СПбГУТ)))

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

8TH INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2019

VIII МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ «АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ В НАУКЕ И ОБРАЗОВАНИИ»

АПИНО

ICAIT

СБОРНИК НАУЧНЫХ СТАТЕЙ

27–28 ФЕВРАЛЯ 2019 ГОДА

ПОДРОБНОСТИ НА САЙТЕ КОНФЕРЕНЦИИ

APINO.SPBGUT.RU

УДК 001:061.3(082)
ББК 72 А43

Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С. В. Бачевского; сост. А. Г. Владыко, Е. А. Аникевич. СПб. : СПбГУТ, 2019. Т. 2. 603 с.

В научных статьях участников конференции исследуются состояние и перспективы развития мирового и отечественного уровня IT и телекоммуникаций. Предлагаются методы и модели совершенствования научно-методического обеспечения отрасли связи и массовых коммуникаций.

Предназначено научным работникам, аспирантам и студентам старших курсов телекоммуникационных и политехнических вузов, инженерно-техническому персоналу и специалистам отрасли связи.

ISBN 978-5-89160-188-8

Научное издание
Литературное редактирование,
корректура Е. А. Аникевич
Оформление Г. И. Юрьев
Верстка Е. М. Аникевич
Подписано в печать 02.09.2019.
Вышло в свет 30.09.2019. Формат 60×90 1/8.
Уст. печ. л. 37,7. Заказ № 055-ИТТ-2019.
пр. Большевиков, д. 22, корп. 1.
Россия, Санкт-Петербург, 193232

ИНФОРМАЦИОННЫЕ ПАРТНЕРЫ

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА

СОДЕРЖАНИЕ

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

УДК 004.046
ГРНТИ 47.13.07

ON THE DESIGN OF VIRTUAL REALITY ENVIRONMENTS IN EDUCATION

F. M. Nuraliev, U. E. Giyosov

Tashkent University of information technologies named after Muhammad al-Khwarizmi

This text deals with the design of virtual reality systems. It is also said here that the results reached with the use of the developed software show the attributes that make the ideal virtual reality for situations of research and learning taking the discipline as a reference of the classroom to the computer labs and making more interesting to the student, making the learning easy. Also of note is the fear that is characteristic only for VR in the field of education.

virtual reality for education, visualization of knowledge; design of virtual reality systems, Smart classes, E-learning, sensors and interactive communication technology,3D, Blender, VRML. virtual laboratory.

1 Introduction

We are aiming at building student vision and focusing on important key trends like mobile learning, online learning and e-textbooks. Each of these trends comprises of the essential components of the student vision in terms of socially-based and digitally rich learning. Providing students increased access to educational resources and experts to identify their caliber and extend learning beyond the capacities or limitations of their school or community.

Exposing students to rich, compelling learning experiences that help develop deeper knowledge and skill especially the problem-solving, creativity and critical thinking which are so highly desired for our world today. Empowering students to take responsibility for their own educational destinies and to explore and innovate thus creating an independent new generation of life long learners. The Augmented reality exercise, wherein models designed to teach concepts like rotation/revolution, solstice/equinox, and seasonal variation of light and temperature,

resulted in an overall significant improvement in student understanding as well as a noticeable reduction in student misunderstandings. Other important conclusions about this system were that AR interfaces not only change the delivery mechanism of instructional content but They fundamentally change the way that content is imparted and conceived, through a unique combination of visual and sensory information that results in a powerful cognitive and learning experience. 21st century learning highlights digital-age literacy, effective communication and high productivity where students have access to rich information and global communication. Teachers support, facilitate, encourage, and collaborate with their students. Pre-requisites for the skill set are basic language literacy, decision making, costs and benefits, pros and cons, rewards and consequences, embrace modern media to think, decide, and communicate thoughts and ideas [2].

2 The solution of the problem

During the last 5 years, technology of virtual reality (VR) evolved from doubtful looking to widely used and implemented. And there was a priori to accept the fact their usefulness. Perhaps for this reason, there were born a lot of misconceptions about VR in general and, in particular, in the field of education. The general misconceptions include the following:

1. «VR was created for entertainment only». This is not true. At the moment, VR has covered many areas: marketing, tourism, real estate, art, education.

2. «VR has a motion sickness problem». This defect was a problem for the first models of helmets. Modern models have no such problem.

3. «VR-helmets cause great harm to human vision». VR-helmets use monitors those don’t radiate any particles (except photons of light), so they don’t cause harm.

4. «VR leads users away from the present reality, causing disorder and creating dependency». Scientific evidence shows that VR, opposed to the altered states of consciousness (caused by hypnosis, chemical drugs, etc.), does not cause the inadequacy of mind, does not reduce the degree of reflection, not characterized by a feeling of ambivalence, alienation of the own «I», etc.

5. «VR kills the live relations and separates people from each other». But the same was talked about mobile phones, SMS-messages, social networks. However, those who consider the use of new technologies escape from reality, forget about their benefits: mobile telephony gives opportunity to connect with the person on the other side of the planet, and social networks allow to enrich remote communication by various types of content and activities.

3 The calculation of generalized evaluations

The main disadvantage of the virtual caves is the high cost, which makes the use of this type of immersive VR limited. On the other hand, the use of an HMD can often cause some level of cyber sickness.

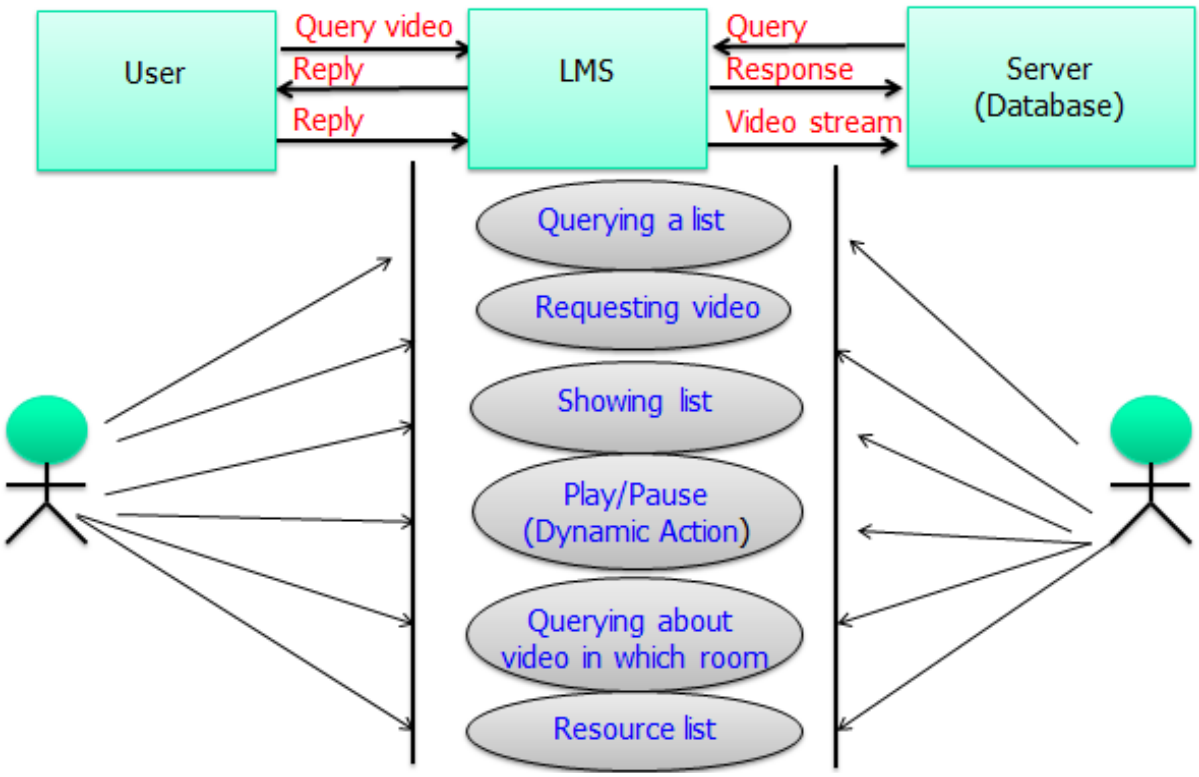


Fig. 1. Viewing of Rough Use Case diagram of the virtual reality in the educational systems

Nevertheless, the use of VR in engineering education spreads further than the use of 3D-VLs.On one hand, VR applications focus on the design and simulation of an engineering project, which are based not only on the use of techniques but also on the interactive verification of the obtained results [13, 15, 16]. On the other hand, other VR applications aim to improve the comprehension of different concepts: the spatial comprehension of abstract concepts, complex three-dimensional graphics, production processes, manufacturing, operation processes, assembly, etc. [14, 17, 18]. Finally, VR learning environments have also been related to serious games since approximately 20 years ago and, in this way, such environments enhance student motivation through a game fiction procedure of the teaching-learning process [19]. Furthermore, kinaesthetic learning and all the embodied elements in learning are supported by VR [4].

To the design of the automatons, the software uses tolls in 3D, as the Blender and the VRML (Virtual Reality Modeling Language) and to the publishing of a page on the internet it is integrated the Program Language PHP (Hypertext Pre Processor). The results reached with the use of the developed software show the

attributes that make the ideal Virtual Reality for situations of research and learning taking the discipline as a reference of the classroom to the computer labs and making more interesting to the student, making the learning easy.

Virtual reality, augmented reality and their variations represent computer interface techniques that take into account the tridimensional space. In this space, the user acts in a multi sensorial way, exploring aspects of this space through the viewing, hearing and tact. According to the available technology it's also possible to explore the smell and the taste. Body perceptions, like cold, heat and pressure, are included in the tact, through the skin (Kimer, 2011).

Virtual reality is characterized by three basic ideas: (Pinho, 2004)

- Immersion: the user has the real sensation of being inside the virtual world of the computer. Devices that make this sensation: digital helmets and digital cave.
- Interaction: the user manipulates virtual objects. Devices that make this sensation: digital gloves.
- Involvement: exploring of a virtual environment, it's as if the user took part of the virtual world and he can interfere directly in result of the application, the user can navigate on the virtual environment in a passive or active way.

3.1 Virtual Reality in the Education

The technological revolution has been permitting the use of new approaches in the teaching-learning process. One of the conductive technologies to the building of innovative tools for the education is the Virtual reality, which offers tridimensional computer environments with advanced forms of interaction that can provide more motivation to the learning process.

A very short time ago, we could consider that the great potential of VR use was in small groups placed in large urban centers and in teaching and researching institutions. However, the integration VR-VRML democratized its access, expanding more and more its potential and using fields (BARILLI et al, 2012). With the help of resources of some modeling and animation programs as the Blender 3D, for example, the VR use can help students in the comprehension and assimilation of concepts, coming up as a valid alternative to get good results. Other benefits are observed with the use of Virtual Reality in the education. According to Clark (2006) the Virtual Reality can be used to make the learning more interesting and fun with the purpose of improving the motivation and attention, decreasing costs when using the objective and the real environment no matter how expensive the simulation is. It also makes possible that situations that were impossible to explored in the real world can be done, for example: exploring a planet like Mars, traveling inside the human body, doing submarines explorations or inside caves, visiting very small places to be seen (molecules) or very expensive or very far away, or yet because this place is in the past (historical places) world [3].

4 Necessity of Virtual Reality in education

The following reasons support virtual reality in education:

- It provides new forms and methods of visualization, drawing on the strengths of visual representations and it provides an alternate method for presentation of material. VR can also more accurately illustrate some features, processes than by other means, allowing extreme close-up examination of an object, observation from a great distance, and observation and examination of areas and events which are unavailable by other means.
- Motivate and encourage active participation and interaction from students rather than passivity. Some types of virtual reality, for example, collaborative virtual reality using text input with virtual worlds, encourage or require collaboration and provide a social atmosphere.
- Virtual reality allows the learner to proceed through an experience during a broad time period. It allows the disabled to participate in an experiment or learning environment & transcends all language barriers. With text access it provides equal opportunity for communication with students in other cultures allowing student to take on the role of a person in different cultures. The potential benefits of the use of VR in education and training: visualization and reification, an alternate method for presentation of material; learning in contexts impossible or difficult to experience in real life; motivation enhancement; collaboration fostering; adaptability, offering the possibility for learning to be tailored to learner's characteristics and needs; and evaluation and assessment, offering great potential as a tool for evaluation because of easy monitoring and recording of sessions in a virtual environment [1].

Based on the experience of implemented development VR content in education can be noted that the technology brings positive results when it is using by short sessions or as simulators and trainers. It is inappropriate to use VR for lectures and seminars. In the development of software solutions should focus on the newest models of VR equipment, the most eco-friendly and ergonomic for user. Hardware and software interface must be as simple as possible for users, especially for teachers.

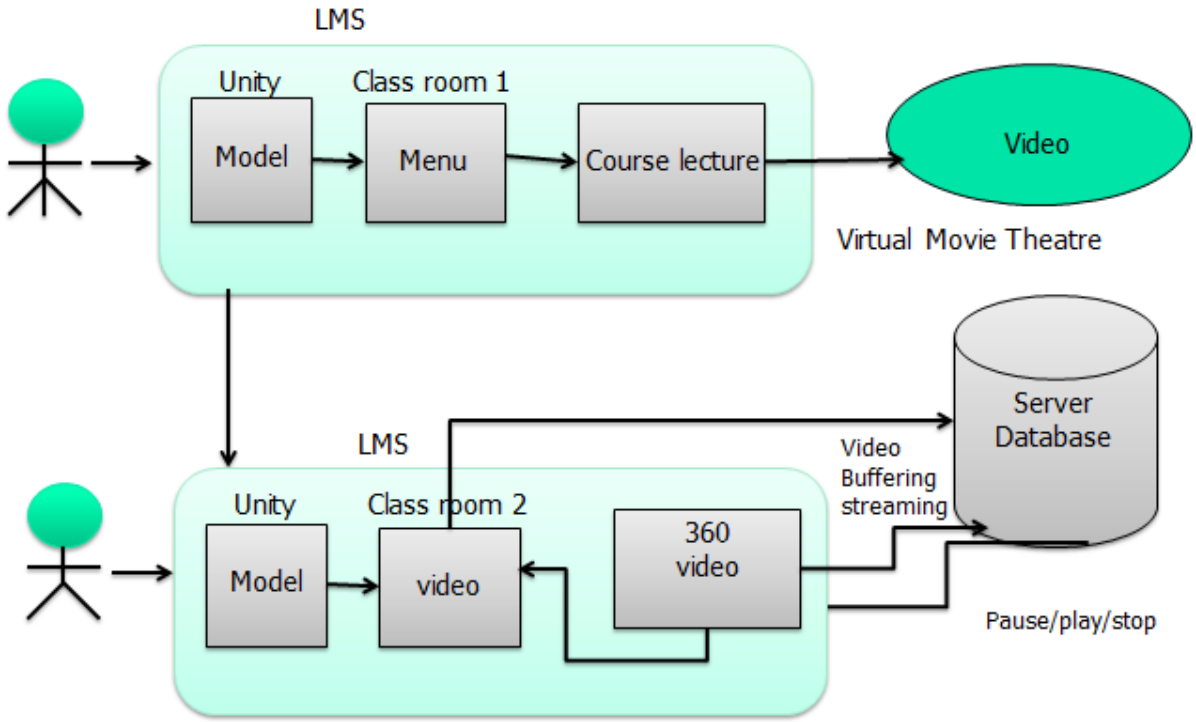


Fig. 2. Viewing of Rough idea integration of applications VR with most common LMS in authorization part and transfer of user activity data from VR to LMS

To reveal the usefulness of VR resources in engineering studies, diverse surveys were carried out during the last seven academic courses to recover the opinion of students enrolled in diverse engineering degrees at different universities. On the basis of the analysis of the database of 200 surveys, students considered that the most important features in VR applications [3, 5] are interactivity, realism (including immersion), motivation, ease of use, and educational usefulness. From these results, several conclusions can be drawn:

- Interactivity and realism are the most important features for motivating students to use a didactic VR application. Taking into account that students are used to handling videogames designed with the latest VR technologies, outdated didactic VR applications do not awake the interest of students. Consequently, a constant effort to update VR application is necessary.
- The students highly rated the realism of the VR applications developed by the authors. Even so, students demand the use of VR resources as much as possible in order to improve their learning experience, according to survey results. Thus, collaboration between experts in a specific subject and VR technicians is necessary for designing a useful and attractive VR environment for students.
- In general terms, all the students consider these didactic VR resources easy to use (as it would be expected, considering the students' familiarity with the latest generation of videogames, which are designed with the same type of VR software).

- VR is not by itself educationally useful and, consequently, an ad hoc methodological approach must be developed using the VR as a didactic tool.
- According to students' opinion, the most important aspects in a didactic VR tool to reach a good level of educational usefulness are: (i) a collection of interactive exercises or problems and (ii) the interactivity, which must be designed for didactic purposes and, hence, the allowed movements should enhance the expected learning.

(a) (b) (c) (d)

Fig. 3. Testing models created with virtual reality applications.
(a), the main view of the educational building, (b) laboratory room's project,
(c) main entrance, (d) schedule table

Viewing of walk inside the main hall while run this application script

```
using UnityEngine;
using System.Collections;

public class walk : MonoBehaviour {
public static int pointlar = 20;
public GameObject[] points = new GameObject[15];
Transform[] all_Point=new Transform[100];
private Vector3 target_Pos;
```

```
private int i = 0;
public float speed_move = 5f;

// Use this for initialization
        string intToStr(int a)
        {
        string s="";
        if(a==0)
        return "0";
        while(a!=0)
                {
                s = (char)((a%10)+'0') + s;
                a = a / 10;
                }
        return s;
        }
        void Start () {
        // tag point assignment
        string k;
        for (int j = 0; j < points.Length; j++) {
                k = intToStr (j);
                //k = (string)(j);
                Debug.Log (k);
                k = "point" + k;

        points [j] = GameObject.FindWithTag (k);
        all_Point [j] = points [j].transform;
                }  }
void Update () {
// object target
target_Pos = all_Point[i].transform.position;
// object movement
transform.Translate(Vector3.Normalize(target_Pos - transform.position)*Time.del-
taTime*speed_move);
// distance to the target
        float distans = Vector3.Distance(target_Pos, transform.position);
                if (distans < 0.5f){
                if (i < points.Length - 1){
                                i++;    }
                        else    {
                                i = 0;  } } }  }
```

Conclusion

The educational software helped to take the Formal Language subject from classrooms to the computer labs, making the teaching/learning process more interesting and pleasant to the students, facilitating the teacher’s work during the

evaluation performance too. The advent of affordable and widespread virtual reality technology and the proliferation of smart phones capable of supporting augmented reality has opened incredible opportunities for improving the way that we learn. Students can now experience the topics they are learning about. Use of virtual reality technology has been shown to increase student engagement and focus, while the immersive and interactive environment encourages the students to become active learners.

References

1. Elesin, C. C., Feshenko, A. V. Virtual reality in education: The doubts and hopes. *Гуманитарная информатика. 2016. Вып. 10. С. 109–114.*

2. Kavita choudhary and Anuradha. Proposed model for virtual reality based smart classes. International journal of information and computation technology. ISSN 0974-2239. 2013. Vol. 3, No. 5. pp. 439–444

3. Piovesan, Sandra Dutra, Passerino, Liliana Maria and Pereira, Adriana Soares. Virtual reality as a tool in the education. Iadis international conference on cognition and exploratory learning in digital age (celda 2012).

4. Vergara, Diego, Rubio, Manuel Pablo and Lorenzo, Miguel, On the design of virtual reality learning environments in engineering. Published: 1 june 2017.

5. Vergara, D.; Rubio, M. P.; Prieto, F.; Lorenzo, M. Enhancing the teaching/learning of materials mechanical Characterization by using virtual reality. J. Mater. Educ. 2016, 38, 63–74.

6. Vergara, D.; Rubio, M.P.; Lorenzo, M. New approach for the teaching of concrete compression tests in large Groups of engineering students. J. Prof. Issues eng. Educ. Pract. 2016.

7. Vergara, D.; Rubio, M. P.; Lorenzo, M. Interactive virtual platform for simulating a concrete compression test. Key eng. mater. 2014, 572, 582–585.

8. Vergara, D.; Rubio, M.P.; the application of didactic virtual tools in the instruction of industrial radiography. J. Mater. Educ. 2015, 37, 17–26.

9. Hashemipour, M.; Manesh, H. F.; Bal, M. A modular virtual reality system for engineering laboratory Education. Comput. Appl. Eng. Educ. 2011, 19, 305–314.

10. Dobrzanski, L. A.; Honysz, R. The idea of material science virtual laboratory. J. Achiev. Mater. Manuf. Eng.2010, 42, 196–203.

11. Xiang, S.; Wang, L. Ch. Vgls: a virtual geophysical laboratory system based on c# and viustools and its Application for geophysical education. Comput. Appl. Eng. Educ. 2017.

12. Hashemipour, M.; Manesh, H. F.; Bal, M. A modular virtual reality system for engineering laboratory Education. Comput. Appl. Eng. Educ. 2011, 19, 305–314.

13. Sampaio, A. Z. Virtual reality technology applied in teaching and research in civil engineering education. J. Inf. Technol. Appl. Educ. 2012, 1, 152–163.

14. Arnay, R.; Hernández-Aceituno, J.; González, E.; Acosta, L. Teaching kinematics with interactive schematics and 3d models. Comput. Appl. Eng. Educ. 2017.

15. Crespo, R.; García, R.; Quiroz, S. Virtual reality application for simulation and offline programming of The mitsubishi move master rv-m1 robot integrated with the oculus rift to improve students training. Proc. Comput. Sci. 2015, 75, 107–112.

16. Górski, F.; Bu´n, P.; Wichniarek, R.; Zawadzki, P.; Hamrol, A. Immersive city bus configuration system for Marketing and sales education. Proc. Comput. Sci. 2015, 75, 137–146.

17. Chou, Ch.; Hsu, H.-L.; Yao, Y.-S. Construction of a virtual reality learning environment for teaching structural Analysis. Comput. Appl. Eng. Educ. 1997, 5, 223–230.

18. Vergara, D.; Rubio, M. P.; Lorenzo, M. Multidisciplinary methodology for improving students' spatial abilities in technical drawing. Sci. J. Educ. Technol. 2015, 5, 1–8.

19. Villagrasa, S.; Fonseca, D.; Durán, J. Teaching case: applying gamification techniques and virtual reality for learning building engineering 3d arts. In proceedings of the second international conference on Technological ecosystems for enhancing multiculturality, salamanca, spain, 1–3 october 2014; acm: New york, ny, usa; pp. 171–177.

УДК 004.056
ГРНТИ 28.23.37

ДИАГНОСТИРОВАНИЕ НАРУШЕНИЙ БЕЗОПАСНОСТИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ КОМБИНИРОВАННОЙ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ

В. С. Авраменко, А. В. Маликов

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Компьютерные инциденты, обнаруживаемые в инфокоммуникационных системах, необходимо диагностировать с целью получения информации для принятия обоснованного решения на реагирование.

Под диагностированием понимается процесс определения значений характеристик нарушений безопасности, таких как тип, цель, источники, причины, результаты и др. Учитывая большой объем разнородных диагностических признаков, используемых на этапе анализа, а также высокие требования по оперативности и достоверности диагностирования компьютерных инцидентов, предлагается использовать искусственные нейронные сети в качестве базы для построения модели, в частности сеть Хопфилда и персептрон.

Комбинированная диагностическая нейронная сеть позволяет совместно использовать достоинства отдельных видов искусственных нейронных сетей и повысить эффективность процесса диагностирования. В связи с тем, что вычисление значений характеристик нарушений безопасности обученной искусственной нейронной сетью осуществляется достаточно быстро, предлагаемый подход позволяет осуществлять оперативное диагностирование характеристик нарушений безопасности с требуемой достоверностью результата.

компьютерный инцидент, нарушение безопасности информации, искусственные нейронные сети, диагностирование, средства защиты.

Расследование компьютерных инцидентов, фиксируемых в современных инфокоммуникационных системах (ИКС), первоначально осуществляется с определения класса компьютерного инцидента. Если нарушение или прекращение функционирования ИКС не связано с нарушением безопасности информации (НБИ), например, из-за непреднамеренных нарушений правил эксплуатации и т. п., то их относят к техническим компьютерным инцидентам. Инциденты, возникающие из-за наличия уязвимостей, позволяющих реализовывать угрозы нарушения конфиденциальности, целостности или доступности информации в ИКС, относятся к компьютерным инцидентам безопасности. Действия в случае обнаружения технических компьютерных инцидентов хорошо проработаны. Компьютерные инциденты безопасности, напротив, вызывают многочисленные трудности при диагностировании.

Поскольку под нарушением безопасности информации понимается событие, заключающееся в появлении или реализации угрозы безопасности информации [1], то характеризовать выявленное нарушение безопасности информации будем с позиции описания угроз безопасности информации.

Основные характеристики нарушения безопасности информации представлены в таблице.

ТАБЛИЦА. Значения характеристик нарушения безопасности информации

№ п/п	Наименование характеристики	Значения характеристики
1.	Вид деструктивного действия	нарушение конфиденциальности информации нарушение целостности информации нарушение доступности информации
2.	Объект воздействия	автоматизированное рабочее место серверное оборудование Сетевое оборудование
3.	Способ реализации	за счет эксплуатации известных уязвимостей за счет эксплуатации новых уязвимостей
4.	Источник нарушения	внешний внутренний
5.	Характер воздействия	преднамеренное непреднамеренное
6.	Результат	изменение (удаление). создание блокировка и др.
7.	Последствия	критический ущерб не критический ущерб
8.	Время	момент обнаружения нарушения средствами зашиты информации
9.	id события	в соответствии с описанием журналов событий

№ п/п	Наименование характеристики	Значения характеристики
10.	id пользователя (id токена)	в соответствии с настройками ИКС
11.	Адрес источника	сетевой адрес (ip-адрес, номер порта)
12.	Адрес назначения	сетевой адрес (ip-адрес, номер порта)

При возникновении НБИ перед администратором возникает задача оперативного определения значений характеристик нарушения безопасности в целях выработки обоснованного решения на реагирование.

Известны работы по идентификации отдельных характеристик нарушений безопасности [2], анализу аномалий, но в целом вопросы разработки методологических основ комплексного анализа НБИ требуют дальнейшего исследования.

Таким образом, оперативный анализ характеристик НБИ с целью повышения оперативности и обоснованности принимаемого решения на реагирование является актуальной проблемой для современных ИКС.

В качестве исходных данных для решения задачи анализа характеристик НБИ в первую очередь целесообразно использовать журналы событий, происходящих в системе, другие источники информации о состоянии ИКС в период подготовки и реализации нарушения безопасности информации.

Многообразие средств автоматизации и защиты обуславливает возможность получения большого количества различного рода признаков НБИ, такие как типы событий, номера портов, адреса, идентификаторы процессов, время обнаружения и другие, что требует решения проблемы эффективной обработки данной информации.

Существуют различные подходы к анализу и обработке больших массивов, регистрируемых служебных данных, их классификации. К их числу относятся кластерный анализ, факторный анализ, искусственные нейронные сети, деревья решений, регрессионный анализ, дискриминантный анализ, корреляционный анализ и другие [3].

Для решения задачи оперативного анализа (диагностирования) нарушений безопасности в ИКС предлагается использовать искусственные нейронные сети (ИНС) [4]. На вход ИНС поступают предварительно обработанные данные из журналов событий, на выходе ИНС – значения характеристик нарушения безопасности. Предварительная обработка данных от источников информации о НБИ заключается в отборе из всего множества регистрируемых событий информативных признаков для диагностирования. При этом для осуществления отбора может применяться как экспертный метод, так и применение вариации нейросети – автоэнкодера (рис. 1). Автоэнкодер позволяет уменьшить размерность пространства входных признаков, путем обобщения взаимозависимых входных признаков. Число нейронов скрытого слоя значительно меньше числа нейронов входного слоя

автоэнкодера. При необходимости проводится нормализация диагностических признаков для приведения их к одному диапазону значений [5].

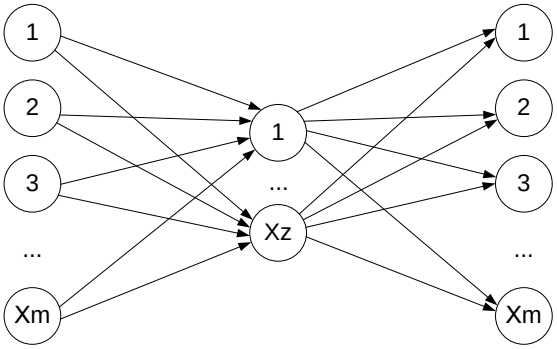


Рис. 1. Структура автоэнкодера для снижения размерности входных данных

После обнаружения НБИ возможны ситуации, когда приходится осуществлять анализ неполного или ограниченного набора диагностических признаков, например, вследствие выхода из строя какого-либо средства защиты, являющегося одним из источников диагностических признаков.

В этом случае целесообразно использовать ИНС Хопфилда (рис. 2), которая способна установить по неполному набору признаков их соответствие одному из эталонных описаний (образов), полученному на этапе обучения.

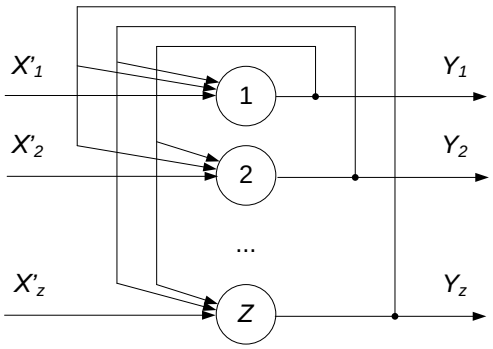


Рис. 2. Структура искусственной нейронной сети Хопфилда для обработки диагностических признаков

Для идентификации бинарной характеристики нарушения безопасности целесообразно использовать трехслойный персептрон, представленный на (рис. 3), состоящий из z нейронов входного слоя, n нейронов скрытого слоя, число которых определяется в процессе обучения ИНС ($n < z$), и одного нейрона выходного слоя.

Задача окончательной классификации решается следующим образом. На этапе обучения на вход персептрона подаются векторы диагностических

признаков, позволяющие однозначно судить о том, какое произошло нарушение (например, нарушение конфиденциальности). Корректировка весовых коэффициентов производится методом обратного распространения ошибки. Функция активации – логистическая.

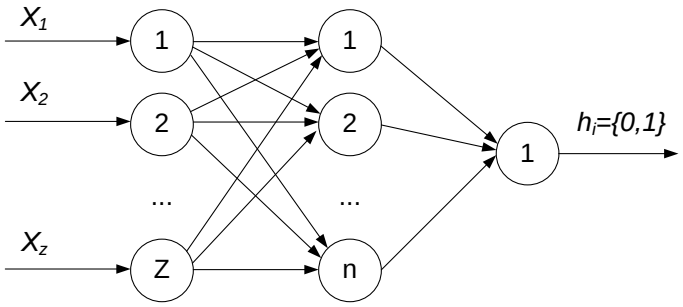


Рис. 3. Структура искусственной нейронной сети для идентификации бинарной характеристики нарушения безопасности

Объединив указанные искусственные нейронные сети в единую последовательную цепочку, получаем комбинированную диагностическую искусственную нейронную сеть (рис. 4). На входе автоэнкодер снижает размерность входных исходных данных *X* и формирует групповые диагностические признаки. Далее они поступают на вход сети Хопфилда, которая сопоставляет набор групповых диагностических признаков с эталонными описаниями НБИ, сохраненными в качестве весовых коэффициентов нейронной сети Хопфилда. Затем выходные значения с сети Хопфилда обрабатываются трехслойным персептроном, который завершает процедуру обработки диагностических признаков и на выходе выдает значение бинарной характеристики нарушения безопасности.

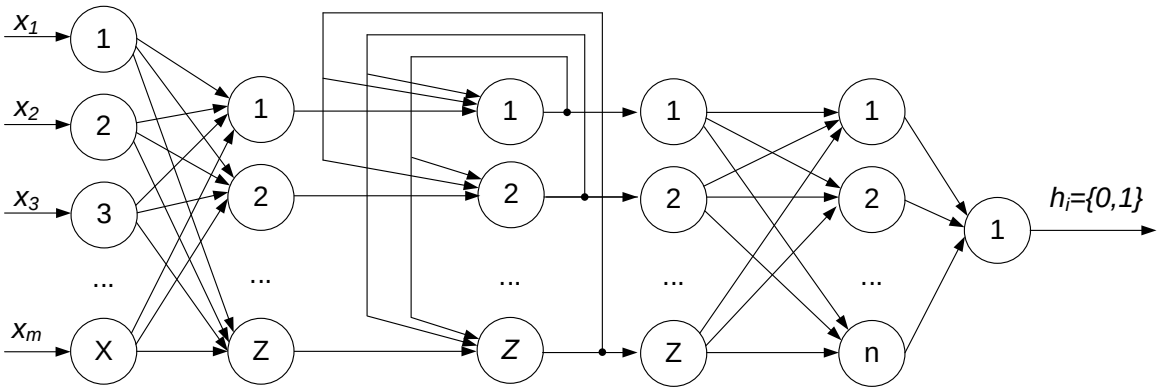


Рис. 4. Структура комбинированной диагностической искусственной нейронной сети

В связи с тем, что обученная нейронная сеть выдает результат достаточно быстро, реализация, предложенной модели анализа НБИ в ИКС на основе диагностической искусственной нейронной сети, позволит в автоматическом режиме в близком к реальному масштабу времени идентифицировать характеристики нарушений безопасности, что в свою очередь позволит обеспечить оперативное и обоснованное реагирование.

Список используемых источников

1. Авраменко В. С., Маликов А. В. Диагностирование нарушений безопасности информации в инфокоммуникационных системах на основе искусственных нейронных сетей // В сб.: Региональная информатика и информационная безопасность. 2017. С. 24–26.

2. Авраменко В. С. Способы идентификации нарушителя безопасности информации в автоматизированных системах на основе информационного почерка // Проблемы технического обеспечения войск в современных условиях. II межвузовская конференция: материалы конференции. Санкт-Петербург, ВАС. СПб., 2017. С. 36–40.

3. Рубаков С. В. Современные методы анализа данных // «Наука. Инновации. Образование». М.: ФГБУ «Российский научно-исследовательский институт экономики, политики и права в научно-технической сфере», 2008. С. 165–176.

4. Осовский С. Нейронные сети для обработки информации / Пер. с польского И. Д. Рудинского. М.: Финансы и статистика, 2002. 344 с.

5. Акинина Н. В., Акинин М. В., Соколова А. В., Никифоров М. Б., Таганов А. И. Автоэнкодер: подход к снижению размерности векторного пространства с контролируемой потерей информации. // Известия ТулГУ. Технические науки. Тула: ФГБОУВПО «Тульский государственный университет», 2016. № 9. С. 3–12.

УДК 004.056.53
ГРНТИ 81.96

ПРОГНОЗИРОВАНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В. С. Авраменко, А. В. Тарасов

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Защита информации в современных автоматизированных системах характеризуется высокой инерционностью мероприятий по поддержанию или восстановлению требуемого уровня защищённости информации от несанкционированного доступа и компьютерных атак. Одним из путей решения проблемы инерционности системы защиты информации в условиях неопределённости угроз является реализация функции прогнозирования защищенности информации. В данной статье представлена статистическая модель прогнозирования показателей защищенности информации.

система защиты информации, угроза безопасности, модель прогнозирования, методы прогнозирования.

Одной из основных проблем защиты информации в автоматизированных системах специального назначения (АССН) является инерционность реагирования на новые, ранее неизвестные защищающейся стороне угрозы безопасности информации, в том числе обусловленные выявленными нарушителями новыми уязвимостями. Наличие уязвимостей в системе защиты или в средствах вычислительной техники является необходимым условием реализации угроз безопасности информации, и в первую очередь – угроз несанкционированного доступа (НСД). Особенно опасны уязвимости «нулевого» дня [1]. Они регулярно обнаруживаются во всех основных операционных системах и приложениях, применяемых в том числе и в АССН.

Таким образом, в условиях информационного противоборства, характеризующихся высокой степенью неопределенности угроз и высокой динамикой процесса их реализации, важнейшую роль играет контроль защищенности, который должен быть упреждающим. Результаты контроля должны предоставляться в сроки, позволяющие предотвратить переход автоматизированных систем в состояние незащищенности информации.

Одним из путей решения проблемы инерционности реагирования на изменение состояния системы защиты информации в АС и условий ее функционирования является реализации функции прогнозирования защищенности информации от НСД.

При прогнозировании защищенности в качестве прогнозной величины могут использоваться такие характеристики защищенности как количество и интенсивность появления уязвимостей (угроз, атак), величина потенциального ущерба и т. д. Также в качестве прогнозной величины могут использоваться показатели защищенности информации.

Одним из простейших показателем защищенности информации от НСД является интенсивность нарушений безопасности $\lambda_{нб}$.

В расчете на наихудший случай, когда нарушитель «идеальный» (имеет высокую квалификацию, постоянно отслеживает появление новых уязвимостей, а также имеет возможность мгновенно использовать их для осуществления НСД к информации, обрабатываемой в АС), интенсивность нарушений безопасности ресурсов соответствует интенсивности возникновения угроз и рассчитывается по формуле:

$$\lambda_{нб} = \frac{1}{T_{зф}},$$

где $T_{зф}$ – среднее время защищенного функционирования средств автоматизации, которое, в свою очередь, определяется в соответствии с выражением:

$$T_{эф} = \frac{T_{пф}}{N_{нб}},$$

где $T_{пф}$ – оцениваемый период функционирования средств автоматизации;

$N_{нб}$ – общее количество нарушений безопасности информации (обнаруженных уязвимостей) за период функционирования.

При расчете интенсивностей нарушений безопасности допустимо использовать поправочные коэффициенты, учитывающие различные факторы, влияющие на интенсивность нарушений (важность и частота использования защищаемой информации в интересах достижения цели функционирования и другие), тогда действительная интенсивность нарушений рассчитывается по формуле:

$$\lambda_{нбд} = \lambda_{нбб} \cdot K_{ni},$$

где $\lambda_{нбд}$ – действительное значение интенсивности нарушений;

$\lambda_{нбб}$ – базовое значение интенсивности нарушений;

K_{ni} – поправочный коэффициент по i-му фактору.

Поправочные коэффициенты интенсивностей нарушений безопасности ресурсов средств автоматизации могут быть определены на основе статистических исследований или экспертным путем.

Для прогнозирования защищенности информации в АССН в целях поддержки принятия решений по защите информации целесообразно использовать комплексные показатели защищенности, учитывающие как процессы нарушения безопасности, так и процессы контроля и восстановления защищенного состояния. В качестве такого показателя целесообразно использовать предложенный в [2] коэффициент защищенности информации $K_{защ}$, рассчитываемый по формуле:

$$K_{защ} = \frac{\mu_{в}}{\lambda_{нбб} + \mu_{в}},$$

где $\mu_{в}$ – интенсивность восстановления защищенности информации от НСД.

Характеристика $\mu_{в}$ отражает деятельность штатных специалистов безопасности информации и возможности самой системы защиты информации (СЗИ), которые влияют на восстановление защищенности информации.

Основной задачей прогнозирования является разработка прогнозной модели. Под прогнозной моделью в общем случае понимается модель объекта прогнозирования, сконструированная на множестве объектов и типов отношений выбранной реальности, исследование которой позволяет получить совокупность выбранных данных о возможных состояниях объекта в будущем и (или) путях и сроках их осуществления.

В самом общем виде прогнозная модель согласно [3] имеет следующий вид:

$$y(t) = tr(t) + S(t) + I(t) + \varepsilon,$$

где $tr(t)$ – тренд, который представляет собой плавно изменяющуюся составляющую, обычно отражающую влияние факторов, оказывающих долговременное воздействие;

$S(t)$ – сезонная или циклическая составляющая, которая отражает регулярную повторяемость процессов во времени (в течение года, недели, суток и др.);

$I(t)$ – интервенции, т. е. резкие изменения под влиянием обстоятельств, которые практически невозможно определить и локализовать во времени с точки зрения возможности предвидения;

ε – нерегулярная составляющая.

Рассмотрим более подробно данные составляющие. Для прогнозирования необходимо использовать статистические данные о применяемых в АССН технических и программных средствах. В связи ограниченностью доступа к таким данным для анализа были построены динамические ряды показателей на основе статистических данных, полученные из открытой базы данных уязвимостей CVSS (ресурс *Vulners.com*) для ОС на базе ядра Debian GNU/Linux, аналогичных применяемой в силовых ведомствах ОС Astra Linux.

Обработка данных производилась в редакторе MS Excel с использованием набора средств анализа данных, предназначенных для решения сложных статистических и инженерных задач. Анализ динамических рядов был произведен в периоды равным неделе, месяцу и году, соответствующим типовым интервалам планирования, с целью выявления существующих закономерностей. Использование более длительных интервалов для перспективного планирования представляется нецелесообразным в связи с недостатком статистических данных.

Сезонная или циклическая составляющая, представляющая собой закономерности, регулярно повторяющиеся из периода в период, при проведении первоначального анализа исходных данных выявлена не была. В итоге получаем следующую прогнозную модель защищенности:

$$y_{\text{защ}}(t) = tr(t) + \varepsilon.$$

Таким образом, для формирования прогноза возникновения угроз защищённости информации от НСД, как случайного нестационарного процесса, необходимо произвести декомпозицию исходного процесса на регулярную (тренд) и нерегулярную составляющие. Тренд описывает устойчивые тенденции изменения показателей защищённости информации от НСД. Нерегулярная составляющая характеризует случайную непрогнозируемую часть и вероятные отклонения фактических значений от тренда, выделенного из исходного процесса.

Выделенный в результате декомпозиции тренд или тенденция может в дальнейшем использоваться в качестве прогнозной математической модели, т. е. модели, применяемой для расчёта прогнозных значений. При выборе метода прогнозирования тренда следует учитывать, что метод прогнозирования, с одной стороны, должен обеспечить функциональную полноту, достоверность и точность прогноза, а, с другой стороны, уменьшить затраты времени и средств на прогнозирование.

Для сравнения точности прогнозов исследуем метод скользящих средних и экспоненциального сглаживания. Для этого произведем обработку статистических данных динамических рядов показателей для ОС Astra Linux. Формула для расчета относительной ошибки прогноза δ на год, месяц, неделю каждого метода согласно [3] имеет следующий вид:

$$\delta = \frac{1}{n}\sum_{t=1}^{n}\frac{|e_t|}{x_t} * 100,$$

где $e_t = x_t - \bar{x}_t$ – ошибка прогноза;

x_t – фактическое значение показателя;

$\bar{x}_t$ – прогнозируемое значение;

n – количество прогнозных значений.

При этом считается, что точность модели является высокой, когда δ < 10 %, хорошей – при δ = 10–20 % и удовлетворительной – при δ = 20–50 %.

По результатам проведенных исследований, представленных в таблице, можно сделать вывод, что метод скользящей средней является более точным, чем метод экспоненциального сглаживания.

ТАБЛИЦА. Сравнение точности полученных прогнозов

Используемый метод	Относительная ошибка, δ (%)		
	на год	на месяц	на неделю
Скользящего среднего	8,54	17,53	21,23
Экспоненц. сглаживания	26,25	52,68	80,92
Используемый метод	Точность модели		
	на год	на месяц	на неделю
Скользящего среднего	выс.	хор.	удовл.
Экспоненц. сглаживания	удовл.	неуд.	неуд.

При сглаживании временного ряда скользящими средними в расчетах участвуют все уровни ряда. Чем шире интервал сглаживания, тем более плавным получается тренд. Сглаженный ряд короче первоначального на $(n - 1)$ наблюдений (n – величина интервала сглаживания). При больших значениях n колеблемость сглаженного ряда значительно снижается.

Применение представленной прогнозной модели защищенности позволяет должностным лицам по защите информации заблаговременно принимать меры по поддержанию требуемого уровня защищенности, при этом разработка и внедрение автоматизированной системы прогнозирования не требует существенных затрат.

Список используемых источников

1. Авраменко В. С., Бобрешов-Шишов Д. И., Маликов А. В. Способ выявления уязвимостей «нулевого дня» на основе анализа поведения эксплойтов // Проблемы технического обеспечения войск в современных условиях. Труды III Межвузовской научно-практической конференции. 2018. С. 45–48.

2. Авраменко В.С., Бушуев С. Н., Козленко А.В. Оценка защищенности информации от НСД в условиях стохастической неопределенности угроз // Вопросы радиоэлектроники. М., 2013. Вып. 1. С. 82–95.

3. Адамов В. Е., Вергилес Э. В. Статистика промышленности: учебник. М.: Финансы и статистика, 2005. 326 с.

УДК 004.7:004.422.8
ГРНТИ 20.01.07

МОДЕЛЬНО-АНАЛИТИЧЕСКИЙ ИНТЕЛЛЕКТ СЕРВИСА ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Е. В. Агапов, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Актуализирована интеллектуализация процесса запуска задач в территориально-распределенных вычислительных системах. Описаны причины разнородности высокопроизводительных вычислительных комплексов и разнотипности запускаемых заданий в территориально-распределенных системах. Предложены инновационные приёмы интеллектуализации процесса запуска задач в территориально-распределенных вычислительных системах. Раскрыто содержание инновационных приёмов интеллектуализации.

интеллектуализация, вычислительная система, запуск заданий, система мониторинга, нейронная сеть.

В наукоёмких отраслях цифровой экономики современная технологическая, приборная и экспериментальная база сопровождается высокопроизводительными территориально-распределёнными вычислительными системами, являющимися неотъемлемыми составляющими информационных инфраструктур. Территориально-распределённые вычислительные системы, развивающиеся в соответствии с определяющими признаками эволюции, применяются для решения актуальных прикладных и фундаментальных задач с распараллеливанием вычислений с целью повышения эффективности вычислительных ресурсов. Эволюционный характер развития территориально-распределённых вычислительных систем является основной первопричиной разнородности высокопроизводительных вычислительных комплексов.

Для корректного функционирования территориально-распределённых вычислительных систем реализуются системы распределения задач по доступным вычислительным ресурсам, осуществляющие планирование выполнения задач и мониторинг состояния вычислительных ресурсов.

Эффект от использования мощностей территориально-распределённых систем находится в непосредственной зависимости от характеристик потоков поступающих на обработку заданий и от характеристик разнородных

высокопроизводительных вычислительных комплексов, задействованных в процессе распределения заданий по ресурсам.

Отраслевое многообразие, динамический характер рыночной экономики, разнообразие стратегий обеспечения устойчивой конкурентоспособности корпораций, использующих ресурсы территориально-распределённых вычислительных систем, разнородность объединённых высокопроизводительных вычислительных комплексов в различных формах сочетаний порождают высокую степень неопределённости условий решения задачи распределения заданий по ресурсам.

Проведённый анализ систем управления ресурсами, систем пакетной обработки заданий и распространённых методов планирования задач в распределённых системах обработки данных показал актуальность разработки новых методов планирования в условиях неполноты информации о ресурсных требованиях [1, 2, 3, 4, 5, 6, 7].

Для преодоления представленной априорной неопределённости предлагается интеллектуализация процесса управления глобальной очередью к её ресурсам. Взаимосогласованная последовательность операций, реализующих метод постановки задания на обработку с учётом разнотипности заданий и разнородности высокопроизводительных комплексов, представляется как модельно-аналитический сервис.

В архитектуру интеллектуальной системы управления глобальным потоком заданий в высокопроизводительной территориально-распределённой системе вводится анализатор кода, мониторинг состояния вычислительных узлов комплекса, математическая модель планирования заданий и система поддержки принятия решения. В концептуальную основу анализатора кода закладывается нейросетевой принцип обработки текстовой информации на базе рекуррентных нейронных сетей.

Нейронная сеть характеризуется следующими особенностями:

1. Модель сети – Sequential (последовательная).

2. Слой долгой краткосрочной памяти LSTM (1 000 элементов, которые используются для хранения информации) с использованием техники dropout для отключения входных связей на 20 % и рекуррентных на 20 %.

3. Полносвязный выходной слой – 6 нейронов с функцией активации «сигмоид».

Ввиду того, что нейронная сеть способна обрабатывать только числовые значения, создаётся словарь слов, где каждому слову присваивается определённый индекс. Информация для словаря собирается следующим образом:

1. Обрабатывается N программ, содержащих различные стандарты параллельного программирования (OpenMP, MPI, CUDA).

2. Текст каждой программы разбивается на слова, удаляются специальные символы, числа. Слова приводятся к единому виду, затем каждое слово заносится в массив.

3. Массив слов сортируется по алфавиту для ускорения процесса сравнения.

4. Каждое слово массива сравнивается со словами из других массивов, вычисляется частота использования слова. В случае использования одного слова в *M* массивах оно исключается из других массивов и перемещается в итоговый массив. Данное действие исключает возможность заносить названия пользовательских переменных, функций и классов.

5. По завершению всех итераций формируется итоговый массив с ключевыми словами параллельных стандартов программирования.

6. Ввиду распространенного использования библиотек общего назначения и общепринятых паттернов написания программного кода, итоговый массив содержит избыточную информацию в виде названия библиотек, переменных, не относящихся к стандартам параллельного программирования. В связи с этим выбирается полностью последовательный код программы, над которым производится предобработка согласно п. 2.

На выходе сети определяется диапазон ядер, рекомендованное количество ядер, их весовые коэффициенты и производится постобработка.

Второй этап интеллектуализации распространяется на совершенствование процессов взаимодействия с системой мониторинга.

В системе мониторинга, развёрнутой на сети автономных интеллектуальных агентов, реализуется процесс сбора необходимой системной информации, анализ производительности, планирование и настройка.

После получения от агентов всех параметров ресурсов с комплексов собранные данные регистрируются в сводной таблице на сервере, где системой поддержкой принятия решений осуществляется её обработка.

Предлагаемое усовершенствование системы распространяется на реализацию системы поддержки принятия решений по выбору подходящего кластера на базе нейронной сети.

На вход второй нейронной сети направляются данные с первой нейронной сети, проводящей обработку текстов программ, и данные с системы мониторинга. На этом этапе в системе поддержки принятия решений корректируется количество процессоров и выбирается высокопроизводительный комплекс.

Представленная интеллектуализация процесса запуска пользовательского задания характеризуется инновационной значимостью предлагаемых формализаций, заключающейся во внедрении нейросетевого подхода к распределению заданий в высокопроизводительных территориально-распределенных системах.

Список используемых источников

1. Система пакетной обработки заданий Torque [Электронный ресурс]. URL: https://www.torque.com/ (дата обращения 20.12.2018).
2. Система пакетной обработки заданий LSF [Электронный ресурс] URL: https://www.lsf.com/ (дата обращения 20.12.2018).
3. Система пакетной обработки заданий Windows compute cluster server [Электронный ресурс]. URL: https://www.wccs.com/ (дата обращения 20.12.2018).
4. Система пакетной обработки заданий Condor [Электронный ресурс]. URL: https://www.condor.org/ (дата обращения 20.12.2018).
5. Система пакетной обработки заданий LoadLever [Электронный ресурс]. URL: https://www.loadlever.com/ (дата обращения 20.12.2018).
6. Система пакетной обработки заданий Cleo [Электронный ресурс]. URL: https://www.cleo.com/ (дата обращения 20.12.2018).
7. Система пакетной обработки заданий Maui [Электронный ресурс]. URL: https://www.maui.org/ (дата обращения 20.12.2018).

УДК 004.942; 004.896
ГРНТИ 28.17.19; 50.51.02

АНАЛИЗ И ФОРМАЛИЗАЦИЯ ЗАДАЧИ СТРУКТУРНО-ПАРАМЕТРИЧЕСКОГО СИНТЕЗА МАГИСТРАЛЬНО-МОДУЛЬНЫХ СИСТЕМ

С. В. Акимов, Г. В. Верхова, Х. М. Кходер

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Модульный принцип построения систем получает все более широкое распространение благодаря гибкости и возможности быстрого комплексирования систем из унифицированных модулей. В связи с этим, в данной работе представлен анализ задачи синтеза магистрально-модульных систем. Также указано, что для автоматизации структурно-параметрического синтеза необходимы специальные многоаспектные модели. Рассмотрена формальная и математическая постановка задачи синтеза магистрально-модульных систем.

магистрально-модульные системы, сложные системы, автоматизация, структурно-параметрический синтез, многоаспектное моделирование, универсальная модель, комплексная модель.

Синтез выступает в качестве комплексной дисциплины и оперирует методами из различных областей знаний, основными из которых можно назвать: базовые дисциплины, системный анализ, теории искусственного интеллекта, инженерия знаний, математическое программирование, теории

предметной области, исследование операций, теория принятия решений, оптимизационные методы, эволюционные мультиагентные системы. В связи с тем, что синтез структур представляет трудноформализуемую задачу, в нем используются как методы дискретной оптимизации, так и эвристические (морфологические, биоинспирированные) методы.

Синтез систем может выполняться как аналитическими, так и численными методами. В аналитическом методе используется алгоритм, который позволяет получить как структуру системы, так и параметры модулей из ее составляющих, причем система обычно получается оптимальной. Тем не менее, подобные алгоритмы определены не более чем для нескольких классов систем, так как являются специализированными и подходят лишь для синтеза систем рассматриваемого класса. В численном методе алгоритм синтеза неизвестен, и задача решается с помощью поисковых оптимизационных методов. Данные алгоритмы делятся на алгоритмы параметрического и структурно-параметрического синтеза.

В структурно-параметрическом синтезе систем поиск технического решения производится в пространстве как структур, так и параметров (номиналов) модулей, составляющих данные структуры. Этим структурно-параметрический синтез принципиально отличается от синтеза параметрического, когда структура задана, не изменяется в процессе синтеза, а поиск ведется в пространстве параметров модулей, из которых данная структура состоит.

В настоящий момент автоматизация структурно-параметрического синтеза систем представляет большое теоретическое и практическое значение. В то же время являются актуальными проблемы автоматизации структурно-параметрического синтеза и разработки его общей теории [1], поскольку проблема синтеза возникает практически перед каждым исследователем, разработчиком или проектировщиком разнообразных сложных технических систем.

Еще сравнительно недавно аргументом оппонентов осуществимости автоматизации структурно-параметрического синтеза мог являться тот факт, что данные задачи, как правило, принадлежат к классу NP-трудных, и в настоящее время отсутствуют алгоритмы, дающие возможность за приемлемое время находить наилучшие решения для таких задач. Согласно мнению таких возражателей, при условии наличия компьютера с абсолютной (нелимитированной) вычислительной мощностью найти решение имеющейся задачи можно было бы без значительных усилий, с помощью обычного перебора всех возможных вариантов сочетаний элементов, параметров и связей. Но, вследствие того, что на данный момент не существует подобных компьютеров, а число комбинаций поистине колоссально, решение такой задачи методом указанного элементарного перебора совершенно не подходит.

В то же время при традиционном проектировании оптимальность разрабатываемой системы также не является гарантированной. Вместе с тем, с массовым внедрением персональных компьютеров, оснащенных вычислительной мощностью, сопоставимой с мощностью самых передовых компьютеров недавних лет, успешной разработкой методологии объектно-ориентированного программирования и мультиагентных технологий, появляется возможность создания методик структурно-параметрического синтеза различных модульных систем [2], применимых на практике. Очевидно, что такой мощный компьютер может перебрать огромное множество структур, которое не поддается никакому сравнению с перебором «ручными» методами.

Есть все основания полагать, что принципиальным отличием систем автоматизированного проектирования (САПР) следующего поколения от ныне существующих САПР будет наличие развитых модулей структурно-параметрического синтеза и глубокая интеграция в единое информационное пространство постиндустриального общества (CALS третьего поколения). Тем не менее, реализация полноценных коммерческих САПР систем, автоматизирующих процесс структурно-параметрического синтеза для широкого класса модулей, пока что сталкивается с рядом сложностей, среди которых:

1. отсутствие подходящей для всех классов проектируемых модулей единой теории структурно-параметрического синтеза.

2. отсутствие поддерживающего процедуру структурно-параметрического синтеза оптимального лингвистического обеспечения.

3. неполная проработка методологических вопросов, раскрывающих удовлетворяющие для решения задач данного рода особенности моделей и алгоритмов.

При автоматизации задачи синтеза магистрально-модульных систем [3], и, в частности, радиоэлектронных средств (РЭС) (рис.), необходимо взаимодействовать с комплексным представлением знаний, которые не могут быть выражены в рамках классических математических моделей, являющихся системами интегро-дифференциальных уравнений. Для отображения различного вида знаний о модуле необходим новый класс моделей, в которых будут учтены различные аспекты: функциональные, конструктивные, структурные, экономические и другие.

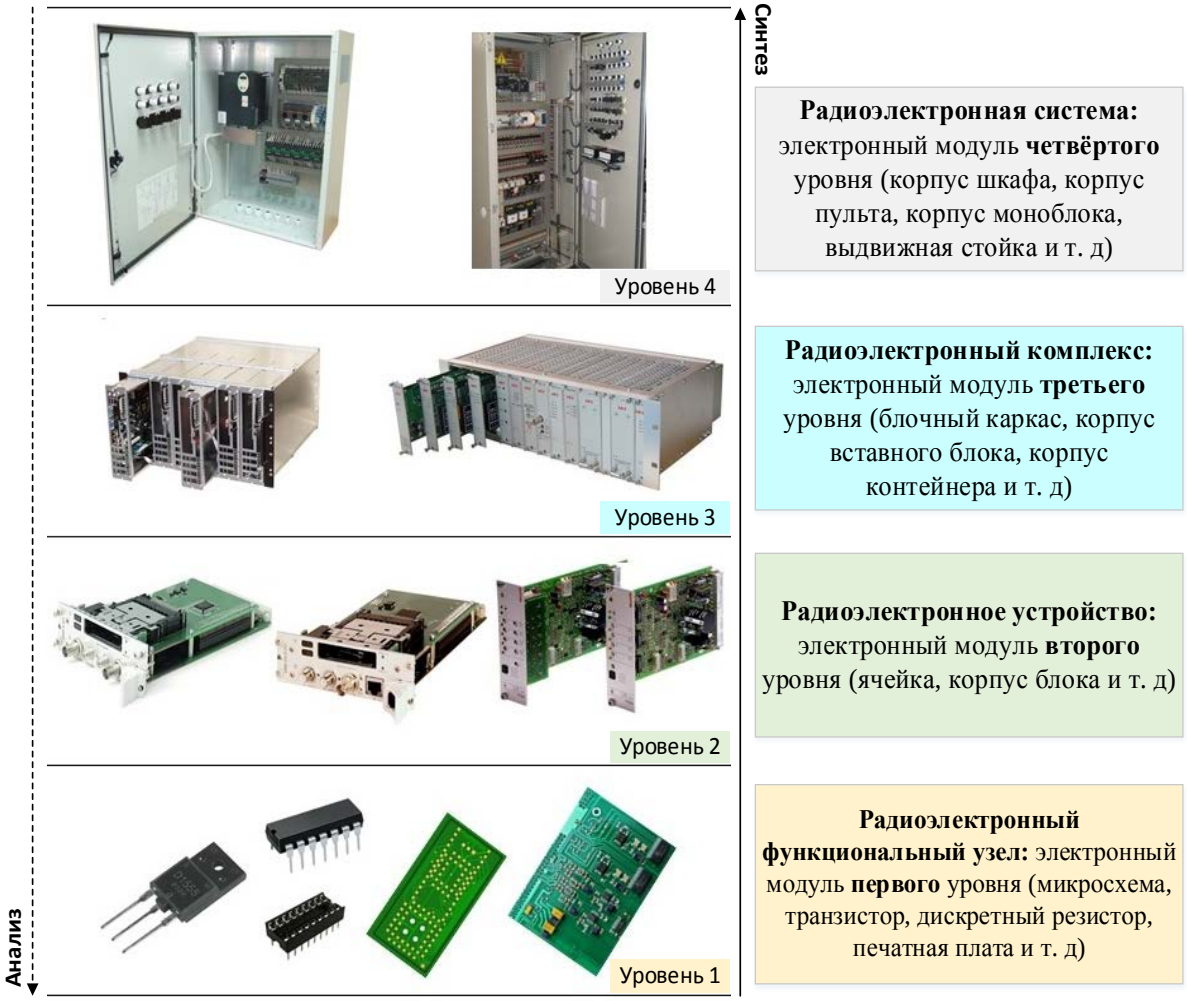


Рисунок. Уровни разукрупнения РЭС по конструктивной и функциональной сложности

Таким образом, для автоматизации структурно-параметрического синтеза магистрально-модульных систем хорошо подходят кибернетические модели в пространстве многоаспектного моделирования [4], к которым могут быть отнесены комплексные и интегративные модели [5, 6].

Рассмотрим формальную и математическую постановку задачи синтеза магистрально-модульных систем. Однозначное описание структуры системы и параметров модулей, из которых она состоит, будем называть спецификацией модульной системы, и обозначим ее буквой *S*. Синтезируемая система *S* может быть представлена тройкой (1):

$$S = < M, R, X >, \quad (1)$$

где M – множество модулей (агрегатов, подсистем), из которых состоит система;

R – множество связей между модулями из M;

X – множество параметров модулей.

Если число модулей в системе равно n, тогда (2):

$$M = \bigcup_{i=1}^{n} M_i = \{M_1, M_2, ..., M_n\}. \quad (2)$$

Отдельный модуль M_i может иметь один или $k(i)$ параметров. Множество параметров всей системы получается путем объединения множеств параметров отдельных модулей, из которых состоит система (в теории оптимального синтеза X часто называют вектором рабочих параметров), тогда (3):

$$X = \bigcup_{i=1}^{n} \bigcup_{j=1}^{k(i)} X_{i,j}. \quad (3)$$

Так как X является множеством параметров модулей M, описывающих его свойства, то выражение (1) представляют в следующем виде (множество модулей и связей между ними) (4):

$$S = < M, R >. \quad (4)$$

Задачу синтеза оптимальной системы можно выразить следующим образом (5):

$$S^{*(K)} = Opt(S, K), \quad (5)$$

где $Opt(S,K)$ – оператор оптимизации системы S по критерию (критериям) K, при наличии ограничений, а $S^{*(k)}$ – система оптимальная по K.

Следовательно, можно сделать вывод, что для решения задачи синтеза магистрально-модульных систем требуются такие действия, как: определение множества модулей, из которых будет состоять система, установление связей между ними и обозначение параметров модулей. При этом могут быть поставлены ограничения на множество модулей, способы их соединения и параметры.

В завершение необходимо отметить, что преимуществом структурно-параметрического синтеза магистрально-модульных систем является универсальность и гибкость, благодаря чему он обеспечивает нахождение как структуры системы, так и параметров модулей, причем класс проектируемых модулей, в отличие от синтеза, выполняемого аналитическими методами, довольно обширен. Условием осуществимости использования структурно-параметрического синтеза магистрально-модульных систем служит наличие универсальных моделей проектируемых систем.

Список используемых источников

1. Янковская Т. А. О задачах структурно-параметрического синтеза при проектировании сложных технических систем // Образовательные ресурсы и технологии. 2014. № 1 (4). С. 170–175.
2. Кходер Х. М, Верхова Г. В., Акимов С. В. Модульная технология проектирования гибких сложных систем // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 9. С. 86–90.
3. Шубарев В. А., Меткин Н. П., Зверев В. Н. Магистрально-модульное построение РЭС – стратегическое направление радиоэлектронного приборостроения // Электроника: наука, технология, бизнес. СПб., 2008. Спецвыпуск. С. 20–23.
4. Акимов С. В., Меткин Н. П. Архитектура среды многоаспектного моделирования для автоматизации решения задач исследования, проектирования и управления // Вопросы радиоэлектроники. 2013. Т. 1. № 1. С. 32–40.
5. Акимов С. В., Демидов А. А, Никифоров О. Г. Методология комплексных моделей системных объектов // Вопросы радиоэлектроники. Серия «Системы отображения информации и управления спецтехникой (СОИУ)», вып. 2, 2012. С. 138–149.
6. Akimov, S. V., Verkhova, G. V. The four-level integrative model methodology of structural and parametric synthesis of system objects // Proceedings of the 19th International Conference on Soft Computing and Measurements, SCM 2016. Pp. 321–323.

УДК 004.946
ГРНТИ 28.17.33

КОНЦЕПЦИЯ КОМПЛЕКСНОЙ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ ОБРАЗОВАТЕЛЬНЫМИ ПРОГРАММАМИ

С. В. Акимов, Г. В. Верхова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлена концепция комплексной автоматизации управления образовательной программой высшего учебного заведения на всех этапах жизненного цикла. В основу системы автоматизированного управления образовательной программой положена многоаспектная модель, отражающая различные стороны образовательной программы. Многоаспектная модель обеспечивает согласованность всех ресурсов и процессов, задействованных при разработке и реализации образовательной программы. Внедрение системы комплексной автоматизации управления образовательной программой обеспечит значительное сокращение временных затрат на подготовку и поддержку актуального состояния сопроводительной документации, сведение к минимуму ошибок, обусловленных человеческим фактором.

многоаспектная модель, образовательная программа, рабочий учебный план, рабочая программа, фонд оценочных средств, интерактивный учебно-методический комплекс, жизненный цикл.

В основу комплексной автоматизации современного университета должна быть положена непрерывная информационная поддержка жизненного цикла основных образовательных программ. Такая поддержка предполагает комплексную автоматизацию разработки и корректировки рабочих учебных планов, учебных программ, фондов оценочных средств, электронных образовательных ресурсов, планирования и распределения учебной нагрузки, материально-технического и кадрового обеспечения учебного процесса.

Киберсреда университета, в которой функционируют электронные образовательные ресурсы, а также обеспечивается непрерывная информационная поддержка жизненного цикла образовательных программ, основывается на трех базовых принципах: 1) агентности, 2) информационного самообслуживания и 3) управляемой информационной открытости [1].

Принцип агентности предполагает формирование мультиагентной сети, в которой каждый участник – юридическое или физическое лицо – самостоятельно регистрируется в виде независимого агента, имея полный контроль над собственным информационным профилем и установлением информационных связей с другими агентами, осуществляемых по запросу с последующим подтверждением. Все участники (агенты) цифровой среды являются равноправными вне зависимости от их положения в иерархии корпоративных отношений. Данный принцип делает киберсреду цифрового университета кардинально отличной от современных корпоративных информационных систем, имеющих централизованное управление, при котором регистрация сотрудников, формирование структуры предприятия и управление правами доступа осуществляется из единого центра. Глобальная академическая киберсреда складывается из локальных киберсред университетов и других организаций, реализуя принцип интероперабельности.

Принцип информационного самообслуживания подразумевает представление информации в киберсреде ее непосредственными обладателями, которые одновременно являются заинтересованными лицами в ее распространении для ограниченного или неограниченного круга лиц. Данный принцип гарантирует высокую степень актуальности и полноты информации, устраняя потребность в посредниках, участвующих в сборе, обработке и представлении информации, как это происходит в существующих корпоративных системах. Верификация информации может осуществляться способами, аналогичными применяемым в бумажном документообороте, путем установления отметок о подтверждении, заверенных электронной подпи-

сью. Кроме того, доступны и другие способы, например, установление ссылок на ресурсы систем научно-технической информации, включая базы данных патентов и индексов цитирования. Применение данного принципа обеспечит непрерывный мониторинг достижений всех участников учебного процесса (студентов, преподавателей, кафедр, факультетов и т. д.).

Управляемая информационная открытость подразумевает свободное распространение информации на основе набора лицензий, накладывающих ограничения на распространение, а также модификацию и удаление информации. Тип лицензии на информационные ресурсы определяется участниками сети, которые являются владельцами информации. Возможность дальнейшего изменения типа лицензии на опубликованный информационный ресурс может быть ограничено, что продиктовано необходимостью сохранения целостности информационных связей.

Информационная поддержка жизненного цикла образовательных программ базируется на системе комплексных моделей, отражающих различные аспекты учебного процесса [2]. На основе этих моделей реализуются процессы планирования, мониторинга и управления. В рамках предложенной концепции отчётная документация носит вспомогательный характер и генерируется автоматически на основе информации, содержащейся в моделях учебного процесса.

Применение интерактивных форм обучения базируется на мультимедийных учебно-методических комплексах, интегрированных в среду цифрового университета. Особенностью интерактивного мультимедийного учебно-методического комплекса является модульное построение курса дисциплины [3]. Каждый учебный модуль является относительно самостоятельным и содержит учебно-методические материалы для теоретических и практических занятий, а также фонд оценочных средств.

Управление индивидуальными траекториями обучения осуществляется на основе квалиметрических компетентностных моделей учащихся, учитывающих динамику академических достижений, личностного и профессионального роста. Интерактивные учебные комплексы имеют информационные связи с рабочими учебными программами и фондами оценочных средств, что гарантирует их взаимную согласованность. Другой особенностью интерактивных учебно-методических комплексов является наличие интегрированных средств квалиметрии, которые обеспечивают всестороннюю оценку качества учебных материалов.

Реализация непрерывной информационной поддержки жизненного цикла основных образовательных программ в рамках цифрового университета обеспечит:

– переход на новый качественный уровень разработки и реализации образовательных программ в рамках единой цифровой среды за счет высокой

степени автоматизации управления системами учебно-методических материалов, контингентом студентов, кадровыми и материально-техническими ресурсами университета;

– разработку и коррекцию основных образовательных программ с учетом потребностей цифровой экономики;

– многократное повышение эффективности учебно-методической работы преподавателей за счет сведение к минимуму рутинной работы, автоматизации процесса создания учебно-методических комплексов дисциплин, согласованных с рабочими программами, повторное использование ресурсов из единого фонда электронных учебных материалов;

– тиражирование опыта ведущих преподавателей и педагогических коллективов в рамках реализации основных образовательных программ с применением гибридных и электронных форм обучения;

– существенное повышение значимости электронного портфолио студента, путем включения его в систему индикаторов освоения компетенций образовательной программы, а также учета индивидуальных достижений и репутации при приеме на образовательные программы следующих уровней (магистратура, аспирантура) и рекомендаций при трудоустройстве;

– повышение качества управления университетом за счет внедрения непрерывного автоматического мониторинга процесса реализации основных образовательных программ; автоматическое вычисление рейтингов преподавателей, кафедр, факультетов и институтов на основе объективных показателей; автоматическое формирование комплектов отчетной документации по принципу «одной кнопки».

Список используемых источников

1. Верхова Г. В., Акимов С. В. Технологии виртуальных предприятий в формировании единой научно-образовательной киберсреды // Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации. Распознавание – 2017 сборник материалов XIII Международной научно-технической конференции. 2017. С. 105–107.

2. Акимов С. В., Верхова Г. В., Меткин Н. П. Теоретические основы CALS. СПб.: Изд-во Санкт-Петербургского гос. ун-та телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2018. 263 с. ISBN: 978-5-89160-172-7.

3. Попов К. А., Сторчилов П. А. Концентрическая модель построения учебного курса, ориентированного на реализацию внутрипредметных связей // Известия Волгоградского государственного педагогического университета. 2014. № 4 (89). С. 206–210.

УДК 004.946
ГРНТИ 28.17.33

ТЕХНОЛОГИЯ ЦИФРОВЫХ ДВОЙНИКОВ В МОНИТОРИНГЕ И УПРАВЛЕНИИ

С. В. Акимов, Г. В. Верхова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлена концепция цифровых двойников и их применение в мониторинге и управлении сложными техническими системами. Цифровой двойник представляет собой виртуальный образ объекта, синхронизированный с представляемым объектом посредством датчиков физических величин и исполнительных устройств. Цифровые двойники переводят процессы мониторинга и управления на качественно новый уровень. Применение цифровых двойников позволит создать глобальную киберсреду мониторинга и управления, обеспечивающую интеграцию отдельных киберфизических систем в единую систему. Формирование такой среды является первоочередной задачей, стоящей перед постиндустриальным обществом.

цифровой двойник, мониторинг, управление, многоаспектные модели, киберсреда, постиндустриальное общество, информационное общество.

Цифровой двойник (рис. 1) представляет собой виртуальный образ объекта, синхронизированный с этим объектом посредством датчиков физических величин и исполнительных устройств [1, 2]. В основу следующего поколения CALS будут положены цифровые двойники, что переведет процессы мониторинга и управления на качественно новый уровень.

CALS является развивающейся технологией и не предполагает наличия окончательной версии своего развития [3, 4]. На первом этапе (CALS I) путем стандартизации протоколов было упрощено взаимодействие между отдельными САПР, при этом передача данных осуществлялась напрямую – с помощью носителя данных или через вычислительную сеть. Структура документооборота на данном этапе развития оставалась подобной структуре бумажного документооборота. Следующий этап (CALS II) подразумевал наличие централизованной базы данных, входящей в состав PDM/PLM, что явилось важным шагом на пути глобальной информатизации и виртуализации предприятий и производств.

На следующем этапе (CALS III) представляется целесообразным вместо интегрированной базы данных использовать многоаспектную среду, базирующуюся на многоаспектных моделях. Подобное решение обеспечит смещение акцентов с отдельных компьютерных систем, автоматизирующих проектирование и управление, на процессы (проектирование, производство,

модернизация) и аспекты (структура, дизайн, функционирование, экономическая эффективность).

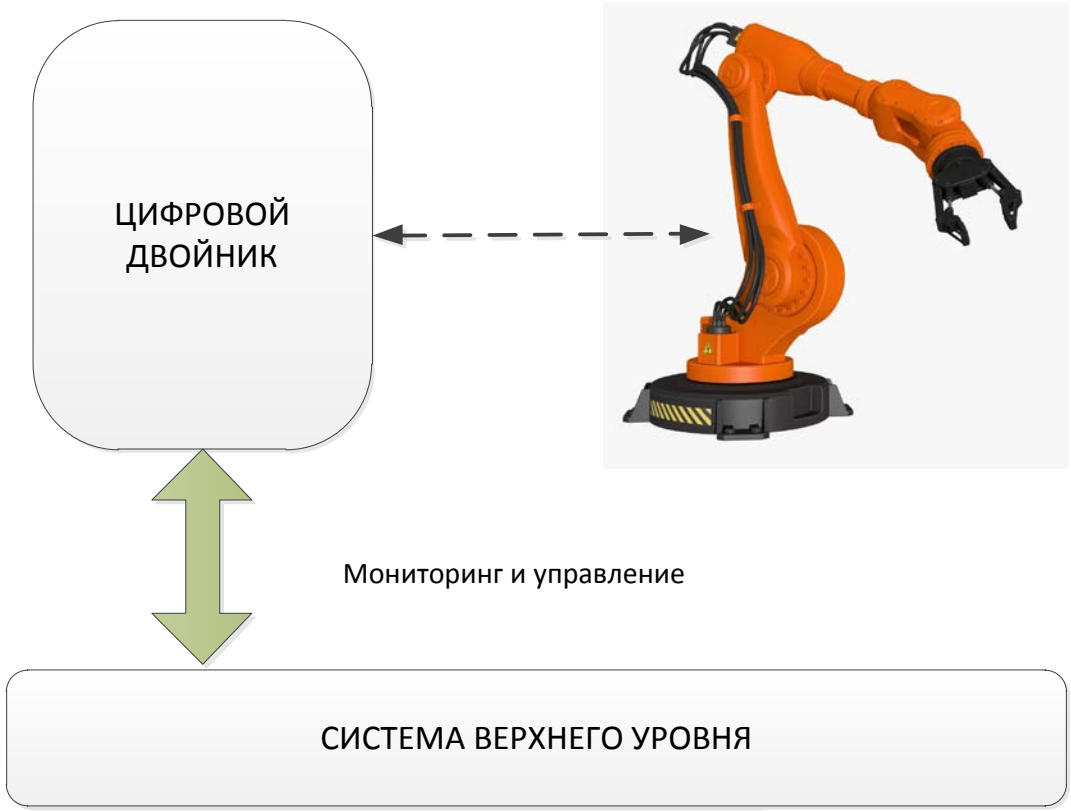


Рис. 1. Концепция цифрового двойника

Применение многоаспектных моделей позволит достичь нового уровня виртуализации, гарантируя полноту и целостность информации на всех этапах жизненного цикла, повышение степени повторного использования технических решений, динамическое формирование групп специалистов и распределенных производств, возможность управления как проектом, так и отдельно взятыми изделиями.

Наиболее подходящей методологией для создания цифровых двойников является методология многоаспектного моделирования. Основными понятиями многоаспектного моделирования являются аспект, модель, пространство, среда и объект. Аспект отражает некоторую сторону объекта, точку зрения, взгляд на объект; носит целевой характер, отражая отношение субъекта к объекту (системе). Примерами аспектов являются: функциональные, технологические, организационно-экономические аспекты, совместимости, надежности, унификации. Модели представляют собой формализмы, обеспечивающие один или несколько аспектов.

Пространство объединяет однотипные формализмы, входящие в состав моделей. К основным пространствам относятся структурно-параметрическое и функционально-алгоритмическое, к вспомогательным – связующее и мультимедийное. Структурно-параметрическое пространство содержит формализмы, реализующие формализованное представление параметров и структурных решений как отдельных системных объектов, так и классов, элементами которых они являются, а также формализованные представления таких объектов. Примерами структурно-параметрических пространств являются пространства принципиальных и функциональных схем, модели данных, множества структурных решений. Функционально-алгоритмические пространства содержат формализмы, обеспечивающие реализацию вычислительных, аналитических, поисковых и управляющих алгоритмов, применяемых при моделировании системных объектов, а также сами эти алгоритмы.

