern image quality assessment // Synthesis Lectures on Image, Video, and Multimedia Processing, 2006, V. 2. – № 1. – pp. 1–156.
4. Wang, Z., Bovik, A. C., Sheikh, H. R., and Simoncelli, E. P. Image quality assessment: from error visibility to structural similarity // IEEE Trans. Image Processing, 2004, V. 13. – № 4. – pp. 600–612.
5. Chandler, D. M. Seven Challenges in Image Quality Assessment: Past, Present, and Future Research', ISRN Signal Processing, 2013, V. 2013. – C. 1–53.
6. Renieblas G. P. et al. Structural similarity index family for image quality assessment in radiological images // Journal of Medical Imaging. – 2017. – Т. 4. – №. 3. – C. 035501.
7. Sheikh H. R., Sabir M. F., Bovik A. C. A statistical evaluation of recent full reference image quality assessment algorithms // IEEE Transactions on image processing. – 2006. – Т. 15. – №. 11. – pp. 3440–3451.
8. Dosselmann R., Yang X. D. A comprehensive assessment of the structural similarity index // Signal, Image and Video Processing. – 2011. – Т. 5. – №. 1. – pp. 81–91.
9. Hore A., Ziou D. Image quality metrics: PSNR vs. SSIM // Proc. Of the 20-th Int. Conf. on Pattern Recognition, 2010. – pp. 2366–2369.
10. Pambrun J. F., Noumeir R. Limitations of the SSIM quality metric in the context of diagnostic imaging // Proc. of the IEEE International Conference on Image Processing, 2015. – pp. 2960–2963.
11. Старовойтов В. В. Уточнение индекса SSIM структурного сходства изображений // Информатика. – 2018. – Т. 15. – №. 3. – С. 41–55.
12. Ponomarenko, N, Jin, L, Ieremeiev, O, Lukin, et.al. Image database TID2013: Peculiarities, results and perspectives // Signal Processing: Image Communication, V. 30. C. 57–77.
13. Gu, K., Zhai, G., Lin, W., Liu, M. The analysis of image contrast: From quality assessment to automatic enhancement' // IEEE Transaction on Cybernetics, 2016. – V. 46. – № 1. – C. 284–297.

Поступила
04.04.2019

После доработки
20.06.2019

Принята к печати
01.07.2019

STAROVOITOV V. V.

THE SSIM INDEX IS NOT A METRIC AND IT IS BADLY EVALUATE THE SIMILITY OF IMAGES

The article explored some properties of a very popular feature of image structural similarity, called the SSIM index. According to <https://scholar.google.com>, the article [3], where it was first described, has made more than 20,800 citations during the last 14 years. This indicator is actively used by the scientific community in imaging research. It acquired the status of an unofficial international standard for assessing image quality in the presence of a template, often referred to as the image quality metric. This article debunks some of the myths that have arisen around this index. A theorem is proved which states that the SSIM index and any of its linear transformations are not metric functions. In many publications and in the Matlab application software package in the description of the ssim function, it is said that the SSIM index is used to measure the image quality. However, this index, as well as any comparison function with a reference image (such as full-reference), in principle, cannot assess the quality of the analyzed images. They estimate only a certain degree of similarity between the template image and its distorted copy. The article also shows that the SSIM index cannot always correctly determine the similarity of images of the same scene, while the Pearson linear correlation coefficient makes it much faster and more accurate.

Keywords. image quality assessment, the SSIM index, Pearson's correlation coefficient.



Старовойтов Валерий Васильевич, доктор технических наук, профессор. Главный научный сотрудник ОИПИ НАН Беларуси. Лауреат премии Ленинского комсомола БССР (1990 г.) и Государственной премии Республики Беларусь (2003 г.). Сфера научных интересов: обработка и анализ цифровых изображений, полученных в разных участках электромагнитного спектра.

Starovoitov Valery, Doctor of Sciences and professor of computer science. He is a Principal research fellow at the United Institute of Informatics Problems, National Academy of Sciences of Belarus (UIIP NAN Belarus). Awards: the Belarus Lenin Komsomol Prize and the State Prize of the Republic of Belarus in science. Research interests of professor Starovoitov are processing and analysis of digital images obtained in different parts of the electromagnetic spectrum.

**УПРАВЛЕНИЕ
ТЕХНИЧЕСКИМИ
ОБЪЕКТАМИ**

**MANAGEMENT OF
TECHNICAL OBJECTS**

УДК 621.372.512

Б. А. ЛЯХ, В. А. КОНДРАТЕНКО, Д. В. МОРОЗОВ

СТРУКТУРА МАТЕМАТИЧЕСКОЙ МОДЕЛИ МНОГОПОЗИЦИОННОЙ СИСТЕМЫ РАДИОМОНИТОРИНГА СИГНАЛОВ КОРОТКОВОЛНОВОГО ДИАПАЗОНА

Военная академия Республики Беларусь

Рассмотрена математическая модель многопозиционной системы радиомониторинга коротковолнового диапазона, позволяющая провести оценку эффективности функционирования многопозиционной системы радиомониторинга сигналов коротковолнового диапазона в неблагоприятных условиях воздействия внешних помех.

Введение

В настоящее время одной из основных задач радиоэлектронной разведки является получение семантической информации путем обработки сообщений, передаваемых по каналам связи КВ-диапазона. Однако использование современных средств радиомониторинга позволяет обрабатывать в среднем только 80–90% перехватываемых сообщений от их общего количества, что обусловлено следующими основными причинами:

1. Для организации радиосвязи в армиях иностранных государств используются адаптивные системы связи КВ-диапазона, которые характеризуются автоматизацией процессов установления радиосвязи и гарантированной передачей информации, адаптивностью к динамичной помеховой обстановке в КВ-диапазоне, возможностью организации аналоговых и цифровых сетей связи.

2. Радиоперехват и обработка сигналов КВ-диапазона осуществляется в одной точке приема, где принимаемый сигнал может быть сильно искажен, что связано со спецификой распространения радиоволн в КВ-диапазоне.

Таким образом, комплексная оптимизация средств радиомониторинга сигналов КВ-диапазона в условиях многолучевого распространения радиоволн и сложной помеховой обстановки на основе применения методики последетекторной обработки при разнесенном приеме средствами радиоперехвата является актуальной научно-технической задачей.

Её решение обеспечит возможность существенного повышения эффективности функционирования системы радиомониторинга сигналов КВ-диапазона, что особенно важно для решения задач обеспечения военной безопасности Республики Беларусь.

Математическое моделирование многопозиционной системы радиомониторинга сигналов коротковолнового диапазона

Многопозиционная система сигналов КВ-диапазона относится к классу больших систем, этапы проектирования, внедрения, эксплуатации и эволюции которой в настоящее время невозможны без использования различных видов моделирования. На всех перечисленных этапах для различных уровней обработки радиосигналов в многопозиционной системе радиомониторинга КВ-диапазона необходимо учитывать следующие особенности: сложность структуры и стохастичность связей между элементами, неоднозначность алгоритмов поведения при различных условиях, большое количество параметров и переменных, неполноту и недетерминированность исходной информации, разнообразие и вероятностный характер воздействий внешней среды и т. д. [1]. Ограниченность возможностей проведения натурных экспериментов для исследования тех или иных процессов функционирования многопозиционной системы радиомониторинга делает актуальной разработку математической модели,

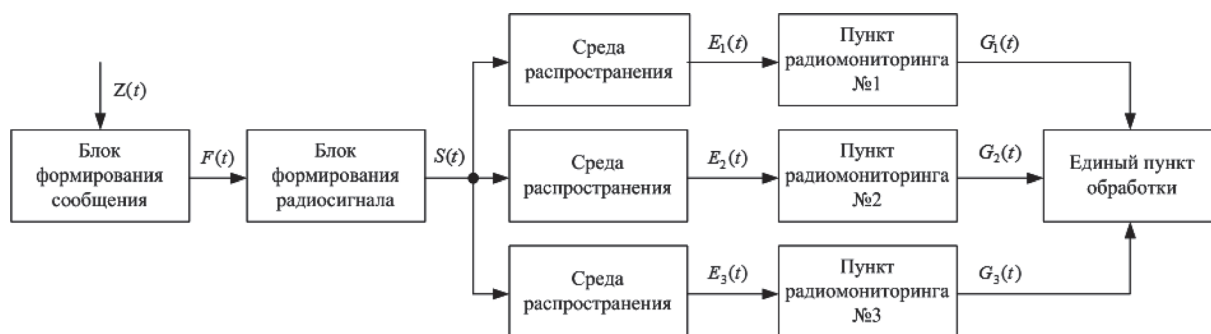


Рис. 1. Структурная схема математической модели многопозиционной системы радиомониторинга коротковолнового диапазона

которая позволит в соответствующей форме представить процессы функционирования многопозиционной системы радиомониторинга, оценить ее эффективность в различных условиях обстановки [2].

На рис. 1 приведена структурная схема математической модели многопозиционной системы радиомониторинга сигналов КВ-диапазона.

Приведенная структурная схема позволяет разработать математическую модель многопозиционной системы радиомониторинга и по результатам моделирования оценить взаимосвязь различных объектов (модулей) системы, провести выборку входных параметров, исследовать вопросы управления и дает возможность выделить те параметры, значения которых подлежат корректировке [3].

Каждый элемент (блок) вышеуказанной структурной схемы системы радиомониторинга является самостоятельной математической моделью. Так, в блоке формирования сообщения осуществляется формирование (моделирование) исходного сообщения по определенному правилу (закону), при котором передаваемая информация $Z(t)$ (текст, звук, изображение и т. д.) преобразовываются в последовательность кодовых символов [4].

На примере стандарта Mil-Std-188-141B (App. C), который активно используется при организации связи в силовых структурах ЕС, производится моделирование относительного восьми позиционного фазоманипулированного сигнала $S(t)$ (далее – ОФМ-8).

Сигнал $S(t)$, на выходе блока формирования радиосигнала можно записать в виде:

$$S(t) = U_0 \cos(\omega_0 t + \Delta\varphi_k + \Delta\varphi_{k-1}), \quad (1)$$

где $U_0(t)$ – амплитуда сигнала; $\omega_0 = 2\pi f_0$ – круговая частота радиосигнала, где f_0 – ча-

стота несущего колебания; $k = 0, 1, 2, \dots$ – отсчеты сигнала; $\Delta\varphi_{k-1}$ – значение фазы предшествующего радиоимпульса; $\Delta\varphi_k$ – фаза текущего выходного символа, (значение фазы выбирается в соответствии с таблицей).

Соответствие состояний символов и фаз выходного сигнала

Значение трибита	Символ в битовом выражении	Фаза выходного сигнала
1	000	0
2	001	$\pi/4$
3	011	$\pi/2$
4	010	$3\pi/4$
5	110	π
6	111	$5\pi/4$
7	101	$3\pi/2$
8	100	$7\pi/4$

В результате моделирования на выходе блока формирования радиосигнала генерируется радиосигнал, пригодный для передачи по каналам радиосвязи в КВ-диапазоне. Спектр полученного сигнала, и его амплитудно-фазовая диаграмма приведены на рис. 2.

Так как в состав предлагаемой многопозиционной системы радиомониторинга входят три разнесенных в пространстве пункта радиоприема, поэтому на данном этапе производится моделирование трех различных путей распространения сигнала $S(t)$. Таким образом, на вход каждого из трех пунктов поступит соответствующий радиосигнал $E_1(t)$, $E_2(t)$ и $E_3(t)$, отличающиеся от сформированного $S(t)$ приобретенными в процессе распространения и приема искажениями.

Так, поступающие на входы пунктов радиомониторинга сигналы можно представить в виде:

$$E_1(t) = (S(t) + \zeta_1(t)) * n_1(t), \quad (2)$$

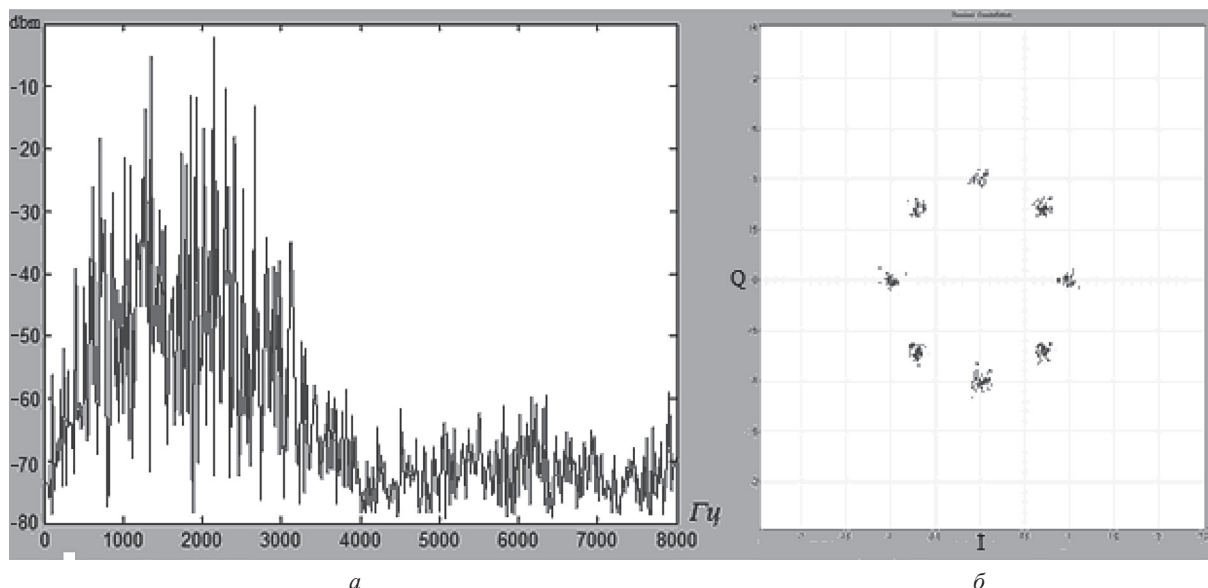


Рис. 2. *a* – спектр формируемого сигнала ОФМ-8; *б* – Амплитудно-фазовая диаграмма формируемого сигнала ОФМ-8

$$E_2(t) = (S(t) + \zeta_2(t)) * n_2(t), \quad (3)$$

$$E_3(t) = (S(t) + \zeta_3(t)) * n_3(t), \quad (4)$$

где $\zeta_1(t)$, $\zeta_2(t)$, $\zeta_3(t)$ – аддитивные помехи, возникающие в приемном тракте первого, второго и третьего пункта радиомониторинга; $n_1(t)$, $n_2(t)$, $n_3(t)$ – мультипликативные помехи, которые воздействуют на сигнал в процессе распространения в пространстве от источника излучения к каждому из пунктов радиомониторинга.

Принятые радиосигналы подвергаются обработке: фильтрации, демодуляции и декодированию в соответствии с протоколом Mil-Std-188–141B (App. C). В случае успешной обработки на выходе каждого из пунктов системы будут получены сообщения $G_1(t)$, $G_2(t)$ и $G_3(t)$ которые должны соответствовать сформированному на начальном этапе моделирования исходному сообщению $Z(t)$.

Однако отмечаются случаи, когда на выходе каждого из трех пунктов радиомониторинга сообщения $G_1(t)$, $G_2(t)$ и $G_3(t)$, отличаются между собой и не соответствуют исходному $Z(t)$. Такая ситуация, чаще всего, возникает при длительном сеансе связи, около 5–10 минут, в течение которого исходное сообщение $Z(t)$ разбивается на множество пакетов, каждый из которых передается отдельно, а на приемной стороне происходит их объединение. В случае ошибочного приема в пунктах радиомониторинга хотя бы одного пакета из множе-

ства пакетов разделенного сообщения $Z(t)$ восстановить переданную информацию не представляется возможным.

В связи с тем, что вероятность того, что в единый момент времени три радиосигнала претерпят одинаковые изменения при распространении в пространстве равна нулю, то для устранения вышеизложенной проблемы авторы предлагают осуществлять совместную обработку в едином пункте, путем объединения результатов демодуляции копий одного и того же сигнала, принятых в каждом из разнесенных в пространстве приемных пунктах. Использование метода автовыбора ветви разнесения и линейного сложения символов, полученных после их демодуляции, позволит повысить достоверность декодирования в несколько раз, по сравнению с существующими системами аналогичного назначения.

Заключение

Представленная модель многопозиционной системы радиомониторинга КВ-диапазона позволяет повысить вероятность получения семантической информации на выходе устройства декодирования.

Целями дальнейших исследований являются: разработка программного обеспечения восстановления исходного сообщения путем объединения результатов демодуляции сигналов, принятых в каждом из разнесенных в пространстве приемных пунктов многопозицион-

ной системы радиомониторинга КВ-диапазона; внедрение предложенной методики восстановления исходного сообщения в существующую

однопозиционную систему радиомониторинга КВ-диапазона без существенных материальных затрат.

ЛИТЕРАТУРА

1. Головин О. В., Простов С. П. Системы и устройства коротковолновой радиосвязи / Под ред. профессора О. В. Головина. – М.: Горячая линия – Телеком, 2006, 598 с.
2. Советов Б. Я., Яковлев С. А. Моделирование систем: Учеб. для вузов. – 3-е изд., перераб. и доп. – М.: Высш. шк., 2001, 343 с.
3. Бусленко Н. П. Моделирование сложных систем. – М.: Наука, 1968, 356 с.
4. Радзиевский В. Г., Сирота А. А. Теоретические основы радиоэлектронной разведки. 2-е изд., испр. и доп. – М.: Радиотехника, 2004, 432 с.

REFERENCES

1. Golovin O. V., Prostov S. P. Sistemy i ustrojstva korotkovolnovoj radiosvjazi / Pod red. professora O. V. Golovina. – M.: Gorjachaja linija – Telekom, 2006, 598 s.
2. Sovetov B. Ja., Jakovlev S. A. Modelirovanie sistem: Ucheb. dlja vuzov. – 3-e izd., pererab. i dop. – M.: Vyssh. shk., 2001, 343 s.
3. Buslenko N. P. Modelirovanie slozhnyh sistem. – M.: Nauka, 1968, 356 s.
4. Radzievskij V. G., Sirota A. A. Teoreticheskie osnovy radioelektronnoj razvedki. 2-e izd., ispr. i dop. – M.: Radiotekhnika, 2004, 432 s.

Поступила
01.04.2019

После доработки
19.06.2019

Принята к печати
01.07.2019

LIAKH B. A., KONDRATYONOK V. A., MOROZOV D. V.

MODELLING OF RADIO MONITORING SYSTEM OF SHORT-WAVE RADIO COMMUNICATION ADAPTIVE SYSTEMS

The structure of model which allows to spend an estimation of system functioning efficiency of radio monitoring system of short-wave radio communication adaptive systems in adverse conditions of influence of external jams is described.

Лях Борис Александрович, начальник научно-исследовательской лаборатории кафедры автоматизации, радиолокации и приемопередающих устройств учреждения образования «Военная академия Республики Беларусь» конт. тел. 8 (029) 681 33 10

Кондратёнок Василий Анатольевич канд. тех. наук, доцент, заместитель директора по научной работе ОАО «КБ РАДАР» конт. тел. 8 (029) 569 10 11

Морозов Дмитрий Васильевич канд. тех. наук, доцент, начальник кафедры информационно-вычислительных систем учреждения образования «Военная академия Республики Беларусь» конт. тел. 8 (029) 514 58 62

УДК 629.735–519

В. А. МАЛКИН¹, И. В. РОЖКОВ², А. А. САНЬКО²

ВЛИЯНИЕ ВЕТРОВЫХ ВОЗМУЩЕНИЙ И НЕЛИНЕЙНОСТЕЙ СЕРВОПРИВОДА НА КОНТУР СТАБИЛИЗАЦИИ ВЫСОТЫ ПОЛЕТА БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

¹ Учреждение образования «Военная академия Республики Беларусь»² Учреждение образования «Белорусская государственная академия авиации»

В статье рассматривается математическая модель ветра с учетом его стохастической составляющей и ветра устойчивого направления, представлены результаты сравнительного анализа влияния параметров ветра на суммарный вектор скорости ветра, действующего на беспилотный летательный аппарат (БЛА). Рассмотрены основные нелинейности элементов сервопривода автопилота и их влияние на выходной сигнал. Рассмотрена реакция контура стабилизации высоты полета БЛА на ветер с учетом нелинейностей элементов сервопривода. Доказана необходимость учета ветра при синтезе систем автоматического управления (САУ) и контуров угловой стабилизации БЛА на этапах, где скорости полета БЛА меньше 30 м/с.

Ключевые слова: ветер; беспилотный летательный аппарат; математическая модель ветра; математическая модель сервопривода, нелинейности сервопривода.

Введение

Задача синтеза САУ БЛА характеризуется сложностью их математических моделей и наличием существенных ограничений и возмущений. К основным ограничениям можно отнести ограничения, обусловленные нелинейностью элементов сервоприводов, входящих в состав автопилота и ветровыми возмущениями, действующими на БЛА. Вопросам разработки робастных САУ БЛА посвящено ряд работ [1–3]. В данных работах рассматривался синтез робастного автопилота, который является универсальным для любых планеров БЛА с весом от 0,5 кг до 50 кг. В данных работах исследовались изменения выходных сигналов автопилота БЛА с учетом вариации его коэффициентов передачи под воздействием внутренних возмущений. Влияние ветровых возмущений, а так же нелинейностей элементов сервопривода на работу контура автопилота БЛА применительно к метеорологическим условиям Республики Беларусь не рассматривалось.