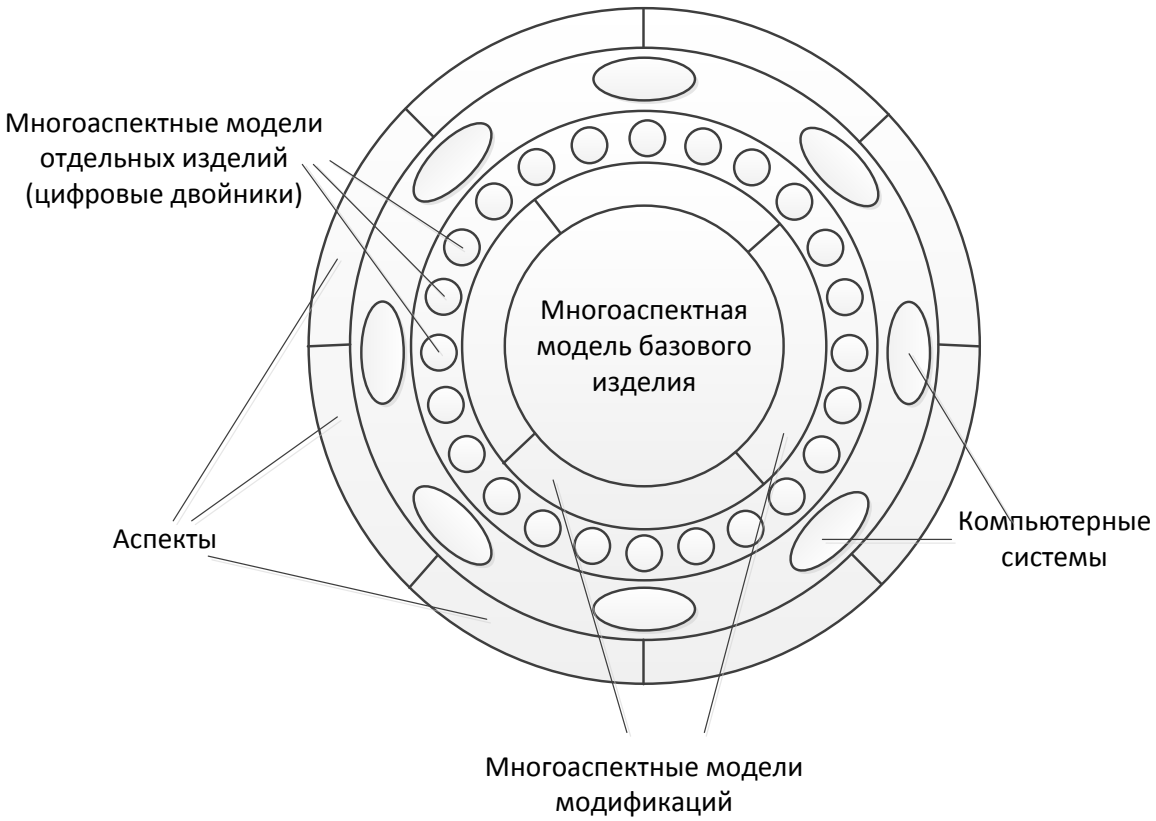


Рис. 2. Цифровые двойники в многоаспектной среде CALS третьего поколения

Связующее пространство обеспечивает связь элементов других пространств. В многоаспектном моделировании оно играет системообразующую роль, сводя отдельные формализмы и модели, представляющие аспекты, в единое целое, выполняя функцию, в чем-то сходную с функцией машины вывода в экспертных системах.

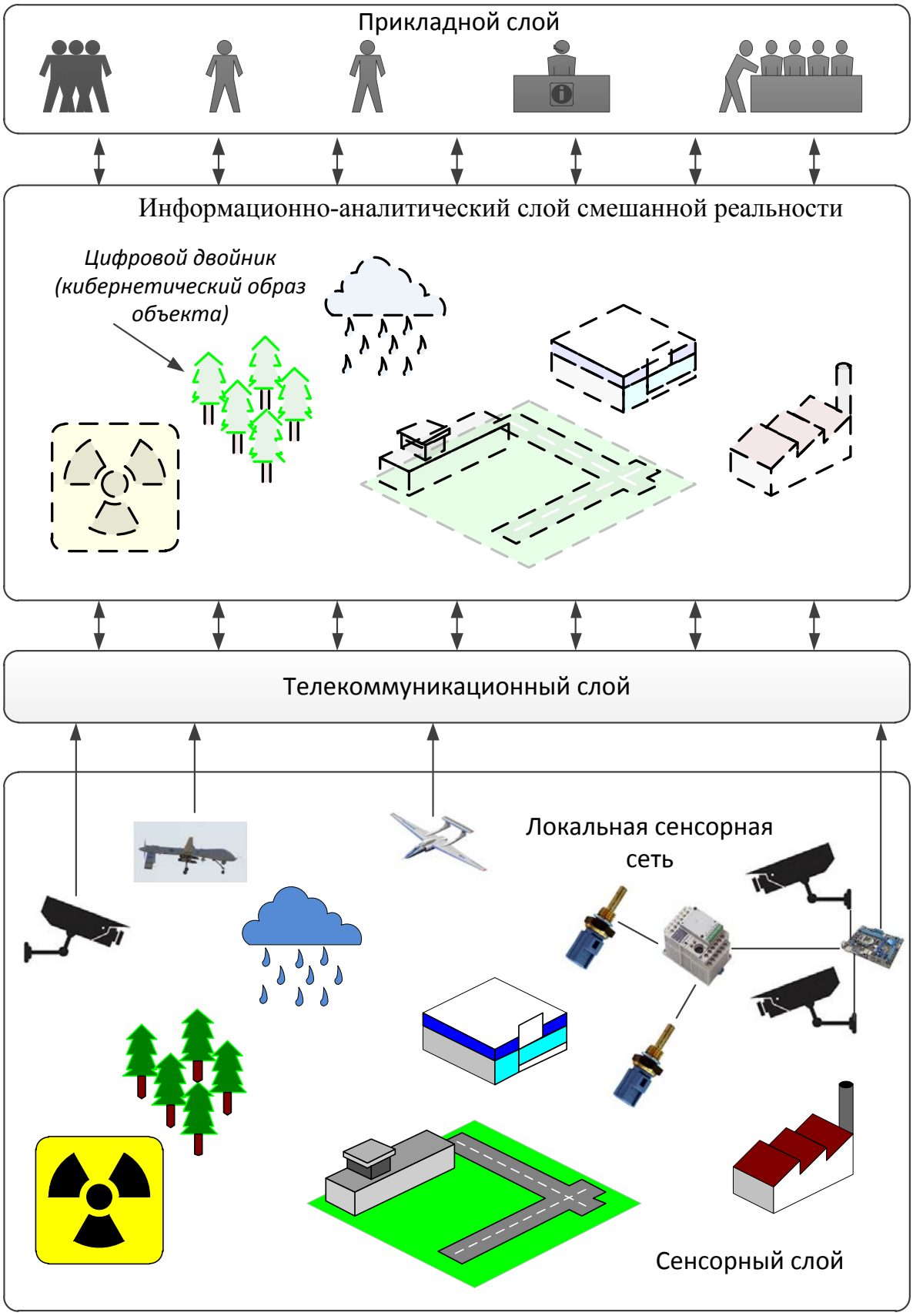


Рис. 3. Архитектура глобальной киберсреды мониторинга и управления, в основу которой положены цифровые двойники объектов

Наиболее адекватным способом реализации CALS третьего поколения является глобальная многоцелевая киберсреда мониторинга и управления, в которой будут функционировать цифровые двойники. Данная киберсреда состоит из четырех слоев (см. рис. 3). Сенсорный слой обеспечивает сбор и первичную обработку информации об объектах мониторинга. В качестве сенсоров выступают всевозможные датчики физических величин и аудиовизуальные средства наблюдения, включая 3D видео высокой четкости.

Сенсоры и средства наблюдения могут быть как стационарными, так и установленными на ПЛА и БПЛА, автоматических зондах, ИСЗ, подводных и надводных плавательных средствах.

Предложенный в статье подход мониторинга и управления базируется на цифровых двойниках, функционирующих в глобальной киберсреде постиндустриального (информационного) общества. Глобальная киберсреда является объединением локальных многоцелевых и специализированных киберсред. В основу цифровых двойников положены многоаспектные модели, которые могут быть использованы на всех этапах жизненного цикла изделия (объекта), для которого создается цифровой двойник. Это обеспечит возможность максимально полного согласования жизненного цикла изделия и его цифрового двойника. Сами цифровые двойники могут состоять из цифровых двойников компонентов, из которых состоит объект. Тем самым обеспечивается отслеживание (а, следовательно, и управление) жизненного цикла не только изделия, но и всех его составляющих. Это поднимает процесс кибернетизации промышленности и общества в целом на качественно новый уровень, недостижимый при использовании традиционных информационных технологий.

Список используемых источников

1. Xiuyu, C., Tianyi, G. Research on the Predicting Model of Convenience Store Model Based on Digital Twins // 2018 IEEE International Conference on Smart Grid and Electrical Automation (ICSGEA). 2018. Pp. 224–226.

2. Xiang, F., Zhi, Z., Jiang, G. Digital twins technolgy and its data fusion in iron and steel product life cycle // 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC). 2018. Pp. 1–5.

3. Saaksvuori, A., Immonen, A. Product Lifecycle Management. Berlin: Springer. 2008. 254 p.

4. Акимов С. В., Верхова Г. В., Меткин Н. П. Теоретические основы CALS. СПб.: Изд-во Санкт-Петербургского гос. ун-та телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2018. 263 с. ISBN: 978-5-89160-172-7.

УДК 004.42
ГРНТИ 50.41.25

ПРОГРАММНЫЙ МОДУЛЬ АВТОМАТИЧЕСКОЙ ГЕНЕРАЦИИ БЛАНКОВ ДЛЯ ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ В ФОРМАТЕ ДОКУМЕНТА MS WORD

С. В. Акимов, Э. Р. Давлетшина, М. Н. Попова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлена разработка прототипа модуля автоматической генерации бланков для выпускных квалификационных работ (ВКР). Целью проекта является генерация бланков ВКР и автоматическое формирование отчетов в формате Microsoft Word. Модуль предназначен для работы в рамках системы комплексной автоматизации высшего учебного заведения, и допускает интеграцию в киберсреду EJ-IK (Education Job International Keeper).

автоматическая генерация, автоматизация, генерация отчетов, C#, Office Open XML.

Технологии автоматической генерации документов, отчетов являются очень востребованными на сегодняшний день, так как это значительно повышает эффективность, производительность и качество процессов подготовки различных отчетов, бланков, как на любом предприятии, так и в образовательных учреждениях. В каждом высшем учебном заведении выпускникам, преподавателям и другим сотрудникам организации предстоит заполнять и составлять множество документов, заявлений и другие формы в бумажном виде. Автоматический генератор документов и рассчитан для того, чтобы упростить процесс рутинного заполнения бланков ВКР, тем самым сведя к минимуму ошибки, возникающие при невнимательности человека. В этом и заключается основная цель и задача настоящего проекта.

Функция данного модуля состоит в том, чтобы автоматически формировать и заполнять бланки для выпускных квалификационных работ в документы формата MS Word. Генерация происходит по нажатию всего одной кнопки.

Система будет генерировать следующие бланки: список ВКР, заявление на тему ВКР, титульный лист, задание, календарный план, отзыв научного руководителя и отзыв рецензента.

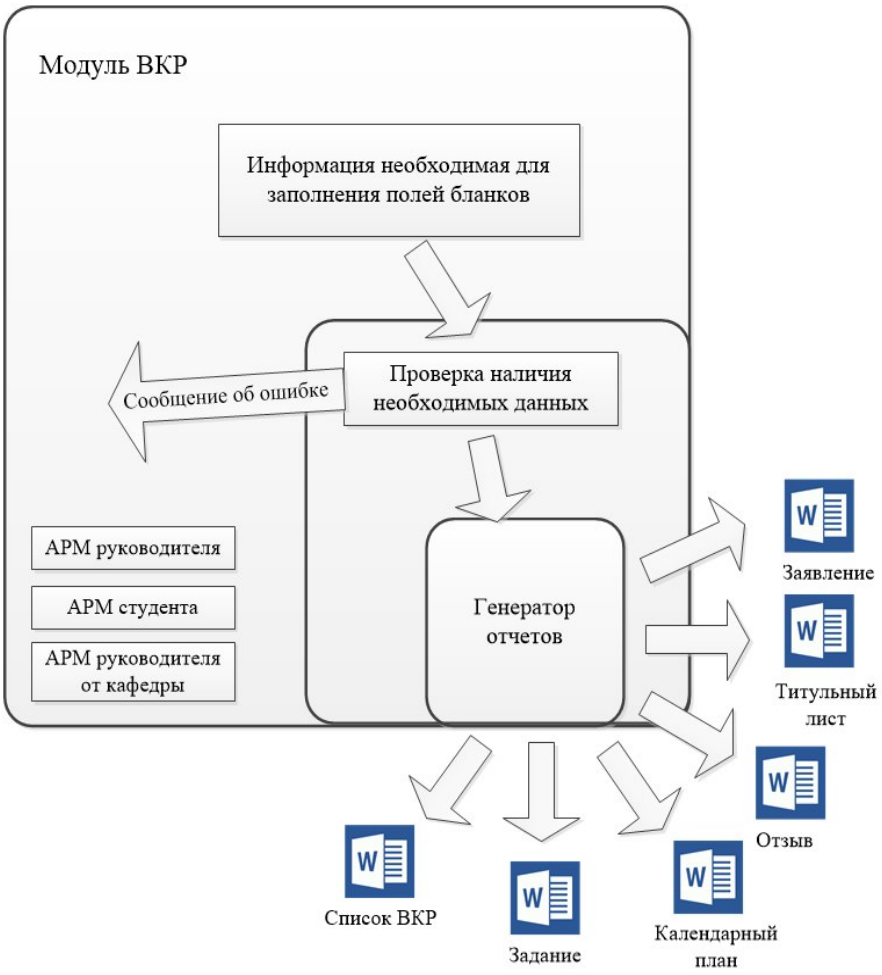


Рис. 1. Место модуля в управлении ВКР

Данный программный модуль является частью автоматизированной системы управления выпускными квалификационными работами, из которого и поступает вся необходимая информация для заполнения полей в бланках [1]. На рис. 1. представлено место программного модуля в автоматизированной системе управления жизненным циклом ВКР.

Для осуществления генерации того или иного бланка модуль получает данные из системы управления ВКР, такие как: название темы ВКР; ФИО и должность научного руководителя; выпускающая кафедра; факультет, направление, специальность, группа и ФИО студента и др.

Разработка осуществлялась на базе объектно-ориентированного программирования, так как этот подход наиболее эффективен и применим для данного модуля. Проект реализуется с помощью языка программирования C#. Для генерации бланков выпускных квалификационных работ использован пакет SDK 2.5 Open XML для Office, который позволяет управлять документами, соответствующими спецификации форматов файлов Office Open XML. Он требуется для того, чтобы сгенерировать программный код на C# для предварительно созданного шаблона документа формата

MS Word. Данные манипуляции проделываются для упрощения работы разработчика в написании кода структуры документов (шаблонов).

Пакет SDK 2.5 Open XML упрощает управление пакетами Open XML и элементами схемы Open XML. Программа выполняет множество стандартных задач, необходимых при работе с пакетами Open XML, поэтому сложные операции можно осуществлять всего несколькими строками кода [2].

Окно программного пакета SDK 2.5 Open XML изображено на рис. 2. Через кнопку Open File загружается документ, для которого необходимо сгенерировать код, затем, нажимая кнопку Reflect Code, справа в окне отображается сгенерированный код всего документа.

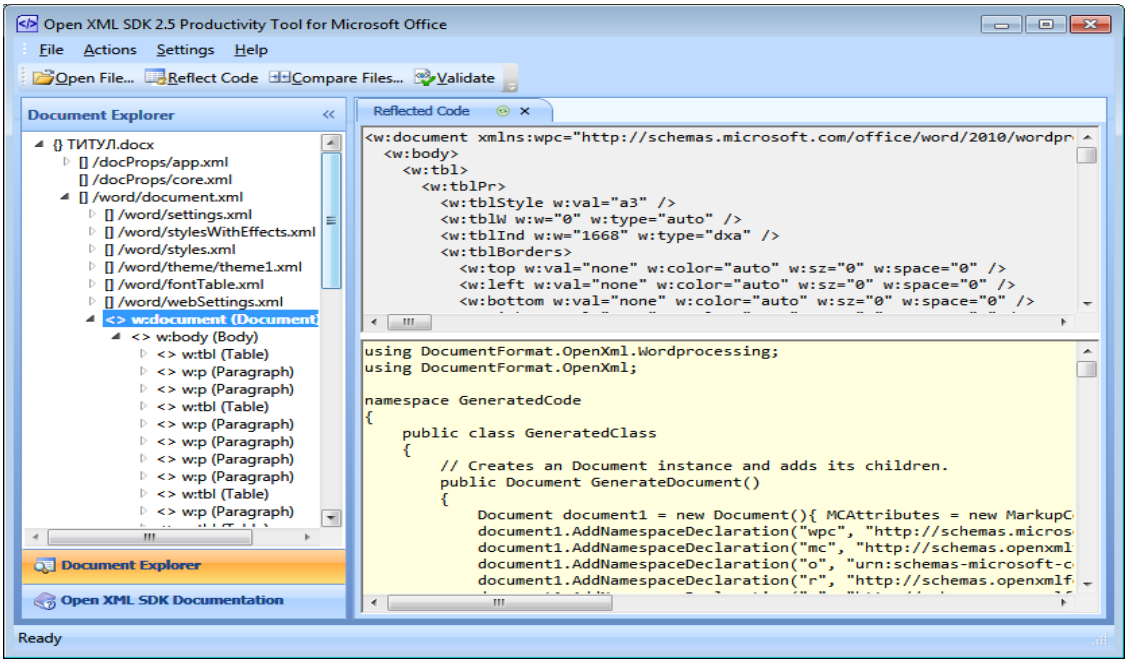


Рис. 2. Рабочее окно SDK 2.5 Open XML

Структура данного модуля представляет генератор бланков, который с помощью заданного шаблона осуществляет его формирование. Каждый бланк для ВКР имеет свой шаблон, чтобы упростить генерацию документа. Выбор шаблона осуществляется по заданному алгоритму. Пример устройства программного модуля можно увидеть на рис. 3.

Для заполнения бланков установим связи между свойствами объектной модели автоматизированной системы управления жизненным циклом ВКР и данными в сгенерированном документе на примере бланка титульного листа (рис. 4).

Основная идея модуля состоит в мгновенной генерации бланков ВКР, быстром формировании отчетов и точном заполнении необходимых документов, по нажатию пользователем всего одной кнопки.

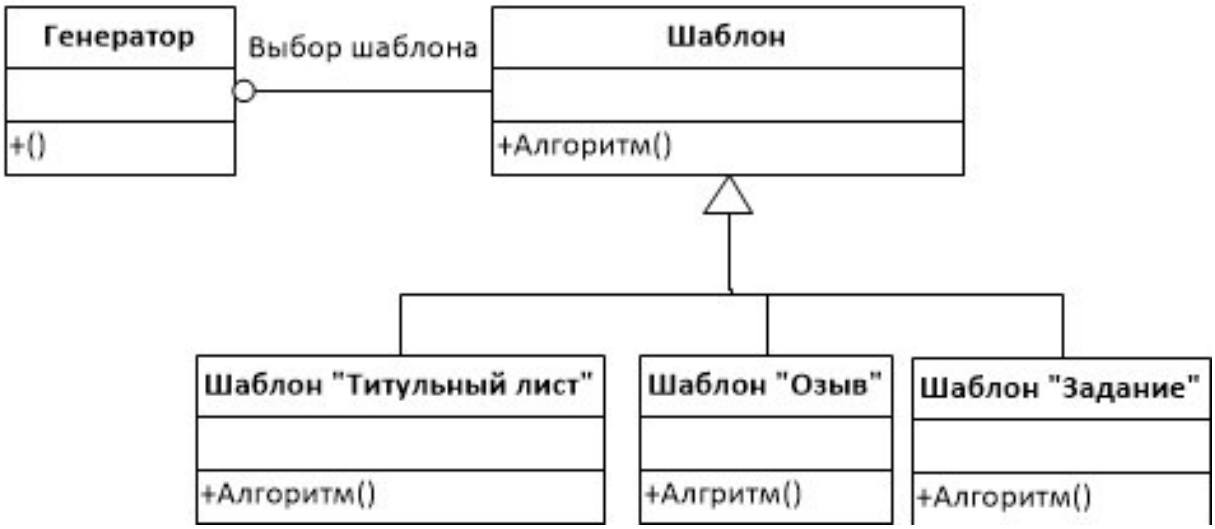


Рис. 3. Архитектура модуля на базе паттерна

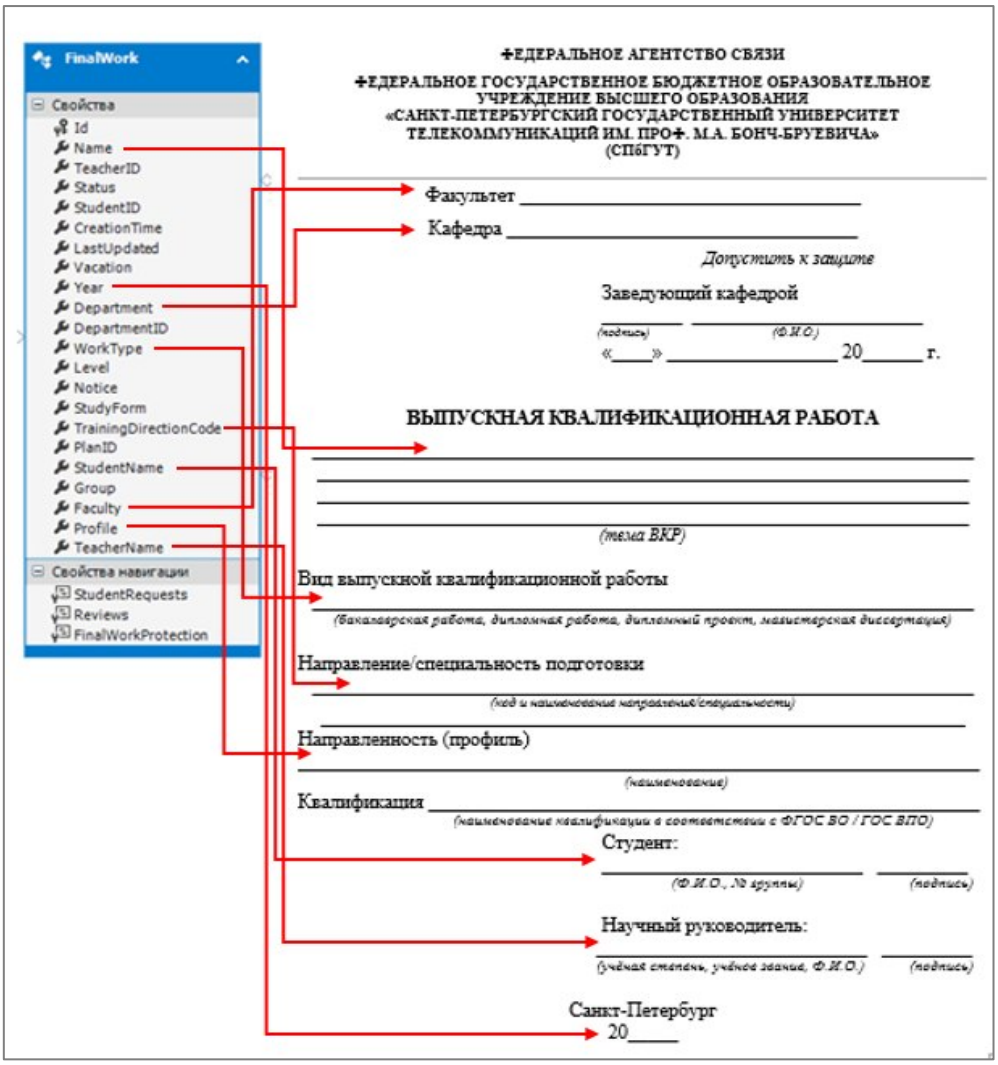


Рис. 4. Связь между свойствами сущности ВКР и бланком титульного листа

Список используемых источников

1. Акимов С. В., Давлетшина Э. Р., Попова М. Н. Модуль управления выпускными квалификационными работами для системы электронного обучения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 443–446.
2. Open XML SDK 2.5// UML: https://msdn.microsoft.com

УДК 004.056.53
ГРНТИ 49.33.35

МЕТОДИКА ПРОВЕРКИ ОБЪЕКТНО-ОРИЕНТИРОВАННОЙ СИСТЕМЫ НА НАЛИЧИЕ ВОЗМОЖНОСТЕЙ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Т. Ю. Алмаев, О. М. Лепешкин

Военная академия связи им. Маршала Советского Союза С. М. Буденного

На сегодняшний день возможность несанкционированного доступа к данным является одной из основных проблем обеспечения безопасности информации. Для решения этой проблемы принято проводить анализ компьютерной системы на основе дискреционной модели безопасности. В связи с чем появляется необходимость выработки методики проверки объектно-ориентированных систем на возможность утечки права доступа.

объектно-ориентированная система, модель безопасности, несанкционированный доступ, методика.

Одним из способов обеспечения безопасности системы является разграничение доступа, при котором пользователи могут получить доступ только к информации, необходимой им для выполнения своих функциональных обязанностей или других задач.

При описании модели разграничения доступа все составляющие операционной системы разделяются на активные, или субъекты, и пассивные, или объекты.

Для описания модели разграничения доступа достаточно указать принципы ограничения доступов некоторых субъектов к некоторым объектам, т.е. описать множество допустимых потоков. Исходя из способов наложения ограничений на доступ различают следующие типы моделей разграничения доступа [1, 3]:

1. Дискреционные политики безопасности.
2. Мандатные политики безопасности.
3. Ролевые политики безопасности.
4. Тематические политики безопасности.
5. Политики безопасности информационных потоков.
6. Субъектно-объектная модель программной среды.

Каждый тип моделей имеет свои достоинства и недостатки, потому в практических решениях чаще всего используют одновременно несколько моделей или комбинацию различных подходов.

В политике *дискреционного доступа* множество допустимых доступов задается для субъектов и объектов явным образом, т. е. перечислением всех допустимых троек субъект-объект-право доступа [2, 3].

В политике *мандатного доступа* множество допустимых доступов задается неявно, через введение для субъектов системы характеристики *уровня допуска,* а для объектов – характеристики *конфиденциальности.* Субъекты наделяются правом порождать потоки в зависимости от соотношения уровня допуска субъекта, порождаемого потока и уровня конфиденциальности объекта.

В политике *тематического доступа* множество допустимых доступов задается неявно с помощью присвоения каждому субъекту множества *разрешенных тематических информационных рубрик,* а каждому объекту присваивается множество *тематических рубрик,* информация по которым содержится в данном объекте.

В политике *ролевого доступа* в системе вводятся дополнительные абстрактные сущности – *роли* (или ролевые субъекты), выступающие типовыми субъектами доступа, с которыми ассоциируются конкретные пользователи. Ролевые субъекты наделяются правами доступа к объектам системы на основе дискреционной или мандатной политик безопасности.

При описании методики будем использовать дискреционную политику безопасности [1, 2, 3, 4]. Среди известных моделей дискреционного разграничения доступа модель Харрисона-Руззо-Ульмана (*Harrison-Ruzzo-Ulman*, HRU) [1, 2, 3] является одной из наиболее проработанных в математическом плане моделей.

В рамках объектно-ориентированной модели у объектов существует два вида полей – *private* **(P)** и *public* **(F)**, а также множество методов **S.** К скрытым полям *(private)* доступ осуществляется методами самого объ-

екта, поэтому разрешения на доступ к таким полям сводятся к разрешениям активизации соответствующих методов объекта. Для открытых полей (*public*) можно считать верным следующее предположение: *открытые поля всех объектов имеют одно и то же множество возможных типов доступа.* Множество доступов к открытым полям обозначим через **R**.

В силу того, что набор методов работы со скрытыми полями у каждого объекта свой определение общей матрицы доступов для всей компьютерной системы лишено смысла. Для построения системы дискреционного разделения доступа модифицируем все объекты системы, введя для каждого объекта $o \in O$ дополнительное *private* поле M, содержащее локальную матрицу доступов, и методы работы с матрицей доступов:

$$o.M: O \times (o.F \cup o.S) \rightarrow 2^R \cup \{0,1\},$$

причем

$$o'.M[o,f] \in 2^R (o, o' \in O),,$$

где $f \in o'.F$, то есть для открытых полей в явном виде задается множество разрешенных доступов, и

$$o'.M[o,s] \in \{0,1\} \ (o, o' \in O),$$

где $s \in o'.S$, то есть для методов определяем разрешение (1) или запрет (0) вызова.

Состояния компьютерной системы в модели HRU изменяются под воздействием запросов на модификацию матрицы доступа в виде команд следующего формата:

Command $g(x_1,\ldots,x_g)$:

If < конъюнкция логических выражений вида $r \in o'.M[o, f]$ или $o'.M[o,s]=1$ >

then < последовательность элементарных операторов >.

HRU-модель системы безопасности называется монооперационной, если каждая команда в этой системе содержит только один элементарный оператор.

HRU-модель системы безопасности называется моноусловной, если каждая команда в этой системе содержит только одно условие. HRU-модель системы безопасности называется моноусловной, если каждая команда в этой системе содержит только одно условие.

HRU-модель системы безопасности объектно-ориентированной компьютерной системы называется монотонной, если команды этой системы не содержат операторов Delete, Deprive и Destroy.

Будем говорить, что состояние системы Q(t) допускает утечку права доступа $r \in R$, если существуют такие команда g, объект o и поле o'.f объекта o', что $r \notin o'.M[o, f](t)$, но $r \in o'.M[o, f](t+1)$, где $Q(t) \rightarrow_g Q(t+1)$.

Будем говорить, что состояние системы Q(t) допускает утечку права вызова, если существуют такая команда g, объект o и метод o'.s объекта o', что $o'.M[o, f](t)=0$, но $o'.M[o, f](t+l)=l$, где $Q(t) \rightarrow_g Q(t+1)$.

Будем говорить, что система r-безопасна, если не существует такой последовательности команд $g_1 \ldots g_T$, $Q(t-1) \rightarrow_{gt} Q(t)$, $t=1,\ldots,T$, и Q(T) допускает утечку права r либо утечку права вызова.

Проведем классификацию объектно-ориентированных моделей безопасности с дискреционным разграничением доступа, разделив все модели на две группы – без наследования классами прав доступа (группа P) и с наследованием классами прав доступа (группа H). В каждой из моделей присутствует свой аналог монооперационной и монотонно-моноусловной системы, допускающих алгоритмическую проверку безопасности. Таким образом, получаем следующую классификацию:

F1. Базовая (неоднородная) модель объектно-ориентированной системы без наследования. В данной модели каждый объект принадлежит определенному классу, при этом все классы независимы.

FZ. Безусловная неоднородная модель, включающая в себя всевозможные команды.

HO. Однородная модель с иерархией. В данной модели все объекты класса обладают одинаковым набором прав доступа к полям и методам всех объектов другого класса, при этом классы связаны между собой иерархией наследования.

H1. Неоднородная модель с иерархией. Отличается от модели F1 заданием строгой связи – иерархии – на множестве классов.

H2. Финально-неоднородная модель с иерархией.

HZ. Безусловная неоднородная модель с иерархией, включающая в себя всевозможные команды.

Составим в пошаговой форме инструкции по проверке объектно-ориентированной модели безопасности на возможность утечки права доступа.

1. В первую очередь необходимо составить список прав доступа и список классов системы с описанием полей и методов. Каждому праву и каждому классу присвоен натуральный порядковый номер.

2. Составить список всех команд системы. Для упрощения дальнейшей обработки данных команду удобно представлять, как объект, содержащий три списка: список аргументов (А), в котором перечислены классы, список условий (У) и список элементарных операторов (О).

3. Установить, относится ли данная система безопасности к одному из классов, допускающих проверку безопасности.

3.1 Алгоритм проверки на монооперационность.

Шаг 1. Устанавливаем значение monooperational:≡ TRUE. Выбираем первую команду из списка команд. Переходим на Шаг 2.

Шаг 2. В текущей команде находим список О. Если указатель первого элемента списка О не указывает на NULL, присваиваем monooperational:≡ FALSE. Переходим на Шаг 3.

Шаг 3. Если monooperational ≡ TRUE и текущая команда – не последняя в списке, переходим на Шаг 4, в противном случае – на Шаг 5.

Шаг 4. Выбираем следующую команду из списка и переходим на Шаг **2.**

Шаг 5. Возвращаем значение переменной monooperational и завершаем работу.

Если по окончании работы алгоритма переменная monooperational принимает значение TRUE, то система является монооперационной. В этом случае мы можем выполнить проверку на r-безопасность системы согласно алгоритму, для монооперационной объектно-ориентированной модели, а именно, изучить результаты применения к системе конечного количества цепочек команд конечной длины, на основании чего сделать выводы о возможности утечки права доступа.

Если система оказалась немонооперационной, переходим к пункту 3.2

3.2 Алгоритм проверки на монотонность и моноусловность.

Шаг 1. Устанавливаем значения monotone:= TRUE, monoconditional:=TRUE. Выбираем первую команду из списка команд. Переходим на Шаг 2.

Шаг 2. В текущей команде находим список У. Если указатель первого элемента списка У не указывает на NULL, присваиваем monoconditional:=FALSE. Переходим на Шаг 3.

Шаг 3. Выбираем первый элементарный оператор из списка О, если он не пуст. Переходим на Шаг 4. Если список пуст, переходим на Шаг 7.

Шаг 4. Если первое поле текущего оператора принимает значение Delete или Destroy, присваиваем monotone:=FALSE. Переходим на Шаг 5.

Шаг 5. Если указатель шестого поля текущего элементарного оператора из списка О указывает на NULL или monotone:=FALSE, переходим на Шаг 7. В противном случае переходим на Шаг 6.

Шаг 6. Выбираем следующий оператор из списка O. Переходим на Шаг 4.

Шаг 7. Если monotone:=TRUE , monoconditional:=TRUE и текущая команда – не последняя в списке, переходим на Шаг 8. В противном случае переходим на Шаг 9.

Шаг 8. Выбираем следующую команду из списка. Переходим на Шаг 2.

Шаг 9. Возвращаем значение переменных monotone и monoconditional. Завершаем работу алгоритма.

Если по окончании работы алгоритма переменные monotone и monoconditional принимают значения TRUE, то система является монотонной и моноусловной. В этом случае мы можем выполнить проверку на r-безопасность системы согласно алгоритму, для моноусловной монотонной объектно-ориентированной модели.

4. Если удалось установить принадлежность системы к одному из рассмотренных выше классов, допускающих проверку безопасности, осталось только произвести необходимую проверку и установить, является ли данная система безопасной.

Приведенная выше методика, безусловно, не может дать исчерпывающего ответа на вопрос о безопасности объектно-ориентированной системы общего вида, поскольку определяемые ею классы безопасности отличаются сниженной функциональностью по сравнению с системами общего вида. Однако это неизбежная плата за возможность гарантировать корректное разграничение прав доступа.

Список используемых источников

1. Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах. Е.: Изд-во Уральского Университета, 2003. 328 с.

2. Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. М.: Яхтсмен, 1996. 192 с.

3. Девянин П. Н. Модели безопасности компьютерных систем: Учебное пособие для студентов высших учебных заведений. М.: Академия, 2005. 144 с.

4. Теоретические основы компьютерной безопасности: учебное пособие для вузов / П. Н. Девянин и др. М.: Радио и связь, 2001. 192 с.

УДК 621.317
ГРНТИ 45.01.85

К ВОПРОСУ О ПРИМЕНЕНИИ ПРОГРАММИРУЕМЫХ ДИСКРЕТНО-АНАЛОГОВЫХ ИНТЕГРАЛЬНЫХ СХЕМ В СОВРЕМЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ

Д. С. Андреев, А. В. Ваганов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается возможность использования программируемых дискретно-аналоговых интегральных схем (ПДАИС) в современных автоматизированных системах управления. Показана актуальность применения данного класса микросхем, а также произведено сравнение их параметров с характеристиками современных аналоговых и цифровых ЭРИ, применяемых для построения систем обработки сигналов. Даны рекомендации к использованию математических моделей для описания подобных систем.

интегральная схема, ПДАИС, аналоговый сигнал, цифровой сигнал.

Важной особенностью развития человеческого общества в настоящее время является все возрастающая роль электроники во всех сферах жизни и деятельности людей. Достижения в данной области в значительной мере способствуют успешному решению сложнейших научно-технических проблем, повышению эффективности научных исследований, созданию новых видов машин и оборудования, разработке эффективных технологий и систем управления, получению материалов с уникальными свойствами, совершенствованию процессов сбора и обработки информации и др.

Началом развития данной области следует считать начало прошлого века, когда электроника как наука сформировалась после изобретения лампового диода, трехэлектродной лампы-триода и электронно-лучевой трубки. Середина годов прошлого века ознаменовалась появлением дискретных полупроводниковых приборов (диодов, транзисторов, тиристоров и т. д.). В период с 1960-х по 1980-е годы появились микросборки и первые интегральные схемы различной степени интеграции, дальнейшее развитие которых вылилось в миниатюризацию и появлением больших и сверхбольших интегральных схем.

К настоящему времени все электронные устройства можно отнести к двум основным группам – это аналоговые и цифровые (дискретные).

К настоящему времени не удается полностью исключить применение и аналоговых систем обработки сигнала, например, в таких областях как радио- и гидролокация, диагностическая медицина, устройства сбора информации в многоканальных системах и т. п. Это объясняется тем, что некоторые первичные измерительные преобразователи (датчики) по-прежнему являются аналоговыми и информативная (полезная) составляющая сигнала, поступающая с выходов таких систем, имеет малую амплитуду на фоне большой статической помехи и крайне низкое соотношение сигнал-шум. В этом случае между датчиком и аналого-цифровым преобразователем основной системы размещают промежуточное звено – аналоговый тракт предварительной (первичной) обработки сигнала, основной функцией которого является нормализация исходного сигнала от датчика и приведение его к виду, обеспечивающему максимальную эффективность его дальнейшей обработки цифровым (вторичным) трактом.

На сегодняшний момент реализация первичного тракта обработки сигнала, как правило, производится на дискретных компонентах – резисторах, конденсаторах транзисторах, операционных усилителях, мультиплексорах, компараторах и т. п. При этом в ряде случаев аналоговая часть занимает значительную часть площади платы электронного устройства, имеет низкую температурную и временную стабильность, а также высокую стоимость. Решить данную проблему при создании разнообразных аналоговых устройств, одновременно снизив стоимость и повысив эффективность проекта в целом, позволяет использование программируемых аналоговых интегральных схем – ПАИС (FPAA). Разработкой подобных систем занимаются несколько фирм: Anadigm (США), Lattice (США), PAC-Designer (США).

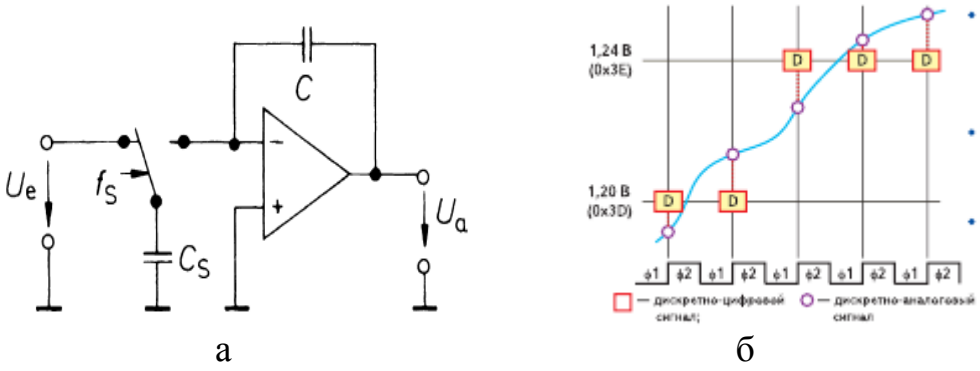
Сравнительные характеристики процессора AN2031E04 фирмы Anadigm с дискретными аналоговыми и цифровыми ЭРИ приведены в таблице.

ТАБЛИЦА. Сравнительные характеристики групп ЭРИ

Параметр \ Тип ЭРИ	Аналоговые	Цифровые	Дискретно-аналоговые
Максимальная частота обрабатываемого сигнала, МГц	10–15	5	2
Точность преобразования сигнала, %	менее 0,1	0,1	0,1
Уровень собственного шума, мкВ√Гц	3–5	–	4
Соотношение сигнал-шум, дБ	менее 60	более 100	90

Параметр \ Тип ЭРИ	Аналоговые	Цифровые	Дискретно-аналоговые
Возможность динамического перепрограммирования	нет	нет	да

Обработка сигнала внутри ПДАИС осуществляется схемами на переключаемых конденсаторах (рис. 1 а) [1]. В отличие от цифровых систем, где сигнал дискретен по времени и квантован по уровню, в дискретно-аналоговых системах сигнал дискретен только по времени (рис. 1 б), в силу этого выходной аналоговый сигнал можно восстановить без искажений по его выборкам и точность преобразования может достигать десятых долей процента.



а б

Рис. 1. Схема инвертирующего *SC*-интегратора (а)
и процесс аналоговой и цифровой дискретизации (б)

Представление дискретизированного по времени сигнала в таких системах есть результат умножения «запомненных» мгновенных значений исходной непрерывной функции $f(nT)$, на специальную импульсную последовательность очень узких импульсов $\tau \to 0$, получая некую импульсную амплитудную модуляцию – дискретизированный эквивалент:

$$f^*(t) = \sum_{n=0}^{\infty} f_n(t) = K \cdot \sum_{n=0}^{\infty} f(nT) \cdot \left[u(t - nT) - u\left(t - (nT + \tau)\right) \right], \qquad (1)$$

где T – период дискретизации, τ – ширина импульса, K – коэффициент передачи буферного усилителя, n – отсчет дискретизированной функции, $u(t)$ – функция Хевисайда.

Период следования импульсов квантования определяется теоремой Котельникова-Шеннона [2]. Для защиты от наложения спектров квантованных сигналов используют инженерное решение, применяемое в цифровой обработке сигналов, когда ещё до квантования сигнала с помощью фильтра

предварительной обработки ограничивают полосу сигнала необходимой ширины.

Структурная схема квантователя показана на рис. 2. Он состоит из идеального квантователя и фиксатора (экстраполятора) нулевого порядка. Идеальный квантователь формирует импульсы бесконечно малой ширины $\tau \to 0$, а фиксатор представляет собой устройство выборки-хранения.

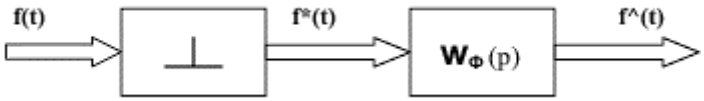


Рис. 2. Структурная схема квантователя непрерывного сигнала дискретно-аналоговой системы.

Для удобства описания дискретно-аналоговых устройств используют аппарат для цифровых систем – *z*-преобразование. Процедура перехода от аналогового аппарата к z-преобразованию состоит из двух этапов. Первый заключается в получении изображения эквивалента сигнала $f^*(t)$ после преобразования Лапласа в виде:

$$F^*(s) \Leftrightarrow \int_{t=0}^{\infty} f^*(t) \cdot e^{-st} dt . \qquad (2)$$

Второй – строиться в предположении, что площадь каждого импульса эквивалента $f^*(t)$ равна $f(nT)$ и, соответственно, в выражении (1) имеет место условие $K = 1/\tau$. Тогда зависимость (2) можно представить в виде:

$$F^*(s) = \sum_{n=0}^{\infty} f(nT) \cdot e^{-snT} = \sum_{n=0}^{\infty} f(nT) \cdot z^{-n}, \qquad (3)$$

где $z = e^{sT}$.

Для примера опишем получение передаточной функции для идеального инвертирующего *SC*-интегратора (рис. 1) в *z*-области. Выражение его передаточной функции во временной области имеет вид:

$$U_a(nT) - U_a((n-1)\,T) = -\frac{C_s}{C} \cdot U_e(nT). \qquad (4)$$

Полагая, что второй член в левой части выражения (4) описывает потенциал, присутствующий на конденсаторе *C* с момента времени $t = (n - 1) \cdot T$ и задержанный на период *T* относительно момента $t = (n - 1)$. Поэтому после *z*-преобразования выражения (4) и представления каждого слагаемого от

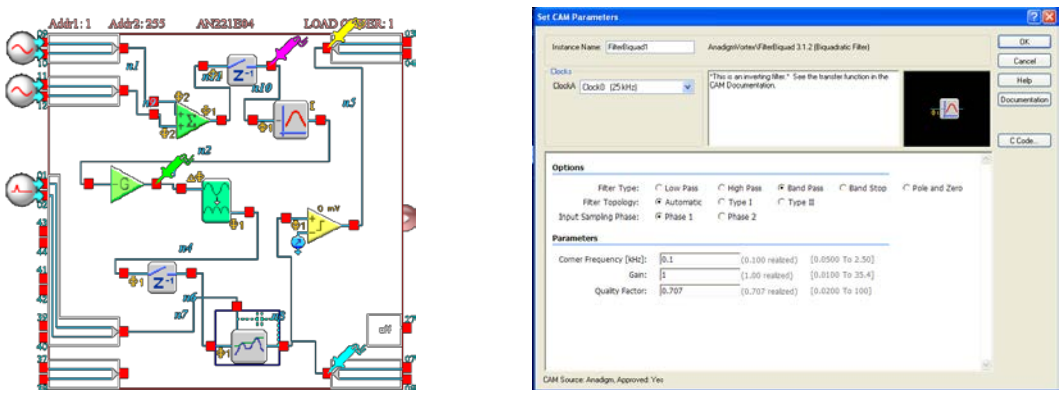
функции z, передаточную функцию SC-интегратора в z-области запишем в виде:

$$H_{sc}(z)=\frac{V_a(z)}{V_e(z)}=-\frac{C_s}{C}\cdot\frac{1}{1-z^{-1}}. \quad (5)$$

Современные дискретно-аналоговые микросхемы являются аппаратно-программными, поэтому для разработки соответствующих программ и отладки проекта в целом используют специализированные пакеты программ. Так для ПАИС фирмы Anadigm разработчики используют программу Anadigm Designer 2, которая позволят осуществлять разработку устройств на основе графического программирования [3].

В качестве примера разработки в такой среде рассмотрим классическую схему устройства, предназначенного для обнаружения сигнала на фоне помех (рис. 3 а), содержащего тракт предварительной обработки сигнала. В качестве источников полезного сигнала и помехи использованы два имитатора генераторов, сигналы от которых поступают на сумматор и далее на полосовой фильтр. После прохождения через прецизионный двухполупериодный выпрямитель сигнал подается на пиковый детектор и далее на рабочий вход компараторов.

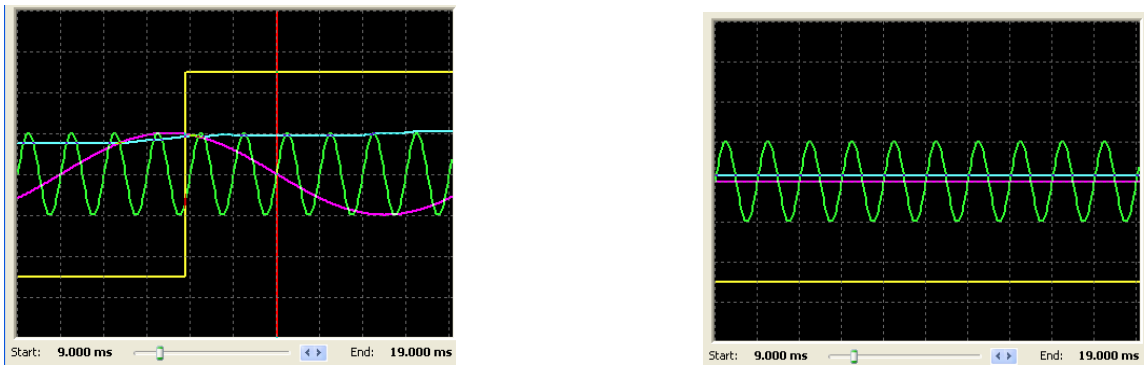
Задание значений коэффициентов передачи усилителей, частот среза фильтров, порога срабатывания компаратора осуществляется в соответствующем меню конкретного функционального конфигурируемого аналогового модуля – КАМа (рис. 3 б). При этом частота тактирования КАМа должна превышать максимальную частоту полезного сигнала как минимум на два порядка. Использование пикового детектора с внешним конденсатором позволяет получать малую скорость спада величины «запомненного» входного сигнала.



а б

Рис. 3. Проект обнаружителя сигнала на фоне помех в среде Anadigm Designer 2 (а) и меню КАМ биквадратного фильтра (б)

Результат моделирования обнаружителя показан на рис. 4, из которого следует, что устройство формирует сигнал высокого уровня на своем выходе при наличии на входе информативной составляющей.



а б

Рис. 4. Результат моделирования обнаружителя в среде Anadigm Designer 2 при наличии информативной составляющей на входе (а) и ее отсутствии (б)

Подводя итоги, следует отметить, что использование дискретно-аналоговых устройств в современных разработках для различных областей, включая и системы управления, является актуальным. Для построения и исследования моделей устройств подобного класса можно использовать хорошо разработанный аппарат передаточных функций в *z*-области. Интуитивно понятная среда программирования и возможность динамического переконфигурирования заметно облегчают, удешевляют и унифицируют процесс проектирования устройств на базе ПДАИС.

Список используемых источников

1. Полищук А. Программируемые аналоговые ИС Anadigm структура и принцип построения. М.: Современная электроника. 2005. № 1.

2. Гауси М., Лакер К. Активные фильтры с переключаемыми конденсаторами. М.: Радио и связь, 1986.

3. Щебра А.: Компоненты и технологии № 12. М.: Современная электроника, 2007.

Статья представлена заведующей кафедрой,
доктором технических наук, профессором Г. В. Верховой.

УДК 519.688
ГРНТИ 20.15.05

К ВОПРОСУ О РАЗРАБОТКЕ ЕДИНОГО АДАПТИВНОГО ОБРАЗОВАТЕЛЬНОГО ON-LINE ПРОСТРАНСТВА

В. В. Антонов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются вопросы разработки программной информационной системы, реализующей дистанционное образование на основе «единого образовательного пространства» и «сценариев обучения». Система адаптирует процесс обучения под уровень знаний конкретного обучающегося.

образовательное пространство, сценарии обучения, адаптивное обучение.

Дистанционной обучение всё больше набирает популярность. Однако качество такого обучения оставляет желать лучшего. В существующих дистанционных курсах не решаются следующие вопросы:

- Нет вариативности сложности курса в зависимости от уровня подготовки студента. Все студенты получают одинаковые задания не зависимо от уровня начальной подготовки
- Нет возможности (или слабая возможность) изменения содержимого курса. Большинство учебных курсов статические сделанные с использование HTML, что делает их поддержку весьма сложным. И требует от преподавателя глубоких знаний HTML, JavaScript, CSS.
- Нет полной единой информационной среды, необходимо периодическое переключение на внешние программы в которых выполняется кодирование, компиляция и запуск программ.
- Оценка знаний осуществляется при помощи тестов, ответы на вопросы которых можно легко списать.

Улучшение качества дистанционного обучения возможно при изменении методики, средств и формы представления знаний. Единое образовательное пространство будет предусматривать возможность выполнять практические и лабораторные работы в web-браузере, в том числе кодирование, компилирование и исправление ошибок. Это позволит студентам осваивать курс с любого устройства на котором не имеется возможность установки специальной среды разработки.

Применение сценариев обучения позволит реализовать вариативность обучения в зависимости от уровня начальной подготовки студентов и отказаться от традиционной системы тестирования для оценки уровня усвоения студентами материала курса.

Подобный инновационный подход позволит поднять уровень качества дистанционного обучения до уровня «персонального обучения».

В процессе реализации проекта необходимо выполнить следующие работы:

- разработка архитектуры системы;
- разработка базы данных системы;
- разработка языка сценариев;
- программная реализация сервера системы;
- создание дистанционного курса.

Сценарии обучения (сценарии в виде xml) обеспечат вариативность курса в зависимости и от психотипа обучающегося и уровня усвоения материала. Вариативность в обучении предполагает зависимость выдаваемых обучающемуся задач в зависимости от результатов выполнения предыдущих. Изучение каждого отдельного учебного модуля проходит по сценарию, который разработан тьютером и внесён в систему.

Легкое наращивание сценариев и их изменение. Через соответствующий инструмент тьютер сможет изменять сценарии обучения. Формат сценариев реализован на основе языка XML, что позволяет легко изменять сценарии в простом текстовом редакторе.

Использование одной оболочки для обучения (все задания выполняются в браузере, тексты программ компилируются и отлаживаются на сервер и ошибки выдаются обратно) позволяет повысить эффективность учебного процесса.

Уровень усвоения знаний оценивается не отдельными тестами (ответы на которые можно списать), а непосредственно выполненными заданиями.

Аналитическая система, разработанная для тьютера, позволит выполнять анализ усвоения учебного курса.

Разработанный язык сценариев позволит строить, на основе имеющейся системы, учебные курсы для других дисциплин. Единственное ограничение – это изучение дисциплины должно вестись на основе языка Java. Например, дисциплины: «Технология разработки программных продуктов», «Интернет технологии», «Разработка программных продуктов для мобильных устройств», «Разработка корпоративных информационных систем» и других.

Основой системы является сервер системы, реализующий акторную модель [1], и база данных (БД) системы. Сервер реализует весь бизнес функционал системы. Хранение результатов обучения осуществляется на сервере БД.

Диаграмма последовательностей (рис.) определяет полный жизненный цикл системы. Пользователь открывает web-браузер на странице входа в систему и вводит логин и пароль. Модуль авторизации системы запрашивает информацию о пользователе. В случае положительного ответа сервер создаёт объект «сессия». Всё дальнейшее взаимодействие осуществляется в рамках этого объекта.

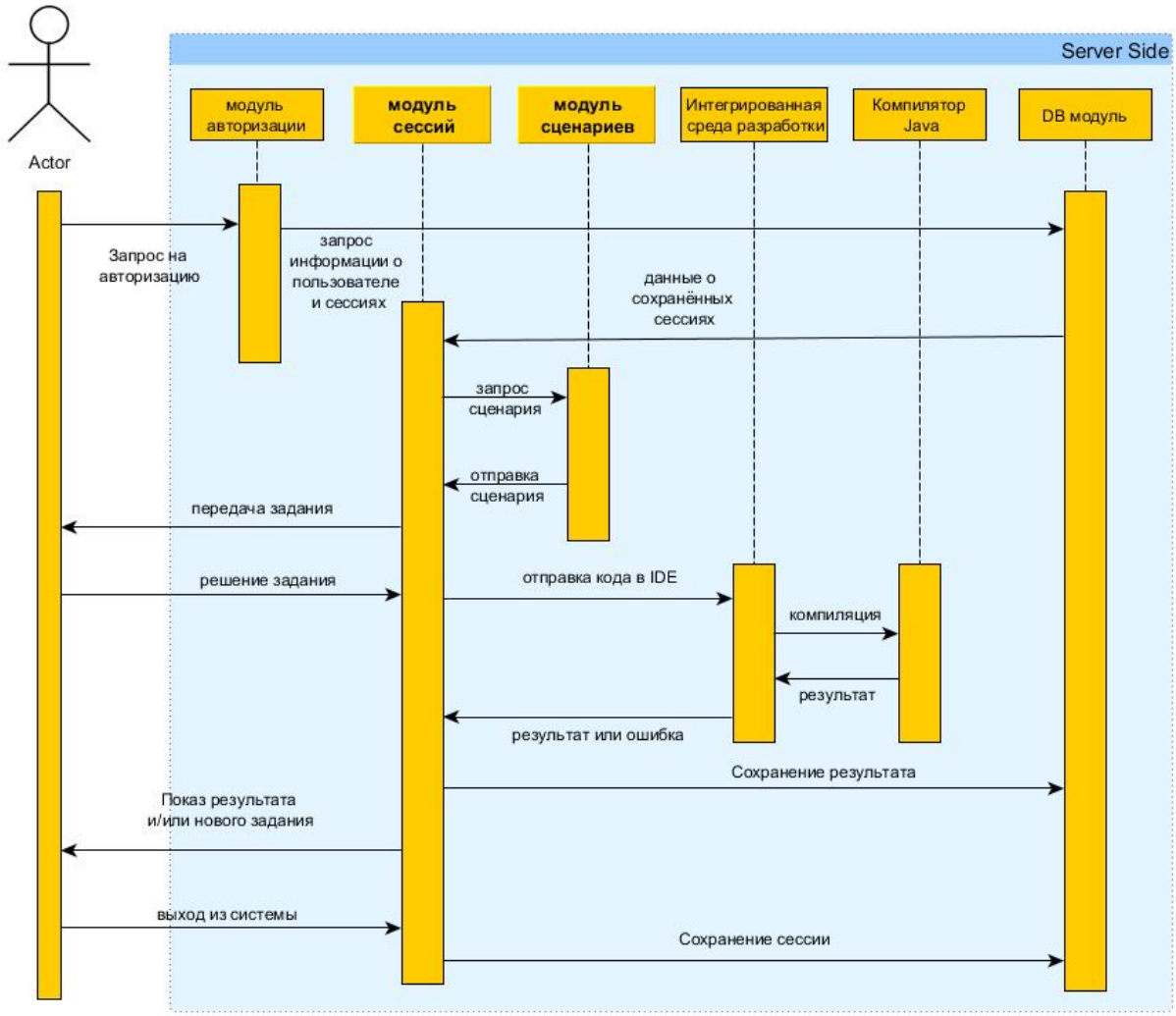


Рисунок. Диаграмма последовательностей работы системы

Этот объект получает из БД информацию о предыдущей сессии и загружает из модуля сценариев нужный сценарий. Объект «сессия» определяет точку остановки предыдущего сценария. Генерирует задание и отправляет его обучающемуся.

Получив задание, обучающийся в окне web-браузера пишет код для решения задания и отправляет его на сервер. Получив результат, объект «сессия» отправляет его внешней интегрированной среде разработки. Среда разработки компилирует код при помощи компилятора и возвращает результат объекту «сессия», который отправляет информацию обучающемуся.

В зависимости от результата объект «сессия» определяет дальнейшие действия системы в зависимости от сценария. Если ошибок нет и задание выполнено, система выдаёт следующее задание, иначе выполняются действия сценария, предусмотренные для неправильного решения. То есть система адаптируется на основании предыдущего результата.

В качестве варианта действий при неправильном ответе, обучающемуся может быть выдан дополнительный справочный материал и задание для его практического закрепления. Глубина вложенности альтернативных сценариев может быть произвольной и расширятся на основе анализа, полученного тьютером в результате прохождения обучения учащимися.

Когда пользователь закончил работу с системой, объект «сессия» сохраняет данные о сессии в базе данных и освобождает память.

Список используемых источников

1. Антонов В. В. О применении акторной модели примитивов в программных реализациях алгоритмов распознавания образовании // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 3. С. 39–43.

Статья представлена заведующей кафедрой,
доктором технических наук, профессором Л. К. Птицыной.

УДК 004.4'2
ГРНТИ 81.14.11

ЭФФЕКТИВНЫЕ ПРОГРАММНЫЕ ИНСТРУМЕНТЫ ДЛЯ 3D МОДЕЛИРОВАНИЯ

Ф. К. Ачилова, Ф. Э. Кодиров

Каршинский филиал Ташкентского университета информационных технологий
имени Мухаммада аль-Хорезми

3D технологии являются передовыми технологиями, заполняющими современную жизнь человека. В основе 3D технологий лежит 3D моделирования. На сегодняшний день трудно представить работу дизайнера, проектировщика, мультипликатора без

использования 3D моделей, построенных с помощью компьютера. Еще более широкому распространению 3D моделирование получило в связи распространением 3D принтеров. Сейчас 3D модели используются во всех отраслях науки, техники, медицины, архитектура и дизайн.

3d моделирования, трехмерная графика, 3D-моделей, Unity 3D.

Сегодня технологии программирования также быстро развиваются, и программисты используют разные языки программирования. Различные языки программирования используются в соответствии с областью разрабатываемой программы. Это, в свою очередь, привело к разработке многих языков программирования и разработке их программного обеспечения. Есть также много видов программирования. Разработка графических программ на языках программирования – сложный процесс. Вот почему было создано отдельное программное обеспечение для производства графического программного обеспечения.

Само графическое программное обеспечение выглядит по-другому, так как существуют разные направления компьютерной графики. Их можно разделить на двух- и трехмерные графические направления в целом. Двумерная графика далека от реальности, и сегодня используется трехмерная графика. Трехмерная графика должна начинаться с трехмерного моделирования. Концепция трехмерного моделирования подразумевает создание трехмерных моделей объектов на компьютере. Трехмерное моделирование, вкратце трехмерное моделирование, может использоваться в языках программирования или в программном обеспечении. Более эффективно разрабатывать 3D-моделирование с использованием готового программного обеспечения. Это создает объекты быстрее и проще. Примером программного обеспечения Autodesk 3ds MAX и Maya является наиболее распространенное программное обеспечение для 3D-моделирования. Возможности этого программного обеспечения обширны, и их можно использовать для создания 3D-моделей.

При работе с трехмерной графикой необходимо сосредоточиться на форме фигур. В этом случае обычная 2D-плоскость соответствует трехмерной графике. В 3D рабочее пространство должно быть выражено таким образом, чтобы не только геометрическая форма моделируемой трехмерной модели, но также ее геометрическое местоположение и местоположение. Трехмерная графика использует Декарт, Цилиндрические и Сферические системы координат. Все трехмерные объекты можно разделить на геометрические и негеометрические объекты. Геометрические объекты в основном используются для построения сценических организаторов: персонажи, объекты и другие объекты – объекты существования. Неогеометрические объекты предназначены для того, чтобы дать сцене ощущение жизни (прямое

освещение), моделирования сил, которые воздействуют на объекты (например, гравитация или ветер) и так далее. Другими словами, отображаемый фрейм точно такой же, как геометрические объекты (линии и подложки), а негеометрические объекты отображаются как промежуточные (оттенки, ускорение и т. д.). Когда 3D-моделирование выполнено, необходимо связать его с программой и использовать программные языки для разработки программ. Языки программирования C / C ++, Java, Python, JavaScript, C #. Для программирования готовых 3D-моделей переводчикам необходим программный код. Это требует много программных кодов. Для оптимизации этих работ был разработан ряд графических программ. Unity 3D, разработанный в 2005 году, является одним из них. «Unity 3D» является одним из самых полезных программ для производства 3D программных продуктов и игр. Unity также может загружать готовые 3D-модели и комбинировать их с написанием сценариев на C # или Javascript. C Unity 3D работать намного проще: автоматическое копирование необходимых материалов в один каталог, отдельные сценарии после записи в объекты, легкий доступ к программному обеспечению и, самое главное, можно скомпилировать.

Постоянное совершенствование компьютерного оборудования и программного обеспечения сделало 3D-технологии доступными. Сегодня 3D-модели повсеместно используют вместо обычных макетов в проектировании для проработки крупных или миниатюрных деталей, а «объемная» визуализация становится одним из инструментов маркетинговых мероприятий, интерактивных тренингов, презентаций. Трехмерные модели реально существующих или абстрактных объектов создаются с помощью специализированных компьютерных программ. 3D-моделирование может быть следующих видов: Создание фотореалистичных изображений, проецируемых на обычный компьютерный монитор или экран. Отдельные программы позволяют осуществлять печать созданной модели на 3D-принтере. Создание стереоизображений для просмотра на обычном компьютерном мониторе (экране) через специальные поляризационные очки или на специализированном 3D-мониторе со стереоскопическим эффектом. Создание компьютерных голограмм. Для достижения наиболее реалистичного эффекта трехмерную модель объекта можно текстурировать (придать визуальные свойства материала), задать освещение, анимировать.

В Unity вы можете просто настроить программу и собрать ее для разных платформ. На рис. 1 показан общий вид рабочего окна Unity. Чтобы создать программное обеспечение, мы должны загрузить разработанные 3D-модели в «Unity» и поместить его в свободное пространство (рис. 2). В нашей программе вы хотите создать самодельный, нет возможности путешествовать. Так что название программы называется «3D Travel». Чтобы совершить путешествие, мы создадим движущийся объект и напишем код на

C #. После того, как программное обеспечение было обработано, оно может быть скомпилировано для следующих платформ:

- для компьютеров с Linux, Windows, Mac;
- для телефонов iOS, Android и BlackBerry;
- для Магазина Windows и Windows Phone;
- на вкладке WebGL;
- Tizen для Xbox;
- для PlayStation 3 и 4;
- для телевизоров Samsung.

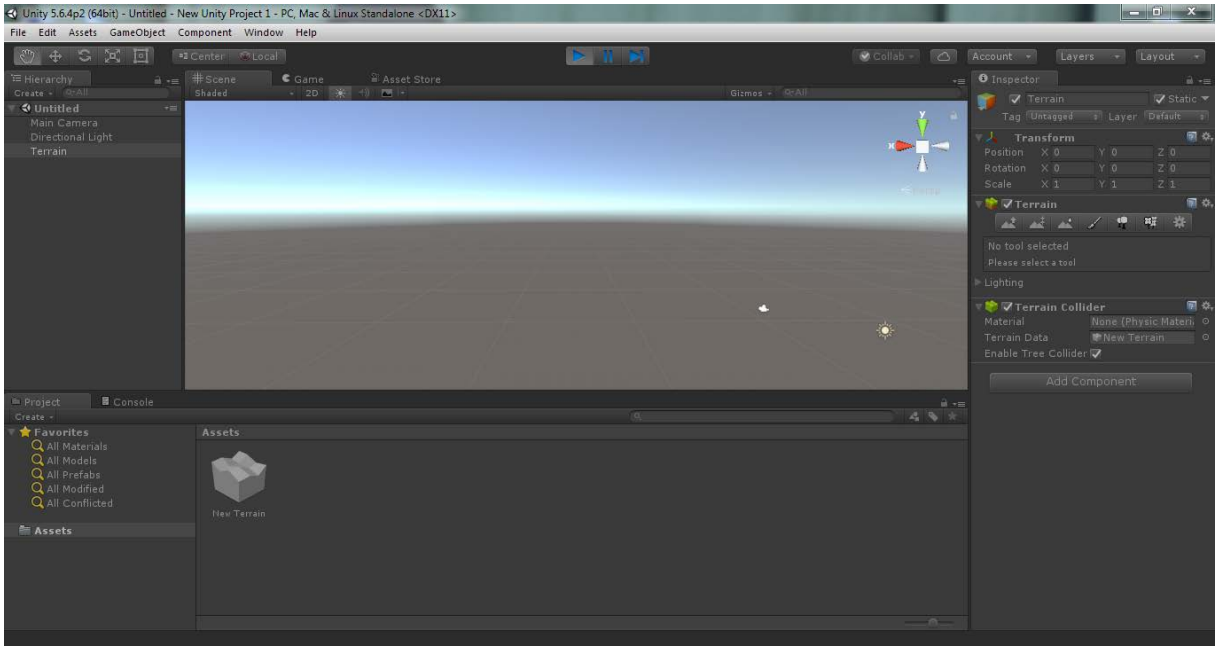


Рис. 1. Вид рабочего окна Unity

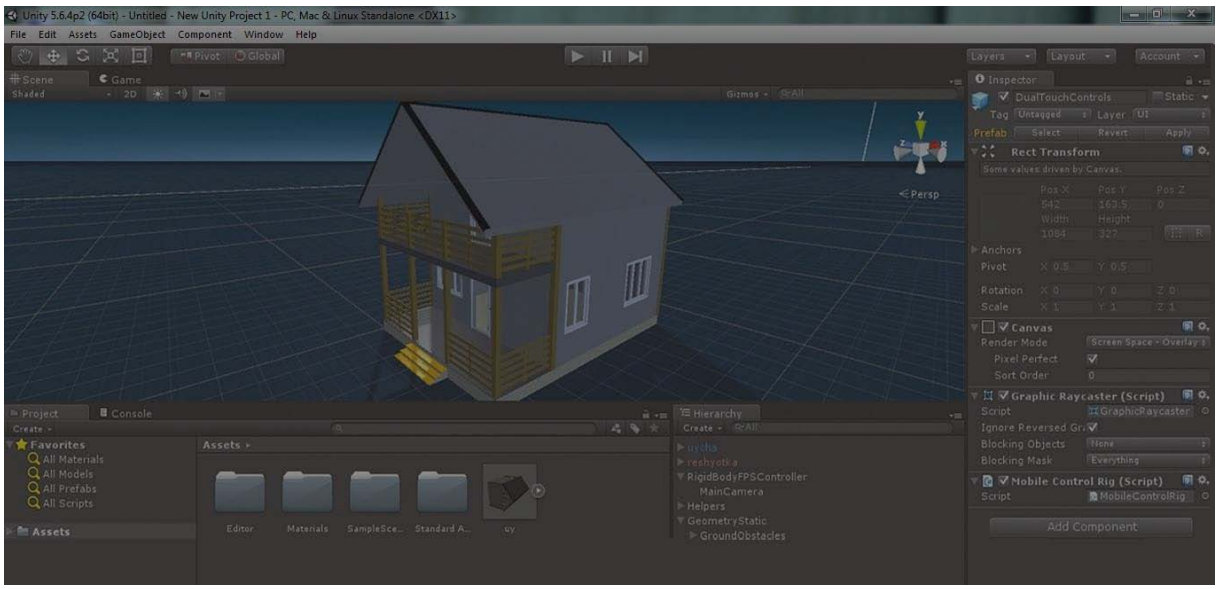


Рис. 2. Расположение 3D дома в Unity

Одним из лучших аспектов Unity является возможность компилировать множество платформ и устройств одновременно. Мы компилируем вышеупомянутое программное обеспечение для платформы, которую мы хотим.

Таким образом, в большинстве случаев сейчас используются различные инструменты, особенно компьютерные и мобильные телефоны. Естественно, спрос на программное обеспечение также растет. Unity выпускает 1, 2, 3, 4, 5 версий с 2005 года. Ожидается, что потенциал Unity, одного из наиболее эффективных программных инструментов для разработки 3D-программного обеспечения для различных устройств и платформ, в будущем будет еще более расширен.

Список используемых источников

1. Петерсон М. 3D Studio MAX искусство трехмерной анимации Platinum Edition Эффективная работа с 3D Studio Max. СПб.: Питер Ком, 1999.

2. 3D Studio VIZ для дизайнера / Хаббелл Д., Бордмэн Т.: ДиаСофт, 2004. 663 с.

3. 3DS MAX 8 для «чайников». Пер. с анг. М.: Издательский дом «Вильямс», 2006. 368 с., ил. Парал. тит. англ.

4. Актуальное моделирование, визуализация и анимация. СПб.: БХВ-Петербург, 2005. 456 с., ил.

Статья представлена научным руководителем, доктором технических наук, профессором И. И. Карцевым.

УДК 519.23
ГРНТИ 27.43.17

ТОЛЕРАНТНЫЙ ИНТЕРВАЛ ДЛЯ РЕГРЕССИИ С ГЕТЕРОСКЕДАСТИЧНЫМИ ОСТАТКАМИ И НАЛИЧИЕМ ЦЕНЗУРИРОВАННЫХ НАБЛЮДЕНИЙ

Е. Г. Баязитов, Е. Т. Сыса

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В работе рассматривается методика точечного и интервального оценивания параметров распределений на примере выборок, полученных при механических испытаниях образцов на усталость. Для выборок, полученных в ходе таких испытаний, характерны следующие особенности: гетероскедастичность остатков регрессионной модели и наличие цензурированных наблюдений. Учет обозначенных особенностей механических

испытаний значительно улучшает точность определения характеристик долговечности. Характеристикой долговечности служит для обоснования оценки гарантированного ресурса, нормируемого по нижней доверительной границе квантиля долговечности.

испытания на усталость, долговечность, толерантная граница, дифференциальная эволюция, метод максимального правдоподобия, цензурированная выборка, гетероскедастичность.

Гетероскедастичность остатков регрессионной модели усталости (1) связана со значительным рассеянием физико-механических свойств материалов образцов, которое является объективным следствием структурной неоднородности и влиянием большого числа конструктивных, технологических и эксплуатационных факторов. Проблемы, связанные с изучением рассеяния усталостной долговечности материалов рассматривались в работах [1, 2, 3].

Другой особенностью циклических испытаний материалов и элементов конструкций являются незавершенные выборочные совокупности, следствием которых является неполнота результатов испытаний. Такие выборки называются цензурированными, и их появление в механических испытаниях весьма определено. При усталостных испытаниях могут образовываться цензурированные справа выборки I и II типа [4, 5, 6]. Основной причиной появления образцов недоведенных до критического состояния – разрушения является: дефицит времени в производственных условиях и установление контрольных временных границ на время испытания образца. Это, прежде всего, относится к зонам больших долговечностей (низким уровням амплитуды переменных напряжений). Так же многократно цензурированные выборки образуются в результате определения наработки ответственных элементов конструкции, достигших или не достигших критического состояния к моменту технического осмотра [1, 2].

Применительно к сплавам на железной основе хорошее соответствие экспериментальным данным при симметричном цикле нагружения в широком диапазоне долговечности имеет следующее уравнение [7]:

$$\lg(\sigma_{max} - \sigma_{-1}) = c - \alpha \lg(N), \qquad (1)$$

где σ_{-1} – предел неограниченной выносливости;

N – долговечность;

c, B, α – параметры.

На рис. 1 представлены результаты усталостных испытаний образцов материалов, включающих наблюдения, снятые с испытания по достижению базового числа циклов (цензурированные справа выборки II типа). Резуль-

таты представлены в полулогарифмических координатах, где по оси абсцисс отложены максимальные напряжения σ_{max}, а по ос и ординат десятичный логарифм циклической долговечности N.

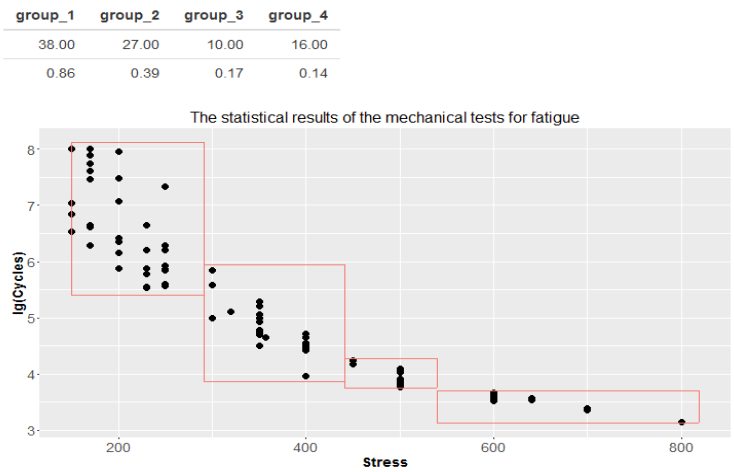


Рис. 1. Результаты усталостных испытаний образцов материалов

В настоящей работе первичная проверка на гетераскедастичность осуществляется графически, путем построения зависимости выборочной дисперсии (S_i^2) величины Y = lg(N) от уровня амплитуды цикла напряжения. Для построения зависимости выборочной дисперсии случайной величины y = lg(N) от уровней неслучайной величины x = σ_{max} целесообразно разбить результаты испытаний на k групп, в связи с малым числом наблюдений для некоторых баз испытания, где, в частности, для некоторых значений испытан лишь один экземпляр. Порядок разбиения может задаваться экспертно, так же исходя из логических соображений, деление рекомендуется проводить с учетом образования «естественных» групп, графически при изменении условной дисперсии или остатков некоторой функциональной зависимости, близости наблюдаемого напряжения к нормативным базам испытания, в зависимости от типа испытания или других факторов. Однако любой выбор выделения групп носит субъективный характер, что впоследствии влияет на дальнейший анализ. На рис. 1 представлен вариант возможного разбиения, учитывающий описанные выше предпосылки для деления. Красным цветом выделены границы, разграничивающие выбранные совокупности наблюдений. Над графиком в виде таблицы выведены размер групп и выборочная дисперсия в первой и второй строке соответственно.

На рис. 2 представлена зависимость выборочной дисперсии от выборочного среднего для внутренних групп (2,3), максимального, минимального значения уровня амплитуды цикла напряжения для 1 и 4 группы соответственно. Пунктирная линия служит кусочно-линейной аппроксимацией выборочных значений. Результат полученного представления свидетель-

ствует о том, что характеристики рассеяния усталостных свойств существенно зависят от долговечности. Для полной кривой усталости, имеющей участки малоцикловой и многоцикловой усталости, эта зависимость имеет монотонный характер, при достаточно больших долговечностях (низких уровнях амплитуды переменных напряжений) рассеяние стабильно возрастает.