Постановка задачи исследования

В данной работе предлагается разработать математическую модель ветра с учетом его

стохастической составляющей и ветра устойчивого направления применительно к особенностям атмосферы территории Республики Беларусь; разработать нелинейную математическую модель сервопривода БЛА; исследовать степень влияния ветра и нелинейностей элементов сервопривода на контур автопилота БЛА по высоте полета.

Решение задачи

Суммарный вектор скорости ветра, действующий на БЛА может быть выражен, как [4]:

$$V_w = V_{ws} + V_{wg}, \quad (1)$$

где V_{ws} – постоянный вектор, который представляет собой ветер устойчивого направления (обычно определяется в инерциальной системе координат – ИСК); V_{wg} – стохастический процесс, который представляет собой воздушные порывы и другие атмосферные возмущения (стохастическая компонента ветра определяется в связанной системе координат – ССК).

Значение V_{ws} для БЛА, можно вычислить, как [5]:

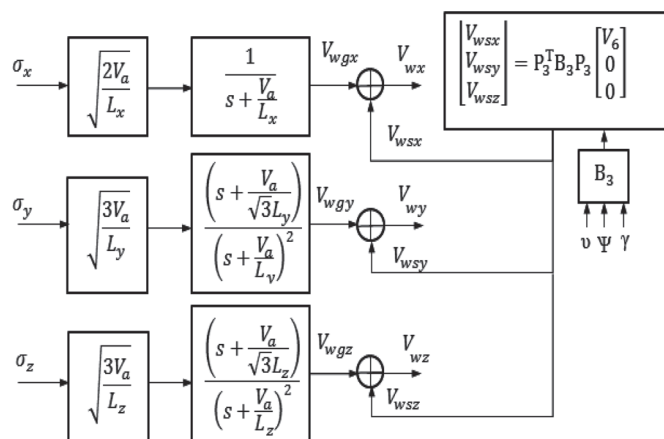


Рис. 1. Функциональная модель расчета ветра, действующего на БЛА в ССК

$$V_{ws} = V_6 \frac{\ln\left(\frac{h}{Z_0}\right)}{\ln\left(\frac{6}{Z_0}\right)}, 1 \text{ м} < h < 300 \text{ м}, \quad (2)$$

где V_6 – среднегодовая скорость ветра на высоте 6 метров для заданного участка местности; h – текущая высота полета БЛА; Z_0 – коэффициент (для указанных высот выбирается 0,15). Например, для Республики Беларусь – $V_6 \approx 2,1$ м/с [6].

Результаты экспериментальных исследований показали, что адекватной моделью порывистой части ветра является случайный процесс, характеризуемый спектральной функцией турбулентности фон Кармана [4]. Для простоты вычисления модели фон Кармана целесообразно использовать передаточные функции Драйдена:

$$\begin{aligned} H_x(s) &= \sigma_x \sqrt{\frac{2V_a}{L_x}} \frac{1}{s + \frac{V_a}{L_x}}, \\ H_y(s) &= \sigma_y \sqrt{\frac{3V_a}{L_y}} \frac{\left(s + \frac{V_a}{\sqrt{3}L_y}\right)}{\left(s + \frac{V_a}{L_y}\right)^2}, \\ H_z(s) &= \sigma_z \sqrt{\frac{3V_a}{L_z}} \frac{\left(s + \frac{V_a}{\sqrt{3}L_z}\right)}{\left(s + \frac{V_a}{L_z}\right)^2}. \end{aligned} \quad (3)$$

где $\sigma_x, \sigma_y, \sigma_z$ – интенсивности турбулентности вдоль осей ССК БЛА; L_x, L_y, L_z – простран-

ственные длины волн (масштаб турбулентности); V_a – воздушная скорость БЛА, без учета величины ветра устойчивого направления.

Параметры для модели порывов ветра (1) определены в MIL-F-8785C [4]. Подходящие параметры в случае малых и средних высот, слабой и умеренной турбулентности представлены в таблице [4, 7].

Параметры модели порыва ветра Драйдена

Описание порыва ветра	h , м	L_x, L_z , м	L_y , м	σ_x, σ_z , м	σ_y , м
Слабая турбулентность	50	200	50	1,06	0,7
Умеренная турбулентность	50	200	50	2,12	1,4
Слабая турбулентность	600	533	533	1,5	1,5
Умеренная турбулентность	600	533	533	3	3

На рис. 1 представлена функциональная модель расчета значений скорости ветра, действующего на БЛА в ССК: B_3 – универсальная матрица направляющих косинусов, предназначенная для преобразования ИСК в ССК; P_3 – перестановочная матрица [8].

Функциональная модель расчета ветра была реализована в среде виртуального моделирования MATLAB. При проведении моделирования были приняты следующие допущения: направление ветра устойчивого направления совпадает с направлением полета БЛА; не учитывались: неровности местности; наличие ветра типа «ножницы». Результаты моделирования представлены на рис. 2–4.

Как видно из рис. 2–3, стохастическая компонента турбулентности ветра, существенно выше значений ветра устойчивого направления, действующего на БЛА. Причем, самое большое отношение V_{wg}/V_{ws} имеет компонента ветра, действующая на БЛА в вертикальном

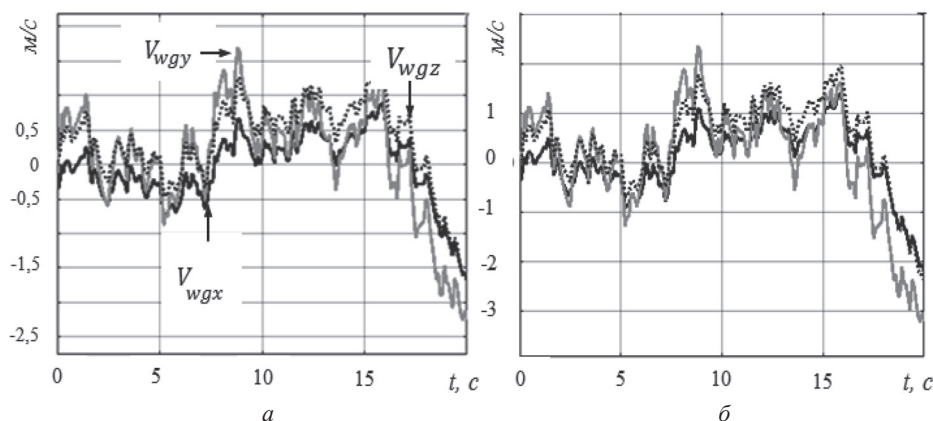


Рис. 2. Результаты моделирования значений стохастической компоненты ветра действующего на БЛА в ССК ($V_a = 15$ м/с, $H = 50$ м): а – при слабой турбулентности; б – при умеренной турбулентности

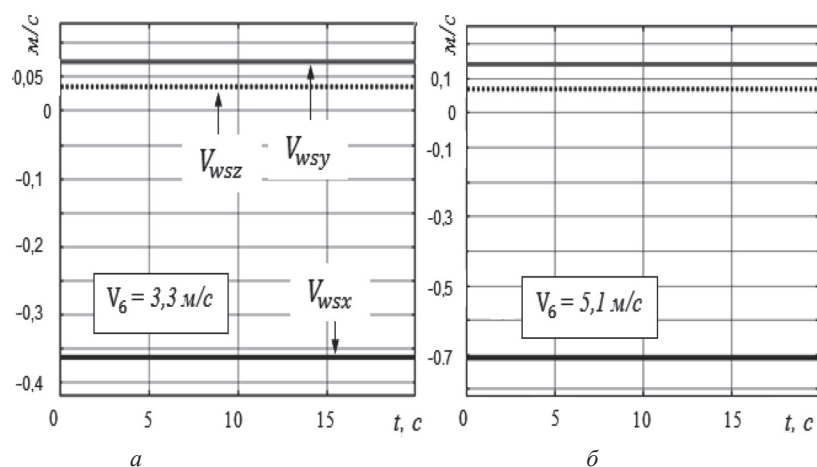


Рис. 3. Результаты моделирования ветра устойчивого направления действующего на БЛА ($V_a = 15$ м/с)

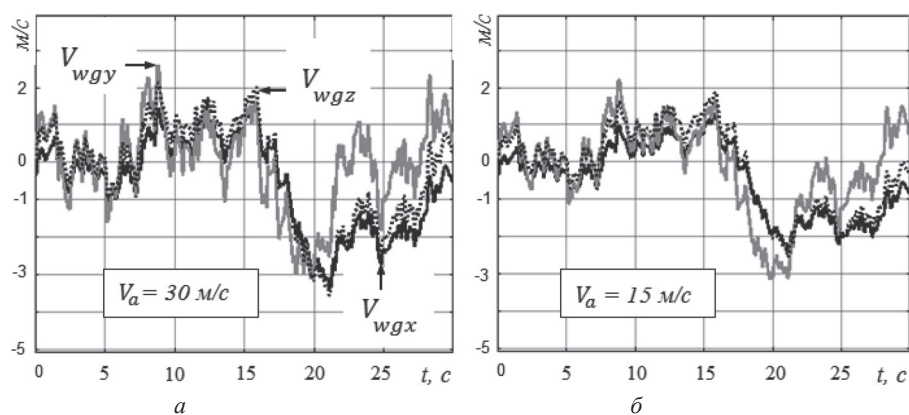


Рис. 4. Результаты моделирования стохастической компоненты ветра, при его умеренной турбулентности ($V_6 = 3,3$ м/с; $H = 50$ м)

направлении – V_{wgy} . Ее наличие может создать сложности при выполнении посадки БЛА как в автоматическом, так и в ручном режиме.

Увеличение значения ветра устойчивого направления в 1,5 раза в ИСК (см. рис. 3), приведет к аналогичному увеличению ветра устойчивого направления, действующего на БЛА в ССК. При увеличении воздушной скорости БЛА в 2 раза, стохастическая компонента ветра

изменится незначительно (10–15%) (см. рис. 4). Стохастическая компонента ветра определяется главным образом интенсивностью и масштабом ее турбулентности в данной географической области, причем с высотой полета БЛА она будет увеличиваться.

Рассмотрим влияние нелинейностей и параметрических возмущений исполнительного элемента продольного канала автопилота БЛА

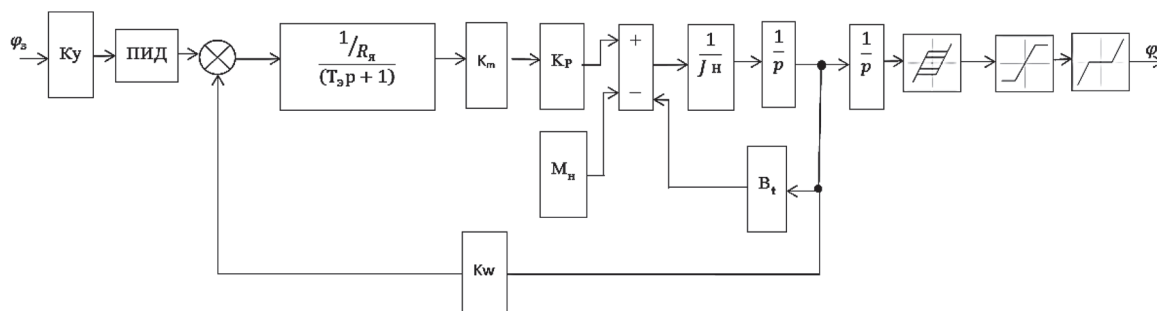


Рис. 5. Упрощенная Simulink-модель сервопривода с учетом действующих нелинейностей и возмущений

на динамические характеристики контура. В качестве исполнительного элемента, был рассмотрен сервопривод типа *Dynamixel rx24-f*.

Основные нелинейности сервопривода [9]:

- зона нечувствительности сервопривода из-за погрешности энкодера: $\Delta = \pm 0,3$ град;
- люфт в пределах ± 5 угл. мин.

Основные параметрические возмущения обусловлены следующими факторами:

- изменением резистивного сопротивления якорной обмотки двигателя постоянного тока в зависимости от изменения температуры окружающей среды:

$$R_{\text{я}} = 1 + \alpha(T_{15} - T_{\text{т}}),$$

где α – температурный коэффициент (для меди – 0,004); $T_{\text{т}}$ – текущая температура ($-40 < T_{\text{т}} < 40$) на высотах до 1 км;

- изменением коэффициента вязкого трения – B_t силиконовой смазки от температуры окружающей среды в пределах 3–5% [10];

- изменением шарнирного момента аэродинамической нагрузки. Величина шарнирного момента аэродинамической нагрузки, действующего на сервомашинку [11]:

$$M_{\text{н}} = \frac{\left(\frac{\rho V_a^2}{2} S_{\text{эф}} 0,005 \varphi_{\text{max}} b \right)}{i} \quad (4)$$

где $S_{\text{эф}}$ – эффективная площадь руля ($0,003 \text{ м}^2$); b – хорда руля ($0,03 \text{ м}$); ρ – плотность воздуха на заданной высоте полета; φ_{max} – максимальный угол отклонения стабилизатора (30 град); i – передаточное отношение силовой проводки (1,33). Допущения: не учитываются упругие деформации механической передачи; аэродинамическая и весовая компенсация руля.

В состав сервопривода *Dynamixel rx24-f* помимо коллекторного двигателя постоянного тока входит и система управления приводом. В качестве системы управления выступает про-

порционально-интегрально-дифференциальный регулятор (ПИД-регулятор):

$$u(t) = K_1 e(t) + K_2 \int_0^t e(t) dt + K_3 \frac{d}{dt} e(t) \quad (5)$$

где $K_1 = 12,147$; $K_2 = 1,792$; $K_3 = 0,01$.

На рис. 5, изображена упрощенная *Simulink*-модель сервопривода с учетом действующих нелинейностей и возмущений. Параметры модели: $T_{\text{э}} = 0,2 \text{ с}$; $K_m = 0,027$; $K_w = 0,027$; $K_p = 193$; $J_{\text{н}} = 6,5595 \cdot 10^{-7} \text{ кг} \cdot \text{м}^2$; $B_t = 0,132$; $K_y = 25$.

Результаты моделирования влияния нелинейностей и возмущений на выходной сигнал сервопривода, приведены на рис. 6. Проведенные исследования показали, что основной нелинейностью влияющей на выходной сигнал сервопривода (см. рис. 6, в) в пределах ($\pm 4\%$), является наличие зоны нечувствительности энкодера. Изменение коэффициента усиления сервопривода вследствие температурных воздействий, невелико в пределах ($\pm 1\text{--}2\%$) (см. рис. 6, а). Изменение нагрузки и других нелинейностей (см. рис. 6, б, г, д, е), так же не значительны и их можно не учитывать при синтезе автопилота БЛА.

На рис. 7, изображена упрощенная структурная схема статического автопилота управления высотой полета БЛА.

Структурная схема, соответствующая передаточной функции $W_{\text{БЛА}}(p)$, представлена рис. 8 [12].

На рис. 8 представлены следующие параметры: $\alpha_{\text{в}}$ – угол ветра, $\alpha_{\text{в}} \approx \frac{V_{\text{wy}}}{V_a}$; K_b – коэффициент передачи по тангажу; T_0 – постоянная времени характеризующая маневренность БЛА в продольном направлении; T_{α} – постоянная времени собственных колебаний БЛА; ξ – коэффициент демпфирования.

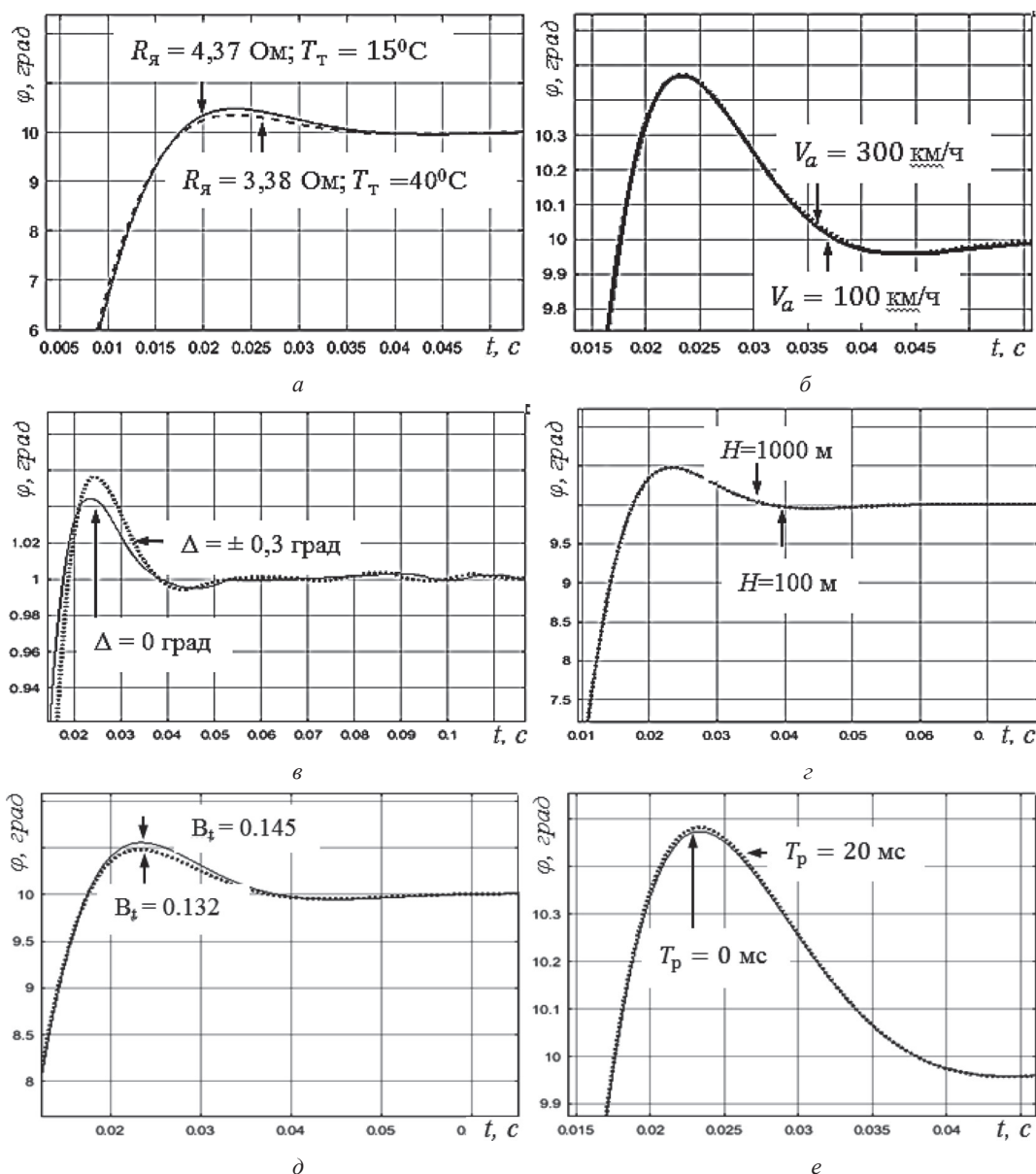


Рис. 6. Реакция сервопривода на управляющее воздействие с учетом нелинейностей и возмущений

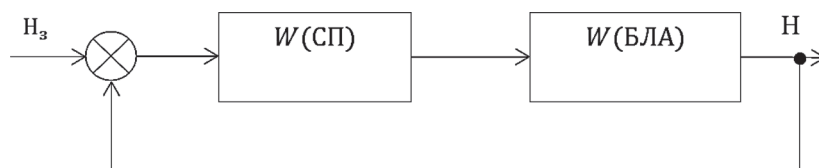


Рис. 7. Упрощенная структурная схема контура стабилизации высоты полета БЛА

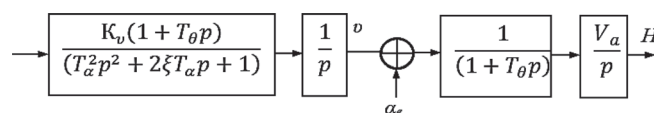


Рис. 8. Структурная схема модели движения БЛА с учетом ветра

Для исследуемого БЛА: $\xi = 0,805$; $T_\alpha = 0,1 \text{ с}$; $T_\theta = 0,229 \text{ с}$; $K_p = 4,365 \text{ 1/с}$ [3].

Результаты моделирования переходных процессов в контуре стабилизации высоты полета

БЛА с учетом нелинейностей сервопривода и ветровых возмущений, представлена на рис. 9. Анализ представленных результатов показал (см. рис. 9, а), что при умеренной турбулент-

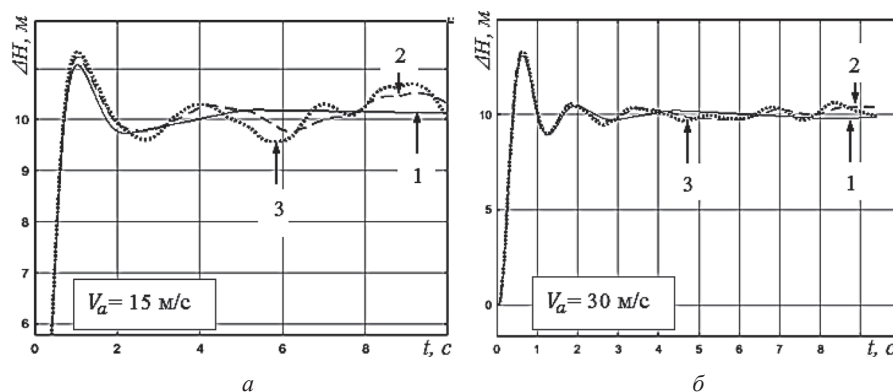


Рис. 9. Реакция модели продольного движения БЛА по высоте полета с учетом нелинейностей сервопривода и ветровых возмущений: 1 – без ветра; 2 – при умеренной турбулентности ветра на $H = 50$ м; 3 – при умеренной турбулентности ветра на $H = 600$ м

ности ветра и малой скорости БЛА ($V_a = 15$ м/с = 54 км/ч), СКО ошибки выходного сигнала по управляющему воздействию составляет примерно 4–5% от установившегося значения. При скорости полета БЛА $V_a = 30$ м/с = 108 км/ч, влияние ветра на ошибку по высоте менее значительно, СКО ошибки составляет всего 2–3% от установившегося значения.