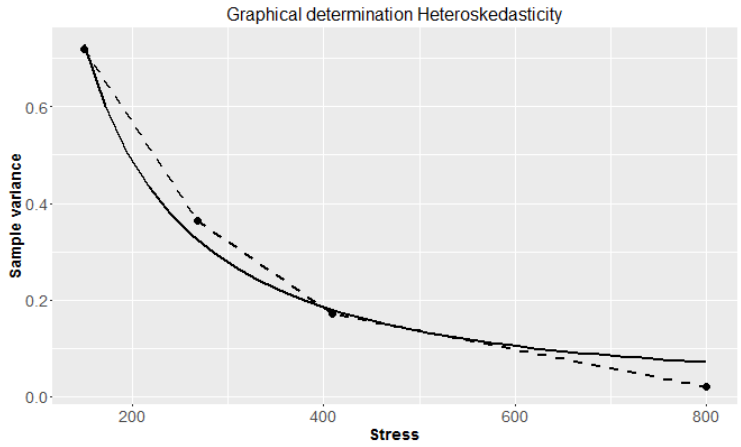


Рис. 2. Зависимость выборочной дисперсии от выборочного среднего

В настоящее время существует разнообразие подходов к анализу результатов механических испытаний и оценке параметров распределений и статистических зависимостей. К числу наиболее распространенных методов относятся метод максимального правдоподобия (ММП) и метод наименьших квадратов (МНК) [6, 8].

В соответствии с методом максимального правдоподобия (ММП) [9, 10] оценки параметров непрерывной не менее двух раз дифференцируемой функции распределения случайной величины в общем случае прогрессивно цензурированной выборки определяются решением системы уравнений максимального правдоподобия. Оценки максимального правдоподобия (ММП-оценки) определяются в точках экстремума функции (2):

$$L = \prod_{i=1}^{k} f_x(x_i) \cdot \prod_{j=1}^{m} [1 - F_x(x_{бi})]^{r_j}, \quad (2)$$

где k – число наблюдений (число объектов достигших критического состояния), m – число баз испытания, пи достижении которых наблюдаются объекты, не достигшие критического состояния, r_j – количество объектов, снятых с испытания на данной базе, $n = k + \sum_{j=1}^{m} r_j$ – общее число испытанных объектов, $x_{бj}$ – значения баз испытания, при которых наблюдаются не достигшие критического состояния объекты.

Для нахождения максимума функции правдоподобия необходимо приравнять частные производные к нулю, получая, тем самым, систему нелинейных уравнений максимального правдоподобия. Как правило, в условиях цензурирования, эта система имеет несколько локальных экстремумов, поэтому любой стандартный метод численного решения систем нелинейных уравнений не сможет дать однозначного результата, так как решение будет в значительной степени зависеть от начального приближения. В этих условиях, в настоящей работе рекомендуемым методом решения оценки параметров функции правдоподобия, служит алгоритм дифференциальной эволюции.

Метод дифференциальной эволюции был разработан Рэйнером Сторном и Кеннетом Прайсом, впервые опубликован ими в 1995 году в работе [11] и развит в дальнейшем в их более поздних работах [12, 13].

На рис. 3 представлены уравнения кривой усталости с учетом гетероскедастичности и наличия цензурированных наблюдений и не учитывающей данные обстоятельства (сплошной и пунктирной линией соответственно). Оценка параметров, доставляющих максимум логарифмической функции правдоподобия (2) уравнения кривой усталости Вейбула (1) произведена алгоритмом дифференциальной эволюции.

Рис. 3. Уравнения кривой усталости
с учетом гетероскедастичности и наличия цензурированных наблюдений

Верхние $\hat{\boldsymbol{y}}_{\mathbf{pu}}$ и нижние $\hat{\boldsymbol{y}}_{\mathbf{pl}}$ доверительные границы [14] для квантиля случайной величины y в двухпараметрической линейной модели определяются из следующих уравнений:

$$\hat{y}_{\mathrm{pu}} = \hat{y}(x_0) + t_{\beta}[\Delta, f] \cdot \delta\{\hat{y}\},$$

$$\hat{y}_{\mathrm{pl}} = \hat{y}(x_0) + t_{1-\beta}[\Delta, f] \cdot \delta\{\hat{y}\},$$

где $t_\beta[\Delta, f]$ – квантиль уровня β нецентрального распределения Стьюдента с параметром нецентральности:

$$\Delta = z_p \cdot \frac{\hat{\sigma}_y(x_0)}{\delta\{\hat{y}\}}.$$

На рис. 4 красной пунктирной линией представлены доверительные границы для квантиля уровня P = 0.01, с доверительной вероятностью 1-α = 0.95 для уравнения кривой усталости Вейбула (1) с учетом цензурированных наблюдений в линейной постановке (3).

$$x = \lg(\sigma_{max} - \sigma_{-1}),\ y = \lg N,\ \ b_1 = b_2 \cdot \bar{x} - b_2 \cdot \lg(a),\ \ b_2 = -\frac{1}{\alpha}. \qquad (3)$$

Учету изменения условной дисперсии служит степенная зависимость, графически представленная на рис. 2.

Рис. 4. Уравнения кривой усталости
с учетом гетероскедастичности и наличия цензурированных наблюдений

Построенные доверительные границы для квантильных кривых усталости учитывающих гетероскедастичность остатков и наличие цензурированных наблюдений, решают задачу обоснования гарантированного ресурса для образцов материала, которые лягут в основу изготовления конструкций и элементов машин.

Список используемых источников

1. Райхер В. Л. Рассеяние усталостной долговечности, М.: МАТИ, Изд. ЛАТМЭС, 2003.
2. Воробьев А. З. и др. Сопротивление усталости элементов конструкций. М.: Машиностроение, 1990.
3. Райхер В. Л. Усталостная повреждаемость. М.: МАТИ, 2006.
4. Cohen, A. C. Progressively Censored Sampling in the Three Parametr Log-Normal Distribution // Technometrics. 1976. Vol. 18. No. 1.

5. Cohen A. C. Multi-Censored Sampling in the Three Parametr Weibull Distribution // Technometrics. 1975. Vol. 17. No. 3.

6. Кендалл Дж., Стьюарт А. Теория распределений. М.: Наука,1966.

7. Степнев М. Н. Статистические методы обработки результатов механических испытаний. Справочник. М.: Машиностроение, 1985.

8. Кендалл Дж., Стьюарт А. Статистические выводы и связи, М.: Наука, 1973.

9. Bartlett, M. S. Properties of Sufficiency and Statistical Test // Proc. Roy. Soc. A. 1937. V. 160, 268 p.

10. Davidson, R., and MacKinnon, J. G. Estimation and Inference in Econometrics, Oxford University Press, New York, NY, USA, 1993.

11. Storn, Rainer and Price, Kenneth. Differential Evolution — A Simple and Efficient Adaptive Scheme for Global Optimization over Continuous Spaces, Technical Report TR-95-012, ICSI, March 1995.

12. Storn, Rainer and Price, Kenneth. Differential Evolution — A Simple and Efficient Heuristic for Global Optimization over Continuous Spaces. 1997.

13. Price, K., Storn, R., Lampinen, J. Differential Evolution: A Practical Approach to Global Optimization. Springer, 2005.

14. Агамиров Л. В., Сухова И. П. О закономерностях рассеяния долговечности в связи с формой кривой усталости. М.: Интермет инжиринг, 2004.

УДК 004.627
ГРНТИ 20.53.17

ИССЛЕДОВАНИЕ МЕТОДОВ СЖАТИЯ ИЗОБРАЖЕНИЙ

Е. Г. Баязитов, В. И. Дмитриев, Г. А. Портнов, П. А. Тимошенко

Военная академия связи им. Маршала Советского Союза С. М. Будённого

Цифровое изображение – это двумерное изображение, представленное в цифровом виде. В зависимости от способа описания, изображение может быть растровым или векторным. Изображения являются очень важными документами на сегодняшний день, для работы с ними в различных приложениях требуется сжатие изображения. Сжатие больше или меньше это зависит от цели применения. Сжатие изображений играет очень важную роль в передача и хранение данных изображения в результате ограничений и хранения. Основной целью сжатия изображения должно являться представление его в наименьшем количестве битов без потери важной информации содержимого исходного изображения.

сжатие изображения, DCT, DWT, OCR, кодирование длин серий.

Сжатие изображений – это применение алгоритмов сжатия данных к цифровым изображениям. Сжатие изображения с помощью, которого мы можем уменьшить объем данных, необходимых для представления цифрового изображения. Он также используется для уменьшая избыточности, во избежание дублирования данных, что будет полезно для увеличения объема хранения и производительности процесса передачи. При сжатии изображений мы не только концентрируемся на уменьшении размера, но также сосредотачиваемся на этом, не теряя качества и информации об изображении.

Многим приложениям требуется большое количество изображений, которые могут быть сохранены на диске для решения всякого рода проблем. Это хранение пространств изображения важно, поскольку меньшее пространство памяти означает меньшее время, требуемое для обработки изображения. Следовательно, требуется сжатие изображения, которое уменьшает объем данных, необходимых для представления цифрового изображения. Образ сжатия – это процесс кодирования изображения для уменьшения количества байтов, необходимых для хранения или передачи образа.

Система сжатия изображений требует двух компонентов:

a) Система кодирования, которая преобразует исходное изображение в сжатое изображение

b) Система декодирования, которая преобразует сжатое изображение в цифровое изображение, которое более идентично оригиналу. Сжатие изображения состоит из трех основных этапов: transform, quantizer и coder, как показано на рис. ниже.

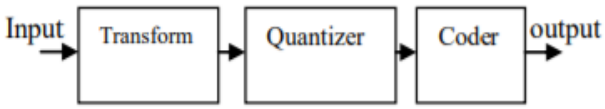


Рисунок. Три этапа цифровой компрессии изображения

Сжатие изображений состоит из двух методов преобразования, которые основаны на частоте. Сначала это дискретное косинусное преобразование (DCT), а второе – дискретное преобразование вейвлета (DWT). Оба метода имеют свои «плюсы и минусы». DWT обеспечивает лучшую степень сжатия без потери большей информации изображения, но ему нужно больше вычислительной мощности. В то время как DCT работает быстро, его можно быстро вычислить, но он имеет блоки артефактов потери некоторой информации. Он содержит обзор различных методов сжатия изображений.

Сжатие изображения

Сжатие изображения решает проблему уменьшения объема информации, необходимой для представления цифрового образ. Это процесс, предназначенный для получения компактного представления изображения, тем самым уменьшая изображение требования к передаче данных. На каждом изображении будут избыточные данные. Избыточность означает дублирование данных на изображении. Либо это может быть повторение пикселя по изображению или рисунку, что повторяется более часто на изображении. Сжатие изображения происходит, используя избыточную информацию в образ. Сокращение избыточности обеспечивает экономию места хранения изображения. Сжатие изображения достигается при уменьшении, устранении одного или нескольких из этих избыточности. В сжатие изображении, можно выделить и использовать три основных избытка данных.

Интер-пиксельная избыточность

Удаление одного или нескольких из трех основных избытков данных. Интер-пиксельная избыточность в изображении соседние пиксели не являются статистически независимыми. Это обусловлено корреляцией между соседних пикселей изображения. Этот тип избыточности называется меж пиксельной избыточностью. Этот тип избыточность иногда называется пространственной избыточностью. Эта избыточность может быть исследована несколькими способами, одна из которых является прогнозирование значения пикселя на основе значений его соседних пикселей. Для этого исходный 2-мерный массив пикселей обычно отображается в другой формат, например, массив различий между смежными пикселями. Если исходные пиксели изображения могут быть восстановлены из преобразованного набора данных, то отображение говорит, что они обратимы.

Кодирование избыточности

Состоит в использовании кодовых слов переменной длины, выбранных в соответствии со статистикой исходного источника, в этом случае, самого изображения или обработанной версии его значений пикселей. Этот тип кодирования всегда обратим и обычно реализованы с использованием справочных таблиц (LUT). Примеры схем кодирования изображений, которые изучают избыточность кодирования – это коды Хаффмана и метод арифметического кодирования.

Психо-визуальная избыточность

Многие эксперименты по психофизическим аспектам человеческого зрения доказали, что человеческий глаз не реагирует с одинаковой чувствительностью ко всей поступающей визуальной информации; некоторые части информации более важны, чем другие. Большинство используемых алгоритмов кодирования изображений используют этот тип избыточности, например, алгоритм дискретного косинусного преобразования (DCT), лежащий в основе стандарта кодирования JPEG.

2. Методы сжатия изображений

На основе наших требований методы сжатия изображений следуют двум основным категориям.

1. Сжатие изображения без потерь
2. Сжатие изображения с потерей

2.1 Методы сжатия без потерь

Сжатие без потерь сжимает изображение, кодируя всю информацию из исходного файла, поэтому, когда изображение распаковывается, оно будет точно идентично исходному изображению. Примеры изображений без потерь сжатие PNG и GIF. Когда использовать определенный формат сжатия изображений, действительно зависит от того, что сжимается.

а) Кодирование длины выполнения

Кодировка длины пробега (RLE) – очень простая форма сжатия изображения, в которой записи данных сохраняются как одно значение данных и количество, а не как исходный запуск. Он используется для последовательных данных, и это полезно для повторяющихся данных. В этом методе заменены последовательности одинакового символа (пикселя), называемые бегами. Длина выполнения кода для полутонового изображения представлена последовательностью {Vi , Ri}, где Vi – интенсивность пикселя, а Ri – к числу последовательных пикселей с интенсивностью Vi. Это наиболее полезно для данных, которые содержит много таких прогонов, например, простые графические изображения, такие как значки, чертежи линий и анимации. Это не полезно для файлов, которые не имеют большого количества прогонов, так как это может значительно увеличить размер файла. Кодировка длины выполняет сжатие без потерь. Кодирование длины пробега используется в факсимильных аппаратах.

б) Энтропийное кодирование

В теории информации энтропийное кодирование представляет собой схему сжатия данных без потерь, которая не зависит от специфических характеристик среды. Один из основных типов энтропийного кодирования создает и присваивает уникальный без префикса символ, который встречается во входе. Эти энтропийные кодеры затем сжимают путем замены каждого входного символа фиксированной длины на соответствующим префиксом переменной свободной длины кодового слова.

c) Кодировка Хаффмана

В информатике и теории информации кодирование Хаффмана является алгоритмом энтропийного кодирования, используемым для сжатия данных без потерь. Он был разработан Хаффманом. Сегодня кодирование Хаффмана часто используется как «back-end». Термин относится к использованию таблицы кодов переменной длины для кодирования источника символов, где таблица кодов переменной длины была получена определенным образом на основе вероятности появления для каждого возможного значения символом источника. Пиксели изображения обрабатываются как символы. Символам, которые встречаются чаще, назначается меньшее количество бит, тогда как символы, которые встречаются реже, присваивается относительно большее количество бит. Код Хаффмана – это префиксный код. Это означает, что (двоичный) код любого символа не является префиксом кода любого другого символа.

d) Арифметическое кодирование

Арифметическое кодирование представляет собой форму энтропийного кодирования, используемого при сжатии данных без потерь. Обычно строка символов, такие как слова «привет», представлены с использованием фиксированного количества бит на символ, как в ASCII-код. Когда строка преобразуется в арифметическую кодировку, часто используемые символы будут сохраняться в маленькие биты и не очень часто встречающиеся символы будут сохранены с большим количеством бит, что приведет к меньшему количеству бит, используемых в общем. Арифметическое кодирование отличается от других форм энтропийного кодирования, таких как кодирование Хаффмана, тем, что разделение ввода на символы компонентов и замена каждого кода, арифметического кодирования кодирует все сообщение в один номер.

2.2. Способы сжатия с потерей

Сжатие с потерей, как следует из названия, приводит к потере некоторой информации. Сжатое изображение похоже на оригинальное несжатое изображение, но не так, как предыдущее, как в процессе сжатия. Наиболее распространенным примером сжатия с потерями является JPEG. Алгоритм, который восстанавливает представление, так же как исходное изображение известно, как техника с потерями. Реконструкция изображения является приближением оригинального изображения, поэтому необходимо измерить качество изображения для техники сжатия с потерями. Метод сжатия с потерями обеспечивает более высокую степень сжатия, чем сжатие без потерь. Производительность схемы сжатия с потерями включают в себя:

- Степень сжатия.
- Отношение сигнал / шум.
- Скорость кодирования и декодирования.

Методы сжатия с потерями включают следующие схемы.

а) Скалярное квантование

Наиболее распространенный тип квантования известен как скалярное квантование. Скалярное квантование, обычно обозначаемое как Y = Q (x), является процессом использования функции квантования Q для отображения скалярного (одномерного) входного значения (x) на скалярное выходное значение Y. Скалярное квантование может быть таким же простым и интуитивным, как округление высокоточных чисел к ближайшему целому числу или к ближайшему краю некоторой другой единицы точности.

б) Векторное квантование

Векторное квантование (VQ) является классическим методом квантования обработки сигналов, что позволяет моделировать функции плотности вероятности путем распределения векторов прототипов. Первоначально он использовался для сжатия изображения. Он работает путем деления большого набора точек (векторов) на группы, имеющие приблизительно то же самое количество ближайших к ним точек. Свойство согласования плотности векторного квантования является мощным, особенно для определения плотности больших и высоко размерных данных. Поскольку точки данных представлены как индекс их ближайшего центроида, часто встречающиеся данные имеют низкую погрешность и высокую погрешность данных. Вот почему VQ подходит для сжатия данных с потерями. Он также может использоваться для коррекции и плотности данных с потерями оценки.

Сегодня изображения являются важными документами для работы с ними в разных приложениях, поэтому их необходимо сжимать. Сжатие более или менее зависит от нашей цели это играет очень важную роль в передаче и хранении данных изображения в результате ограничений хранения. Основная цель сжатие изображения представляет собой изображение в наименьшем количестве бит без потери существенной информации содержимое в исходном изображении. В этой статье представлены различные методы сжатия изображений. После изучения всех методов обнаруживаем, что методы сжатия изображений без потерь наиболее эффективны по сравнению с потерями. А с потерями обеспечивает более высокую степень сжатия, чем сжатие без потерь.

Список используемых источников

1. Гонсалес Рафаэль К., Вудс Ричард Э. Цифровая обработка изображений, 2-е изд. NJ: Prentice Hall, 1992.

2. Фирас А. Джассим и Хинд Э. Кассим Пять модульных методов сжатия изображений // SIPIJ. 2012. Vol. 3. No. 5. С. 19–28.

3. Sahami, S. и Shayesteh, M. G. Двухуровневая техника сжатия изображений с использованием нейронных сетей // IET Image Process. 2012. Vol. 6, Вып. 5. С. 496–506.

4. Shantagiri, Pralhadrao V. и Saravanan, K. N., Уменьшение размера пикселя, алгоритм сжатия изображений без потерь // IJCSIT. 2013. Том 5.

УДК 004.77
ГРНТИ 47.14

ПОРТАТИВНЫЙ ПРОИГРЫВАТЕЛЬ ПОТОКОВОГО РАДИО

К. В. Белоус, Е. В. Давыдова, Е. А. Пиликина, А. П. Шабанов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современные скорости подключения к глобальной телекоммуникационной сети Интернет позволяют прослушивать потоковые радиостанции с высоким качеством вещания. Аппаратные компоненты позволяют реализовать портативный проигрыватель потокового радио с использованием небольших денежных затрат.

потоковое радио, микроконтроллерная плата, программирование, Arduino.

В настоящее время в Интернет вещает большое количество сетевых радиостанций различных жанром и языков. Несмотря на то, что существуют

специализированные сервисы по прослушиванию, например, Яндекс.Музыка, Soundstream, LastFm и др., обладающие огромной базой данных музыкальных композиций, они не всегда могут удовлетворить желания пользователя по прослушиванию конкретных типов радиопрограмм. Кроме того, данные музыкальные сервисы требуют наличие или компьютера, или мобильного телефона или планшета, что в некоторых случаях может быть неудобно или невозможно.

Для того, чтобы добиться миниатюризации устройства, что, помимо всего прочего, приведёт к снижению энергопотребления, можно воспользоваться микроконтроллерной платой ESP-32, обладающего следующими характеристиками:

- процессор: Xtensa Dual-Core 32-bit LX6, 160 МГц или 240 МГц;
- ОЗУ: 448 КБ;
- ПЗУ: 520 КБ;
- Flash-память модуле: 1, 2, 4… 64 Мб;
- Беспроводные интерфейсы:
- Wi-Fi: 802.11b/g/n/e/i, до 150 Мбит/с HT40;
- Bluetooth: v4.2 BR/EDR и BLE.

Рис. 1. Внешний вид платы ESP-32

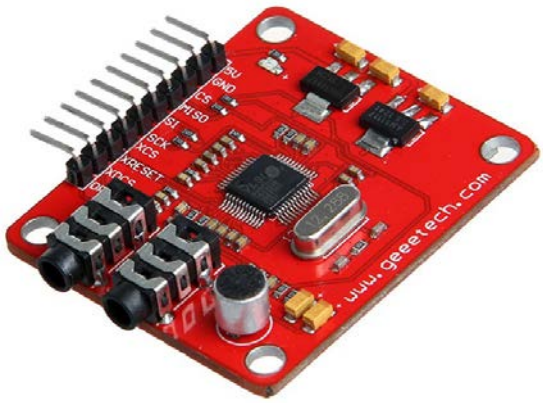


Рис. 2 Внешний вид платы VS1053

Периферийные интерфейсы:

- 12-bit SAR АЦП до 18 каналов;
- 2 × 8-бит ЦАП;
- 10 × сенсоров;
- Температурный сенсор;
- × SPI;
- 2 × I²S;
- 2 × I²C;
- 3 × UART;

Внешний вид платы ESP-32 представлен на рис. 1.

Для декодирования потокового аудио используется плата VS1053B (рис. 2). Модуль поддерживает несколько типов аудиофайлов – Ogg Vorbis, MP3, AAC, WMA, MIDI-. VS1053B включает технологию EarSpeaker, позволяющую создавать эффект пространственной обработки звука. Модуль поддерживает запись в Ogg Vobis.

На плате присутствует индикация питания напряжениями 2,8 и 3,3 В.

Для хранения звуковых файлов используется SD карта. Основные характеристика платы представлены ниже:

- Питание 5 В;
- Частота тактового генератора 12,288 МГц.

Поддержка форматов:

- Ogg Vorbis;
- MP3 MPEG 1 и 2 Audio слой III (CBR + VBR + ABR);
- MP1 и MP2 и MPEG 1 и 2 Audio Layers 1 и 2 опционально;
- MPEG4 / 2 AAC-LC (+PNS), HE-AAC v2 (Level 3) (SBR + PS);
- WMA4.0, 4.1, 7, 8, 9 All Profiles (5-384 Кбит/сек);
- FLAC без потерь аудио с плагином программного обеспечения (до 24 бит, 48 кГц);
- WAV (PCM + IMA ADPCM);
- General MIDI 1 / SP-MIDI формат 0.

Запись в форматах:

- Ogg Vorbis с плагином программного обеспечения;
- IMA ADPCM;
- 16-бит PCM.

Обобщённая структурная схема проигрывателя представлена на рис. 3. Схема соединений модулей системы представлена в таблице.

Рис. 3. Внешний вид платы ESP-32

ТАБЛИЦА. Схема соединения компонентов системы

VS1053	ESP32
VIN	+5 V
GND	GND
D19	MISO
XDCS	D33X
XRST	EN
SCK	D18
XCS	D32
DREQ	D35
MOSI	D23

Для загрузки прошивки используется среда программирования Arduino IDE. Настройка среды разработки сводится к добавлению ссылки для скачивания пакета плат https://raw.githubusercontent.com/espressif/arduino-esp32/gh-pages/package_esp32_index.json и выбору в менеджере плат платы ESP-32 (Dev Mode). После выполнения прошивки платы и её перезагрузки, подключение к сети и последующий запуск происходит в течение 10 сек.

Список используемых источников

1. Официальный сайт разработчика платы ESP-32 [Электронный ресурс]. URL: http://esp32.net (дата обращения 25.02.2018).

УДК 004.021
ГРНТИ 47.49.29

АЛГОРИТМ НЕЛИНЕЙНОЙ ФИЛЬТРАЦИИ, ОСНОВАННЫЙ НА БАЙЕСОВСКОМ ПОДХОДЕ К РЕШЕНИЮ ЗАДАЧИ ОЦЕНИВАНИЯ ДЛЯ СИСТЕМ С ДИСКРЕТНЫМ ВРЕМЕНЕМ

Д. А. Белоцветов, Н. С. Козин, Д. С. Лебедев, М. З. Лещук

Военная академия связи им. Маршала Советского Союза С. М. Будённого

На практике нелинейные алгоритмы оценивания применяются, но, в основном, ограничиваются простейшими вариантами, такими как расширенный фильтр Калмана. Более мощные алгоритмы существуют, но применяются редко, поскольку требуют больших вычислительных затрат.

Но постоянный темп развития и увеличения вычислительных мощностей современной аппаратуры, стимулирует к разработке более мощных и высокоточных алгоритмов.

Ниже рассмотрен один из вариантов алгоритмов нелинейной фильтрации, основанный на байесовском подходе к решению задачи оценивания для систем с дискретным временем. Главная идея алгоритма является представление апостериорной плотности распределения оцениваемого вектора состояния в виде ансамбля взвешенных точек, регулярно распределенных в некоторой области фазового пространства.

расширенный фильтр Калмана, нелинейная фильтрация, ансцентный фильтр, гауссовское распределение.

Введение

Определение с максимально возможной точностью координат и скоростей объектов по последовательности измерений, формируемых радиолокационной системой, является центральной задачей любой системы слежения за целями в военной или гражданской сфере. Для ее решения разработано значительное число алгоритмов, базирующихся на рекуррентном алгоритме фильтра Калмана.

Но при решении данной задачи возникают сложности. Одна из наиболее существенных является нелинейный характер моделей движения и измерений во многих практических задачах. Нелинейность появляется по многим причинам – в силу нелинейной связи систем координат, используемых в уравнениях объекта наблюдения и измерителя, из-за нелинейного характера самих уравнений. Нелинейные задачи возникают при построении адаптивных систем, реализуемых путем включения неопределенных параметров в оцениваемый вектор состояния [1]. Во многих случаях упрощение и игнорирование нелинейностей существенно снижает эффективность алгоритмов оценивания координат и скоростей.

Ансцентный фильтр

Данный алгоритм является заменой расширенному фильтру Калмана, с которым он сравним по вычислительной сложности. При этом он часто позволяет получить лучшие по точности оценки, поскольку реализует не аналитическую, а статистическую линеаризацию нелинейностей.

Алгоритм использует допущения в виде аддитивных моделей оцениваемого и наблюдаемого процессов согласно формулам:

$$x_k = f_k(x_{k-1}) + v_k,$$

$$z_k = h_k(x_k) + w_k.$$

Возмущение объекта v_k и шум измерений w_k представляют собой нормально распределенные случайные величины с нулевым средним и ковариационными матрицами, равными, соответственно, Q_k и R_k .

В алгоритме применяется аппроксимация распределений случайных величин x_k и z_k после соответствующих нелинейных преобразований гауссовскими распределениями с аналогичными моментами первого и второго порядков. При этом для расчета необходимых характеристик распределений величин x_k и z_k – математического ожидания и ковариационной матрицы, используется представление исходных случайных величин в виде набора взвешенных точек.

Входными данными для ансцентного фильтра является математическое ожидание $\bar{x}$ и ковариационная матрица P_{xx} n-мерной величины x.

Первый этап заключается в представлении входной величины x в виде набора $2n + 1$ «сигма-точек» с координатами $\{x_{k-1}^i\}^{2n}$ и весами $\{W_{k-1}^i\}^{2n}$, определяемыми по формулам:

$$\chi^0 = \bar{x},$$
$$\chi^i = \bar{x} + \left(\sqrt{(n+k)P_{xx}}\right)_i,$$
$$\chi^{i+n} = \bar{x} - \left(\sqrt{(n+k)P_{xx}}\right)_i,$$
$$W^0 = \frac{k}{n+k},$$
$$W^i = \frac{n+k}{2},$$
$$W^{i+n} = \frac{n+k}{2},$$

где $i = 1\ldots n$, $k \in R$ – масштабный коэффициент, $\left(\sqrt{(n+k)P_{xx}}\right)_i$ – i-я строка матричного квадратного корня из $[(n+k)P_{xx}]$. Масштабный коэффициент нужен для настройки аппроксимации моментов более высокого порядка и позволяет уменьшить ошибки преобразования. В случае гауссовой величины масштабный коэффициент определяется по эвристическому правилу $n + k = 3$.

Второй этап – этап экстраполяции.

Предполагаем что на $(k-1)$-й момент времени известны математическое ожидание и ковариационная матрица оцениваемого вектора, равные, соответственно $\hat{x}_{k-1}$ и P_{k-1}.

Для предсказания на следующий момент времени k используются формулы:

$$\chi_{k|k-1}^i = f_{k-1}(x_{k-1}^i),$$
$$\hat{x}_{k|k-1} = \sum_i^{2n} W_{k-1}^i \cdot \chi_{k|k-1}^i,$$
$$P_{k|k-1} = Q_{k-1} + \sum_i^{2n} W_{k-1}^i \left[\chi_{k|k-1}^i - \hat{x}_{k|k-1}\right]\left[\chi_{k|k-1}^i - \hat{x}_{k|k-1}\right]^T,$$

$$\hat{z}_{k|k-1} = \sum_{i}^{2n} W_{k-1}^{i}\, h_{k-1}\left(\chi_{k|k-1}^{i}\right).$$

На третьем этапе рассчитывается коэффициент фильтрации и обновляются параметры по формулам:

$$K_k = P_{zx} S_k^{-1},$$
$$S_k = P_k + P_{zz},$$
$$P_{xz} = \sum_{i}^{2n} W_{k-1}^{i} \left[\chi_{k|k-1}^{i} - \hat{x}_{k|k-1}\right]\left[h\left(\chi_{k|k-1}^{i}\right) - \hat{z}_{k|k-1}\right]^T,$$
$$P_{zz} = \sum_{i}^{2n} W_{k-1}^{i} \left[h\left(\chi_{k|k-1}^{i}\right) - \hat{z}_{k|k-1}\right]\left[h\left(\chi_{k|k-1}^{i}\right) - \hat{z}_{k|k-1}\right]^T.$$

Обновление параметров происходит по формулам:

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + K_k\left(z_k - \hat{z}_{k|k-1}\right),$$
$$P_{k|k} = P_{k|k-1} - K_k S_k K_k^T.$$

Наиболее сложной вычислительной операцией алгоритма является вычисление матричного квадратного корня, однако для ее выполнения существуют достаточно эффективные численные процедуры.

Заключение

В случае если функция пересчета состояния системы и функция наблюдений сильно нелинейные, расширенный фильтр Калмана дает плохие результаты. Это связано с вычислением ковариации с помощью линеаризации нелинейной модели. Ансцентный фильтр Калмана использует детерминированную выборку, известную как ансцентное преобразование для выбора минимального набора точек (называемых сигма-точками) вокруг среднего значения. Сигма-точки пропускаются через нелинейные функции, по которым затем восстанавливается среднее значение и ковариация.

В результате получается фильтр, который более точно фиксирует среднее значение и ковариацию. Помимо этого, подобный подход снимает требование на вычисление Якобианов, что для сложных функций может представлять серьезную проблему.

Список используемых источников

1. Фарина А., Студер Ф. Цифровая обработка радиолокационной информации. Сопровождение целей: пер. с англ. / Под ред. А. Н. Юрьева. М.: Радио и связь, 1993. 319 с.

2. Шахтарин Б. И. Нелинейная оптимальная фильтрация в примерах и задачах. М.: Гелиос АРВ, 2008. 344 с.

3. Daum, F. Nonliner Filters: Beyond the Kalman Filter // IEEE A&E Systems Magazine. Vol. 20. No. 8, August 2005. Pp. 57–69.

4. Haug, A. J. Bayesian Estimation and Tracking. Practical Guide. Hobo-ken: John Wiley & Sons, 2012.

5. Микаэльян С. В. Методы фильтрации на основе многоточечной аппроксимации плотности вероятности оценки в задаче определения параметров движения цели при помощи измерителя с нелинейной характеристикой // Наука и образование: научное издание МГТУ им. Н. Э. Баумана. 10.10.11. URL: http://technomag.bmstu.ru/doc/238271.html (дата обращения 01.10.17).

6. Naerum, E., King, H. H., Hannaford, B. Robusness of unscented Kalman filter for state and parameter estimation in an elastic transmission. URL: http://www.roboticsproceedings.org/rss05/p25.pdf (дата обращения 01.10.17).

УДК 004.81
ГРНТИ 28.23.23

АРХИТЕКТУРА И АЛГОРИТМЫ ФУНКЦИОНИРОВАНИЯ КОГНИТИВНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Д. А. Белоцветов[1], В. И. Комашинский[2]

[1]Военная академия связи им. Маршала Советского Союза С. М. Будённого
[2]Институт проблем транспорта им. Н. С. Соломенко Российской академии наук

Любая интеллектуальная система предназначена для ведения определенных видов деятельности, которые, вместе взятые, составляют ее функциональные возможности. Центральный вопрос, который стоит перед разработчиком когнитивной архитектуры, как обеспечить агентам доступ к различным источникам знаний. Например, знания об окружающей среде приходят через ощущение, знания о последствиях нынешней ситуации приходят через планирование, рассуждения и предсказания, знания от других агентов приходят через общение, а знания из прошлого приходит через запоминание и

обучение. Чем больше таких возможностей поддерживает архитектура, тем к большему количеству источников знаний она может получить доступ, чтобы информировать о своем поведении.

Другой ключевой вопрос заключается в том, поддерживает ли когнитивная архитектура какую-то возможность напрямую, используя встроенные процессы, или вместо этого она обеспечивает пути реализации этой возможности с точки зрения знаний. Проектные решения такого рода влияют на то, чему агент может учиться на собственном опыте, что разработчики могут оптимизировать в самом начале, и какую функциональность можно получить от специализированных представлений и механизмов.

архитектура и алгоритмы, когнитивные системы, вычислительные системы.

Когнитивная архитектура определяет базовую инфраструктуру интеллектуальной системы. Вкратце, архитектура включает в себя те аспекты когнитивного агента, которые постоянны во времени и в различных областях применения. Они, как правило, включают в себя: краткосрочную и долгосрочную память, в которых хранится содержимое об убеждениях, целях и знаниях агента; представление элементов, которые содержатся в этих видах памяти, и их организацию в крупномасштабные ментальные структуры; функциональные процессы, которые действуют в этих структурах, в том числе механизмы обеспечения производительности, которые их используют, и механизмы обучения, которые их изменяют.

Исследования когнитивных архитектур важны, потому что они поддерживает главную цель искусственного интеллекта и когнитивной науки: создание и понимание искусственных агентов, которые поддерживают те же возможности, что и люди. Некоторые работы сосредоточены на моделировании инвариантных аспектов человеческого познания, в то время как в других работах архитектуры рассматриваются в качестве эффективного пути к созданию интеллектуальных агентов. Тем не менее, эти цели не противоположны друг другу.

Когнитивная архитектура ACT

Когнитивная архитектура ACT-R (рис. 1) связана, прежде всего, с моделированием человеческого поведения, которое непрерывно развивается с конца 1970-х годов. Версия ACT-R6 состоит из набора модулей, каждый из которых обрабатывает различные типы информации. К ним относятся сенсорные модули для обработки визуальных данных, двигательные модули для действий, модуль намерений для целей и декларативный модуль для долгосрочных декларативных знаний. Каждый модуль имеет связанный с ним буфер, который хранит реляционную декларативную структуру – порции памяти.

Долговременная память продукционных правил координирует обработку модулей. Условия каждой продукции тестируют порции памяти в буферах краткосрочной памяти, в то время как ее действия изменяют применение этих буферов. Некоторые изменения модифицируют существующие структуры, тогда как другие инициируют действия в соответствующих модулях, таких как выполнение команды двигателя или извлечение порции памяти из долгосрочной декларативной памяти. Каждая порция декларативной памяти имеет активацию соответствующей базы, которая отражает ее прошлое использование и влияет на ее извлечение из долговременной памяти, в то время как каждая продукция имеет ожидаемую стоимость и вероятность успеха. Система выбирает продукцию с самой высокой полезностью и выполняет ее действия.

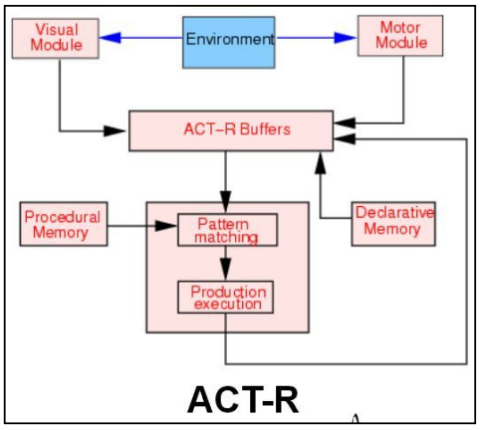


Рис. 1. Архитектура ACT

Сообщество ACT-R использует свою архитектуру для моделирования различных явлений экспериментальной психологии, взятых из литературы, включая аспекты памяти, внимания, рассуждений, решения задач и обработки языка. В большинстве публикаций сообщалось о точном совпадении с полученными для человека количественными данными о времени реакции и проценте ошибок. Совсем недавно связал модули ACT-R с различными областями мозга и разработал модели, которые согласуются с результатами исследований визуализации мозга (*brain-imaging studies*).

Когнитивная архитектура Soar

Soar (рис. 2) – это когнитивная архитектура, непрерывное развитие которой ведется с начала 1980-х годов. Процедурные долгосрочные знания в Soar принимают форму продукционных правил, которые в свою очередь, организованы в терминологии операторов, связанных с пространствами задач. Некоторые операторы описывают простые, примитивные действия, которые изменяют внутреннее состояние агента или генерируют примитивные внешние действия, в то время как другие операторы описывают более абстрактные деятельности. На протяжении многих лет Soar представляла все долгосрочные знания

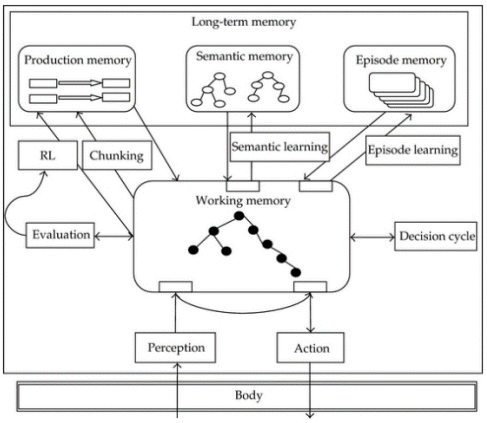


Рис. 2. Архитектура SOAR

в этой форме, но в последнее время были добавлены отдельные эпизодическая память и семантическая память. Эпизодическая память хранит историю предыдущих состояний, в то время как семантическая память содержит ранее известные факты. Все задачи в Soar сформулированы как попытки достижения поставленных целей. Этот процесс может привести к динамической генерации иерархии целей, в которой задачи разлагаются на подзадачи по мере необходимости. «Состояние» конкретной цели включает в себя все свойства задач, находящихся выше нее в иерархии, плюс любые дополнительные когнитивные структуры, необходимые для выбора и применения операторов в этой подцели.

Soar имеет несколько механизмов обучения для различных видов знаний: разбиение данных на порции и обучение с подкреплением позволяют приобрести процедурные знания, тогда как эпизодическое и семантическое обучение позволяют приобрести соответствующие им виды декларативных знаний. Разбиение данных на порции происходит, когда в подцели производится один или несколько результатов. Исследователи использовали Soar для разработки разнообразных изощренных агентов, которые продемонстрировали впечатляющую функциональность. Наиболее заметным был агент TAC-Air-Soar, который моделировал пилотов истребителей в военных учениях, в которых применялись сценарии воздушных боев. Другой успех связан с использованием Soar в моделировании деталей обработки человеческого языка, категоризации и других аспектов познания.

Когнитивная архитектура ICARUS

ICARUS (рис. 3) является более новой архитектурой, в которой хранятся две различные формы знаний. Концепции описывают классы ситуаций окружающей среды в терминах других понятий и ощущений, в то время как навыки указывают, как достичь целей путем декомпозиции их в упорядоченные подцели. Как концепции, так и навыки включают отношения между объектами, и оба вызывают иерархическую организацию долговременной памяти, причем концепции основываются на ощущениях, а навыки на исполняемых действиях. Кроме того, навыки относятся к концепциям целей, которые достигаются, условиям их инициации и условиям их продолжения. Базовый интерпретатор архитектуры ICARUS работает в цикле «распознавание-действие». На каждом шаге архитектура помещает описания видимых объектов

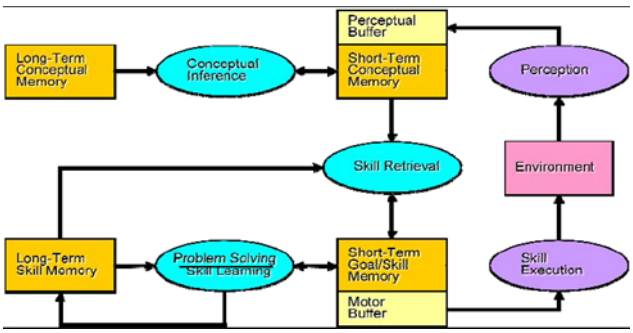


Рис. 3. Архитектура ICARUS

в перцепционный буфер. Система сравнивает примитивные концепции с этими ощущениями и добавляет совпадающие экземпляры в кратковременную память, как убеждения. Если же ICARUS не может найти приемлемый путь в иерархии навыков, который имеет отношение к цели верхнего уровня, он прибегает к решению задачи с использованием варианта анализа «средства-цели». Этот модуль следует за любым навыком, который позволил бы достичь текущей цели.

Исследователи использовали ICARUS для разработки агентов для ряда областей, которые включают комбинацию вывода, исполнения, решения задач и обучения. К их числу относятся такие задачи, как Ханойская башня, вычитание в столбик, пасьянс Свободная ячейка и планирование логистики. Они также использовали архитектуру для управления синтетическими персонажами в моделируемых виртуальных средах.

Когнитивная архитектура PRODIGY

PRODIGY (рис. 4) – еще одна когнитивная архитектура, получившая широкое развитие с середины 1980-х. Эта архитектура включает в себя два основных вида знания. Правила предметной области кодируют условия, при которых действия имеют определенные последствия, где последствия описываются как добавление или удаление выражений первого порядка. Они относятся как к физическим действиям, которые влияют на окружающую среду, так и к правилам вывода, которые являются чисто когнитивными. Напротив, правила управления указывают условия, при которых в процессе поиска эта архитектура должна выбрать, отвергнуть или предпочесть заданный оператор, набор операторов привязки, состояние задачи или цель.

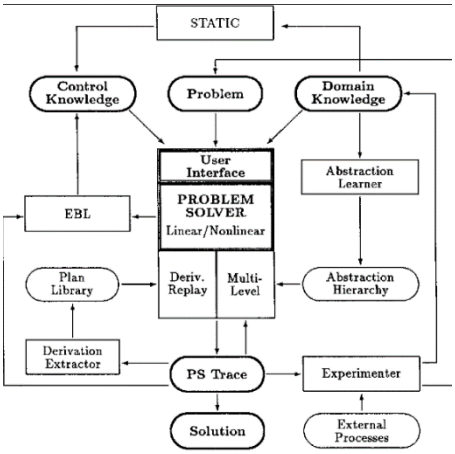


Рис. 4. Архитектура PRODIGY

Поиск опирается на анализ «средства-цели», выбирающий оператор, который уменьшает некоторую разницу между текущим состоянием и целью, что в свою очередь может привести к подзадачам с собственными текущими состояниями и целями. В каждом цикле PRODIGY использует свои правила управления, чтобы выбрать оператор, набор связей, состояние или цель, отвергнуть их или предпочесть одни другим. В отсутствие таких знаний управления, эта архитектура делает выбор случайным образом и производит поиск типа «сначала-вглубь» с возвратом при анализе «средства-цели».

Хотя большинство исследований в этих рамках посвящено исключительно планированию и решению задач, PRODIGY также легла в основу впечатляющей системы с перемежающимся планированием и выполнением для мобильного робота, который принимал асинхронные запросы от пользователей.

Список используемых источников

1. Langley, P. et al., Cognitive architectures: Research issues and challenges, Cognitive Systems Research (2008), doi:10.1016/j.cogsys.2006.07.004

2. Комашинский В. И., Комашинский Д. В. Когнитивная метафора в развитии телекоммуникационных и индустриальных сетевых инфраструктур или первые шаги к постинформационной эпохе // Технологии и средства связи. 2015.

УДК 621.39
ГРНТИ 48.33.35

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ МОБИЛЬНЫХ БЕСПРОВОДНЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ АКТИВНЫХ ДАННЫХ

В. В. Беляев, И. И. Комаров, Е. О. Ласкус

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В статье рассматриваются возможные уязвимости и угрозы в мобильных беспроводных сетях, построенных с применением технологии активных данных, а также применение данной технологии с целью устранения существующих проблем информационной безопасности.

активные данные, беспроводные сети, MANET, информационная безопасность.

Введение

В настоящее время активно развиваются технологии мобильных беспроводных сетей, в частности технологии беспилотных транспортных средств. На данный момент у данной технологии остаются открытыми вопросы организации данных сетей, а также обеспечения их информационной безопасности. В настоящее время в качестве средства, позволяющего ре-

шить данные проблемы, предлагается технология активных данных. В данной работе рассматриваются уязвимости мобильных беспроводных систем и возможные способы использования активных данных для их устранения.

Концепция активных данных

Концепция активных данных является развитием технологии терминальных программ. Терминальная программа – программа, создающая выходные данные и использующая для этого в качестве входных данных только информацию, содержащуюся в коде самой программы. Возможность терминальных программ в процессе коммуникации выполнять активные действия на принимающих устройствах делает сеть передачи данных программно-определяемой, что позволяет в реальном времени менять топологию сети. Поэтому активные данные, являющиеся терминальными программами, в процессе передачи настраивают оборудование, использующееся при их передаче, и управляют самим процессом [1].

Для передачи активных данных производится их сепарация на инициализирующий (транспортный) поток и порождающую программу. Это позволяет осуществлять адаптацию передаваемого контента под особенности сети и ограничения со стороны физических каналов связи. Передача осуществляется пакетами, имеющими в своей структуре три компонента: сигнатуру, предназначенную для идентификации пакета активных данных (ПАД), программу, исполняемую после получением на принимающем узле, и инициализирующий поток, не являющийся обязательной частью ПАД и передающийся лишь в случае необходимости.

Использование активных данных

Мобильные беспроводные сети

Рассматриваемые в данной работе сети относятся к классу MANET (*mobile ad-hoc network*) – беспроводных самоорганизующихся сетей, состоящих из мобильных (т. е. способных перемещаться) устройств. Отличительными особенностями сетей данного типа является динамически изменяющаяся топология сети вследствие движения узлов сети и отсутствие централизованного управления в сети, где каждый узел выполняет роль маршрутизатора.

Уязвимости и угрозы в MANET сетях

Самоорганизующимся MANET сетям присущи следующие уязвимости:

- Каналы передачи данных уязвимы к прослушиванию и подмене сообщений по причине общедоступной среды передачи.

- Узлы слабо защищены от злоумышленника и могут быть изъяты им из сети и использованы в собственных целях.
- Классические системы безопасности, такие как центры сертификации, неприменимы вследствие отсутствия централизованной инфраструктуры.

По причине данных уязвимостей самоорганизующиеся MANET сети уязвимы к классическим типам угроз. Однако в силу присущих им особенностей (например, ограниченному ресурсу источников питания узлов) они также подвержены специфическим угрозам [2].

- **Атака посредника.** Атака, при которой нарушитель изменяет связь между узлами, которые при этом продолжают считать, что общаются непосредственно друг с другом. Данная атака влечет нарушение конфиденциальности информации, так как информация, передаваемая между узлами, проходит и через скомпрометированный нарушителем узел. Однако, в зависимости от целей нарушителя, она может повлечь за собой и нарушение целостности или доступности информации: нарушитель может подменять передаваемые данные на собственные или вовсе не передавать данные узлу-получателю, в то время как узел-отправитель будет считать их доставленными.
- **Атака обхода.** Атака, при которой нарушитель направляет трафик по неоптимальному и выгодному для него маршруту, располагая на основном пути виртуальные узлы, что делает его для узла-передатчика более дорогим с точки зрения расхода ресурсов сети на передачу.
- **Эгоистичность.** Угроза, характерная для всех мобильных самоорганизующихся сетей, вызванная склонностью узлов к сохранению собственных ограниченных ресурсов (например, заряда батареи). С этой целью узлы ограничивают предоставление собственных услуг маршрутизации другим узлам, что нарушает доступность информации в сети.
- **Испытание бессонницей.** Атака, при которой нарушитель повышает мощность работы целевого узла, вынуждая его производить большее количество действий, например, направляя через него дополнительный объем трафика. В результате этой атаки целевой узел либо прекращает работу из-за полного расхода энергии аккумулятора, либо ограничивает свою работу, проявляя эгоистичность. В обоих случаях, данная атака нарушает доступность информации в сети.

Применение активных данных в мобильных сетях

Среди возможных сценариев использования активных данных можно выделить характерные для MANET сетей:

- **Определение и подготовка программного окружения принимающего узла.** Исполняемая программа определяет наличие на узле-приемнике требуемой программы-декодера. В случае ее отсутствия программа-декодер запрашивается у узла-источника. Данный сценарий необходим для первоначальной настройки сети и при добавлении в неё новых элементов.
- **Использование программы-декодера.** Передача программы-декодера производится вместе с инициализирующим потоком в едином ПАД. Формирование программы-декодера под программное окружение принимающего узла позволяет сформировать уникальный декодер, который может быть активирован только на целевом узле. Это позволяет избежать несанкционированного доступа к конфиденциальной информации.
- **Динамическая реконфигурация узлов.** Программа при исполнении на узле определяет возможность создания новых каналов связи с другими узлами путем реконфигурации программной части текущего узла с целью оптимизации (т. е. минимизации времени или затрачиваемых ресурсов) передачи ПАД. Использование данной возможности активных данных позволяет избежать неэффективных маршрутов передачи данных в сети.
- **Комплексное тестирование сети.** Для проверки окружения узлов и характеристик каналов связи между ними на соответствие требованиям производится выполнение программы на всех узлах сети: при выполнении на узле программа проводит его тестирование, а при коммуникации с экземплярами программы на других узлах проверяет состояние каналов связи. При проведении тестирования сети становится возможным выявление неэффективных каналов связи, узлов, проявляющих необычное поведение, и виртуальных узлов

Заключение

В данной работе представлена концепция организации систем передачи активных данных, а также описаны возможности применения активных данных для настройки сетевого оборудования с целью управления процессами маршрутизации и передачи данных в сети и для обеспечения информационной безопасности в данных сетях.

Список используемых источников

1. Кулешов С. В., Цветков О. В. Активные данные в цифровых программно-определяемых системах // Информационно-измерительные и управляющие системы. 2014. № 6. С. 12–19.

2. Бельфер Р. А. Угрозы информационной безопасности в беспроводных саморегулирующихся сетях // Вестник МГТУ им. Н. Э. Баумана. Сер. Приборостроение. Спец. вып. Технические средства, 2011. С. 116–124.

УДК 004.85
ГРНТИ 20.53.19

РАЗРАБОТКА ПО СИСТЕМЫ АНАЛИЗА И МОБИЛЬНОГО МОНИТОРИНГА НА БАЗЕ ОС ANDROID

Е. А. Бовыкин, М. А. Хвостов, В. А. Чебыкин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлена разработка мобильной система мониторинга и контроля качества технологического процесса. Система использует алгоритмы машинного обучения и выгодно отличается от аналогов устранением ряда недостатков, может найти применение при организации производства в различных отраслях.

разработка под Android, Kotlin, машинное обучение, математическое моделирование.

Анализ основных мобильных SCADA систем TeslaModbusSCADA, HMI Modbus TCP, Bluetooth Free, myMOBILE, Scada Touch Lite (HMI-Modbus) выявляет следующие общие недостатки:

- слабые механизмы безопасности на стороне сервера;
- небезопасное хранение данных;
- недостаточная защита транспортного уровня;
- непреднамеренная утечка данных;
- плохо реализованные авторизация и аутентификация;
- некорректное использование криптографии;
- инъекция кода на стороне клиента;
- влияние недостоверных входных данных на безопасность;
- неправильное управление сессией;
- недостаточная защита приложения;
- отсутствие парольной защиты;
- отказ в обслуживании (DoS).

Так же в ходе анализа были обнаружены множественные уязвимости, позволяющие злоумышленникам совершать атаки на систему в целом или часть системы.

В ходе работы была разработана система мониторинга и контроля качества технологического процесса, избавленная от вышеперечисленных недостатков. Система контроля качества использует анализ данных для прогнозирования наличия отказов в технологическом процессе с использованием алгоритмов машинного обучения.

Модель контроля качества изделия в технологическом процессе *M* представляется следующим образом:

$$M =< X, y >,$$

где $X =< x_1, x_2, ..., x_n >, x_i \in R$ – набор показаний промежуточных датчиков,

$y \in \{0,1\}$ – решение системы контроля качества о наличии брака в изделии.

Задачей является прогнозирование решение системы контроля качества *y* по вектору *X*, или некоторым его компонентам

$$X_{comp} =< x_{i_1}, x_{i_2}, ..., x_{i_k} >, i_j \in \{1,2,...,n\}.$$

Показание промежуточного датчика может являться вещественным числом $x_i \in R$, или принимать фиксированный набор значений $x_i \in \{v_1, v_2, ..., v_m\}$, в частности быть либо 0, либо 1 $x_i \in \{0,1\}$.

Для каждого x_i может быть задано уникальное значение t_i, показывающее, в какой момент времени было снято показание датчика. В таком случае вектор *X* представлен в виде $X =< x_1, x_2, ..., x_n, t_1, t_2, ..., t_n >, x_i, t_i \in R$, и для решения задачи прогнозирования могут быть применены модели, работающие с временными рядами.

Для прогнозирования брака используются следующие математические модели:

- KNeighbors – К-ближних соседей;
- SVN – Метод опорных векторов;
- DecisionTree – Дерево решений;
- RandomForest – Случайный лес;
- GaussianNB – Наивный байесовский классификатор.

Сравнение качественных характеристик моделей приведено в таблице. В случае высоких требований к качеству модели следует использовать SVN или RandomForest. В случае высоких требований к скорости прогнозирования следует использовать SVN, DecisionTree или GaussianNB.

ТАБЛИЦА. Сравнение характеристик используемых моделей

Модель	Простота обучения	Скорость прогнозирования	Качество модели
KNeighbors	Да	Низкая	Низкое
SVN	Нет	Высокая	Высокое
DecisionTree	Да	Высокая	Низкое
RandomForest	Нет	Средняя	Высокое
GaussianNB	Да	Высокая	Среднее

Для обеспечения навигации в приложении используется библиотека Cicerone – читается как чи-че-ро-не.

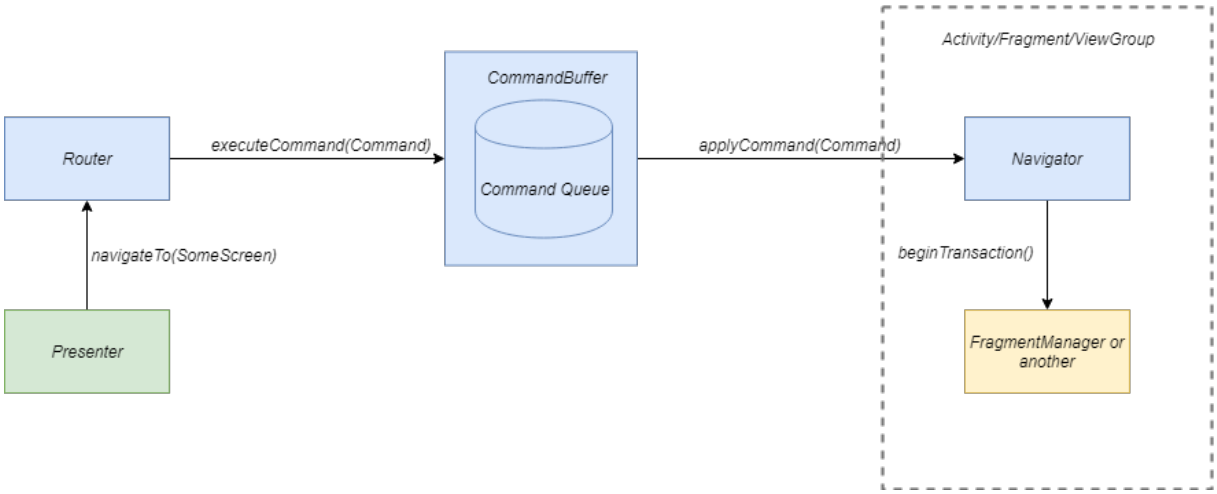


Рисунок. Структура библиотеки

На рисунке приведены четыре основные сущности:

- Command – это простейшая команда перехода, которую выполняет Navigator.
- Navigator – непосредственная реализация «переключения экранов» внутри контейнера.
- Router – это класс, который превращает высокоуровневые вызовы навигации в набор Command.
- CommandBuffer – отвечает за сохранность вызванных команд навигации, если в момент их вызова нет возможности осуществить переход.

Основные преимущества библиотеки:

- не завязана на Fragment’ы;
- не фреймворк;
- предоставляет короткие вызовы;
- легка в расширении;

- приспособлена для тестов;
- не зависит от жизненного цикла

В качестве архитектуры приложения используется паттерн RxPM – реактивная версия паттерна Presentation Model.

- PresentationModel хранит состояние для View, реагирует на UI-события, изменяя модель и состояние View.
- View подписывается на изменения состояния и отправляет действия пользователя в PresentationModel.
- Model – это слой, за которым скрывается бизнес-логика, хранение и получение данных.

Для построения пользовательского интерфейса используется библиотека Anko. Anko является DSL – domain specific language – предметно-ориентированным языком, построенным с помощью языка высокого уровня Kotlin.

Так как любое Android приложение является многопоточным, для работы с аснхронностью и асинхронными потоками данных используется библиотека RxJava 2, которая реализует в себе паттерн Наблюдатель (Observer) и помогает управлять потоками данных. Эта библиотека так же сочетается с паттерном RxPM. Источником данных для нее может выступать любой поток, начиная от пользовательского ввода, и заканчивая данными взятыми из базы данных или сети.

Для внедрения зависимостей (*Dependency Injection*) используется библиотека Koin. В полном соответствии с принципом единственной ответственности [1] объект отдаёт заботу о построении требуемых ему зависимостей внешнему, специально предназначенному для этого общему механизму.

Список используемых источников

1. Martin, Robert C. Clean Code: A Handbook of Agile Software Craftsmanship. Pearson Education, 2008. 157 с. ISBN 978-0-13-608325-2.

2. Пол Д., Харви Д., Александер У. Android 6 for Programmers: An App-Driven Approach, 2016. 512 с. ISBN 978-5-496-02371-9, 978-0134289366

3. Rasmussen, C. E. & Williams, C. K. I., Gaussian Processes for Machine Learning, the MIT Press, 2006. 248 p. ISBN 026218253X.

УДК 621.398; 658.5.012.7
ГРНТИ 50.45.29; 50.03.03

ТЕХНОЛОГИИ МОНИТОРИНГА ПРЕДПРИЯТИЕМ СВЯЗИ ТОПОЛОГИИ ТРАСС ЛИНИЙ СВЯЗИ

В. В. Ботяков, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются вопросы существующего порядка и организации регламентированного учета волоконно-оптических линий связи. Применительно к сложившимся объективным условиям перехода к цифровой экономике страны выработаны организационные и организационно-технические предложения по вводу, обработке и поддержанию в актуальном состоянии пространственных данных о линиях связи, а также их реализуемость при незначительном изменении задействованного в настоящее время ресурса и средств предприятия.

оператор связи, основные средства, радиочастотная метка, радиочастотная идентификация, пространственные данные, автоматизация учета пространственно-временных данных

Значительные успехи в реализации программы «Цифровая экономика Российской Федерации» в отрасли «Связь» обусловлены интенсификацией работ по автоматизации задач организаций связи, которые стандартизованы в соответствии с концепцией NGOSS [1], например, учета ресурсов (рис. 1).

Особенности организации и реализации автоматизированного учета основных средств организации связи, содержащих драгоценные металлы, на основе данных радиочастотной идентификации [3] и пространственных данных объекта учета [4] представлены в [5].

Компьютерные системы и комплексы автоматизации задач инвентаризации и технического учета сетевых ресурсов (NRI, *Network*

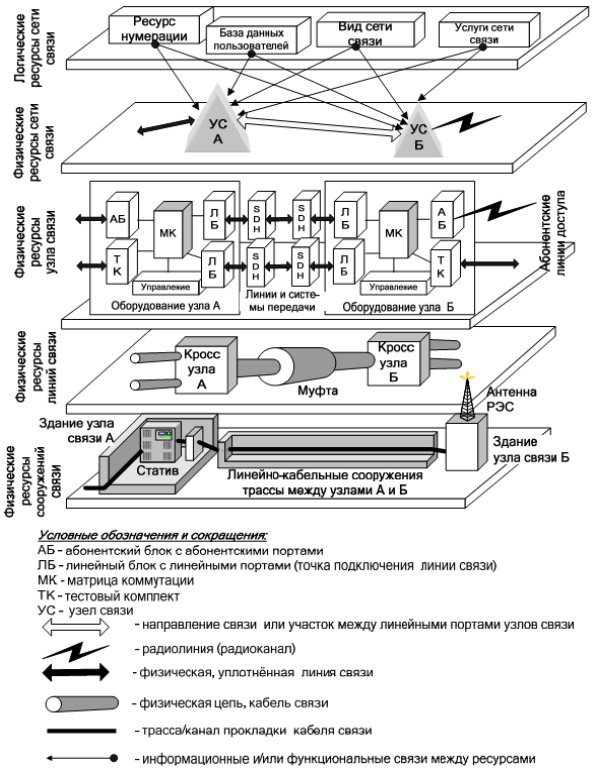


Рис. 1. Логические и физические ресурсы организации связи [2]

Resource Inventory), используемые организациями связи, ориентированы на различную номенклатуру объектов учета и их атрибутов, увязанных с бизнес-процессами основной деятельности оператора связи, например:

− система «АРГУС NRI» ООО «НТЦ-АРГУС» (г. Санкт-Петербург) обеспечивает автоматизацию учёта, обработки и анализа информации по линейно-техническим объектам, сооружениям сети и услугам связи [6];

− система «MoBill-Cross» ООО «Мобилл плюс» (г. Уфа) предназначена для учёта и паспортизации линейно-кабельных сооружений, сетей передачи данных, а также местных кабельных сетей [7];

− система «M2000 Управление ресурсами» ООО «Амфител Плюс» (г. Казань) реализует конвергенцию технологий учета, паспортизации и распределения технических ресурсов организаций электросвязи [8].

Несмотря на высокий достигнутый технический уровень представленных систем (программных средств) и аналогичных им существуют определенные трудности в оперативной актуализации данных о сетевых элементах (типа волоконно-оптических линий связи), так как являются и пассивными (волоконно-оптические кабели и оптические муфты), и расположены вне непосредственной доступности (в грунте).

Для таких сетевых элементов, несмотря на охранно-предупредительные меры, регламентированные Правительством РФ в [9] с учетом требований статьи 106 [10] в соответствии с частью 16 статьи 26 [11], которые принимаются с целью недопущения повреждений кабельных линий связи при производстве работ вблизи или в охранной зоне кабеля, актуальным является «привнесение» им свойства «активности».

Протяжённость линий связи значительна, а срок эксплуатации достаточно длителен. Нарушение целостности волоконно-оптических линий связи, влечёт за собой снижение качества, а в некоторых случаях и полную остановку процесса передачи информации, а вместе с ним и нормативное функционирование линии связи, что несёт в себе для оператора связи как материальные, так и репутационные потери.

С целью предупреждения механических повреждений кабелей и сооружений связи при производстве сторонними организациями и землепользователями работ в охранных зонах линий связи эксплуатационные организации связи должны выполнять комплекс мероприятий, направленный на предупреждение таких ситуаций.

Организация учета обусловлена необходимостью получения своевременных и точных сведений о местонахождении линий связи; документальным подтверждением прохождения трасс, с привязкой к местности, учёта в структурных подразделениях организации связи в целом; подтверждением достоверности данных в представляемой отчетности.

Современные технические средства трассировки подземных коммуникаций [12, 13] разработаны для различных типов объектов поиска (электрических, сигнальных кабелей, кабелей связи, трубо- и газопроводов) и дополнительных идентификационных средств - маркеров:

− трассо-маркероискатели Dynatel серии 2250M-iD компании «3M» для поиска электронных маркеров и чтения / записи пользовательских данных во внутреннюю память интеллектуальных маркеров компании «3M» позволяет осуществлять абсолютную идентификацию неметаллических инженерных коммуникаций и специальных точек на трассе;

− маркероискатель «Сталкер ПМ-2» АО «НПФ "РАДИО-СЕРВИС» предназначен для поиска околоповерхностных, шаровых, дисковых, полноразмерных пассивных электронных маркеров(в том числе интеллектуальных) и определения их глубины залегания, с возможностью последующей записи показаний с привязкой к координатам, полученным от внешнего GPS/ГЛОНАСС модуля и их передачу в компьютер;

− маркероискатель TEMPO EML-100 Marker-Mate компании «TEMPO» (США) предназначен для определения местозаложения электронных маркеров подземных коммуникаций любых типов и производителей (до 7 типов);

− шаровой пассивный маркер 3M™ EMS компании 3M с самовыравнивающуюся конструкцией диаметром 10,4 см, которая обеспечивает точное горизонтальное положение независимо, как оно размещается в земле, без внешнего источника питания, водостоек, дальность (глубина) обнаружения 1,5 метра;

− интеллектуальный маркер 3M EMS-iD компании 3M работает на определённой радиочастоте как и пассивный маркер по специальному 64-битному идентификационному коду, который передаётся к маркероискателю с отражённым сигналом.

Технические средства трассировки подземных коммуникаций имеют ряд недостатков:

− отсутствие интеграции информации из интеллектуальных маркеров и данных GPS;

− применение интеллектуальных маркеров не в составе оптической муфты;

− отсутствие интеграции пространственных данных и атрибутов с учетными данными кабельных линий связи;

− отсутствие интеграции с другими автоматизированными системами организации связи, которые функционально также ведут учет электронных данных об изделиях (средствах, оборудования).

В ходе проведенного исследования возможных направлений снижения выявленных недостатков, рассмотрены существующие подходы и решения по использованию радиочастотных меток и радиочастотной идентификации (RFID) волоконно-оптических линий связи.

Процесс контроля и учёта линий связи может быть улучшен за счет обязательной маркировки линий связи при помощи RFID-меток.

Системотехнические решения по построению системы контроля волоконно-оптических линий связи с применением средств радиочастотной идентификации, включают:

− оснащение линий связи RFID-метками, находящимися внутри оптической муфты;

− доразвертывание инфраструктуры связи техническими средствами съема информации с применением технологии GPS;

− развертывание подсистемы RFID-терминалов;

− интеграцию пространственных данных и атрибутов с учетными данными линий связи.

Для поставленной задачи целесообразно применить считыватели UHF диапазона, оснащённые GPS приёмником, что обеспечит интеграцию пространственных данных, а также дальность считывания до 60 метров в зависимости от используемой метки.

Основной экономической выгодой использования RFID-систем является ускорение и уменьшение трудоемкости операций учета объектов – приемка, отгрузка, инвентаризация, поиск заданных объектов.

Также важным является возможность снижения влияния человеческого фактора, регистрация меток может происходить без участия человека, тем самым оптимизируя трудовые ресурсы и риски.

Проработанный вариант системотехнических решений представлен на рис. 2.

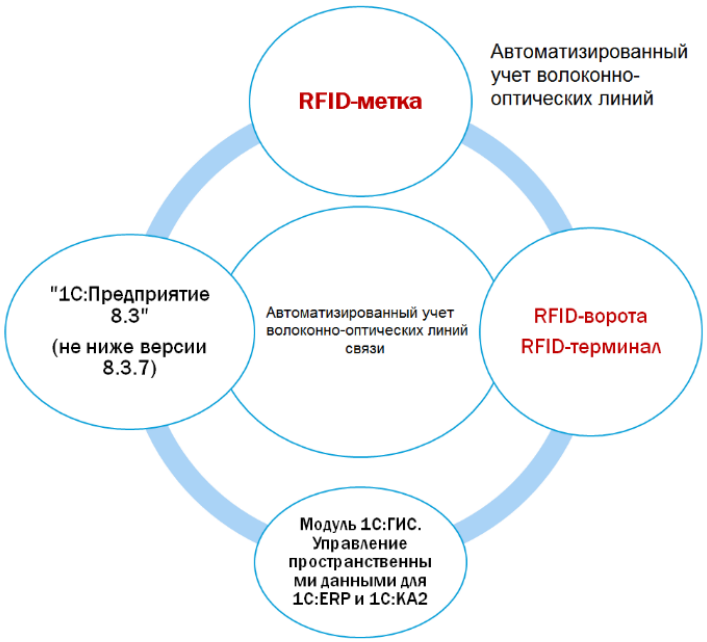


Рис. 2. Системотехнические решения
по обеспечению учета пассивных элементов линий связи

Внедрение предлагаемых системотехнических решений обеспечит:

− учёт пассивных элементов волоконно-оптических линий связи с пространственным позиционированием их местонахождения;

− автоматизацию ввода и выгрузки данных о пассивных элементах волоконно-оптических линий связи, включая пространственные данные;

− ведение и поддержание в актуальном состоянии информационной базы данных о линиях связи, с атрибутами их пространственных данных.

Список используемых источников

1. ГОСТ Р 53633.0-2009. Информационные технологии (ИТ). Сеть управления электросвязью. Расширенная схема деятельности организации связи (eTOM). Общая структура бизнес-процессов.

2. Гребешков А. Автоматизированная система технического учета и паспортизации телекоммуникационных ресурсов // Технологии и средства связи. 2009. № 4. С. 48–51.

3. Ботяков В. В. Программная реализация интерфейсной модели учета драгоценных металлов в основных средствах предприятия связи на основе пространственных данных // 72-я регион. науч.-технич. конф. студентов, аспирантов и молодых ученых "СТУДЕНЧЕСКАЯ ВЕСНА – 2018" 23–24 мая 2018 года. СПб. : СПбГУТ, 2018. С. 27.

4. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб.: ГУАП, 2016. 325 с.

5. Ботяков В. В., Шестаков А. В. Использование пространственных данных об основных средствах предприятия связи в автоматизированном учете драгоценных металлов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т. 2. С.84–88.

6. АРГУС NRI. Система инвентарного учета и паспортизации. Общее описание [Электронный ресурс]. URL: http://argustelecom.ru/2018-01-argus-nri-obshhee-opisanie.pdf (дата обращения 11.02.2019).

7. MoBill-Cross [Электронный ресурс]. URL: https://www.mobill.ru/pages/o-kompanii.html (дата обращения 11.02.2019).

8. "M2000 Управление ресурсами" [Электронный ресурс]. URL: http://www.amfitel.ru/products/m2000-resource-management (дата обращения 11.02.2019).

9. Постановление Правительства РФ "Об утверждении Правил охраны линий и сооружений связи Российской Федерации" от 09.06.1995 № 578.

10. Земельный Кодекса Российской Федерации.

11. Федеральный закон «О внесении изменений в Градостроительный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 03.08.2018 № 342-ФЗ.

12. Трассопоиск и маркировка [Электронный ресурс]. URL: https://www.3mrussia.ru/3M/ru_RU/company-ru/all-3m-products/~/All-3M-Products/-/-/?N=5002385+8709315+8710662+8711017&rt=r3 (дата обращения 11.02.2019).

13. Маркероискатель «Сталкер» ПМ-2. Руководство по эксплуатации. РАПМ.464419.001 РЭ [Электронный ресурс]. URL: https://electroprogress.ru/files/products/re-pm-2-izm0.pdf (дата обращения 11.02.2019).

14. Tempo [Электронный ресурс]. URL: http://compplus.spb.ru/index.php?option=com_virtuemart&page=shop.browse&manufacturer_id=14&Itemid=4 (дата обращения 11.02.2019).

УДК 004.05
ГРНТИ 50.41

ВЫБОР ПОКАЗАТЕЛЕЙ ДЛЯ ОЦЕНКИ КАЧЕСТВА ПРОГРАММНЫХ СРЕДСТВ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Д. А. Бочкарев[1], А. И. Вакалюк[1], О. И. Пантюхин[2]

[1]Военная академия связи им. Маршала Советского Союза С. М. Будённого
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Оценка качества программных средств специального назначения является сложным процессом, основу которого составляет выбор показателей качества. Особенностью разработки программных средств специального назначения является необходимость строгого соблюдения государственных стандартов как в области качества программного обеспечения, так и в области разработки систем специального назначения.

программное обеспечение, оценка качества, государственный стандарт, показатели качества.

Оценка качества выпускаемой продукции в целом и программных средств в частности является одной из основных задач как разработчика (производителя) продукта, так и заказчика. От правильности выбранных подходов к определению показателей качества и своевременности предпринятых действий по оценке качества зависят итоговые затраты и сроки завершения работ по выпуску разрабатываемого изделия.

При разработке программных изделий специально назначения необходимо руководствоваться ГОСТ Р 51189-98. Данный стандарт распространяется на любые программные средства, программные изделия, программы и другие виды и (или) компоненты программной продукции специального назначения (далее – программные средства специального назначения, ПССН).

Учитывая специальные условия применения ПССН необходимо уделить особое внимание свойствам, определяющим их качество.

Определим основные понятия качества для ПССН [2]:

− качество программного средства – совокупность свойств программного средства, которые обусловливают его пригодность удовлетворять заданные или подразумеваемые потребности в соответствии с его назначением

− характеристика качества (программного средства) – набор свойств программного средства, посредством которых описывается и оценивается его качество.

− показатель качества (программного средства) – характеристика качества программного средства, обладающая количественным значением.

Основными принципами проектирования и создания ПССН являются: принцип системности; принцип технологической полноты [1].

Принцип системности разработки ПССН заключается в том, что взаимосвязанные задачи и вопросы, возникающие в процессе проектирования таких средств, решают не по отдельности, а совместно, с учетом влияния принимаемых решений на целевые показатели разработки данного ПССН при взаимодействии всех его составных частей. Принцип технологической полноты заключается в том, что при проектировании ПССВ учитывают необходимость в обеспечении выполнения всего жизненного цикла каждого ПССН – от формирования исходных требований к нему и до снятия с применения.

Исходя из данных принципов необходимо на ранних стадиях разработки определить характеристики качества, разрабатываемого ПССН, а также показатели качества и критерии его оценки.

Для этого составим общий список свойств ПССН, характеризующие его качество, устанавливаемые государственными стандартами.

ГОСТ 28195-89 «Оценка качества программных средств. Общие положения» вводит следующую номенклатуру показателей качества и характеризуемые ими свойства ПССН: показатели **надежности**: устойчивость функционирования, работоспособность; показатели **сопровождения**: структурность, простота конструкции, наглядность, повторяемость; показатели **удобства применения**: легкость освоения, доступность эксплуатационных программных документов, удобство эксплуатации и обслуживания; показатели **эффективности**: уровень автоматизации, временная эффективность, ресурсоемкость; показатели **универсальности**: гибкость, мобильность, модифицируемость; показатели **корректности**: полнота реализации, согласованность, логическая корректность, проверенность.

Согласно ГОСТ 28806-90 «Качество программных средств. Термины и определения» характеристиками и подхарактеристиками качества ПССН могут быть: **функциональность**: адекватность, правильность, комплексируемость, нормосоответствие; **надежность**: завершенность, отказоустойчивость, восстанавливаемость программного средства; **удобство использования**: понимаемость, осваиваемость, управляемость; **эффективность:**

времяемкость, ресурсоемкость; **сопровождаемость**: анализируемость, модифицируемость, стабилизированность, тестируемость; **мобильность**: адаптируемость, настраиваемость, заменоспособность.

Представленные перечни имеют как общие характеристики, так и различающиеся, некоторые из различных по наименованию – одинаковы по содержанию. Проанализировав государственные стандарты [1, 2] можно сделать вывод, что при определении показателей качества разрабатываемого ПССН необходимо руководствоваться следующим обобщенным перечнем характеристик и подхарактеристик качества ПССН:

- **надежность:**
- устойчивость функционирования, работоспособность, завершенность, отказоустойчивость, восстанавливаемость**;**
- **сопровождаемость:**
- простота конструкции (анализируемость), наглядность, повторяемость, модифицируемость, стабилизированность, тестируемость;
- **удобство применения (использования):**
- легкость освоения (понимаемость), доступность эксплуатационных программных документов (осваиваемость), удобство эксплуатации и обслуживания (управляемость);
- **эффективность:**
- уровень автоматизации, временная эффективность, ресурсоемкость;
- **универсальность**:
- гибкость, мобильность (адаптируемость), настраиваемость, заменоспособность;
- **корректность:** полнота реализации, согласованность, логическая корректность, проверенность**.**
- **функциональность:**
- адекватность, правильность, нормосоответствие, комплексируемость, защищенность.

При разработке требований к ПССН на стадии жизненного цикла «Формирование требований» [1], необходимо конкретизировать указанный перечень с учетом назначения ПССН и требований областей применения Если ПССН включает в себя отдельные составные части, то необходимо определить перечень показателей для каждой из них, так как показатели для ПССН в целом могут отличаться от требований к составным частям. На стадии «Разработка концепции» исходя из принятых показателей выбрать и обосновать критерии оценки качества. Далее перечень показателей качества и критерии оценки указывают в разделе «Требование к программе или программному изделию» технического задания.

При разработке программы и методики проведения испытаний необходимо определить методику оценки качества ПССН по указанному в техни-

ческом задании перечню показателей. Подходы к процессу оценивания качества ПССН определены в ГОСТ Р ИСО/МЭК 9126-93 «Информационные технологии. Оценка программной продукции. Характеристики качества и руководство по их применению», а также в ГОСТ 28195-89 «Оценка качества программных средств. Общие положения».

Задача оценки качества программных средств специального назначения не сводится только лишь к адекватному определению перечня показателей качества разрабатываемого ПССН. Основную часть данного процесса составляют определение методики оценки для конкретного программного средства, установление критериев оценки, измерение значений показателей и другие. Однако правильный выбор показателей является необходимым условием для разработки качественного продукта.

Список используемых источников

1. ГОСТ Р 51189-98. Средства программные систем вооружения. М.: Стандартинформ, 2010.

2. ГОСТ 28806-90. Качество программных средств. Термины и определения. Сб. ГОСТов. М.: Стандартинформ, 2005.

3. ГОСТ 28195-89. Оценка качества программных средств. Общие положения. М.: Издательство стандартов, 1989.

4. ГОСТ Р ИСО/МЭК 9126-93. Информационные технологии. Оценка программной продукции. Характеристики качества и руководство по их применению. М.: ИПК Издательство стандартов, 2004.

УДК 004.9
ГРНТИ 20.23.17

РАЗРАБОТКА СИСТЕМЫ ДЛЯ ОНЛАЙН ОБУЧЕНИЯ

И. Р. Бунеев, В. Н. Лукьянчик

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Образовательные онлайн-курсы набирают популярность у желающих повысить квалификацию или освоить новую профессию. Зародившаяся на Западе индустрия дистанционных обучающих платформ позволяет получить достаточно качественное образование, если речь идет о введении в профессию начинающих специалистов, либо о получении дополнительных знаний. В статье рассматривается процесс разработки веб-системы для оказания услуг в сфере онлайн-обучения, а также проектирование веб-системы средствами языка UML.

онлайн обучение, проектирование, uml, idef0, диаграмма деятельности, диаграмма вариантов использования, диаграмма классов, веб-разработка, web-программирование.

На сегодняшний день становится очевидным тот факт, что без образования практически невозможно устроиться на работу с достойной заработной платой. Современные требования к кандидатам на различные должности включают наличие нескольких образований. Если же говорить о более престижных должностях с хорошей заработной платной, то нужно иметь два и более образования. Обучение в вузе занимает достаточно много времени. Поэтому большинство граждан предпочитают краткосрочные курсы для повышения своей квалификации и улучшения различных навыков.

Дистанционное обучение помогает получить образование быстро, не выходя из дома. Ключевым элементом построения онлайн обучения является использование интернет-технологий. Все экзамены сдаются на компьютере в удобное для студента время. В условиях жесткой конкуренции, предприниматели вынуждены осваивать новые инструменты и технологии, чтобы опережать конкурентов. Указанные выше причины способствуют стремительному развитию дистанционного обучения. **Преимуществами данного вида обучения являются: приемлемая стоимость;** удобство сдачи экзаменов и контрольных работ; короткие сроки обучения. Данный способ образования отлично подходит для обучения персонала, особенно в организациях, где работники часто сменяются. Проведя анализ данной области можно сделать вывод о том, что данный вид услуг на сегодняшний день является актуальным и требует повышенного внимания.

Перед разработкой программы был проведен сравнительный анализ функциональных возможностей аналогичных программных продуктов. Для исследования были выбраны GeekBrains и ИНТУИТ. Данные представлены в таблице.

ТАБЛИЦА. Сравнительный анализ аналогичных программных продуктов

Критерий	**GeekBrains**	**ИНТУИТ**
Стажировка	частично	нет
Видеокурсы	есть	частично
Сертификация	есть	есть
Повышение квалификации	нет	есть
Профессиональная подготовка	нет	есть
Высшее образование	нет	есть
Канал на YouTube	есть	есть
Тесты	есть	есть
Трудоустройство	нет	нет
Форум	есть	частично
Бесплатное обучение	есть	есть

Критерий	GeekBrains	ИНТУИТ
Современный дизайн	есть	нет
Домашнее задание	есть	нет

Сегодня процесс создания сложных программных приложений невозможно представить без процесса проектирования. Моделирование средствами IDEF0 является одним из первых этапов изучения любой системы. Опишем процесс проведения онлайн обучения. На первом этапе формируются программы обучения. На вход поступают книги, финансы, научные журналы. Далее преподаватели составляют рабочую программу, план обучения, разрабатывают лекции, задания, критерии оценки. На выходе получаем сформированный учебный курс.

После того как курс разработан и готов к эксплуатации, происходит набор группы используя различные средства маркетинга. Затем происходит оплата за обучение и наступает этап образовательного процесса, в котором учувствуют преподаватели и учебные группы. Выходными элементами данного процесса являются прибыль и клиенты, удовлетворенные полученными знаниями. Диаграмма IDEF0 описывающая основные процессы в области онлайн обучения представлена на рис. 1.

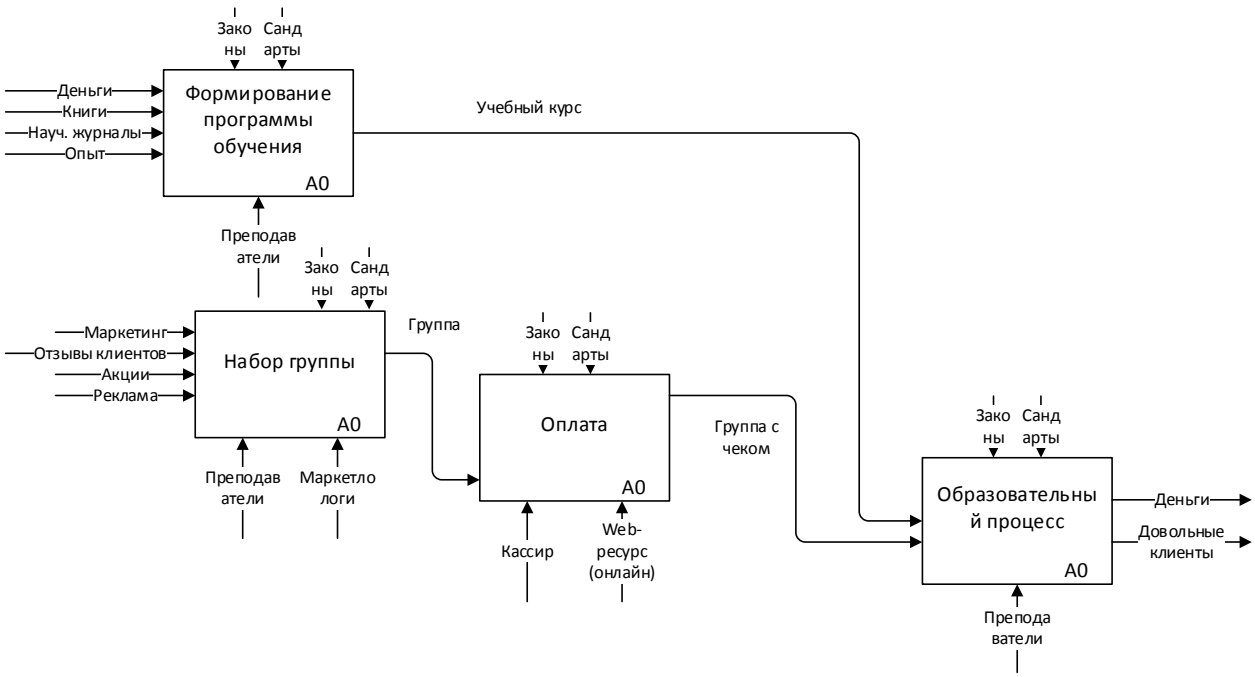


Рис. 1. Диаграмма IDEF0 основных процессов в области онлайн обучения

Далее наступил этап концептуального проектирования предметной области для последующей разработки базы данных, на котором была использована ER-модель («сущность – связь»), предложенная Питером Ченом,

в 1976 году. С её помощью были выделы ключевые сущности и обозначены связи между этими сущностями. Во время проектирования базы данных было выполнено преобразование ER-модели в конкретную схему базы данных на основе выбранной реляционной модели данных. Концептуальная схема базы данных изучаемой предметной области представлена на рис. 2.

При разработке программы была использована свободная реляционная система управления базами данных MySQL. У данной базы данных множество достоинств: данная система распространяется бесплатно, имеет хорошую поддержку в API любых языков программирования.

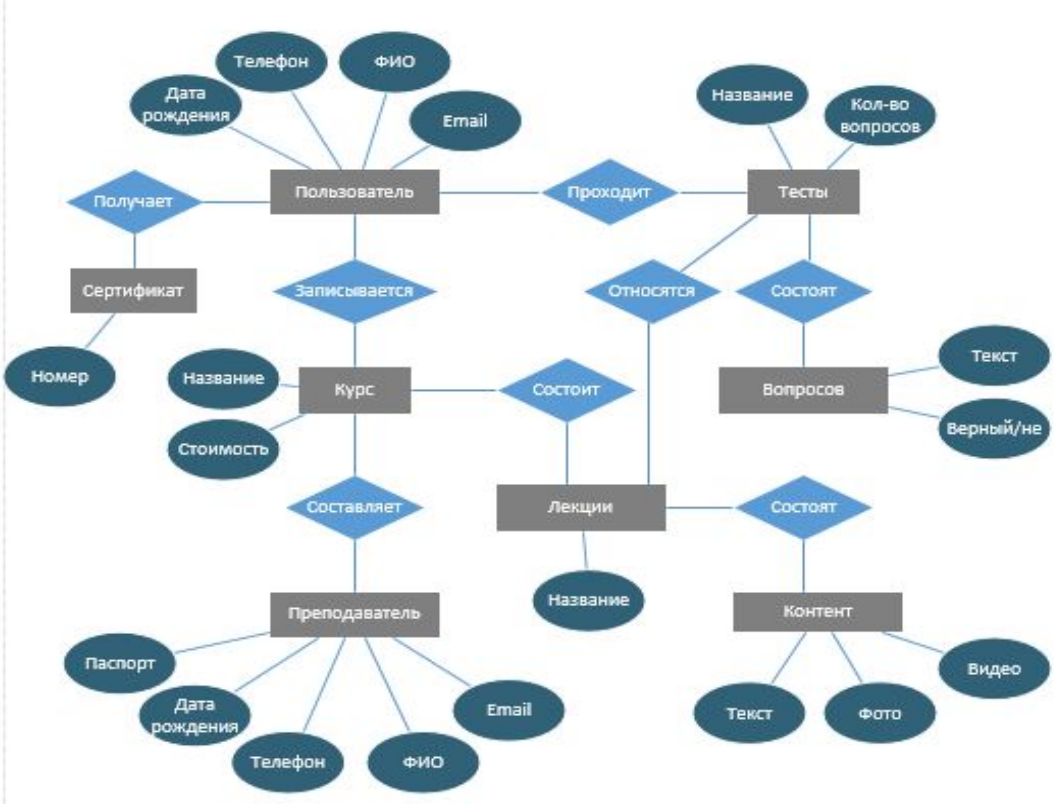


Рис. 2. Концептуальная схема базы данных

Основными отношениями в базе данных являются «курс» и «студент». Приложение написано на PHP фреймворке Yii2. Разработанная программа состоит из нескольких подсистем. Первая – это подсистема хранения данных, которая предназначена для хранения данных о пользователях системы, данных необходимых для формирования аналитических отчетов, а также для хранения всей необходимой информации для обеспечения всего образовательного процесса, включая лекции, видео уроки, задания.

Подсистема формирования отчетности предназначена для создания и формирования отчетов в виде удобном для вывода на печатающие устройства на основе данных системы. Отображения регламентированных отчетов с помощью веб-интерфейса, вывода подготовленных отчетных форм на печать.

На этапе проектирования был использован язык графического моделирования UML. На рис. 3 представлена диаграмма деятельности для процесса регистрации в системе.

На рис. 4 представлена диаграмма последовательности для процесса добавления курса.

Скриншоты работы программы представлены работы программы представлены на рис. 5.

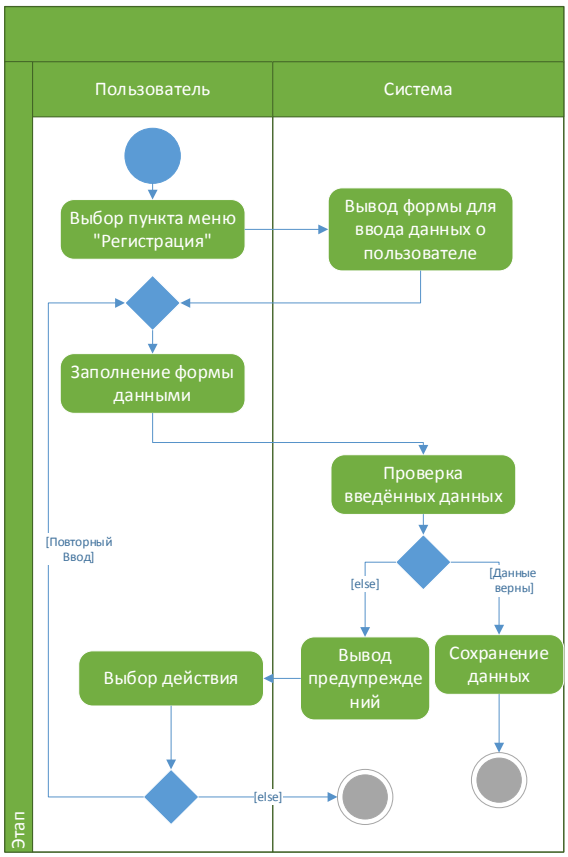


Рис. 3. Диаграмма деятельности для процесса регистрации в системе

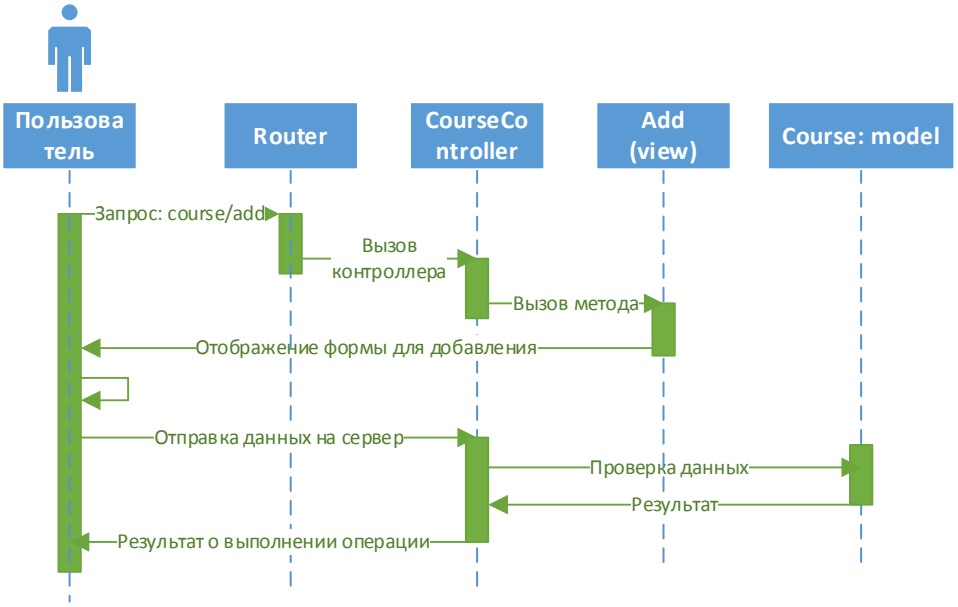


Рис. 4. Диаграмма последовательности для процесса добавления курса

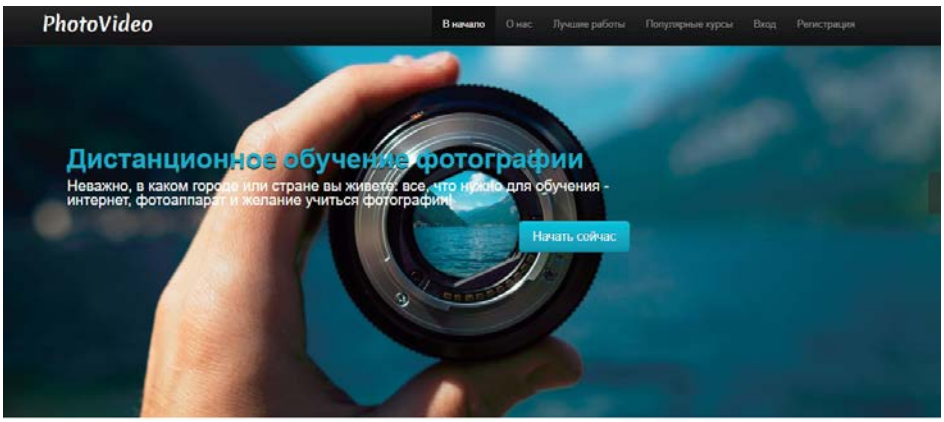


Рис. 5. Главная страница сайта

Список используемых источников

1. Захарова У. С., Можаева Г. В., Бабанская О. М., Танасенко К. И. Развитие онлайн-обучения в программе томского регионального центра компетенций в области онлайн-обучения // Открытое и дистанционное образование. 2017. № 4 (68). С. 25–31.

2. Кобылянский В. Г., Осяев Д. С. Сравнение web-технологий доступа к данным. Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2016. С. 71–75.

3. Петрянин Д. Л., Горячев Н. В., Юрков Н. К. Анализ систем защиты информации в базах данных. Пенза: Пензенский государственный университет, 2013. С. 115–122.

4. Магомедова М, Н. Проектирование информационных систем посредством интеграции технологий объектно-ориентированного программирования и нотаций IDEF // Объектные системы. Ростов-на-Дону, 2013. С. 30–32

УДК 351.354
ГРНТИ 82.05.21

ФОРМАЛИЗАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОСФЕРНОЙ БЕЗОПАСНОСТИ РЕГИОНА

В. Г. Бурлов, М. О. Лепешкин

Санкт-Петербургский политехнический университет Петра Великого

Управление социальными и экономическими системами, обеспечением техносферной безопасности региона использует модели на основе анализа. Использование таких моделей не обеспечивает гарантии достижения цели формирования процессов с заданными свойствами. Модель управления, основанная на синтезе и законе сохранения целостности объекта, позволяет решить обратную задачу управления и сформулировать условия применения программно-целевого управления.

техносферная безопасность, модель управления, закон сохранения целостности объекта, модель на основе синтеза.

1. Формализация динамической модели управления обеспечением техносферной безопасности региона

Управление обеспечением техносферной безопасности (ТБ) региона необходимо осуществлять на основе результатов моделирования процессов социально-экономического развития в рамках выбранной концепции управления. В системотехнике существует только два подхода к разработке систем (Г. Х. Гуд, Р. Э. Маккол [1, 2]):

1. Разработка системы (модели) на основе анализа.
2. Разработка системы (модели) на основе синтеза.

Динамическая модель на основе синтеза формализована в виде системы нелинейных дифференциальных уравнений. Определяются три основных системообразующих показателей деятельности региона, соответствующие по закону сохранения целостности объекта В. Г. Бурлова трем базовым взаимосвязанным свойствам («объективность», «целостность», «изменчивость» или «объект», «цель», «действие») [3, 4, 5]:

− демографический показатель **«x»** (показатель численности населения),

− показатель развития экономики **«y»** (ВВП на душу населения в регионе);

− показатель обеспечения ТБ региона **«z»** (расходы на обеспечение ТБ на душу населения в регионе) (рис.).

Все показатели представлены в виде относительных, приведённых, безразмерных величин.

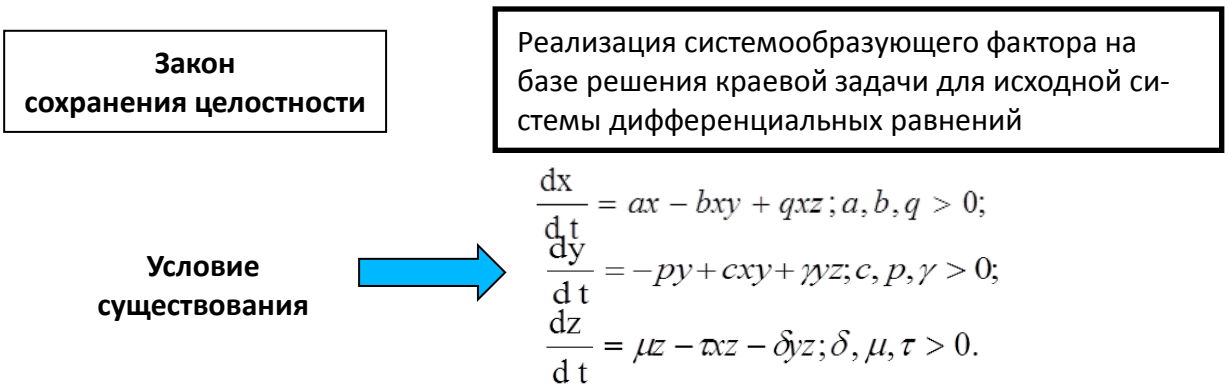


Рисунок. Динамическая модель управления обеспечением техносферной безопасности региона

Моделирование управления на основе синтеза и закона сохранения целостности объекта представлено в работах М. О. Лепешкина [6, 7].

2. Вывод первого дифференциального уравнения

Введём следующие обозначения.

x – демографический показатель, который определяется как

$$x = \frac{x^*(t_0) + x^*(t)}{x^*(t_0)},$$

где $x^*(t)$ – (текущее значение демографического показателя в момент времени t.

$x^*(t_0)$ – (значение демографического показателя изменчивости в момент времени t_0.

Производная показателя «x» $\frac{\mathrm{dx}}{\mathrm{d\,t}}$ есть скорость изменения популяции человека. Скорость изменения **«x»** пропорциональна количеству населения региона. То есть чем больше количество населения, тем и больше его прирост.

$$\frac{\mathrm{dx}}{\mathrm{d\,t}} = ax,$$

где «**a»** – коэффициент демографической активности.

Определим влияние на скорость изменения демографического показателя двух других системообразующих показателей.

«y» – показатель экономического развития. Количественно оценивается ВВП на душу населения в регионе. Количество «**y»** ВВП на душу населения в регионе будут снижать скорость прироста демографического показателя«**x»** на величину, пропорциональную величине «**bxy».**

Дифференциальное уравнение, описывающее изменение демографического показателя «x» примет следующий вид:

$$\frac{\mathrm{dx}}{\mathrm{d\,t}} = ax - bxy,$$

где «**b»** – коэффициент негативного отношения к деторождению (1-2 ребёнка – допустимо; а 3–5 – уже много).

Для данного значения демографического показателя «**x»** показатель обеспечения ТБ «**z»** будет способствовать увеличению скорости прироста популяции человека, пропорционально величине **qxz.** Поэтому, чем больше расходов на обеспечение ТБ в регионе, тем выше скорость роста количественного состава населения этого региона.

Дифференциальное уравнение преобразуется к следующему виду:

$$\frac{\mathrm{dx}}{\mathrm{d\ t}} = ax - bxy + qxz,$$

где «**q**» – коэффициент обеспеченности региона ТБ.

3. Вывод второго дифференциального уравнения

«y» – показатель развития экономики, который определяется как

$$y = \frac{y^*(t_0) + y^*(t)}{y^*(t_0)},$$

где $y^*(t)$ – текущее значение показателя экономического развития в момент времени t;

$y^*(t_0)$ – значение показателя экономического развития в момент времени t_0 (ВВП на душу населения). Производная показателя «y» $\frac{\mathrm{dy}}{\mathrm{d\ t}}$ – есть скорость изменения показателя развития экономики.

Скорость изменения показателя экономического развития (ВВП на душу населения в регионе) пропорциональна количеству ВВП в реальном секторе экономики на душу населения в регионе со **знаком «минус»** (чем больше реально создано ВВП на душу населения в регионе, тем сложней увеличивать и наращивать ВВП)

$$\frac{\mathrm{dy}}{\mathrm{d\ t}} = -py,$$

где «**p**» – коэффициент развития реального сектора экономики.

Для данного значения показателя развития экономики «**y**» демографический показатель «**x**» при заинтересованности людей будет наращивать скорость изменения показателя развития реального сектора экономики на величину, пропорциональную величине «**cxy**», где **«c»** – коэффициент заинтересованности людей в развитии экономики.

Дифференциальное уравнение преобразуется к следующему виду:

$$\frac{\mathrm{dy}}{\mathrm{d\ t}} = -py + cxy.$$

Для данного значения показателя развития экономики «**y**» количество «**z**» – расходов на обеспечение ТБ будут способствовать увеличению скорости прироста показателя развития экономики на величину, пропорциональную величине «**γyz**». (Чем больше расходов на обеспечение ТБ поступает для развития реального сектора экономики региона, тем выше скорость роста показателя развития экономики).

Дифференциальное уравнение имеет следующий вид:

$$\frac{dy}{dt} = py - cxy + \gamma yz,$$

где «**γ**» – коэффициент обеспечения ТБ реального сектора экономики.

4. Вывод третьего дифференциального уравнения

«z» – показатель расходов на обеспечение ТБ. Он определяется как

$$z = \frac{z^*(t_0) - z^*(t)}{z^*(t_0)},$$

где $z^*(t_0)$ – значение показателя расходов на обеспечение ТБ в начальный момент времени t_0;

$z^*(t)$ – значение показателя расходов на обеспечение ТБ на текущий момент времени (t).

Производная этого показателя «**z**» $\frac{dz}{dt}$ есть скорость изменения показателя расходов на обеспечение ТБ. Скорость изменения показателя расходов на обеспечение ТБ **«z»** пропорциональна количеству израсходованных средств на обеспечение ТБ**.** То есть чем большее количество израсходованных средств на обеспечение ТБ в обществе, тем выше скорость её наращивания.

$$\frac{dz}{dt} = \mu z,$$

где **«μ»** – коэффициент наращивания расходов на обеспечение ТБ региона.

Демографически показатель «**x**» будет уменьшать скорость изменения показателя обеспечения ТБ на величину, пропорциональную величине **τxz.** (С увеличением количества населения уменьшается скорость изменения обеспечения ТБ), где **«τ»** – коэффициент соответствия населения обеспечению ТБ.

Дифференциальное уравнение примет следующий вид:

$$\frac{\mathrm{dz}}{\mathrm{d\ t}} = \mu z - \tau xz.$$

Для фиксированного показателя расходов на обеспечение ТБ **«z»** увеличение . ВВП на душу населения в регионе способствует уменьшению скорости прироста показателя обеспечения ТБ пропорциональную величине **γyz.** То есть, чем больше развивается реальный сектор экономики региона, тем меньше расходов на обеспечение ТБ «приходится» к ВВП на душу населения в регионе одному.

А дифференциальное уравнение примет следующий вид:

$$\frac{\mathrm{dz}}{\mathrm{d\ t}} = \mu z - \tau xz - \delta yz,$$

где **«δ»** – коэффициент соответствия развития экономики обеспечению ТБ.

5. Модель управления социально-экономическим развитием региона

$$\left.\begin{aligned} \frac{\mathrm{dx}}{\mathrm{d\ t}} &= ax - bxy + qxz; a, b, q > 0; \\ \frac{\mathrm{dy}}{\mathrm{d\ t}} &= -py + cxy + \gamma yz; c,\ p, \gamma > 0; \\ \frac{\mathrm{dz}}{\mathrm{d\ t}} &= \mu z - \tau xz - \delta yz; \delta, \mu, \tau > 0. \end{aligned}\right\}$$

где **«x»** – показатель численности населения региона;

«y» – показатель экономического развития региона;

«z» – показатель обеспечения ТБ региона.

«a» – коэффициент демографической активности;

«b» – коэффициент негативного отношения людей к деторождению;

«q» – коэффициент обеспеченности региона ТБ;

«c» – коэффициент заинтересованности людей в развитии экономики;

«p» – коэффициент развития реального сектора экономики;

«γ» – коэффициент обеспечения ТБ реального сектора экономики;

«μ» – коэффициент наращивания расходов на обеспечение ТБ региона;

«τ» – коэффициент соответствия населения обеспечению ТБ;

«δ» – коэффициент соответствия развития экономики обеспечению ТБ.

Таким образом, системообразующей основой динамической модели является система дифференциальных уравнений и трёх безразмерных относи-

тельных показателей: социального, экономического и технико-технологического. Девять коэффициентов системы дифференциальных уравнений реализуют механизмы управления процессами обеспечения ТБ региона.

Список используемых источников

1. Маккол Р. Справочник по системотехнике / под ред. А. В. Шиленко. М.: Советское радио, 1970. 688 с.

2. Гуд Г., Маккол Р. Системотехника: введение в проектирование больших систем. М.: Советское радио, 1962. 383 с.

3. Бурлов В. Г. Основы моделирования социально-экономических и политических процессов. Ч. 1. (Модели. Технологии). СПб.: Стратегия будущего, 2007. 278 с.

4. Бурлов В. Г. Основы моделирования социально-экономических и политических процессов Ч. 2. (Методология. Методы). СПб.: Изд-во СПБГПУ, 2007. 265 с.

5. Бурлов В. Г. Закон сохранения целостности объекта – методологическая основа решения задач информационной войны и обеспечения безопасности. Нейрокомпьютеры и их применение Тезисы докладов. 2017. С. 261–263.

6. Лепешкин О. М. Синтез модели процесса управления социальными и экономическими системами на основе теории радикалов. автореферат дис. ... доктора технических наук. СПб.: С.-Петерб. гос. политехн. ун-т., 2014. 33 с.

7. Лепешкин О. М., Лепешкин М. О., Бурлов В. Г. Синтез модели процесса управления техническими системами на основе теории радикалов // В книге: Нейрокомпьютеры и их применение Тезисы докладов. Под редакцией А. И. Галушкина, А. В. Чечкина, Л. С. Куравского, С. Л. Артеменкова, Г. А. Юрьева, П. А. Мармалюка, А. В. Горбатова, С. Д. Кулика. 2016. С. 18-В.

УДК 658.5
ГРНТИ 50.53.19

РАЗРАБОТКА СИСТЕМЫ АВАРИЙНОЙ СИГНАЛИЗАЦИИ НА ОПАСНЫХ ПРОИЗВОДСТВАХ

А. В. Ваганов, С. И. Лебедев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются пути создания системы предупреждения персонала предприятий, в основе которых лежат опасные технологические процессы, о возникновении внештатной ситуации. Показана актуальность разработки таких систем для широкого круга производств, рассмотрены общие концепции их построения. Разработана структура интеллектуальной адаптивной системы аварийной сигнализации (ИАСАС), предполагающей оценку степени угрозы для человека и адаптирующуюся к

изменениям условий окружающей среды. Даны рекомендации к выбору конструкции корпуса системы, выбору элементной базы, а также приведены математические модели для описания отдельных элементов системы.

Разработан алгоритм, позволяющий обеспечить ИАСАС требуемые параметры по надежному обнаружению аварийной ситуации, уменьшающий вероятность ложных тревог.

система аварийной сигнализации, безопасность, производство.

Важнейшим аспектом любого производства является безопасность его персонала. Работа с опасными и легковоспламеняющимися веществами, газовой аппаратурой и химическими материалами приводит к тому, что человеческие жизни могут зависеть от нескольких секунд на обнаружение опасности и нескольких минут на эвакуацию. Важной задачей является создание системы безопасности, которая будет надежно функционировать в независимости от изменения внешних условий и надежно предупреждать персонал предприятия о возникновении внештатной ситуации.

Рассматривая современные систему аварийной сигнализации (САС) следует отметить тенденцию к появлению интегрированных систем, поскольку она способна объединить различные системы сигнализации в одну общую. Все устройства, входящие в систему САС: видео наблюдение, датчики пожарной охраны, электронные замки, шлейфы сигнализации, отображаются на мнемосхемах объекта в виде символов. Оператор способен управлять системой простым кликом мыши. И наконец, интегрированных систем безопасности могут быть объединены единой системой жизнеобеспечения, что сможет обеспечить новое качество жизни и безопасность персонала.

В нашей стране данному вопросу также уделяется много внимания. Разработаны специальные законы и правила, обеспечивающие безопасность людей на предприятиях. Понятие и виды опасных производственных объектов закреплены в Федеральном законе от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов». В данном законе прописаны следующие госты: ГОСТ 22.0.05-97/ГОСТ Р 22.0.05-94 – техногенные чрезвычайные ситуации, ГОСТ Р 22.1.10-2002 - мониторинг химических опасных, ГОСТ Р 22.8.05-99- аварийно-спасательные работы при ликвидации последствий аварий на химически опасных объектах.

Системы безопасности могут быть классифицированы по типу производственного предприятия. Например, промышленного, розничного, государственного и др. В качестве примера рассмотрим два вида САС: гражданскую и производственную. Что касается гражданской системы безопасности, то она может состоять из следующих элементов: пульт контроля и управления, ИБП, адресный релейный модуль, контроллер двухпро-

водных линий связи, извещатель дымовой, блок речевого оповещения, оповещатели речевые. Данная система работает в следующем порядке: сначала включается система оповещения о пожаре. Так же автоматически включается пожаротушение. Затем включается функция дымоудаления, чтобы обезопасить людей от едкого запаха. Огромную роль играет отключение тока и перевод систем в автономный режим.

На современных предприятиях САС имеет более сложную структуру (рис. 1). Рассматриваемая система контроля содержания в воздухе летучих соединений позволяет обнаружить и подать сигнал о превышении ПДК токсичных и взрывоопасных газов.

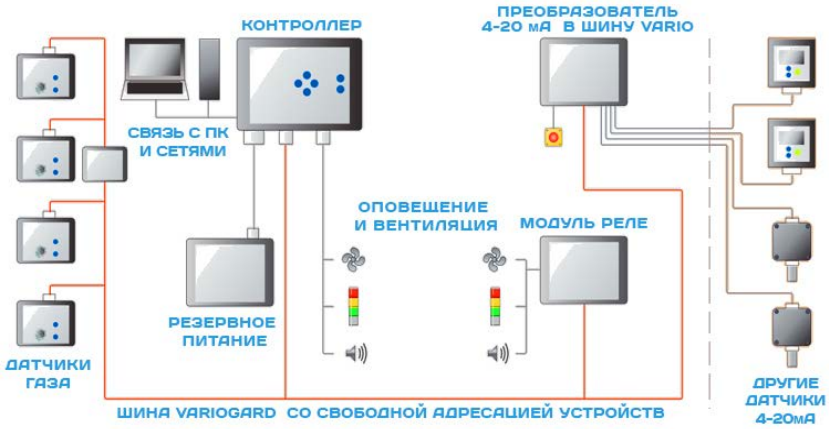


Рис. 1. Система контроля загазованности

Рассмотренные выше системы, не смотря на свою сложность и функциональность, тем не менее обладают следующими недостатками: сложность в эксплуатации, относительно высокая стоимость, наличие высококвалифицированного персонала, отсутствует универсальность. Поэтому задачей является устранение недостатков и создание системы безопасности, которая будет универсальна, обладать функцией интеллектуальной оценки степени опасности ситуации, удобна в обслуживании, а также адаптироваться к изменениям условий эксплуатации. Возможно использование более гибких настроек для данной аппаратно-программной системы.

Общая структура, предлагаемой ИАСАС, приведена на рис. 2. Она включает в себя: управляемый объект (техпроцесс), измерительные устройства, тракт предварительной обработки сигнала, цифровой мультиплексор, аналого-цифровой преобразователь, микроконтроллер, систему управления, устройство управления.

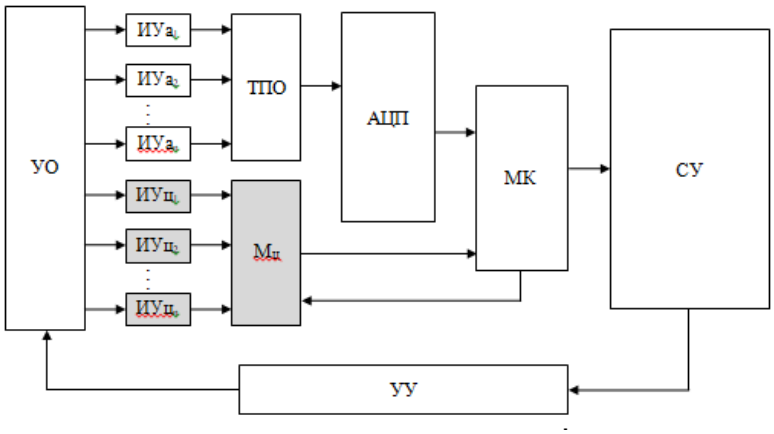


Рис. 2. Структурная схема ИАСАС

В систему могут входить как цифровые, так и аналоговые первичные измерительные преобразователи (микрофоны, вибродатчики и т. п.) Структурная схема тракта первичной обработки сигнала от таких устройств представлена на рис. 3, где: $Д_1$ – датчик дыма, $Д_2$ – метанометр, $Д_3$ – вибродатчик, $Д_4$ – датчик поступления воды, $Д_5$ – датчик запыленности, ДУ – дифференциальный усилитель, У – усилитель, ФП – полосовой фильтр, ПД – пиковый детектор, ПУ – пороговое устройство, АЦП – аналогово-цифровой преобразователь

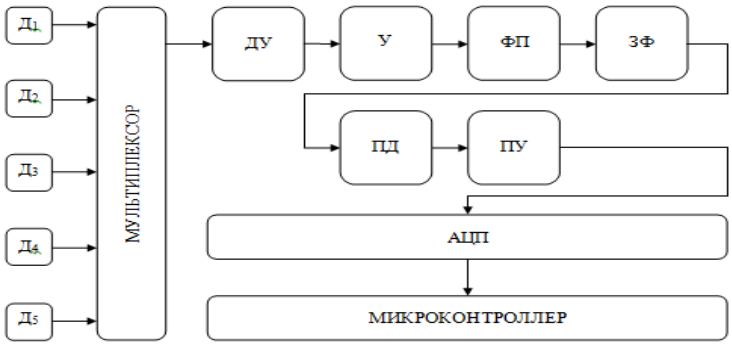


Рис. 3. Структурная схема аналогового сигнала

Данный тракт строится на основе современных дискретно-аналоговых систем обработки – динамически программируемых аналоговых сигнальных процессорах (*dpASP*). Математический аппарат таких систем представляет собой совокупность передаточных функций. Так для фильтра нижних частот передаточная функция в *dpASP* описывается следующей зависимостью:

$$\frac{U_{out}(s)}{U_{in}(s)} = \frac{\pm 4\pi^2 f_0^2 G}{s^2 + \frac{2\pi f_0}{Q} s + 4\pi^2 f_0^2}, \quad (1)$$

где G – коэффициент усиления в полосе пропускания, f_0 – частота среза, Q – добротность.

Передаточная функция режекторного фильтра в *dpASP*:

$$\frac{U_{out}(s)}{U_{in}(s)} = \frac{-G_H s^2 - 4\pi^2 f_0^2 G_L}{s^2 + \frac{2\pi f_0}{Q} s + 4\pi^2 f_0^2}, \quad (2)$$

где G_L – коэффициент усиления по постоянному току,

G_L – коэффициент усиления высоких частот,

f_0 – центральная частота.

Как было отмечено выше, разрабатываемая аппаратно-программная ИАСАС, является адаптивной и интеллектуальной. Это обеспечивается наличием специального алгоритма (рис. 4).

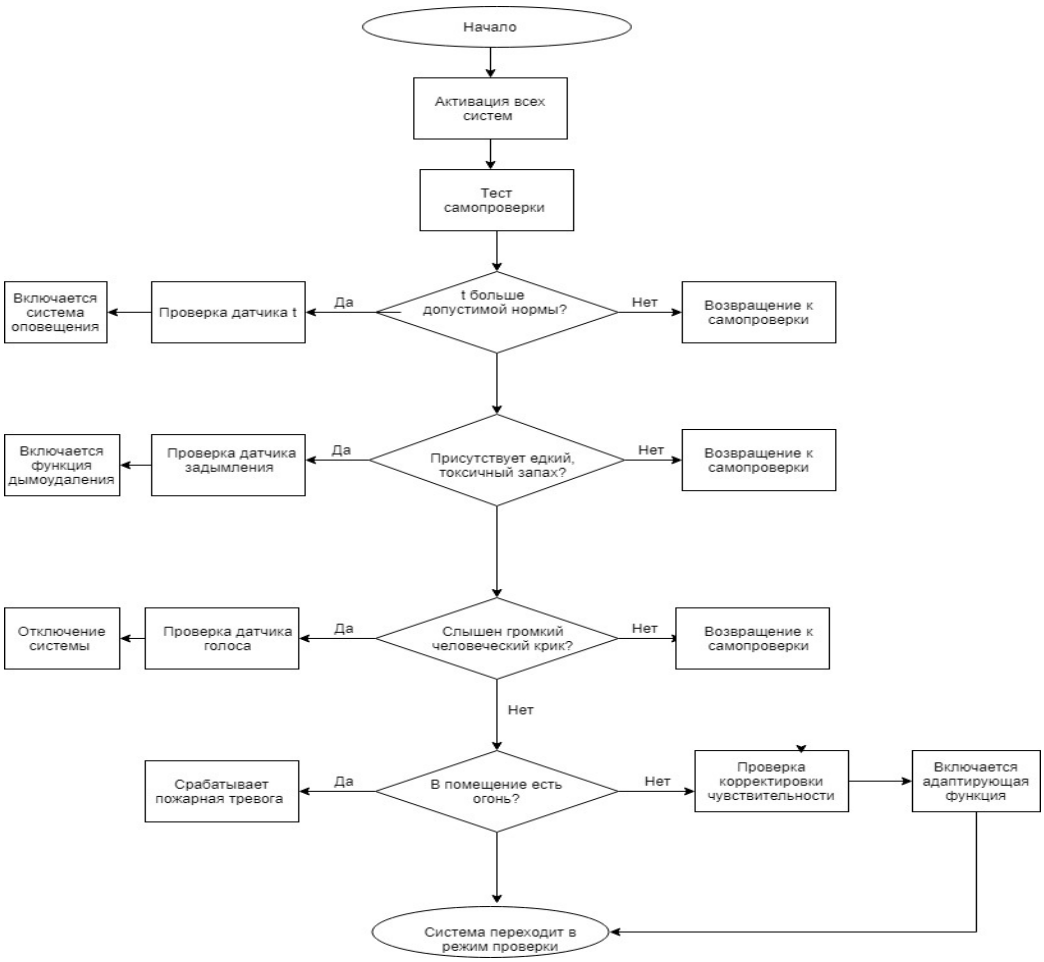


Рис. 4. Блок-схема алгоритма работы ИАСАС

Как следует из рис. 5 при запуске ИАСАС производит самопроверку всех своих систем, после чего последовательно опрашивает каждый из датчиков аварийной сигнализации. При отсутствии от них сигналов тревоги САС производит опрос датчиков внешней среды для последующей интеллектуальной подстройки своих параметров. В случае поступления сигналов от аварийных датчиков ИАСАС производит оценку ситуации и включает необходимые системы активной защиты.

Подводя итоги, следует отметить, что задача разработки интеллектуальной адаптивной ИАСАС, безусловно, является актуальной задачей и в полной мере отвечает современным концепциям в данной области. В статье показаны структура и алгоритм функционирования системы безопасности, а также предложена реализация тракта предварительной обработки сигналов на основе *dpASP*, являющегося динамически конфигурируемой структурой, обеспечивающей компактность и универсальность систем аварийной сигнализации.

Список используемых источников

1. Магауенов Р. Г. Системы охранной сигнализации. Основы теории и принципы построения. М.: Горячая линия – Телеком, 2004. 367 с. ISBN 5-93517-147-3.

2. Баратов А. Н., Пчелинцев В. А. Пожарная безопасность. М.: Изд-во Ассоциации строительных вузов, 2006. 144 с.

2. Федеральный закон от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов».

3. ГОСТ Р 22.1.10-2002. Мониторинг химических опасных объектов.

4. ГОСТ 22.0.05-97/ГОСТ Р 22.0.05-94. Техногенные чрезвычайные ситуации.

5. ГОСТ 50775-95. Системы сигнализации. Основные положения.

6. directory.ifsecglobal.com – фирмы выпускающие аварийные системы безопасности для производственных объектов.

Статья представлена заведующей кафедрой,
доктором технических наук, профессором Г. В. Верховой.

УДК 621.391
ГРНТИ 47.05.15

УСТРАНЕНИЕ ВЛИЯНИЯ ПОМЕХ НА ЭЛЕКТРОННЫЕ УЗЛЫ, БЛОКИ И ПРИБОРЫ В СОВРЕМЕННЫХ АСУ

А. В. Ваганов, К. В. Назаров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается теория обеспечения электромагнитной совместимости различных устройств электронного оборудования, применяемого в современных системах автоматизированного управления предприятий. Произведен обзор основных источников и причин появления электромагнитных помех в цепях предварительной и основной обработки сигналов. Приводятся аналитические зависимости, позволяющие оценить влияние различных источников помех на тракт первичной обработки сигнала.

Даны практические рекомендации для проектирования систем первичного и вторичного электропитания, аналоговых и цифровых каналов передачи и обработки данных. Рассмотрены варианты конструкций приборов и размещения в них блоков, позволяющие минимизировать влияние помех на электронные системы АСУ.

электромагнитная совместимость, источники помех, оценка влияния и минимизация помех.

В настоявшее время системы автоматизированного управления (АСУ) находят все более широкое применение в современном производстве. Их использование позволяет повысить эффективность производства, снизить затраты и повысить качество выпускаемой продукции.

Одной из разновидностей АСУ является автоматизированная система управления технологическими процессами (АСУ ТП). Она характеризуется наличием самостоятельных функций и целей управления, а также специализированного оборудования, которое содержит большое количество электронных блоков и модулей, объединенных в систему. Обобщенная структура АСУ ТП показана на рис. 1, где: управляемый объект (УО), измерительные устройства (ИУ), тракт предварительной обработки сигнала (ТПО), цифровой мультиплексор (Мц), аналого-цифровой преобразователь (АЦП), микроконтроллер (МК), систему реагирования и управления (СУ), устройство управления (УУ).

Управление подобной системой осуществляется посредством передачи сигналов и команд управления между различными ее участками. При передаче таких сигналов важно, чтобы на него не воздействовали внешние фак-

торы – помехи. Помеха – это внешнее или внутреннее воздействие, приводящее к искажению информации во время ее хранения, преобразования, обработки и передачи. Так, например, аналоговый сигнал от первичного измерительного преобразователя при воздействии помехи может искажается, а появления ложного импульса в дискретной системе может привести к некорректной обработке информации и даже сбою системы. Поэтому задача обеспечения минимизации воздействия помех на жизненно важные узлы АСУ ТП – является актуальной и современной задачей.

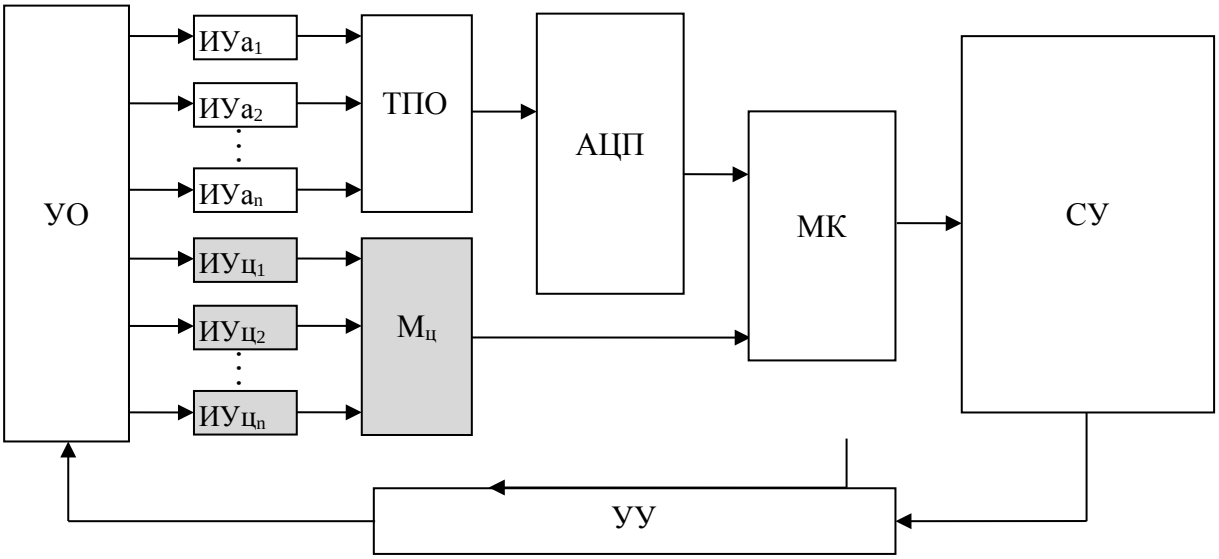


Рис. 1. Структурная схема АСУ ТП

Помехи делятся на: естественные (атмосферные) и искусственные (индустриальные, электронные, энергетические). По месту расположения источника помехи относительно исследуемого электронного устройства различают внешние (внесистемные, внеблочные), внутренние (внутрисистемные) и собственные помехи.

Наиболее уязвимым к помехам является тракт первичной обработки сигнала, содержащий аналоговый датчик, линию связи с первичным трактом обработки сигнала. На рис. 2 и 3 показан механизм формирования сигнала помехи в линии связи для противофазной и синфазной помех соответственно. Противофазные (симметричные) помехи преобладают при низких частотах. Как следует из рис. 2 ток помехи I_S, протекая по замкнутому контуру, состоящему из датчика, линий связи и входного усилителя вызывает падение напряжения помехи на входном сопротивлении R последнего.

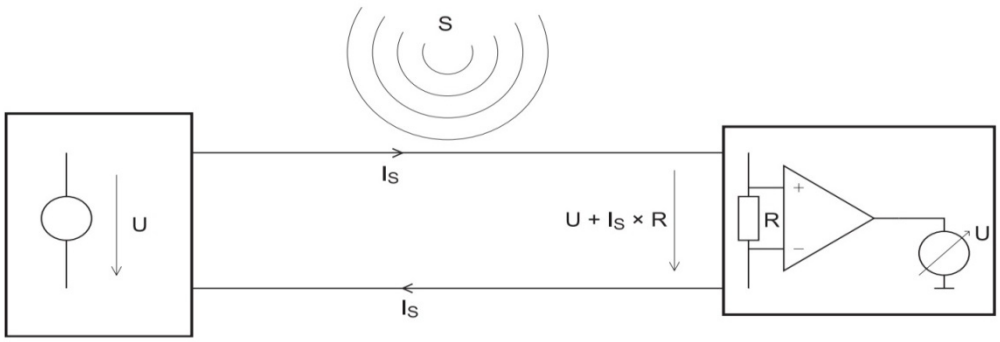


Рис. 2. Противофазная помеха
(*S* – электромагнитная помеха, I_S – ток помехи)

Синфазные (ассиметричные) помехи формируются в сигнальной цепи из-за наличия паразитных емкостей C_P. Так как данные емкости при низких частотах обладают высоким полным сопротивлением, то значимые токи помех I_{S1} и I_{S2} протекают только при высоких частотах сигнала помехи *S*. На измерительном сопротивлении *R* при этом формируется сигнал помехи с амплитудой $\Delta Vs = V_{S1} - V_{S2}$. Обнаружение таких помех затруднено тем, что не всегда очевидно, где цепь тока помехи замыкается паразитными емкостями.

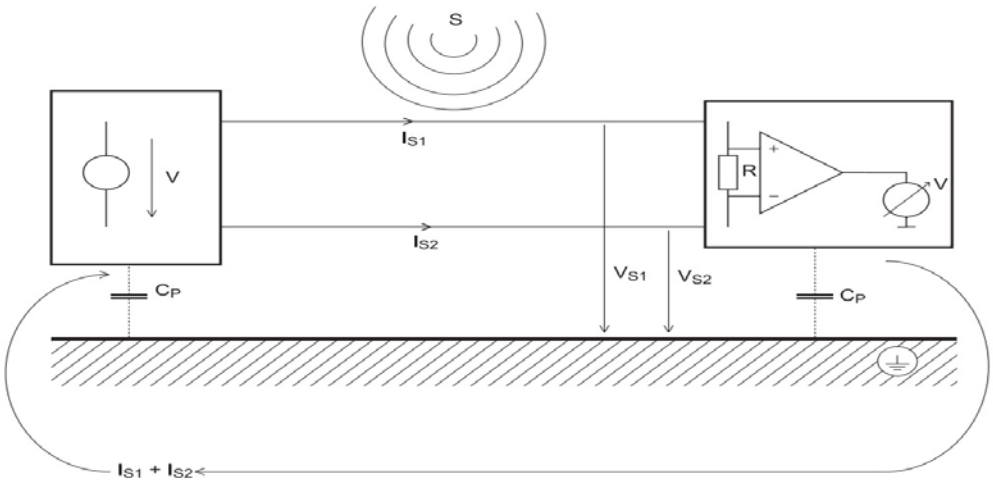


Рис. 3. Синфазная помеха
(*S* – электромагнитная помеха, I_{S1},
I_{S2} – токи первой и второй составляющей сигнала помехи соответственно,
C_P – паразитная емкость)

Понимание причин возникновения помех при проектировании систем автоматизации позволяет избежать ряда ошибок в выборе и размещении оборудования в системе. Как правило, для минимизации помех в трактах как первичной, так и вторичной обработки сигнала эффективны следующие ме-

роприятия: экранирование сигнального кабеля (витая пара, каоксиал), межблочное экранирование, организация соединений между каскадами в виде токовой петли или дифференциального входа-выхода, применение различных фильтров (полосовые, режекторные), правильное размещение самих блоков друг относительно друга внутри корпуса прибора.

Скручивание кабеля (витая пара) – это скручивание выходящих и входящих проводов особенно эффективно для снижения индуктивного воздействия (рис. 4) [1]. При этом образуется много маленьких поверхностей А, на которых индуцируются частичные напряжения помехи с чередующимися знаками ± U_S. Скручивание тем эффективнее, чем меньше поверхность петель. Это достигается за счет увеличения количества витков.

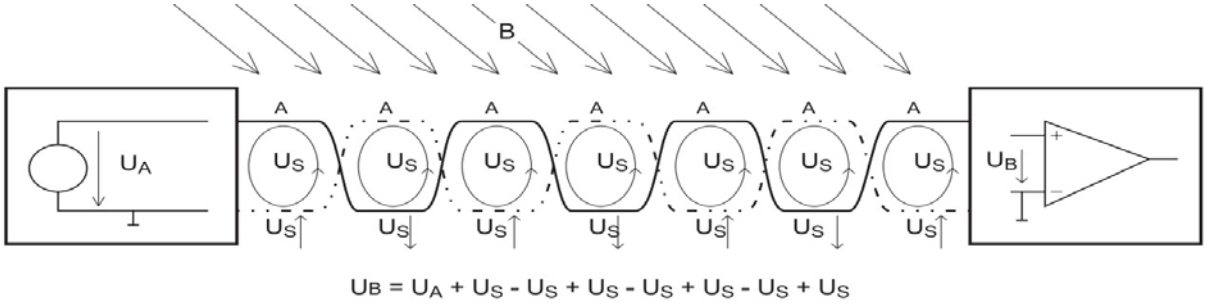


Рис. 4. Модель сигнального кабеля «витая пара»

Электрическое экранирование является одной из возможных мер обеспечения электромагнитной совместимости аппаратуры в части подавления влияния на аппаратуру переменного электрического поля [2]. При этом эффективность экранирования по электрической составляющей для металлического сплошного экрана $Э_{экр}$ рассчитывается по формуле:

$$Э_{экр} = (\frac{\delta \cdot Z}{\rho})^{\frac{1}{2}} \cdot (\frac{\lambda}{R_э})^{\frac{1}{3}} \cdot (1 - \pi \cdot \frac{m}{\lambda}) \cdot \exp(2\pi \cdot \frac{d}{m}), \quad (1)$$

где δ – глубина проникновения,

Z – волновое сопротивление электромагнитного поля,

ρ – удельное сопротивление материала экрана,

λ – длина волны Э/М помехи,

$R_э$ – эквивалентный радиус экрана,

d – толщина металлического листа экрана,

m – наибольший размер технологических отверстий (щелей).

Вычисление амплитуды сигнала помехи, наведенной в сигнальном проводнике от расположенного рядом другого проводника $U_{п\ эл}$, в соответствии с рис. 5 можно выполнить по зависимости (2).

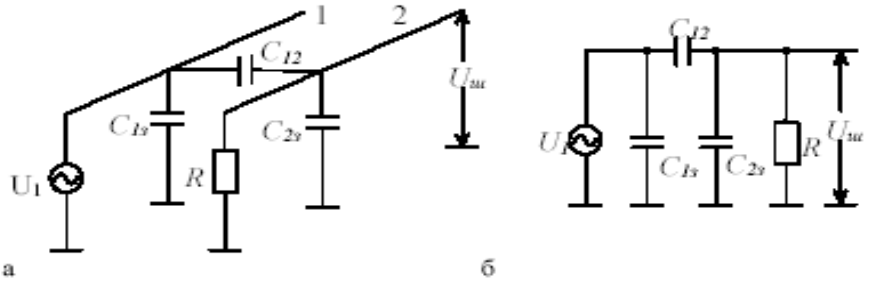


Рис. 5. Емкостная связь между двумя проводниками:
а – физическое представление; б – эквивалентная схема

При этом полагаем значение емкостей проводников относительно земли много меньше емкости между ними $C_{1з} \approx C_{2з} << C_{12}$.

$$U_{\text{пэл}} = \frac{U_1}{Э_{\text{экр}}} \cdot \left(\frac{R_c}{R} + 1 \right)^{-1}, \quad R_c = \left(2 \cdot \pi \cdot F \cdot C_{12} \right)^{-1} = \left(2 \cdot F \cdot \frac{\pi^2 \cdot \varepsilon \cdot L}{\ln(D/d)} \right)^{-1}, \qquad (2)$$

где F – частота сигнала,
R – сопротивление нагрузки,
C_{12} – емкость между проводниками,
L – длина проводников,
ε – диэлектрическая проницаемость,
D – расстояние между проводниками,
d – диаметр проводников.

Интерфейс «токовая петля» (рис. 6) применяется для передачи информации по линии связи в режиме однофазного сигнала. При этом в передатчике вместо источника напряжения используется источник (генератор) тока, так как в этом случае он не зависит от параметров нагрузки.

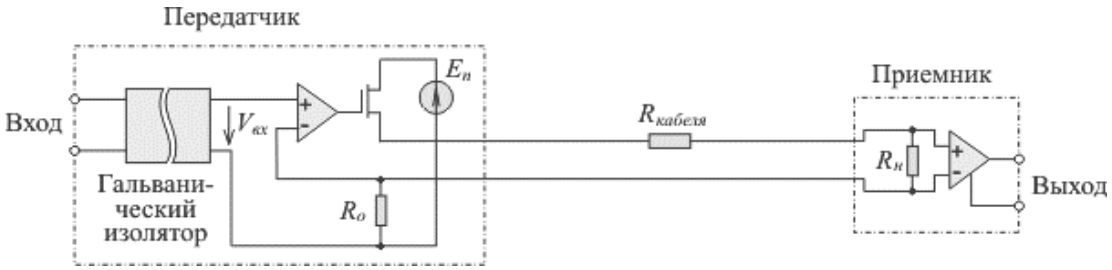


Рис. 6. Организация линии связи по типу «токовой петли»

Таким образом, проектируя, например, тракт предварительной обработки сигнала (ТПОС) в АСУ можно оценить эффективность каждого из способов минимизации помех для данного тракта на основе следующей зависимости [3]:

$$\delta P_{\text{сш}i} = \frac{\left(P_{\text{до}i} - P_{\text{после}i}\right)^2}{\left(P_{\text{до}i} + P_{\text{после}i}\right)} \cdot 100\%, \qquad (3)$$

где $P_{\text{до}\,i}$ и $P_{\text{после}\,i}$ – соотношения сигнал-помеха на выходе ТПОС до и после использования i-го способа минимизации влияния помех соответственно.

Итоговую оценку эффективности каждого из способов удобно проводить путем построения общей диаграммы, состоящей из секторов различной площади, число которых равно числу оцениваемых способов защиты.

Общими рекомендациями для улучшения электромагнитной совместимости устройств АСУ является: разнесение сигнальных и силовых (питающих, управляющих) цепей друг относительно друга, экранирование импульсных модулей питания, наличие гальванически развязывающих устройств в сигнальных цепях между блоками и т. п.

Подводя итоги, следует отметить, что вопрос электромагнитной совместимости различных электронных устройств внутри блоков и приборов АСУ является весьма актуальным. В статье были рассмотрены основные и наиболее эффективные способы защиты электронных устройств от воздействия помех, а также даны рекомендации для улучшения электромагнитной совместимости устройств между собой. Предложен простой способ оценки эффективности рассмотренных способов защиты от помех для тракта предварительной обработки сигнала АСУ.

Список используемых источников

1. Электромагнитная совместимость (ЭМС) в приводной технике (Издание 12/2002).

2. Лотоцкий В. Л. Электромагнитная совместимость устройств систем управления: Учебное пособие. М.: МИРЭА, ГНИИ ИТТ «Информатика», 2002. 61 с.

3. Хабигер Э. Электромагнитная совместимость. Основы ее обеспечения в технике. М.: Энергоатомиздат, 1995. 304 с.

Статья представлена заведующей кафедрой,
доктором технических наук, профессором Г. В. Верховой.

УДК 004.7:004.422.8
ГРНТИ 20.01.07

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ КВАНТОВОЙ КРИПТОЗАЩИТЫ

И. А. Важенин, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Определена система исходных предположений, допускающих аналитическое моделирование процессов функционирования средств квантовой криптозащиты. Выбраны профили качества функционирования средств квантовой криптозащиты. Приведено описание моделей процессов квантовой криптозащиты. Раскрыт метод определения показателей качества функционирования средств квантовой криптозащиты.

квантовая криптозащита, средства, модель, профиль качества, анализ.

Средства квантовой криптозащиты, имея собственный профиль физических особенностей их реализации [1], в контексте информационной безопасности могут рассматриваться как составляющие одной из подсистем комплексной системы защиты информации от несанкционированного доступа. В связи с этим возникает объективная необходимость формирования новых формализаций, позволяющих, с одной стороны, учесть физические и технологические особенности их реализаций в определении и оценивании типовых профилей их качества, а, с другой стороны, обеспечить сквозное связывание с формализациями, входящими в методологический профиль оценивания показателей и критериев качества комплексных систем защиты информации от несанкционированного доступа [2].

Формирование моделей процессов квантовой криптозащиты базируется на математическом аппарате конечных цепей Маркова. При этом считается, что модели процессов квантовой криптозащиты в дальнейшем смогут использоваться для решения следующих задач:

- составление описаний состояний процессов квантовой криптозащиты;
- определение рационального варианта способов и методов квантовой криптозащиты;
- сравнительный анализ влияния различных способов и методов квантовой криптозащиты на показатели качества их функционирования;
- выбор технологий квантовой криптозащиты.

Рассматриваемый подход к формированию моделей процессов квантовой криптозащиты позволяет отразить многообразие способов, методов и

технологических приемов в организации и функционировании возможных вариаций в реализации производимых средств.

При формировании модели рассматриваемый процесс квантовой криптозащиты представляется моделью в виде конечной поглощающей однородной цепи Маркова. Согласно теории марковских цепей при описании процесса квантовой криптозащиты в виде конечной поглощающей однородной цепи Маркова принимается следующая система допущений.

Первое допущение:

- процесс квантовой криптозащиты является процессом смены конечного числа состояний.

Второе допущение:

- поведение процесса квантовой криптозащиты после момента времени t при фиксированном состоянии в этот момент не зависит от его поведения до момента t, т. е. соблюдается такая закономерность: если в данный момент времени t процесс квантовой криптозащиты находится в состоянии i, то в последующий момент времени s процесс квантовой криптозащиты будет находиться в состоянии j с некоторой переходной вероятностью $p_{i,j}(t, s)$ независимо от поведения процесса квантовой криптозащиты до указанного момента времени t.

Третье допущение:

- переходные вероятности $p_{i,j}(t, s)$ зависят лишь от разности $(s - t)$;

$$p_{i,j}(t, s) = p_{i,j}(s - t);\ \ i, j \in \Omega,$$

где Ω – конечное множество состояний процесса квантовой криптозащиты.

Четвёртое допущение:

- среди конечного множества состояний процесса квантовой криптозащиты присутствует хотя бы одно такое состояние, из которого возможен переход с вероятностью, равной единице, только на самого себя. Подобного типа состояния называются поглощающими, а все другие – невозвратными.

Пятое допущение:

- в каждом состоянии процесс квантовой криптозащиты пребывает в течение одной условной единицы времени.

При выполнении перечисленных условий составляется конкретная форма описания модели. Для описания определяется конечное множество состояний, среди которых отмечаются начальное и поглощающее состояние. За начальным состоянием закрепляется первый номер, за одним из поглощающих состояний – последний номер, а за остальными состояниями – различные промежуточные номера. Каждое поглощающее состояние может связываться с заключительной операцией процесса квантовой криптозащиты при определенном сочетании внутренних и внешних факторов, а

невозвратное состояние – с промежуточными операциями. Если ни одно из выделенных состояний не соответствует поглощающему состоянию, то вводится псевдосостояние. Псевдосостояние вводится таким образом, чтобы его непосредственным предшественником было только конечное ($s-1$)-е состояние, а непосредственным преемником – только само псевдосостояние s. В подобном случае s-е состояние будет единственным поглощающим состоянием. При этом момент перехода от ($s-1$)-го состояния к s-му состоянию рассматривается как момент окончания выполнения процесса квантовой криптозащиты.

По описанию конечного множества состояний составляется стохастическая матрица **P** переходных вероятностей:

$$\mathbf{P} = \begin{bmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,s-1} & p_{1,s} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,s-1} & p_{2,s} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ p_{s-1,1} & p_{s-1,2} & \cdots & p_{s-1,s-1} & p_{s-1,s} \\ 0 & 0 & & 0 & 1 \end{bmatrix},$$

где первое состояние является начальным, а s-е состояние – одним из множества поглощающих состояний или единственным поглощающим состоянием.

При формировании модели должны соблюдаться следующие условия:

$$\sum_{j=1}^{s} p_{i,j} = 1,\ i = 1,2\ldots,\ s;$$

$$0 \le p_{i,j} \le 1,\ \ i,j = 1,2,\ldots,s;$$

$$p_{k,k} = 1,\ k \in \mathbf{W};$$

$$p_{k,i} = 0,\ i = k,$$

где **W** – множество поглощающих состояний.

Для наглядности описания стохастической матрицы временной аргумент при вероятностях перехода опускается, что не ограничивает общности представления конечной поглощающей однородности цепи Маркова. При достаточно небольшом значении s конечная поглощающая однородная цепь

Маркова может наглядно представляться графом. В этом случае между конечным множеством вершин графа устанавливается взаимно однозначное соответствие. Вершины графа соединяются дугами, имеющими направления переходов между состояниями. Каждая вершина может сопровождаться не более одной дуги петли. Любая пара вершин может связываться между собой не более, чем двумя дугами. В случае наличия двух связывающих дуг они могут иметь только противоположные друг другу направления. На дугах проставляются переходные вероятности. По графу легко определяется стохастическая матрица **P**. Построение графа не является обязательным моментом в процессе представления модели многоагентной системы.

На втором этапе моделирования процесса квантовой криптозащиты по известным соотношениям для марковских цепей находятся показатели её качества.

В контексте анализа комплексных систем защиты информации от несанкционированного доступа в качестве типового профиля качества средств квантовой криптозащиты выбирается статистический временной профиль, заполняемый динамическими характеристиками в виде плотности распределения вероятностей времени квантовой криптозащиты и числовых характеристик.

Определение стохастической матрицы **P** позволяет перейти к определению статистических характеристик времени функционирования средств квантовой криптозащиты. При определении используются следующие известные соотношения:

$$\mathbf{T} = (\mathbf{I} - \mathbf{Q})^{-1},$$

$$\mathbf{D} = \mathbf{T}(2\mathbf{T}_0 - \mathbf{I}) - \mathbf{T}^*,$$

$$\mathbf{T} = \mathbf{T}\boldsymbol{\lambda},$$

$$\mathbf{d} = (2\mathbf{T}-\mathbf{I})\mathbf{t}-\mathbf{t}^*,$$

где $\mathbf{I}$ – $(M \times M)$ – единичная матрица;

$\mathbf{Q}$ – $(M \times M)$ – матрица переходов во множестве невозвратных состояний;

$\mathbf{T}$ – $(M \times M)$ – матрица, образованная элементами $T_{i,\mathrm{j}}$ $i,j = 1,2,\ldots,M$;

$T_{i,j}$ – математическое ожидание количества пребываний марковской цепи в j-м состоянии, если за исходное принять i-е состояние;

$\mathbf{T_0}$ – $(M \times M)$ – матрица, получаемая из квадратной матрицы $\mathbf{T}$ заменой нулями всех элементов, не лежащих на главной диагонали;

$\mathbf{T^*}$ – матрица, получаемая из матрицы $\mathbf{T}$ возведением в квадрат каждого элемента;

$\mathbf{t}$ – $(M \times 1)$ – вектор-столбец, состоящий из элементов T_i;

T_i – среднее время, затрачиваемое на выполнение операций квантовой криптозащиты при i-м исходном состоянии;

$\boldsymbol{\lambda} – (M \times 1)$ – вектор-столбец, состоящий из элементов D_i;

D_i – дисперсия дискретного времени квантовой криптозащиты при i-м исходном состоянии;

t* – матрица, получаемая из матрицы **t** возведением в квадрат каждого элемента;

M – число невозвратных состояний.

Элементы матрицы **Q** находятся посредством переустановки строк и столбцов в матрице переходов **P**, соответствующей процессу смены состояний процесса квантовой криптозащиты при её представлении в следующей канонической форме:

$$\mathbf{P} = \begin{bmatrix} \mathbf{Q} & \mathbf{R} \\ \mathbf{E} & \mathbf{N} \end{bmatrix}.$$

Показатель T_1 определяет математическое ожидание дискретного времени процесса квантовой криптозащиты. Математическое ожидание времени выполнения каждого подпроцесса, соответствующего невозвратному состоянию, определяется величиной $T_{1,j}$, где j принадлежит множеству невозвратных состояний. D_1 является дисперсией дискретного времени процесса квантовой криптозащиты. $D_{1,j}$ при условии, что j принадлежит множеству невозвратных состояний, представляет собой дисперсию дискретного времени выполнения соответствующего подпроцесса.

Методы линейной алгебры позволяют также находить распределения вероятностей дискретного времени выполнения отдельных подпроцессов процесса квантовой криптозащиты и всего процесса в целом.

Согласно теории цепей Маркова $u(k)$ плотность распределения вероятностей $k = 1, 2, ..., N, ...$ времени квантовой криптозащиты определяется по формуле:

$$u(k) = P_{1,s}^{(k)} - P_{1,s}^{(k-1)},$$
$$k = 1, 2, ..., K, ...;$$

где $P_{1,s}^{(k)}$ – $(1, s)$-й элемент k-й степени матрицы **P**;

$P_{1,s}^{(k-1)}$ – $(1, s)$-й элемент $(k-1)$-й степени матрицы **P**;

k – дискретное время квантовой криптозащиты.

Рассмотренная формализация математического обеспечения для системы определения динамических характеристик средств квантовой криптозащиты может рассматриваться как канва методологии формирования их модельно-аналитического интеллекта, предназначенного для контроля качества реализации возложенных на них задач в условиях последовательной обработки информации.

Список используемых источников

1. Квантовая криптография: идеи и практика / под ред. С. Я. Килина, Д. Б. Хорошко, А. П. Низовцева. Мн., 2008. 392 с.

2. Птицын А. В., Птицын Л. К. Генерация системно-аналитического ядра безопасных информационных технологий. СПб.: Изд-во Политехн. ун-та, 2011. 263 с.

УДК 159.923
ГРНТИ 15.41.39

ПРИЗНАКИ И КРИТЕРИИ ДЕСТРУКТИВНОСТИ ЛИЧНОСТИ И ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ НА ОСНОВЕ ИНТЕРНЕТ-КОНТЕНТА И ПОВЕДЕНИЯ СУБЪЕКТОВ В СОЦИАЛЬНЫХ СЕТЯХ

Н. П. Ванчакова[1], Л. А. Виткова[2,3], И. В. Котенко[2,3], Н. В. Красильникова[1], Л. В. Страх[1], А. В. Тишков[1], А. А. Чечулин[2,3]

[1]Первый Санкт-Петербургский государственный медицинский университет им. И. П. Павлова
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[3]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Сетевое общение является важнейшим средством коммуникации в современном мире. Многие молодые люди ведут себя открыто и даже беспечно, особенно студенты, лишь недавно покинувшие родительский дом. Зачастую молодежь оставляет достаточно контента в соцсетях, по которому возможно обнаружить появившиеся и проследить динамику развивающихся деструктивных элементов поведения. Наиболее опасным поведением в сети признается экстремизм. В настоящей работе предлагается семиступенчатая шкала оценки деструктивности поведения и ее связь с десятью признаками экстремизма в сети, основанными на Федеральном Законе № 114-ФЗ «О противодействии экстремистской деятельности».

деструктивное поведение, социальные сети, экстремизм.

Рассматривая феномены агрессивного, деструктивного поведения молодежи по отношению к социуму, исследователь сталкивается с затруднением анализа данного явления, поскольку статьи различных исторических периодов имеют «..высокий субьективизм исследователей, направленных идейнополитическими и социальнофилософскими установками» [1]. Тем не менее анализ статей последних лет позволяет выделить феномены терроризма и экстремизма как крайне негативные и опасные проявления поведения молодежи. Таким образом, мы можем условно предположить негативный вектор поведения молодежи от экстремизма до терроризма и рассмотреть его по этапам.

Терроризм определяется как «идеология насилия и практика воздействия на общественное сознание, на принятие решений органами государственной власти, органами местного самоуправления или международными организациями, связанная с силовым воздействием, устрашением населения и/или иными формами противоправных насильственных действий» [2].

Экстремизм – это «приверженность к крайним мерам и взглядам, радикально отрицающим существующие в обществе нормы и правила через совокупность насильственных проявлений, совершаемых отдельными лицами и специально организованными группами и сообществами» [3]. Работы различных авторов показали, что экстремизм в своей крайности приводит к терроризму [4].

А. А. Затолокин считает, что экстремизм начинается с правового нигилизма. «Проявление симптомов экстремизма на ранней стадии выражается в нивелировании общественно значимых норм и правил: в сквернословии, в нарушении правил дорожного движения, в распитии спиртных напитков на территории детских площадок, в выгуле собак без поводка и намордника ..» [5].

Современный экстремизм имеет две тенденции – он в основном носит информационный характер и характерен для молодежи. Деструктивное сетевое поведение рассматривается в данном исследовании как признак приверженности негативному поведению, крайним проявлением которого является экстремизм.

Цель работы – определить понятие сетевого деструктивного поведения, создать классификацию видов такого поведения и оценить его выраженность.

Согласно [6], для экстремизма в информационном поле интернет сети характерно: «..большую часть ежедневной аудитории онлайн-ресурсов составляют лица, моложе 30 лет, а аудитория социальных сетей – это преимущественно подростки и молодые люди от 14 до 20 лет, т. е. учащиеся школ и вузов. Молодежь привлекают анонимность и масштабность сети Интернет, которая на сегодняшний день является эффективным инструментом пропаганды террористической и экстремистской деятельности».

Авторы Р. Л. Лашин и С. А. Чурилов описывают техники быстрого распространения информации (продвижение необходимых хештегов) и манипулятивные механизмы формирования общественного мнения: формирование идеологии «свой–чужой», превосходства одной национальности над другой, стереотипизация образа «врага», публикация непроверенной информации, намеренное искажение фактов, создание своего «языка общения», апелляция к авторитетам, наглядная агитация и т. п.

Большинство авторов статей показывает значимость профилактики или интенсивного воздействия социума на начальную «зародышевую» стадию экстремизма в сети интернет. Для реализации этих процессов необходимо выявить феномен и описать его признаки. А. А. Затолокин прослеживает экстремизм как социальное заболевание и изучает его эпикриз.

На основе сопоставления методов профилактической медицины и методов борьбы с экстремизмом, академик И. А. Гундаров, описывает 3 подхода в противодействии социально значимым заболеваниям:

1 подход: «симптоматический» (нейтрализация симптомов);

2 подход: «патогенетический» (блокировка механизмов распространения);

3 подход: «этиологический» (устранение причины)» [7].

Опираясь на анализ схожести распространения эпидемии и нездоровой информации в сетях, мы определили начальную стадию экстремизма в сети интернет как сетевое деструктивное поведение далее.

Сетевое деструктивное поведение – это поведение субъекта, которым он отражает свои деструктивные интересы, фантазии, намерения, выражаемые и реализуемые с помощью возможностей интернета, и которое приобретает вирулентный характер. Под вирулентным понимается распространение деструктивного контента по сети одному и более пользователей.