Заключение

1. Применительно к метеорологическим условиям территории Республики Беларусь стохастическая компонента ветра существенно больше значения ветра устойчивого направления.

2. При крейсерских скоростях полета БЛА более 100 км/ч, влиянием ветровых возмущений можно пренебречь.

3. Нелинейности элементов сервопривода, за исключением зоны нечувствительности энкодера, не оказывают существенного влияния на работу автопилота БЛА.

При синтезе контуров угловой стабилизации и САУ БЛА применительно к метеорологическим условиям территории Республики Беларусь учет ветровых возмущений целесообразно производить для скоростей полета БЛА менее 100 км/ч.

ЛИТЕРАТУРА

1. Робастный автопилот канала тангажа летательного аппарата: пат. 18251 Респ. Беларусь / В. А. Малкин, Ю. В. Гриднев, А. Н. Пальцев, А. А. Цанава; заявитель Государственное научное учреждение «Физико-технический институт Национальной академии наук Беларуси». – № а 20111592; заявл. 24.11.11; опубл. 30.06.13 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2013. – С. 8.
2. Гриднев, Ю. В. Робастный автопилот канала тангажа беспилотного летательного аппарата / Ю. В. Гриднев, А. Г. Иванов // Доклады БГУИР. – 2017. – № 3 (150). – С. 40–44.
3. Распопов, Б. Я. Автопилот мини-беспилотного летательного аппарата / Б. Я. Распопов [и др.] // Мехатроника, автоматизация, управление. – 2008. – № 10. – С. 19.
4. Рэндал У. Биард, Тимоти У. МакЛэйн. Малые беспилотные летательные аппараты: теория и практика. – Москва: ТЕХНОСФЕРА, 2015. – 312 с.
5. [Электронный ресурс]. – Режим доступа: <https://www.mathworks.com/help/aerotbx/environment.html>. – Дата доступа: 5.03.2019.
6. [Электронный ресурс]. – Режим доступа: <https://www.energywind.ru/recomendacii/skorost-vetra-belarus.html>. – Дата доступа: 20.02.2019.
7. Flying Qualities of Piloted Airplanes. U. S. Military Specification MIL-F-8785C. Washington, D. C.: U. S. Department of Defense, 1980.
8. Санько, А. А. Основы построения и алгоритмы работы навигационных систем воздушных судов: пособие по изучению дисциплины. Часть 1 / сост.: А. А. Санько, В. М. Дедков. – Минск: БГАА, 2016. – 96 с.
9. Сервопривод: доклады научно-методического семинара, 31 января 2013 года / М-во образования и науки Российской Федерации, Нац. исследовательский ун-т «МЭИ», Каф. автоматизированного электропривода; [редкол.: А. С. Анучин, М. Г. Бычков, А. Н. Ладыгин]. – Москва: Изд-во МЭИ, 2013. – 88 с.: ил., табл.; 21 см.; ISBN 978–5–7046–1367–1.
10. [Электронный ресурс]. – Режим доступа: <https://www.mirsmazok.ru/smazki/dlya-chego-nuzhna-silikonovaya-smazka/>. Дата доступа: 5.03.2019.
11. Мхитарян, А. М. Аэродинамика: учебник для авиац. специальностей вузов / А. М. Мхитарян. – изд. 2-е, перераб. и доп. – Москва: Машиностроение, 1976. – 446 с.

12. Михалев, И. А. Системы автоматического управления полетом самолета. Методы анализа и расчета / И. А. Михалев. – Москва: Машиностроение, 1971. – 464 с.

REFERENCES

1. **Robust** autopilot of the pitch channel of the aircraft: pat. 18251 Rep. Belarus / V. A. Malkin, Yu. V. Gridnev, A. N. Fingers, A. A. Tsanova; applicant State Scientific Institution «Physico-Technical Institute of the National Academy of Sciences of Belarus.» – № a 20111592; declare 24.11.11; publ. 30.06.13 // Afitsyny bul. / Nat. center of intellectual. ulasnasti. – 2013. – p. 8.
2. **Gridnev, Y. V.** Robust autopilot of the pitch channel of an unmanned aerial vehicle / Y. V. Gridnev, A. G. Ivanov // Reports of BGUIR. – 2017. – № 3 (150). – P. 40–44.
3. **Raspopov, B. Ya.** Autopilot of a mini unmanned aerial vehicle / B. Ya. Raspopov [et al.] // Mechatronics, automation, control. – 2008. – № 10. – p. 19.
4. **Randal W. Byard, Timothy W. McLain.** Small unmanned aerial vehicles: theory and practice. – Moscow: TECHNO-SPHERA, 2015. – 312 p.
5. **[Electronic resource].** – Access mode: <https://www.math-works.com/help/aerotbx/environment.html>. – Access date: 5.03.2019.
6. **[Electronic resource].** – Access mode: <https://www.energywind.ru/recomendacii/skorost-vetra-belarus.html>. – Access Date: 20.02.2019.
7. **Flying** Qualities of Piloted Airplanes. U. S. Military Specification MIL-F-8785C. Washington, D. C.: U. S. Department of Defense, 1980.
8. **Sanko, A. A.** Basics of construction and algorithms of the navigation systems of aircraft: a manual for the study of discipline. Part 1 / comp.: A. A. Sanko, V. M. Dedkov. – Minsk: BGAA, 2016. – 96 p.
9. **Servo drive:** reports of the scientific and methodological seminar, January 31, 2013 / Ministry of Education and Science of the Russian Federation, Nat. Research University «MEI», Kaf. automated electric drive; [Edited: A. S. Anuchin, M. G. Bychkov, A. N. Ladygin]. – Moscow: MEI Publishing House, 2013. – 88 pp., Ill., Tabl.; 21 cm; ISBN 978–5–7046–1367–1.
10. **[Electronic resource].** – Access mode: <https://www.mirsmazok.ru/smazki/dlya-chego-nuzhna-silikonovaya-smazka>. Date of access: 5.03.2019.
11. **Mkhitaryan, A. M.** Aerodynamics: a textbook for aviats. university specialties / A. M. Mkhitaryan. – ed. 2nd, Pererab. and add. – Moscow: Mechanical Engineering, 1976. – 446 p.
12. **Mikhalev, I. A.** Automatic flight control systems of the aircraft. Methods of analysis and calculation / I. A. Mikhalev. – Moscow: Mechanical Engineering, 1971. – 464 p.

Поступила
14.03.2019

После доработки
20.06.2019

Принята к печати
01.07.2019

MALKIN V. A., ROZHKOVI I. V., SAN'KO A. A.

INFLUENCE OF WIND DISTURBANCES AND NONLINEARITIES OF SERVO DRIVE ON THE CONTOUR OF STABILIZATION OF THE FLIGHT OF HEIGHT OF UNMANNED AERIAL VEHICLE

The article discusses a mathematical model of wind, taking into account its stochastic component and wind of a steady direction, presents the results of a comparative analysis of the effect of wind parameters on the total wind velocity vector acting on unmanned aerial vehicles (UAV). The main non-linearities of the autopilot servo elements and their influence on the output signal are considered. The reaction of the contour of the UAV flight altitude stabilization to the wind is considered, taking into account the nonlinearity of the servo drive elements. Proved the need to take into account the wind in the synthesis of automatic control systems (ACS) and the contours of the angular stabilization of the drone at stages where the flight speed of the drone is less than 30 m / s.

Keywords: wind; unmanned aerial vehicle; mathematical model of wind; matematic servo model, servo nonlinearity.



Малкин Виталий Александрович – доктор технических наук, профессор, профессор кафедры авиационных радиоэлектронных систем учреждения образования «Военная академия Республики Беларусь»

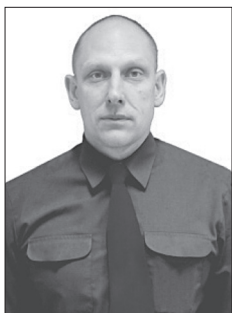
Мобильный телефон для связи (персональный): + 37529 362 62 19.



Рожков Игорь Владимирович – магистр технических наук, аспирант, старший преподаватель кафедры беспилотных авиационных комплексов и боевого управления учреждения образования «Белорусская государственная академия авиации»

E-mail: 7528972@mail.ru

Мобильный телефон для связи (персональный): + 37529 752 89 72.



Санько Андрей Анатольевич – кандидат технических наук, доцент, профессор кафедры воздушных судов и авиационного оборудования, учреждения образования «Белорусская государственная академия авиации»

E-mail: min.777.144@mail.ru

Мобильный телефон для связи (персональный): + 37544 582 47 22.

**ОБРАБОТКА
ИНФОРМАЦИИ
И ПРИНЯТИЕ РЕШЕНИЙ**

**DATA PROCESSING
AND
DECISION-MAKING**

Е. А. БЛИНОВА, А. А. СУЩЕНЯ

ПРИМЕНЕНИЕ НЕСКОЛЬКИХ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ ДЛЯ ОСАЖДЕНИЯ СКРЫТЫХ ДАННЫХ В ЭЛЕКТРОННЫХ ТЕКСТОВЫХ ДОКУМЕНТАХ

Белорусский государственный технологический университет

Приведено формальное описание метода и алгоритма встраивания скрытого сообщения или цифрового водяного знака в файлы электронных документов Microsoft Word формата .DOCX на основе двух стеганографических методов. Электронный документ Microsoft Word формата .DOCX используется в качестве стеганографического контейнера. Один из методов использует особенности отображения документа текстовым процессором и состоит в том, что текстовый процессор допускает смещение скрытых символов, таких как пробелы, табуляции и абзацы, в тексте относительно линии набора. Второй метод использует особенности формата электронного текстового документа формата .DOCX, который представляет собой архив, содержащий файлы в формате Open XML и медиафайлы. Таким образом, для осаждения скрытого сообщения могут быть использованы специализированные стеганографические методы, предназначенные для файлов формата XML. В данном случае используется метод замены кавычек. Осаждение скрытого сообщения одним из методов предусматривает контроль целостности сообщения посредством второго метода. В зависимости от емкости стеганографического контейнера выбирается метод для осаждения сообщения и метод для контроля целостности сообщения. Рассмотрен алгоритм обратного стеганографического преобразования для извлечения сообщения и подтверждения целостности электронного документа. Разработано приложение для выполнения осаждения скрытого сообщения в электронном текстовом документе в зависимости от емкости контейнера. Проанализирована возможность совместного применения различных стеганографических методов с целью формирования многоключевой стеганографической системы, предназначенной для идентификации на основе цифрового водяного знака электронного документа Microsoft Word формата .DOCX.

Ключевые слова: стеганография, электронный документ, формат .DOCX

Введение

В настоящее время является актуальной задача передачи скрытых сообщений в открытых источниках или размещения скрытых меток в открытых данных для подтверждения авторства на эти данные. Методы, реализующие такое скрытие, называются стеганографическими методами, данные, в которых размещаются скрытые сообщения, – стеганографическими контейнерами, а сами скрытые сообщения – стеганосообщениями. Под стеганографическим ключом понимается место и порядок скрытия сообщения в открытых данных. Стеганографическая система объединяет все вышеперечисленное. Математическая модель стеганографической системы может быть представлена в следующем виде:

$$S = \text{Emb}(C, M, K), \quad (1)$$

$$M = \text{Ext}(S, K), \quad (2)$$

где C – множество всех контейнеров, K – множество стеганографических ключей, M – множество скрытых сообщений, S – множество контейнеров с осажденной информацией, $\text{Emb}()$ и $\text{Ext}()$ – функции встраивания скрытого сообщения в файл-контейнер и извлечения из файла-контейнера соответственно. [1]

Для скрытия информации или осаждения скрытых меток используются различные виды файлов-контейнеров: текстовые документы в разнообразных форматах, изображения, звук, видео. Для каждого типа файлов-контейнеров разработаны разнообразные методы, комбинирующие стандартные синтаксические методы текстовой стеганографии и методы, основанные на специфических свойствах документа-контейнера, например, осаждение скрытой информации в метаданных изображения или особенностях форматирования текста электронного текстового документа.

Основными направлениями применения стеганографических методов являются внесение различных стеганографических меток в каждую копию электронного документа (Digital Fingerprint), внесение одинаковых стеганографических меток во все копии документа (Watermarking) и скрытая передача и хранение данных. Следует отметить, что при стеганографическом преобразовании данные не шифруются, однако, часто предполагается, что скрытое сообщение может быть предварительно зашифровано криптографическими методами для дополнительной защиты данных.

В связи с широким распространением, электронные документы Microsoft Office часто используются в качестве файлов-контейнеров. Для них применяются методы, которые используют наравне с классическими методами текстовой стеганографии методы, свойственные контейнеру, такие как формат и смещение текста, размещение диакритических знаков, наличие истории редактирования и прочей служебной информации, что позволяет добиться увеличения скрытности и пропускной способности. В статье рассматривается совместное применение двух различных стеганографических методов осаждения скрытой информации в электронных документах Microsoft Word формата .DOCX.

Основная часть

Основной проблемой при применении стеганографических методов для осаждения скрытой информации в электронных документах Microsoft Word формата .DOCX с использованием специфических методов, свойственных контейнеру, является проблема разрушения скрытого сообщения после изменения форматирования текста. В связи с этим, предлагается использовать два стеганографических метода, использующих различные свойства контейнера, для взаимного контроля друг друга. Один метод использует изменения межстрочного расстояния для неотображаемых символов, а второй – особенность описания электронного документа Microsoft Word формата .DOCX в формате XML.

Метод изменения межстрочного расстояния, или line-shift coding, успешно применялся для маркирования технической документации для предотвращения утечек со стороны допу-

щенных к ней специалистов. В его стандартной реализации предлагалось скрывать стеганосообщение в изменении высоты межстрочных интервалов, причем для каждой копии документа выбирался свой набор межстрочных интервалов, что позволяло выявить источник несанкционированных копий. Однако такой метод имеет несколько существенных недостатков: он обладает малой пропускной способностью и может быть выявлен для электронного документа путем изменения параметров размера и начертания шрифта.

Была предложена модификация стеганографического метода изменения межстрочного расстояния электронного документа, заключающаяся в том, чтобы производить смещение не всей строки, а только неотображаемых символов (пробелов, табуляций, знаков переноса строки, неразрывных пробелов, абзацев и т. д.) [2]. В качестве редактора электронных текстовых документов использовался редактор Microsoft Word 2010, однако изменение высоты строки, как для полной строки, так и для отдельных символов существует и в других текстовых редакторах. В Microsoft Word такое смещение производится как Шрифт/Интервал/Смещение.

Отметим, что, как видно из рис. 1, б, изменение начертания и размера шрифта не влияют на отображение электронного текста из-за особенностей реализации контейнера. Также отметим, что стандартными средствами текстового редактора различные высоты смещения символов текста не определяются, в отличие от других свойств формата (размера, начертания и пр.), и могут быть определены только визуально, либо программно. При переносе текста между различными редакторами электронных текстовых документов смещение неотображаемых символов переносится только в некоторых редакторах электронных документов. Было протестировано внедрение скрытой информации в некоторые, наиболее часто применяющиеся, редакторы электронных документов: Microsoft Word (версии от 2000 до 2010), Adobe InDesign версии CS5 и ранее, Corel версии X6 и ранее. При переносе в Adobe Acrobat изменение междустрочного интервала неотображаемых символов, к сожалению, невозможно из-за особенностей экспорта в формат .pdf [3].

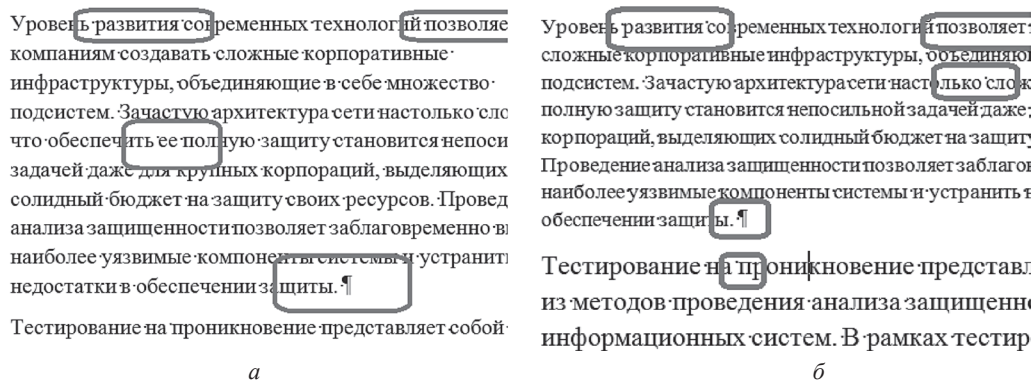


Рис. 1. *а* – текст со смещенными неотображаемыми символами; *б* – Текст со смещенными неотображаемыми символами с изменением начертания и размера шрифта

Второй метод, использующий особенности описания электронного документа Microsoft Word формата .DOCX в формате XML, состоит в следующем. Файл формата .DOCX не является расширенным файловым форматом, а представляет собой архив. Формат файла основан на Open XML, подробно описанный в стандарте ECMA-376: Office Open XML File Formats, и использует сжатие по алгоритму ZIP для уменьшения размера файла. Данный архив содержит два типа файлов – файлы формата XML с расширениями xml и rels и медиа-файлы, например, изображения. Логически файл состоит из трех видов элементов: типов, частей и связей. Типы – это список сущностей, встречающихся в документе, например, типов медиа-файлов или частей документов, части – это отдельные части документа, для каждой части документа создан отдельный файл формата XML. Между частями документа устанавливаются связи. Таким образом, можно сказать, что файл формата .DOCX представляет собой набор сжатых файлов формата XML, причем все текстовое содержимое электронного документа Microsoft Word формата .DOCX находится в одном XML файле, а именно в document.xml. Файл document.xml представляет собой XML файл в элементной форме, где каждому элементу обычно соответствует один атрибут. Теги начинаются с «w:» и обозначают:

<w:document> – тег свойства документа, указываются пространства имен, используемые при построении XML файла;

<w:body> – тег тела документа, является корневым тегом для частей документа;

<w:p> – тег абзаца документа, где указываются свойства абзаца, такие как выравнивание, абзацные отступы и т. д.;

<w:r> – тег фрагмента текста, для которого указываются особенности форматирования данного участка текста, такие как размер шрифта, высота межстрочного интервала, цвет и т. д.;

<w:t> – тег текста, в котором содержится текст части документа.

Теги <w:p> и <w:r> содержат вложенный тег <w:sectionPr> для описания особенностей форматирования именно этого участка. Например, тег описания свойств абзаца <w:pPr> содержит в себе вложенный тег описания интерлиньяжа <w:spacing w:lineRule=«exact» w:line=«360»/>, который обозначает, что высота межстрочного интервала задана точно и составляет 18 пунктов, так как параметр «w:line» измеряется в двадцатых долях пункта. Для описания форматирования отдельных символов используется тег <w:rPr>. Например, в следующей конструкции <w:rPr> <w:sz w:val=«28»/> <w:szCs w:val=«28»/> </w:rPr> параметр <w:sz w:val=«28»/> измеряется в ½ пункта и в данном случае указывает, что кегль данного участка текста равен 14 пунктам, а параметр <w:szCs w:val=«28»/> используется для отображения специфических шрифтов, например арабского.

Известно, что интерпретация XML документа допускает различный регистр тегов и порядок следования атрибутов. Кроме того, XML документ безразличен к типу кавычек – для обрамления значений атрибутов могут использоваться как двойные, так и одинарные кавычки, причем при визуальном анализе документа Microsoft Word со стороны пользователя никаких отличий видно не будет. Был предложен стеганографический метод замены типа кавычек с двойных на одинарные в XML документе [4–8].

Name	Size	Packed	Type
..			Локальный диск
_rels			Папка с файлами
theme			Папка с файлами
document.xml	8 143	1 467	Документ XML
fontTable.xml	1 334	465	Документ XML
settings.xml	2 486	938	Документ XML
styles.xml	28 719	2 860	Документ XML
webSettings.xml	576	280	Документ XML

Selected 8 143 bytes in 1 file Total 2 folders and 41 258 bytes in 5 fil

```

<w:rFonts w:cs="Times New Roman" w:hAnsi="Times New Roman" w
<w:sz w:val="28"/>
<w:szCs w:val="28"/>
</w:rPr>
<w:t xml:space="preserve">включены краткие теоретические сведен
</w:t>
</w:r>

```

Рис. 2. Структура документа формата.DOCX

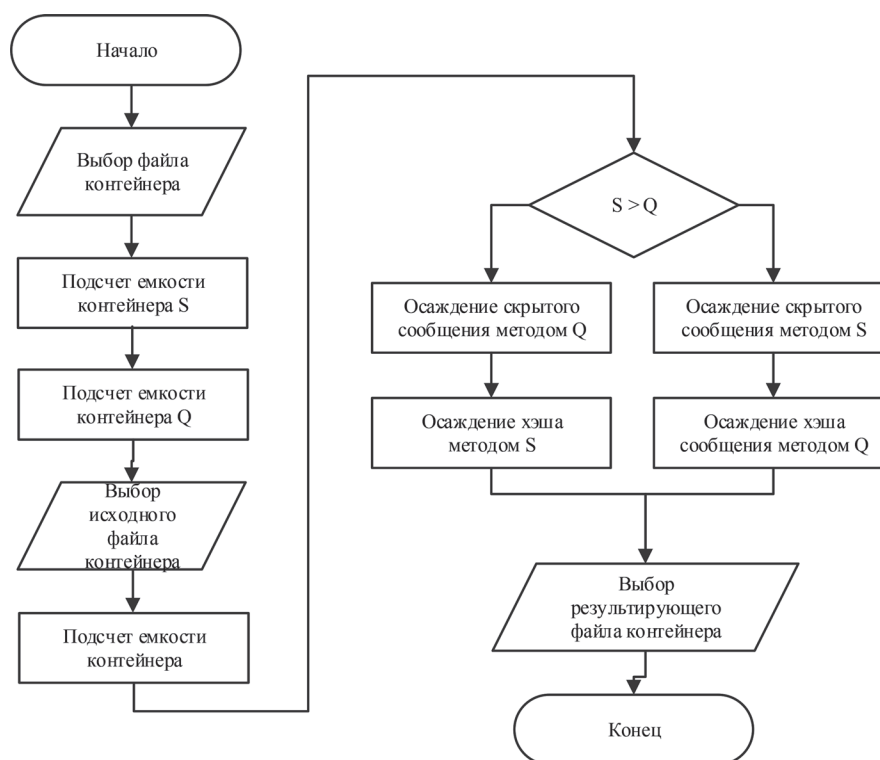


Рис. 3. Алгоритм осаждения скрытого сообщения в документ формата .DOCX

Таким образом, существуют два метода, каждый из которых позволяет осадить некоторое скрытое сообщение, используя особенности формата файла электронного документа. Будем использовать один из методов для осаждения скрытой информации в файл контейнер, а второй – для контроля целостности файла контейнера. Для осаждения сообщения будем приводить его к виду бинарной последовательности. Выбор метода осаждения выполняется исходя из емкости контейнера, которую можно рассчитать следующим образом. Подсчитыва-

ется количество неотображаемых символов в файле контейнере. Визуально незаметное смещение может производиться в диапазоне ± 1 пункт, что дает 6 бит скрытого сообщения на 3 неотображаемых символа. Для метода замены типа кавычек подсчитывается количество пар кавычек в файле document.xml, одна пара кавычек соответствует 1 биту скрытого сообщения.

Алгоритм осаждения скрытого сообщения в файл контейнер изображен на рис. 3. Обозначим метод изменения межстрочного расстоя-

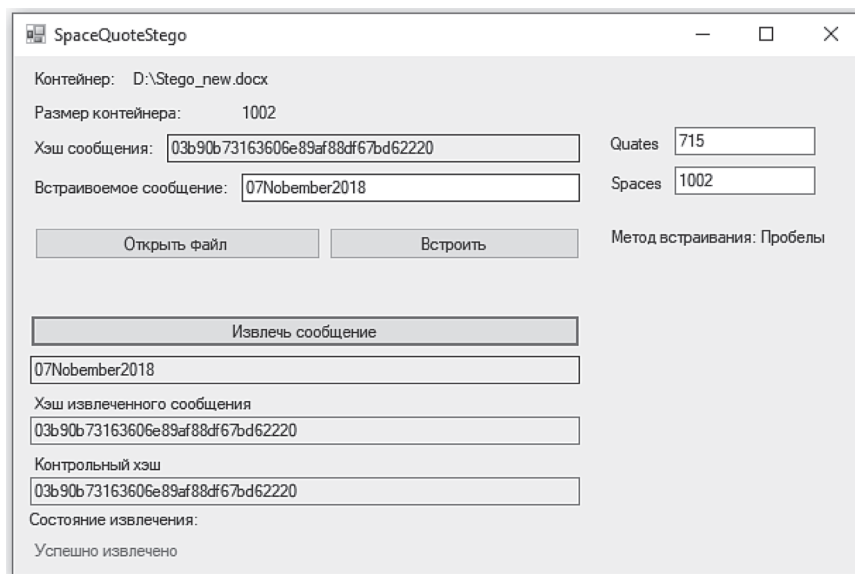


Рис. 4. Интерфейс программного средства SpaceQuoteStego

ния для неотображаемых символов как S , а метод замены типа кавычек с двойных на одинарные – Q .

Для реализации осаднения скрытых сообщений в документы формата .DOCX был разработан программный продукт SpaceQuoteStego [9].

SpaceQuoteStego позволяет создавать стеганографические контейнеры на основе электронных документов формата .DOCX. В этом программном средстве реализован вышеописанный алгоритм осаднения скрытого сообщения в электронных документах формата .DOCX с некоторыми ограничениями: из неотображаемых символов рассматриваются только пробелы, доступно осаднение только буквенно-цифровых комбинаций и пробелов, хеширование производится по методу MD5. После указания исходного файла вычисляется емкость контейнера в зависимости от применяемого метода осаднения. После ввода скрытого сообщения, вычисляется его хэш, и происходит осаднение сообщения и хэша. При извлечении требуется указать файл, из него извлекается сообщение и вычисляется хэш сообщения, ко-

торый сравнивается с контрольным значением хэша, извлеченным при помощи другого метода.

Заключение

В статье рассмотрена система комбинированного применения двух стеганографических методов, основанная на различных свойствах электронного текстового документа Microsoft Word формата .DOCX. Каждый из методов может быть использован либо для осаднения данных, либо для хранения значения хэша данных, чем осуществляется проверка целостности сообщения при внесении изменений в файл контейнер. Одним из методов является метод изменения межстрочного расстояния для неотображаемых символов, второй использует особенности описания электронного документа в формате XML. Разработано приложение, позволяющее создавать стеганографические контейнеры из электронных документов с использованием данного подхода, что может быть применено для скрытой передачи и хранения данных и подтверждения права собственности на информацию, представленную в цифровом виде.

Литература

1. **Урбанович, П. П.** Защита информации методами криптографии, стеганографии и обфускации: учеб.метод. пособие / П. П. Урбанович. – Минск: БГТУ, 2016. – 220 с.
2. **Блинова, Е. А.** Стеганографический метод на основе изменения межстрочного расстояния неотображаемых символов строк электронного текстового документа // Материалы 80 конференции профессорско-преподавательского состава БГТУ. – Минск. – 2016. – с. 11.
3. **Блинова, Е. А.** Стеганографический метод на основе изменения междустрочного расстояния неотображаемых символов строк электронного текстового документа // Труды БГТУ. Сер. Физико-мат. науки и информатика № 6. – Минск: БГТУ. – 2016. – С. 166–169.

4. Сушеня, А. А. Стеганографическое преобразование текстов-контейнеров на основе языков разметки / А. А. Сушеня // 68-я научно-техническая конференция учащихся, студентов и магистрантов, 17–22 апреля, Минск: сборник научных работ: в 4 ч. Ч. 4 / Белорусский государственный технологический университет. – Минск: БГТУ, 2017. – С. 145–149.
5. Сушеня, А. А. Способ стеганографического осаждения информации в документ с расширением .DOCX / А. А. Сушеня // XXI Республиканская научная конференция студентов и аспирантов, 19–21 марта, Гомель: сборник научных работ / Гомельский государственный университет имени Ф. Скорины. – С. 303–304.
6. Сушеня, А. А. Идея и архитектура веб-приложения, использующего в качестве стеганографического контейнера документы формата DOCX / А. А. Сушеня // Международная научно-практическая конференция, 14–18 мая, Минск: сборник научных работ / Белорусский государственный университет. – С. 170.
7. Сушеня, А. А., Блинова Е. А., Урбанович П. П. Модификация стеганографического метода изменения междустрочного расстояния электронного документа // Технические средства защиты информации: Тезисы докладов XVI Белорусско-российской научно-технической конференции, 5 июня 2018 г. Минск. Минск: БГУИР, 2018. – С 90–91.
8. Сушеня, А. А. Программное средство стеганографического преобразования текстов-контейнеров на основе языка разметки XML / А. А. Сушеня // 69-я научно-техническая конференция учащихся, студентов и магистрантов, 2–13 апреля, Минск: сборник научных работ: в 4 ч. Ч. 4 / Белорусский государственный технологический университет. – Минск: БГТУ, 2018. – С. 81–84.
9. WhiteSpaceStego [Электронный ресурс]: <https://github.com/bntdeep/WhiteSpaceStego> Дата доступа: 07.11.2018.

REFERENCES

1. Urbanovich P. P. Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii [The protection of information based on the methods by cryptography steganography and obfuscation]. Minsk. BSTU Publ., 2017. 220 p.
2. Blinova E. The steganography method based on the line-shift coding method on non-displayed symbols of the electronic text document, Proc. of 80th International Scientific Conference on Belarusian State Technological University of Faculty members, Researchers and graduate students, Minsk, Belarus, 2016, p. 11.
3. Blinova E. The steganography method based on the line-shift coding method on non-displayed symbols of the electronic text document // Trudy BGTU [Proceedings of BSTU], series 3, Physics and Mathematics. Informatics, 2016, no. 6, pp. 166–169.
4. Sushchenia, A. A. Steganography transformation text containers based on markup languages / A. A. Sushchenia // 68 scientific conference of students, students and undergraduates: collection of scientific works, Minsk, April 17–22, 2017: in 4 parts/Belarusian State University of Technology. -Mn.: BSTU, 2017. -Ch. 4. – С. 145–149.
5. Sushchenia, A. A. Steganographic method of information embedding into a document with the extension Sushchenia / A. A. Sushchenia // XXI Republican Scientific Conference of Students and Postgraduates, March 19–21, Gomel: Collection of Scientific Works / F. Skorina Gomel State University. – С. 303–304.
6. Sushchenia, A. A. The idea and architecture of a web application that uses DOCX-format documents as a steganographic container / A. A. Sushchenia // International Scientific and Practical Conference, May 14–18, Minsk: collection of scientific papers / Belarusian State University. – С. 170.
7. Sushchenia, A. A., Blinova E. A., Urbanovich P. P. Steganographic method modification of the changing line distance of an electronic document // Technical means of information protection: Abstracts of the 16th Belarusian-Russian Scientific and Technical Conference, June 5, 2018, Minsk. Minsk: BSUIR, 2018. – С 90–91.
8. Sushchenia, A. A. Software for steganographic transformation of text-containers based on XML markup language / A. A. Sushchenia // 69th Scientific and Technical Conference of Pupils, Students and Undergraduates, April 2–13, Minsk: a collection of scientific work: at 4 pm. Part 4 / Belarusian State Technological University. – Minsk: BSTU, 2018. – p. 81–84.
9. WhiteSpaceStego: <https://github.com/bntdeep/WhiteSpaceStego>. 07.11.2018.

Поступила
11.05.2019

После доработки
23.06.2019

Принята к печати
01.07.2019

BLINOVA E. A., SUSCHENIA A. A.

SEVERAL STEGANOGRAPHIC METHODS USING FOR EMBEDDING OF HIDDEN DATA IN ELECTRONIC TEXT DOCUMENTS

The description of the method and algorithm for embedding a hidden message or a digital watermark into files of Microsoft Word electronic documents in .DOCX format based on two steganographic methods is given. A Microsoft Word electronic document in .DOCX format is used as a steganographic container. One of the methods uses the features of displaying a document by a word processor and the word processor allows the displacement of hidden characters, such as spaces, tabs and paragraphs, in the text relatively to the line of text. The second method uses the feature of the .DOCX format electronic text document that a document is an archive containing Open XML format files and media files, so specialized steganographic methods for XML files can be used for embedding a hidden message. In this case the quotes replacement method is used. The embedding of a hidden message by one of the methods is used for checking the integrity of the other message through the second method. Depending on the capacity of the steganographic container a method can be chosen to embed the message and

a method to control the integrity of the message. The algorithm of the inverse steganographic transformation for extracting a message and confirming the integrity of an electronic document is considered. The application is developed to perform the embedding of a hidden message in an electronic text document depending on the capacity of the container. The possibility of using of some steganographic methods is analyzed with the aim of forming a multi-key steganographic system intended for a digital watermarking of an electronic document Microsoft Word format .DOCX.

Keywords: steganography, electronic document, line-shift coding.



Блинова Евгения Александровна – старший преподаватель кафедры ИСИТ Белорусского государственного технологического университета. Научные интересы: стеганография, базы данных, обработка данных.

Evgenia Blinova – senior teacher at Information systems and technologies Department at Belorussian State Technological University. Scientific interests: Steganography, Database Administration, Programming and Security.

Email: eugenia.blinova@gmail.com.



Сушченя Артём Александрович закончил Белорусский государственный технологический университет по специальности «Информационные системы и технологии» (2018), обучается в магистратуре по специальности «Системный анализ, управление и обработка информации». Научные интересы: стеганографические методы скрытой передачи информации.

Sushchenia Artsiom graduated from Belarusian State Technological University with a specialty in «Information systems and technologies» (2018), working on master degree «System Analysis, Information Control and Processing». Scientific interests: steganography methods of hidden information transfer.

Email: asuschenya@gmail.com.

УДК 043.5

Л. В. КУЗЬМИЧ, Д. П. ОРНАТСЬКИЙ, В. П. КВАСНИКОВ

МОДЕЛИРОВАНИЕ АНАЛОГОВОГО ИНТЕРФЕЙСА ДЛЯ ДИСТАНЦИОННЫХ ИЗМЕРЕНИЙ

Национальный авиационный университет, г. Киев, Украина

Данная работа ориентирована на поиск возможностей по повышению точности дистанционных измерений и помехозащищенность аналоговых интерфейсов централизованного типа с помощью резистивных тензодатчиков путем внедрения новой структурной схемы и способа коррекции ошибок, что позволяет уменьшить уровень ошибок по отношению к известным аналогам в десятки раз.

Разработана схема аналогового интерфейса, содержащая измерительную цепь, тензодатчик, вход которого соединен с источником питания через аналоговый демультиплексор, а выходы измерительной цепи через аналоговый мультиплексор подключены к измерительному усилителю, и двухканальный аналого – цифровой преобразователь с одновременной выборкой. Измерительная цепь выполнена в виде трех резистивных делителей тока, где один делитель образован резистивным тензодатчиком и резистором, а два других – образцовыми резисторами.

Выполнено моделирование схемы аналогового интерфейса на основе измерительного усилителя с дифференциально – токовыми входами и усовершенствовано схему и алгоритм безрозрывной аддитивно – мультипликативной коррекции, что позволяет уменьшить влияние входных коррелированных шумов операционных усилителей и сетевых наводок на «общее» сопротивление.

Ключевые слова: аналоговый интерфейс, демультиплексор, измерительный усилитель, преобразователь, тензодатчик.

Введение

Способ передачи данных от первичных датчиков к вторичным приборам путем использования аналоговых интерфейсов с проводными линиями связи в дистанционных измерительных системах на данный момент есть достаточно популярным, несмотря на большое количество развитых и более технологических проводных и беспроводных цифровых интерфейсов. Это подтверждается тем, что ученые и производители микросхем продолжают предлагать новые интегральные решения для аналоговой передачи информации [1–3].

Такие решения объясняются рядом причин. В системах промышленной автоматики существует большое количество разработанных и изготовленных много лет назад устройств, использующих аналоговые каналы передачи данных. Это могут быть датчики, исполнительные устройства, устройства регистрации и тому подобное. Замена этого оборудования идет медленно и требует очень боль-

ших капиталовложений. Кроме того, перевод какого-либо производства целиком на цифровые сети означает одномоментную замену практически всего оборудования и информационных кабельных сетей. Такая масштабная реконструкция требует не только огромных средств, но и остановки производственного процесса, что во многих случаях недопустимо. Поэтому при создании или модернизации автоматических систем управления приходится использовать аналоговые каналы передачи данных для получения информации от датчиков и передачи управления на исполнительные механизмы. [4–6]

Проведенный нами анализ отечественных и зарубежных публикаций показал, что на сегодняшний день оптимизация аналоговых интерфейсов направлена на уменьшение не только инструментальных погрешностей, но и на устранение методических погрешностей, в частности ошибок наложения спектров и погрешностей восстановления сигнала [7–10].

Резистивные тензодатчики превращают в изменение своего сопротивления деформации, которая практически является равной деформации объекта в месте закрепления датчика. Эти датчики являются пассивными и для их возбуждения (инициализации) используют источник питания, подключенный к измерительной цепи, содержащий тензодатчики [11–13].

Задачей моделирования аналогового интерфейса для дистанционных измерений с помощью мультиплексора и резистивных тензодатчиков является повышение помехозащищенности и точности измерений аналого-цифрового интерфейса для многоканальных дистанционных измерений.

Основная часть исследования

Аналоговый интерфейс для дистанционных измерений с помощью мультиплексора и резистивных тензодатчиков относится к области измерительной техники, а именно – к электрическим измерениям неэлектрических величин, в данном случае механических.

Известный аналоговый интерфейс для дистанционных измерений с помощью резистивных тензодатчиков [1], который содержит в своем составе последовательно соединенные элементы: измерительная цепь с резистивными тензодатчиками, измерительный усилитель и аналоговый преобразователь логометричного типа. Источником питания является источник постоянного напряжения, гальванически изолированное от земли.

Сигнал с выхода измерительной цепи передается на вход измерительного усилителя с помощью проводных линий связи. Несимметрия этих линий с учетом значительного входного сопротивления измерительного усилителя приводит к тому, что возникает разность потенциалов (напряжение помехи), которая может быть сравнима с полезным сигналом, который может быть искажен даже слабой помехой. Еще одним недостатком данного интерфейса является то, что данной схеме не учитывается изменение сопротивления тензодатчиков в процессе эксплуатации, что, в свою очередь, снижает точность измерения при автокоррекции.

Аналогово-цифровой интерфейс для дистанционных измерений [14] содержит последовательно соединенную измерительную цепь,

в которую включен тензодатчик, вход которого связан с источником питания, измерительный усилитель, выполненный на операционных усилителях, включенных по двухкаскадной схеме, и аналого-цифровой преобразователь логометричного типа, причем входные и выходные линии связи измерительной цепи являются проводочными. Источник питания выполнен в виде источника постоянного тока без гальванической развязки, связанного с входом измерительной цепи через аналоговый демultipлексор, управляющий вход которого подключен к микроконтроллеру, входом связан с аналого-цифровым преобразователем, измерительная цепь выполнена в виде трех резистивных делителей тока, где один делитель образован резистивным тензодатчиком и подстроечным резистором, а два других – образцовыми резисторами, и в измерительном усилителе операционные усилители первого каскада включены по схеме инвертора тока.

Недостатком данной конструкции является наличие погрешностей, возникающих из-за коррелированных шумов операционных усилителей, и наведение на «общее» сопротивление в «земельном» контуре.

Поставленная задача решается тем, что аналоговый интерфейс для дистанционных измерений на базе резистивного тензодатчика содержит последовательно соединенные измерительную цепь, в которую включен тензодатчик, и вход которого соединен с источником питания через аналоговый демultipлексор, а выходы измерительной цепи через аналоговый мультиплексор подключены к входам измерительного усилителя с дифференциальными входами и первым и вторым выходами, выполнен на операционных усилителях, и двухканальный аналого – цифровой преобразователь с одновременной выборкой, причем входные и выходные линии связи измерительной цепи являются проводочными, согласно предложению источник питания выполнен в виде источника постоянного тока без гальванической развязки, связанного с входом измерительной цепи через аналоговый демultipлексор, управляющий вход которого подсоединен к микроконтроллеру, входом связанного с аналого-цифровым преобразователем, первый вход которого подключен к первому выходу измерительного усилителя, а второй выход

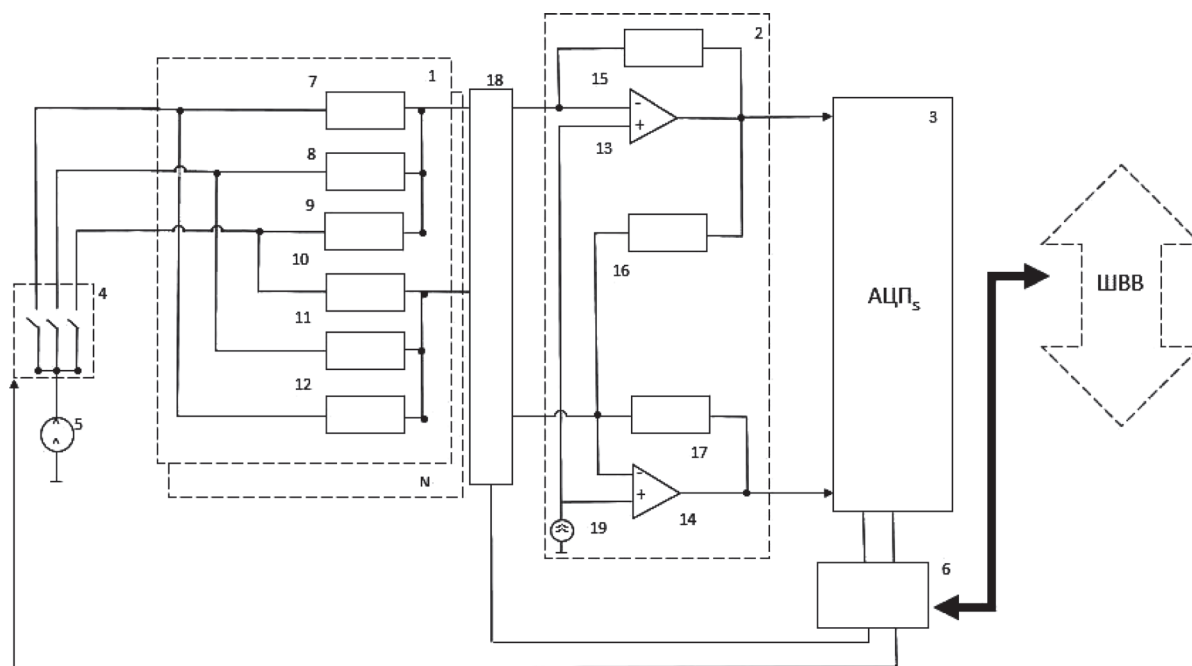


Рис. 1. Схема электрическая, функциональная аналогового интерфейса для дистанционных измерений с помощью мультиплексора и резистивных тензодатчиков: 1 – измерительная цепь N -го количества; 2 – измерительный усилитель с дифференциально-токовыми входами; 3 – двухканальный аналого-цифровой преобразователь с одновременной выборкой; 4 – аналоговый демультиплексор с третьим состоянием; 5 – источник постоянного тока; 6 – микроконтроллер; 7 – резистивный тензодатчик; 8–11 – образцовые резисторы; 12 – подстроечные резисторы; 13–14 – операционные усилители с дифференциально-токовыми входами; 15–17 – резисторы; 18 – аналоговый дифференциальный мультиплексор; 19 – ЭДС, является эквивалентом коррелированных шумов и напряжений в «земельном» контуре через «общее» сопротивление

которого подключен ко второму входу АЦП, измерительная цепь выполнена в виде трех резистивных делителей тока, где один делитель образован резистивным тензодатчиком и подстроечным резистором, а два других – образцовыми резисторами, и в измерительном усилителе операционные усилители первого каскада выполнены по схеме инвертора тока.