К. В. Злоказов [8] приводит классификацию деструктивного поведения на интра-, интер- и метаперсональное. Интраперсональная деструкция направлена на самоизменение и самоповреждение, как физическое, так и психологическое. Интерперсональное деструктивное поведение связано с взаимодействием субъектов диалога, из которых один, агрессор, повышает свое самоуважение за счет другого, жертвы. Наконец, третий, метаперсональный вид деструктивного поведения связан с взаимодействием личности и социальной группы – либо чрезмерным слиянием, либо отрицанием социальной роли. Отрицание социальной роли заключается в противодействии правилам и устоям в семье, в рабочем коллективе, в гражданском обществе. Начиная от внутренней поддержки негативных общественных настроений и заканчивая участием в организованных акциях протеста, такое метаперсональное деструктивное поведение ведет к экстремизму.

О. В. Зеленина, П. Е. Суслонов [9] описали 10 признаков оценки информационного материала в интернете на предмет экстремистской направленности. Данные позиции коррелирует с Федеральным Законом № 114-ФЗ «О противодействии экстремистской деятельности» [10]. Эти признаки можно рассматривать как горизонтальную дизъюнктную классификацию. Каждый вариант деструктивного поведения можно отнести к одному из элементов такой классификации. В данной работе мы предлагаем шкалу ступеней деструкции, которая может сделать такую классификацию двумерной, дополнив каждый ее элемент оценкой от 1 до 7.

Векторов увеличения деструктивности три. Первый – переход от трансляции чужого мнения к собственным убеждениям. Второй – от разовой демонстрации протеста к постоянному ношению знаков и символов на себе. Третий – от поддержки деструктивной идеи в целом до организации мероприятий и сообществ, посвященных деструктивной борьбе. Также признаком повышения деструктивности является переход от невербальных символов к вербальным призывам, обезличенным и персональным.

Итак, перечислим эти ступени. Ступень 1: «Разочарование». Субъект страдает от отрицательных эмоций и транслирует свое состояние в сеть через репосты и лайки соответствующих постов, в которых отображаются в рисунках или слоганах негативные переживания, с намеком на ненормативную лексику.

Ступень 2: «Агрессивный протест». Субъект выкладывает собственные фотографии, выражающие протест через жесты, мимику, одежду, макияж и пр. Это виртуальное действие не имеет продолжения, оно является кратковременным отражением переживания субъекта.

Ступень 3: «Демонстративная агрессия». Субъект носит элемент или элементы знаков и символов протеста на себе: это может быть тату, пирсинг, стрижка и пр. В любом случае этот элемент имиджа является стабильным и демонстративным. Пока он не ведет агрессивную пропаганду деструктивных действий, но четко закрепляет свою принадлежность к некоторой деструктивно настроенной группе.

Ступень 4: «Невербальный призыв к общему протесту». Кричащий целостный облик: одежда, обувь, пирсинг, татуировки, имидж отображает роль – обращение общего внимания на себя. На этой ступени толкование протеста отдается наблюдателю, но интерес у наблюдателя и эмоции гарантированы.

Ступень 5: «Поиск всех, кто имеет те же чувства». Навязывание, провокационное запугивание, объединение на фоне единства в негативной мотивации с целью поиска единомышленников. Появляется воздействие словом: текстовые призывы, размышления, идет привлечение внимания и присоединения.

Ступень 6: «Делай как я в виртуальности». Предложение поведения и образа жизни с негативным контекстом, конкретные рецепты игр с сознанием, пропаганда: «элитность инакомыслия», ценность провокационного или деструктивного поведения.

Ступень 7: «Делай как я в реальности». Призыв к акциям протеста с конкретным указанием места и времени, убеждение вступления в ряды радикальных группировок, а также призыв к посещению сквотов, приему наркотиков, коллективным самоубийствам.

Перечисленные ступени деструктивного сетевого поведения можно соотнести с предложенными екатеринбургскими учеными [9] признаками оценки материалов в интернете, которые носят экстремистскую направленность: 1. Насильственное изменение основ конституционного строя и нарушение целостности РФ – следует обращать внимание не на цели, а на методы, с помощью которых предлагается их осуществить. 2. Публичное оправдание терроризма и иная террористическая деятельность. 3. Возбуждение социальной, расовой, национальной или религиозной розни. 4. Пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии. 5. Нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии. 6. Пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения. 7. Публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения. 8. Публичное заведомо ложное обвинение лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, в совершении им в период исполнения своих должностных обязанностей деяний, указанных в настоящей статье и являющихся преступлением. Клеветой является распространение сведений о лице, заведомо не соответствующих действительности и задевающих его честь и достоинство. 9. Организация и подготовка указанных деяний, а также подстрекательство к их осуществлению. 10. Финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг.

Связь признаков экстремистской информации в интернете и ступенями деструктивного сетевого поведения приведена в таблице.

ТАБЛИЦА. Соотнесение признаков информационной экстремистской направленности и ступеней деструктивного сетевого поведения

Признак	1	2	3	4	5	6	7	8	9	10
Ступени	1-7	2-6	5-7	5-7	6-7	2-7	6-7	5-7	6-7	6-7

Таким образом, мы видим, что сетевое деструктивное поведение на своих верхних ступенях имеет выраженные признаки информационной экстремистской направленности. Начальные ступени сетевого деструктивного поведения могут быть зафиксированы системой воспитательной работы в образовательных учреждениях и станут основой для пропедевтики и профилактики распространения экстремистской информации, коррекции поведения молодежи в сетях и в социальной среде.

Работа выполнена при финансовой поддержке Гранта РФФИ (проект РФФИ мк 18-29-22034) в СПИИРАН.

Список используемых источников

1. Диль В. А. Современный экстремизм: тенденции развития и социокультурные модификации // Вестн. Том. гос. ун-та. 2011. № 344. С. 46–49.

2. Федеральный закон Российской Федерации от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму», ст. 3. URL: http://pravo.gov.ru/proxy/ips/?docbody= &nd= 10210519

3. Российский энциклопедический словарь / Гл. ред. А. М. Прохоров. М.: Научное изд-во «Большая Российская энциклопедия», 2000. Т. 2. С. 1832.

4. Awan, I. Cyber-Extremism: Isis and the Power of Social Media // Society. 2017; 54(2):138.

5. Затолокин А. А. Экстремизм как социальная болезнь // Общество и право. 2014. № 3. С. 229–232.

6. Лашин Р. Л., Чурилов С. А. Противодействие экстремизму и терроризму в сети интернет и образовательной среде // ОБЗОР.НЦПТИ. 2015. № 7. С. 34–39.

7. Гундаров И. А. Демографическая катастрофа в России: причины н пути преодоления / Почему вымирают русские. М.: Эксмо-Пресс. 2004. С. 48–57.

8. Злоказов К. В. Деструктивное поведение в различных контекстах его проявления // Вестник Удмуртского университета. Серия «Философия. Психология. Педагогика». 2016. Т. 26. № 4. С. 67–73.

9. Зеленина О. В., Суслонов П. Е. Методика выявления признаков экстремизма. Процессуальные исследования (экспертизы) аудио-, видео- и печатных материалов. Научно-методическое пособие Екатеринбург. Уральский юридический институт МВД России. 2009. URL: http://do.gendocs.ru/ docs/index-295684.html

10. Федеральный закон Российской Федерации от 23.11.2015 г. N 314-ФЗ «О противодействии экстремистской деятельности». URL: http://pravo.gov.ru/proxy/ips/ ?docbody=&nd=102079221.

УДК 004.946
ГРНТИ 28.17.33

ДЕТЕКТОРЫ МАРКЕРОВ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

Г. В. Верхова, М. М. Котельников

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Одной из важнейших функций в технологии дополненной реальности является обнаружение маркера дополненной реальности. Такое обнаружение выполняется по ключевым точкам маркера дополненной реальности. Рассмотрены основные детекторы маркеров дополненной реальности и алгоритмы, применяемые в данных детекторах. Приведены требования, предъявляемые к ключевым точкам маркеров дополненной реальности. Рассмотрены алгоритмы детекторов Моравеца, Харриса и Стефана, а также FAST и SURF детекторов. Указаны особенности данных детекторов, их достоинства и недостатки.

детектор маркера дополненной реальности, маркер дополненной реальности, ключевая точка дополненной реальности, алгоритмы обнаружения ключевых точек, детектор Моравеца, детектор Харриса и Стефана, детектор FAST, детектор SURF.

Одной из важнейших функций в технологии дополненной реальности является обнаружение маркера дополненной реальности [1]. Ключевая точка маркера дополненной реальности – это такая точка, расположенная на изображении (на объекте физической реальности), имеющая следующие свойства:

– имеет ясное, математически обоснованное определение;

– имеет четко определенное положение в пространстве изображения;

– обладает устойчивостью при локальных и глобальных изменениях в области изображения (изменения освещенности или яркости);

– окрестность одной ключевой точки изображения можно однозначно обнаружить в окрестности некоторой другой ключевой точки.

Рассмотрим типовые алгоритмы для определения ключевых точек на изображении.

Детектор Моравеца. На изображении существует большое количество ключевых точек, одним из разновидностей которых являются углы на изображении. Это объясняется тем, что углы могут быть однозначно сопоставимы на паре изображений. Для поиска расположения углов используются локальные детекторы, на вход которых подается изображение в черно-белом виде. Результатом работы этих детекторов является матрица, которая

определяет вероятность нахождения угла в определенных пикселях изображения. Далее матрица обрабатывается, с целью отсечения пикселей, обладающих меньшей вероятностью, которая задается некоторым порогом. Точки, которые остались после обработки называются особыми.

Детектор Моравеца является один из самых простых детекторов для углов. В соответствии с этим методом необходимо вычислять с помощью смещения маленького квадратного окна W с центром в координатах (x, y), изменение интенсивности пикселей на координатах (x, y). Смещение данного окна выполняется в восьми направлениях (по горизонтали 2 задается 3x5, 5x5, 9x9 пикселей. При выполнении детектирования выполняются следующие шаги:

Шаг 1. Для всех направлений смещения

$$(u,v) \in \{(1,0),(1,1),(0,1),(-1,1),(-1,0),(-1,-1),(0,-1),(1,-1)\}$$

по (1):

$$V_{x,y}(x,y) = \sum_{a,b \in W} \left(I(x+u+a, y+v+b) - I(x+a, Y+b)\right)^2, \quad (1)$$

где $I(x, y)$ – интенсивность пикселя у которого координаты (x, y) в базовом изображении, вычисляется изменение интенсивности.

Шаг 2. При помощи вычисления оценочной функции (2)

$$C(x,y) = min\{V_{u,v}(x,y)\} \quad (2)$$

создается карта, которая содержит вероятности присутствия углов во всех пикселях изображения: находится направление с наименьшим изменением интенсивности, так как у угла должны быть смежные ребра. Отбрасываются пиксели, с меньшим пороговым значением оценочной функции

Повторяющиеся углы отсекаются с помощью процедуры Non-Maximal-Suppression. В результате все элементы карты не равные нулю, будут соответствовать углам, которые расположены на изображении. Основным недостатком такого детектора является его неизотропность, заключающаяся в том, что если присутствует ребро, которое не находится в направлении соседей (горизонтальное, вертикальное или диагональное), то наименьший суммой квадратов разностей будет большой и угол будет неправильно выбран в качестве точки интереса.

Детектор Харриса и Стефана основан на детекторе Моравеца. Основным его преимуществом является анизотропность по всем направлениям. По некоторым направлениям, которые задаются по условию, вычисляются производные, а функция интенсивности раскладывается в ряд Тейлора.

$$I(x+u+a, y+v+b) \sim I(x+a, y+b) + u\frac{\partial I}{\partial x} + v\frac{\partial I}{\partial y} = I(x+a, y+b) + \frac{\partial I}{\partial x}\frac{\partial I}{\partial y}\begin{bmatrix} u \\ v \end{bmatrix}. \quad (3)$$

Исходя из этого уравнения, изменение интенсивности $V_{u,v}(x, y)$ в каждом пикселе можно представить в виде (4):

$$\begin{aligned} & V_{x,y}(x, y) = \\ & = \sum_{a,b \in W} \left(\frac{\partial I}{\partial x}\frac{\partial I}{\partial y}\begin{bmatrix} u \\ v \end{bmatrix} \right)^2 = \sum_{a,b \in W} [u\, v] \begin{bmatrix} \frac{\partial I}{\partial x} \\ \frac{\partial I}{\partial y} \end{bmatrix} \frac{\partial I}{\partial x}\frac{\partial I}{\partial y}\begin{bmatrix} u \\ v \end{bmatrix} = \\ & = [u\, v] \left(\sum_{a,b \in W} [u\, v] \begin{bmatrix} \frac{\partial I}{\partial x} \\ \frac{\partial I}{\partial y} \end{bmatrix} \frac{\partial I}{\partial x}\frac{\partial I}{\partial y} \right) \begin{bmatrix} u \\ v \end{bmatrix} = \\ & = [u\, v] A_{u,v}(x, y) \begin{bmatrix} u \\ v \end{bmatrix}. \end{aligned} \quad (4)$$

В автокорреляционной матрице Харриса $A_{u,v}(x, y)$ выбирается взвешенная свертка производных с весовыми коэффициентами, соответствующими окну Гаусса. Такое окно имеет размер 3x3 пикселя и коэффициенты 0,04, 0,12, 0,04, 0,12, 0,36, 0,12,0,04. Матрица Харриса является полуопределенной положительной матрицей. Точки изображения можно классифицировать на точки и углы, благодаря вычислению собственных значений матрицы Харриса:

– если собственные значения автокорреляционной матрицы довольно большие, то есть незначительный сдвиг окна ведет к большим изменениям интенсивности, то пиксель принимается за угол;

– если одно собственное значение существенно превосходит другое, это значит, что окно сместилось перпендикулярно по отношению к выступу, следовательно, пиксель принадлежит ребру;

– если собственные числа равны нулю или очень близки к нему, тогда в пикселе не содержатся ни ребра, ни углы.

Вычисление свертки с Гауссовским ядром делает данный метод более трудоемкий, по сравнению с методом Моравеца. Также на результаты данного метода существенно влияет шум, для минимизации которого требуется увеличивать окно Гаусса, что ведет к повышению вычислительной трудоемкости.

Алгоритм Харриса и Стефана является анизотропным в вертикальном и горизонтальном направлениях, это связано с тем, что автокорреляционная матрица только в этих направлениях имеет первые производные. По сравнению с детектором Моравеца, этот метод обладает свойством инвариантности относительно поворотов и за счет введения свертки с весовыми коэффициентами Гаусса, количество ошибок нахождения углов не так уж велико. При изменении масштаба изображения результаты обнаружения существенным образом меняются.

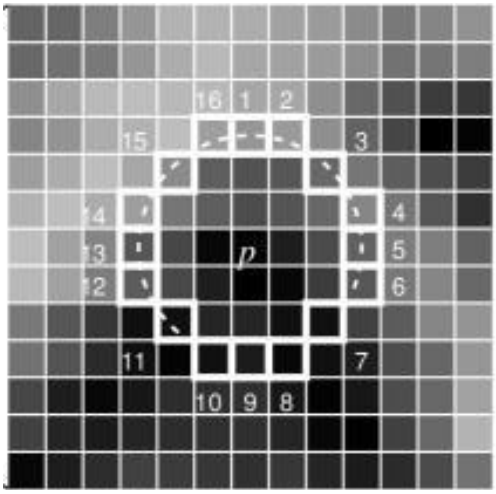


Рисунок. Принцип действия детектора FAST

*Детектор FAST***.** Все перечисленные детекторы для поиска ключевых точек изображения, в частности их углов, работают с пикселями исходного изображения напрямую. Другим подходом – является использование технологий машинного обучения. Такая технология используется для обучения классификатора точек на совокупности изображений. Данный детектор строит дерево решений для классификации пикселей.

Для каждого пикселя некоторого изображения объектом рассмотрения является окружность, которая состоит из 16-ти пикселей окрестности, центром которой является интересующая нас точка (рис.).

Каждый пиксель, который входит в состав окрестности по отношению к центральному пикселю может быть в одном из 3-х состояний, которое определяется по (5):4

$$S_{p\to x}=\begin{cases} d,\ I_x \le I_p - t \ \ |(\text{темнее}) \\ s,\ I_p - t < I_x < I_p + t |(\text{подобный}) \\ b,\ I_p + t \le I_x \ |(\text{светлее}) \end{cases} \qquad (5)$$

Детектор SURF. Детектирование особых точек выполняется на базе матрицы Гессе. С помощью применения Гессиана достигается инвариантность относительно изменения типа «поворот», но не относительно преобразования масштаба, ввиду чего в SURF используются фильтры различного масштаба для расчета Гессиана. Допустим, что изображение задано матрицей интенсивностей I, рассматриваемый пиксель обозначим $X=(x,y)$, а ъ σ – масштаб фильтра. Тогда матрицу Гессе можно представить в виде (6):

$$H(X,\sigma)=\begin{bmatrix} L_{xx}(X,\sigma) & L_{xy}(X,\sigma) \\ L_{xy}(X,\sigma) & L_{yy}(X,\sigma) \end{bmatrix}, \quad (6)$$

где $L_{xx}(X,\sigma)L_{xy}(X,\sigma)L_{xy}(X,\sigma)L_{yy}(X,\sigma)$ – свертки аппроксимации второй производной ядра Гаусса с изображением I. Экстремум определителя матрицы Гессе достигается в точках с максимальным изменением градиента яркости. Таким образом, SURF проходится фильтром с ядром Гаусса по всему изображению и обнаруживает точки с самым большим значением определителя матрицы Гессе. Следует подчеркнуть тот факт, что такой проход обеспечивает обнаружение светлых пятен на темном фоне и наоборот.

Затем для всех найденных ключевых точек вычисляется ориентация – это направление преобладания перепада яркости. Термин «ориентация» очень близок к понятию градиента, но для нахождения ориентации ключевой точки используется фильтр Хаара. На базе имеющейся информации создаются дескрипторы для всех ключевых точек:

– вокруг точки выполняется построение квадратной окрестности размером 20s, где s – масштаб, на котором получен определитель матрицы Гессе с наибольшим значением.

– полученная в результате квадратная область делится на блоки, и в итоге область будет разделена на 4x4 региона.

– для всех блоков производится расчет более простых признаков. И как итог, образуется вектор, который содержит 4 элемента: 2 – сумма модулей точечных градиентов, 2 – это суммарный градиент по квадранту.

– дескриптор создается с помощью склеивания взвешенных описаний градиента для шестнадцати квадрантов вокруг ключевой точки. Выполняется взвешивание компонентов дескриптора на коэффициенты ядра Гаусса. Веса нужны для лучшей устойчивости к шумам в дальних точках.

– к дескриптору добавляется след матрицы Гессе. Эти элементы нужны для распознавания светлых и темных пятен. Для темных точек на светлом фоне след положительный, а для светлых на темном – отрицателен.

Алгоритм SURF применяется для обнаружения объектов. Но дескриптор не использует данных об объектах. Метод SURF плохо работает с объектами простой формы, т. к. изображение рассматривается как единое целое и происходит выделение особенностей всего изображения.

Рассмотренные детекторы широко применяются в различных приложениях дополненной реальности, включая системы и среды электронного обучения [2, 3].

Список используемых источников

1. Верхова Г. В., Акимов С. В., Котельников М. М. Обобщенная модель системы дополненной реальности // Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации. Распознавание – 2018. Сборник материалов XIV международной научно-технической конференции. 2018. С. 75–77.

2. Morey, S., Tinnell, J. Augmented Reality: Innovative Perspectives across Art, Industry, and Academia. Parlor Press, 2016. 368 p.

3. Papagiannis, H. Augmented Human: How Technology Is Shaping the New Reality. O'Reilly Media, 2017. 156 p.

УДК 65.011.56
ГРНТИ 50.47.02

АДАПТИВНЫЕ СИСТЕМЫ

Г. В. Верхова, Е. А. Макаренко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Внешние возмущения могут привести не только к изменению координат, но и параметров системы. Изменения параметров, выходящие за предусмотренные границы, может привести к ошибкам, ухудшению функционирования или полной потере работоспособности системы. В данной статье рассмотрено понятие адаптивных систем, причины применения принципов адаптации. Рассмотрено каким образом осуществляется адаптация, а также недостатки применения адаптивных систем.

адаптивные системы, проблемы адаптации, свойства адаптации, реализация адаптивного управления.

Существует большое количество объектов, для которых необходимо или целесообразно применять принципы адаптации. Количество таких объектов растёт с развитием техники.

Причины применения принципов адаптации можно объединить в две группы: изменчивость и сложность характеристик объектов и внешней среды и рост требований к точным и технико-экономическим характеристикам систем.

Адаптация – это процесс изменения параметров, структуры систем или управляющих воздействий на основе информации, получаемой во время управления, с целью достижения определенного (оптимального) качества управления при начальной неопределенности и/или изменяющихся условиях работы.

Отличие адаптивных систем от оптимальных состоит в том, что в то время, как в оптимальных системах показатель качества обеспечивается при определенных параметрах объекта, в адаптивных системах – при различных параметрах за счет действия дополнительных элементов адаптации.

Адаптивная (приспосабливающиеся) система – это система, которые автоматически приспосабливаются к изменениям внешней среды. Любая система с обратной связью по существу автоматически приспосабливается к изменениям внешней среды, но именно адаптивная система может приспосабливаться к непредвиденным изменениям.

Для повышения точности системы необходимо менять настройки корректирующих звеньев системы в соответствии с изменениями внешней среды. В адаптивных системах этот процесс автоматически. Путем изменения структуры и параметров управляющего устройства такие системы обеспечивают необходимое качество управления. Определить качество управления системы возможно с помощью определенных параметров, к примеру, показателя точности работы или качества переходного процесса, производительность системы и др. Структурная схема самонастраивающейся системы управления представлена на рис. 1.

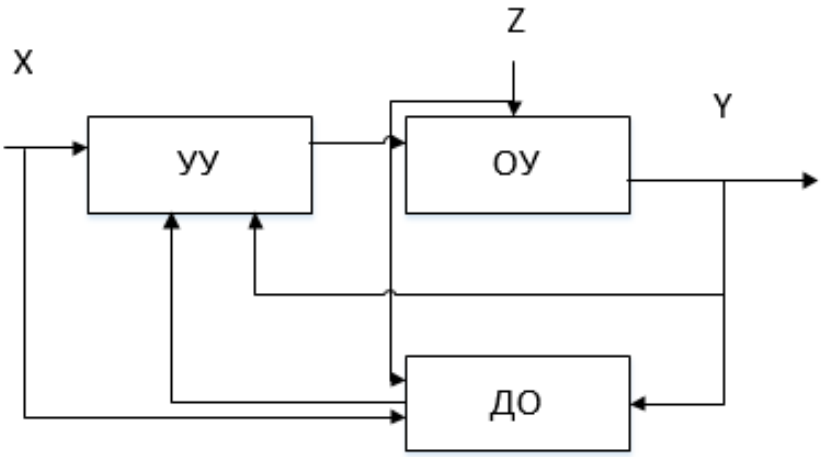


Рис. 1. Структурная схема самонастраивающейся системы управления

На рис. 1 обозначение УУ – управляющее устройство, ОУ – объект управления и ДО – датчик отклонений.

В настоящее время реализация адаптивного управления осуществляется на основе идентификации объекта управления с последующим решением задачи параметров ПИД-регулятора. Недостатками такого подхода является сложность реализации процедуры идентификации и ограниченные возможности изменения динамических свойств. Помимо настройки параметров регулятора, можно так же путем включения в состав устройства устройств управления, который позволит обеспечить необходимое качество систем автоматического регулирования (САР).

Адаптация осуществляется таким образом, что параметры объекта управления не меняются и соответствуют настройке, предшествующей запуску системы. В процессе работы меняется коэффициент передачи корректора или создаваемый им фазовый сдвиг. В качестве корректирующего устройства используется двухканальное псевдолинейное, обеспечивающее независимую корректировку амплитудно-частотной (АЧХ) и фазо-частотной (ФЧХ) характеристик. Корректоры, используемые для изменения динамических свойств САР, можно разделить на линейные, нелинейные и псевдолинейные.

Недостатком линейных корректоров является то, что изменение параметров влияет как на АЧХ, так и на ФЧХ. В этом случае, добиваясь необходимой ФЧХ можно получить АЧХ, возрастающую в области средних и высоких частот, что приводит к уменьшению запаса устойчивости САР. И аналогично имея необходимую АЧХ, можно получить ФЧХ разомкнутой системы, принимающую отрицательное значение, что так же снижает запас устойчивости.

В связи с этим, результаты исследований показали, что процедура адаптации линейных корректоров возможна лишь при ограниченных по диапазону и характеру изменениях параметров объекта управления. Проблемой применения нелинейных корректоров является учёт зависимости частотных характеристик от амплитуды гармонических колебаний входного сигнала.

Применение адаптивного псевдолинейного корректора позволяет получить требуемые амплитудные и фазовые характеристики. Обычно эти устройства имеют два канала, амплитудный и фазовый, которые настраиваются независимо друг от друга, а та же частотные характеристики псевдолинейных корректирующих устройств не зависят от амплитуды гармонических колебаний входного сигнала. В связи с этим наиболее эффективными для реализации адаптивных систем будут псевдолинейные корректирующие устройства. Такой комплекс устройств обеспечит требуемое качество в широком диапазоне, а также позволит повысить формирование управляющего устройства и повысить качество управления.

Как правило, такие системы обладают некоторыми или всеми перечисленными ниже свойствами:

1. Они могут адаптироваться (самооптимизироваться) при изменении (нестационарном) условий окружающей среды и требований к системе.

2. Они могут обучаться для осуществления заданного вида фильтрации и выполнения задачи принятия решения. Системы с такими свойствами можно автоматически синтезировать через обучение. Адаптивные системы можно в некотором смысле «запрограммировать» процессом обучения.

3. Они не требуют тщательно разработанных методов синтеза, обычно необходимых для неадаптивных систем. Наоборот, их можно считать «самоорганизующимися».

4. Они могут экстраполировать модель поведения для функционирования в новых условиях после обучения на конечном и часто небольшом числе обучающих сигналов или ситуаций.

5. Они могут в некоторой степени восстанавливаться, т. е. адаптироваться к определяемым внутренним дефектам.

6. Их можно рассматривать как нелинейные системы с изменяющимися во времени параметрами.

7. Их сложнее анализировать, чем неадаптивные системы, но они позволяют значительно увеличить область функционирования системы, когда параметры входного сигнала не известны или изменяются во времени.

Беспоисковые системы регулируют управляющие параметры на основе сравнения параметров заданной эталонной модели и фактических выходных параметров. Структурная схема беспоисковой системы представлен на рис. 2.

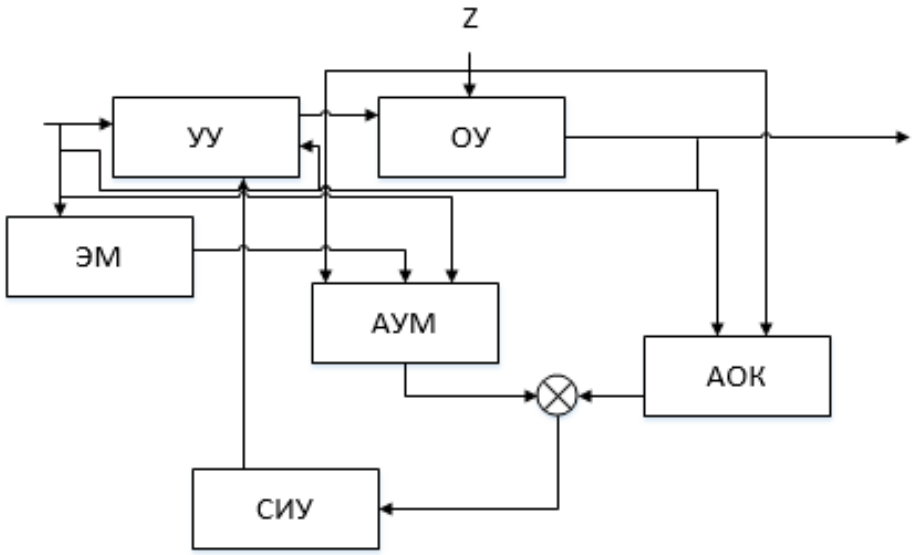


Рис. 2. Структурная схема беспоисковой системы.

На рис. 2 обозначение УУ – управляющее устройство, ОУ – объект управления, ЭМ – эталонная модель, АУМ – анализатор качества управления эталонной одели, АОК – анализатор основного контура системы и СИУ – самонастраивающееся исполнительное устройство.

Достигнутый за последнее время прогресс в разработке и производстве микросхем привел к созданию очень компактных, экономичных и надежных устройств обработки сигналов, конкурирующих с биологическими нейронными системами по размерам и, очевидно, превосходящих биологические системы по быстродействию.

В результате этого значительно расширилась область их применения во всех видах цифровой обработки сигналов, в том числе адаптивной обработки.

В настоящее время адаптивные системы применяются в таких областях, как связь, радиолокация, гидролокация, сейсмология, проектирование механических систем, навигация и биомедицинская электроника.

Адаптивное моделирование используется при проектировании и диагностике электронных и механических систем.

Список используемых источников

1. Яковлев В. Б. Адаптивные системы автоматического управления Л.: Изд-во Ленингр. ун-та, 1984. 204 с.
2. Александров А. Г. Оптимальные и адаптивные системы М.: 2003. 78 с.
3. Жиров М. В., Макаров В. В., Солдатов В. В. Идентификация и адаптивное управление технологическими процессами с нестационарными параметрами М.: 2011. 208 с.
4. Бобцов А. А., Никифоров В. О., Пыркин А. А. Адаптивное управление возмущенными системами СПб.: Университет ИТМО, 2015. 126 с.

УДК 004.056.5
ГРНТИ 20.53.19

СПОСОБ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТ АНАЛИЗА НА ОСНОВЕ ПРИМЕНЕНИЯ ИНТЕРПРЕТАТОРОВ БАЙТ-КОДА

А. Н. Вихарев, Д. О. Маркин

Академия Федеральной службы охраны Российской Федерации

В статье описан способ защиты программного обеспечения от анализа на основе применения виртуальных машин с неивестной архитектурой и алфавитом байт-кода. Представлены схемы формирования байт-кода и кода виртуальной машины. Обоснована применимость обфускации на основе виртуальных машин с неизвестной архитектурой и алфавитом байт-кода. Предложен способ их применения для защиты программного обеспечения от анализа.

виртуальная машина, обфускация, интерпретатор, байт-код, реверс-инжиниринг, дизассемблирование, отладка.

Повсеместное внедрение информационных технологий, средств автоматизации и автоматизированных систем в повседневную жизнь, развитие цифровой экономики значительно повышает роль программного обеспечения в современной экономике. В связи с этим недостаточная защищенность программного обеспечения от анализа, нарушения его работоспособности,

модификации и других угроз может привести к серьезным неблагоприятным последствиям различного характера. Таким образом, проблема обеспечения защищенности программного обеспечения (ПО) является актуальной и требует применения новых методов и средств, способных обеспечить требуемый уровень защиты в современных условиях.

Проблема защиты программных реализаций на основе применения технологий виртуализации и других методов затрагивалась в научных трудах В. Ю. Аранова [3], А. С. Петрова [1, 2], а также В. А. Захарова, П. Д. Зегжды, В. П. Бойко, В. С. Заборовского, Н. Н. Кузюрина, А. В. Шокурова, Р. И. Подловченко, В. П. Иванникова, К. Сомборсона, Д. Викстромома и других. В указанных работах отмечалась необходимость защиты программных реализаций от технологий обратной разработки, основанных, в том числе на методах статического и динамического анализа ПО.

Основными задачами защиты программных реализаций являются:

- Недопущение несанкционированного изменения алгоритма поведения программы.
- Защита обрабатываемых данных от нелегитимного пользователя.
- Обеспечение защиты программного обеспечения от несанкционированного копирования.

Под защитой авторы понимают такой метод выполнения программы, при котором невозможно выявить процесс обработки данных [1, 2] и восстановление алгоритма работы программы, либо максимально его затруднить решение данных задач.

Применяемые в настоящее время методы защиты условно делятся на организационно-инфраструктурные и функциональные. Первые направлены на формирование доверенной вычислительной среды (например, операционные системы Android, iOS используют для этих целей изолированную программную среду на основе встроенных служб сертификации и лежащих в их основе несимметричных криптосистем), тогда как вторые – на блокирование действий, разрушающих существующие средства защиты программ от копирования и обратного проектирования.

Ряд функциональных методов защиты основан на применении алгоритмов и методов преобразования исполняемого кода прикладных программ к виду, затрудняющему анализ алгоритмов (обфускации). При этом обфускации может подвергаться как исходный текст программы и, соответственно, получаемый из него машинный код, так и ее алгоритм (поток управления). Подобные запутывающие преобразования обладают специфическими свойствами, существенно затрудняющими применение средств анализа данных [3] и, соответственно, восстановление алгоритма работы анализируемого приложения.

К недостаткам применения методов обфускации можно отнести следующие:

− код программы после обработки обфускатором может стать более зависимым от программно-аппаратной платформы или компилятора;

− обфускатор затрудняет анализ кода с одной стороны для исследователя, с другой стороны – для разработчика; это приводит к тому, что на этапе отладки ПО систему защиты приходится отключать;

− ни один из существующих *известных* обфускаторов не гарантирует достаточного уровня сложности декомпиляции (деобфускации) и не обеспечивает безопасности, сопоставимой с уровнем современных криптографических алгоритмов;

− в обфускаторах могут содержаться ошибки, не учитывающие некоторые особенности модели приложения, обфускацию которого они выполняют, поэтому существует ненулевая вероятность того, что прошедший через обфускатор код потеряет работоспособность (чем сложнее разрабатываемая программа, тем больше эта вероятность).

Одним из эффективных способов обфускации является виртуализация кода, основанная на технологиях виртуальных машины. Применение такого подхода позволяет преобразовать машинные команды исходного приложения в произвольный, как правило, неизвестный никому, кроме разработчика, байт-код, которые будет выполняться на соответствующей ему (байт-коду) виртуальной машине (интерпретатору), который, в свою очередь, будет входить в состав защищаемого приложения.

Для исполнения защищаемого программного кода на виртуальной машине он должен быть преобразован в байт-код, который может быть выполнен данной виртуальной машиной. Схема формирования байт-кода с учетом его алфавита и архитектуры виртуальной машины представлена на рис. 1.

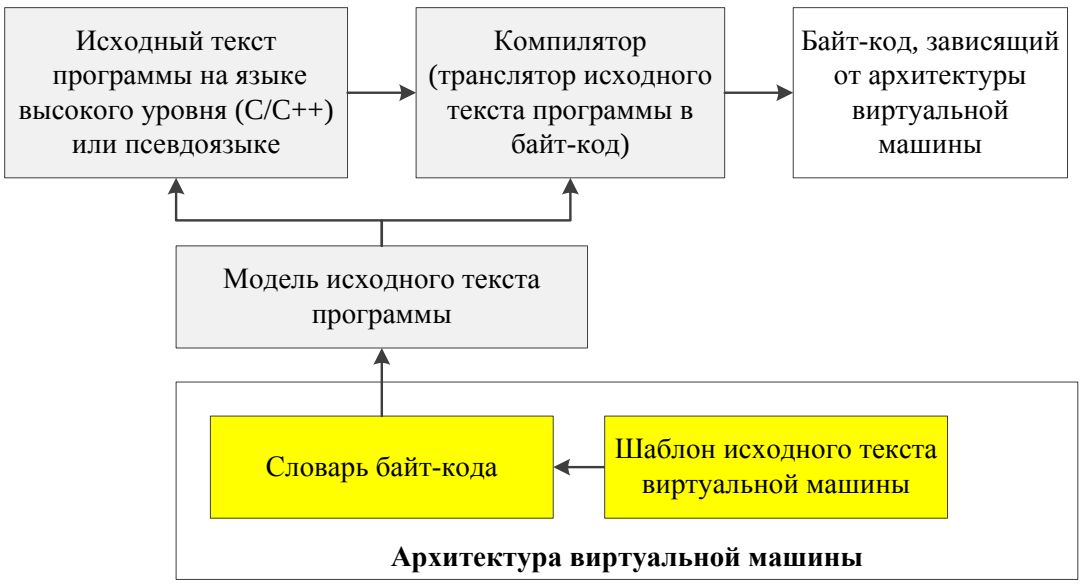


Рис. 1. Схема формирования байт-кода виртуальной машиной

В свою очередь, исполняемый машинный код виртуальной машины также должен быть сформирован с учетом словаря используемого словаря байт-кода, а также избранной архитектуры виртуальной машины. С учетом изложенного схема формирования виртуальной машины будет выглядеть так, как представлено на рис. 2.

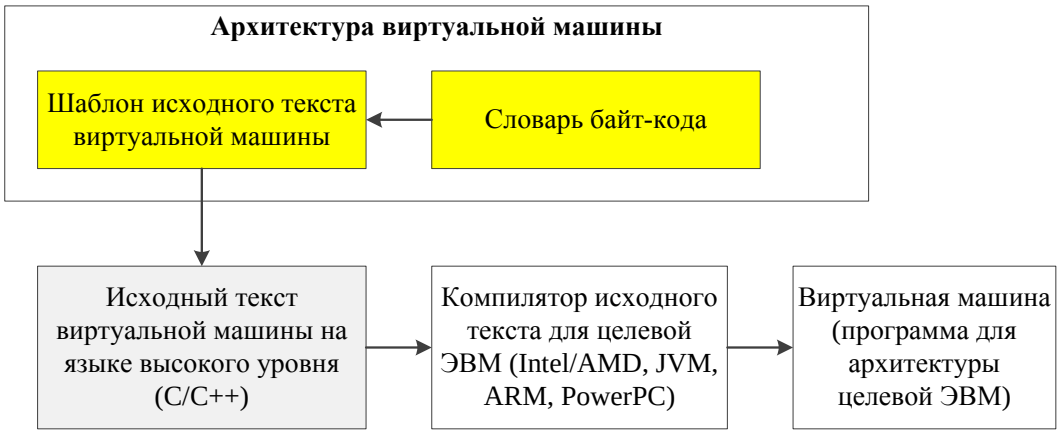


Рис. 2. Схема формирования виртуальной машиной

В настоящее время известно достаточно большое количество различных виртуальных машин, применяемых, как правило, в целях повышения совместимости между различными аппаратными архитектурами. Примерами виртуальных машин являются: VMware, VirtualBox, QEMU, Nox, Bochs, JVM, Colinux, AlphaVM-Free(-Pro), CHARON-AXP(-VAX), Denali, DOSBox, DOSEMU, Icore virtual accounts, Jail, KVM, OpenVZ, Parallels Workstation, PearPC, Virtual PC, Hyper-V, Virtuozzo, VMware ESX Server, SimNow, Solaris Zones, Xen, z/VM.

Процесс обфускации может быть условно разделен на несколько этапов. Схема процесса представлена на рисунке 3.

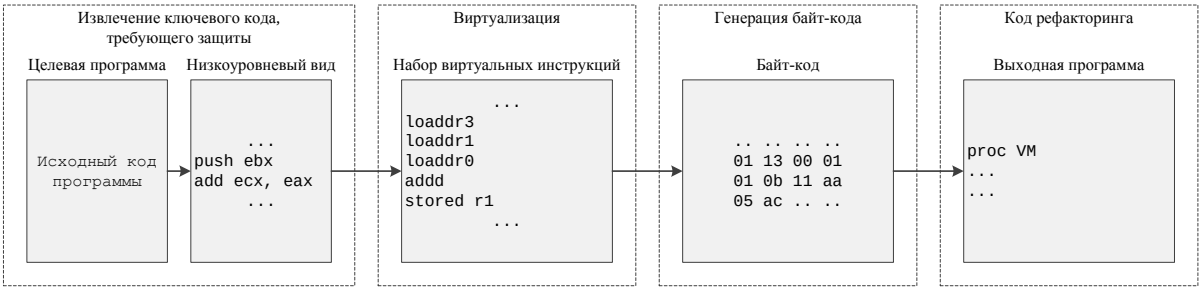


Рис. 3. Процессы преобразований кода

Как правило, формирование байт-кода осуществляется в виде преобразования машинных команд в байт-код, однако возможна и трансляция исходного текста на языке высокого уровня или псевдоязыке сразу в байт-код.

Порядок преобразования защищаемого кода программы в байт-код следующий:

− сегмент кода, который должен быть защищен, извлекается скомпилированного двоичного файла, который был скомпонован в код сборки (набор машинных команд для архитектуры целевой ЭВМ);

− машинный код программы транслируется в виртуальные команды, то есть машинное независимое промежуточное представление, используемое виртуальными машинами;

− переведенные виртуальные инструкции являясь функционально эквивалентными исходному коду программы, кодируются в соответствии с принятым алфавитом байт-кода.

В процессе исполнения защищаемого приложения сформированный байт-код передается как входные данные модулю приложения – виртуальной машине, которая его и обрабатывает.

Сущность защиты программного кода на основе обфускации с использованием виртуальных машин заключается в том, чтобы заставить исследователя перейти от анализа машинных инструкций известной архитектуры (например, x86) к незнакомому набору виртуальных команд, которые увеличат сложность и, соответственно, затрачиваемое время на анализ защиты.

Для того, чтобы преодолеть защитные механизмы, исполняемые встроенной в приложение виртуальной машиной как инструкции байт-кода, необходимо решить следующие задачи:

1) проанализировать работу компонентов интерпретатора виртуальной машины:

− выделить машинные коды инструкций байт-кода;

− определить фактические инструкции, исполняемые при выполнении обнаруженных инструкций байт-кода;

− выделить семантику инструкций байт-кода на основе анализа фактически исполняемых машинных инструкций;

− восстановить логику работы целевого кода (алгоритм).

Полученная информация об исследуемом приложении позволить исследователю либо разработать эквивалентное приложение, либо модифицировать исследуемое, внедрив необходимый функционал, либо убрать ненужный.

С учетом того, что архитектура виртуальной машины и алфавит инструкций байт-кода может повторяться в иных реализациях защитных механизмов в других приложениях, то полученную информацию о них исследователь может использовать повторно. Исходя из этого, при разработке виртуальной машины и выборе кода инструкций байт-кода целесообразно также использовать механизмы обфускации, например, формируя коды команд псевдослучайным образом.

Список используемых источников

1. Петров А. С., Петров А. А. Методы защиты программного кода // Системы обработки информации. 2010. Выпуск 3 (84). С. 68–71.

2. Петров А. С., Петров А. А. Технология защиты программного кода посредством применения виртуальной машины // Вестник ВНУ. 2009. № 9 (103), часть 1. С. 117–122.

3. Аранов В. Ю. Метод и средства защиты исполняемого программного кода от динамического и статического анализа : автореф. дис. … канд. техн. наук : 05.13.19 / Аранов Владислав Юрьевич. Санкт-Петербург, 2014. 18 с.

4. Kuang, Kaiyuan; Tang, Zhanyong; Gong, Xiaoqing; Fang, Dingyi; Chen, Xiaojiang; Wang, Zheng Enhanced virtual-machine-based code obfuscation security through dynamic bytecode scheduling // Computers & Security. 2018. № 74. Pp. 202–220.

УДК 004.05
ГРНТИ 49.27.01

ЗАЩИТА ИНФОРМАЦИИ В ПЕРСПЕКТИВНЫХ СЕТЯХ РАДИОСВЯЗИ НА ОСНОВЕ ВРЕМЕННОЙ МЕТКИ

М. А. Власенко, В. И. Дмитриев, Д. А. Иванов, Ш. В. Мамаджанова, Е. А. Хохлачева

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Сегодня проблема защиты информации от несанкционированного доступа является как никогда актуальной. Это связано с огромными постоянно растущим числом компьютерных атак ежедневно, учащением вспышек вредоносного ПО, увеличением количества атак, спонсируемых государствами, требованиями наивысшей защищённости объектов военного назначения для сохранения в секрете информации, содержащей военную тайну.

хеширование, временная метка, программа, интерфейс.

Хеширование – преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом. Функция, воплощающая алгоритм и выполняющая преобразование, называется «хеш-функцией» или «функцией свёртки». Исходные данные называются входным массивом, «ключом» или «сообщением». Результат преобразования (выходные данные) называется «хешем», «хеш-кодом», «хеш-суммой», «сводкой сообщения» [1].

«Временная метка» есть ни что иное, как добавление текущего времени в качестве параметра для функции хеширования блока данных. Таким обра-

зом, значение функции, вычисленное к определённый момент времени будет отличаться от значения при тех же входных данных в другой момент времени. При этом на практике будет уже невозможно получить то же самое значение хеш-функции, используя данные того же самого блока в следующие моменты времени

Алгоритм выполнения программы последовательно осуществляет:

Этап 1. Пользователь формирует новые блоки сообщений;

Этап 2. По нажатию кнопки «Добавить блок» все сообщений добавляются в новый блок, который привязывается к предыдущему, храня его значение хеш-функции;

Этап 3. При добавлении нового блока формируется его собственное хеш-значение, которое, оно также записывается в поле каждого блока;

Этап 4. Пользователь изменяет сообщение в существующем блоке или добавляет к нему новое, это приводит к изменению хеш-значение и, как следствие, нарушению последовательности, что видно при проверке (по нажатию кнопки «Проверить корректность») [2]. Пример простой программы, выполняющей хеширование, показан на рис. 1.

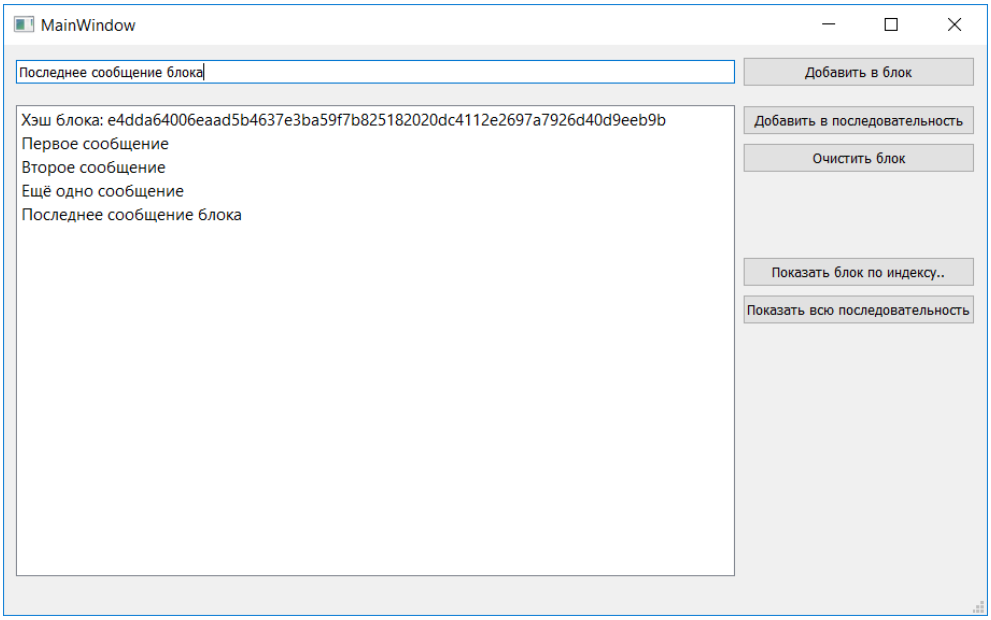


Рис. 1. Реализация простой программы хеширования

Для реализации графической составляющей была выбрана библиотека *Qt*, предоставляющая кроссплатформенные решения для построения пользовательских графических интерфейсов. Внешний вид среды *QtDesigner* показан на рис. 2, 3.

Интерфейс приложения позволяет пользователю добавлять новые данные (сообщения) в блоки, редактировать данные блоки, добавлять их к об-

щей последовательности. При этом, редактирование данных в уже сформированной последовательности, очевидно, приведёт к нарушению всей цепочки, так как блок, в котором произошло изменение, получит новое значение хеш-функции, а следующий будет хранить старое. Даже если вернуть старые данные, хеш-значение уже не будет прежним, в этом случае защиту неизменности данных возьмёт на себя именно «временная метка». На рис. 4 продемонстрирован пример формирования последовательности.

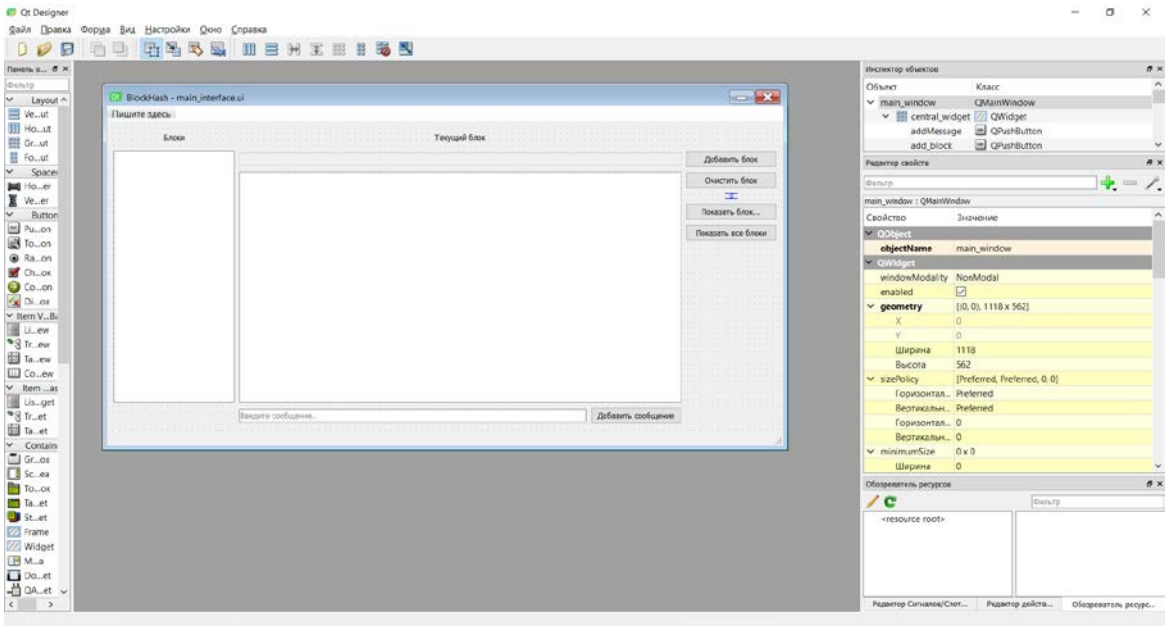


Рис. 2. Среда разработки пользовательского интерфейса

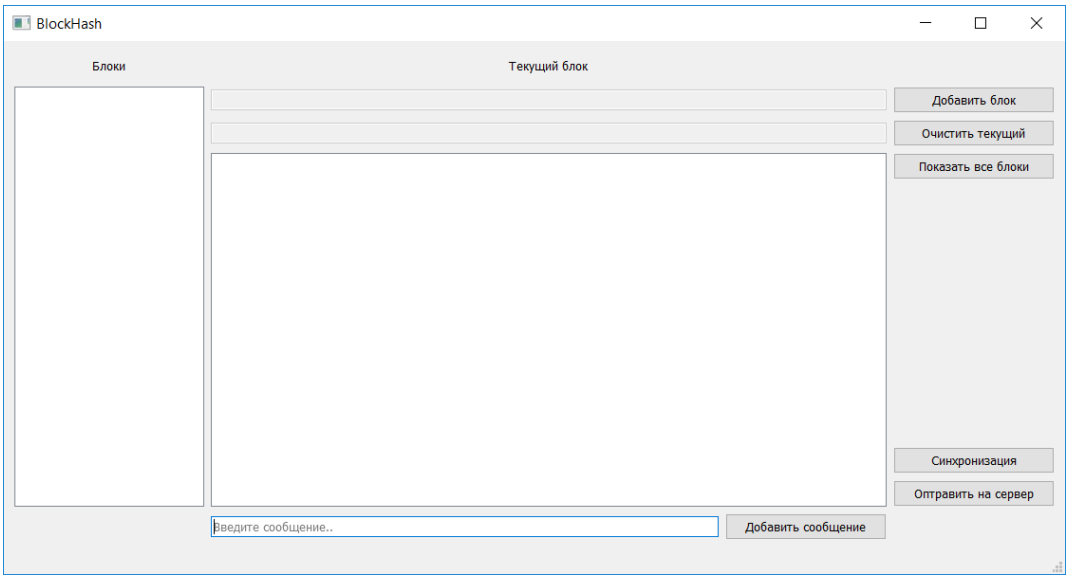


Рис. 3. Внешний вид клиентского приложения для хеширования блоков данных

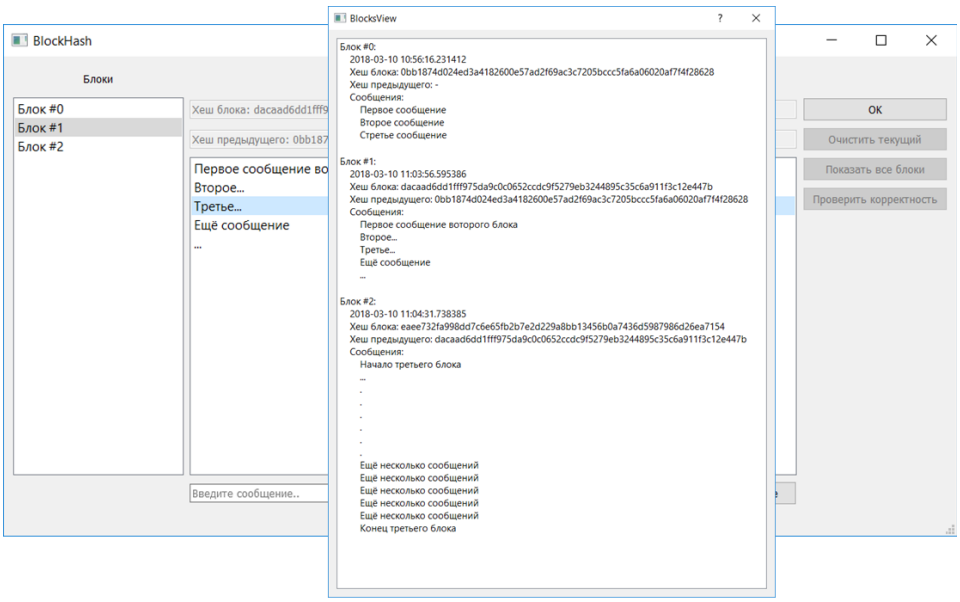


Рис. 4. Пример формирования последовательности из шести блоков

Синхронизация с сервером – это возможность любого клиентского приложения «сверить» его последовательность с той, что храниться на сервере, и восстановить её целостность в случае нарушения. При условии целостности цепочки клиентское приложение позволяет отправлять на сервер сформированную часть последовательность, которая будет продолжением общей последовательности, хранящейся удалённо. На рис. 5 – пример удачной синхронизации с сервером.

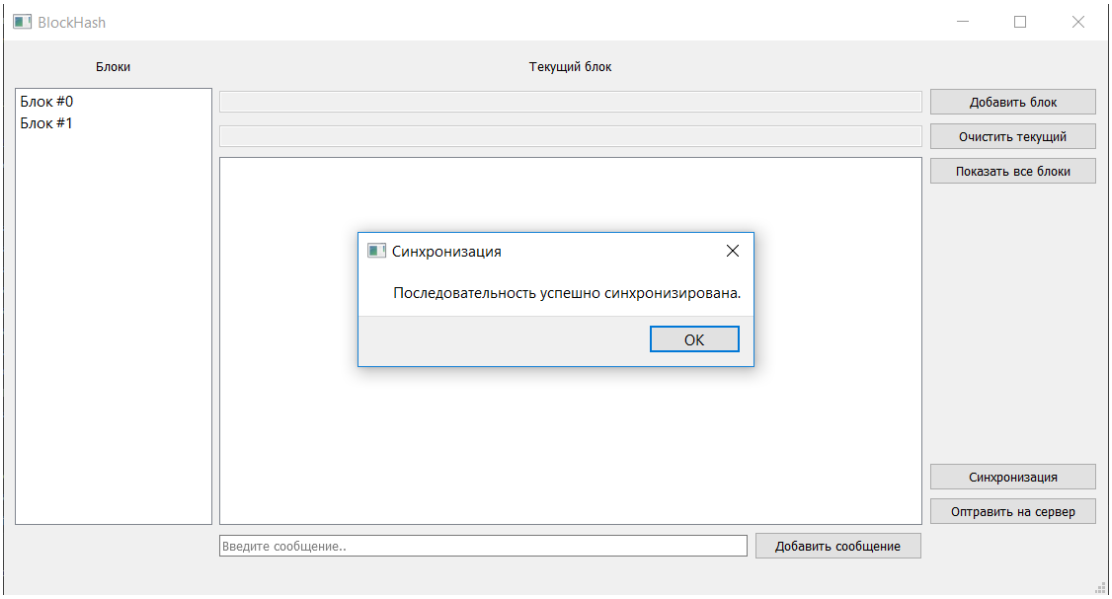


Рис. 5. Пример удачной синхронизации с сервером

Список используемых источников

1. Чудеса хеширования [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/the-wonders-of-hashing/3633 (дата обращения 10.04.2018).
2. Олифер В. Компьютерные сети. Принципы, технологии, протоколы (5-е издание). СПб.: Питер, 2016. 992 с.

УДК 004.942
ГРНТИ 28.17.31

АНАЛИЗ МЕТОДОВ МОДЕЛИРОВАНИЯ БИЗНЕС-ПРОЦЕССОВ В ЗАДАЧАХ ОЦЕНКИ ЭФФЕКТИВНОСТИ МОДЕРНИЗАЦИИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ

Д. В. Волошененко, Л. Д. Комарова, В. Л. Литвинов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются методы моделирования бизнес-процессов в задачах оценки эффективности модернизации информационной инфраструктуры предприятия. Проведен анализ существующих методов моделирования бизнес-процессов и методов оценки эффективности информационных технологий в бизнесе. Выявлена и обоснована необходимость совместного использования методов моделирования бизнес-процессов и методов оценки эффективности модернизации информационной инфраструктуры предприятия. На основе проведенного исследования авторами предлагается выделить совместный метод оценки эффективности с учетом моделирования бизнес-процессов как вспомогательного инструмента.

оценка эффективности, информационная инфраструктура, функционально-стоимостной анализ, методы моделирования бизнес-процессов.

Целью исследования является выявление связи между основными методами моделирования бизнес-процессов, используемыми в оценке эффективности модернизации информационной инфраструктуры предприятия, и теми методами оценки эффективности, в которых они применяются.

Объектами исследования выступают методы моделирования бизнес-процессов и методы оценки эффективности информационной системы управления предприятием.

В настоящее время имеется довольно большое количество методов моделирования бизнес-процессов. Данные методы имеют отношение к различным видам моделирования (функциональное, объектное, имитационное) и помогают найти пути оптимизации деятельности предприятия. Они содержат графические и текстовые средства, с помощью которых можно наглядно продемонстрировать основные связи между компонентами процесса, сами процессы и их основные параметры.

В основе многих современных методов моделирования бизнес-процессов лежат методология SADT (*Structured Analysis and Design Technique* – метод структурного анализа и проектирования), семейство стандартов IDEF (*Icam DEFinition*, где Icam – это *Integrated Computer-Aided Manufacturing*) и алгоритмические языки.

Выделяют следующие методы моделирования бизнес-процессов [1]:

1. Flow Chart Diagram IDEF0 – методология, предназначенная для формализации и описания бизнес-процессов.

2. IDEF3 – концепция моделирования и стандарт документирования процессов, происходящих в системе.

3. DFD (*Data Flow Diagramming*) – диаграмма потоков данных. Парадигма графического структурного анализа.

4. Цветные сети Петри – этот метод представляет модель процесса в виде графа, применимого для динамического моделирования поведения процесса.

5. UML – унифицированный объектно-ориентированный язык моделирования, позволяющий моделировать отдельные статические или динамические аспекты процесса.

Наряду с методами моделирования бизнес-процессов существуют методы оценки эффективности информационной инфраструктуры предприятия, в том числе информационной системы управления предприятием (ИСУП).

В таблице 1 [2] приведены наиболее часто встречающиеся методы оценки эффективности и возможности их применения на разных этапах жизненного цикла (ЖЦ) ИСУП.

Следует отметить, что только в двух методах оценки эффективности ИСУП используется моделирование бизнес-процессов: функционально-стоимостной анализ (ФСА) и экспресс-метод диагностики бизнес-процессов.

Связанность методов моделирования бизнес-процессов, а именно IDEF0, и ФСА заключается в том, что оба метода рассматривают финансово-хозяйственную деятельность предприятия как множество последовательно выполняемых функций, а дуги входов, выходов, управления и механизмов функций IDEF0-модели соответствуют стоимостным объектам и ресурсам ФСА-модели.

Из концептуальной модели ФСА-метода (рис. 1) видно, что Ресурсы (Затраты) в ФСА-модели – это входные дуги, дуги управления и механизмов в IDEF0-модели (рис. 2 [3]), Продукты (Стоимостные объекты) ФСА-модели – это выходные дуги IDEF0-модели, а Действия ФСА метода – это работы в IDEF0-модели.

На более низком уровне, а именно, уровне функционального блока, связь IDEF0- и ФСА-моделей базируется на трех принципах:

1. Функция характеризуется числом, которое представляет собой стоимость или время выполнения этой функции;

2. Стоимость или время функции, которая не имеет декомпозиции, определяется разработчиком модели;

3. Стоимость или время функции, которая имеет декомпозицию, определяется, как сумма стоимостей (времен) всех подфункций на данном уровне декомпозиции.

ТАБЛИЦА 1. Возможности применения методов оценки эффективности ИСУП на разных этапах ее ЖЦ

Наименование метода оценки	Возможности применения для оценки эффективности		
	проектируемой информационной системы		существующей информационной системы
	на стадии разработки	на стадии внедрения	
Расчет рентабельности инвестиций – Return on Investment (ROI)	+	+	-
Расчет совокупной стоимости владения – Total Cost of Ownership (TCO)	+	+	+
Расчет экономической добавленной стоимости – Economic value added (EVA)	-	-	+
Оценка реальных опционов – Real option valuation (ROV)	+	+	+
Метод прикладной информационной экономики – Applied information economics (AIE)	-	-	+
Потребительский индекс	-	-	+
Расчет экономической ценности – Economic value sourced (EVS)	-	-	+
Система сбалансированных показателей – Balanced ScoreCard (BSC)	+	+	+
Гартнер-измерение	-	-	+
Метод жизненного цикла искусственных систем – System Life Cycle Analysis (SLCA)	+	+	+

Наименование метода оценки	Возможности применения для оценки эффективности		
	проектируемой информационной системы		существующей информационной системы
	на стадии разработки	на стадии внедрения	
Методика быстрого экономического обоснования – Rapid Economic Justification (REJ)	+	+	+
Методы экспертной оценки	+	+	+
Функционально-стоимостной анализ (ФСА) – Activity Based Costing (ABC)	+	+	+
Экспресс-метод диагностики бизнес-процессов	+	+	+

Следующим методом, включающим в себя моделирование бизнес-процессов, является экспресс-метод диагностики бизнес-процессов, не входящий в перечень наиболее используемых методов оценки ИСУП, но проанализированный авторами настоящей статьи в ходе исследования. Здесь используются количественные показатели бизнес-процессов, такие как: сложность, процессность, контролируемость, ресурсоемкость и регулируемость. Данные показатели отличают этот метод от ФСА, в котором используются стоимостные показатели.

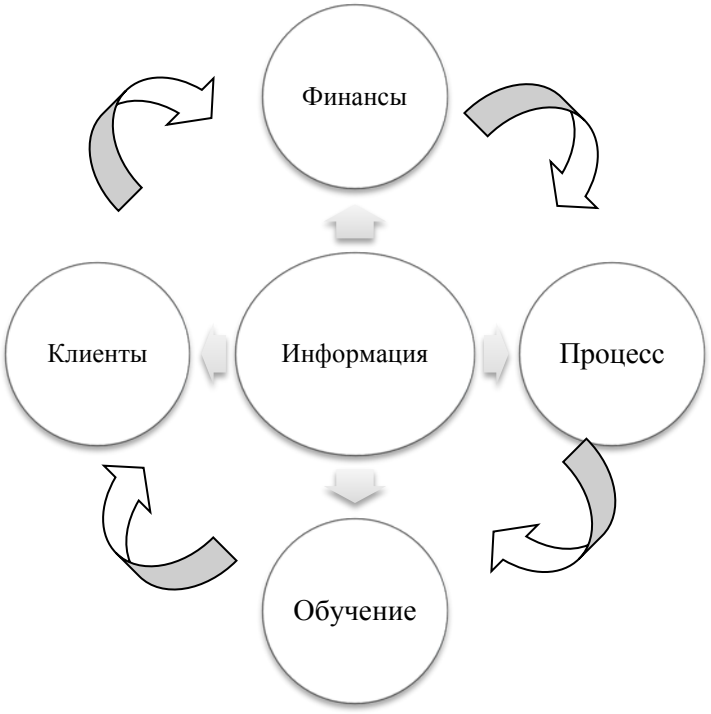


Рис. 1. Концептуальная ФСА-модель

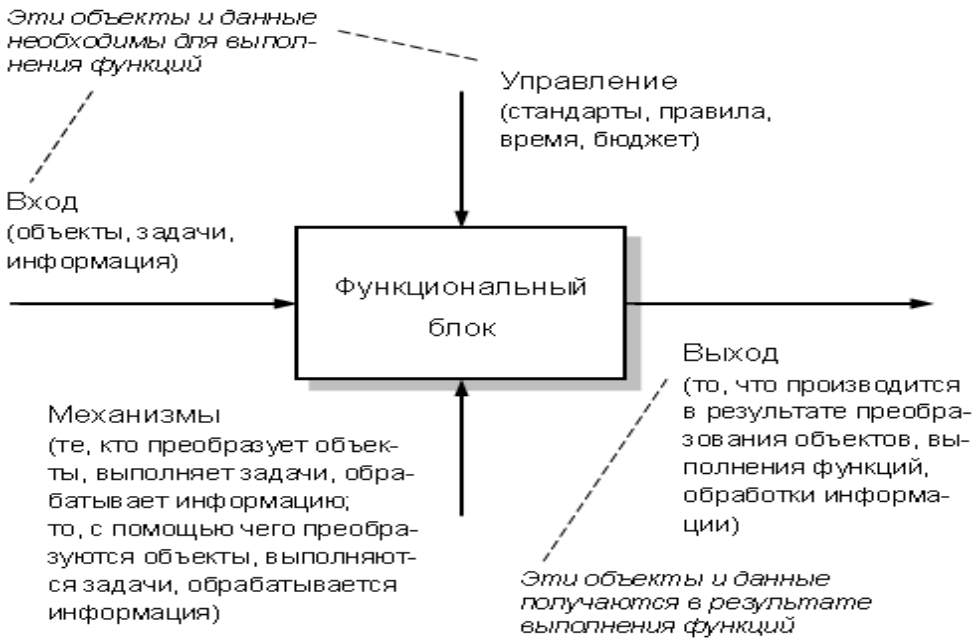


Рис. 2. Связь ФСА и IDEF0 модели

Для каждого показателя выведена формула для расчета, представленные в таблице 2 [4]. Сумма показателей бизнес-процессов должна соответствовать следующему нормативу: $1 \leq \Sigma k_i < 2{,}86$, в противном случае модель бизнес-процесса не является эффективной.

ТАБЛИЦА 2. Показатели эффективности бизнес-процесса, их расчет и значения

Показатели эффективности бизнес-процессов	Вид коэффициента	Формулы расчета коэффициентов	Значение коэффициента
Сложность	$k_{сл}$	$k_{сл} = \Sigma П_{ур}/\Sigma П_{экз}$	$k_{сл} \leq 0{,}66$
Процессность	$k_{пр}$	$k_{пр} = \Sigma П_{раз}/\Sigma П_{кп}$	$k_{пр} < 1$
Контролируемость	$k_{отв}$	$k_{отв} = С_П/\Sigma П_{кп}$	$k_{отв} = 1$
Ресурсоемкость	$k_р$	$k_р = Р/\Sigma П_{вых}$	$k_р < 1$
Регулируемость	$k_{рег}$	$k_{рег} = \Sigma П_{рег}/\Sigma П_{кп}$	$k_{рег} \geq 1$

Значения для расчета показателей эффективности являются количественными значениями параметров модели бизнес-процессов на основе данных из IDEF0 и DFD диаграмм: количество уровней бизнес-процессов $П_{ур}$; количество экземпляров бизнес-процессов $П_{экз}$; количество разрывов процессов в экземплярах бизнес-процессов $П_{раз}$; количество классов бизнес-про-

цессов $П_{кп}$; число собственников бизнес-процессов $С_П$; количество использованных ресурсов в бизнес-процессе Р; количество «выходов» в экземплярах бизнес-процессов $П_{вых}$; количество регламентирующей нормативной документации $П_{рег}$.

Анализ показал, что наиболее используемыми методами моделирования являются IDEF0 и DFD. Выделенные методы используются для оценивания эффективности в функционально-стоимостном анализе и экспресс-методе диагностики бизнес-процессов с помощью моделирования. Это приводит к тому, что с помощью данных методов на всех этапах жизненного цикла можно провести оценку эффективности с использованием одних и тех же диаграмм для расчета, как стоимостных критериев, так и количественных.

Список используемых источников

1. Вендров А. М. Методы и средства моделирования бизнес-процессов // Jet Info. 2004. № 10 (137).

2. Высочина М. В. Анализ методов оценки эффективности информационной системы управления предприятием // Культура народов Причерноморья. 2009. № 161. С. 86–89.

3. Анисифоров А. Б., Анисифорова Л. О. Методики оценки эффективности информационных систем и информационных технологий в бизнесе [Электронный ресурс]: учебное пособие. СПб.: Санкт-Петербургский государственный политехнический университет, 2014. URL: http://elib.spbstu.ru/dl/2/3876.pdf/download/3876.pdf (дата обращения: 20.02.2019).

4. Чупров К. К. Экспресс-метод диагностики бизнес-процессов компании // Консультант директора. 2005. № 20. С. 6–10.

УДК 654.739
ГРНТИ 49.33.29

МЕТОДЫ ПОСТРОЕНИЯ ЭФФЕКТИВНОЙ ТОПОЛОГИИ ИГРОВЫХ ПЕРСОНАЖЕЙ ПОСРЕДСТВОМ РЕТОПОЛОГИИ ВЫСОКОПОЛИГОНАЛЬНЫХ МОДЕЛЕЙ

Д. В. Волошинов, А. С. Зайцева, А. М. Лысенко, А. М. Сосновских

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время существует множество программ и инструментов для создания хорошо детализированных трёхмерных объектов как с применением метода скульптинга, так и фотограмметрии. Но в обоих случаях, результатом работы является очень плотная полигональная сетка с почти хаотичной топологией. Такой объект не применяется в игровых целях, так как с анимацией огромного количества полигонов в реальном времени справится далеко не каждый компьютер, который будет иметь разные характеристики в зависимости от пользователя, который использует этот продукт. Выходом из этой проблемы является уменьшение количества полигонов и построение более эффективной и правильной топологии 3D-модели с использованием различных инструментов для ретопологии.

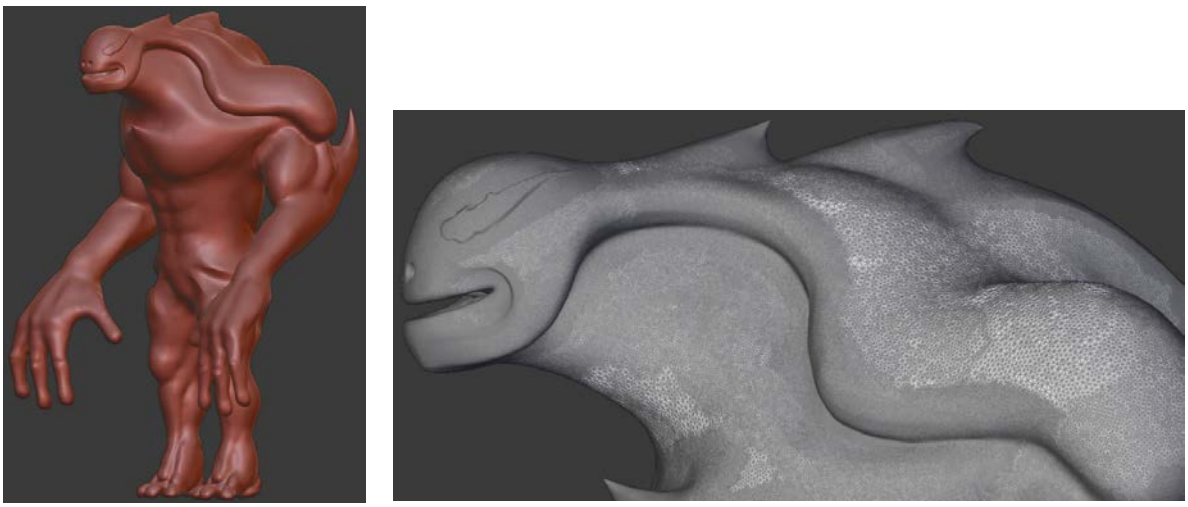
полигональная сетка, 3D-модели, ретопология.

Ретопология – процесс построения топологии, того как полигоны формируют 3D-модель, заново, с целью сделать полигональную сетку менее плотной и пригодной для анимации, а так же для уменьшении количества полигонов или для дальнейшего моделирования более мелких деталей персонажа с использованием различных методов. Последний вариант применяется в основном для получения возможности перенести мелкие детали на низкополигональную модель, которая будет применяться в игре.

В настоящее время существует целый ряд инструментов, позволяющих сделать ретопологию 3D-модели различным способами. Наиболее удобными и качественными являются следующие программы: ZBrush, 3D-Coat.

Для проведения процесса ретопологии будет использована данная модель (рис. 1 а).

Трехмерная модель получена скульптингом (метод трехмерного моделирования) в 3D-пакете Blender и имеет более двух миллионов полигонов. На рис. 1 б показана полигональная сетка модели и видно насколько она плотная и хаотичная.



а б

Рис. 1. Изображение трехмерной модели

На данный момент, во всех профессиональных студиях по разработке компьютерных игр на очень качественные и проработанные модели приходится около 20–30 тысяч полигонов. Со временем эти цифры увеличатся, так как с каждым годом производительность компьютеров растёт и это позволит разработчикам поднять уровень качество моделей на более высокий уровень.

Процесс ретопологии бывает автоматическим и ручным. У каждого из методов есть свои плюсы и минусы. Рассмотрим каждый их них более подробно и сравним.

В программе ZBrush применятся только автоматический режим. Однако, можно управлять некоторыми параметрами, которые влияют на результат. Одним из таких параметров является целевое число полигонов после процесса перестроения сетки и возможность указать направление того, как полигоны должны располагаться. В данном случае было выставлено результирующее число равное 8.5, что означает, что программа постарается выполнить процесс и минимизировать реальное число полигонов до целевого. А также были указаны направления построения новой топологии с помощью кривых (рис. 2).

Рис. 2. Направления новой топологии на трехмерной модели

Программа 3D-Coat позволяет осуществить как ручную, так и автоматическую ретопологию объекта. Последняя опция представляет из себя очень похожий процесс, который используется в ZBrush. Так же присутствует возможность рисовать кривые поверх 3D-модели, управляющие построением новой топологии. Имеется возможность указывать места более плотной сетки, где количество полигонов будет значительно больше, чем в других местах объекта. Ниже приведены параметры, используемые для авторетопологии (рис. 3).

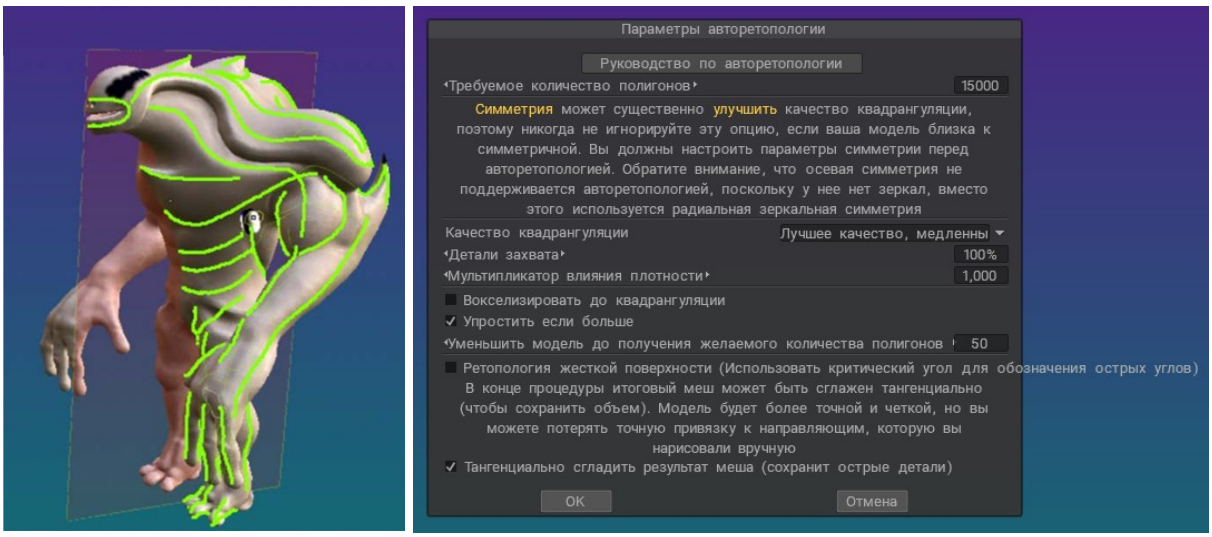


Рис. 3. Трехмерная модель в программе 3D-Coat

Ручной же метод более длительный, но более гибкий. Он позволяет полностью выбирать то, как будут располагаться полигоны и формировать сетку.

Одним из самых базовых и простых является инструмент «Узлы». Принцип действия заключается в расположении точки непосредственно и её проецировании на высокополигональный объект. При достаточном количестве точек, расположенных рядом – можно образовать полигон. Так же точки можно двигать после расстановки. Процесс проиллюстрирован на рис. 4.

Рис. 4. Образование полигонов

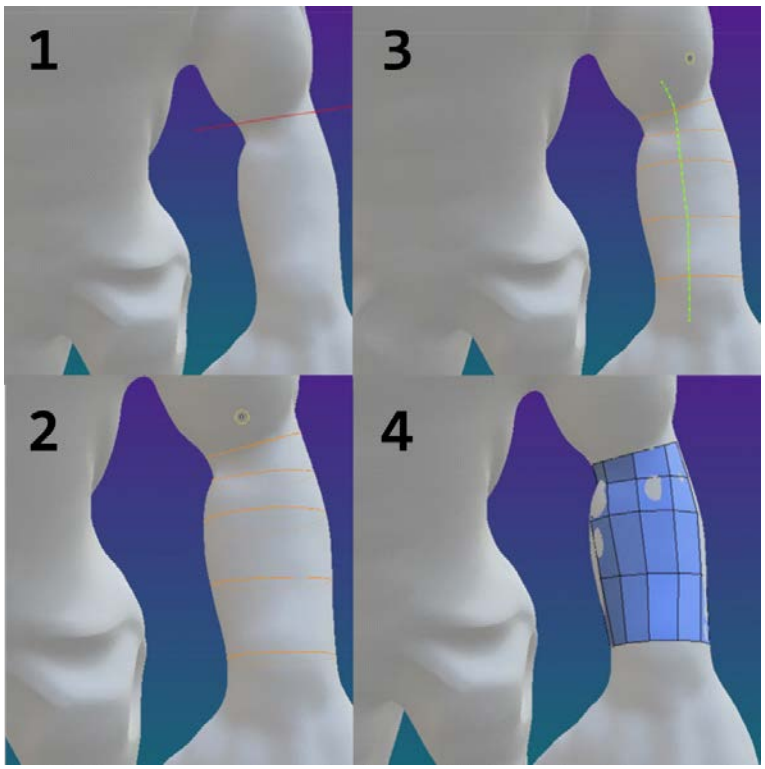


Рис. 5. «Штрихи»

Другим не менее важным является инструмент под названием «Штрихи». Его очень удобно применять на цилиндрических формах – например, конечности, но не обязательно. Если провести линию, как бы отсекая, например, руку данного объекта, то в том месте появится окружность, охватывающая модель. Проведя несколько таких контуров и соединив их одной линией, как будет продемонстрировано на картинке, можно указать в настройках программы количество полигонов, которые буду образовывать данную цилиндрическую форму. Процесс наглядно изображен на рис. 5.

Процесс ручной ретопологии очень трудоёмкий и долгий, но результаты практически всегда лучше, так как сам человек управляет процессом, а не компьютер. Следовательно, в определенных местах можно «сэкономить» полигоны, а где-то сделать модель более детальной. Далее будут приведены результаты ретопологии, проведенные ранее.

ТАБЛИЦА. Значения времени передачи кадра
при различных соотношениях параметров

Программа	Направляющие	Количество полигонов
ZBrush	с направляющими	28434
ZBrush	без направляющих	25424
3D-Coat	с направляющими	26456
3D-Coat	без направляющих	24350
3D-Coat	Ручной метод	19580

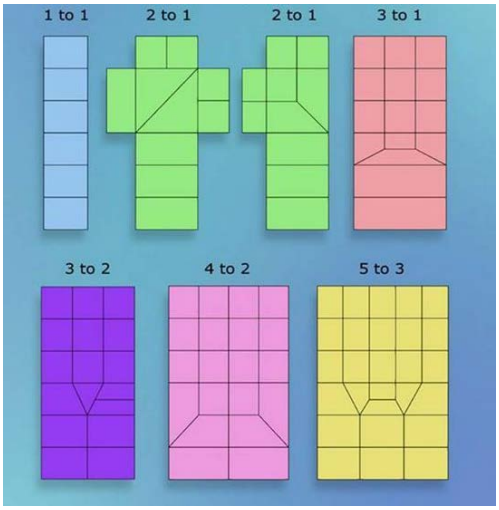


Рис. 6. Ретопология

По полученным из таблицы результатам видно, что методы автоматической ретопологии с использованием кривых имеют более правильную топологию, но при этом количество полигонов значительно больше, чем без использования вспомогательных направляющих линий. Если говорить о количество полигонов, то самое наименьшее оно в случае ручной ретопологии, так как имелась возможность упростить сетку модели, в тех местах, где пользователь или игрок не будет видеть 3D-объект полноценно. Так же экономии и снижению полигонажа способствовали различные методы построения правильной топологии, например, переходы от трёх полигонов к одному полигону.

У методов без использования кривых имеются свои минусы. Так, например, в ZBrush направление распространения полигонов идёт по диагонали, где ожидалось увидеть его по горизонтали. А в 3D-Coat часть объекта была просто отсечена, и такая модель уже не сможет использоваться ни для анимирования, ни для запекания карты нормалей – так как для этого процесса минимальным требованием является повторение контуров высокополигонального объекта. Чаще всего такие методы используются для статичных предметов, таких как здания или интерьер, которые не буду перемещаться и менять свою форму в реальном времени. Проблемные участки приведены на изображениях ниже на рис. 7 и 8.

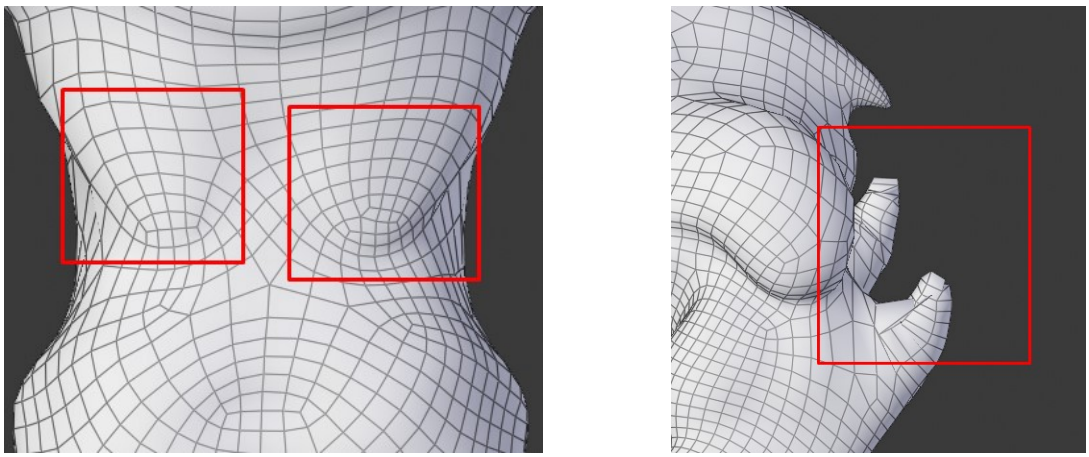


Рис. 7. 3D coat

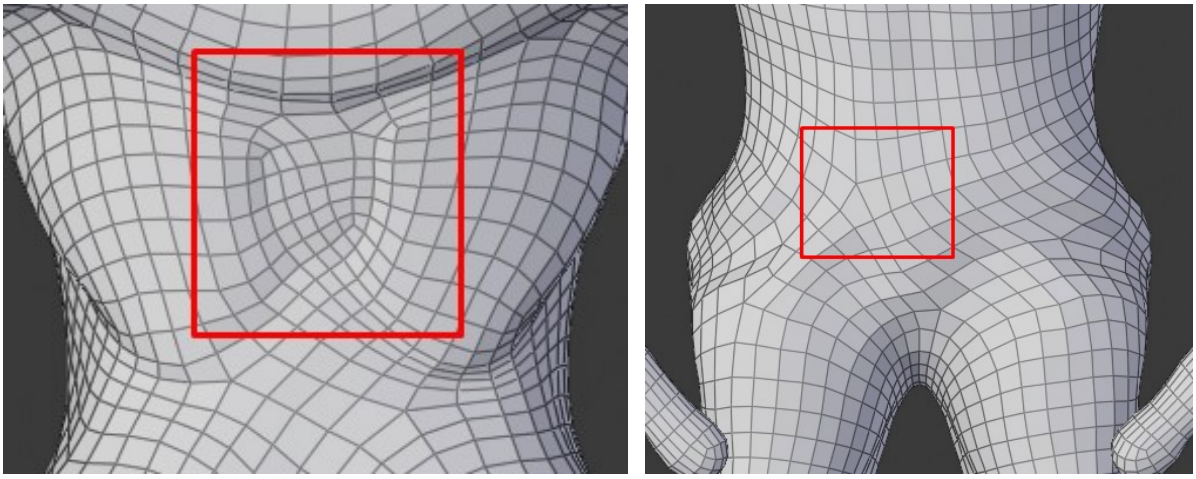


Рис. 8. ZBrush

У методов с использованием кривых имеются средние показатели как по полигонажу так и по топологии. Плюсом является частичная управляемость процессом и быстрота выполнения ретопологии. Авторетопология с управляющими кривыми является самым оптимальным решением перестроения имеющейся полигональной сетки по критериям качества и времени.

Ручная ретопология имеет наивысший показатель по качеству и управлению топологией, но время, затрачиваемое на её создание, является критическим фактором. Данный метод чаще всего используется при необходимости анимирования органических моделей, таких как люди и животные.

Список используемых источников

1. Сосновских А. М., Трифанов М. А., Волошинов Д. В., Кокорин М. С. 3D-сканирование и дополненная реальность // Неделя науки СПбПУ Материалы научной конференции с международным участием. 2016. С. 157–159.

УДК 621.382.002; 621.382.049.77.002
ГРНТИ 47.13.11

ПРОБЛЕМЫ ВЗАИМОДЕЙСТВИЯ ИОННЫХ ПОТОКОВ С ПОВЕРХНОСТЬЮ ТВЕРДОГО ТЕЛА

П. А. Волынкин, Н. А. Капуров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

При изготовлении ряда изделий нано- и микроэлектроники предъявляются повышенные требования по воспроизводимости геометрии поверхности, получаемой ионной обработкой. При бомбардировке формируемой поверхности тяжелыми ионами имеют место три основных процесса: эрозия основным потоком ионов, эрозия отраженными от стенок маски и формирующихся стенок в самом образце, а также реосаждение – осаждение только что распыленного материала маски и образца на поверхность изделия. Для поиска методов автоматизированного управления процессом формообразования изделия требуется разработка математической модели процесса.

микроэлектроника, технология, ионное травление, эрозия, отражение, реосаждение, математическая модель.

К множеству изделий нано и микроэлектроники предъявляются повышенные требования по воспроизводимости геометрии поверхности, получаемой ионной обработкой [1, 2, 3, 4].

Так при формирование глубоких канавок из двуокиси кремния в конденсаторах необходима простая, легко поддающаяся электрическим расчетам поверхность с плоским дном и отвесными стенками. В реальности, однако наблюдается искажение формы канавок.

Критичные к геометрии глубокие канавки используются при изоляции высокоскоростных биполярных приборов в оптоэлектронике. При изготовлении ионной бомбардировкой линз Френеля предъявляются высокие требования к воспроизводимости заданного профиля линзы.

В последнее время получили широкое распространение приборы на ПАВ-структурах, где используются межэлектродные канавки с варьируемой в соответствии с заданным законом глубиной.

Особо актуальной становится проблема формообразования при изготовлении кристаллических элементов с обратной мезаструктурой для получения ВЧ монолитных пьезоэлектрических резонаторов и фильтров, используемых в частотоизбирательных контурах аппаратуры связи.

Наиболее доступная крестообразная конструкция монолитного фильтра выполняется на пьезоэлектрической пластине в виде двух акустически

связанных резонаторов, собственная резонансная частота каждого из которых определяется локальной толщиной пластины и массой электродов [5] (рис. 1).

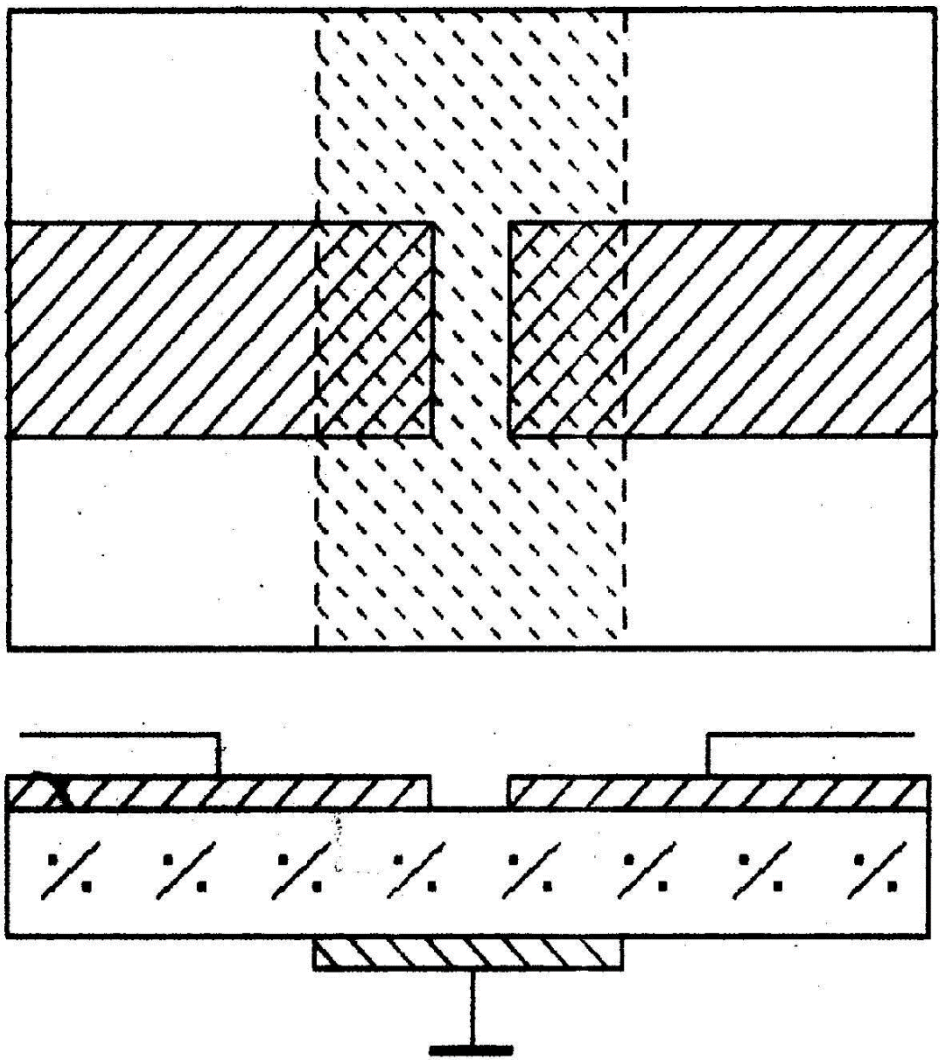


Рис. 1. Крестообразная конструкция пьезоэлемента для монолитного фильтра

Типовая схема включения такого фильтра представлена на рис. 2.

Удаление материала с исходной пластины толщиной порядка 60 мкм осуществляется путем ионной бомбардировки открытой части поверхности с использованием свободной маски. Однако, для малых толщин мембраны (менее 50 мкм) остро встает проблема обеспечения совпадения собственных частот связанных резонаторов, образующих фильтр [6].

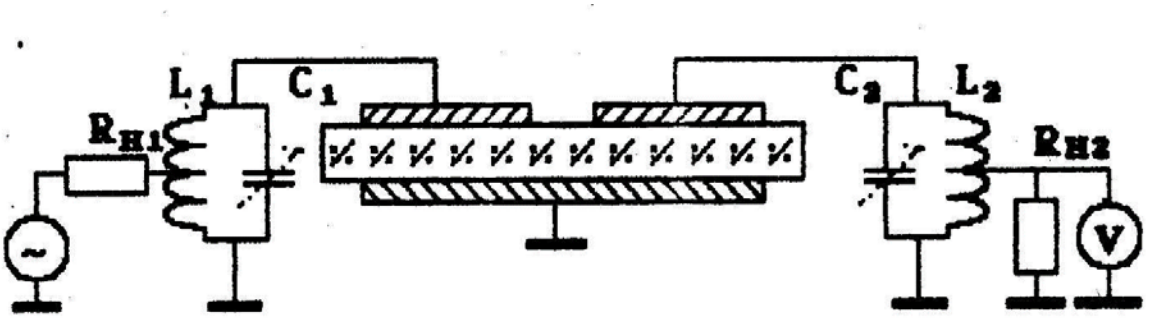


Рис. 2. Типовая схема включения фильтра

Процессы, которые широко применяются в технологии микросхем, по физико-химическому механизму делятся на три основных вида: ионное травление (ИТ), ионно-химическое правление (ИХТ) и плазмохимическое травление (ПХТ). Каждый из них имеет достоинства и недостатки. Поэтому с точки зрения обеспечения поверхностей заданной геометрии при травлении был проведен сравнительный анализ этих трех механизмов, который показал, что:

- ПХТ и ИХТ обладают на порядок более высокой скоростью травления, чем ИТ. Однако, спецификой ПХТ и ИХТ является наличие целого ряда гомо- и гетерогенных реакций, протекающих одновременно большей частью независимо друг от друга.

В связи с этим ПХТ и ИХТ значительно уступают механизму ИТ по воспроизводимости и однородности скорости травления и, следовательно, формируемой геометрии поверхности. Причем, последнее особенно проявляется при увеличении глубины травления.

При ИТ, как чисто физическом процессе, количество трудноконтролируемых и управляемых технологических параметров значительно меньше. Поэтому для получения поверхностей, критичных к геометрии, предподчтение отдается механизму ИТ.

Ионное травление же в зависимости от способа облучения поверхности разделяется на ионно-лучевое (ИЛТ) и ионно-плазменное травление (ИПТ).

В первом случае (ИЛТ ионной пушкой формируется ионный луч, направляемый на мишень с образцами. При достоинствах этого метода (возможность регулирования энергии ионов и угла их падения на образец) имеется и ряд серьезных недостатков:

− во-первых, ионные пушки представляют собой достаточно сложные устройства, в связи с чем контроль и управление процессом значительно усложняются;

− во-вторых, неоднородность ионного потока по диаметру луча приводит к необходимости для достижения равномерности травления вводить системы сложного перемещения образцов под ионным лучом;

− в-третьих, конструкция каждого типоразмера ионной пушки требует длительной экспериментальной отработки, так как отсутствуют инженерные методики их расчета.

Дополнительные трудности вызывает необходимость нейтрализации объемного заряда в луче и на поверхности образцов. Это приводит к созданию и размещению – дополнительных устройств в рабочем объеме или в конструкции пушки, что во многих случаях не позволяет обеспечить равномерную по поверхности образца нейтрализацию положительного заряда (еще один источник неравномерности травления).

В случае ИПТ образец помещают в рабочей камере на электрод с отрицательным потенциалом, формирующим электрическое поле, вытягивающее положительно заряженные ионы из газоразрядной плазмы. В ряде разновидностей метода сам электрод участвует и в создании газового разряда. Когда травлению подвергается образец из диэлектрика или высокоомного полупроводника, необходима компенсация образующегося на обрабатываемой поверхности положительного заряда, что достигается за счет облучения образца электронами из какого-либо специального источника или подведением к электроду с образцами высокочастотного потенциала. В последнем случае в течении отрицательной полуволны ВЧ напряжения происходит травление, а в течении положительной – компенсация положительного заряда электронами, вытягиваемыми из плазмы полем. Это разновидность ИПТ – ВЧ ИПТ.

С точки обеспечения равномерности скорости травления по мишени, на которой может размещаться несколько десятков образцов, и получения высокой воспроизводимости геометрии формируемых поверхностей, предпочтение отдается методу ИПТ для диэлектриков – ВЧ ИПТ).

Эксперименты изготовления канавок и пьезоэлементов методом ВЧ ИПТ показали наличие и в этом случае неоднородности (выпуклая линза при металлической маске толщиной 100 мкм) по толщине мембраны порядка 0.5 мкм (10 %). Линзовидность при осевой симметрии приводит к возможному разбросу резонансных частот резонаторов (в случае точности позиционирования лазерного луча порядка 10 мкм). Параллельно с обеспечением максимальной равнотолщинности мембраны возникает требование плавности перехода «мембрана-стенка», вытекающее из необходимости обеспечения механической прочности этого узла и предотвращения механических напряжений, которые могут возникнуть в узлах с резкой неоднородностью геометрии.

Изучение этих факторов путем планирования и реализации физического эксперимента малоперспективно и затруднительно ввиду большого числа предполагаемых факторов (более 10), низкой скорости травления материала (около 2–3 мкм/час) и большой глубины травления (порядка 50 мкм), которая требуется для обеспечения контроля с заданной точностью

(менее 0.1 мкм) профиля поверхности профилометрическими средствами [7].

В связи с этим возникает необходимость исследования процесса массопереноса при ионном травлении, разработки математической и вычислительной моделей процесса формообразования поверхности твердого тела, подвергаемого воздействию ионного потока.

Список используемых источников

1. Lieberman, M. A., Lichtenberg, A. J. Principles of Plasma Discharges and Materials Processing. John Wiley & Sons, 2005.

2. Ghodssi, R., Lin, P. MEMS Materials and Processes Handbook. Springer, 2011. XXXV. Pp. 1–118.

3. Mahameed, R., Sinha, N., Pisani, M. B. and Piazza, G. Dual-beam actuation of piezoelectric AlN RF MEMS switches monolithically integrated with AlN contour-mode resonators // J. Micromech. Microeng. 2008. V. 18. N. 9. P.105011.

4. Chin Yong Huan, Haslina Jaafar, Nurul Amziah Md Yunus Classification on MEMS Accelerometer and Device Application // Universiti Putra Malaysia. 2014. Pp.11–13.

5. Волынкин П. А. Модель эволюции поверхности-кристаллических элементов с обратной меза-структурой при ионном травлении // Математическое моделирование и САПР радиоэлектронных систем СВЧ на ОИС: Материалы III Всесоюзной НТК. М.: Радио и связь. 186 с.

6. Волынкин П. А. Изменение рельефа и структуры поверхности танталата лития при ионной бомбардировке // Взаимодействие атомных частиц с твердым телом: Материалы IX Всесоюзной НТК. М., 1989. Т.1. Ч.1. С. 121.

7. Volynkin P. A. Modeling o 1 surface evolution duringion // Микроэлектроника-90: Материалы III Международной НТК. Минск, 1990.

УДК 621.382.002; 621.382.049.77.002
ГРНТИ 47.13.11

МОДЕЛИРОВАНИЕ ЭРОЗИИ ПОВЕРХНОСТИ ТВЕРДОГО ТЕЛА ПРИ ИОННОМ ТРАВЛЕНИИ

П. А. Волынкин, А. А. Савинов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В микроэлектронной промышленности с годами все актуальней становится необходимость получения точного профиля поверхности твердого тела. Ряд изделий микроэлектроники изготавливаются с использованием технологии ионного травления (ионно-лучевое, ионно-плазменное). В ходе удаления с открытой части материала изделия имеют место три основных процесса: эрозия поверхности основным потоком ионов, эрозия отраженными от боковых стенок маски и формируемой поверхности потоками

ионов, реосаждения - перепыление только что удаленного материала маски и самого материала изделия. При формировании достаточно тонких элементов изделий существенно возрастает влияние относительной погрешности профиля формируемый поверхности на качественные характеристики изделия (например, на частоту пьезоэлектрического резонатора с обратной меза-структурой). В связи с этим возникает необходимость изучения методом математического и компьютерного моделирования этих процессов с целью поиска факторов для оперативного управления формируемым профилем.

микроэлектроника, технология, ионное травление, эрозия, отражение, реосаждение, математическая модель.

Ионное травлением связано с удалением вещества с плоскости твердого тела посредством бомбардировки поверхности заряженными ионами. Технология применима с такими материалами, как металлы, стекло и полимеры. В микроэлектронике ионное травление используется, как правило, с целью очистки поверхности твердого тела, выявления структуры поверхности, создания необходимого рельефа, очистки поверхности от различных примесей [1, 2].

При травлении твёрдого тела, в разряженном пространстве размещается пластина заготовки (рис. 1). Сверху на маскированной пластиной создается тлеющий разряд, который заполнен электронно-ионной плазмой. Поверхность пластины подвергается бомбардировке ионами плазмы с положительным зарядом, в результате чего, с поверхности выбиваются атомы слой за слоем, т. е. происходит травление. Когда травлению подвергается образец из диэлектрика или высокоомного полупроводника, необходима компенсация образующегося на обрабатываемой поверхности положительного заряда, что достигается за счет облучения образца электронами из какого-либо специального источника или подведением к электроду с образцами высокочастотного потенциала. В последнем случае в течении отрицательной полуволны ВЧ напряжения происходит травление, а в течении положительной – компенсация положительного заряда электронами, вытягиваемыми из плазмы полем. Подобная разновидность ионно-плазменного травления именуется высокочастотным ионно-плазменным травлением [3].

Существует два вида ионного травления: ионно-плазменное и ионно-лучевое травление.

При ионно-лучевом травлении, твердое тело помещается в высоковакуумную камеру, после чего ионной пушкой формируется ионный луч, направляемый затем на мишень с образцами.

Метод имеет существенные достоинства:

1. Имеется возможность регулирования энергии ионов.
2. Угол падения на образец может подвергаться корректировке.

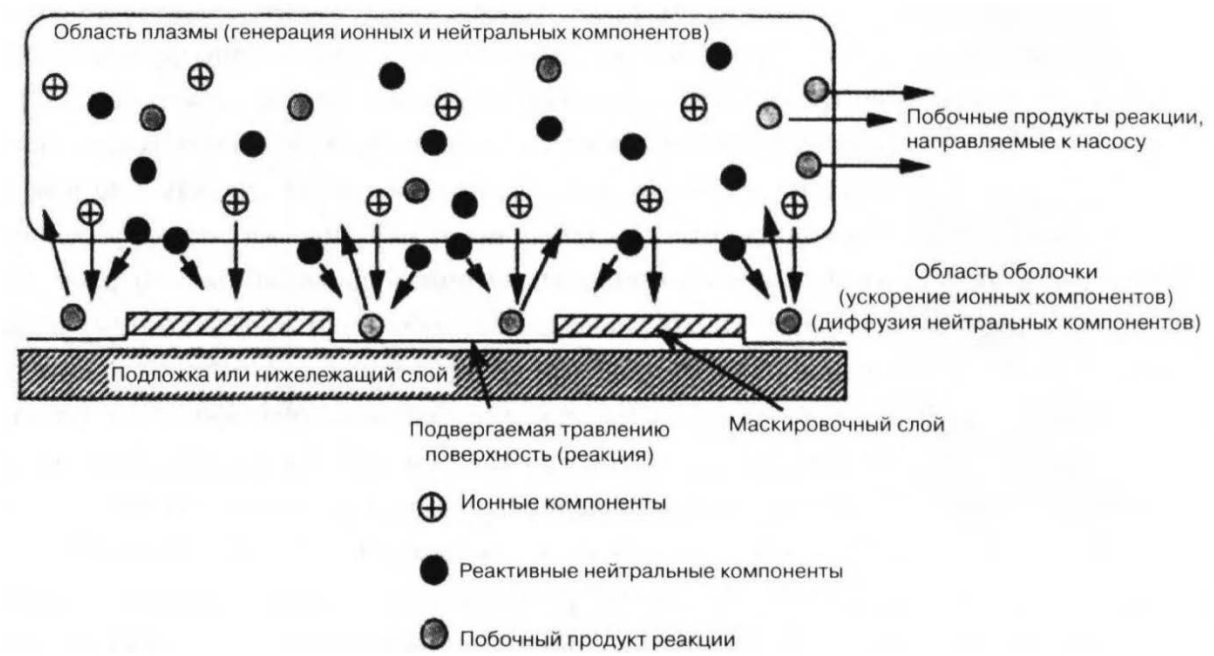


Рис. 1. Схема процесса ионного травления

При всех плюсах этого метода имеется и ряд серьезных недостатков:

1. Ионные пушки представляют собой достаточно сложные устройства, в связи с чем контроль и управление процессом значительно усложняются.

2. Неоднородность ионного потока по диаметру луча приводит к необходимости для достижения равномерности травления вводить системы сложного перемещения образца под ионным лучем.

3. Конструкция каждого типоразмера ионной пушки требует длительной экспериментальной отработки, так как отсутствуют инженерные методики их расчета.

4. Трудности вызывает также необходимость нейтрализации объемного заряда в луче и на поверхности образцов. Это приводит к созданию и размещению дополнительных устройств в рабочем объеме или в конструкции пушки, что во многих случаях не позволяет обеспечить равномерную нейтрализацию положительного заряда, отсюда создается неравномерность травления [4].

В случае ионно-плазменного травления образец помещается в рабочей камере на электрод с отрицательным потенциалом, формирующим электрическое поле, вытягивающее положительно заряженные ионы из газоразрядной плазмы.

Разновидностью ионного травления также является ионно-химическое травление. При использовании этого метода, в плазму добавляется химически активный газ, как правило кислород, а на скорость травления оказывает влияние химическое взаимодействие между вводимым газом и атомами подложки.

В процессе снятия материала с открытой части поверхности твердого тела, происходят процессы, которые можно разбить на две группы [3, 4] (рис. 2):

1. Процессы массопереноса при ионной бомбардировке:

- Эрозия поверхности основным потоком ионов – процесс удаления материала вещества за счет выбивания его атомов ионами, бомбардирующими поверхность с некоторого источника;
- Эрозия потоками ионов, отраженными от боковых стенок маски и формируемой поверхности – процесс эрозии, в котором источником ионов могут служить отвесные или крутые боковые стенки как маски, так и самой формируемой структуры;
- Реосаждение – процесс осаждения только что распыленного с соседних участков поверхности маски или самого объекта травления вещества;
- Диффузия вещества.

2. Процессы формирования исходного потока ионов. Сюда относятся факторы, по которым определяется неоднородность исходного потока ионов по энергии ионов, углу падения ионов на поверхность, плотности потока ионов.

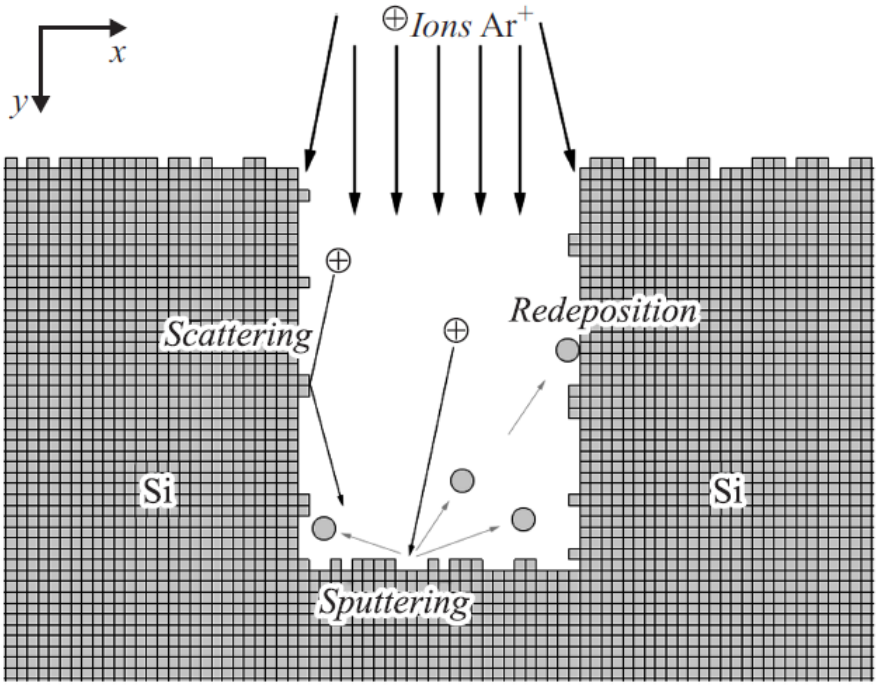


Рис. 2. Процессы массопереноса при ионной бомбардировке

Необходимо заметить, что эти группы тесно взаимосвязаны и влияют друг на друга, неоднородный поток ионов зависит от профиля формируемой поверхности, а сам в свою очередь влияет на количественные соотношения между процессами массопереноса.

В современной микроэлектронике ионное травление используется в изготовлении пьезоэлектрических резонаторов и фильтров, а также автоэмиссионных катодов для систем формирования мощных электронных потоков в устройствах вакуумной СВЧ электроники (рис. 3, 4, 5, 6).

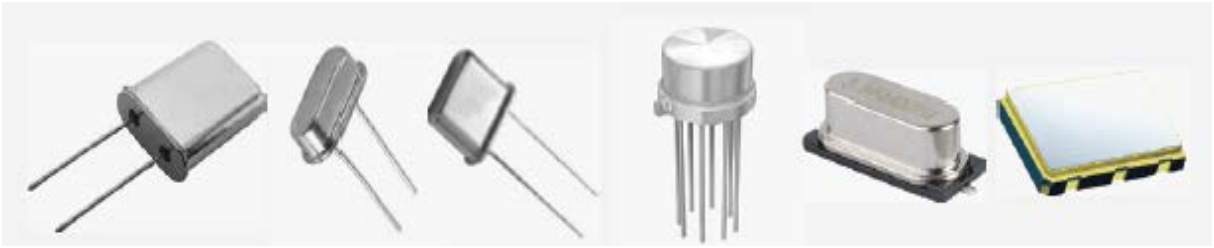


Рис. 3. Пьезоэлектрические резонаторы.

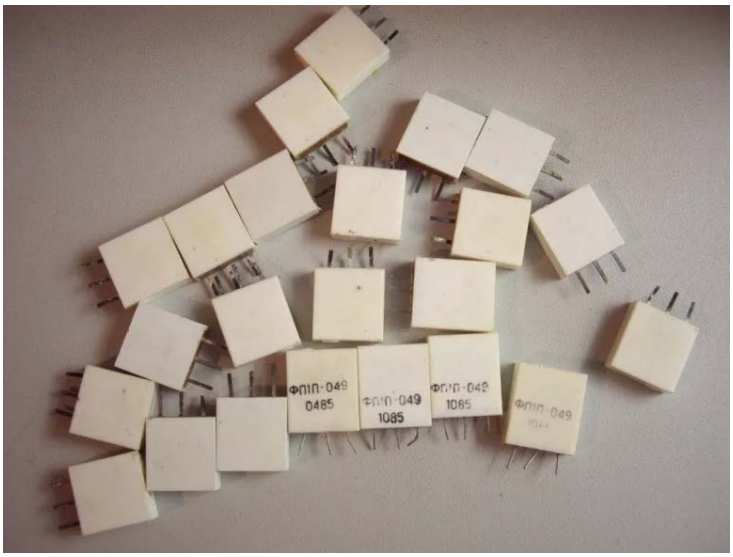


Рис. 4. Пьезоэлектрические фильтры

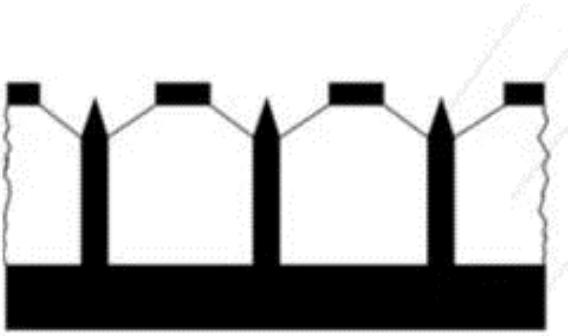


Рис. 5. Автоэмиссионный катод

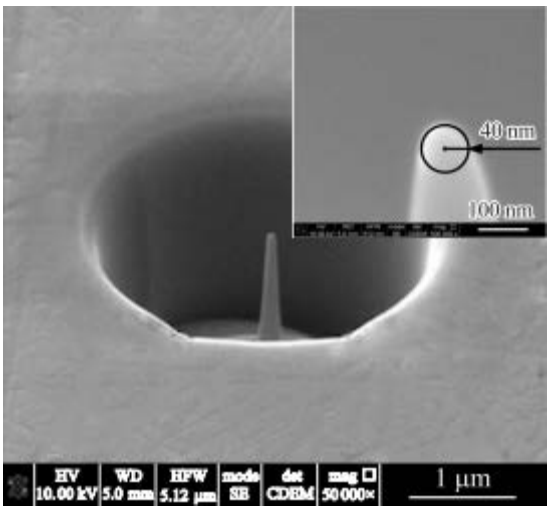


Рис. 6. РЭМ изображения автоэмиссионного катода

В ходе анализа процессов массопереноса твердых тел при воздействии на них ионных потоков [5] можно сделать следующие заключения:

1. Если реакция травления ионно-возбуждаемая, то боковое травление отсутствует, но в условиях ионно-ускоряемых реакций происходит боковой подтрав под маску, причем величина подтрава определяется скоростью протекания реакции. Для минимизации бокового травления в условиях ионно-ускоряемых реакций целесообразно вводить в рабочий газ добавки, обеспечивающие рекомбинацию активных компонент. Функция таких добавок заключается либо в связывании активных веществ на поверхности с образованием летучих соединений, либо в предотвращении образования пассивирующей пленки. Детали механизмов, ответственных за протекание этих процессов, до конца не выяснены. Следовательно, и степенью анизотропии травления можно управлять, регулируя состав рабочего газа.

2. Образование граней, возникновение канавок и повторное осаждение – три явления, проистекающие из физического распыления, которые могут влиять на профиль края вытравливаемого элемента. Степень их проявления зависит от интенсивности распыления и ионного потока, поэтому часто их можно полностью подавить.

3. Скорость ионно-плазменного травления зависит от угла падения ионов на поверхность материала, подвергаемого травлению, и для большинства материалов максимальна, когда этот угол отличен от 90°. Образующаяся грань наклонена по отношению к падающим ионам на угол, соответствующий максимальной скорости травления. Эта грань не оказывает влияния на профиль края вытравливаемого элемента до тех пор, пока не пересечет поверхность подложки.

4. Распыленный материал, не вошедший в состав летучих соединений, конденсируется на любой близлежащей поверхности. Распыленный материал распределяется в пространстве приблизительно по косинусоидальному закону, и поэтому значительная его часть может повторно осаждаться на стенках близлежащих элементов маски, что приводит к изменению профиля краев и размеров вытравливаемых элементов. Избежать этого можно, подбирая состав рабочего газа, параметры плазмы и маскирующие материалы так, чтобы происходило образование только летучих продуктов реакций.

5. Даже такой фактор, как толщина маски играет важную роль. Так, например, при толстой маске в результате получается выпуклая линза, а при тонких – вогнутая. Это говорит о необходимости подбора маски оптимальной толщины во избежание больших отклонений от плоскостности.

Подводя итог, необходимо поставить цель и задачи на дальнейшую работу по этой теме. В первую очередь, необходимо проанализировать существующие системы моделирования процесса эрозии поверхности твердого

тела при ионном травлении, после чего произвести и обосновать выбор технологических средств для разработки своей системы. Следующим шагом станет непосредственно разработка новой системы моделирования эрозии, её тестирование, модернизация.

Список используемых источников

1. Lieberman, M. A., Lichtenberg, A. J. Principles of Plasma Discharges and Materials Processing. John Wiley & Sons, 2005.

2. Chin Yong Huan, Haslina Jaafar, Nurul Amziah Md Yunus. Application // Universiti Putra Malaysia. 2014. Pp. 11–13.130.

3. Волынкин П. А. Модель эволюции поверхности-кристаллических элементов с обратной меза-структурой при ионном травлении// Математическое моделирование и САПР радиоэлектронных систем СВЧ на ОИС: Материалы III Всесоюзной НТК. М.: Радио и связь. 186 с.

4. Волынкин П. А. Изменение рельефа и структуры поверхности танталата лития при ионной бомбардировке // Взаимодействие атомных частиц с твердым телом: Материалы IX Всесоюзной НТК. М., 1989. Т. 1. Ч. 1. 121 с.

5. Volynkin, P. A. Modeling of surface evolution during ion beam etching // Микроэлектроника-90: Материалы III Международной НТК. Минск, 1990.

УДК 004.58
ГРНТИ 20.51.23

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ОЦЕНКИ ЧЕЛОВЕКО-МАШИННЫХ ИНТЕРФЕЙСОВ

А. В. Вострых

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Постоянно растущие информационные потребности современного пользователя различных систем далеко не всегда находят отражение в существующем программном окружении. Интерфейс, как посредник между системой и человеком, в настоящее время по большей части находится на уровне искусства и интуиции, что приводит к негативным последствиям, начиная от личного дискомфорта пользователя и заканчивая тяжёлыми авариями и катастрофами. Сегодня остро стоит вопрос: «С помощью чего и как эффективнее можно измерить соответствие информационной системы потребностям пользователей?»

В работе показана актуальность данного вопроса, описаны параметры оценки соответствия интерфейсов человеко-ориентированным подходам, проведён сравнительный анализ существующих методов оценки интерфейсов по учёту этих параметров.

человеко-машинный интерфейс, информационные потребности, информационные возможности, оценка эффективности.

Современный человек постоянно сталкивается с потребностью в информации и её обработке, для принятия решений, выполнения своих функциональных обязанностей на работе, удовлетворения личных интересов и проблем. Эти потребности можно объединить в особую категорию – «информационные потребности человека» (далее – ИПЧ), которые под влиянием стремительно и динамично развивающегося мира трансформируются в многогранные желания потребителей, такие, например, как: получать актуальную и индивидуальную информацию быстро, своевременно и беспрерывно; иметь возможность обрабатывать, удалять, изменять, корректировать данные; легко обмениваться информацией; хранить информацию и быть уверенным в соблюдении конфиденциальности и целостности.

Для удовлетворения этих потребностей в течение нескольких десятилетий создаются и совершенствуются различные информационные системы. С каждым годом объём накопленной информации и количество функционального инструментария таких систем постоянно растет, предоставляя потребителям весь спектр своих возможностей, которые можно объединить в категорию «информационные возможности системы» (далее – ИВС), к которой в частности относятся: предоставление пользователями всего накопленного массива информации в круглосуточном и беспрерывном режиме (практически не зависимо от их местонахождения); предоставление возможности обрабатывать, корректировать, удалять, создавать информацию, а также обмениваться ею между другими пользователями и самой системой; разграничение доступа к информации и т. д.

Обладая высокой сложностью, проявившейся в процессе эволюционного (а иногда и революционного) развития и постоянной модернизации (модификации) с расширением их функционала, системы стали трудно доступны для работы не только рядовым пользователям, но и в большинстве случаев даже профессионалам. С целью ликвидации появившегося барьера между системой и человеком разрабатываются и внедряются человеко-машинные интерфейсы. Они, как связующее звено между двумя категориями – ИПЧ и ИВС, создаются для полноценного и всестороннего комфортного взаимодействия. В настоявшее время специалисты по разработке интерфейсов стремятся к совершенствованию «посредников» путём внедрения человеко-ориентированных подходов, которые в максимальной степени упрощают взаимодействие пользователей с системой. Создаются правила и принципы, по которым должен строиться интерфейс. Так, согласно [1, 2, 3], для осуществления взаимодействия интерфейс должен обладать следующими составляющими и свойствами:

− необходимым набором элементов управления системой, позволяющим использовать весь спектр её возможностей, её элементы должны располагаться гармонично, учитывая особенности когнитивного восприятия человека, предугадывая желания и прогнозируя поведение пользователей, а также быть пригодным для обучения;

− учитывать психологические и физические особенности человека, представляя результаты работы в визуально-комфортном виде;

− обеспечивать защиту информации включая меры по обеспечению целостности и конфиденциальности информации при условии ее доступности для пользователей, имеющих соответствующие права и т. д.

Однако, современные человеко-машинные интерфейсы нельзя назвать истинно человеко-ориентированными по следующим принципиальным причинам:

1) Современные интерфейсы часто бесполезно модернизируются и модифицируются (нарушается принцип KISS от англ. «*keep it simple and straightforward»),* что заставляет пользователей заново переучиваться для работы с новой версией программы; при этом возникает противоречие, связанное с различием в скорости модификации интерфейсов и скорость изменения соотношений ИПЧ и ИВС. Яркими примерами являются излишне частые изменения в интерфейсах программ MapInfo, Microsoft Office, Adobe. Так интерфейс Microsoft Word с 2007 версии по 2016 изменяясь, становится менее наглядным, пропадает структура, усложняется читабельность, появляются бесполезные элементы, возникает перенасыщение информацией, расставляются непонятные акценты, как например подсветка вкладки «Файл» (в 2010 и 2013 версиях), хотя она не является активной, в то время как работающая вкладка «Главная» практически неотличима от остальных.

2) Современные интерфейсы заставляют изучать тысячи новых сочетаний клавиш. Почти каждая команда имеет свою комбинацию горячих клавиш, тем самым нарушается принцип монотонности интерфейса [4], усложняется процесс обучения, повышаются трудозатраты на разработку программ, приводя к противоречию, в разности соотношений темпов роста количества инструментов в интерфейсе и сложности обучения работы с ним, которая в разы возрастает с появлением дублирующих команд. Так, например, в Adobe Photoshop более 80 сочетаний клавиш, которые дублируют основные команды.

3) При разработке современных интерфейсов не учитывается принцип универсальности. Рассматривая производителей программного обеспечения одного направления можно заметить, что подходы к расстановке одних и тех же функциональных элементов, их группировка, визуальное отображение и механизмы управления во многом отличаются как между конкурирующими фирмами, например, Corel и Adobe, так и продукты созданные внутри компании Corel paint shop и CorelDraw, Adobe Photoshop и Adobe

Illustrator. Это приводит к противоречию количества целей (которое практически не изменяется) и возрастающему объёму навыков, которыми должен обладать пользователь. Например, программы компании Adobe (Photoshop, Illustrator, Lightroom), используют разные сочетания клавиш для одинаковых операций, таких как: «отмена действия» в Photoshop Ctrl+Alt+Z, в Illustrator нажатие Ctrl+Z; «изменение масштаба» в Photoshop сочетание Alt +колёсико мыши, в Lightroom нажатие на клавишу «пробел».

4) Современные интерфейсы позволяют начинающим пользователям вносить слишком критичные изменения в настройки, которые могут отразиться на скорости работы программы, изменить внешний вид интерфейса и принципы работы некоторых инструментов (нарушается принцип *mistake-proofing*). Возврат к первоначальным настройкам может быть крайне затруднён или даже не возможен. Например, в программе Photoshop в несколько кликов можно изменить параметры производительности системы, удалить или применить нежелательные цветовые профили, обновить настройки сохранения проектов.

5) Современные интерфейсы не в полной мере учитывают психологические и физиологические особенности человека; они переполнены данными и элементами управления, которые зачастую даже не сгруппированы (нарушаются принципы композиции). В таком изобилии информационных сигналов локус внимания легко теряется [4], что даёт возможность сознанию упустить предупреждение об ошибке или не заметить включенный режим. Возникающее при этом противоречие основано на постоянные увеличения умственной нагрузки на пользователя или оператора, в то время как психофизиологические ресурсы человека ограничены и остаются на одном и том же уровне. По причине этого распространённого недостатка интерфейсов происходят аварии и катастрофы.

Исходя из содержаний категорий ИПЧ и ИВС и соотношения их элементов выявлен ряд параметров оценки интерфейса, как элемента выполняющего связующую функцию в рамках человеко-ориентированного подхода. К ним относятся: сложность навигации, уровень умственной нагрузки на пользователя, сложность визуального восприятия интерфейса, скорость работы пользователя в системе, результативность, полезность, соответствие ожиданиям пользователей, избыточность представленной информации, информативность, контролируемость, целостность, надёжность (устойчивость к ошибкам), ментальная совместимость оператора и интерфейса, доступность элементов. Для оценки интерфейсов, в настоящее время, существует достаточно большое количество численных методов. Степень охвата ими оценочных параметров приведена в таблице.

ТАБЛИЦА. Соотношение охвата методами оценки человеко-машинных интерфейсов параметров оценки

Наименование методов	Оценка параметров													
	Сложность навигации	Умственная нагрузка	Сложность визуализации	Скорость работы	Результативность	Полезность	Соответствие ожиданиям	Избыточность информации	Информативность	Контролируемость	Целостность	Надёжность	Ментальную совместимость	Доступность элементов
Количество перерабатываемой информации (Шенон) [6]		+	+											
Количество перерабатываемой информации (Хартли) [7]		+	+											
Количество переработанной информации (Фаткин) [8]	+	+	+		+									
Ценность данных (Харкевич) [9]					+									
Избыточность данных (Парк) [10]		+	+					+						
Информативность (Горячкин) [11]									+					
Насыщенность (Горячкин) [11]			+					+						
Сложности поиска (Емельянова) [5]	+	+	+		+			+						
Наглядность (Диковицкий) [12]	+		+		+		+							
Селективность (Мучник) [5]		+	+					+	+	+				
Визуальная простота (Комбер-Мэлтби) [13]	+		+											
Визуальная простота (Стикел) [14]	+		+						+					
Ситуационная интерпретируемость (Кузнецов) [15]	+		+						+					
Лаконичность (Шенон) [6]						+			+					
Структурность (Звенигородский-Коломыйцев) [16]	+	+	+						+		+			
Целостность (Емельянова) [5]	+	+	+								+			
Закон Хика [18]	+	+	+	+	+									
Закон Фитса [19]				+										
Методы GOMS [1]	+	+		+	+	+								+
Вероятности исправной работы системы (Дружинин) [20]												+		
Декомпозиции ментальных операторов (Оксанич) [17]	+	+		+	+	+							+	

Проанализировав существующие методы [4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20], оказалось, что большая часть из них оценивает визуальную составляющую интерфейсов и умственную нагрузку на человека, в то время как, такие важные параметры как надёжность, контролируемость, соответствие ожиданиям пользователя, доступность элементов остаётся практически без внимания.

Некоторые параметры, а именно: пригодность для индивидуализации, управляемость, пригодность для обучения [1, 2, 3], существующими методами не оцениваются вообще.

То можно сделать вывод, что сегодня, не существует чётких понятий с помощью чего и как можно оценить интерфейсы на соответствие человеко-ориентированным принципам [1]. Более того не существует ранжирования параметров по степени значимости, тем самым не понятно какой метод будет более эффективным при проведении оценки.

Список используемых источников

1. ГОСТ Р ИСО 9241-210—2012. Эргономика взаимодействия человек—система. Часть 210. Человеко-ориентированное проектирование интерактивных систем. Москва Стандартформ 2013.

2. ГОСТ Р 55241.50-2014/ISO/TR 16982:2002 Эргономика взаимодействия человек-система. Методы обеспечения пригодности использования в человеко-ориентированном проектировании.

3. ГОСТ Р ИСО 9241-20-2014 Эргономика взаимодействия человек-система. Часть 20. Руководство по доступности оборудования и услуг в области информационно-коммуникационных технологий

4. Раскин Джеф. Интерфейс Новые направления в проектировании компьютерных систем. Санкт-Петербург; Москва: Символ, 2007. 257 с.

5. Емельянова Ю. Г., Фраленко В. П., Хачумов В. М. Методы комплексного оценивания когнитивных графических образов // Программные системы: Теория и приложения. № 3 (38). С. 49–63.

6. Shannon, C. E. A mathematical theory of communication // Bell System Technical Journal. 27:3 (1948). Pp. 379–423.

7. Hartley, R. V. L. Transmission of information // Bell System Technical Journal. 7:3 (1928). Pp. 535–563.

8. Фаткин Л. В. Количественные оценки деятельности оператора системы централизованного контроля и управления: автореф. дис. … канд. техн. наук. М., 1966. 13 с.

9. Харкевич. А. А. Проблемы кибернетики. Т. 4. М.: Физматгиз, 1960. С. 53–57.

10. Park, K. S. Human Reliability: Analysis, Prediction, and Prevention of Human Errors, Elsevier, New York, 1987, 340 p.

11. Горячкин Б. С. «Оценка выходных экранных форм автоматизированной системы обработки информации и управления» // Международный научно-исследовательский журнал. 2016. № 10. С. 24–27.

12. Диковицкий В. В., Шишаев М. Г., Ломов П. А. «Формализация задачи построения когнитивных пользовательских интерфейсов мульти предметных информационных ресурсов» // Труды Кольского научного центра РАН. Информационные технологии. 2013. No. 5. С. 90–97.

13. Comber, T., Maltby, J. R. Investigating layout complexity. Design, specification, and verification of interactive systems // Proceedings of the Eurographics Workshop in Namur (Belgium, Namur, 5–7 June 1996).

14. Stickel, C., Ebner, M., Holzinger, A. The XAOS metric— understanding visual complexity as measure of usability // 6th Symposium of the Work Group Human-Computer Interaction and Usability Engineering on HCI in Work and Learning, Life and Leisure 2010.

15. Кузнецов Л. А., Бугаков Д. А. Разработка меры оценки информационного расстояния между графическими объектами // ИУС. 2013. No. 1. С. 74–79.

16. Звенигородский А. С., Коломыйцев О. А. «Оценка визуальной информации в технических системах» // Искусственный интеллект. 2011. No. 4. С. 19–23.

17. Оксанич И. Н. Модель декомпозиции ментальных операторов в проблемно-ориентированном интерфейсе пользователя и ее экспериментальное исследование. Математические машины и системы. 2010. Выпуск № 1. Т. 1.

18. Hick, W. E. On the rate of gain of information // Quarterly Journal of Experimental Psychology. 1952. № 4. Pp. 11–26.

19. Fitts, P. M. The information capacity of the human motor system in controlling the amplitude of movement // Journal of Experimental Psychology. 1954. Vol. 47 (6). Pp. 381–391.

20. Дружинин Г. В., Степанов С. В. Теория надёжности радиоэлектронных систем в примерах и задачах: учеб. пособие для вузов. М.: Энергия, 1976. 448 с.

Статья представлена научным руководителем,
доктором технических наук, профессором М. В. Буйневичем

УДК 004.056
ГРНТИ 81.93.29

О ПОДГОТОВКЕ И ИСПОЛЬЗОВАНИИ РЕСУРСОВ ЕСЭ РОССИИ ДЛЯ ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ ЗО КИИ

О. В. Вышлов, С. С. Довгий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Угрозы в области обеспечения информационной безопасности, в том числе использование информационно-телекоммуникационных технологий для нанесения экономического и другого ущерба, в том числе путем оказания деструктивного воздействия на объекты критической информационной инфраструктуры, вызывают необходимость научного подхода к нормативно-техническому регулированию деятельности в области защиты информации, содержащейся в критических процессах.

критическая информационная инфраструктура, критический процесс, нормативно-техническое регулирование, защита информации.

С 1 января 2018 года вступил в силу 187-ФЗ «О безопасности критической информационной инфраструктуры». Указанным законом на Правительство Российской Федерации возложена обязанность установления требований по обеспечению безопасности информационно-телекоммуникационных сетей, которым присвоена одна из категорий значимости и которые включены в реестр значимых объектов критической информационной инфраструктуры. Кроме того, на Министерство цифрового развития, связи и массовых коммуникаций России возложена обязанность установления порядка, технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры.

Федеральным органам исполнительной власти предоставлено право устанавливать дополнительные требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, содержащие особенности функционирования таких объектов в установленной сфере деятельности.

Одним из 5 направлений Государственной программы «Цифровая экономика Российской Федерации» является направление «Информационная безопасность». Задачей направления является достижение целевого состояния, при котором создан каркас инфраструктуры безопасности цифровой экономики, в том числе в области новейших технологий, обеспечен цифровой суверенитет Российской Федерации к 2020 г.

Сети связи, используемые для организации взаимодействия ЗО КИИ, обеспечивают передачу информации, содержащейся в управленческих, технологических, производственных, финансово-экономических и иных процессах. Задачами системы информационной безопасности сетей связи ЗО КИИ являются:

1. Предотвращение неправомерного доступа к информации, передаваемой в сети связи ЗО КИИ, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

2. Недопущение воздействия на средства и системы связи, в результате которого может быть нарушено и (или) прекращено функционирование значимых объектов критической информационной инфраструктуры;

3. Восстановление функционирования сети связи ЗО КИИ, в том числе за счет создания резервных каналов и маршрутов;

4. Непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

По состоянию на дату написания настоящей статьи Постановление Правительства Российской Федерации «Об утверждении порядка подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры» не принято. Проект такого постановления получил отрицательную оценку регулирующего воздействия.

Пунктом 5 проекта Порядка предусматривается заключение договора на выполнение работ по подготовке к использованию ресурсов сети электросвязи.

Пункт 6 проекта Порядка в целях обеспечения взаимодействия и функционирования значимых объектов предусматривает заключение договора использования ресурсов сети электросвязи.

В соответствии с пунктами 8–10 проектируемого Порядка оператор связи при поступлении инициативы субъекта КИИ проводит присоединение (подключение) объекта КИИ к единой сети электросвязи, что подразумевает под собой заключение еще одного договора присоединения (подключения).

Кроме того, пунктом 11 проекта Порядка также предусматривается заключение договора по обеспечению информационной безопасности, который заключается при наличии соответствующей лицензии у оператора связи и по инициативе субъекта КИИ.

Таким образом, при анализе норм проектируемого регулирования можно сделать вывод, что проектируемое регулирование предполагает заключение 4 различных договоров между оператором связи и субъектом КИИ.

Проектом Порядка предусмотрено, что для сетей связи ЗО КИИ используются ресурсы выделенных сетей связи, технологических сетей связи, сетей связи специального назначения. По согласованию с ФСТЭК России, при отсутствии технической возможности использования указанных категорий сетей электросвязи либо необходимости дополнительного резервирования каналов связи допускается использование ресурсов сети связи общего пользования.

Для того, чтобы сформулировать четкий и исчерпывающий перечень требований к подготовке ресурсов сетей связи для работы с ЗО КИИ, необходимо разработать комплекс организационно-технических мероприятий по следующим направлениям:

1. Разграничение ответственности оператора связи и субъекта ЗО КИИ по обеспечению защиты информации.

2. Непрерывность оказания услуг связи субъектам ЗО КИИ, включая вопросы качества (QoS).

3. Меры по обеспечению устойчивого функционирования сетей связи, в том числе услуги по обеспечению защиты от компьютерных атак.

4. Взаимодействие центров управления сетями связи с центрами управления ЗО КИИ.

5. Особенности эксплуатационно-технического обслуживания сетей связи, обеспечивающих взаимодействие ЗО КИИ.

6. Взаимодействие между оператором связи и субъектом ЗО КИИ по обнаружению, предупреждению и ликвидации последствий компьютерных атак и при реагировании на компьютерные инциденты.

7. Защита информации субъектов ЗО КИИ вне контролируемых зон операторов связи.

В рамках настоящей статьи рассматриваются подходы к комплексу организационно-технических мероприятий первых двух пунктов из приведенного выше перечня.

В части разграничения ответственности оператора связи и субъекта ЗО КИИ по обеспечению защиты информации целесообразно установить порядок, при котором оператор связи не несет ответственности за защиту информации, в том числе криптографическую, передаваемую субъектом ЗО КИИ. Такой подход полностью соответствует требованиям 149-ФЗ «Об информации, информационных технологиях и о защите информации». Субъект ЗО КИИ может защищать такую информацию самостоятельно, либо поручить выполнение функций по защите информации третьей стороне на основании договора. Недостатком такого подхода является необходимость создания подразделений по защите информации

Объектам КИИ, сбои в работе которых могут повлечь за собой причинение ущерба здоровью одного человека, должна быть присвоена 3 категория значимости (основание – Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения, утвержденного постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»).

По данным статистического сборника Росстата «Здравоохранение в России 2017», в сфере здравоохранения функционирует 5 357 больничных организаций, 682 диспансера, 49 больниц скорой медицинской помощи, 19 126 амбулаторно-поликлинических организаций. Требования проектируемого регулирования будут распространяться на каждую из перечисленных организаций.

Для всех таких медицинских организаций в случае их отнесения к третьей (минимальной) категории, в соответствии с положениями Приказа ФСТЭК № 239 «Об утверждении требований по обеспечению безопасности ЗО КИИ Российской Федерации», предусмотрено выполнение 94 мер,

направленных на обеспечение безопасности для значимого объекта КИИ. В целях реализации указанных мер субъектам КИИ придется либо расширять штат сотрудников и создавать специализированные подразделения, либо заключать договора на предоставление услуг по защите информации.

Организационно-технические мероприятия по подготовке использования ресурсов ЕСЭ России в сетях связи ЗО КИИ должны обеспечить приемлемый уровень надежности и непрерывности услуг связи. Текущие тенденции развития рынка услуг связи показывают, что субъекты ЗО КИИ будут покупать исключительно услуги связи, оказываемые посредством сети передачи данных. Единственным документом, устанавливающим технические нормы на показатели надежности сетей связи, являются «Требования к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования», утвержденные Приказом Мининформсвязи от 27 сентября 2007 г. № 113. Этим документом установлен коэффициент готовности для сетей передачи данных не хуже 0,99. Для ЗО КИИ такой коэффициент готовности не приемлем.

Научное обоснование требований к коэффициенту готовности и иным существенным параметрам ресурсов ЕСЭ России для сетей связи ЗО КИИ должно учитывать, как категории значимости связываемых объектов КИИ, так и отраслевую специфику связываемых объектов. Очевидно, что устанавливать одинаковые требования к коэффициенту готовности предоставляемой услуги связи для АСУ ТП в области атомной энергии и для районной поликлиники нецелесообразно. Представляется необходимым установить нормативно-техническим документом, обязательным к исполнению субъектами ЗО КИИ и операторами связи, методику расчета требуемого коэффициента готовности и иных существенных параметров услуг связи для сетей связи ЗО КИИ. Разработка такой методики представляет собой отдельную научную задачу, задание на которую должно быть согласовано с федеральными органами исполнительной власти, наделенными соответствующими полномочиями по исполнению требований 187-ФЗ «О безопасности критической информационной инфраструктуры».

Приведенный выше анализ проблем реализации требований, предъявляемых к сетям связи ЗО КИИ показывает, что задача обеспечения безопасного функционирования объектов КИИ не может быть решена использованием ресурсов сети связи общего пользования. С высокой степенью вероятности, для выполнения всех установленных требований в Российской Федерации должна быть создана выделенная сеть связи, единственным назначением которой должен стать информационный обмен, обеспечивающий функционирование ЗО КИИ.

Список используемых источников

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.
2. Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
3. Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 09.08.2018) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
4. Приказ Мининформсвязи РФ от 27.09.2007 № 113 «Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования».
5. Ватрушкин А. А. Правовые основы обеспечения кибербезопасности критической инфраструктуры Российской Федерации // Правосудие и правоохранительная деятельность в евразийском пространстве. 2017. № 6 (31). С. 78–84.
6. Калашников А. О. Управление информационными рисками объектов критической информационной инфраструктуры Российской Федерации // Вопросы кибербезопасности. 2014. № 3 (4). С. 35–41.

Статья представлена заведующим кафедрой,
кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056
ГРНТИ 81.93.29

ОБНАРУЖЕНИЕ ВЕБ-РОБОТОВ НА ОСНОВЕ АНАЛИЗА ГРАФА ПОСЕЩЕНИЙ

Ю. А. Гатчин[1], А. Г. Коробейников[2], А. А. Менщиков[1]

[1]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
[2]Санкт-Петербургский филиал ФГБУН Института земного магнетизма, ионосферы и распространения радиоволн им. Н. В. Пушкова РАН

Современные исследования свидетельствуют о том, что роботизированный трафик на веб-ресурсах по объему и интенсивности преобладает над пользовательским. Веб-роботы угрожают приватности данных, авторскому праву, а также влияют на производительность, безопасность и искажают статистику посещений. Возникла необходимость обнаружения и противодействия таким средствам. Существующие методики предполагают использование синтаксической и аналитической обработки логов веб-сервера для обнаружения веб-роботов. В данной статье предлагается анализировать граф посещений веб-роботов, с учётом времени, тематики, а также связности

посещенных страниц. Производится анализ производительности, точности и полноты обнаружения, а также сравнение с результатами существующих подходов.

веб-роботы, граф посещений, парсинг, краулинг, противодействие парсингу, сбор информации, информационная безопасность, защита веб-ресурсов.

Введение

Веб-роботы – это специализированные средства сбора информации с веб-ресурсов [1]. Вредоносные веб-роботы несут угрозу безопасности информации на веб-ресурсе, а также оказывают влияние на производительность сайта, сбивают статистики, используемые для правильного кеширования и маркетинговых исследований [2]. Наиболее распространёнными угрозами являются манипуляции с метриками, автоматизация действий с целью получения выгоды, кража информации и другие [3]. Проблема противодействия веб-роботам на сегодняшний день становится заметной. OWASP выпустили проект, посвященный угрозам автоматизации, где классифицируют их и предоставляют имеющуюся информацию для обнаружения и противодействия таким средствам [4, 5].

Существующие сегодня способы обнаружения веб-роботов можно разделить на четыре категории: синтаксический анализ логов, статистический анализ трафика, аналитические методы и технические методы [6]. В основном, существующие подходы анализируют шаблоны поведения пользователей и роботов на веб-ресурсе, однако, не принимая во внимание структуру самого веб-ресурса. Использование знания о структуре сайта, тематики его страниц, типах файлов и связности страниц между собой даёт пространство для уточнения шаблонов поведения и более точного обнаружения автоматизированных посещений.

Анализ шаблонов поведения

Для обнаружения веб-роботов необходимо отличать шаблоны поведения, характерные для обычных пользователей и для автоматизированных средств. Система получает на вход данные о запросах пользователей к веб-ресурсу (HTTP заголовки, логи веб-сервера), а также формирует граф переходов между страницами веб-ресурса, включая в каждый узел графа информацию о типе и содержании конкретной страницы.

Рассмотрим сессию S, содержащую n упорядоченных запросов пользователя, где каждый запрос r^i отправлен с одного адреса источника и имеет одинаковое значение HTTP поля User-Agent.

$$S = (r^1, r^2, \dots, r^n).$$

Граф посещений веб-ресурса G – это набор вершин V, представляющих страницы веб-ресурса и коллекция упорядоченных рёбер-ссылок E между соответствующими страницами. Графы строятся как для самого веб-ресурса, так и для каждой сессии в отдельности.

$$G = (V, E).$$

Поведение веб-роботов по целям и механизмам осуществления отличается от поведения обычных пользователей [7]. Большая часть веб-роботов стремится ускорить процедуру сбора информации и уменьшить себестоимость реализации и функционирования [8]. Однако, существуют роботы, скрывающие своё присутствие и имитирующие действия пользователей. Существуют также публичные облачные сервисы, предоставляющие платные услуги по массовому сбору информации.

Рисунок. Типовая архитектура веб-робота

На основе графа поведения пользователей, можно изучать характеристики их действий, что позволяет отличать шаблоны поведения роботов от поведения людей [9]. К таким параметрам относятся структурные характеристики самих запросов в рамках сессии, временные параметры, а также поведенческие метрики, такие как: количество входящих и исходящих ребер, меры центральности, вес вершины в соответствии с алгоритмом PageRank [10], глубина просмотра относительно точки входа, количество циклов и возвратов на предыдущую страницу.

Результаты

Для реализации данного метода использовался набор логов средней популярности веб-ресурса, содержащего уникальный контент, а также разветвленную навигационную структуру сайта. В первую очередь данные были очищены и был произведен процесс идентификации сессий с использованием адреса источника, версии браузера пользователя, а также длительности сессии в 30 минут.

Был написан собственный парсер-структуры и связности веб-ресурса, который составил карту переходов и ссылок между страницами, а также определил тип ресурса каждой вершины графа [11, 12, 13]. Для каждой вершины были рассчитаны характеристики, указанные в предыдущей секции. Для каждой полученной сессии были рассчитаны характеристики, а также средние, медианные и среднеквадратическое отклонение характеристик каждой из вершин, пройденных в рамках данной сессии. Таким образом использовались не только характеристики самой сессии, но и параметры веб-ресурса.

Каждая сессия была в полуавтоматическом режиме маркирована как «веб-робот», «человек», «не определено» на основе структурного содержания запросов, адреса источника, информации из публичных баз данных. Все точно определенные сессии использовались для формирования обучающей выборки для процесса классификации сессий.

На основе имеющихся данных были обучены классификаторы. Наилучшие результаты обнаружения показал градиентный бустинг с использованием библиотеки xgboost [14] (представлены в таблице).

ТАБЛИЦА. Результаты обнаружения веб-роботов

	Точность	Полнота	F1-мера
False	0.94	0.89	0.91
True	0.78	0.87	0.82
Avg/Total	0.89	0.88	0.89

Для проверки результатов размеченные данные были разделены на 10 блоков, к которым была применена кросс-валидация. Использование предлагаемых характеристик в сочетании с классическими структурными и временными методами принесли наиболее высокие результаты, превосходящие отдельные результаты классических методов.

Выводы

Были проанализированы поведенческие характеристики пользователей веб ресурса с целью обнаружения автоматизированных посещений. Данные

характеристики могут быть использованы совместно со структурными и временными методами для организации процесса обнаружения и противодействия автоматизированному сбору информации с веб-ресурсов.

Результаты показывают повышение точности и полноты обнаружения веб-роботов при использовании дополнительных характеристик самого веб-ресурса, а также с учётом графа переходов пользователей по веб-ресурсу. Данные результаты открывают возможности дальнейшего уточнения обнаружения за счет внедрения дополнительных характеристик, а также использования семантического анализа тематики страниц веб-ресурса.

Список используемых источников

1. Zabihimayvan, M. et al. A soft computing approach for benign and malicious web robot detection // Expert Systems with Applications. 2017. Т. 87. Pp. 129–140.

2. Menshchikov, A., Komarova, A., Gatchin, Y. A., Korobeynikov, A. G., Tishukova, N. A Study of Different Web-Crawler Behaviour // Proceedings of the 20th Conference of Open Innovations Association FRUCT. 2017. Pp. 268–274.

3. Doran, Derek and Gokhale, Swapna S. Web robot detection techniques: overview and limitations. Data Mining and Knowledge Discovery. 2011. Pp. 183–210.

4. OWASP Automated Threats to Web Applications [Электронный ресурс]. URL: https://www.owasp.org/index.php/OWASP_Automated_Threats_to_Web_Applications free (дата обращения 16.01.2019).

5. Коробейников А. Г. Математические основы криптографии. Учебное пособие. СПб.: СПб ГИТМО (ТУ), 2002. 41 с.

6. Doran, D., Gokhale, S. S. An integrated method for real time and offline web robot detection // Expert Systems. 2016. Т. 33. No. 6. Pp. 592–606.

7. Stassopoulou, Athena, and Dikaiakos, Marios D. Web robot detection: A probabilistic reasoning approach // Computer Networks. 2009. V. 53. V 3. Pp. 265–278.

8. Doran, Derek, S. Gokhale A Classification Framework for Web Robots // Journal of American Society of Information Science and Technology. 2012. V. 63. Pp. 2549–2554.

9. Brown, K., Doran, D. Contrasting Web Robot and Human Behaviors with Network Models // arXiv preprint arXiv:1801.09715. 2018.

10. PageRank [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/PageRank (дата обращения 16.01.2019).

11. Гришенцев А. Ю., Коробейников А. Г. Понижение размерности пространства при корреляции и свертке цифровых сигналов // Известия высших учебных заведений. Приборостроение. 2016. Т. 59. № 3. С. 211–218.

12. Гришенцев А. Ю., Коробейников А. Г., Величко Е. Н., Непомнящая Э. К., Розов С. В. Синтез бинарных матриц для формирования сигналов широкополосной связи // Радиотехника. 2015. № 9. С. 51–58.

13. Коробейников А. Г., Сидоркина И. Г., Блинов С. Ю., Лейман А. В. Алгоритм классификации информации для решения задачи фильтрации нежелательных сообщений // Программные системы и вычислительные методы. 2012. № 1. С. 89–95.

14. Xgboost. GitHub. [Электронный ресурс]. URL: https://github.com/ dmlc/xgboost

УДК 004.056.05
ГРНТИ 81.93.29

ПРАКТИЧЕСКИЕ ОСОБЕННОСТИ ПОСТРОЕНИЯ ЦЕНТРОВ ГОССОПКА НА ОСНОВЕ НОРМАТИВНЫХ ТРЕБОВАНИЙ

Ю. А. Гатчин, Е. С. Юмашева

Санкт-Петербургский национально исследовательский университет информационных технологий, механики и оптики

В статье рассматриваются этапы развития нормативно-правовой базы, регламентирующей деятельность по обеспечению безопасности критической информационной инфраструктуры. А также рассмотрены некоторые практические особенности построения центров ГосСОПКА для значимых и незначимых объектов критической информационной инфраструктуры.

критическая информационная инфраструктура, государственная система обнаружения и предупреждения компьютерных атак, безопасность объектов.

Эволюция нормативной базы по ГосСОПКА

Развитие данной тематики началось в 2009 году с Указа Президента РФ № 157 о стратегии национальной безопасности РФ до 2020 года. Именно в рамках экого указа были сформированы направления государственной политики, связанные с защитой автоматизированной системы управления техническими процессами (АСУ ТП) и критически важных объектов. В данном документе появились термины: КИИ – критические информационные инфраструктуры; ГосСОПКА – единая государственная система обнаружения и предупреждения компьютерных атак на КИИ.

Следующим этапом стал Указ Президента РФ № 31с 2013 года о создании системы ГосСОПКА [1]. Указ инициировал создание системы ГосСОПКА, а так же определил полномочия ФСБ РФ. ФСБ поручено создать систему ГосСОПКА в рамках которой реализуется ряд мероприятий, которые исполняются ФСБ, они проводят различные мероприятия в том числе и оценивать степень защищенности КИИ. В рамках Указа Президента РФ № 31с была разработана Концепция ГосСОПКА № К 1274 [2]. Документ, определяющий иерархию центров ГосСОПКА, делящий их по территориальному, ведомственному признакам и определяющий цели и задачи, которые возникают в рамках всей системы.

На основе Концепции ФСБ России разработали Методические рекомендации по созданию центров ГосСОПКА. Документ определяет функции сегмента ГосСОПКА, а именно:

− инвентаризация;

- выявление уязвимостей;
- анализ угроз ИБ;
- повышение квалификации персонала;
- прием сообщений об инцидентах;
- обнаружение атак;
- анализ событий ИБ;
- регистрация инцидентов;
- реагирование на инциденты и ликвидация последствий;
- расследование инцидентов;
- анализ результатов ликвидации последствий.

Все этот состоит из процессов информационной безопасности, которые необходимо выполнять определенными техническими средствами, которые в свою очередь определены в методической документациях:

- средства взаимодействия персонала;
- средства взаимодействия с НКЦКИ ГосСОПКА;
- средства инвентаризации информационных систем;
- средства выявления уязвимостей;
- средства анализа событий информации;
- средства учета и обработки инцидентов.

В середине 2017 года принят ФЗ № 187 «О безопасности критической информационной инфраструктуры РФ» [3] и 22.12.2017 выходит обновленная версия Указа Президента РФ № 31с Указ Президента РФ № 620 о совершенствовании ГосСОПКА. Здесь особый акцент идет на то что система создана и её необходимо развивать и совершенствовать, это говорит о намерениях государства в обеспечении национальной безопасности РФ (таблица).

Изменения Указа Президента РФ № 620 относительно Указа № 31с:

1. Появилась ссылка на 187-ФЗ;
2. ФСБ России может контролировать защищенность не только КИИ, но и в целом информационных ресурсов РФ от атак;
3. ФСБ России разрабатывает методические рекомендации:
   - по обнаружению компьютерных атак на информационные ресурсы РФ;
   - по предупреждению и установлению причин компьютерных инцидентов, связанных с функционированием информационных ресурсов РФ, а также по ликвидации последствий этих инцидентов.

Затем 01.01.2018 вступает в силу Федеральный закон № 187 о безопасности КИИ. Рассматривая часть, относящуюся к ГосСОПАКА стоит отметить следующее:

1. Закон установил права и обязанности субъектов КИИ;

1.1 Задачи по защите значимых объектов КИИ:

- Защита от неправомерного доступа к информации, обрабатываемой КИИ;
- Защита от негативного воздействий, в результате которых может быть нарушено и (или) прекращено функционирование объекта КИИ;
- Восстановление функционирования объекта КИИ;
- Непрерывное воздействие с ГосСОПКА.

2. Закон наделил ФСБ России (**Федеральный орган исполнительной власти уполномоченный**) полномочиями:

2.1 Создает национальный координационный центр по компьютерным инцидентам;

2.2 Контролирует субъектов КИИ по реагированию на инциденты;

2.3 Устанавливает порядок информирования об инцидентах, определяет состав предоставляемой информации;

2.4 Устанавливает требования к средствам ГосСОПКА;

2.5 Организует установку на объекты КИИ технических средств ГосСОПКА и устанавливает требования к ним;

2.6 Организует и проводит оценку безопасности объектов КИИ.