На рис. 1 показана схема предложенного аналогового интерфейса для дистанционных измерений с помощью мультиплексора и резистивных тензодатчиков.

В качестве аналогового дифференциального мультиплексора используется интегральная микросхема типа MAX 307 фирмы MAXIM, которая имеет следующие технические характеристики:

- Максимальное сопротивление в открытом состоянии 100 Ом;
- Максимальный ток утечки 2 нА;
- Максимальная разница между сопротивлениями параллельных каналов 5 Ом;
- Время включения и выключения 0,2 мкс.

Данный мультиплексор обеспечивает коммутацию восьми дифференциальных входов.

В качестве операционных усилителей используется интегральная микросхема типа UA747 фирмы Texas Instruments, которая содержит два операционных усилителя общего применения типа mA741C. Основные характеристики (типичные значения):

- Напряжение смещения нуля 2,0 мВ;
- Дрейф напряжения смещения нуля не более 15 мкВ / 0 С;
- Максимальный входной ток смещения нуля 80 нА;
- Коэффициент усиления дифференциального сигнала 200000.
- Максимальная разность входных токов 30 нА.
- Входное сопротивление 2 Мом.

Аналоговый интерфейс для дистанционных измерений с помощью мультиплексора и резистивных тензодатчиков работает следующим образом. Цикл измерения состоит из четырех рабочих тактов. В первом такте демультиплексор 4 находится в «третьем состоянии», то есть когда все ключи данного демультиплексора закрыты и ток инициализации I_0 не попадают в измерительную цепь 1. При этом

результаты измерения выходных напряжений операционных усилителей OU_1 и OU_2 запоминаются в памяти компьютера под названием « U_{11} » и « U_{12} ».

Во втором такте ключ K_1 демultipлексора 4 замыкается, ключи K_2 и K_3 разомкнуты. В этом случае запоминаются результаты измерения операционных напряжений операционных усилителей OU_1 и OU_2 под названием « U_{21} » и « U_{22} ».

В третьем такте замыкается ключ K_2 к демultipлексора 4, а ключи K_1 и K_3 – разомкнуты. В таком случае результаты измерения операционных напряжений операционных усилителей OU_1 и OU_2 запоминаются под названием « U_{31} » и « U_{32} ».

В четвертом такте ключи K_1 и K_2 разомкнуты, а ключ K_3 – замкнутый. В этом случае запоминаются результаты измерения операционных напряжений операционных усилителей OU_1 и OU_2 под названием « U_{41} » и « U_{42} ».

Скорректированный результат измерения вычисляем по формуле:

$$\delta = \delta_{\text{ном}} \left[\frac{\frac{U_{22} - U_{12}}{U_{21} - U_{11}} - \frac{U_{42} - U_{12}}{U_{41} - U_{11}}}{\frac{U_{32} - U_{12}}{U_{31} - U_{11}} - \frac{U_{42} - U_{12}}{U_{41} - U_{11}}} \right], \quad (1)$$

При этом, в отличие от классического метода образцовых мер [3, 14, 15], данный метод отличается «безрозрывностью» измерительного звена, позволяет компенсировать большее количество влияющих факторов, в частности коррелированных шумов операционных усилителей и шумов, обусловленных наличием общего контура заземления, сопротивления аналоговых коммутаторов. Например, в [4] приводится коррекция ошибок аналогового интерфейса для работы с тензодатчиками, существенным недостатком которой является существенное влияние сопротивления аналоговых коммутаторов, уменьшает эффективных подавления систематических составляющих погрешностей. Кроме этого, к недостаткам таких схем (использующие мостовые усилители) относится необходимость дополнительного каскада для ограничения полосы частот канала.

Для того, чтобы проверить эффективность предложенного способа по коррекции влияния различных влияющих факторов, получаем

функцию преобразования для всего измерительного канала, воспользовавшись линейной функцией преобразования тензодатчика и моделируя влияние измеряемой величины определенными значениями сопротивлений тензодатчика:

Для проверки этого была создана модель, в которой использованы параметры реальных компонентов, а именно 8-канального аналогового дифференциального мультимплексора (тип MAX 307 фирмы MAXIM) и операционных усилителей OU_1 и OP_2 общего пользования типа MA741.

Выходное сопротивление источника тока инициализации было избрано по параметрам источника тока в интегральном выполнении типа REF200 фирмы Burr-Brown 10 МОм в худшем случае.

На рис. 2 показано электрическую модель измерительного канала в программной среде Elektronik Workbench, где:

I_1 – источник тока инициализации ($I_0 = 1 \text{ мА}$);

R_1 – резистор, который моделирует выходное сопротивление источника тока I_1 ;

K_1, K_2, K_3 – аналоговый демultipлексор, который переключает ток инициализации источника тока I_1 между образцовыми и измерительными резистивными поделками тока;

R_2, R_3 – делитель тока, который образуется резистором R_2 , меняется в зависимости от измеряемого давления в пределах от 7500 Ом до 7537,5 Ом, и образцовым резистором R_3 , равный начальному значению сопротивления тензодатчика, то есть 7500 Ом;

R_4, R_5 – делитель тока, который образуется резистором R_4 , равный максимальному сопротивлению тензодатчика ($R_4 = 7537,5 \text{ Ом}$), и резистором R_5 , равной начальному значению сопротивления тензодатчика ($R_5 = 7500 \text{ Ом}$);

R_6, R_7 – делитель тока, который имитирует нулевой разбаланс тензомоста ($R_6 = R_7 = 7500 \text{ Ом}$);

R_8, R_9 – опоры параллельных каналов мультимплексора в замкнутом состоянии ключа дифференциального аналогового мультимплексора.

Для мультимплексора типа MAX 307 $R_8 = 95 \text{ Ом}$, $R_9 = 100 \text{ Ом}$.

R_{10}, R_{11}, C_1 – цепь, корректирующая коррелированную часть шумов на входе операционных усилителей в DA_1 и DA_2 , которая идентич-

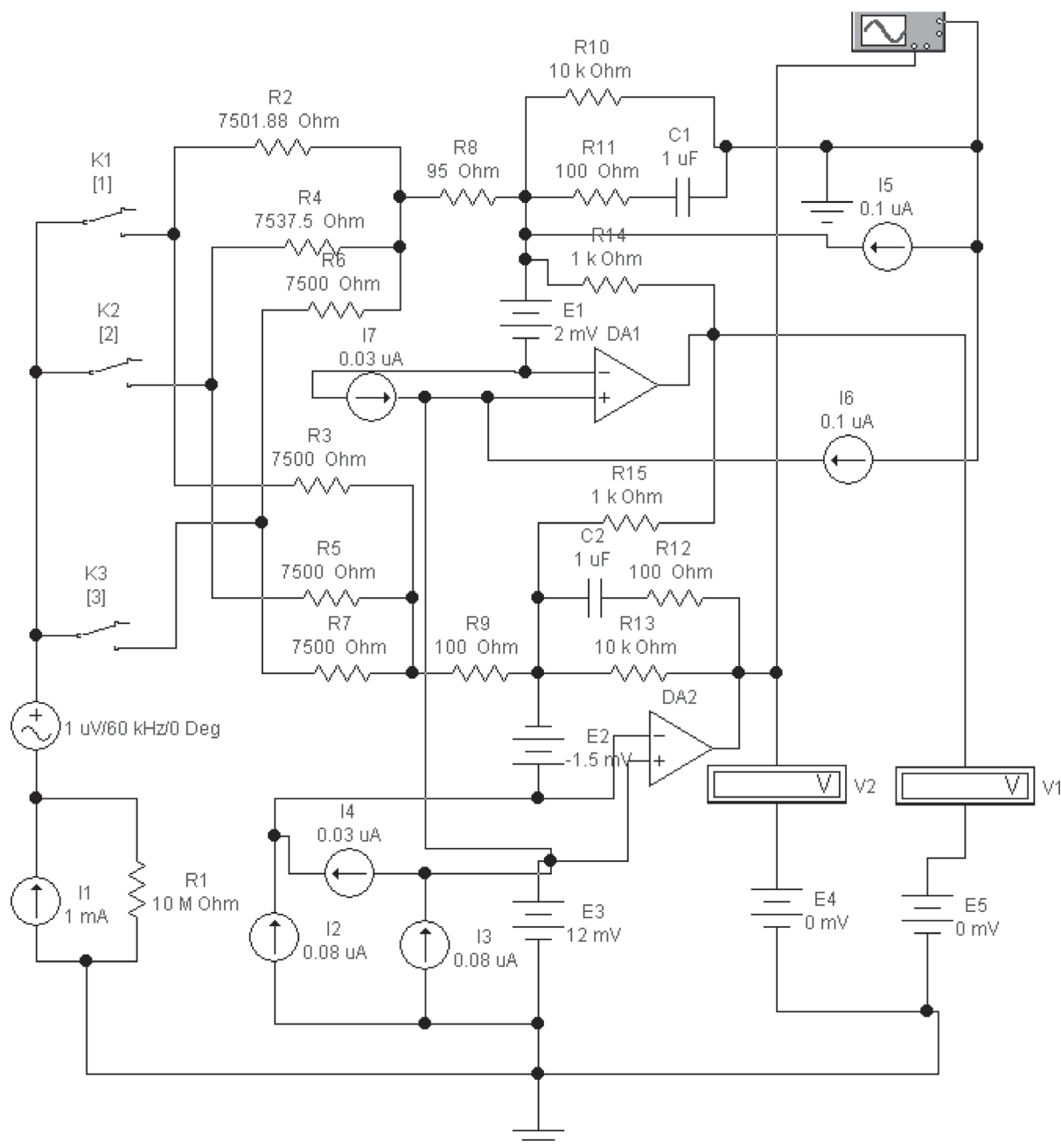


Рис. 2. Электрическая модель измерительного канала в программной среде Electronic Workbench

на цепи отрицательной обратной связи (R_{12} , R_{13} , C_2) инвертирующего сумматора на операционном усилителе DA_2 , также выполняет роль ограничителя полосы частот полезного сигнала на уровне 16 Гц;

$$C_1 = C_2 = 1 \text{ мкФ},$$

$$R_{10} = R_{11} = R_{12} = R_{13} = 10 \text{ кОм};$$

R_{14} , R_{15} – резисторы инвертора тока, выполненного на операционном усилителе DA_1 ;

$$R_{14} = R_{15} = 1 \text{ кОм}.$$

Измерительный усилитель с дифференциально – токовыми входами состоит из инверто-

ра тока (DA_1 , R_{14} , R_{15}) и инвертирующего сумматора (DA_2 , R_{13} , C_2 , R_{12}). (DA_1 , R_{14} , R_{15}).

E_1 – напряжение смещения нуля операционного усилителя DA_1 . $E_1 = +2 \text{ мВ}$ согласно технических характеристик МА 741.

E_2 – напряжение смещения нуля операционного усилителя DA_2 . $E_1 = +1,5 \text{ мВ}$ как наилучшее значение неидентичности напряжения смещения E_1 (порядка 20%).

E_3 – моделирование «синфазного» напряжения по земляному контуру. Принимаем $E_3 = 12 \text{ мВ}$.

Результаты моделирования измерительного канала

Рд, [Ом]	$\Delta\delta$	δ	U_{11} , мВ	U_{12} , мкВ	U_{21} , мВ	U_{22} , мВ	U_{31} , мВ	U_{32} , мВ	U_{41} , мВ	U_{42} , мВ
7500,000	0	0	13,2	0,2	-486,7	-1,928	-485,5	-25,9	-486,7	-1,928
7501,875	0,025	0,024686	13,2	0,2	-486,6	-3,114	-485,5	-25,9	-486,7	-1,928
7503,750	0,050	0,024816	13,2	0,2	-485,6	-3,114	-485,5	-25,9	-486,7	-1,928
7505,625	0,075	0,075022	13,2	0,2	-486,5	-5,532	-485,5	-25,9	-486,7	-1,928
7507,500	0,100	0,075022	13,2	0,2	-486,5	-5,532	-485,5	-25,9	-486,7	-1,928
7509,375	0,125	0,125025	13,2	0,2	-486,4	-7,933	-485,5	-25,9	-486,7	-1,928
7511,250	0,150	0,150042	13,2	0,2	-486,3	-9,133	-485,5	-25,9	-486,7	-1,928
7513,125	0,175	0,174964	13,2	0,2	-486,3	-10,33	-485,5	-25,9	-486,7	-1,928
7515,000	0,200	0,199996	13,2	0,2	-486,2	-11,53	-485,5	-25,9	-486,7	-1,928
7516,875	0,225	0,224985	13,2	0,2	-486,2	-12,73	-485,5	-25,9	-486,7	-1,928
7518,750	0,250	0,250033	13,2	0,2	-486,1	-13,93	-485,5	-25,9	-486,7	-1,928
7520,625	0,275	0,27509	13,2	0,2	-486,0	-15,13	-485,5	-25,9	-486,7	-1,928
7522,500	0,300	0,30009	13,2	0,2	-486,0	-16,33	-485,5	-25,9	-486,7	-1,928
7524,375	0,325	0,324954	13,2	0,2	-485,9	-17,52	-485,5	-25,9	-486,7	-1,928
7526,250	0,350	0,349958	13,2	0,2	-485,9	-18,72	-485,5	-25,9	-486,7	-1,928
7528,125	0,375	0,375045	13,2	0,2	-485,8	-19,92	-485,5	-25,9	-486,7	-1,928
7530,000	0,400	0,400143	13,2	0,2	-485,7	-21,12	-485,5	-25,9	-486,7	-1,928
7531,875	0,425	0,424949	13,2	0,2	-485,7	-22,31	-485,5	-25,9	-486,7	-1,928
7533,750	0,450	0,450062	13,2	0,2	-485,6	-23,51	-485,5	-25,9	-486,7	-1,928
7535,625	0,475	0,475081	13,2	0,2	-485,6	-24,71	-485,5	-25,9	-486,7	-1,928
7537,500	0,500	0,501877	13,2	0,2	-485,5	-25,99	-485,5	-25,9	-486,7	-1,927

I_2, I_3 – токи смещения нуля операционного усилителя DA_2 . $I_2 = I_3 = 80$ нА согласно технических характеристик МА 741.

I_4 – разница токов смещения нуля операционного усилителя DA_2 . $I_4 = -30$ нА согласно технических характеристик МА 741.

I_5, I_6 – токи смещения нуля операционного усилителя DA_1 . $I_5 = I_6 = 100$ нА согласно технических характеристик МА 741.

I_7 – разница токов смещения нуля операционного усилителя DA_1 . $I_7 = +30$ нА как худший расбаланс по токах смещения.

При таких значениях аддитивных погрешностей операционных усилителей (максимально возможных) соотношение С / Ш на выходе измерительного усилителя будет составлять около 10 децибел. Это свидетельствует о том, что помеха имеет весомый вклад.

V_2 – вольтметр на выходе измерительного усилителя.

V_1 – вольтметр на выходе операционного усилителя DA_1 .

E_4, E_5 – источники напряжений для внедрения дифференцированного метода измерения выходных напряжений операционных усилителей соответственно DA_1 та DA_2 , что позволяет уменьшить влияние погрешности квантования.

Другие параметры операционных усилителей DA_1 и DA_2 были взяты из технических характеристик МА 741 по типовым значениям.

В таблице приведены результаты моделирования измерительного канала для 21 значения сопротивления резистивного полупроводникового тензодатчика высокотемпературного на основе карбида кремния при $\kappa = 5$ и начальном сопротивлении датчика $R_{d0} = 7,5$ кОм. Параметры OU_1 выбраны следующими:

- ток смещения 100 нА;
- разница токов смещения +30 нА;
- напряжение смещения нуля +2 мВ;
- входное сопротивление 1 МОм.

Параметры OP_2 выбраны следующими:

- ток смещения 80 нА;
- разница токов смещения -30 нА;
- напряжение смещения нуля +1,5 мВ;
- входное сопротивление 1 МОм.

Используя программную среду NUMERY, было определено регрессионное уравнение функции преобразования измерительного канала, что позволило определить систематические и случайные составляющие погрешности измерительного канала без учета погрешностей датчика.

Тогда регрессионное уравнение функции преобразования измерительного канала первого порядка будет иметь следующий вид:

$$\begin{cases} y = a_0 + a_1x + a_2x^2, \\ a_0 = -6,95 \cdot 10^{-6}, \\ a_1 = 1,000163, \\ a_2 = 0,00007, \\ \sum \delta_{\text{нев}}^2 = 9,48 \cdot 10^{-8}, \end{cases} \quad (2)$$

где y – выходной сигнал на выходе измерительного усилителя; a_0, a_1, a_2 – коэффициенты регрессии; x – текущее значение входной измеряемой величины; $\sum \delta_{\text{нев}}^2$ – сумма квадратов

невязок между текущим значением выходной величины и ее математическим ожиданием.

Заключение

Из приведенного анализа результатов моделирования установлено, что доминировать будет случайная аддитивная составляющая погрешности. Поскольку при моделировании единственной случайной составляющей погрешности является погрешность квантования, то использование дифференциального метода измерения выходного напряжения существенно улучшит метрологические характеристики.

ЛИТЕРАТУРА

1. Аш Дж. Датчики измерительных систем: в 2-х книгах. Кн. 1. / пер. с франц. / [Текст] / Дж. Аш – М.: Мир, 1992. – 480 с.
2. L. V. Kuzmich, Y. S. Tsekhmaystruk. Modern state of mechanical deformation measurement of complex technical systems [electronic resource] / Materials of the XIII international scientific and technical conference «AVIA – 2017». – Mode of access to the site: <http://avia.nau.edu.ua/avia2017/>.
3. L. Kuzmych; O. Kobylanskyi; M. Duk. Current state of tools and methods of control of deformations and mechanical stresses of complex technical systems. Proc. SPIE 10808, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2018, 108085J (1 October 2018); doi: 10.1117/12.2501661
4. L. Kuzmych, V. Kvasnikov. Study of the durability of reinforced concrete structures of engineering buildings. Advances in Intelligent Systems and Computing Volume 543, 2017, Pages 659–663 International Conference on Systems, Control and Information Technologies, SCIT 2016; Warsaw; Poland; 20 May 2016 through 21 May 2016; Code 187699.
5. Куликовский К. Л., Купер В. Я. Методы и средства измерений [Текст] / К. Л. Куликовский. – М.: Энергоатомиздат, 1986. – 448 с.
6. Digital's Kompensation sverfahren zur Verbesserung von Messfuhlern. Erb. K., Fisher P. «Bulletin SEV/VSE», 1989, 80, № 7, 8, 365–368.
7. National Instruments, SCXI Universal Strain Grade Input: SCXI-1540. – [Электронный ресурс] – Режим доступа: http://www.ni.com/pdf/products/us/4scxisc293_ETC_196.pdf.
8. SCXI-1126. User Manual. Eight-Channel Isolated Frequency Input Module for Signal Conditioning. National Instruments Corporation. 1998–2003.
9. Field Wiring and Noise Considerations for Analog Signals [Electronic resource] / Publish Date: Mar 11, 2014. – Available at: <http://www.ni.com/white-paper/3344/en/>
10. Классен К. Б. Основы измерений. Электронные методы и приборы в измерительной технике [Текст] / К. Б. Классен. – М.: Постмаркет, 2000. – 352 с.
11. Ункзер, Дж. Соединяемость: интеллектуальные датчики или интеллектуальные интерфейсы [Текст] / Дж. Ункзер // Датчики и системы. – 2002. – № 10. – С. 50–55.
12. Rus, G. Optimized damage detection of steel plates from noisy impact test [Text] / G. Rus, S. Y. Lee, S. Y. Chang, S. C. Wooh // International Journal for Numerical Methods in Engineering. – 2006. – Vol. 68, Issue 7. – P. 707–727. doi: 10.1002/nme.1720.
13. Harada, T. Droplet generation using a torsional Langevin-type transducer and a micropore plate [Text] / T. Harada, N. Ishikawa, T. Kanda, K. Suzumori, Y. Yamada, K. Sotowa // Sensors and Actuators A: Physical. – 2009. – Vol. 155, Issue 1. – P. 168–174. doi: 10.1016/j.sna.2009.08.007.
14. Патент на полезную модель № 109796, кл. G01R21/00, 2016, Бюл. № 17.
15. Schroder, A. Evaluation of cost functions for FEA based transducer optimization [Text] / A. Schroder, J. Rautenberg, B. Henning // Physics Procedia. – 2010. – Vol. 3, Issue 1. – P. 10031009. doi: 10.1016/j.phpro.2010.01.129.