ТАБЛИЦА. Приказы по ГосСОПКА

Приказы по ГосСОПКА	
Приняты:	**Проекты:**
Приказ ФСБ России от 24.07.2018 № 366 о Национальном координационном центре по компьютерным инцидентам	**Приказ ФСБ России** об утверждении Требований к средствам ГосСОПКА
Приказ ФСБ России от 24.07.2018 № 367 об утверждении Перечня информации, предоставляемой в ГосСОПКА, и Порядка предоставления информации в ГосСОПКА.	**Приказ ФСБ России** об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятие мер по ликвидации последствий компьютерных атак
Приказ ФСБ России от 24.07.2018 № 368 об утверждении Порядка обмена информацией о компьютерных инцидентах	**Приказ Минкомсвязи России** об утверждении порядка, технических условий установки и эксплуатации средств для поиска признаков атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ

Общая структура ГосСОПКА

ГосСОПКА – это система из ведомственных и корпоративных центров. Ведомственные создаются в обязательном порядке, корпоративные создаются по инициативе владельцев критически важных объектов. Эти центры образуют иерархию, т.е. во главе стоит главный центр ГосСОПКА, созданный на базе 8-го центра ФСБ, ведомственные и корпоративные центры находятся в подчиненном положении.

Соответственно каждый центр отвечает за свою зону. Ведомственный отвечает за все информационные ресурсы ведомства, корпоративный центр фактически самостоятельно определяет свою зону ответственности. Например, сервисная компания в составе государственной корпорации, её центр будет отвечать за противодействие атакам на информационные ресурсы этой корпорации.

Основная задача системы ГосСОПКА обнаружить невыявленные места уязвимости, предусмотреть возможные сценарии реагирования, скоординировать реакцию на атаку, провести расследование и учесть этот опыт для избежания подобных ошибок в дальнейшем. Данный набор функций показывает, что центр ГосСОПКА достаточно большое структурное подразделение, в котором должны быть специалисты высокой квалификации (вирусные аналитики, специалисты по тестированию на проникновение т. е. редкие специальности) и как правило в отдельно взятых коммерческих компаниях и органов власти специалистов таких квалификаций нет.

Для решения решения проблемы недостатка квалификации в рамках системы ГосСОПКА организуется 2 вида взаимодействия:

1. Вертикальное – центра ГосСОПКА с федеральной службой безопасности (главным центром). Например, если произошел инцидент, с которым центр ГосСОПКА справился: проблему обнаружили, локализовали и устранили, то данный центр уведомляет главный центр о данном инциденте, были притяну определенные меры, которые эффективно справились с атакой. На основании такой информации Главный центр может давать другим центрам рекомендации, при подобных инцидентах. Если происходит принципиально новая атака центр ГосСОПКА может обратиться в Главный центр за методической помощью, таким образом Главн центр подключается к решению возникшей проблемы. Также 8-й центр ФСБ обладает определенными возможностями обнаруживать атаки самостоятельно, в рамках оперативной работы или используя свои технические средства, в случае, когда ведомственный или корпоративный центр, пропустил атаку, он может получить информацию из Главного центра о возникшей проблеме, или же конкретное решение проблемы.

2. Горизонтальное. Например, создается центр ГосСОПКА в ведомстве и возникает потребность в специалисте определенной специфики, например, специалист по расследованию инцидентов, в таких случаях методические рекомендации центров ГосСОПКА позволяют делегировать часть своих полномочий или пользоваться услугами друг друга. Так же горизонтальное взаимодействие может быть событийным т. е. единоразовые.

Задачи: Определение состояние защищенности, зоны ответственности

Основные задачи по созданию центров не отличаются от классической работы, связанной с построением проекта по информационной безопасности:

− Определение основных информационных систем и инфраструктур, требующих защиты, и составления перчня;

− Определение модели угроз;

− Определить фактические возможности текущей инфраструктуры и опираясь на модель угроз реализовать защиту;

− Определение инструментов и ресурсов персонала, которые потребуются для реализации защиты.

Однако, несмотря на простоту первичных задач, во многих случаях они сопровождаются большими трудностями. Одним из таких примеров является территориально распределенные сегменты ГосСОПКА, со сложной комплексной инфраструктурой, и выявление каналов выхода в Интернет, и какие сервисы используются за годы существования компании становится достаточно трудоемкой, комплексной задачей.

Также при построении центров стоит учитывать его ежедневные задачи, которые разделены на 4 блока:

1. Управление инцидентами ИБ:
   1.1. Анализ событий ИБ;
   1.2. Обнаружение компьютерных атак;
   1.3. Регистрация инцидентов;
   1.4. Реагирование и ликвидация инцидентов;
   1.5. Поиск причин появления инцидента;
   1.6. Анализ результатов и устранение последствий инцидентов.
2. Анализ защищенности инфраструктуры:
   2.1. Инвентаризация ресурсов;
   2.2. Анализ угроз ИБ.
3. Работа с персоналом:
   3.1. Прием сообщений персонала о возможных инцидентах;
   3.2. Регулярная работа с персоналом, направленная на повышение его квалификации.
4. Информационное взаимодействие с вышестоящим центром.

Подводя итоги стоит отметить, что модель построения центров ГосСАПКА, в которой ключевыми элементами являются ведомственные и корпоративные центры, объединяет специалистов реагирования и расследования компьютерных инцидентов в единое экспертное сообщество, которое обменивается обезличенной информацией об угрозах безопасности. Это в свою очередь повышает ценность вклада каждого из участников взаимодействия в обеспечении общей безопасности всех объектов КИИ, а также позволяет рассчитывать, как на помощь регулятора, так и на помощь других специалистов, имеющих опыт в решении данной проблемы.

Список используемых источников

1. Указ Президента РФ от 15.01.2013г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Собрание законодательства РФ. 21.01.2013. № 3. Ст. 178.

2. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации : утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274.

3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Рос. газета. № 167. 31.07.2017.

4. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. URL: http://kremlin.ru/acts/bank/41460.

5. Указ Президента РФ от 23.01.2015 № 31 «О дополнительных мерах по противодействию незаконному обороту промышленной продукции» // Собрание законодательства РФ. 26.01.2015. № 4. Ст. 643.

6. Кузнецов П. У. Отдельные аспекты формирования правового обеспечения международной информационной безопасности // Вестн. УрФО. 2016. № 4 (22). С. 38–43.

УДК 004.932.2
ГРНТИ 28.23.15

СИСТЕМА РАСПОЗНАВАНИЯ СЖАТЫХ НЕПОДВИЖНЫХ ГРАФИЧЕСКИХ СООБЩЕНИЙ ФОРМАТА JPEG, СОДЕРЖАЩИХ ТЕКСТОВЫЙ КОНТЕНТ

Л. А. Гращенко, А. М. Ревякин, А. В. Скурнович

Академия Федеральной службы охраны Российской Федерации

В статье приводится описание системы распознавания графических сообщений формата JPEG на предмет наличия на изображении электронных копий текстовых документов. В основу предлагаемого решения положен принцип мажоритарного принятия решения по результатам работы трех двухклассовых классификаторов. Рабочий словарь признаков сформирован путем полного перебора 10 нормированных статистических показателей, отражающих частотные особенности изображения. Результаты предварительных испытаний показывают, что предлагаемая система распознавания функционирует с точностью 0,98 и полнотой 0,95.

графическое сообщение, формат JPEG, текстовый контент, частотные характеристики.

Большинством современных программных платформ реализуются стандартные процедуры считывания неподвижных графических сообщений (НГС). В нашем случае неподвижные графические сообщения (НГС) – это информация о графических объектах, передаваемая по каналам связи (телекоммуникационным сетям) или хранящаяся в цифровом виде на машинных носителях информации.

Под сжатыми НГС с текстовым контентом подразумеваются электронные копии текстовых документов, сформированные при помощи цифровых фото или видеокамер, а также с помощью оборудования сканирования. Такие НГС могут передаваться по электронной почте, в мессенджерах и соцсетях в виде файлов популярного на сегодняшний момент формата сжатия цифровых изображений JPEG.

Под распознаванием сжатых НГС в формате JPEG понимается процедура разделения входного массива сжатых НГС на два класса: первый – содержащих текстовый контент (текстовые документы, [1]) и второй –содержащих прочие виды контента (рисунки, графики, пейзажи, портреты и т.д.).

Данная процедура основывается на выработанных решающих правилах системы распознавания, включающей модельное описание НГС [2, 3] и математический аппарат ряда классификаторов с обучением.

Алгоритм распознавания сжатых НГС в формате JPEG, позволяющий различать указанные классы цифровых изображений включает следующие основные этапы:

– вычисление статистических характеристик распознаваемого НГС и формирование вектора признаков рабочего словаря;

– распознавание НГС с применением системы обученных классификаторов.

В целях диверсификации рисков ошибочного принятия решения в результате распознавания объектов только одним обученным классификатором, предлагается реализовывать процедуру распознавания с применением трех классификаторов разного типа. Решение об отнесении НГС к определенному классу принимается по мажоритарному принципу с учетом весовых коэффициентов значимости, вычисляемых на основе значений ошибок первого и второго родов, допущенных классификаторами на этапе их обучения.

Для обучения классификаторов формировалась выборка НГС в количестве 4500 объектов каждого класса. Размер обучающей выборки определялся исходя из требуемых параметров точности и надежности получаемой оценки показателя эффективности обучения. У всех НГС, включенных в обучающую выборку, при помощи автоматического анализатора производится вычисление значений признаков рабочего словаря. Состав и размер рабочего словаря был установлен экспериментально в ходе реализации двухэтапной процедуры отбора потенциально информативных признаков из числа признаков априорного словаря [4].

В априорный словарь признаков вошли следующие статистические характеристики НГС:

1) центральные моменты μ порядка s (s = 2..10), вычисляемые из распределений коэффициентов ДКП сжатых НГС формата JPEG:

$$\mu^{(s)} = \frac{1}{n}\sum_{i=1}^{n}\left(x_i - \overline{x}_в\right)^s, \qquad (1)$$

где s – порядок центрального момента,

n – количество коэффициентов ДКП составляющей Y цветовой схемы YCrCb (исключая DC-коэффициенты и *AC*-коэффициенты ДКП со значением 0, 1 и −1),

x_i – значение i-го *AC*-коэффициента ДКП,

$x_в$ с чертой – выборочное среднее всех выбранных *AC*-коэффициентов.

2) Отношение *r* количества DC-коэффициентов ДКП, значения которых изменяются с наиболее частого значения на большее или меньшее, к общему количеству DC-коэффициентов составляющей *Y* цветовой схемы YCrCb.

Далее все полученные значения признаков для всех объектов обучающей выборки подвергались нормированию.

При формировании рабочего словаря критерием информативности признаков при их отборе с помощью каждого отдельного классификатора принимается *F*-мера [5].

Наилучшим вариантом признакового пространства признается тот набор признаков (та структура вектора), которому соответствовало максимальное значение *F*-меры.

Для создания системы распознавания применялись три классификатора – Байеса (КБ), основанный на линейном дискриминантном анализе (ЛДА) и на основе метода опорных векторов (МОВ) с радиальной базисной функцией. Выбор в пользу перечисленных классификаторов был сделан на основе анализа их возможностей по решению задачи двухклассового распознавания, а также с учетом исходных данных и условий реализации этапов обучения и распознавания.

Классификатор Байеса, в случае если признаки распределены по нормальному закону, дает минимум значения условного среднего риска при классификации, однако по условию решаемой задачи требуется снизить количество ложно-положительных решений, что на практике при использовании только байесовского классификатора затруднительно. Поэтому для того чтобы минимизировать вероятность ложной тревоги при заданном значении вероятности правильного распознавания наряду с Байесовским правилом необходимо использовать другие методы распознавания.

В качестве дополнительного классификатора, наряду с КБ, в предлагаемой системе распознавания используется математический аппарат линейного дискриминантного анализа.

Классификатор ЛДА относит объект распознавания, представленный вектором *X*, к одному из заданных классов, по сформированному на этапе обучения прогностическому правилу. В [6] приводиться доказательство теоремы о том, что оптимальным линейным прогностическим правилом является то правило, вид разделяющей функции которого задается следующим выражением:

$$Y(X) = V^{-1}(\overline{X}^{(1)} - \overline{X}^{(2)}) \times (X - \frac{1}{2}(\overline{X}^{(1)} + \overline{X}^{(2)})), \qquad (3)$$

где $X^{(k)}$ с чертой – вектор средних нормированных значений признаков объектов обучающей выборки k-го класса;

k = 1, 2;

V – оценка ковариационной матрицы, которая вычисляется как:

$$V = \frac{1}{n_1 + n_2 - 2}(\hat{X}'^{(1)T}\hat{X}'^{(1)} + \hat{X}'^{(2)T}\hat{X}'^{(2)}), \quad (4)$$

где n_1 и n_2 – количество сжатых НГС в формате JPEG в соответствующих парах классов в обучающей выборке;

$\hat{X}'^{(k)}$ – двумерные массивы, у которых по строкам расположены значения признаков объектов k-го класса, вычисленных в соответствии с выражением (7):

$$\hat{X}'^{(k)} = \vec{X}'^{(k)} - \overline{X}_j'^{(k)},\ j = 1,\ldots,n_k,\ k = 1,2, \quad (5)$$

где $\vec{X}'^{(k)}$ – массив значений признаков объектов k-го класса из обучающей выборки;

$\overline{X}_j'^{(k)}$ – массив, у которого по столбцам расположены средние значения признаков k-го класса.

Таким образом, для поступившего объекта X по формуле, определяемой выражением 5, вычисляется значение линейной разделяющей функции $Y(X)$. Если $Y(X) \geq 0$, то классификатор относит анализируемый объект к классу сжатых НГС в формате JPEG, содержащих текстовый контент, в противном случае при $Y(X) < 0$ объект признается принадлежащим к другому классу.

В качестве третьего классификатора в разработанной системе распознавания использовался МОВ с радиальной базисной функцией Гаусса. Применение именно данного классификатора из существующих систем распознавания на основе МОВ эффективно с позиций двух параметров: точности классификации и времени, затрачиваемого на процедуры обучения и принятия решения.

Алгоритм МОВ в общем случае будет задаваться выражением:

$$a(x) = sign\left(\sum_{j=1}^{n}\omega_j x^j - \omega_0\right) = sign\left(\langle\omega, x\rangle - \omega_0\right), \quad (6)$$

где $x = \left\{x^1,\ldots,x^n\right\}$ – признаковое описание объекта x, а вектор $\omega = (\omega^1,\ldots,\omega^n) \in R^n$ и скалярный порог $\omega_0 \in R$ являются параметрами алгоритма классификации. При этом для построения алгоритма распознавания используется нелинейный пороговый классификатор, а классификатор с

определенным типом ядра, в качестве которого выступает радиальная базисная функция Гаусса:

$$K\left(x_i, x\right) = \exp\left(-\beta\left\|x_i - x\right\|^2\right), \tag{7}$$

где β – параметр алгоритма, подбираемый экспериментально, а функция $K(x_i, x)$ вычисляет оценку близости объекта x к опорному вектору x_i.

На основе исходных данных алгоритма, полученных в процессе сбора и анализа априорной информации, осуществляется процедура обучения описанных выше классификаторов, при этом объем обучающей выборки должен рассчитываться исходя из требуемых значений точности и надежности получаемых статистических оценок.

Для каждого из используемых классификаторов по итогам их обучения рассчитывается величина F_{1i}-меры. По завершению этапа обучения, для классификаторов вычисляются значения их весовых коэффициентов значимости согласно выражению:

$$c_{знач.i} = 1 - \frac{F_i}{\sum_{i=1}^{K} F_i}, \tag{8}$$

где K – количество классификаторов, используемых в системе распознавания.

Весовые коэффициенты значимости являются вспомогательными коэффициентами, которые используются на этапе распознавания сообщений для реализации принятия решения по мажоритарному принципу.

По результатам классификации каждый из классификаторов вычисляет значение коэффициента принадлежности сообщения к одному из заданных классов:

$$\alpha_i = \begin{cases} -1, & \textit{если НГС содержит текстовый контент} \\ 1, & \textit{если НГС не содержит текстовый контент} \end{cases}, \tag{9}$$

После процедуры классификации, на основе рассчитанных значений коэффициентов принадлежности α_i выражение (9), а также весовых коэффициентов значимости $c_{знач.i}$ выражение (8), рассчитанных на этапе обучения классификаторов, вычисляется мажоритарная сумма:

$$S = \sum_{i=1}^{K} \alpha_i c_{знач.i}, \tag{10}$$

где K – количество используемых классификаторов.

Правило распознавания сообщений, в случае использования мажоритарной суммы (10), формулируется следующим образом: если значение мажоритарной суммы $S \geq 0$, то анализируемое сжатое НГС в формате JPEG признается не содержащим текст (текстовый документ), в противном случае сообщение признается содержащим текстовый документ.

При помощи разработанного специализированного ПО (№ 2018618022 в Реестре программ для ЭВМ) с использованием выборки сжатых НГС в формате JPEG двух классов, в которую вошли 1000 экземпляров электронных копий текстовых документов и 1 000 экземпляров цифровых фото пейзажей и мультипликационной цифровой графики, тестирование разработанной системы показало результат распознавания с точностью 0,98 и полнотой 0,95.

Список используемых источников

1. ГОСТ 2.105-95 Межгосударственный стандарт. Общие требования к текстовым документам.

2. Ревякин А. М. Подходы к разработке модели распознавания сжатого неподвижного графического сообщения формата JPEG // Современные проблемы физико-математических наук: материалы III междун. научно-практ. конф., Орел, 23–26 нояб. 2017 г. Орел : ОГУ, 2017. С. 357–362.

3. Ревякин А. М., Скурнович А. В., Иванов В. А. Модель системы обнаружения текстового контента в неподвижных графических сообщениях формата JPEG. // Наука и Технологии : журнал «Телекоммуникации». 2018. № 11. С. 30–35.

4. Дуда Р., Харт М. Распознавание образов и анализ сцен / пер. с англ. под редакцией Стефанюка В. Л. М.: Мир, 1976. 511 с.

5. Баженов Д. Оценка классификатора (точность, полнота, F-мера) [Электронный ресурс] // Суровая реальность. 2012. URL: http://www.bazhenov.me/blog/2012/07/21/ classification-performace-evaluation. (Дата обращения: 18.12.2018).

6. Дубров А. М., Мхитарян В. С., Трошин Л. И. Многомерные статистические методы. М.: Финансы и статистика, 2003. 352 с.

7. Скурнович А. В., Стельмах Э. П., Молчанов А. Н., Молчанов И. Н. Способ распознавания текстовой информации и оценки ее полноты в электронных документах сети Интернет. Пат. 2550543 Российская Федерация; заявитель и патентообладатель ГКОУ ВПО Академия ФСО России. – № 2013155172/08; заявл. 11.12.13; опубл. 10.05.15.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом А. В. Скурновичем.

УДК 004.58
ГРНТИ 20.01.04

МЕТОДЫ ПРОЕКТИРОВАНИЯ ИНТЕРФЕЙСА ОБРАЗОВАТЕЛЬНОЙ ПЛАТФОРМЫ НА БАЗЕ UX И UI ДИЗАЙНА

К. В. Григоренко, Л. П. Козлова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В контексте взаимодействия с человеком, пользовательский интерфейс является ключевой точкой коммуникации между пользователем и программным обеспечением компьютера. Результат данного взаимодействия зависит от дизайна пользовательского интерфейса, который, в свою очередь, играет приоритетную роль в разработке образовательного программного обеспечения. Принципы и концепции проектирования интерфейса следует рассматривать в неотъемлемой связке с проектированием пользовательского опыта.

пользовательский интерфейс, пользовательский опыт, проектирование пользовательского интерфейса, интерфейс образовательной платформы.

Пользовательский интерфейс является точкой взаимодействия между пользователем и программным обеспечением компьютера, успех которого зависит во многом от дизайна пользовательского интерфейса. Пользовательский интерфейс играет важную роль в разработке образовательного программного обеспечения для электронного обучения.

Одним из актуальных вопросов является создание адаптированного пользовательского интерфейса для электронного обучения. Усвоение информации и обучаемость зависят не только от материала и способностей учащегося, но и соответствующим образом разработанного программного обеспечения.

Пользовательский интерфейс, созданный без учёта нужд пользователей, вынуждает совершать ошибки, усложняет достижение целей, также может терять необходимую функциональность и вызывать отторжение, что влечёт за собой отказ от использования. Проектирование необходимо начинать с понимания предполагаемых пользователей, включая их возраст, особенности восприятия, образование, культурные ценности, мотивацию, цели и особенности личности. Таким образом, разработка специального профиля для пользовательского интерфейса позволяет сконцентрироваться на решении определённых задач посредством программного обеспечения.

Процесс проектирования пользовательского интерфейса включает в себя четыре основных действия:

- анализ и моделирование пользователя, задачи и среды;
- создание дизайна интерфейса;
- внедрение интерфейса;
- проверка интерфейса.

Рисунок. Процесс проектирования пользовательского интерфейса

Процесс проектирования дизайна пользовательского интерфейса имеет цикличный характер в процессе создания программного обеспечения (рис.), т. к. интерес пользователей, уровень их квалификации, появление новых технологий и стремление к разнообразию ведут к растущему спросу, что провоцирует необходимость внесения изменений и цикличного характера разработки.

Этап анализа включает в себя следующие шаги:

- исследование всех возможных пользовательских стратегий;
- уменьшение нагрузки на память и восприятие пользователя;
- формирование последовательной логики прототипа интерфейса.

Знание факторов, влияющих на преподавание и обучение, позволит разработчику принимать обоснованные решения в процессе создания интерфейса и курса. Следует анализировать факторы, влияющие на преподавание и обучение, которые связаны с пользовательским интерфейсом.

Педагогические стимулы могут представлять собой мотивирование или принуждение. Системы электронного обучения должны быть спроектированы таким образом, чтобы чувство потребности и мотивации постоянно росло, а чувство принуждения уменьшалось.

Далее приведены некоторые возможности интерфейса для повышения вовлеченности в системах электронного обучения.

Использование голосовых элементов интерфейса способствует росту чувству доверия и заинтересованности [1]. Конкретный тип голоса может влиять на то, насколько учащимся нравится оратор и насколько усердно они пытаются понять представленный материал. Учащиеся дали более положительные оценки интерфейсу, который сопровождается человеческим голосом, а не синтезированным [2].

Речь и текст должны быть представлены в неформальном стиле, рекомендуется использовать местоимения от первого лица и от второго лица вместо местоимений от третьего лица. Исследования показывают, что вовлечение в интерактивный разговор с другими способствуют усваиванию информации [3].

Использование различных цветовых схем важно для группировки и акцентирования информации, помимо интерфейсных решений. Следует отметить, что при использовании более 10 цветов восприятие информации затрудняется. Правильное использование цветов ускоряет просмотр. В интерфейсе необходимо свободное пространство, вносящее элемент упорядоченности и структурирования информации. Использование тёмного текста на светлом фоне ускоряет чтение [4].

Стратегия контроля обучающихся стала более ценной, чем контроль преподавателей или программ. В настоящее время используемые стратегии управления учащимся концентрируются на выборе тем и распределении контента, выборе учебных компонентов и контроле взаимодействия между учеником и преподавателем [5].

Фоновая музыка может поспособствовать обучению посредством влияния на настроение, увеличения концентрации, а также отвлечения от шума [6]. При выборе фоновой музыки следует учитывать, что прослушивание музыки создаёт дополнительную когнитивную нагрузку.

В электронных курсах неуместные визуальные эффекты должны быть сведены к минимуму, фоновая музыка и шумные звуки должны быть удалены, а также должен использоваться четкий, лаконичный и соответствующий текст. Таким образом, устранение ненужной информации приводит к снижению когнитивного давления, что даёт больше возможностей для обработки [7].

Электронные курсы должны включать практические занятия с разбором в примерах и упражнениях. Форма и внешний вид образовательной среды должны основываться на фактической среде, в которой учащиеся в конце курса должны представить полученную информацию. Рекомендуется использовать учебные материалы, включающие комбинацию визуальных и слуховых элементов.

Следует избегать следующих решений в формировании интерфейса и подаче материала:

- отсутствие изображения при необходимости представления наглядного примера;
- слишком высокая скорость воспроизведения обучающего материала;
- некачественное звуковое сопровождение курса;
- отсутствие гибкости интерфейса.

Учащиеся должны иметь доступ к уже изученному контенту. Всякий раз, когда слова или фразы, которые используются в тексте, пересекаются с учебным материалом, они должны действовать как ссылки для навигации, описания или возврата пользователя на предыдущую страницу.

Дизайн пользовательского интерфейса являет собой не только художественный феномен, но и ключевой инструмент во взаимодействии человека с технологией. В процессе проектирования дизайна пользовательского интерфейса следует проводить предварительный анализ целевой аудитории и включать специальные технологии, в случае сферы электронного обучения – способствующие достижению образовательных целей.

Список используемых источников

1. Wang, N. et al. The politeness effect: Pedagogical agents and learning outcomes // International journal of human-computer studies. 2008. Vol. 66. No. 2. Pp. 98–112.

2. Atkinson, R. K., Mayer, R. E., Merrill, M. M. Fostering social agency in multimedia learning: Examining the impact of an animated agent's voice // Contemporary Educational Psychology. 2005. Vol. 30. No. 1. Pp. 117–139.

3. Beck, I. L. et al. Questioning the author: A yearlong classroom implementation to engage students with text // The Elementary School Journal. 1996. Vol. 96. No. 4. Pp. 385–414.

4. Sklar, J. Principles of web design: the web technologies series. Cengage Learning, 2011.

5. Li, X., Soh, L. K. A literature review on learner control strategies in software tutoring systems // CSE Technical reports. 2003. 71 p.

6. Griffin, M. Background Music and the Learning Environment: Borrowing from other Disciplines // Online Submission. 2006.

7. Clark, R. C., Mayer, R. E. E-learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning. John Wiley & Sons, 2016.

УДК 536.9
ГРНТИ 29.35.19

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ ПРИБЛИЖЕНИЯ ПРИ ИССЛЕДОВАНИИ РАССЕЯНИЯ СВЕТА В НЕОДНОРОДНОЙ СРЕДЕ

Л. А. Груздева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрено применение методов приближения при решении уравнения переноса для сред с различными показателями анизотропии. Строгие методы решения уравнения переноса. Менее точный метод, метод Монте-Карло. Приближение однократного рассеяния. Приближение двукратного рассеяния. Диффузное приближение для случаев изотропной среды. Малоугловое приближение для однородных сред. Распространение короткого ограниченного импульса в неоднородной среде (малоугловое приближение).

уравнение переноса, однократное рассеяние, двукратное рассеяние, диффузное приближение, малоугловое приближение, метод Морте-Карло.

Все среды, где возможно распространение оптических сигналов,-атмосфера, вода, космическое пространство -имеют локально неоднородную структуру (загрязнения воды и воздуха, тепловые флуктуации параметров сред, космическая пыль), что приводит к рассеянию и поглощению света при его распространении в глубь среды.

В оптическом диапазоне длин волн наличие неоднородностей среды вызывает значительную пространственную диффузию световой энергии в направлении от оси излучения. Для коллимированного источника света в удалении от излучателя световой пучок расплывается в пространстве. Это приводит к дополнительному ослаблению световой энергии на оси пучка и ухудшению угловой разрешающей способности локатора.

Физическое состояние среды, в особенности характеристики ее неоднородностей, в сильной степени влияют на характеристики световых полей.

Поглощение света связано с диссипацией энергии поля, вызванной переходом ее в другие виды энергии, например, в тепловую и химическую. В некоторых случаях важную роль в поглощении света играют также процессы фотосинтеза в биологических организмах, взвешенных в среде. Характерной особенностью распространения электромагнитных волн в неоднородной среде является множественность последовательных актов рассеяния –каждая из неоднородностей порождает вторичную волну, кото-

рая сама испытывает рассеяние, то есть создает последующие волны от других неоднородностей, что в сильной степени усложняет анализ характеристик поля. При малых объемах среды характеристики светового поля в основном обусловлены падающей и однократной рассеянной волнами, энергия которых значительно превышает энергию многократно рассеянных волн вследствие малости амплитуды вторичного рассеяния. При анализе локальных рассеивающих свойств среды допустимо рассматривать только однократное рассеяние.

При рассмотрении в малом объеме среды рассматриваются два параметра: коэффициент рассеяния объема, связан с суммарной величиной энергии, рассеянной по всем направлениям и индикатриса рассеяния, которая определяет относительное распределение энергии в зависимости от углового направления.

Поглощение определяется только коэффициентом поглощения, связанным с полной величиной потерь световой энергии в объеме среды.

Причиной рассеяния электромагнитных волн является неоднородность электрических свойств среды. Для волн оптического диапазона существенны неоднородности, вызванные тепловыми флуктуациями плотности вещества, флуктуациями ориентации молекул и вкрапления некоторых посторонних образований (различные виды аэрозолей в воздухе, частички пыли в космическом пространстве, загрязнения и биологические организмы в воде).

Рассеяние электромагнитных волн в оптической локации играет определяющую роль.

Определение характеристик светорассеяния в больших объемах среды, которое производится при анализе структуры световых полей в оптической локации делается на основе использования данных о локальных свойствах рассеяния и поглощения. Ослабление светового пучка при распространении в среде происходит вследствие поглощения и рассеяния. В соответствии с этим, коэффициент ослабления Ɛ является суммой двух коэффициентов – коэффициента рассеяния б и коэффициента поглощения К: $\varepsilon = б + К$.

Все три коэффициента имеют размерность обратной длины. Коэффициент ослабления ε морской воды в спектральной области минимального ослабления для различных акваторий лежит в пределах 0,12 ÷ 1,4 м-1. Коэффициент рассеяния б может составлять 60 ÷ 90 % от величины Ɛ, при этом зависимости между б и отношением $\mu = б / \varepsilon$ для различных районов не обнаруживается. В вертикальном направлении морская вода является неоднородной. Коэффициенты ε и б являются функциями глубины *z*.

Рассеяние в воде обусловлено, главным образом, частицами крупных размеров (P >> **1**). Энергетическая характеристика светового поля- интенсивность излучения I является удобной для использования в теории светорассеяния применительно к задачам оптической локации. При описании

светового поля через интенсивность излучения не учитываются волновые свойства света. Это описание соответствует физической модели, где рассматривается рассеяние частиц на хаотически расположенных в среде рассеивающих центрах. Эволюция системы частиц в такой модели описывается уравнением переноса излучения. Теория переноса, не являясь строгой в математическом отношении, позволяет исследовать случайно-неоднородную среду. Основными величинами, используемыми в теории, являются лучевая интенсивность, поток, плотность энергии и средняя интенсивность. Общий вид уравнения переноса имеет вид:

$$\frac{I}{C}\frac{\partial I(\mathrm{r},S,t)}{\partial t} + I\nabla(\mathrm{r},S,t) + \mu I(\mathrm{r},S,t) = \mathrm{r_p}\int I(\mathrm{r},S\,t)p(S,S')dS' + S(\mathrm{r},S,t), \quad (1)$$

где $I(r,\mathrm{S},\mathrm{t})$ – лучевая интенсивность, равная мощности, которая может быть принятой из бесконечно малого телесного угла ΔS приемником с бесконечно малой апертурой Δa, находясь в точке r в частотном диапазоне (v, v+Δv) при $\Delta v \to 0$;

μ – коэффициент ослабления экстинкции);

$\mathrm{r_p}$ – коэффициент рассеяния; C-скорость света в среде.

Уравнение переноса является сложным, поэтому при его решении зачастую прибегают к различным приближениям: – диффузное приближение; – малоугловое приближение.

В диффузном приближении предполагается, что диффузная волна взаимодействует с большим числом частиц и рассеивается почти изотропно и угловое распределение диффузной интенсивности также изотропно. Но угловая зависимость не может отсутствовать полностью, так как в этом случае поток $\overline{F}$ был бы равен нулю и не было бы переноса энергии.

Математически диффузная интенсивность в диффузном приближении описывается формулой [1]

$$I_d(\overline{\mathrm{r}},\widehat{S}) = U_d(\overline{\mathrm{r}}) + \frac{3}{4\pi}\overline{F}_d(\overline{\mathrm{r}})\,\hat{S}, \quad (2)$$

где U_d – средняя интенсивность,

$\overline{F}_d$ – вектор потока.

Формулу (2) можно рассматривать как первые два члена разложения в ряд Тейлора по степеням *cos* Θ, где Θ – угол между $\overline{F}$ и $\hat{S}$,и, следовательно, второе слагаемое в формуле должно быть значительно меньше первого:

$$U_d >> |\overline{F}_d|.$$

После подстановки (2) в уравнение переноса, можно получить стационарное уравнение диффузии для средней диффузной интенсивности U_d.

Однократное рассеяние и двукратное приближение

Для однородных сред получено три выражения для мощности отраженного сигнала: два в малоугловом приближении и в диффузном приближении Применимы к большинству практических задач ввиду относительной простоты их аппарата. Однако эти методы могут быть использованы только для небольших оптических глубин. Желательно использование этих методов в сочетании с другими, дающими более точный результат при больших τ и применимых на малых оптических глубинах (например, метод диффузионного приближения).

Многократное рассеяние

Теорию многократного рассеяния в первом приближении можно сформулировать на основе уравнения радиолокации или на языке лучевой интенсивности. Уравнение радиолокации для мощности P_r, рассеянной случайно частицами, дается формулой:

$$\frac{P_r}{P_t} = \int_V \frac{\lambda^2}{(4\pi)^3} \frac{G_t(\hat{i}) G_r(\hat{O})}{R_1^2 R_2} P < 6_{bi}(\hat{O}, \hat{i} > exp(-\tau_1 - \tau_2) dV_t, \qquad (3)$$

где P_t излученная мощность, а G_t и G_r коэффициент усиления передатчика и приемника соответственно. Смысл величин R_1 и R_2 ясен.

Теория многократного рассеяния верна, если интенсивность диффузного рассеяния мала по сравнению с затухающей интенсивностью падающего излучения. Это условие выполняется в двух случаях:

1. Для плоской волны, падающей на облако случайно распределенных частиц, эта теория верна, когда оптическая толщина облака частиц не превышает примерно 0,4 (τ < 0,4), а частицы в основном поглощающие (альбедо Wo $\lesssim$ 0,5).

2. Для волн, сосредоточенных в узком конусе, например, эта теория применима при значительно больших расстояниях, особенно, если частицы поглощающие (Wo $\lesssim$ 0,9). Такая ситуация возникает при распространении волн СВЧ-диапазона в дожде и в радиолокационных приложениях.

Метод Монте-Карло

Так как точного решения уравнения переноса в общем виде нет поэтому невозможно точно описать распространение света в случайно-неоднородной среде, однако, метод Монте-Карло позволяет учесть особенности

среды. Он заключается в компьютерном моделировании процесса распространения света в неоднородных средах. Метод Монте-Карло – менее точный метод, но он позволяет описывать принимаемые сигналы с достаточно высокой степенью точности, но применение его также сопряжено с большими вычислительными трудностями, что позволяет использовать его для небольших оптических глубин ($\tau <= 10$), а также использование этого метода может вести к неконтролируемым ошибкам в расчетах. Оперативное применение метода Монте-Карло невозможно из-за большого времени на расчет каждого сигнала. Возможно применение этого метода для оценки точности расчета по другим методам.

Выводы

Строгие методы решения уравнения переноса, позволяющие точно описать сигнал обратного рассеяния сопряжены с большими вычислительными трудностями и недостаточно разработаны на данный момент. Менее точный метод Монте-Карло позволяет описывать принимаемые сигналы с достаточно высокой степенью точности, но применение его также сопряжено с большими вычислительными трудностями, что позволяет использовать его для небольших оптических глубин ($\tau <= 10$), а также использование данного метода может вести к неконтролируемым ошибкам в расчетах [2]. Оперативное применение метода Монте-Карло невозможно из-за большого времени на расчет каждого сигнала. Возможно применение этого метода для оценки точности расчета по другим методам [3].

Методы однократного и двукратного приближения могут быть использованы только для небольших оптических глубин. Желательно использование этих методов в сочетании с другими, дающими более точный результат при больших τ и применимых на малых оптических глубинах (например, метод диффузионного приближения). Для однородных сред получены три выражения для мощности отраженного сигнала: два в малоугловом приближении и в диффузном приближении.

Для дальнейшей работы можно упростить рассмотренные выше выражения если рассматривать совмещенные излучатель и приемник с параллельными оптическими осями.

Список используемых источников

1. Исимару А. Распространение и рассеяние волн в случайно-неоднородных средах. М.: Мир,1981. 281 с

2. Метод Монте-Карло в проблеме переноса излучения / Сб. под ред. Г. И. Марчука. М.: Атомиздат, 1967.

3. Креков Г. М. и др. Об алгоритмах метода Монте-Карло для решения задач теории распространения узких пучков света // Известия вузов. Физика. 1968. № 5.

*Статья представлена заведующим кафедрой,
доктором технических наук, профессором Д. В. Волошиновым.*

**УДК 004.75
ГРНТИ 50.53.17**

РАЗРАБОТКА МАКЕТА И МЕТОДИКИ КОНФИГУРИРОВАНИЯ МОДУЛЯ ИНТЕЛЛЕКТУАЛЬНОЙ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ НА БАЗЕ СВОБОДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Е. В. Грушевая, С. М. Макеев

Академия Федеральной службы охраны Российской Федерации

В работе рассматривается результат работы по разработке макета и методики конфигурирования модуля интеллектуальной обработки больших данных на базе свободного программного обеспечения. Представлена структурная схема макета, а также последовательность действий по настройке модуля интеллектуальной обработки больших данных, которая позволяет снизить количество ошибок при настройке.

большие данные, Apache Spark, кластер Apache Hadoop, методика настройки.

Объемы обрабатываемых данных во всех областях человеческой деятельности продолжают расти быстрыми темпами. Для обработки больших данных традиционные средства оказались не эффективными [1]. Для решения данной проблемы сообществом программистов был создан специализированный фреймворк Apache Spark – универсальная и высокопроизводительная вычислительная платформа, которая способна молниеносно обрабатывать различные форматы данных и имеющая простой *API* интерфейс на языках Python, Java, Scala, SQL [2]. Apache Spark имеет достаточно простую структуру, представленную на рис. 1.

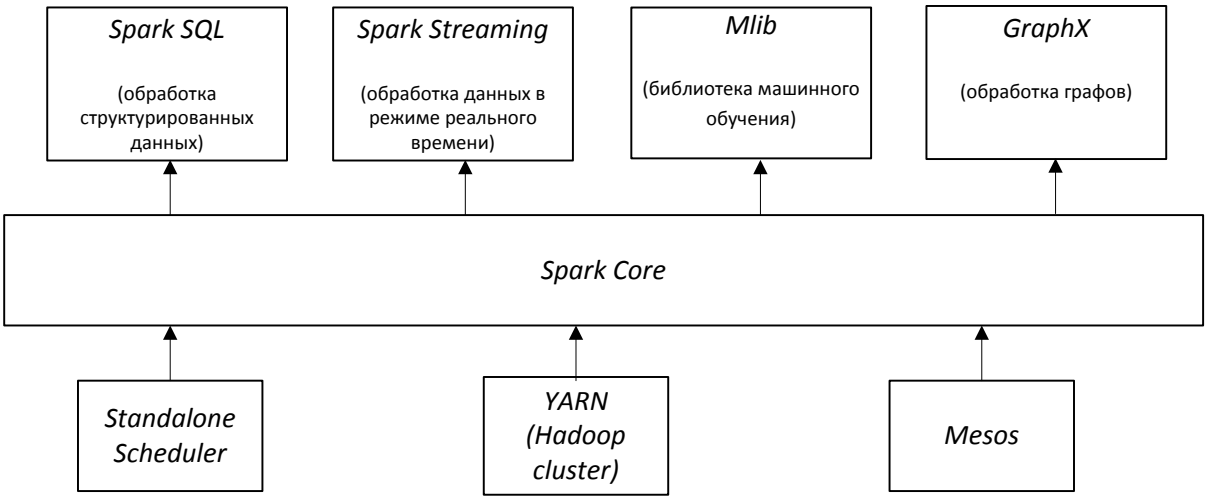


Рис. 1. Структурная схема Apache Spark

Основным компонентом, реализующим управление фреймфорком, является Spark Core. В его основные функции входит осуществление планирования заданий, управление памятью, обработка ошибок, взаимодействие с системами хранения данных, например, HDFS. Также Spark Core обеспечивает взаимодействие с диспетчерами кластера такими, как Hadoop YARN, Mesos, Standalone Scheduler, которые позволяют организовать эффективное горизонтальное масштабирование вычислительного кластера от одного узла до многих тысяч узлов [2].

Для обработки больших данных в состав Apache Spark входит достаточно большое количество инструментов таких, как Spark SQL, Spark Streaming, MLlib, GraphX. Spark SQL – это пакет для работы со структурированными данными. Он позволяет извлекать данные с помощью инструкций на языке SQL. Spark Streaming- это компонент для обработки потоковых данных (файлы журналов веб-серверов, очереди сообщений, посылаемых пользователями веб-служб). MLlib – это библиотека, реализующая механизмы машинного обучения. GraphX – это библиотека обобщенных алгоритмов работы с графами [3].

В рамках исследования был разработан макет, состоящий из трех вычислительных узлов: один управляющий узел или Hadoopmaster, два рабочих узла, HadoopSlave1 и HadoopSlave2 соответственно. Все узлы реализованы в виде виртуальных машин с операционной системой Ubuntu-Server 14.04. В качестве вычислительной платформы использовался кластер Apache Hadoop, поверх которого был установлен фреймворк Apache Spark. Также в рамках макета используется распределенная файловая система HDFS. В качестве диспетчера кластера был выбран Hadoop YARN, так как он входит по умолчанию в состав кластер Apache Hadoop. Для интеллекту-

альной обработки больших данных в стенде была настроена специализированная библиотека машинного обучения MLlib [4]. На рис. 2 представлена структурная схема макета.

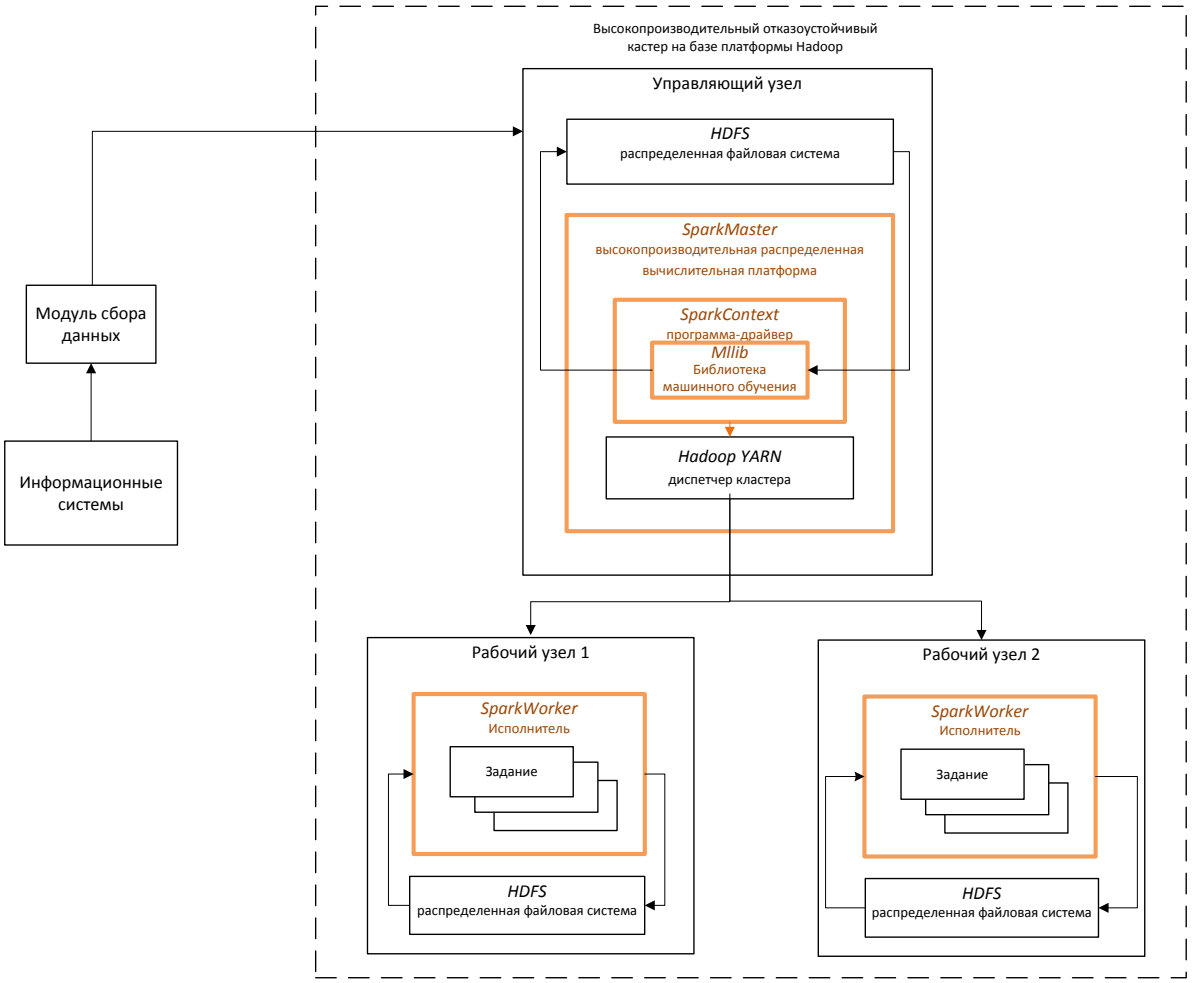


Рис. 2. Структурная схема макета

Общая последовательность действий при разработке макета представлена на рис. 3. Установка и настройка модуля сбора и файловой системы HDFS в данной работе не рассматриваются.

На первом этапе происходит установка и настройка узлов кластера Apache Hadoop. На втором этапе на готовый кластер устанавливается Apache Spark [5]. Этап настройки подробнее представлен на рис. 4.

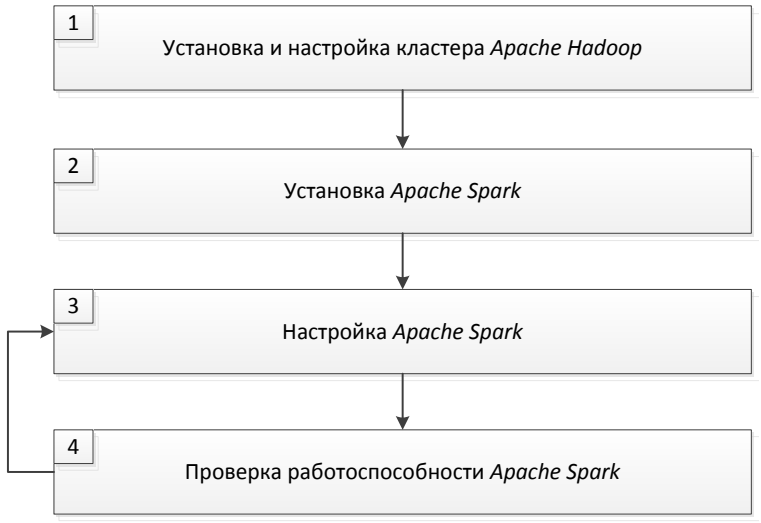


Рис. 3. Алгоритм установки макета

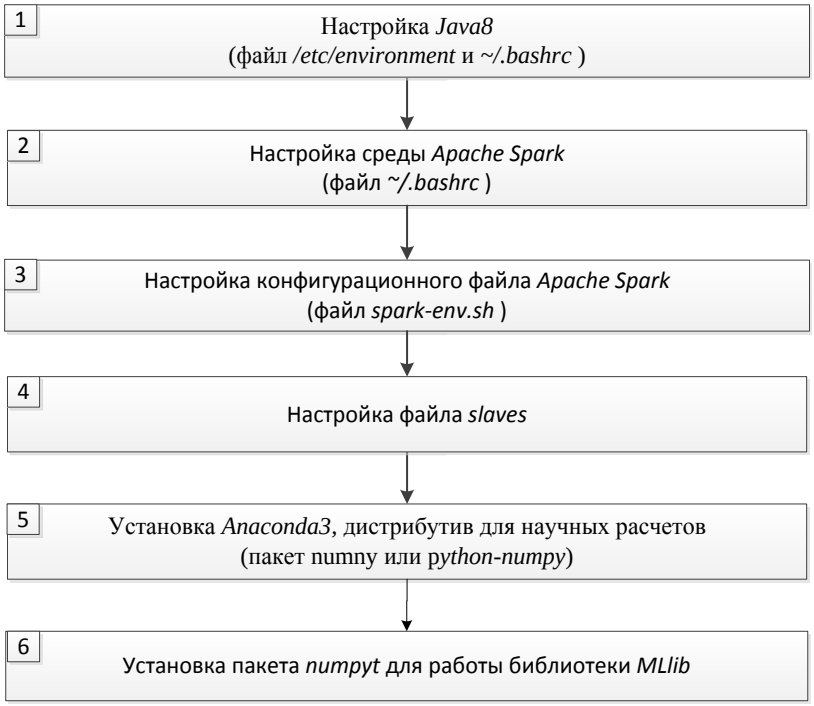


Рис. 4. Алгоритм настройки Apache Spark

После настройки фреймворка проверяется его работоспособность. Это можно сделать с помощью команды jps. При наличии записей на управляющем и рабочих узлах, представленных на рис. 5, Apache Spark готов к работе [5].

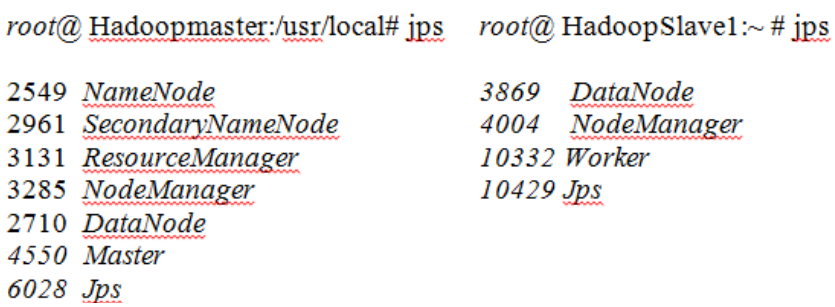


Рис. 5. Проверка работоспособности Apache Spark

Таким образом, в результате исследования был разработан макет кластера для обработки больших данных, состоящий из трех узлов, управляющего и двух рабочих. На основе созданного стенда была также разработана методика по конфигурированию модуля интеллектуальной обработки больших данных, позволяющая снизить количество ошибок при настройке модуля интеллектуальной обработки больших данных неподготовленным пользователем.

Список использованных источников

1. Vorobiev, A. A., Makeev, S. M., Grushevaya, E. V., Mysin, O. D., Shnibaev, V. V. Method of configuring modules for collection, storage and processing of big data on the basis of free software // Modern informatization problems in the technological and telecommunication systems analysis and synthesis (MIP-2019’AS): Proceedings of the XXIVth International Open Science Conference (Yelm, WA, USA, January 2019) / Editor in Chief Dr. Sci., Prof. O. Ja. Kravets. Yelm, WA, USA: Science Book Publishing House, 2019. Pp. 382–387.

2. Холден Карау Изучаем Spark. Молниеносный анализ данных. М.: ДМК пресс, 2015. 304 с.

3. Официальный сайт разработчиков Spark: работа с библиотекой MLlib [Электронный ресурс]. URL: https://spark.apache.org/docs/latest/mllib-feature-extraction.html

4. Настройка мини кластера *Apache Spark* [Электронный ресурс]. URL: http://blog.ditullio.fr/2015/10/24/mini-cluster-part-iii-hadoop-spark-installation

УДК 004.85
ГРНТИ 28.23.25

ИЗМЕРЕНИЕ КОЛМОГОРОВСКОЙ СЛОЖНОСТИ ДВОИЧНЫХ СТРОК НА БАЗЕ АВТОЭНКОДЕРОВ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Автоэнкодеры являются популярными моделями обучения, потому что они концептуально просты, легки в обучении и обеспечивают эффективный код. Данная работа показывает, как можно получить значимую оценку некоторой совокупности данных в виде двоичных строк, которая измеряет, насколько хорошо автоэнкодер может представлять эти данные.

автоэнкодер, колмогоровская сложность, нейронные сети, модели обучения.

Колмогоровская сложность двоичной строки x определяется как длина самой короткой программы, которая вычисляет x:

$$K(x) = \min \{l(p): U(p) = x\},$$

где p – программа,

$l(p)$ – длина этой программы,

U – универсальная машина Тьюринга U.

Очевидно, что строки с простой регулярной структурой имеют низкую колмогоровскую сложность. Например, строка 1010…10 длиной два миллиона, содержит мало информации, поскольку может быть вычислена весьма короткой программой:

for i = 1 to 1000000 **print** (10).

С другой стороны, если мы рассмотрим длинную нерегулярную случайную строку 111010110000010 ... , тогда гораздо труднее найти короткую программу, которая выводит эту строку. Причем, можно доказать, что в общем случае длинные случайные строки не могут генерироваться короткими программами и, следовательно, они имеют высокую колмогоровскую сложность.

Важным свойством K является то, что она практически не зависит от выбора конкретной машины Тьюринга U. Действительно, возьмем в приведенном выше определении K некоторую другую универсальную машину

Тьюринга U'. Поскольку U' универсальна, существует программа q, которая позволяет U' моделировать U:

$$U'(q)\,(p) = U(p).$$

Отсюда следует, что использование U' вместо U в определении колмогоровской сложности K выше влечет за собой дополнительную сложность в виде константы $l(q)$ бит, причем эта константа не зависит от сложности строки x, которую мы измеряем, и для универсальных машин Тьюринга эта константа будет мала. Это свойство инвариантности делает K удобной универсальной мерой сложности любых двоичных строк [1].

Несмотря на то, что невозможно гарантировать абсолютный минимум найденной с помощью некоторой программы сложности, важно иметь достоверный инструмент для сравнения сложности строк x_i и x_j одинаковой длины.

Пусть некоторая программа p позволяет вычислять строку x_i, при использовании некоторой исходной строки x_i' в качестве входного аргумента, а также строку x_j, при использовании входного аргумента x_j'. Если строки x_i' и x_j' имеют одинаковую длину, то можно утверждать, что сложности строк x_i и x_j совпадают.

Поставим задачу определения класса строк $X = \{x_1, x_2, \ldots, x_n\}$ одинаковой длины, имеющих одинаковую сложность. Для решения этой задачи необходимо разработать такую программу p, которая при заданном входном аргументе x_i' вычисляет строку x_i из X.

Для разработки программы используем автоэнкодер, который осуществляет последовательное применение функции кодера $x' = f(x)$ и декодера $x* = g(x')$, где x – входной вектор, x' – его латентное представление или сжатый образ, а x^* – восстановленный входной вектор. Общая структура автоэнкодера показана на рис. 1.

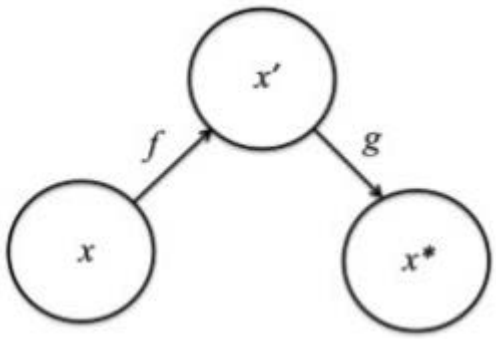


Рис. 1. Общая структура автоэнкодера

Очевидно, что некоторым приближением решения нашей задачи будет являться часть программы, реализующая функцию декодера g. При этом латентное представление будет играть роль входного аргумента, а решение будет настолько приближенным, насколько удовлетворительным с практической точки зрения можно будет считать равенство

$$x = x^* + \Delta x,$$

где Δx определяет степень несовпадения входного x и восстановленного x^* векторов. Процесс обучения автоэнкодера описывается просто как минимизация функции потерь

$$L(x, g(f(x))) \rightarrow \min,$$

где L – функция, штрафующая восстановленный входной вектор $x^* = g(f(x))$ за отличие от x, и вычисляемая, например, как среднеквадратическая ошибка.

Современные библиотеки моделирования нейронных сетей позволяют решить задачу построения автоэнкодера для определенного класса входных векторов X с заданной наперед среднеквадратической ошибкой. Эта ошибка может быть выбрана так, что упомянутая выше степень несовпадения входного x и восстановленного x^* векторов будет вполне допустимой.

В работах [2, 3] авторами решалась задача количественной оценки распределения информационных долей в пиксельных матрицах на основе колмогоровской сложности, что по сути определяет возможность использования инструмента для сравнения сложности строк не гарантирующего абсолютного минимума оценки и имеющего допустимую погрешность.

Проиллюстрируем сложность автоэнкодера, сформированного с помощью библиотеки Keras для совокупности MNIST на примере, показанном на рис. 2.

```
input_size = 784
hidden_size = 64
output_size = 784
x = Input(shape=(input_size,))
# Encoder
x’ = Dense(hidden_size, activation='relu')(x)
# Decoder
x* = Dense(output_size, activation='sigmoid')(x’)
autoencoder = Model(input=x, output=x*) autoencoder.compile(optimizer='adam', loss='mse')
```

Рис. 2. Программный код моделирования автоэнкодера

Отметим, что для оценки сложности следует брать не программу моделирования автоэнкодера, представленную выше, а результирующую нейронную сеть, полученную после обучения автоэнкодера с заданной точностью.

Список используемых источников

1. Li, M., Vitanyi, P. An introduction to Kolmogorov complexity and its applications. Springer Verlag. Third Edition, 2008. ISBN 987-0-387-49820-1.

2. Litvinov, V. L., Kozlova, L. P., Filippov, F. V. The use of a matrix decompositions for dimension reduction of training sample // 2017 IEEE II International Conference on Control in Technical Systems (CTS) 2017 IEEE II International Conference on Control in Technical Systems (CTS). Dr. Mikhail Shestopalov; Co-chair of the Conference Organizing Committee, Chair of the IEEE Russia NW Section; Vice Rector for Research, Saint Petersburg Electrotechnical University “LETI”, 2017. С. 282–284. DOI: 10.1109/CTSYS.2017.8109546.

3. Литвинов В. Л., Филиппов Ф. В. Использование сингулярного разложения для оценки информационной емкости компонент изображения // XXI Международная конференция по мягким вычислениям и измерениям (SCM-2018). Сборник докладов в 2-х томах. Санкт-Петербург. 23–25 мая 2018 г. СПб.: СПбГЭТУ «ЛЭТИ», 2018. Т 1. С. 670–673.

УДК 004.93
ГРНТИ 28.21.15

ИНФОРМАЦИОННЫЕ АСПЕКТЫ ЦИФРОВОГО СГЛАЖИВАНИЯ СЛУЧАЙНЫХ СИГНАЛОВ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются возможности информационной оценки процессов сглаживания случайных сигналов цифровыми фильтрами с использованием понятия энтропийного потенциала. Значение энтропийного потенциала определяется как половина диапазона равномерного распределения, имеющего такую же энтропию, как и закон распределения наблюдаемого параметра.

цифровое сглаживание сигналов, энтропия, энтропийный потенциал.

В настоящее время достаточно актуальной является использование информационных оценок в задачах интеллектуального анализа возникновения состояний неопределенности в системах обработки данных различного рода. Причиной возникновения состояний неопределенности при сглаживании случайных сигналов является априорная неопределенность по отношению к характеристикам воздействующих на полезный сигнал помех.

Рассмотрим процесс сглаживания случайных сигналов рекурсивными цифровыми фильтрами [1] заданного класса, которые задаются передаточной функцией:

$$\Phi(z) = \frac{K(z)}{Q(z)},$$

где z – аргумент Z-преобразования, а многочлены

$$K(z) = \sum_{i=0}^{N} k_i z^i \text{ и } \; Q(z) = \prod_{i=1}^{M}(z - j_i)\,, j_i < |1|$$

определяются исходя из требований несмещенности регулярной составляющей входного сигнала, а также оптимальными условиями подавления аддитивной стационарной помехи с заданной корреляционной функцией.

Если входной сигнал может принимать n дискретных значений

$$x_i (i = 1, \dots, n)$$

с вероятностью $P(x)$, то неопределенность состояний x_i выражается энтропией [2]:

$$H_x = -\sum_{k=0}^{n} p(x_i)\log(p(x_\text{i}).$$

При непрерывном распределении плотности вероятности x степень неопределенности входного сигнала определяется как

$$H_x = -\int_{xmin}^{xmax} p(x)\log(p(x)dx - \log \varepsilon,$$

где $p(x)$ – плотность вероятности распределения x,

ε – шаг квантования переменной.

Первый член этого выражения

$$h_x = -\int_{xmin}^{xmax} p(x)\log(p(x)dx$$

представляет собой дифференциальную энтропию, а вторая часть выражения определяет значение энтропии, порождаемое шагом квантования сигнала.

В дальнейшем, при оценке количества информации будем использовать только h_x, так как при постоянном шаге квантования его значение не будет влиять на оценку количества информации.

Для описания состояний неопределенности сигналов на входе и выходе цифрового фильтра используем понятие энтропийного потенциала [3] Δ_e и комплексного энтропийного потенциала L_Δ, причем

$$L_\Delta = \frac{\Delta_e}{|x_n|} = \frac{K_e\,\sigma}{|x_n|},$$

где σ – среднее квадратичное отклонение для сигнала *x*,

K_e – значение энтропийного коэффициента,

x_n – величина значения сигнала, на базе которого анализируется его состояние неопределенности.

Значение энтропийного потенциала определяется как половина диапазона равномерного распределения, имеющего такую же энтропию, как и закон распределения наблюдаемого параметра.

При этом энтропия случайной величины, распределенная по равномерному закону в интервале $[-\Delta_e, \Delta_e]$ рассчитывается по формуле

$$H(x) = \ln(2\Delta_e).$$

Тогда выражение для энтропийного потенциала произвольного закона распределения *x* имеет следующий вид

$$\Delta_e = \frac{1}{2} e^{H(x)} = \text{К}_e\sigma.$$

Состояние неопределенности для процесса сглаживания случайных сигналов можно охарактеризовать значениями энтропийных потенциалов входного Δ_{ex} и выходного Δ_{ey} сигналов, а динамику изменения состояния неопределенности – отношением энтропийных потенциалов

$$\frac{\Delta_{ex}}{\Delta_{ey}} = \frac{\frac{1}{2}e^{H(x)}}{\frac{1}{2}e^{H(y)}} = \text{e}^{H(x)-H(\text{y})} = e^{I(x,y)},$$

где *I(x,y)* – количество информации, порожденное процессом сглаживания случайного сигнала *x*.

Далее можно определить

$$I(x,y) = \ln\frac{\Delta_{ex}}{\Delta_{ey}} = \ln\frac{K_{ex}\sigma_x}{K_{ey}\sigma_y} = \ln\frac{K_{ex}}{K_{ey}} + \ln\frac{\sigma_x}{\sigma_y} = I_i + I_p.$$

Под I_i понимается интеллектуальная составляющая, а I_p – энергетическая составляющая количества информации [3].

Рассмотрим процесс сглаживания случайных сигналов цифровым фильтром с передаточной функцией [4]

$$\Phi(z) = \frac{b_0\,(z+1)}{(z-\gamma)^2},$$

где $b_0 = (1-\gamma)^2$.

Для данного класса фильтров обеспечивается оптимальное сглаживание случайных сигналов с аддитивной помехой, обладающей любой автокорреляционной функцией.

Значение дисперсии случайной ошибки на выходе рассматриваемого фильтра определяется выражением

$$\sigma_y^2 = \frac{1}{2}\frac{(1-\gamma)}{(1+\gamma)}.$$

Соответственно, информационный портрет данного класса цифровых фильтров будет иметь следующий вид:

$$I(x,y) = I_i + \ln\frac{1}{\sqrt[2]{\frac{0{,}5(1-\gamma)}{1+\gamma}}}.$$

Если пренебречь значением I_i [3], то графическое изображение информационного портрета цифрового фильтра будет иметь следующий вид (рис.).

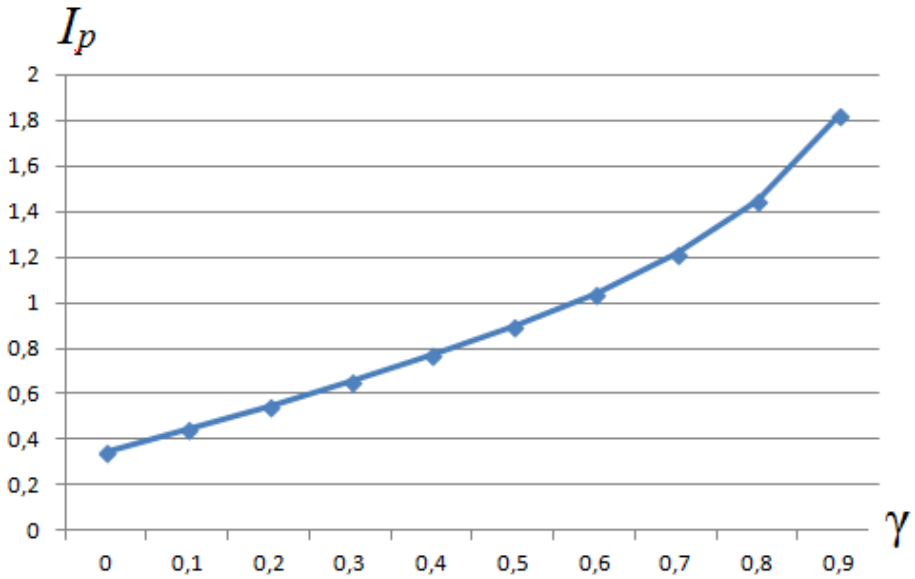


Рисунок. Информационный портрет цифрового сглаживающего фильтра

Список используемых источников

1. Кузин Л. Т. Расчет и проектирование дискретных систем управления. М.: Машгиз. 1962.
2. Николаев В. И. Информационная теория контроля и управления. Л.: Судостроение. 1973.
3. Лазарев В. Л., Травина Е. А. Синтез и расчет систем автоматического управления: учеб. пособие. СПб.: Университет ИТМО, 2018. 34 с.
4. Губин А. Н. О выборе параметров при синтезе оптимальных операторов обработки цифровой информации в АСУ ТП / в сб.: Проблемы системотехники и АСУ. Л.: СЗПИ, 1981. С. 137–141.

УДК 681.518
ГРНТИ 28.19.27

ИССЛЕДОВАНИЕ ОНТОЛОГИЧЕСКИХ МЕТОДОВ УПРАВЛЕНИЯ ИНФОКОММУНИКАЦИОННЫМИ СТРУКТУРАМИ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Концепция семантической разметки для формализации информационных ресурсов приводит к возможности структурной универсализации модели управления. Конкретизация любой информационной структуры возможна на базе онтологии соответствующей предметной области. Фундаментальная научная задача состоит в разработке универсальных методов управления инфокоммуникационными структурами, полученными с применением формализованных процедур структурирования информационных ресурсов, специфицированных онтологиями.

онтология, инфокоммуникационные структуры, отказоустойчивые системы.

Цель исследуемого проекта состоит в разработке универсальных методов управления информационными структурами, пригодных для использования в различных предметных областях. Работа по достижению поставленной цели сводится к решению следующих основных задач [1]:

- исследование и разработка методов автоматизации построения информационных структур (с использованием моделей нейронных сетей);
- исследование и разработка структурных и семантических моделей управления информационными структурами (с использованием языковых и программных средств структуризации информации);

- исследование и разработка универсальных методов управления информационными структурами (с использованием подходов классической теории управления и теории структур).

В настоящее время эволюция принципов адаптации и развитие методов технической диагностики привели к идее построения систем, обеспечивающих при появлении определенного вида неисправностей, работоспособность основной системы управления, возможно, с частичной потерей качества процессов, не допуская развитие ситуации до отказов в работе объекта управления или аварии. Такие системы получили название толерантных систем (*Fault-Tolerant Control System* – FTCS) или систем отказоустойчивого управления (СОУ) [2].

Функционирование толерантных систем предполагает решение задачи оценки текущего состояния системы и наличие системы более высокого уровня, осуществляющей необходимую корректировку системы управления этим процессом, включающую, в том числе, ее реконфигурацию.

В общем случае, отказоустойчивые системы, реализующие принцип супервизорного управления, базируются на комбинировании (рис. 1):

- обнаружении, локализации и идентификации отказов (неисправностей);
- робастного управления;
- реконфигурации / реструктуризации системы.

Рис. 1. Принципы супервизорного управления

Проектирование отказоустойчивых систем требует формализации описания предметной области, что может быть сделано средствами онтологического подхода. При этом необходимо получить модель собственно системы M_S (R), в соответствии с принципом последовательного раскрытия неопределенности ранга R [3].

- M_S (0) = <X> – нулевой ранг неопределенности системы – множество переменных, существенных для описания системы, то есть совокупность информационных сущностей без информации о причинно-следственных связей между ними.
- M_S (1) = <X, G> – задает топологию системы. Бинарное множество G задает связи между сущностями.
- M_S (2) – структурная модель, которая содержит информацию о типах связей между сущностями.
- M_S (3) – полная параметрическая онтологическая модель.

При проектировании реализуется принцип эволюционного развития, при котором сначала формируется топология системы, затем выбираются структуры связей и, наконец, оптимизируются параметры:

$$M_S\,(0) \text{ –> } M_S\,(1) \text{ –> } M_S\,(2) \text{ –> } M_S\,(3).$$

Одним из подходов, который может применен для проектирования толерантных систем, – использование методов теории управления структурами [1]. В общем виде задача формулируется следующим образом.

Если объект (структура) описывается функционалом $F(Q)$ какого-либо n-мерного аргумента Q, то преобразование S аргумента Q, оставляющее неизменным функционал $F(Q)$, т.е. влекущее тождество:

$$F(SQ) = F(Q),$$

называется симметрией данного функционала, а само тождество называется структурным тождеством этой симметрии. Задача, таким образом, сводится к нахождению этой симметрии.

Конечно, в силу того, что обнаружение, локализация и идентификация отказов (неисправностей) является некорректной математической задачей, чувствительной к малым изменениям аргумента, реальная толерантная система позволяет реализовать инвариантность к возникшим неисправностям только до ε.

Другой задачей, в которой концепция семантической разметки для формализации информационных ресурсов дает инновационные результаты – это разработка интерфейсов с динамическими данными [4].

Для редакторов, программ, в которых наборы входных/выходных данных генерируются логикой приложения, а также гибко конфигурируемых приложений наборы входных/выходных данных, структуру каждого набора, а также сценарий диалога невозможно определить на этапе проектирования интерфейса.

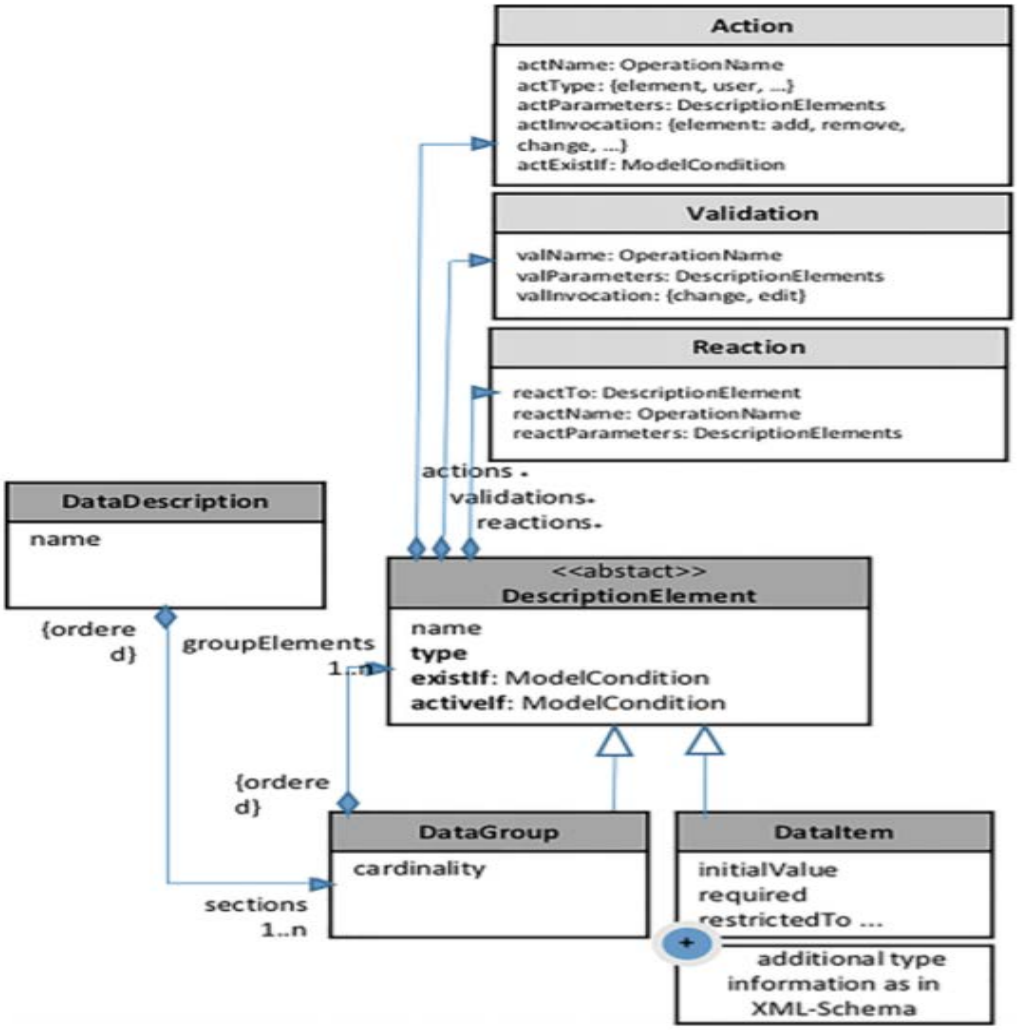


Рис. 2. Метамодель, описанная с помощью UML нотации

Определение интерфейса в рамках онтологического подхода предполагает наличие только той информации, которая может измениться в жизненном цикле информационной системы. Разработчики приложений используют эти знания для создания подходящих интерфейсов для представления данных: разумный набор данных, группирование и последовательность элементов ввода, отображение/скрытие разделов или навигация между страницами. Это знание неявно используется разработчиком и основано на его опыте или других правилах, которые являются неявным знанием. Основная

идея данного подхода включить эти семантические знания в модель, ориентированную на данные, вместе с обработанными данными приложения.

В статье [4] описана методология автоматической генерации программного кода пользовательского интерфейса по его проекту, представлен анализ онтологического подхода к автоматизации проектирования пользовательского интерфейса. Метамодель, описанная с помощью *UML* нотации, показана на рис. 2 (см. выше).

Список используемых источников

1. Золотов О. И., Пустыльников Л. М. Принципы управления структурами. СПб.: СПбГУТ, 2018. 405 с. ISBN 978-5-89160-162-8.

2. Шестопалов М. Ю. Системы отказоустойчивого управления технологическими процессами. СПб.: Элмор, 2013. 308 с. ISBN 5-7399-0201-0.

3. Душин С. Е., Зотов Н. С., Имаев Д. Х. и др. Теория автоматического управления / под ред. В. Б. Яковлева. М.: Высш. школа, 2005. 567 с.

4. Губин А. Н., Литвинов В. Л., Литвинов Д. В., Филиппов Ф. В. Анализ методов проектирования пользовательских интерфейсов на базе онтологии предметной области. // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. В 4-х т. 2018. С. 253–257.

УДК 004.414.38
ГРНТИ 20.15.05

ЗАДАЧИ УПРАВЛЕНИЯ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ АРХИТЕКТУРОЙ ВУЗА

Т. Н. Гурьева, Л. Ю. Шарабаева

Северо-Западный институт управления РАНХ и ГС

Рассматривается архитектурный подход к управлению информационно-технологической инфраструктурой вуза для достижения стратегических целей. Основное направление работы заключается в совместном использовании общих данных, исключении дублирования бизнес-функций, координации управления пользователями, ресурсами, информационной безопасностью за счет улучшений в управлении комплексом прикладных систем.

архитектура предприятия, информационно-технологическая инфраструктура, ИТ-менеджмент, SLA, BISL, COBIT, ITIL.

Современный этап развития информационного общества в России ставит перед вузами задачи трансформации деятельности, решение которых позволит быстрее реагировать на изменения внешней среды, рынка и технологий. К сожалению, вузы прилагают усилия по трансформации своей деятельности зачастую за счет осуществления локальных изменений. Однако получение положительного локального эффекта в значительной степени зависит от способности адекватно представить деятельность вуза в целом. Не видя целого, затруднительно не только найти оптимальное решение, отвечающее стратегическим интересам образовательной организации, но и грамотно сформировать требования к любым частным изменениям.

Исследования последних лет наглядно демонстрируют целесообразность применения так называемого «архитектурного подхода», обеспечивающего целостное понимание устройства любого типа предприятия. Понятие «архитектура предприятия» (АП) рассматривается как фундаментальная организация предприятия, воплощенная в ее компонентах, их взаимосвязях друг с другом и со средой, а также совокупность руководящих принципов проектирования и развития предприятия [1].

Методология архитектуры предприятия реализует идею системного подхода к управлению и изменению организаций в условиях цифровой экономики и сильной зависимости стратегии развития от информационных технологий [2].