REFERENCES

1. Ash J. Datchiki izmeritelnih sistem: v 2 knigah. Kn.1. – М.: Mir, 1992. – 480 p.
1. L. V. Kuzmich, Y. S. Tsekhmaystruk. Modern state of mechanical deformation measurement of complex technical systems [electronic resource] / Materials of the XIII international scientific and technical conference «AVIA – 2017». – Mode of access to the site: <http://avia.nau.edu.ua/avia2017/>.
2. L. Kuzmych; O. Kobylanskyi; M. Duk. Current state of tools and methods of control of deformations and mechanical stresses of complex technical systems. Proc. SPIE 10808, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2018, 108085J (1 October 2018); doi: 10.1117/12.2501661.

3. **L. Kuzmych, V. Kvasnikov.** Study of the durability of reinforced concrete structures of engineering buildings. *Advances in Intelligent Systems and Computing* Volume 543, 2017, Pages 659–663 International Conference on Systems, Control and Information Technologies, SCIT 2016; Warsaw; Poland; 20 May 2016 through 21 May 2016; Code 187699.
4. **Kulikovskiy K. L., Kuper V. Y.** *Metody i sredstva izmereniy.* – M. Energoatomizdat, 1986. – 448 p.
5. **Digital's** Kompensation sverfahren zur Verbesserung von Messfuhlern. Erb. K., Fisher P. «Bulletin SEV/VSE», 1989, 80, № 7, 8, 365–368.
6. **National Instruments,** SCXI Universal Strain Grade Input: SCXI-1540. – [Электронный ресурс] – Режим доступа: http://www.ni.com/pdf/products/us/4scxisc293_ETC_196.pdf.
7. **SCXI-1126.** User Manual. Eight-Channel Isolated Frequency Input Module for Signal Conditioning. National Instruments Corporation. 1998–2003.
8. **Field Wiring and Noise Considerations for Analog Signals** [Electronic resource] / Publish Date: Mar 11, 2014. – Available at: <http://www.ni.com/white-paper/3344/en/>
9. **Klassen K. B.** *Osnovy izmereniy. Elektronnye metody i pribory v izmeritelnoy tehnike.* M.: Postmarket, 2000. – 352 p.
10. **Uikzer J.** Soedinyayemost: intellektualnye datchiki ili intellektualnye interfeisy // *Datchiki i sistemy.* – 2002. № 10. – P. 50–55.
11. **Rus, G.** Optimized damage detection of steel plates from noisy impact test [Text] / G. Rus, S. Y. Lee, S. Y. Chang, S. C. Wooh // *International Journal for Numerical Methods in Engineering.* – 2006. – Vol. 68, Issue 7. – P. 707–727. doi: 10.1002/nme.1720.
12. **Harada, T.** Droplet generation using a torsional Langevin-type transducer and a micropore plate [Text] / T. Harada, N. Ishikawa, T. Kanda, K. Suzumori, Y. Yamada, K. Sotowa // *Sensors and Actuators A: Physical.* – 2009. – Vol. 155, Issue 1. – P. 168–174. doi: 10.1016/j.sna.2009.08.007.
13. **Patent № 109796, G 01R21/00, 2016, Bul. № 17.**
14. **Schroder, A.** Evaluation of cost functions for FEA based transducer optimization [Text] / A. Schroder, J. Rautenberg, B. Henning // *Physics Procedia.* – 2010. – Vol. 3, Issue 1. – P. 10031009. doi: 10.1016/j.phpro.2010.01.129.

Поступила
08.12.2018

После доработки
21.06.2019

Принята к печати
01.07.2019

KUZMYCH L. V., ORNATSKYI D. P., KVASNIKOV V. P.

SIMULATION OF THE ANALOGUE INTERFACE FOR REMOTE MEASUREMENTS

This work is aimed at finding possibilities for increasing the accuracy of measurements and interfering analog interfaces for remote measurements using resistive strain gauges by introducing a new structural scheme, which is shown on the Fig. 1. It shows us the Schematic of the electrical functional analog interface for remote measurement using multiplexer and resistive strain gauges, which contains a measuring chain, a transmitter; the input of which is connected to a DC source through an analog demultiplexer; and the outputs of the measuring chain through the analog multiplexer are connected to the measuring amplifier, and a two-channel analog-digital converter with simultaneous sampling. The measuring chain is made in the form of three resistive current dividers, where one divider is formed by a resistive strain gauge and adjusting resistor, and two others – exemplary resistors.

By introducing a new structural scheme, it will be possible to increase the accuracy of measurements and impedance of analog interfaces for remote measurements using resistive strain gauges. In this case, unlike the classical method of model measures, this method is distinguished by the «indistinguishability» of the measuring line, which makes it possible to compensate for a greater number of influential factors, in particular, the correlated noise of operational amplifiers and noise caused by the presence of the overall ground loop, the resistance of analogue switches and lines of communication.

At the Fig. 2 we can see the electric model of the measuring channel in the software Elektronik Workbench.

From the analysis of the simulation results it was found that the random additive component of the error would dominate. Since in the simulation of the only random component of the error there is a quantization error, the use of the differential method of measuring the output voltage will significantly improve the metrological characteristics.

Keywords: analogue interface, demultiplexer, measuring amplifier, converter, strain gauge.

**Кузьмич Людмила Владимировна**

к. т. н., доцент, докторант кафедры компьютеризированных электротехнических систем и технологий, Национальный авиационный университет.

E-mail: klv@nau.edu.ua.

<https://orcid.org/0000-0003-0727-0508>.

Lyudmyla Kuzmych

PhD, Associate Professor, Postdoctoral Fellow of the Department of the computerized electrotechnical systems and technologies, National Aviation University.

**Орнатский Дмитрий Петрович**

д. т. н., профессор, заведующий кафедрой информационно – измерительных систем, Национальный авиационный университет.

E-mail: odp@nau.edu.ua.

Dmytro Ornatskyi

Doctor of Science, Professor, Professor, Head of the Department of Information and Measurement Systems, National Aviation University.

**Квасников Владимир Павлович**

д. т. н., профессор, Заслуженный метролог Украины, заведующий кафедрой компьютеризированных электротехнических систем и технологий, Национальный авиационный университет,

E-mail: kvp@nau.edu.ua.

Volodymyr Kvasnikov

Doctor of Science, Professor, Honored Metrologist of Ukraine, Head of the Department of the computerized electrotechnical systems and technologies, National Aviation University.

ЗАЩИТА ИНФОРМАЦИИ

INFORMATION SECURITY

В. Ф. ГОЛИКОВ, М. Л. РАДЮКЕВИЧ

ФОРМИРОВАНИЕ ОБЩЕГО СЕКРЕТА С ПОМОЩЬЮ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Белорусский национальный технический университет
Научно-производственное республиканское унитарное предприятие
«Научно-исследовательский институт технической защиты информации»

В работах [1–3] предлагается использование двух синхронизируемых искусственных нейронных сетей (ИНС), соединенных открытым каналом связи для конфиденциального формирования общего криптографического ключа. В [3] рассматриваются возможности по формированию такого же ключа третьей стороной, прослушивающей канал связи и синхронизирующей свою сеть. Вместе с тем, остаются мало исследованными вопросы практической пригодности данной технологии для ответственных криптографических приложений. Отсутствуют рекомендации по выбору параметров используемых сетей, обеспечения приемлемого быстродействия и гарантированной конфиденциальности сформированного общего секрета.

В связи с этим представляет интерес обоснование рациональных значений параметров ИНС с точки зрения криптографических требований и анализ безопасности предлагаемого способа формирования криптографических ключей.

Ключевые слова: синхронизируемые искусственные нейронные сети, атака, общий криптографический ключ, параметры искусственных нейронных сетей.

Введение

Абоненты A и B , имеют идентичные ИНС, соединенные открытым каналом связи [1, 2] (рис. 1). Каждая ИНС, состоит из одного слоя персептронов. Каждый персептрон имеет n входов и прямоугольную функцию активации σ^* (рис. 2).

До начала синхронизации абоненты A и B независимо друг от друга формируют вектор весовых коэффициентов (BK)

$$\vec{w}^A = wa_{11}, wa_{12}, \dots, wa_{1n}, wa_{21}, wa_{22}, \dots, wa_{2n}, \dots, wa_{K1}, wa_{K2}, \dots, wa_{Kn}, \quad (1)$$

$$\vec{w}^B = wb_{11}, wb_{12}, \dots, wb_{1n}, wb_{21}, wb_{22}, \dots, wb_{2n}, \dots, wb_{K1}, wb_{K2}, \dots, wb_{Kn}, \quad (2)$$

где $wa_{ij}, wb_{ij} \in [-L, L], i = 1, 2, \dots, K; j = 1, 2, \dots, n; L$ – целое число.

Каждый элемент этих векторов w_{ij} есть случайное целое число с дискретным равномерным законом распределения (рис. 3)

$$P(w_{ij} = s_{ij}) = \frac{1}{2L+1},$$

где $s_{ij} = -L, -L+1, \dots, -1, 0, 1, \dots, L-1, L$.

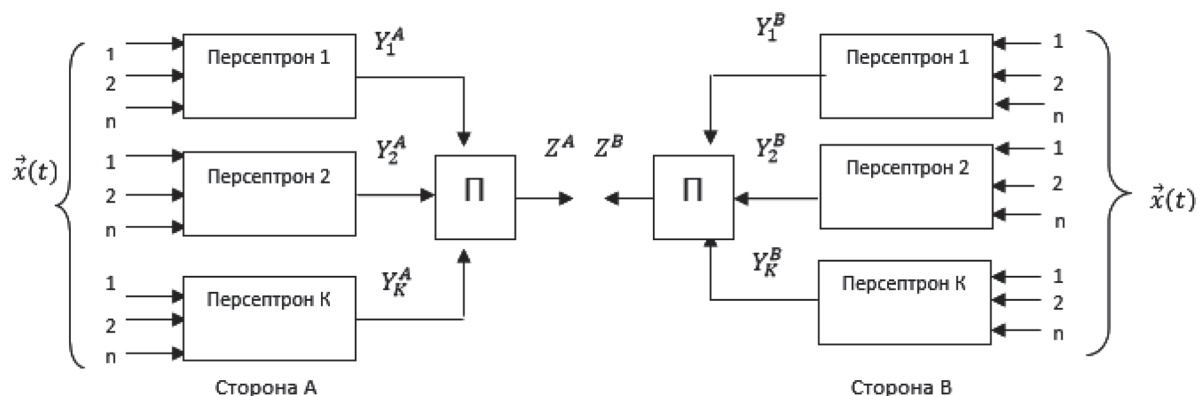


Рис. 1. Синхронизируемые ИНС

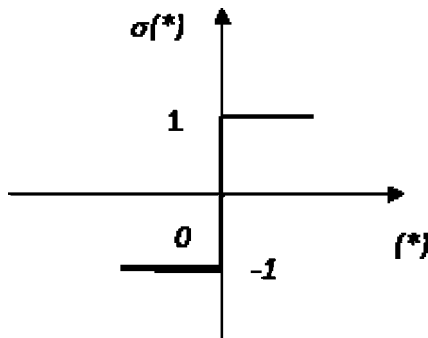


Рис. 2. Функция активации

Каждый шаг синхронизации начинается с подачи на входы обеих сетей выбранного случайным образом вектора

$$\vec{x}(t) = x_{11}, x_{12}, \dots, x_{1n}, x_{21}, x_{22}, \dots, x_{2n}, \dots, x_{K1}, x_{K2}, \dots, x_{Kn}, \quad (3)$$

где $x_{ij} \in [-1, 1]$ – дискретная случайная величина с равномерным распределением, $t = 1, 2, \dots$ – номер такта (далее все рассматриваемые величины зависят от t , но для упрощения записи эта зависимость в обозначениях отсутствует).

Для каждого персептрона выходная величина равна

$$Y_i^{A/B} = \sigma \left(\sum_{j=1}^n w_{ij}^{A/B} x_{ij} \right) \quad (4)$$

Индекс A/B означает, что операция касается обеих сетей A и B , а единичный индекс – что операция касается одной сети соответственно. Функция активации $\sigma(*)$ имеет вид

$$\sigma(*) = \begin{cases} 1, & \sigma(*) \geq 0, \\ -1, & \sigma(*) < 0. \end{cases} \quad (5)$$

Затем вычисляется выходная величина Z для каждой из сетей

$$Z^{A/B} = \prod_{i=1}^K Y_i^{A/B} = \prod_{i=1}^K \sigma \left(\sum_{j=1}^n w_{ij}^{A/B} x_{ij} \right) \quad (6)$$

На основании сравнения обоих полученных выходных величин реализован процесс синхронизации. Коррекция векторов весов обеих сетей происходит только тогда, когда обе выходные величины равны друг другу ($Z^A = Z^B$). Внутри данной сети корректируются веса только тех персептронов, выходная величина которых равна величине Z всей сети. Процесс коррекции идет по правилу Хэбба

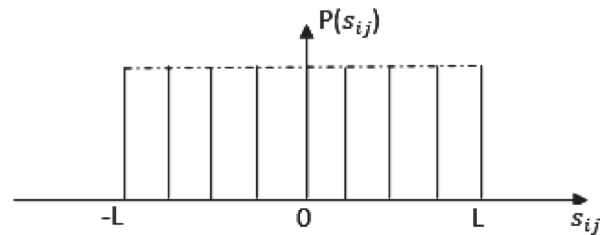


Рис. 3. Закон распределения начальных значений весовых коэффициентов

$$w_{ij}^{A/B} = \begin{cases} w_{ij}^{A/B} + Z^{A/B} x_{ij}, & \text{если } Z^A = Z^B \text{ и } Z^{A/B} = Y_i^{A/B}, \\ w_{ij}^{A/B}, & \text{в противном случае.} \end{cases}$$

Кроме того, учитывается ограничение $w_{ij}^{A/B} \in [-L, L]$

$$w_{ij}^{A/B} = \begin{cases} \pm L, & \text{если } |w_{ij}^{A/B}| > L, \\ w_{ij}^{A/B}, & \text{в противном случае.} \end{cases}$$

Процесс синхронизации продолжается до полного совпадения векторов $\vec{w}^a, \vec{w}^b$, после чего абоненты A и B имеют общую секретную информацию, представляющую собой последовательность десятичных чисел вида

$$\vec{w}^{A/B} = w_{11}, w_{12}, \dots, w_{1n}, w_{21}, w_{22}, \dots, w_{2n}, \dots, w_{K1}, w_{K2}, \dots, w_{Kn}. \quad (7)$$

Общее секретное число можно сформировать из (7), например, как конкатенацию значений ВК

$$S = w_{11} \| w_{12} \| \dots \| w_{1n} \| w_{21} \| w_{22} \| \dots \| w_{2n} \| \dots \| w_{K1} \| w_{K2} \| \dots \| w_{Kn}. \quad (8)$$

1. Статистические закономерности процесса синхронизации

1.1. Неопределенность момента наступления полной синхронизации

В процессе синхронизации ИНС обмениваются через открытый канал связи только выходными величинами сетей $Z^{A/B}$, поэтому не знают равны ли ВК их сетей или нет. Следовательно, они не знают, нужно ли им продолжать цикл синхронизации или можно остановиться.

Неопределенность относительно наступления полной синхронизации ВК для абонентов приводит к тому, что процесс синхронизации может продолжаться уже после выравнивания

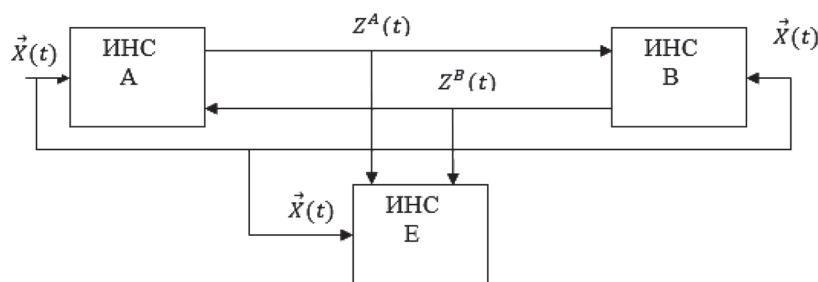


Рис. 4. Схема взаимодействия сетей: t – номер такта синхронизации, $\vec{X}(t)$ – вектор синхронизирующих случайных воздействий, $Z^A(t)$, $Z^B(t)$ – выходные величины сетей А и В соответственно

ВК. Это с одной стороны увеличивает время формирования общего ключа и повышает шансы злоумышленника на реализацию возможных атак [3], с другой – могут иметь место случаи преждевременной остановки процесса синхронизации. В [4] предложен способ определения момента наступления полной синхронизации, основанный на том, что после наступления полной синхронизации выходные величины сетей всегда равны. Поэтому, если в процессе синхронизации наблюдается длительное равенство выходных величин сетей, то есть основания полагать о наступлении полной синхронизации. Экспериментальное исследование, приведенное с помощью имитационной модели [4], показало, что в процессе синхронизации пока $\vec{w}^A(t) \neq \vec{w}^B(t)$, наблюдаются такты, в которых $Z^A(t) \neq Z^B(t)$, и такты, в которых $Z^A(t) = Z^B(t)$. Действительно, как показали эксперименты, довольно часто встречаются отрезки тактов длиной до нескольких сотен и более совпадений $Z^A(t) = Z^B(t)$, однако синхронизация еще не достигнута. Таким образом, решение этой задачи носит вероятностный характер и базируется на результатах имитационного моделирования. Так или иначе, но процесс формирования общего ключа должен заканчиваться сравнением $\vec{w}^A(t_c)$ и $\vec{w}^B(t_c)$, чтобы А и В были уверены в идентичности полученных результатов. Эта процедура может выполняться с применением хэширования, т. е. сравниваются хэш-значения векторов $h[\vec{w}^A(t_c)]$ и $h[\vec{w}^B(t_c)]$ или шифрованием и расшифрованием отрывка текста, с использованием в качестве ключей вышеуказанных векторов.

Наряду с проблемой своевременной остановки процесса синхронизации существует проблема выбора параметров СИНС: K , n , L . Выбор этих параметров необходимо произвести исходя из криптографических соображений, имея ввиду конфиденциальность сфор-

мированного ключа и время формирования т. е. количество тактов синхронизации, потраченных на это. Поскольку эти характеристики зависят [3] от параметров сетей и моделей поведения третьей стороны E , пытающейся узнать значение ключа, то далее следует рассмотреть статистические закономерности процесса синхронизации при наличии криптоаналитика E .

1.2. Модели поведения криптоаналитика

Рассмотрим основные известные атаки на формируемый ключ со стороны третьей стороны, «прослушивающей» канал связи, по которому синхронизируемые сети обмениваются информацией.

Схема взаимодействия сетей абонентов и криптоаналитика представлена на рис. 4.

Архитектура и параметры всех сетей идентичны (рис. 1).

1.2.1. Силовая атака

Силовая атака, также известная как полный перебор – метод взлома, являющийся самым универсальным, однако и самым долгим. Относится к классу методов поиска решения исчерпыванием всевозможных вариантов. Сложность полного перебора зависит от количества всех возможных значений формируемого ключа.

Для того чтобы оценить эффективность силовой атаки, необходимо рассчитать количество всевозможных значений всей совокупности весовых коэффициентов. Всевозможное количество значений рассчитывается по формуле:

$$n = (2L + 1)^{n \cdot K} \quad (9)$$

Для количественной оценки выберем нейросеть с параметрами $n = 25$, $K = 3$, $L = 8$. Подставляя соответствующие значения в формулу, получим количество комбинаций, равное

$1,9 \cdot 10^{92}$. При скорости перебора, равной 1 миллиарду комбинаций в секунду, на полный перебор всех комбинаций уйдет $6,02 \cdot 10^{75}$ лет, что намного больше предположительного времени актуальности зашифрованной информации. Из этого следует, что данный метод не подходит для взлома, даже при относительно небольших значениях параметров сети.

1.2.2. Простая атака

При простой атаке для взлома ключа криптоаналитику необходимо иметь свою собственную нейросеть, имеющую такую же структуру, как и сети легитимных абонентов.

При начале сеанса выработки ключа криптоаналитик подключает свою сеть к каналу связи, и, при помощи перехватываемых векторов синхронизирующих случайных воздействий и выходных величин сетей A и B , обучает сеть E по следующим правилам обучения:

1) Если сети A и B получили разные выходные величины ($Z^A \neq Z^B$), то сеть E не меняет своих весов.

2) Если сети легитимных пользователей получили одинаковые выходные величины ($Z^A = Z^B$) и к тому же выходная величина оппонента E равна выходным величинам наблюдаемых сетей ($Z^A = Z^B = Z^E$), то сеть E производит коррекцию своих ВК.

3) Если выходы обеих сетей согласованы ($Z^A = Z^B$), а криптоаналитик E получает другую выходную величину ($Z^A = Z^B \neq Z^E$), то сеть E пропускает коррекцию, так как ее пропускают сети A и B .

Это приводит к тому, что количество коррекций сети E оказывается меньше, чем количество коррекций ИНС у A и B и это приводит к задержке в процессе обучения сети оппонента относительно времени синхронизации наблюдаемых сетей. Это отставание является главным элементом безопасности процесса синхронизации. Если процесс синхронизации завершится на довольно раннем этапе, то оппонент будет не в состоянии синхронизировать свои вектора весов с наблюдаемыми сетями. Следовательно, чем больше эта задержка, тем выше уровень безопасности.

1.2.3. Геометрическая атака

Для ослабления эффекта отставания в количестве коррекций применяется атака под на-

званием геометрическая. При возникновении случая 3, т. е. при ($Z^A = Z^B \neq Z^E$), делается предварительная коррекция, выходной величины того персептрона сети E , у которого величина $\sum w_{ij}^E x_{ij}$ наименьшая по абсолютному значению.¹ Это приводит к изменению знака выбранного персептрона на противоположный, аналогично и знака всей сети, что переводит сеть в случай 2. Эффективность такой атаки в среднем выше чем эффективность простой атаки, поэтому в дальнейшем будем считать основной моделью поведения E .

1.3. Конфиденциальность сформированного общего ключа

Так как процессы синхронизации, протекающие в рассматриваемых сетях, являются случайными, то и исследование должно проводиться с использованием математических вероятностных моделей.

Обозначим количество назначенных тактов синхронизации через d , количество фактических тактов синхронизации до достижения равенства ВК сетей A и B через t_{AB} , а сетей A и E через t_{AE} . Величины t_{AB} и t_{AE} – дискретные случайные величины, законы распределения которых зависят от параметров сетей L , n , K . В некоторых источниках, например [5], для оценки уровня безопасности процесса синхронизации в рассматривается параметр, названный коэффициентом безопасности $r = T_{AE} / T_{AB}$, где T_{AB} – среднее время до полной синхронизации сетей A и B , T_{AE} – среднее время до полной синхронизации сетей A и E . С помощью этого параметра можно проследить тенденцию зависимости безопасности от параметров сети. Однако для криптографических применений важна не безопасность в среднем, а конкретно в каждом сеансе формирования, поэтому далее рассматриваются другие критерии.

В процессе синхронизации могут произойти следующие события:

1. Сети A и B достигли синхронизма (их веса стали равны друг другу), E смог обучить свою сеть. Для этого события выражение вероятности запишется в виде $P(t_{AB} \leq d, t_{AE} \leq d)$. Это событие является неблагоприятным, так как сформированный ключ сразу дискредитируется.

2. Сети A и B достигли синхронизма, E не успел обучить свою сеть. Для этого события

выражение вероятности запишется в виде $P(t_{AB} \leq d, t_{AE} > d)$. Это событие является благоприятным, так как ключ был сформирован и не дискредитирован.

Остальные события нас не интересуют, так как в случае их наступления A и B не достигают синхронизма, следовательно, ключ не будет сформирован.

Вероятность сложного события $(t_{AB} \leq d, t_{AE} \leq d)$, пренебрегая взаимосвязью частных событий можно представить следующим образом:

$$\begin{aligned} P(t_{AB} \leq d, t_{AE} \leq d) &= \\ &= P(t_{AB} \leq d)P(t_{AE} \leq d / t_{AB} \leq d) \approx \\ &\approx P(t_{AB} \leq d)P(t_{AE} \leq d). \end{aligned} \quad (10)$$

По аналогии преобразуется выражение $P(t_{AB} \leq d, t_{AE} > d)$. Данные преобразования позволяют нам перейти к одномерным вероятностям, что упрощает расчетную часть.

Исходя из выше описанных правил, задача анализа безопасности сводится к расчету вероятности удачной синхронизации сетей A и B ($P(t_{AB} \leq d)$), а также удачной либо неудачной попытки обучения сети E ($P(t_{AE} \leq d), P(t_{AE} > d)$) при выбранных значениях d .

Аналитический расчет этих вероятностей не представляется возможным из-за высокой сложности. Поэтому расчет проводился методом статистического моделирования. Для этого была разработана программная модель СИНС и сети криптоаналитика E . С помощью этой модели была имитирована реальная синхронизация. Повторяя этот процесс многократно, вычислены статистические значения искомых вероятностей для различных параметров сетей.

Исследования показали, что независимо от вида атаки обеспечивается

$$P(t_{AB} \leq d) > P(t_{AE} \leq d) \quad (11)$$

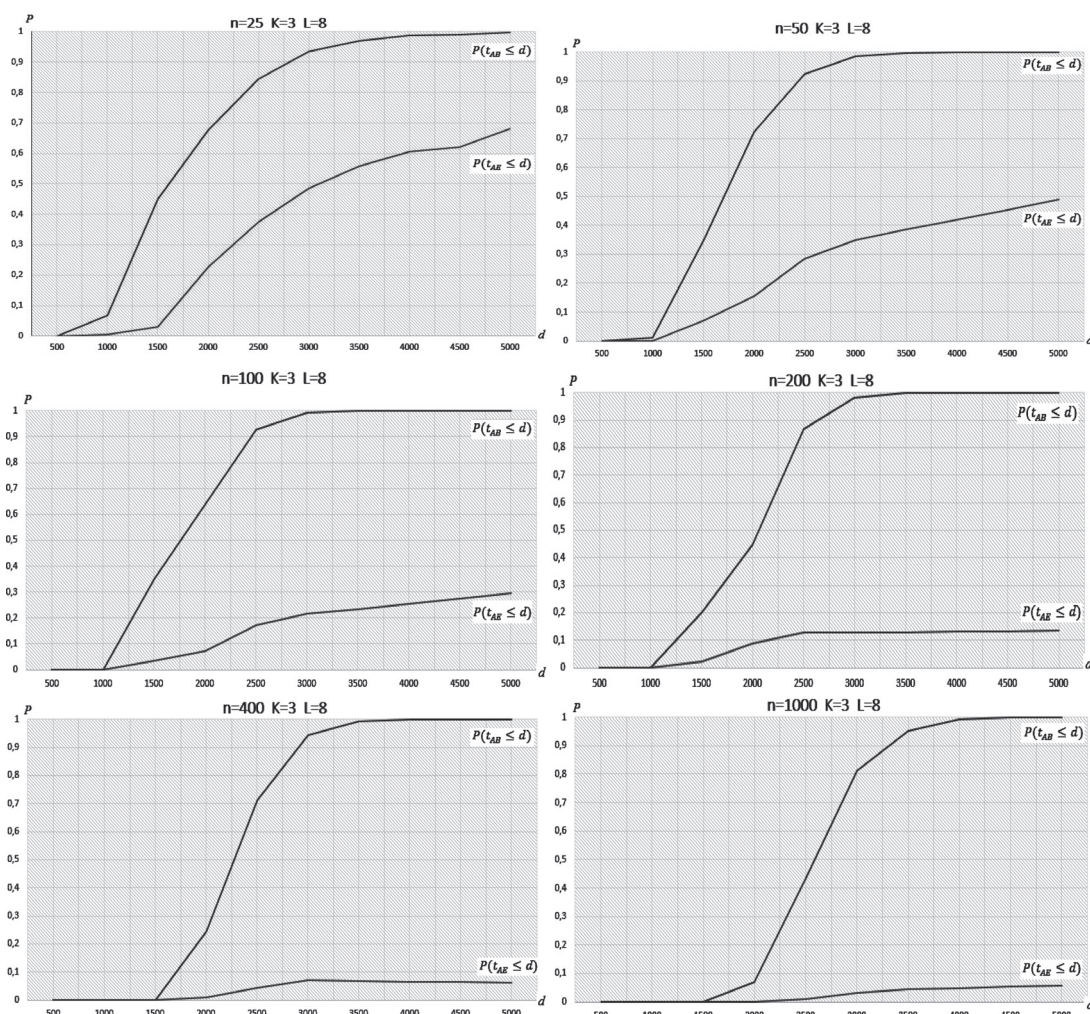


Рис. 5. Результаты имитационного моделирования

Выражение (11), однако, совсем не означает, что в процессе атаки обязательно произойдет событие $t_{AB} \leq d \leq t_{AE}$. Т. е. могут иметь место успешные атаки, при которых окажется $t_{AE} \leq t_{AB} \leq d$. С наличием таких реализаций и связаны основные сомнения в безопасности анализируемого метода открытого формирования общего секрета.

На рис. 5 приведены вероятности $P(t_{AE} \leq d)$, полученные методом имитационного моделирования при некоторых значениях параметров сетей. Анализируя результаты моделирования, полученные авторами статьи и другими исследователями [3], можно выявить важные закономерности, которые могут быть использованы для принятия конкретных решений.

2. Выбор параметров и обоснование структуры ИНС

Анализ результатов моделирования и работ других авторов позволяет сформулировать предложения по обоснованию структуры и параметров СИНС.

Решение этой задачи, на наш взгляд, следует начать с выбора диапазона значений ВК, который вместе с количеством входов n и числом персептронов K задает с одной стороны множество возможных значений $\bar{w}^{A/B}$, с другой сильно влияет на длительность процесса согласования ВК сетей A и B . Увеличение L приводит к увеличению множества возможных значений $\bar{w}^{A/B}$, т. е. к увеличению криптостойкости, но при этом увеличивается длительность процесса согласования ВК, т. е. снижается скорость работы алгоритма. С точки зрения обеспечения требуемой криптостойкости следует отдать предпочтение первому фактору. Поэтому величину L будем выбирать исходя из криптографических факторов.

В результате полной синхронизации A и B формируют общую последовательность десятичных чисел (8), состоящую из целых положительных и отрицательных чисел из интервала $[-L, L]$. Для использования этой последовательности чисел в качестве криптографического ключа ее следует преобразовать в бинарную.

Возникает вопрос о выборе разрядности двоичного числа при переходе от десятичного формата ВК к двоичному. Как уже указывалось выше, диапазон изменения значений де-

сятичных чисел w_{ij} задается величиной L и равен $[-L, L]$. Таким образом, количество возможных значений w_{ij} равно $2L + 1$. Двоичным числом длиной l можно описать 2^l десятичных чисел, а так как $2L + 1$ нечетное число, то точное его описание для произвольно выбранных значений L невозможно. Избыточная разрядность нежелательна, так как это приведет к избыточному количеству нулей в ключевой последовательности. Поэтому возможна следующая методика. Уменьшим количество возможных значений w_{ij} на единицу и вычислим необходимую разрядность l :

$$2L = 2^l, \text{ откуда } l = \ln(2L). \quad (12)$$

В табл. 1 приведены значения L и соответствующие значения l .

Таблица 1. Соответствие разрядности двоичного числа десятичному

L	2	4	8	16	32
l	2	3	4	5	6

Тогда таблица для перевода десятичных чисел в двоичные, например, для $L = 4$ имеет вид в табл. 2.

Таблица 2. Перевод десятичного числа в двоичное

$w_{ij(10)}$	0	1	2	3	4	-1	-2	-3	-4
$w_{ij(2)}$	000	001	010	011	100	101	110	111	—

Из последней таблицы видно, что трехразрядных чисел не хватает для замены всех десятичных чисел выбранного интервала. Замена на одно из уже используемых двоичных чисел возможна, но нежелательна, так как это нарушает равномерность распределения чисел. Лучший вариант это переход на несимметричный интервал $[L_1, L_2]$ (для рассматриваемого случая: $L_1 = -3, L_2 = 4$), но при этом нужно изменить и функцию активации, сдвинув ее вправо на единицу рис. 6.

С учетом (12) длина сформированной секретной последовательности в битах равна

$$r_{(2)} = nK \ln(2L). \quad (13)$$

Необходимую длину ключа, как следует, из (13) можно обеспечить соответствующим выбором n, K, L , учитывая при этом, что $d \leq T$, где T – допустимое число тактов, отведенное на сеанс связи. Эксперименты показывают, что обеспечение необходимой величины $r_{(2)}$ це-

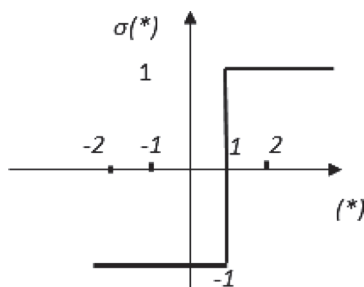


Рис. 6. Функция активации для несимметричного интервала

лесообразно обеспечивать выбором $n \geq 1000$ при $K = 3$, $L = 8$. При этом согласно графикам (рис. 6) обеспечивается $P(t_{AB} \leq d) = 0,994$, $P(t_{AE} \leq d) = 0,005$ при $d = 4000$ тактов. Увеличение L в 2 раза вызывает увеличение d примерно в 10 раз при некотором снижении величины $P(t_{AE} \leq d)$, к аналогичным результатам приводит и увеличение K . Таким образом, если выбрать: $n = 1000$, $K = 3$, $L = 8$, $d = 4000$, то можно с вероятностью $P(t_{AB} \leq d) = 0,994$ сформировать общую бинарную последовательность длиной $r_{(2)} = 12\,000$ битов, конфиденциальность которой не менее $P(t_{AE} \leq d) = 0,045$.

Возникает вопрос насколько достигнутые значения вероятностей удовлетворяют криптографическим требованиям. Вероятность $P(t_{AB} \leq d)$ является важной характеристикой, но не критичной, так как, если формирование общего ключа в данном сеансе не состоится, то его можно повторять до получения успеха. Другое дело с вероятностью $P(t_{AE} \leq d)$. Полученные цифры можно трактовать, как то, что из каждой 1000 сформированных ключей, криптоаналитик буде знать 45. В некоторых случаях такая конфиденциальность может оказаться недостаточной.

Заключение

Таким образом из рассмотренного можно сделать следующие выводы:

- при использовании СИНС для формирования общего секретного ключа необходимо исходить из приемлемых значений вероятностей $P(t_{AB} \leq d)$ и $P(t_{AE} \leq d)$;
- для обеспечения требуемой стойкости к возможным атакам следует выбирать: $L \geq 8$, $K \geq 3$, $n \geq 1000$.

ЛИТЕРАТУРА

1. **Kanter, I.** The Theory of Neural Networks and Cryptography, Quantum Computers and Computing / I. Kanter, W. Kinzel. – 2005. Vol. 5, n. 1. – P. 130–140.
2. **Kinzel, W.** Neural Cryptography / W. Kinzel, / I. Kanter // 9th International Conference on Neural Information Processing, Singapore, 2002.
3. **Ruttor, A.** Dynamics of neural cryptography / A. Ruttor, I. Kanter, and W. Kinzel // Phys. Rev. E, 75(5):056104, 2007.
4. **Голиков В. Ф., Брич Н. В., Пивоваров В. Л.** «О некоторых проблемах в задачах распределения криптографических ключей с помощью искусственных нейронных сетей», Системный анализ и прикладная информатика, № 1–3, 2014.
5. **Плонковский, М.** Криптографическое преобразование информации на основе нейросетевых технологии / М. Плонковский, П. П. Урбанович // Труды БГТУ. Сер. VI. Физико-математические науки и информатика; под ред. И. М. Жарского. – Минск: БГТУ, 2005.

REFERENCES

1. **Kanter, I.** The Theory of Neural Networks and Cryptography, Quantum Computers and Computing / I. Kanter, W. Kinzel. – 2005. Vol. 5, n. 1. – P. 130–140.
2. **Kinzel, W.** Neural Cryptography / W. Kinzel, / I. Kanter // 9th International Conference on Neural Information Processing, Singapore, 2002.
3. **Ruttor, A.** Dynamics of neural cryptography / A. Ruttor, I. Kanter, and W. Kinzel // Phys. Rev. E, 75(5):056104, 2007.
4. **Golikov V. F., Brich N. V., Pivovarov V. L.** «On some problems in the distribution of cryptographic keys using artificial neural networks», System Analysis and Applied Informatics, № 1–3, 2014.
5. **Plonkovski, M.** Cryptographic transformation of information based on neural network technology / M. Plonkovski, P. P. Urbanovich // Proceedings of BSTU. Series VI. Physics and Mathematics and Informatics; by ed. I. M. Zharsky. – Minsk: BSTU, 2005.

HOLIKAU U. F., RADZIUKEVICH M. L.

GENERATION A SHARED SECRET USING ARTIFICIAL NEURAL NETWORKS

Belarusian National Technical University

Scientific Production Republican Unitary Enterprise «Research Institute for the Technical Protection of Information»

In the Kanter's and Kinsella's works is proposes the use of two synchronized artificial neural networks (SANN) connected by opening communication channel to confidential formation of a common cryptographic key. At the same time, there are few

questions of practical suitability of this technology for cryptographic applications. There are no recommendations on the choice of parameters of the used networks, ensuring acceptable speed and guaranteed confidentiality of the generated general secret.

In this regard, it is interesting to substantiate the rational values of the parameters of ANN from the point of view of cryptographic requirements and security analysis of the proposed method of formation of cryptographic keys.

Keywords: *synchronized artificial neural networks, attack, common cryptographic key, parameters of the synchronized artificial neural networks.*



Голиков Владимир Федорович

Доктор технических наук, профессор кафедры «Информационные технологии в управлении» Белорусского национального технического университета. Сфера научных интересов: защита информации, криптография.

E-mail: vgolikov@bntu.by



Радюкевич Марина Львовна

Магистр технических наук. Начальник испытательной лаборатории по требованиям безопасности информации научно-производственного республиканского унитарного предприятия «Научно-исследовательский институт технической защиты информации». Победитель конкурса молодых ученых на XXIV научно-практической конференции «Комплексная защита информации».

E-mail: 1218a@list.ru

**ИНФОРМАЦИОННЫЕ
ТЕХНОЛОГИИ
В ОБРАЗОВАНИИ**

**INFORMATION
TECHNOLOGIES
IN EDUCATION**

УДК 004.942

Ю. Б. ПОПОВА

ОТ LMS К АДАПТИВНЫМ ОБУЧАЮЩИМ СИСТЕМАМ

Белорусский национальный технический университет

Использование информационных технологий и, в частности, автоматизированных систем управления обучением, увеличивает возможности как преподавателя, так и обучаемого, в достижении своих целей в образовательном процессе. Такие системы предоставляют учебный контент, помогают организовать и контролировать обучение, собирают статистику прогресса, а также могут учитывать индивидуальные особенности каждого пользователя системы. Целью данного исследования является определение направления развития современных обучающих систем и технологий их реализации. Была рассмотрена эволюция автоматизированных систем управления обучением, переход к интеллектуальным обучающим системам, основные этапы работы таких систем, проанализированы виды последовательностей обучения, выявлена трансформация в адаптивные обучающие системы, приведена схема работы системы и ее математическая модель. В качестве механизмов реализации обучающих систем определены экспертные системы, теория нечетких множеств и нечеткой логики, кластерный анализ, а также генетические алгоритмы и искусственные нейронные сети. Искусственная нейронная сеть в адаптивной обучающей системе позволит создавать уникальную программу обучения, которая будет отталкиваться от имеющихся знаний и уровня восприятия учебного материала обучающимся. Формализовав интеллектуальные процессы, которые осуществляют как преподаватель, так и обучающийся, можно автоматизировать определенную часть функций преподавателя, сократить затраты на ручной труд, что позволит более просто осуществлять контроль за учебным процессом, а также сделать процесс обучения более эффективным.

Ключевые слова: автоматизированные системы управления обучением, LMS, интеллектуальные обучающие системы, адаптивные обучающие системы, искусственная нейронная сеть.

Введение

Информатизация образования является одним из приоритетных направлений развития каждого современного государства, реализуя принципы повышения качества и доступности. Совершенствование системы непрерывного образования позволит создать условия для формирования гибких образовательных траекторий, обеспечит реакцию системы образования на динамично изменяющиеся потребности личности, общества, экономики. Одновременно появятся возможности для выравнивания доступа к качественному образованию на всех уровнях образовательной системы. Повышение качества профессионального образования в современных условиях возможно только на основе активизации инновационных процессов в данной сфере, обеспечения интеграции образовательной, научной и практической деятельности. Это снимет проблему замкнутости системы образования, откроет ее внешним воздействиям, приведет к постоянному обновлению содержания

образования и технологий обучения. Реализация такого подхода возможна посредством применения автоматизированных систем управления обучением (англ. Learning Management Systems, LMS), которые в последнее время претерпевают значительную трансформацию. Целью данного исследования является определение направления развития современных обучающих систем и технологий их реализации. Для достижения данной цели рассмотрим эволюцию автоматизированных систем управления обучением, определим основные этапы их работы, формализуем задачу обучения, проанализируем основные математические методы, применяемые для решения задачи обучения.

Автоматизированные системы управления обучением являются основой учебного процесса и используются для организации и проведения аудиторных и дистанционных занятий, разработки, управления и распространения учебных материалов с обеспечением совместного доступа. Создаются данные материалы в визуальной учебной среде с зада-

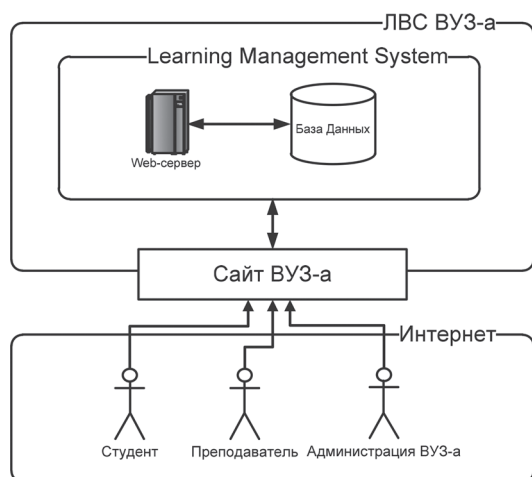


Рис. 1. Общая схема организации работы типичной LMS ВУЗа

нием последовательности изучения. В состав системы, как правило, входят различного рода индивидуальные задания, проекты для работы в малых группах и учебные элементы для всех студентов, основанные как на содержательной компоненте, так и на коммуникативной [1]. В русскоязычной литературе в качестве синонима LMS встречаются термины СДО – система дистанционного обучения, а также СУО – система управления обучением.

В настоящее время существует множество систем управления обучением, причем каждая из них имеет как очевидные преимущества, так и недостатки, обусловленные разработками программных продуктов под определенные цели. Довольно подробная классификация таких систем приведена в [2], а схема организации работы LMS в локальной вычислительной сети (ЛВС) высшего учебного заведения (ВУЗ) может быть представлена в виде:

Как следует из рис. 1, физически система управления обучением размещается на сервере учреждения образования. Информация о пользователях системы, а также весь учебный контент хранятся в базе данных. Доступ к LMS возможен как по локальной сети, так и по сети Интернет. Как правило, в таких системах выделяют три категории пользователей:

- обучающиеся с целью получения знаний;
- преподаватели с целью размещения учебных материалов и организации процесса обучения;
- администрация ВУЗа с целью наблюдения за процессом и сбором статистики об успеваемости.

Неотъемлемой частью всех автоматизированных систем управления обучением является наличие возможности тестирования знаний. Преподаватели могут создавать тесты для контроля знаний, чтобы оценить уровень подготовки обучающихся на данный момент времени, либо тесты для самоконтроля, которые могут быть использованы студентами для самоподготовки. В обоих случаях все обучающиеся работают с одинаковыми по сложности вопросами вне зависимости от своего уровня подготовки, а результаты тестов не могут указать, какие именно пробелы в знаниях имеются у тестируемых. Поэтому возникла необходимость в интеллектуальной составляющей LMS, что привело к появлению интеллектуальных обучающих систем (ИОС) [3–4].

Интеллектуальные обучающие системы позволяют реализовать процесс обучения с помощью динамически развивающейся базы знаний, с учетом оптимального варианта обучения для каждого обучаемого, при наличии автоматизированного учета и анализа получаемой информации, поступающей в базу данных [5]. В большинстве своем ИОС – это высокоструктурированные системы для обучения, в которых определяется программным образом формат обучения, возможности и формы деятельности обучаемого, реализуется постепенное приближение к поставленной цели обучения. В [6] к основным этапам работы ИОС относят построение курса обучения и поддержку в решении задач.

Целью этапа построения курса обучения является предоставление обучаемому наиболее оптимальной, унифицированной последовательности блоков знаний для изучения, а также последовательности заданий (примеров, вопросов, задач и т. д.) для практических занятий. Различают следующие виды построения последовательностей: активные и пассивные [6]. Активное построение последовательности предусматривает наличие активной цели обучения, т. е. наличие определенной подмножества понятий для овладения. Подобные системы с активной последовательностью могут создать наиболее приемлемый индивидуальный путь для достижения целей обучения. Пассивная последовательность не требует активной цели и включается в процесс, когда пользователь не способен решить

поставленную задачу или ответить на вопрос корректно.

Поддержка и помощь в решении задач обычно рассматривается как основная характеристика систем ИОС. Как правило, выделяют три способа поддержки в решении задач: интеллектуальный анализ решений обучаемого, интерактивная поддержка в решении задач и поддержка в решении задач на примерах [6]. Эти способы предназначены для того, чтобы помочь студенту в процессе решения поставленной задачи, однако их реализация происходит по-разному.

Интеллектуальный анализ решений обучаемого работает с итоговыми ответами на задачи. В процессе анализа решенной задачи система должна оценить верность и корректность решения и, по возможности, определить, какие пробелы в знаниях повлекли за собой ошибку, и как эти пробелы можно закрыть. Интеллектуальные анализаторы решений могут предоставлять обучаемым обратную связь и обновлять модель обучаемого.

Интерактивная поддержка в решении задач предоставляет при необходимости интеллектуальную помощь обучаемому в процессе решения задачи. Уровень поддержки может отличаться в зависимости от сложности задания и модели обучаемого. Системы, в которых используется подобный способ, наблюдают за действиями обучаемых, анализируют их и используют полученные данные для принятия решения о необходимости помощи такими способами, как, например, советы, подсказки или сообщения о неверно сделанном в процессе решения шаге.

Поддержка в решении задач на примерах предоставляет возможность обучаемым решать задачи без акцентирования внимания на их ошибках, предлагая примеры схожих задач, успешно решенных ими ранее.

Таким образом, интеллектуальные обучающие системы с обратной связью, способные оказывать поддержку в решении задач, т. е. адаптироваться к модели обучаемого, а также к образовательному контенту, получили название адаптивных обучающих систем (АОС).

Адаптивные обучающие системы анализируют знания обучающегося на каждом этапе изучения материала и позволяют строить индивидуальную траекторию обучения. Также

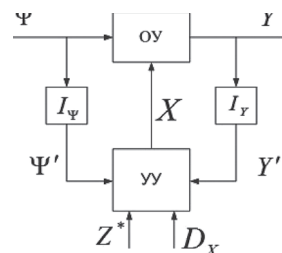


Рис. 2. Общая структура АОС [8]

могут быть учтены психофизические особенности индивидуумов. Следует отметить сложность разработки таких систем и не всегда высокую точность. В первую очередь это связано с трудностями формализации знаний. Некоторые модели представления знаний в обучающих системах были описаны в [7], а процесс обучения сформулирован в [8] как задача управления. Ученик при этом выступает в качестве объекта управления (ОУ), а АОС выполняет функции устройства управления (УУ). На рис. 2 приняты следующие обозначения: Ψ – состояние внешней среды; Y – состояние ученика; I_Ψ , I_Y – соответствующие измерители; Ψ' , Y' – результаты измерения величин Ψ , Y ; X – управляющие воздействия; D_X – ресурсы (ограничения на управление); Z^* – цель управления, состоящая в переводе ученика в требуемое состояние Y^* .

Во введенных обозначениях общее правило функционирования АОС в [8] представлено в следующем виде: АОС, получая на вход информацию о состоянии среды Ψ' и состоянии ученика Y' , а также информацию о цели Z^* и ресурсах D_X , выдает на выход допустимое управление

$$X = A(\Psi', Y', Z^*) \in D_X,$$

переводящее ученика из текущего состояния в состояние, близкое к Y^* . Здесь A – алгоритм управления процессом обучения. Предполагается, что модель ученика, связывающая наблюдаемые входы и выходы, имеет вид $Y' = M_L(\Psi', X)$. В [8] задача синтеза оптимального управления X^* с учетом μ^* , как символа некоторой меры близости, записывается в виде:

$$\min_X \mu(Y - M_L(\Psi', X)) = \mu(Y - M_L(\Psi', X^*)), \\ X \in D_X.$$

Несмотря на сложность разработки адаптивных систем обучения, такой подход является крайне актуальным в настоящее время по

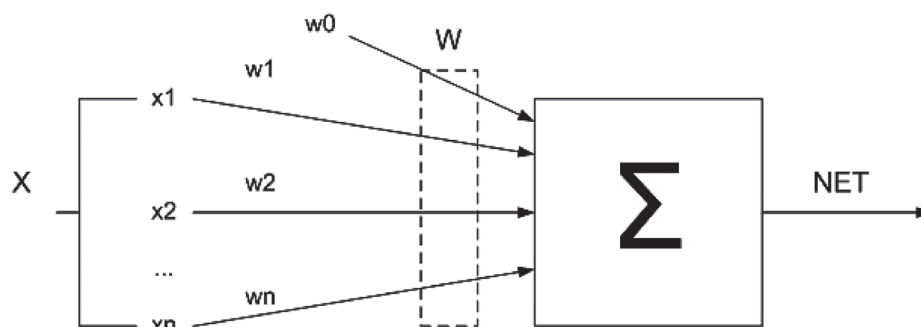


Рис. 3. Модель искусственного нейрона

причине развития непрерывного образования. Человек находится в этом процессе в течение всей своей жизни, хочет заниматься обучением в любом удобном для него месте, в любое свободное для него время, в кратчайшие сроки, не тратя при этом лишних средств.

Математические методы, применяемые в адаптивных обучающих системах. При реализации процесса адаптации одним из важнейших моментов является выбор математических методов. Анализ литературных источников позволил выделить 4 категории методов, применяемых в АОС.

Первая категория включает методы, основанные на теории экспертных систем и реализующие построение хода курса обучения наряду с интеллектуальным анализом результата опроса обучаемого [9]. Плюсом использования таких методов при разработке АОС является предоставление большого круга способов анализа действий, осуществляемых экспертными системами. К минусам можно отнести сложность наполнения базы знаний и регулировки параметров экспертной системы.

Вторая категория представляет собой математические методы, использующие теорию нечетких множеств и нечеткой логики [7]. АОС, в которых применяются такие методы, зачастую реализуют технологию построения последовательности курса обучения. Основной особенностью таких АОС является адаптивность процесса построения курса обучения с учетом неопределенности уровня знаний обучаемого. К недостаткам таких систем можно отнести сложность в выборе параметров алгоритмов нечеткой логики.

К третьей категории были отнесены методы на основе статистических подходов. Такие методы решают задачи классификации в АОС, например, разбиение обучающихся на класте-

ры в зависимости от уровня предварительной подготовки [10].

Четвертая категория объединяет методы, основанные на теории эволюционных алгоритмов (генетические алгоритмы, искусственные нейронные сети и т. д.). Основной используемой технологией здесь является интеллектуальный анализ ответов обучаемого. К особенностям таких систем относят их широкое применение в задачах адаптивного контроля знаний [11]. В качестве недостатка выступает отсутствие единого способа обоснования принимаемых решений в искусственных нейронных сетях и проблема сходимости генетических алгоритмов.

Искусственные нейронные сети в адаптивных обучающих системах. Исходя из недостатков всех групп, для создания наиболее эффективной адаптивной обучающей системы был выбран метод четвертой группы, основанный на использовании искусственной нейронной сети (ИНС). В модели ИНС простые узлы (их называют нейроны либо нейроды (neurodes), либо обрабатывающие элементы (ОЭ), либо юниты) связаны друг с другом и образуют сеть узлов [11]. Одно из подобий ИНС биологическим нейронным сетям заключается в том, что функции выполняются юнитами все вместе, параллельно.

Искусственный нейрон имитирует в первом приближении свойства биологического нейрона. На вход искусственного нейрона поступает некоторое множество сигналов $x_1, x_2, \dots, x_n$, каждый из которых является выходом другого нейрона. Каждый вход умножается на соответствующий вес $w_1, w_2, \dots, w_n$, аналогичный синаптической силе, и все произведения суммируются, определяя уровень активации нейрона. На рис. 3 представлена модель, которая реализует эту идею.

Для эффективной адаптивной обучающей системы нужны свойства, которые являются основными для искусственных нейронных сетей:

– Самообучение – это одно из самых важных преимуществ ИНС перед другими традиционными алгоритмами. Обучение заключается в поиске коэффициентов связей между нейронами. В процессе обучения искусственная нейронная сеть способна находить зависимости между входными и выходными данными, а также совершать обобщение. Это означает, что, если обучение было успешным, то сеть способна вернуть верный результат на основании данных, которые отсутствовали в обучающей выборке.

– Быстродействие. Каждый из нейронов, по сути, является микропроцессором, но, поскольку искусственная нейронная сеть состоит из тысяч таких нейронов, между которыми распределяется задача, ее решение происходит намного быстрее, чем при использовании обычных алгоритмов решения.

– Адаптация к изменениям. Способность искусственной нейронной сети адаптироваться к изменениям позволит ей работать в правильном режиме все время.

Практическая реализация применения искусственной нейронной сети для адаптивного обучения находится на стадии апробирования для учебных дисциплин «Тестирование и от-

ладка программного обеспечения», «Надежность программного обеспечения», «Модульное тестирование» для подготовки инженеров-программистов на факультете информационных технологий и робототехники Белорусского национального технического университета.

Заключение

Проведенные исследования позволили проследить путь совершенствования обучающих систем от автоматизированных систем управления обучением к интеллектуальным обучающим системам, а затем и к адаптивным обучающим системам. Искусственная нейронная сеть в адаптивной обучающей системе позволит создавать уникальную программу обучения, которая будет отталкиваться от имеющихся знаний и уровня восприятия учебного материала обучающимся. Такой подход позволит построить индивидуальную траекторию обучения, учитывающую психофизические особенности обучаемого. Формализовав интеллектуальные процессы, которые осуществляют как преподаватель, так и обучающийся, можно автоматизировать определенную часть функций преподавателя, сократить затраты на ручной труд, что позволит более просто осуществлять контроль за учебным процессом, а также сделать процесс обучения более эффективным.

Литература

1. Ellis, Ryann K. Field Guide to Learning Management Systems // ASTD Learning Circuits [Электронный ресурс]. – 2009. – Режим доступа: http://www.astd.org/~media/Files/Publications/LMS_fieldguide_20091 – Дата доступа: 03.11.2018.
2. Попова, Ю. Б. Классификация автоматизированных систем управления обучением / Ю. Б. Попова // Системный анализ и прикладная информатика. – 2016. – № 3. – С. 51–58.
3. Брусиловский, П. Л. Адаптивные и интеллектуальные технологии в сетевом обучении / П. Л. Брусиловский // Новости искусственного интеллекта. – 2002. – № 5. – С. 25–31.
4. Брусиловский, П. Л. Интеллектуальные обучающие системы / П. Л. Брусиловский // Информатика. Информационные технологии. Средства и системы. – 1990. – № 2. – С. 3–22.
5. Семенова, Н. Г. База знаний интеллектуальной обучающей системы технической дисциплины / Н. Г. Семенова, А. М. Семенов, И. Б. Крылов // Вестник Оренбургского государственного университета. – 2013. – № 9. – С. 44–54.
6. Пелюшенко, А. В. Обучающие среды и интеллектуальные обучающие системы: возможности использования в образовательном процессе / А. В. Пелюшенко // Известия Волгоградского государственного технического университета. – 2006. – № 3. – С. 48–50.
7. Попова, Ю. Б. Представление знаний в обучающих системах на основе теории нечетких множеств / Попова, Ю. Б., Бураковский А. И. // Системный анализ и прикладная информатика. – 2016. – № 2. – С. 58–65.
8. Модельное обеспечение автоматизированных обучающих систем. Обзор // Наука и образование: [Электронный ресурс] / МГТУ им. Н. Э. Баумана / Карпенко А. П., 2011. – Режим доступа: <http://technomag.edu.ru/doc/193116.html> – Дата доступа: 09.11.2018.
9. Стандарты в сфере дистанционного обучения [Электронный ресурс]. – Режим доступа: <http://dist.by/distantionnoe/16-standarty-v-sfere-distantionnogo-obucheniya> – Дата доступа: 20.10.2018.
10. Информационно-коммуникационные технологии в образовании [Электронный ресурс]. – Современные тенденции в кластерном анализе. В. Б. Бериков, Г. С. Лбов. – Режим доступа: <http://www.ict.edu.ru/ft/005638/62315e1-st02.pdf> – Дата доступа: 09.11.2018.

11. Попова Ю. Б., Яцынович С. В. Обучение искусственных нейронных сетей методом обратного распространения ошибки. // [Электронный ресурс]. – Режим доступа: <http://www.bntu.by/news/67-conference-mido/4860-2016-11-18-15-47-40.html> – Дата доступа: 01.10.2018.

REFERENCES

1. Ellis, Ryann K. Field Guide to Learning Management Systems // ASTD Learning Circuits [Elektronnyj resurs]. – 2009. – Rezhim dostupa: http://www.astd.org/~media/Files/Publications/LMS_fieldguide_20091 – Data dostupa: 03.11.2018.
2. Popova, Ju. B. Klassifikacija avtomatizirovannyh sistem upravlenija obucheniem / Ju. B. Popova // Sistemnyj analiz i prikladnaja informatika. – 2016. – № 3. – S. 51–58.
3. Brusilovskij, P. L. Adaptivnye i intellektual'nye tehnologii v setevom obuchenii / P. L. Brusilovskij // Novosti iskusstvennogo intellekta. – 2002. – № 5. – S. 25–31.
4. Brusilovskij, P. L. Intellektual'nye obuchajushhie sistemy / P. L. Brusilovskij // Informatika. Informacionnye tehnologii. Sredstva i sistemy. – 1990. – № 2. – S. 3–22.
5. Semenova, N. G. Baza znaniy intellektual'noj obuchajushhej sistemy tehnicheckoj discipliny / N. G. Semenova, A. M. Semenov, I. B. Krylov // Vestnik Orenburgskogo gosudarstvennogo universiteta. – 2013. – № 9. – S. 44–54.
6. Peljushenko, A. V. Obuchajushhie sredy i intellektual'nye obuchajushhie sistemy: vozmozhnosti ispol'zovaniya v obrazovatel'nom processe / A. V. Peljushenko // Izvestija Volgogradskogo gosudarstvennogo tehnicheckogo universiteta. – 2006. – № 3. – C. 48–50.
7. Popova, Ju. B. Predstavlenie znaniy v obuchajushhih sistemah na osnove teorii nechetkih mnozhestv / Popova, Ju. B., Burakovskij A. I. // Sistemnyj analiz i prikladnaja informatika. – 2016. – № 2. – S. 58–65.
8. Model'noe obespechenie avtomatizirovannyh obuchajushhih sistem. Obzor // Nauka i obrazovanie: [Elektronnyj resurs] / MGTU im. N. Je. Bauman / Karpenko A. P., 2011. – Rezhim dostupa: <http://technomag.edu.ru/doc/193116.html> – Data dostupa: 09.11.2018.
9. Standarty v sfere distancionnogo obucheniya [Elektronnyj resurs]. – Rezhim dostupa: <http://dist.by/distantsionnoe/16-standarty-v-sfere-distantsionnogo-obucheniya> – Data dostupa: 20.10.2018.
10. Informacionno-kommunikacionnye tehnologii v obrazovanii [Elektronnyj resurs]. – Sovremennye tendencii v klaster-nom analize. V. B. Berikov, G. S. Lbov. – Rezhim dostupa: <http://www.ict.edu.ru/ft/005638/62315e1-st02.pdf> – Data dostupa: 09.11.2018.
11. Popova Ju. B., Jacynovich S. V. Obuchenie iskusstvennyh nejronnyh setej metodom obratnogo rasprostraneniya os-hibki. // [Elektronnyj resurs]. – Rezhim dostupa: <http://www.bntu.by/news/67-conference-mido/4860-2016-11-18-15-47-40.html> – Data dostupa: 01.10.2018.

Поступила
15.04.2018

После доработки
26.06.2019

Принята к печати
01.07.2019

Popova Y. B.

FROM LMS TO ADAPTIVE TRAINING SYSTEMS

Belarusian National Technical University

The use of information technology and, in particular, learning management systems, increases the ability of both the teacher and the learner to achieve their goals in the educational process. Such systems provide educational content, help organize and monitor training, collect progress statistics, and can also take into account the individual characteristics of each user of the system. The purpose of this study is to determine the direction of development of modern learning systems and technologies for their implementation. The evolution of learning management systems, the transition to intelligent learning systems, the main stages of such systems were reviewed, the types of learning sequences were analyzed, the transformation into adaptive learning systems was identified, and the scheme of the system and its mathematical model were presented. Expertise systems, the theory of fuzzy sets and fuzzy logic, cluster analysis, as well as genetic algorithms and artificial neural networks are defined as the mechanisms for implementing the learning systems. An artificial neural network in an adaptive learning system will allow you to create a unique training program that will build on existing knowledge and the level of perception of educational material by students. By formalizing the intellectual processes that both the teacher and the student carry out, it is possible to automate a certain part of the teacher's functions, reduce the cost of manual labor, which will make it easier to monitor the learning process and also make the learning process more efficient.

Keywords: learning management system, LMS, intelligent learning systems, adaptive learning systems, artificial neural network.



Yuliya B. Popova, PhD, Associate Professor of the Department of software for information systems and technologies at the Belarusian National Technical University. Her research interests include methods and algorithms of optimization in technical systems, engineering of adaptive learning systems and learning management systems (LMS), modeling of student knowledge, software testing and quality assurance.

E-mail: julia_popova@mail.ru

Попова Юлия Борисовна, доцент, кандидат технических наук, доцент кафедры программного обеспечения информационных систем и технологий БНТУ. Ее научные интересы связаны с методами и алгоритмами оптимизации технических систем, разработкой адаптивных обучающих систем, автоматизированных систем управления учебным процессом, моделированием знаний, а также с вопросами тестирования и качества программного обеспечения.

Работа выполняется в рамках научно-исследовательской работы ГБ № 16–274 «Модели, методы, технологии создания прикладных комплексов для инженерных и компьютерных систем».