Согласно стандарту ISO15704:2000 архитектура предприятия должна включать роли людей, описание процессов и представление всех вспомогательных технологий на протяжении всего жизненного цикла предприятия. Модель АП используется для анализа существующего и проектирования будущего состояния предприятия, а также для представления альтернативных сценариев его развития. Большое значение в интегрирующей роли АП имеют находящиеся в ее основе методы: системный подход, моделирование, повторное использование знаний, решение практических проблем на основе научных знаний.

Комплексная автоматизация современного вуза должна охватывать все этапы жизненного цикла научно-образовательного процесса, осуществляемого в едином информационном пространстве, которое формируется с использованием архитектурного подхода. Архитектура вуза – это общая модель, которая объединяет его деловые процессы с информационными технологиями, исходя из общего стратегического плана развития.

Описание информационно-технологической архитектуры вуза должно включать в себя описание архитектуры информации и архитектуры прикладных систем, а не только технологического уровня АП как такового. Основное направление работы заключается в совместном использовании общих данных, исключении дублирования бизнес-функций, координации

управления пользователями, ресурсами, информационной безопасностью за счет улучшений в управлении комплексом прикладных систем.

Рассмотрим подробнее возможности управления информационно-технологической архитектурой вуза для достижения стратегических целей.

Области управления информационными технологиями в соответствии с моделью Лойена и Делена [3] подразделяются на следующие:

- управление информационно-технологической инфраструктурой,
- управление приложениями,
- управление информацией.

Под управлением информацией со стороны организации-пользователя подразумевается управление функциональными возможностями информационного обеспечения и поддержка пользователей. Эта область управления выступает в качестве владельца и заказчика информационного обслуживания.

Управление приложениями включает управление приложениями и базами данных. Цель – управление информационными системами (приложениями) и поддержка процесса их эксплуатации на протяжении всего жизненного цикла приложения. Важно помнить, что сфера образования требует для обучения наличия специфических приложений. Для повышения качества образовательного процесса важным аспектом является возможность мониторинга деятельности обучаемых и поддержки диалога «преподаватель-студент» в реальном времени. Такие приложения влияют на мотивацию при обучении, позволяют своевременно обнаружить проблемы студента.

Управление инфраструктурой отвечает за управление эксплуатацией информационных систем, в том числе за работу оборудования, сопровождение соответствующих программных продуктов и данных. Основная задача состоит в создании и поддержании в работоспособном состоянии приложений и инфраструктуры, на которой они исполняются.

Информационное обслуживание вуза регламентируется в рамках регулярного ИТ-менеджмента и состоит в предоставлении информационных сервисов (ИТ-сервисов) заданного качества подразделениям вуза. Объектами ИТ-менеджмента являются: инфраструктура, приложения, организационная структура.

Работа департамента ИТ в соответствии с классическим циклом управления (PDCA-циклом) организуется по следующим функциональным направлениям: планирование и организация; разработка, приобретение и внедрение; предоставление и сопровождение ИТ-сервиса; мониторинг [4].

Сложность управления информационной инфраструктурой вуза определяется постоянными изменениями окружающей среды, появлением новых целей и новых технических решений. Изменения во внешнем и внутреннем окружении требуют изменения процессов управления для

обеспечения соответствия новым требованиям множества участников, вовлеченных в создание и использование ИТ-ресурсов. Контроль соответствия – ключевая функция ИТ-менеджмента. Другая важная функция заключается в предоставлении технологий, на базе которых согласуются интересы всех сторон, вовлеченных в деятельность организации. И вместе они, применительно к ИТ-службе, составляют цикл планирования и реализации любых управленческих мероприятий внутри нее. Под эффективным управлением подразумеваются наличие четких процессов обслуживания, управление изменениями всех эксплуатируемых систем, решение рутинных задач.

Модель эффективной системы ИТ-менеджмента требует согласования трех факторов: задач деятельности, стиля управления ИТ-сервисами и целей вуза. При этом особое внимание уделяется выработке показателей производительности, ориентированных на задачи деятельности [5]. Для автоматизации и оптимизации внутренних рабочих процессов ИТ-службы используются информационные системы класса IT Governance, поддерживающие лучшие практики ИТ-управления: ITIL, COBIT, SLA, BISL.

Требования к информационному обслуживанию могут формулироваться в процессе формирования соглашения об уровне обслуживания SLA (*service level agreement*) [6].

Как правило, в *SLA* речь идет о технологических параметрах (например, доступность, производительность приложений и серверов). Параметры качества ИТ-сервиса и результаты их измерения с точки зрения функционального менеджмента должны формулироваться в терминах предметной области, а не на языке ИТ. То есть должны определять требования к возможностям программного обеспечения (какие услуги программное обеспечениедолжно предоставлять, какую реакцию демонстрировать в ответ на определенные действия и в определенных ситуациях).

Методологические рекомендации основных видов деятельности в области ИТ-менеджмента и реализации архитектуры предприятия отличаются по диапазону задач, которые они решают, и подходам, которые используют.

Опыт функционального управления накоплен в библиотеке Business Information Services Library (BISL) [7]. Это библиотека услуг бизнес-информации. Её использование относится не к предоставлению ИТ -услуг, а к спросу и использованию информации и связанных с ней технологий, т. е. к организации-пользователю (в нашем случае-вузу). Спрос и использование находятся в зоне ответственности руководства вуза, а предложение, напротив – в зоне ответственности ИТ-отделов. Стратегическая цель управления бизнес-информацией заключается в установлении соответствия между информационными функциями системы и ее контентом, что сводится к атри-

буции задач на поле информационной политики, определению контента информационных функций и ИТ-поддержки, позволяя сформулировать соглашения об уровне обслуживания и набор внутрикорпоративных правил.

Control Objectives for Information and related Technology (COBIT) [8]. Это рамочная модель, определяющая набор универсальных задач управления ИТ-процессами для контроля за их деятельностью, аудита и предоставления отчетности по метрикам. Он предлагает руководство, помогающее предприятиям руководить и управлять «факторами влияния», связанными с информацией и ИТ, чтобы достичь целей и, таким образом, создать ценность для заинтересованных сторон.

BISL и COBIT можно рассматривать в качестве взаимодополняющих фреймворков. Они раскрывают два основных аспекта, необходимых для эффективного управления бизнес-информацией: BISL – необходимые виды деятельности по управлению бизнес-информацией; COBIT – управление деятельностью, ресурсами и рисками по получению и производству бизнес-информации.

Каждый фреймворк нацелен на управление деятельностью организации, предоставляющей ИТ-услуги, но *COBIT* сосредоточен на управлении деятельностью, в то время как *BISL* – на результатах этой деятельности. *BISL* рассматривает шесть из семи факторов влияния.

Для управления инфраструктурой информационных технологий и организации взаимодействия ИТ-организации с пользователями может использоваться библиотека IT Infrastructure Library (ITIL v. 2, v. 3) [9]**,** которая описывает процессный подход к предоставлению и поддержке ИТ-услуг, соответствующий стандарту ISO 9000, определяющему требования к системе менеджмента качества организаций и предприятий. Одной из основных целей внедрения ITIL является повышение качества оказания ИТ-услуг.

На корпоративном уровне рассматриваются связи между бизнес-процессами и их информационная поддержка. На уровне бизнес-процесса формируются требования к информации, предъявляемые отдельными бизнес-процессами. На системном уровне рассматриваются специфические требования пользователей к информационным системам.

Разработка модели информационной политики организации находится в зоне ответственности функционального ИТ-менеджмента. Управление приложениями и ИТ-инфраструктурой осуществляет дальнейшую трансляцию этой модели в приложения и инфраструктуру.

Исходными данными для формирования модели информационной политики, определяющей требования к информационным системам, являются артефакты архитектурной деятельности: описание основных бизнес-процессов, связей между стратегическими целями предприятия и бизнес-процессами; связей между приложениями, выполняющими обработку данных,

и бизнес-процессами; связей между приложениями и существующими информационными системами.

Список используемых источников

1. Кудрявцев Д. В., Зараменских Е. П., Арзуманян М. Ю. Разработка учебной методологии управления архитектурой предприятия // Открытое образование. 2017. Т. 21. № 4. С. 84–92.

2. Дмитриева Н. Г. Методологические модели управления информационным обеспечением // Труды НГТУ им. Р. Е. Алексеева. 2017. № 1 (116). С. 11–22.

3. BiSL – A Framework for Business Information Management – 2nd edition [Электронный ресурс]. URL: https://books.google.ru/books/about/ BiSL_A_Framework_for_Business_Informatio.html?hl=ru&id=CZJmAwAAQBAJ.

4. Долженко А. И. Управление информационными системами // INTUIT, 2008.

5. Мизерник Д. IT Governance: эффективное управление ИТ-службой [Электронный ресурс]. URL: http://www.osp.ru/os/2005/01/185191/

6. Черняк Л. Библиотеки передового опыта и парадоксы управления ИТ // Открытые системы. СУБД. 2005. № 1.

7. ASLBiSLFoundation [Электронный ресурс]. URL: http://www.aslbislfoundation.org/ru/bisl.

8. COBIT an ISACA Framework [Электронный ресурс]. URL: http://www.isaca.org/cobit.

9. Онлайн-сервис AXELOSGlobalbestpractice [Электронный ресурс]. URL: http://www.axelos.com/IT-Service-Management-ITIL.

УДК-004.056.53
ГРНТИ 28.21.19

ПОДХОД К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ КАНАЛА УПРАВЛЕНИЯ РОБОТИЗИРОВАННЫХ СИСТЕМ

Е. И. Данилова, А. М. Крибель, С. Н. Ракицкий, Д. С. Ракицкий

Военная академия связи им. Маршала Советского Союза С. М. Буденного

На сегодняшний день исследования в области робототехники являются весьма актуальными. Роботизированные комплексы могут в разы повысить производительность, не совершая ошибок вследствие «человеческого» фактора. Такие комплексы относят к киберфизическим системам. Неотъемлемой частью киберфизических систем является система управления. Эту систему, как и любой информационный канал, необходимо защищать от компьютерных атак, чтобы избежать перехвата киберфизических систем злоумышленниками. В статье разработан робототехнический комплекс и система, позволяющая управлять этим комплексом по надежному криптографически стойкому соединению. Основным элементом данной системы является криптографический чип stm32f415. Он позволяет уменьшить нагрузку на центральный процессор для

выполнения алгоритмов управления, освободив его от криптографических операций, тем самым, гарантируя выигрыш во времени.

канал управления, киберфизические системы, роботизированные системы, криптографические алгоритмы.

Автоматизированные и роботизированные системы обладают неразрывной связью между входящими в них вычислительными и физическими элементами. Сегодня представители таких систем могут быть найдены в самых разнообразных областях – космос, автомобильные, химическая технология, гражданская инфраструктура, энергетика, здравоохранение, производство, транспорт, и потребительские устройства. Такой класс систем часто рассматривается как киберфизические системы.

С одной стороны, киберфизические системы за счет распределенной сети датчиков и блоков управления позволяют решить многие практические задачи, позволяющие как сэкономить время, так и уменьшить человеческие потери, за счет выполнения наиболее опасных заданий роботизированными системами.

С другой стороны, за счет использования открытых радиоканалов и известных протоколов киберфизические системы подвержены воздействию компьютерных атак, которые в наилучшем случае могут привести к нарушению работоспособности сети, а в худшем к перехвату управления.

К наиболее распространенным компьютерным атакам на киберфизические системы относятся:

Активные виды компьютерных атак - компьютерные вирусы, модифицированные драйвера, целенаправленные атаки.

Пассивные виды компьютерных атак – подслушивание, парольные атаки, имитация удостоверения, атаки на уровне приложений [1, 3, 4].

Учитывая вышеизложенное, в настоящее время остро стоит вопрос о защите киберфизических систем и каналов управления ими. С этой целью предлагается использовать криптографические протоколы и алгоритмы. Выделяют следующие виды криптографических преобразований:

1. Симметричное шифрование – TDES, DES, AES, ГОСТ 28147-89;
2. Ассиметричное шифрование – RSA, DSA, Эль-Гамаль;
3. Электронная цифровая подпись–FDH, ESDSA, ГОСТ Р 34.10-2012;
4. Хеш-функция – MD 2/4/5/6, SHA, ГОСТ Р 34.11-94.

Из перечисленных выше криптографических алгоритмов, для реализации защиты канала управления киберфизической системы, рациональным является симметричный алгоритм *AES*, который отличается криптостойкостью и быстродействием.

В настоящее время криптография решает следующие основные задачи:

1. Обеспечение конфиденциальности сообщений – решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права к ней.

2. Обеспечение целостности данных – гарантированная невозможность несанкционированного изменения информации.

3. Аутентификация – подтверждение подлинности сторон и самой информации в процессе обмена данными.

4. Невозможность отказаться от авторства – предотвращение отказа абонента от совершенных им действий.

Эти задачи защиты данных реализованы в специальном аппаратном блоке, который называют криптографическим ускорителем (криптографическим блоком). Криптографические ускорители работают отдельно от основного ядра процессора, что позволяет ему сохранять свои ресурсы для выполнения следующих задач [2, 5, 6]:

− обслуживание для организации обмена с периферийными устройствами;

− обработку данных;

− осуществление беспроводного соединения с другими устройствами;

− управляющие и другие алгоритмы;

− ускорители позволяют шифровать данные по алгоритмам DES/TDES/AES, вычислять хеш-функции SHA-1/MD5/HMAC и генерировать случайные числа.

С целью проверки работы криптографического ускорителя была разработана роботизированная система (рис. 1), состоящая из следующих частей:

− BeagleBoneBlack (главный процессор роботизированной системы);

− Mini Maestro 18–Channel USB Servo Controller (драйвер–двигатель);

− MG996R (сервоприводы);

− STM32F415 (криптографический чип);

− Блок питания;

− Wifi адаптер.

Рис. 1. Роботизированная система в сборке

Корпус представляет собой металлический скелет, который связывает и объединяет необходимую периферию в единое целое, при этом, обеспечивая защиту и целостность компонентов. Все детали, из которых он состоит, были спроектированы в программе КОМПАС–3D *V*16 и вырезаны на фрезерном станке. Управление роботизированной системой осуществляется использованием wi-fi адаптера в качестве передатчика радиосигнала.

Для обеспечения криптографически стойкого протокола управления в роботизированной системе используется микроконтроллер с 32-разрядным

ядром ARM Cortex–M4F с криптографическим ускорителем stm32f415rgt производства компании «STMicroelectronics».

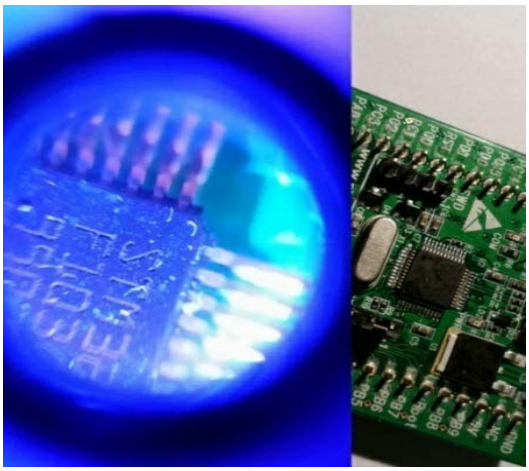


Рис. 2. Криптографический чип STM32F415

Используя техническую документацию, был проведен анализ выводов криптографического чипа с выводами микроконтроллера stmf0, после которого было принято решение внедрить чип в плату stm32f0discovery, заземлив несколько контактов (рис. 2).

Для того, чтобы чип дешифровал принятые пакеты, в качестве алгоритма дешифрования использовался AES с длиной ключа 128 бит. Данный алгоритм был выбран за своё быстродействие и криптостойкость.

В качестве алгоритма распределения ключей был рассмотрен и реализован алгоритм Диффи–Хеллмана, который позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищенный от подмены, канал связи.

Функциональная схема криптографически стойкого протокола управления роботизированной системой представлена на рис. 3.

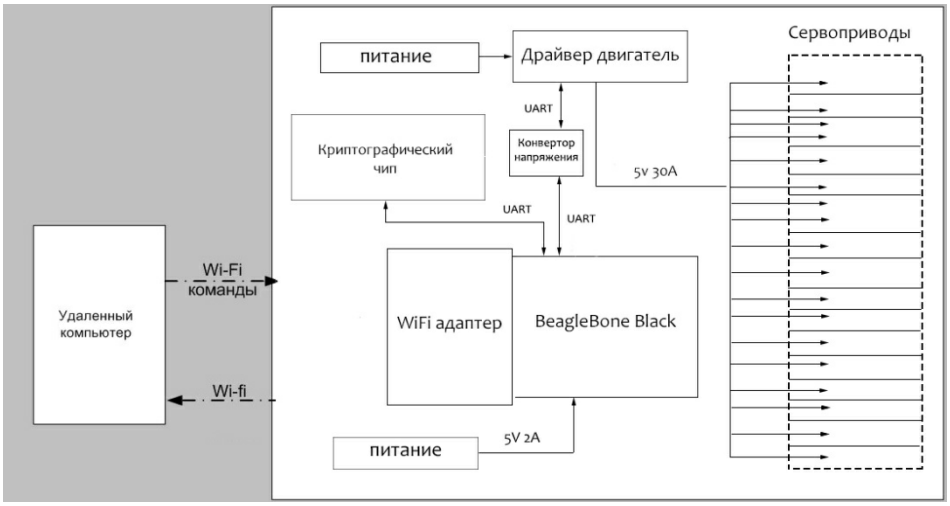


Рис. 3. Функциональная схема

В качестве центрального процессора и электронного мозга для робота был выбран одноплатный компьютер BeagleBoneBlack (BBB) [7].

С целью подключения драйвера-двигатель (*MiniMaestro* 18–*ChannelUSBServoController*) к главному процессору (*BeagleBoneBlack*) по UART–интерфейсу был взят конвертор ADuM1201, который предназначен

для преобразования электроэнергии одних параметров или показателей качества в электроэнергию с другими значениями параметров или показателей качества. На рис. 4 изображена плата перед вытравкой, нарисованная в программе *P–CAD* 2006.

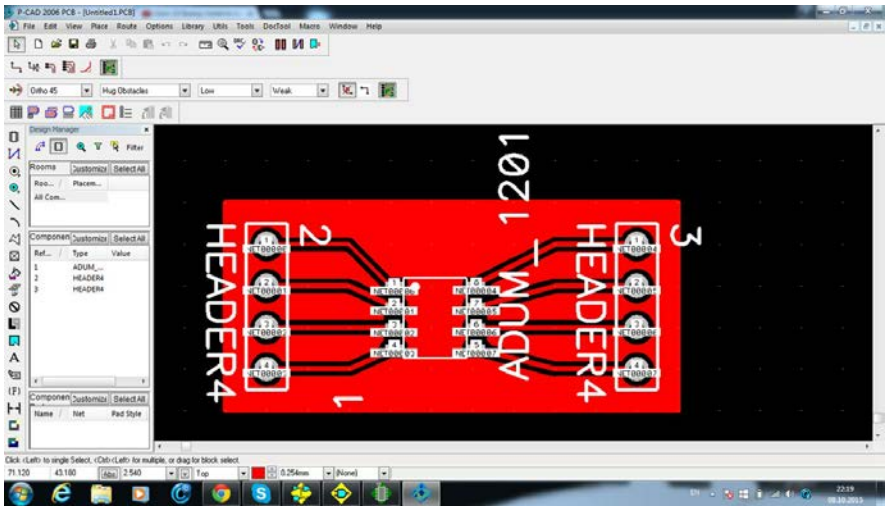


Рис. 4. Схема конвертора

Для того чтобы провести исследования реализованной криптографической системы на предмет обнаружения проблем и ошибок, был осуществлен перехват и анализ передаваемых пакетов с помощью программы Wireshark.

На рис. 5 можно увидеть, что с помощью Клиентской программы, передается сообщение «ololololo» роботу в открытом (незашифрованном) виде.

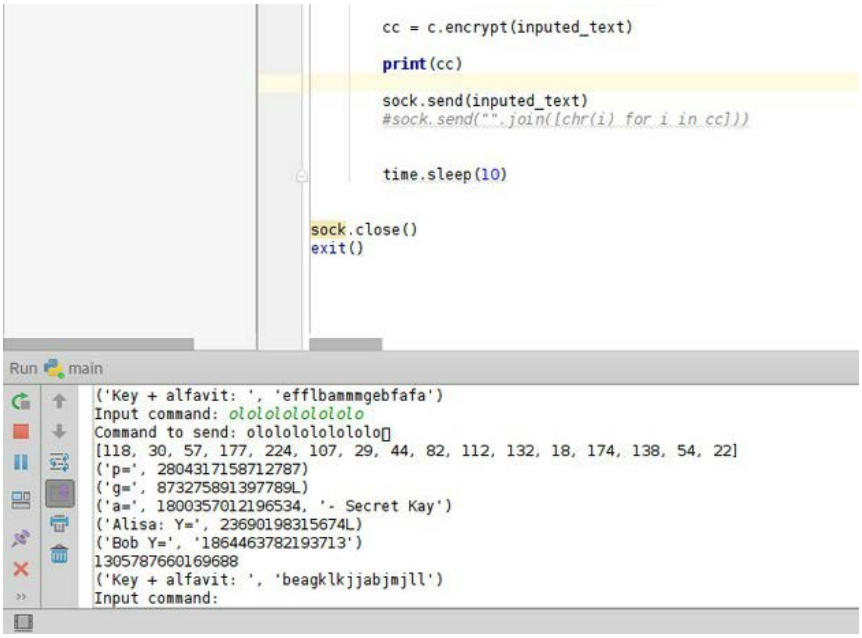


Рис. 5. Передача незашифрованного сообщения роботизированной системе

Предварительно авторизовавшись в wi-fi сети, нужно запустить Wireshark, с помощью которого будут перехвачены передаваемые пакеты. На рис. 6 видно отправляемое слово.

Теперь передаем зашифрованное слово. Находим передаваемый пакет и видим шифротекст длиной в 16 байт (рис. 7).

Анализ пакетов реализованной криптографической системы на предмет обнаружения проблем и ошибок с помощью программы Wireshark показал, что команда, передаваемая роботизированной системе, является зашифрованной, а шифрование wi-fi сети (WPA2), в отличие от технологии Bluetooth, является дополнительным препятствием к расшифрованию секретной команды злоумышленником. Кроме этого, организована постоянная смена крипто-ключей, тем самым исключена возможность их подбора [8].

Анализ пакетов реализованной криптографической системы на предмет обнаружения проблем и ошибок с помощью программы Wireshark показал, что команда, передаваемая роботизированной системе, является зашифрованной, а шифрование wi-fi сети (WPA2), в отличие от технологии *Bluetooth*, является дополнительным препятствием к расшифрованию секретной команды злоумышленником. Кроме этого, организована постоянная смена крипто-ключей, тем самым исключена возможность их подбора [8].

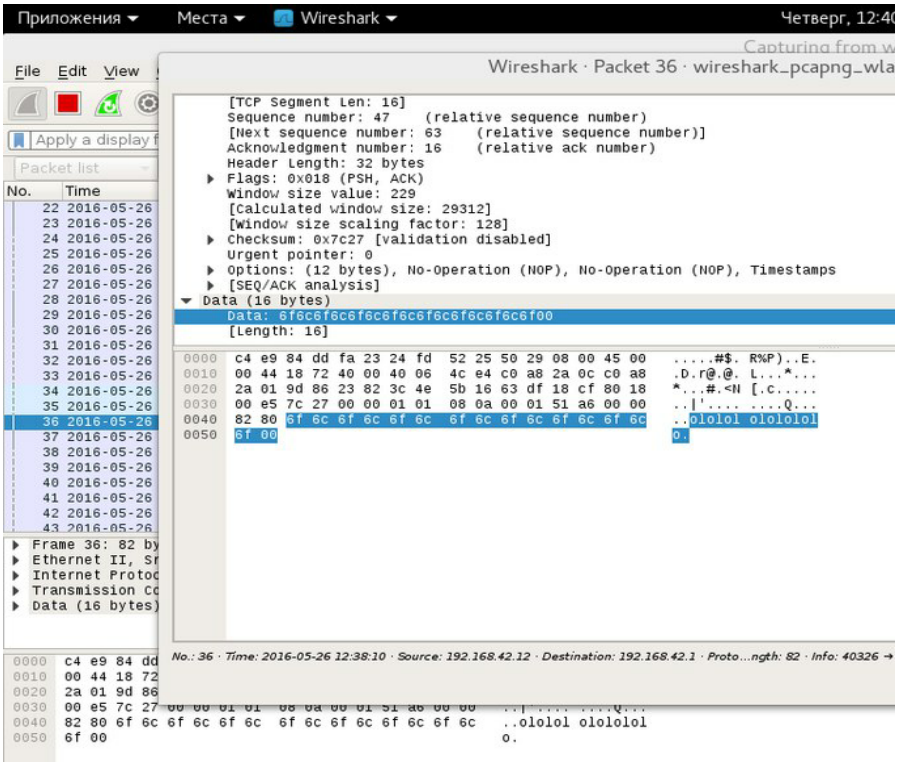


Рис. 6. Перехват незашифрованного сообщения с помощью программы Wireshark

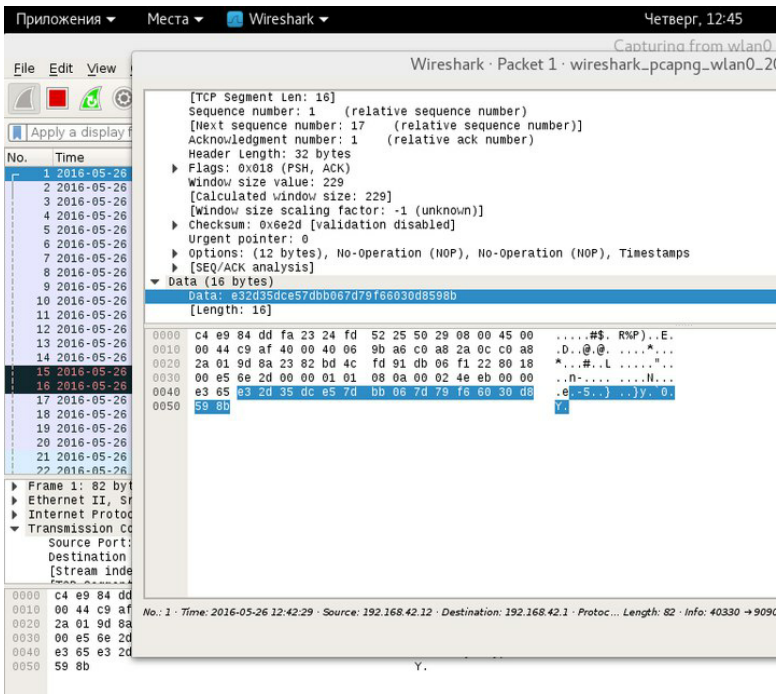


Рис. 7. Перехват зашифрованного сообщения с помощью программы Wireshark

Таким образом, в настоящей статье представлен пример создания роботизированного комплекса, как элемента КБС, с защищенной системой управления им на основе алгоритма шифрования AES, являющимся на сегодняшний момент наиболее криптостойким.

Кроме того, для защиты от атаки «грубого перебора» криптографического ключав системе управления необходимо реализовывать алгоритм распределения ключей, позволяющий генерировать новый ключ, каждый раз перед выполнением команды.

Список используемых источников

1. Reference manual STM32F405/415, STM32F407/417, STM32F427/437 and STM32F429/439 advanced ARM®–based 32–bit MCUs [Электронный ресурс] // STMicroelectronics, 2016. 1744 p.

2. Схема обмена ключами Диффи — Хеллмана [Электронный ресурс]э URL: http://kaf403.rloc.ru/POVS/Crypto/DiffieHellman.html

3. [BeagleBone Black] Enable All UART Ports at Boot [Электронный ресурс]. URL: https://billwaa.wordpress.com/2014/10/13/beaglebone–black–enable–all–uart–ports–at–boot.

4. Данилова Е. И., Лаута О. С., Митрофанов М. В., Ракицкий С. Н. Компьютерные атаки и их характеристики // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сб. научн. ст. В 4-х т. 2018. С. 297–301.

5. Hexapod–робот под управлением ROS [Электронный ресурс]. URL: http://www.pvsm.ru/diy–ili–sdelaj–sam/62026.

6. Пентестинг и тестирование на проникновение [Электронный ресурс]. URL: http://www.psyhocode.com/pentesting/.

7. Программирование STM32F4. USART [Электронный ресурс]. URL: http://micro-technics.ru/programmirovanie–stm32f4–usart–primer–programmy/

8. Васюков Д. Ю., Коцыняк М. А., Коцыняк М. М., Лаута О. С., Лаута А. С. Устройство обнаружения удаленных компьютерных атак. Патент на изобретение RUS 2540838 03.03.2014.

УДК 681.518.5
ГРНТИ 47.61.01

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ГЕНЕРИРОВАНИЯ СИГНАЛА ВОЗБУЖДЕНИЯ ДЛЯ ИМПЕДАНСНОЙ СПЕКТРОСКОПИИ ВО ВРЕМЕННОЙ ОБЛАСТИ

А. М. Демидов, Е. С. Денисов, Г. В. Никишина

Казанский национальный исследовательский технический университет им. А. Н. Туполева – КАИ

Широкое распространение литиевых аккумуляторов и других электрохимических источников энергии приводит к появлению необходимости разработки новых методов диагностики, обеспечивающих достаточную точность и быстродействие, при невысокой стоимости. Хорошие перспективы здесь имеет электрохимическая импедансная спектроскопия во временной области. Данный метод позволяет использовать энергию электрохимического источника энергии для генерирования входного сигнала, что, в свою очередь, позволяет снизить сложность, вес, размеры и стоимость измерительной аппаратуры. Предложенная система состоит из двух основных частей: 1) схема контроля режимов работы и 2) управляемая нагрузка. Также система позволяет генерировать любой входной сигнал. Схема контроля режимов работы использует информацию о текущем напряжении и токе исследуемого электрохимического источника энергии. В системе используется ПИД-регулятор, в память которого заносится набор коэффициентов, которые выбираются в зависимости от текущего напряжения электрохимического источника.

электрохимические источники энергии, литиевые аккумуляторы, электрохимическая импедансная спектроскопия.

В настоящее время электрохимические источники энергии (ЭХИЭ) являются основными элементами питания в современных портативных устройствах и автономных электронных системах. В большинстве случаев информация о состоянии элемента питания является критически важной, так как часто они используются в устройствах, требующих обеспечения автономной работы в течении долгого времени.

Для поддержания ЭХИЭ в работоспособном состоянии требуется соответствующая система диагностики. Здесь следует особенно выделить электрохимическую импедансную спектроскопию (ЭИС) [1, 2] и шумовые методы диагностики [3, 4, 5, 6, 7]. Однако данные методы являются достаточно дорогостоящими и требуют сложного оборудования, которое трудно использовать в процессе нормального функционирования ЭХИЭ. В [8, 9] предлагается метод, использующий переходную характеристику в качестве диагностического параметра. Преимуществом предложенной системы является комбинирование высокой информативности импедансной спектроскопии и малого времени измерения переходных процессов. Измерение переходной характеристики является распространённым методом исследования линейных электрических схем. Из теории об ЭИС известно, что любой ЭХИЭ может быть представлен линейной эквивалентной схемой, при условии малых изменений режима работы.

Существуют три основных метода для анализа переходных характеристик: 1) анализ во временной области, 2) анализ в частотной области, 3) метод исследования эквивалентной схемы. Все вышеуказанные методы подтверждают достаточность и информативность переходной характеристики в качестве диагностического средства для ЭХИЭ.

Для реализации предложенного способа была разработана экспериментальная установка. Установка позволяет измерять переходную характеристику напряжения/тока ЭХИЭ с одновременной записью фактической температуры во время эксперимента. Структурная схема установки представлена на рис. 1.

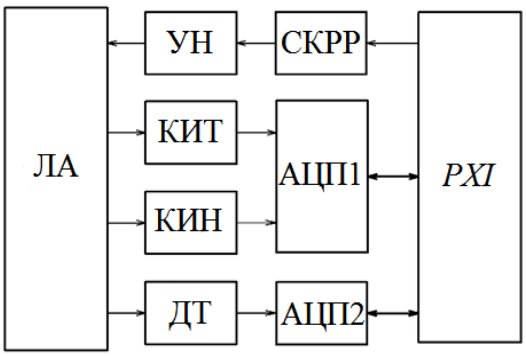


Рис. 1. Структурная схема экспериментальной установки:
ЛА – литиевый аккумулятор,
УН – управляемая нагрузка,
КИН – канал измерения напряжения,
КИТ – канал измерения тока,
ДТ – датчик температуры,
СКРР – схема контроля режимов работы,
АЦП1 и АЦП2 – аналого-цифровые преобразователи,
PXI – это *PXI*-платформа

Установка работает следующим образом. Режим работы ЭХИЭ определяются управляемой нагрузкой (УН) и схемой контроля режимов работы (СКРР). УН и СКРР обеспечивают в гальваностатический, потенциостатический и режим постоянной нагрузки. Для обеспечения автоматического управления режимом работы батареи СКРР получает информацию из каналов измерения тока (КИТ) и напряжения (КИН). Сопротивление активной нагрузки (Rн) также служит шунтом для измерения тока, поэтому оно изготовлено из супер-

фехралевой проволоки *GS SY* с чрезвычайно низким коэффициентом температурного сопротивления. Сигналы измерения тока и напряжения передаются на аналого-цифровой преобразователь (АЦП1), который реализован на основе модуля *PXI*-5922 компании National Instruments Inc. АЦП имеет 24-битное разрешение с собственным уровнем шума 3,4 мкВ. (среднеквадратичное значение) в диапазоне от −10 В до 10 В для частот дискретизации до 50 кГц. В реальном применении его можно заменить на менее дорогой аппарат без существенного снижения качества.

Канал измерения температуры включает датчик температуры (ДТ), который опрашивается АЦП2 с частотой дискретизации 1 Гц. Общая погрешность измерения температуры не превышает 1 °C.

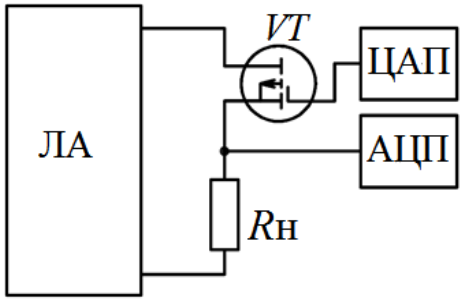


Рис. 2. *VT* – транзистор,
*R*н – активная нагрузка,
ЦАП – цифро-аналоговый преобразователь,
АЦП – аналого-цифровой преобразователь

В рамках данной работы, входной сигнал системы генерировался с помощью СКРР и УН. СКРР основана на алгоритме ПИД-регулятора, управляющий сигнал которого был получен следующим образом:

$$U(t) = K_{\text{П}}\left[\varepsilon[n] + K_{\text{И}}\sum_{i=1}^{n}\varepsilon[n] + K_{\text{Д}}(\varepsilon[n] - \varepsilon[n-1]\right],$$

где $K_{\text{П}}, K_{\text{И}}, K_{\text{Д}}$ – пропорциональный, интегральный и дифференциальный коэффициенты, соответственно, $\varepsilon[n] = \text{ИЗ} - \text{У}$, где ИЗ – измеренное значение, У – уставка.

Любой входной сигнал может быть обеспечен соответствующим изменением уставки во времени. В рамках настоящей работы рассматривается сигнал возбуждения для импедансной спектроскопии во временной области, более конкретно, мы сосредоточимся на формировании ступенчатого сигнала, который используется в [9]. Для обеспечения такого сигнала возбуждения необходимо переключаться между двумя заданными значениями уставки. Конкретные параметры сигнала возбуждения зависят от выбранных ПИД-коэффициентов и параметров изменения уставки. Чтобы проверить это предположение, СКРР на основе алгоритма ПИД-регулятора и УН были смоделированы в среде графического программирования Laboratory Virtual Instrument Engineering Workbench (LabVIEW) от National Instruments. Моделирование показало, что входной сигнал также зависит от напряжения питания. Исследования показали, что переходной процесс занимает около

30 тактов микропроцессора при питании 3 В. Более высокое напряжение питания приводит к более быстрому отклику. Дальнейшее увеличение напряжения питания дает возможность уменьшить время отклика примерно до 2–3 тактов, но с перерегулированием (переходной процесс при питании 15 В). Этот факт очень важен для генерации сигнала возбуждения, потому что мы используем напряжение батареи, изменяющееся в процессе разряда, в качестве источника питания для УН. Для оценки влияния этого эффекта на реальную систему было проведено экспериментальное исследование. Для эксперимента была использована следующая конфигурация установки (рис. 1). Она включает в себя СКРР на основе микроконтроллера ATMega328 и ЦАП, выполненный на MCP4921. УН представлен мощным полевым транзистором IRFZ44N. Проволока из суперфехрали GS SY служит токовым шунтирующим сопротивлением. ПИД-контроллер, реализованный на ATMega328 (СКРР), дает возможность создавать ступенчатый сигнал входного напряжения путем изменения уставки. Однако проблема заключается в определении коэффициентов ПИД-регулятора.

Эксперимент показывает следующие результаты. В то время как ПИД-регулятор настроен на 100 % *SOC* (состояние заряда) литиевой батареи (4,2 В), переходный процесс при 0 % *SOC* (состояние заряда) (3,2 В) занимает 900 мкс, что более чем в десять раз превышает значение при 100 % SOC (состояние заряда), где занимает всего 44 мкс. Зависимость времени переходного процесса от *SOC* (состояние заряда) при постоянных ПИД-коэффициентах показано на рис. 3.

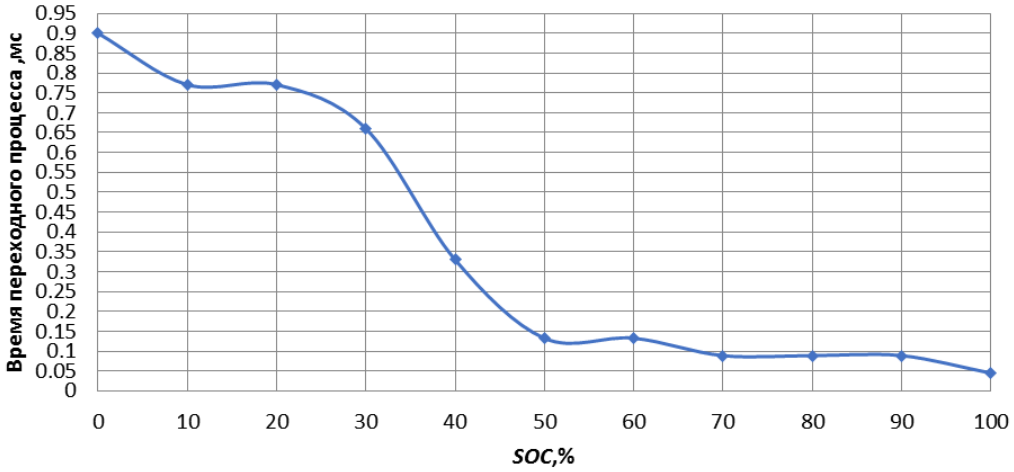


Рис. 3. Зависимость времени переходного процесса от SOC (состояние заряда) литиевого аккумулятора

В то же время было установлено, что изменение ПИД-коэффициентов позволяет уменьшить время переходного процесса и достичь тех же 44 мкс при 0 % *SOC* (состояние заряда), что и при 100 % *SOC* (состояние заряда).

Для более высоких значений *SOC* (состояние заряда) при данных значениях коэффициентов появляется перерегулирование. Следовательно, чтобы обеспечить соответствующий входной сигнал возбуждения, необходимо изменять коэффициенты ПИД во время разряда. Это может быть реализовано посредством использования набора коэффициентов, хранящихся в памяти микропроцессора. Подходящие коэффициенты из набора выбираются исходя из фактического напряжения батареи. Такой подход позволяет обеспечить надежный и недорогой инструмент для генерирования сигнала возбуждения для систем электрохимической импедансной спектроскопии во временной области.

Основной причиной разработки системы, представленной в этой работе, является создание недорогого и быстрого инструмента для диагностики литиевых батарей. Одним из лучших кандидатов на эту роль является электрохимическая импедансная спектроскопия во временной области. Одной из основных трудностей для такой системы является генерирование сигнала возбуждения высокого качества из-за высокой мощности и емкости, характерных для тестируемых систем (аккумуляторы, топливные элементы и т. д.). Представленный здесь подход позволяет использовать энергию тестируемого электрохимического источника энергии для генерирования сигнала возбуждения. Это позволяет снизить сложность измерительной аппаратуры. Важнейшим преимуществом представленной системы является то, что она может быть потенциально встроена в портативные устройства или в электромобиль для предоставления надежной диагностической информации без значительного увеличения стоимости.

Список используемых источников:

1. Asghari, S., Mokmeli, A., Samavati, M. Study of PEM fuel cell performance by electrochemical impedance spectroscopy // International Journal of Hydrogen Energy. Sep. 2010. Vol. 35. No. 17. Pp. 9283–9290.

2. Osaka, T., Nara, H., Mukoyama, D., Yokoshima, T. New analysis of electrochemical impedance spectroscopy for lithium-ion batteries // Journal of Electrochemical Science and Technology. Dec. 2013. Vol. 4. No. 4. Pp. 157–162,

3. Martemianov, S., Adiutantov, N., Evdokimov, Yu., Madier, L., Maillard, F., Thomas, A. New methodology of electrochemical noise analysis and applications for commercial Li-ion batteries // Journal of Solid State Electrochemistry. Apr 2015. Vol. 19. No. 9. Pp. 2803–2810,

4. Denisov, E., Evdokimov, Y., Martemianov, S., Thomas, A., Adiutantov, N. Electrochemical noise as a diagnostic tool for PEMFC // Fuel Cells. Nov. 2016. Vol. 17. No. 2. Pp. 225–237.

5. Martinet, S., Durand, R., Ozil, P., Leblanc, P., Blanchard, P. Application of electrochemical noise analysis to the study of batteries: state-of-charge determination and overcharge detection // Journal of Power Sources. Oct. 1999. Vol. 83. No. 1–2. Pp. 93–99.

6. Timergalina, G., Denisov, E. Study of lithium battery fluctuations in the open-circuit conditions // Int. Conf. on Actual Problems of Electron Devices Engineering (APEDE). Nov. 2018. Pp. 153–155,

7. Astafev, E., Ukshe, A., Dobrovolsky, Yu. Measurement of electrochemical noise of a Li/MnO2 primary lithium battery // Journal of Solid State Electrochemistry. Nov. 2018. Vol. 22. No. 11. Pp. 3597–3606.

8. Denisov, E., Nigmatullin, R., Evdokimov, Y., Timergalina, G. Lithium battery transient response as a diagnostic tool // Journal of Electronic Materials. May 2018. Vol. 47. No. 8. Pp. 4493–4501.

9. Timergalina, G., Nikishin, T., Denisov, E., Nigmatullin, R. Application of new signal processing methods for electrochemical power source relaxation modes detection // Systems of Signal Synchronization, Generating and Processing in Telecommunications. Jul. 2017. Pp. 1–5.

УДК 004.457
ГРНТИ 49.33; 20.53

ПРЕДЛОЖЕНИЯ ПО СОЗДАНИЮ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА УПРАВЛЕНИЯ УЗЛОМ СВЯЗИ ПУНКТА УПРАВЛЕНИЯ

А. В. Довжик, В. Г. Иванов, А. С. Кобелев, А. В. Лавров

Военная академия связи им. Маршала Советского Союза С. М. Будённого

В статье представлена концепция автоматизации процессов оперативно-технической службы на примере создания программно-аппаратного комплекса организации формирования документов на узлах связи. Рассматривается назначение, структура, возможности и принцип работы комплекса.

электронная документация, ECM-системы, оперативно-технические данные, клиент-серверное приложение, Web-сервер.

Система управления узлом связи является совокупностью функционально и организационно связанных между собой органов управления элементами узла связи, пунктов управления элементами узла связи и технической основы системы управления, которая включает информационные, вычислительные, служебные телекоммуникационные ресурсы и специальные средства, базирующиеся на комплексах программно-аппаратных средств [1].

Основным документом, определяющим задачи стационарного узла связи, порядок и сроки их выполнения, а также порядок эксплуатации узла

связи в мирное время, при приведении в высшие степени боевой готовности и в военное время, является боевой приказ командира бригады связи (территориальной), который разрабатывается на основании боевого распоряжения бригаде.

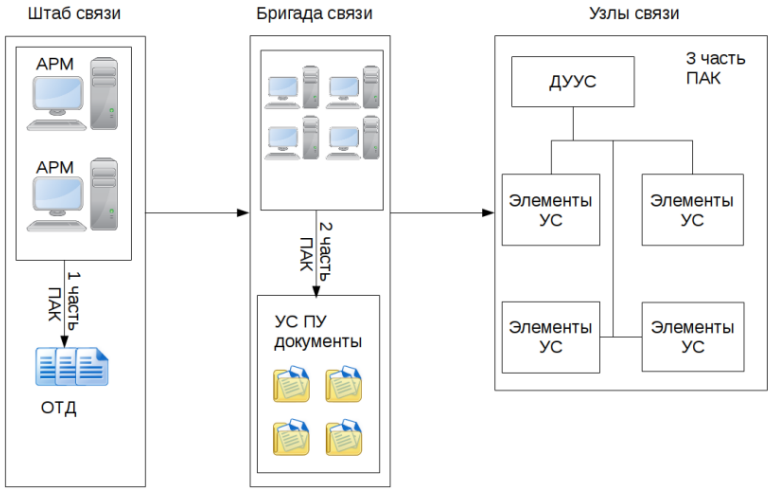


Рис. 1. Структура программно-аппаратного комплекса

В соответствии с требованиями руководящих документов в боевом приказе стационарному узлу связи должен быть определен и порядок организации оперативно-технической службы, а также вопросы боевой и морально-психологической подготовки личного состава, привлекаемого для несения дежурства.

В эпоху внедрения вычислительных систем в организации для решения проблем производственных процессов стоит задача в проектировании и реализации систем электронного документооборота, позволяющих быстро и эффективно сформировать необходимые документы, исключая возможные ошибки на начальном этапе.

Разрабатываемый программный комплекс предназначен для автоматизированной организации оперативно-технических данных в органах управления связи и документов оперативно-технической службы на узлах связи пунктах управления. Данный комплекс позволяет автоматически формировать следующие документы оперативно-технической службы в табличном виде:

- Оперативно-технические данные (в табличном виде);
- Схема-приказ УС ПУ, элементу УС ПУ, аппаратной (боевому посту) (в табличном и ламельном виде);
- Схема калибрования УС (в табличном и ламельном виде);
- Схема электроснабжения УС (в табличном и ламельном виде);

- Схема организационно-технической структуры УС ПУ.

Программный комплекс состоит из нескольких модулей-программ, представленных на рис. 1. Общая концепция заключается в разбиении модулей на клиентскую и серверную части, где под клиентами подразумеваются должностные лица органов управления связи (ДЛ ОУС) с АРМ, отвечающие за организацию разработки документов связи и контроля за состоянием связи. В серверной составляющей фигурируют дежурные, роль которых – контроль за действиями ДЛ ОУС (регистрация, удаление, изменение прав доступа к тем или иным документам), редактированием структуры документов, организацией и мониторингом работы узлов связи, и т. п.

На рис. 2 представлена функциональная схема работы двух модулей программного комплекса формирования оперативно-технических данных. Согласно функциональной схеме работа программного комплекса начинается с авторизации уже существующих пользователей по имеющимся идентификаторам, либо регистрация нового пользователя с присвоением ему логина и пароля. При положительном результате авторизации пользователю открывается главное меню программы. В меню предоставляется выбор между работой с оперативно-техническими данными и документами оперативно-технической службы. Перейдём к непосредственному описанию модулей программы.

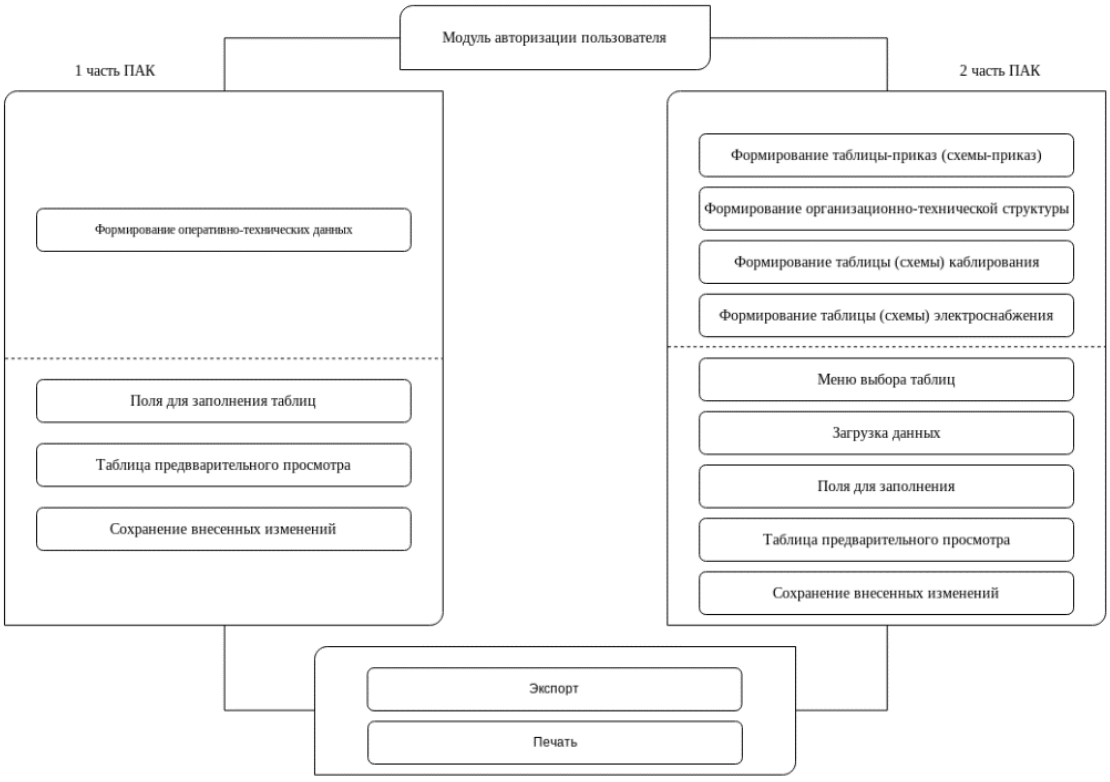


Рис. 2. Функциональная схема двух модулей программы

Первый модуль комплекса отвечает за формирование оперативно-технических данных, которое заключается в заполнении пользователем полей таблицы определенного стандарта. При заполнении полей вносимые данные отображаются в таблице предварительного просмотра. По окончанию или в любой момент работы с таблицей программа позволяет сохранять документ, экспортировать его в файлы с расширением «.ods», а так же осуществлять печать сформированного документа.

При работе со вторым модулем программного комплекса, отвечающего за формирование документов оперативно-технической службы, пользователь попадает в меню выбора таблиц-приказов, с которыми ему необходимо работать. После выбора необходимой таблицы-приказа он получает для работы таблицу, основная часть которой является результатом работы первого модуля программы. Далее пользователь начинает заполнение пустых полей формируемой таблицы-приказа. При заполнении полей вносимые данные отображаются в таблице предварительного просмотра. По окончанию или в любой момент работы с таблицей программа позволяет сохранять документ, экспортировать его в файлы с расширением «.ods», а так же осуществлять печать сформированного документа. В любой момент времени пользователь может выйти в главное меню и начать работать с другой таблицей (приказ-таблицей), к которой он имеет права доступа, либо к ранее формируемыми им документам.

Третий модуль предназначен для организации контроля обеспечения связи узлом связи согласно разработанным документам. Начало работы заключается в регистрации пользователя путем заполнения электронного журнала. Контроль за состоянием связи осуществляется через установление связи с рабочими местами начальников станций, которые указаны в загружаемых таблицах-приказах. Наличие данного модуля позволит обеспечить автоматизированное управление как стационарным, так и полевым узлом связи.

Со стороны программного обеспечения, необходимого для разработки, была выбрана разработка на операционной системе специального назначения Astra Linux версии «Смоленск». В составе данной ОС имеются защищенные система управления базами данных Postgres SQL, Web-сервер Apache2, а также интерпретатор языка Python. Данные программные средства являются минимальной составляющей для разработки Web-приложений, поэтому было принято решение спроектировать два модуля макета под Web-сервис. Функциональная схема приведена на рис. 3.

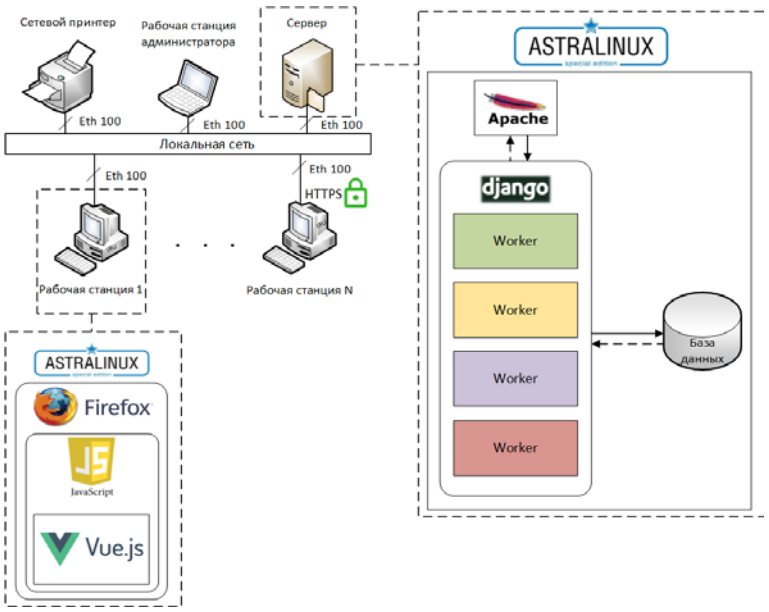


Рис. 3. Структурная схема программно-аппаратного комплекса.

Наиболее распространенным стилем архитектуры построения веб-служб является REST (*Represenational State Transfer*) – передача состояния представления. В общем случае является простым интерфейсом управления информацией без использования каких-то дополнительных внутренних прослоек. Для Django есть своя собственная библиотека, отвечающая данному стилю, – Django REST framework [2].

Представленные фреймворки языка Python подходит как написания серверной, так и клиентской части программ. Для большей гибкости было предложено использовать фреймворк для создания пользовательских интерфейсов Vue.js языка JavaScript [3]. Среди обилия других решений в данной области фреймворк был выбран как легкий в изучении, поддерживаемый и тестируемый JavaScript-фреймворк. Одним из достоинств языка является добавление Vue в готовый проект, что позволяет расширить функциональность и интерактивность существующего приложения.

Apache HTTP сервер, согласно официальной документации [4], является мощным, гибким веб-сервером, поддерживающим протокол HTTP/1.1, включая реализацию RFC2616. Кроме активной поддержки со стороны сообщества легок в настройке, а также поддерживает возможность видоизменения путём написания собственных модулей. Для ОССН на странице справочного центра есть руководство по настройке для версий 1.2 и 1.6.

Данный макет позволит непосредственно улучшить разработку необходимых документов оперативно-технической службы, а также произвести качественный мониторинг состояния связи на контролируемых узлах.

Список используемых источников

1. Основы эксплуатации полевых узлов связи пунктов управления / В. Г. Иванов, С. А. Панихидников, С. Л. Халепа, О. П. Тевс, Д. Д. Корякин, М. А. Гудков, О. А. Михалев. СПб.: СПбГУТ, 2017. 180 с.
2. Официальный сайт Django-REST Framework [Электронный ресурс] // Encode OSS Ltd 2011. URL: https://www.django-rest-framework.org/
3. Руководство фреймворка Vue.js [Электронный ресурс]. URL: https://ru.vuejs.org/v2/guide/
4. Официальная документация Apache HTTP Server [Электронный ресурс] // The Apache Software Foundation 2018. URL: https://httpd.apache.org/docs/2.4/

УДК 004.056.5
ГРНТИ 81.93.29

ТРЕБОВАНИЯ К ПРОЦЕССАМ И КОМПОНЕНТАМ УСТРАНЕНИЯ НЕОПРЕДЕЛЕННОСТИ АНАЛИЗА СМЫСЛОВОГО НАПОЛНЕНИЯ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ В ИНТЕРЕСАХ ОБНАРУЖЕНИЯ И ПРОТИВОДЕЙСТВИЯ ВРЕДОНОСНОЙ ИНФОРМАЦИИ

Е. В. Дойникова[1,2], И. Б. Паращук[1,2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

С учетом результатов анализа современных требований к процессам и элементам систем контроля цифрового сетевого контента, предложен подход к формулировке базовых требований к компонентам устранения неопределенности оценки и категоризации смыслового наполнения информационных объектов, составляющих содержание сервисов, предоставляемых сетью Интернет. Данный подход реализуется с учетом того факта, что устранение неопределенности оценки и категоризации смыслового наполнения информационных объектов будет осуществляться с использованием методов обработки неполных, противоречивых и нечетких знаний. Выполнение данных требований позволит интеллектуальным сканерам (классификаторам) оперативно, достоверно и адекватно выявлять признаки и противодействовать вредоносной (нежелательной, сомнительной) информации в цифровом сетевом контенте.

требования, неопределенность, контент, информационный объект, компонент, вредоносная информация, смысловое наполнение, оценка.

Компоненты устранения неопределенности (неполноты и противоречивости) анализа, оценки и категоризации смыслового наполнения информационных объектов являются элементом усовершенствованных классификаторов информационных объектов и придают им способности обработки неполных, противоречивых и нечетких знаний [1]. В рамках исследования требований, которые могут и должны быть предъявлены к процессам и компонентам устранения неопределенности оценки и категоризации смыслового наполнения информационных объектов на основе использования методов обработки неполных, противоречивых и нечетких знаний, необходимо вначале проанализировать базовые требования, предъявляемые к процессам оценки и категоризации, требования к итогам этих процессов – результатам (полученным оценкам и категориям).

Ключевыми требованиями к процессам оценки и категоризации в условиях неполноты, противоречивости и нечеткости исходных (наблюдаемых, анализируемых, контролируемых) данных являются: оперативность: данные процессы должны быть реализованы за время, не превышающее заданное; комплексность: данные процессы должны охватывать все аспекты, все грани смыслового наполнения информационных объектов; адекватность (достоверность): соблюдение определенного уровня соответствия полученных в ходе этих процессов оценок и категорий (полученного образа) реальным оценкам уровня нежелательности, сомнительности и вредоносности информации (достоверность, как соответствие реальности); объективность: реализация процессов оценки и категоризации должна быть обоснована, аргументирована, исходя из научно апробированных критериев; непрерывность: процессы оценки и категоризации смыслового наполнения информационных объектов в условиях неопределенности должны реализовываться постоянно, в динамике без временных перерывов и сбоев; полнота и точность: отображение всей предметной области (области нежелательной, сомнительной и вредоносной информации) в рамках аналитической обработки цифрового сетевого контента; открытость: должны быть всегда понятны и доступны к обсуждению в экспертной среде и изменению (коррекции, в случае необходимости) наборы простых правил и критериев, на основе которых осуществляются процессы оценки и категоризации смыслового наполнения информационных объектов в условиях неопределенности.

Наряду с требованиями к процессам оценки и категоризации, существует ряд требований к самой информации (измерительной информации о смысловом наполнении информационных объектов), которая оценивается и категорируется в рамках обнаружения и противодействия нежелательной, сомнительной и вредоносной информации [2]. Эти требования соответствуют содержанию понятий «единства» и «точности» измерений в процессе оценивания и категоризации:

1. Результаты измерений в рамках оценивания и категоризации смыслового наполнения информационных объектов в условиях неопределенности должны быть выражены в узаконенных единицах. Иногда это называют измеримостью информации, т. е. информацию о смысловом наполнении информационных объектов при любом аспекте исследования всегда должно быть возможно оценить на основе введенной субъектом метрической (количественной) или иной шкалы измерения;

2. Должна быть достаточно точно определена погрешность выполненных измерений в рамках оценки и категоризации смыслового наполнения информационных объектов;

3. Эта погрешность не должна превышать допустимых пределов;

4. Понятность информации о смысловом наполнении информационных объектов – простота восприятия результатов оценки и категоризации;

5. Устойчивость информации о смысловом наполнении информационных объектов – сохранение точности результатов оценки и категоризации;

6. Ценность информации о смысловом наполнении информационных объектов – полезность результатов оценки и категоризации;

7. Учет динамичности информации о смысловом наполнении информационных объектов – ее способности к изменению во времени. Иными словами, любая зафиксированная информация о смысловом наполнении информационных объектов со временем устаревает;

8. Преобразуемость информации о смысловом наполнении информационных объектов, т. е. ее способность на основе введенных субъектом операторов преобразования информации, изменять свою форму, меру, место и актуальность;

9. Размножаемость информации о смысловом наполнении информационных объектов. В первую очередь, размножаемость в аспекте множества каналов ее распространения, во вторую, в аспекте «простоты» копирования и возможной множественности доступа к ней.

При этом существует ряд факторов, влияющих на выбор метода оценки и категоризации смыслового наполнения информационных объектов в условиях неопределенности: для каждого типа оцениваемых в условиях неопределенности признаков нежелательной, сомнительной и вредоносной информации в смысловом наполнении информационных объектов существуют свои методы оценки и категоризации, существуют конкретные особенности их реализации; для оценки и категоризации смыслового наполнения информационных объектов существенную роль играет объем и качество исходных данных.

Именно поэтому с высокой вероятностью оценка и категоризация происходят в условиях неполноты, противоречивости и нечеткости этих (наблюдаемых, анализируемых, контролируемых) данных, с применением экспертных методов, методов нечеткой логики, нейронных сетей [3] и др.;

при оценке и категоризации смыслового наполнения информационных объектов принципиально важно учитывать динамику показателей, характеризующих признаки нежелательной, сомнительной и вредоносной информации; при выборе методов оценки и категоризации смыслового наполнения информационных объектов в условиях неопределенности следует принимать во внимание не только глубину расчетных данных, но и горизонт прогнозирования параметров, характеризующих признаки нежелательной, сомнительной и вредоносной информации; большое значение имеет срочность и технические возможности проведения оценки и категоризации смыслового наполнения информационных объектов в условиях неопределенности; эффективность применения методов оценки и категоризации смыслового наполнения информационных объектов в условиях неопределенности повышается при формализации признаков нежелательной, сомнительной и вредоносной информации с целью математического моделирования их воздействия на граждан и общество; следует учитывать требования законов, иных Руководящих документов, государственных контролирующих органов к тезаурусу, учету и формированию отчетности о наличии в цифровом контенте нежелательной, сомнительной и вредоносной информации.

К компонентам устранения неопределенности оценки и категоризации смыслового наполнения информационных объектов, входящим в состав усовершенствованных классификаторов, могут быть предъявлены основные (базовые) требования [4]:

по постоянной готовности – в организационном смысле: к способности этих компонент в установленные сроки начать оценку и категоризацию смыслового наполнения информационных объектов в условиях неопределенности и успешно выполнить поставленные задачи; в техническом смысле: к доступности компонент устранения неопределенности оценки и категоризации для эксплуатации, контроля или технического обслуживания;

- по устойчивости – к способности компонент устранения неопределенности оценки и категоризации возвращаться в равновесное состояние после окончания действия возмущения, нарушившего это равновесие;
- по масштабируемости (мобильности-переносимости) – к способности компонент устранения неопределенности оценки и категоризации изменять свою конфигурацию (архитектуру) и переносимости на другую аппаратную платформу;
- по безопасности работы – к способности компонент устранения неопределенности оценки и категоризации осуществлять защиту ресурсов одних пользователей от других и установление квот по вычислительным ресурсам на процессы оценки и категоризации[81];

- по производительности – к способности компонент устранения неопределенности оценки и категоризации с высокой эффективностью осуществлять обработку больших потоков данных. Это требование характеризуется степенью реализации двух ключевых факторов: объем обрабатываемых данных и вычислительная мощность компонент устранения неполноты и противоречивости. Помимо этого, к компонентам устранения неопределенности оценки и категоризации смыслового наполнения информационных объектов, входящим в состав усовершенствованных классификаторов, могут быть предъявлены дополнительные требования: по модульности – к способности компонент устранения неопределенности быть разделенными на модули по функциональному признаку; по функциональной избирательности – к способности компонент устранения неопределенности иметь в своем составе (сформировать) часть важнейших модулей в виде ядра; по генерируемости – к способности компонент настраиваться под конкретные вычислительные комплексы и под конкретный круг решаемых неопределенных задач; по виртуализации – к способности этих компонент использовать единую схему распределения ресурсов по принципу виртуальной машины (памяти, консоли); по независимости программ оценки и категоризации в условиях неопределенности от внешних устройств; по совместимости – к способности компонент устранения неопределенности выполнять на своей аппаратной платформе программы, написанные для различных операционных систем; по открытости – к способности компонент устранения неопределенности быть доступными для анализа; по многозадачности – к способности одновременно выполнять множество программ; по многопользовательскому режиму – к способности большому числу пользователей одновременно работать с одной и той же компонентой; по защищенности – к способности защитить память процессора данного компонента; по экономичности работы – к способности компонент устранения неопределенности считывать с диска только те части программы, которые действительно используются для ее выполнения; по поддержке ряда различных распространенных файловых систем, всех стандартных форматов данных, протоколов различных сетей.

Выполнение данных требований к компонентам устранения неопределенности оценки и категоризации смыслового наполнения информационных объектов, позволит интеллектуальным сканерам (классификаторам) оперативно, полно (достоверно), точно и адекватно выявлять признаки и противодействовать нежелательной, сомнительной и противоречивой информации в цифровом сетевом контенте.

Работа выполнена при финансовой поддержке РНФ (проект 18-11-00302).

Список используемых источников

1. Котенко И. В., Паращук И. Б. Общая архитектура интеллектуальной системы аналитической обработки цифрового сетевого контента в интересах защиты от нежелательной информации // Материалы конференции «Информационные технологии в управлении» (ИТУ-2018). СПб.: АО «Концерн «ЦНИИ «Электроприбор», 2018. 742 с. С. 501–505.

2. Паращук И. Б., Агеев А. С. Повышение достоверности оценки смыслового наполнения информационных объектов на основе обработки неполных, противоречивых и нечетких знаний // Материалы конференции «Информационные технологии в управлении» (ИТУ-2018). СПб.: АО «Концерн «ЦНИИ «Электроприбор», 2018. 742 с. С. 495–500.

3. Авраменко В. С., Бобрешов-Шишов Д. И., Маликов А. В. Анализ компьютерных инцидентов безопасности с применением искусственных нейронных сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. В 4-х т. СПб.: СПбГУТ, 2018. Т. 2. 670 с. С. 7–11.

2. Паращук И. Б., Дойникова Е. В., Котенко И. В. Подход к выработке требований по устранению неполноты и противоречивости оценки и категоризации смыслового наполнения информационных объектов // Региональная информатика (РИ-2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». Санкт-Петербург, 24-26 октября 2018 г.: Материалы конференции. СПб.: СПОИСУ, 2018. 631 с. С. 162–164.

УДК 654.739
ГРНТИ 81.93.29

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАЗ ДАННЫХ 1С:ПРЕДПРИЯТИЯ

В. О. Долгун, Д. Б. Казаков, В. С. Руссия, А. А. Швидкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлены недостатки системы 1С, связанные с проблемами обеспечения целостности, конфиденциальности и безопасности финансовой документации. Предложен общий подход к использованию системы 1С, включающей сервер приложений, сервер баз данных SQL и пользовательские рабочие станций. Рассмотрены методические аспекты обеспечения защиты данных, хранящихся и обрабатывающихся в системах 1С.

защита данных, 1С:Предприятие, SQL, базы данных, целостность.

В настоящее время продукты компании 1С все чаще используют для бухгалтерского и управленческого учета. Однако стоит отметить, что данные системы имеют недостатки, связанные с обеспечением целостности и конфиденциальности, а также с организацией безопасности финансовой документации.

Проблема информационной безопасности возникает в различных областях финансовых учетных систем. Самой известной системой ведения бухгалтерского учета на сегодняшний момент является программный продукт 1С.

Обеспечение информационной безопасности – задача, требующая особого внимания при реализации и внедрении системы безопасности различных типов подключений 1С. Для обеспечения защиты информации внутри продукта 1С важно понимать какой тип подключения будет использоваться:

1) с применением файлового формата;

2) с использованием СУБД.

Рассмотрим первый вариант файлового формата содержания базы данных. Файловые базы 1С являются наиболее уязвимыми к физическому воздействию. Это связано с особенностью архитектуры данного типа баз данных. Директорию необходимо держать открытой, с полными правами доступа к каталогу всем пользователям операционной системы или домена, использующих базу данных. В результате любой пользователь, имеющий право работать в файловой базе 1С, может скопировать и удалить информационную базу 1С (рис. 1).

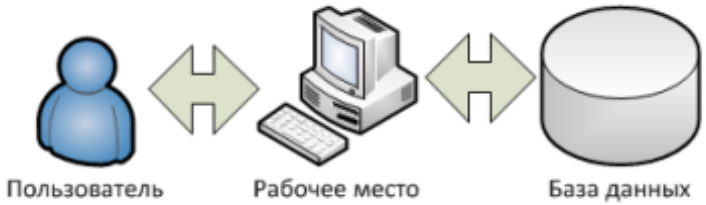


Рис. 1. Файловый вариант базы данных

Получить доступ в файловую базу, а также снять внутреннюю аутентификацию можно даже в случае, когда учетные записи пользователей созданы внутри базы данных. Для этого необходимо в каталоге найти файл «1Cv8.1CD» и открыть его любым доступным Hex-редактором. Для того, чтобы найти необходимую для редактирования строку нужно нажать сочетание клавиш Ctrl+F, выбрать из списка кодировку «Unicode», в строке поиска ввести значение «users.usr» и нажать поиск (рис. 2). После того, как будет найдена нужная строка, в колонке со значением «9», параметр «00»

меняется на «01». Затем таким же способом нужно найти строку со значением «v8users» и в ней изменить символ «v» на «h», так чтобы в итоге получилось «h8users».

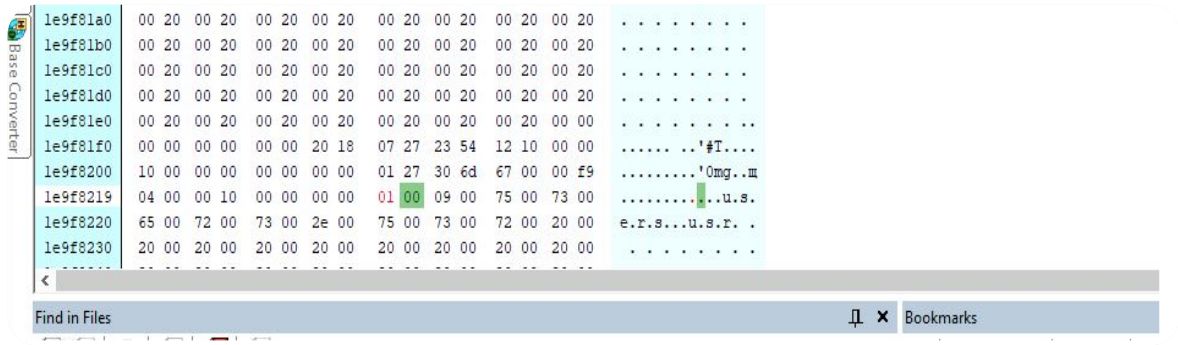


Рис. 2. Получение доступа в файловую базу данных

Рассмотрим второй вариант использования 1С с базами в системе управления в формате клиент-серверного подключения: в качестве хранилища баз 1С используются СУБД (PosgreSQL, MS SQL), а в качестве промежуточной службы связи 1С и СУБД используются сервер 1С:Предприятия (рис. 3) [1].

Такой вариант использования наиболее популярен во многих компаниях, так как происходит доработка стандартной конфигурации 1С под конкретные требования предприятия. Однако в процессе доработки и администрирования, а также во время постоянных испытаний доработанного или нового интерфейса и функционала специалисты часто пренебрегают правилами сетевой безопасности.

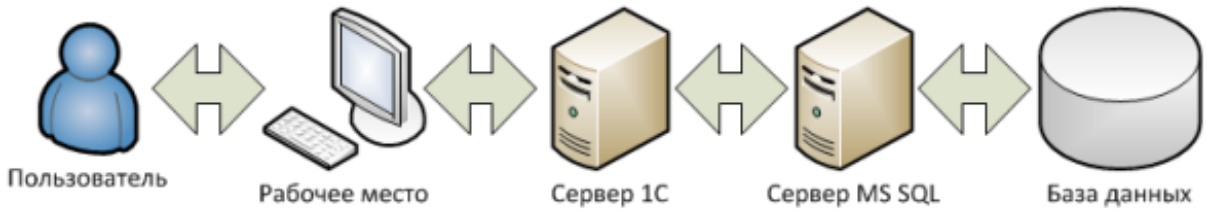


Рис. 3. Клиент-серверный вариант подключения к 1С

Особенностью клиент-серверного варианта подключения является большое количество звеньев системы, а именно: пользователь, рабочее место, терминальный сервер, сервер 1С:Предприятия, сервер MS SQL, база данных.

На каждом этапе обработки и передачи информации существуют свои угрозы:

- простые и общедоступные пароли пользователей;

- доступ пользователей к административным действиям конфигуратора;
- уязвимости операционной системы и СУБД;
- отсутствие разграничений прав доступа в 1С;
- доступ к данным сервера СУБД;
- вирусы, шпионские программы и многое другое.

При выборе файлового варианта баз 1С необходимо воспользоваться следующими рекомендациями:

- использовать разграничения прав доступа NTFS;
- настроить подключение, только доверенных usb-устройств;
- использовать только доверенные сайты из «белого» листа;
- использовать авторизацию Windows для входа и для доступа к сетевым ресурсам;
- использовать шифрованные диски или шифрованные папки, которые позволят сохранить конфиденциальную информацию даже при выгрузке базы 1С;
- установить политику автоматической блокировки пользовательского профиля;
- разграничить права доступа на уровне 1С.

При выборе варианта работы в СУБД необходимо воспользоваться следующими рекомендациями [2]:

- учетные данные для подключения к СУБД не должны иметь административных прав;
- необходимо разграничивать права доступа к базам СУБД, например, создавать для каждой информационной базы свою учетную запись, что позволит минимизировать потерю данных при взломе одной из учетных записей;
- следует ограничить физический и удаленный доступ к серверам баз данных и 1С:Предприятия;
- необходимо использовать шифрование баз данных. Это позволит сохранить конфиденциальные данные в случае, когда злоумышленник имеет физический доступ к файлам СУБД;
- необходимо использовать шифрование или установку пароля на резервные копии данных;
- необходимо вести журнал авторизации внутри 1С.

В обязательном порядке необходимо создать администраторов кластера 1С и сервера 1С, так как полный доступ к информационным базам по умолчанию будет предоставлен всем пользователям системы.

Сетевая безопасность – это набор требований, предъявляемых к инфраструктуре компьютерной сети предприятия и политикам работы в ней, при

выполнении которых обеспечивается защита сетевых ресурсов от несанкционированного доступа. В рамках рекомендуемых действий по организации и обеспечению сетевой безопасности целесообразно рассмотреть следующие:

- в компании должен быть внедрен единый регламент информационной безопасности с соответствующими инструкциями;
- должна присутствовать система комплексного мониторинга действий пользователей и оперативного оповещения нарушений нормального состояния всех общедоступных ресурсов, работа которых важна для Компании;
- ограничение доступа пользователей к нежелательным сайтам, в том числе к файлообменникам;
- наличие централизованной системы управления и обновления антивирусным ПО, а также политик регулярных обновлений ОС;
- ограничение запуска съемных флэш носителей;
- пароль должен состоять из не менее восьми символов, содержать цифры, а также буквы верхнего и нижнего регистров;
- должна быть защита и шифрование ключевых папок обмена информацией, в частности файлов обмена 1С и системы клиент-банк.

Следует отметить, что файловый режим работы не может обеспечить должную защиту в случае, когда файл хранится на сетевом ресурсе или находится на общедоступном компьютере. Защита файла в данном случае определяется политикой безопасности организации. Безопасность клиент-серверного решения, в отличие от файлового, определяется не только политикой безопасности организации, но и средствами обеспечения безопасности, которые используются на сервере базы данных и внутри 1С

Список используемых источников

1. Бондарев В. В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства. М.: Изд-во МГТУ им. Н. Э. Баумана, 2017. 225 с.: ил. ISBN 978-5-7038-4757-2.

2. Баймакова И. А., Новиков А. И., Рогачев А. И., Хыдыров А. Х. Обеспечение защиты персональных данных. М., 2010. 270 с. ISBN 978-5-9677-1455-9.

Статья представлена заведующим кафедрой,
доктором технических наук, профессором Л. К. Птицыной.

УДК 654.739
ГРНТИ 28.23.23

АРХИТЕКТУРА РАСПРЕДЕЛЁННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ УПРАВЛЕНИЯ УМНЫМ ДОМОМ

В. О. Долгун, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Актуализировано развитие систем управления умным домом. Систематизировано представление знаний о системах управления умным домом. Описаны преимущества распределённых интеллектуальных систем управления умным домом. Рассмотрены проблемы распределенных систем. Сформирован базис архитектур систем управления умным домом. Описаны особенности построения систем управления умным домом.

умный дом, интеллектуальные системы, методы.

Комплекс стандартов СТО НП «АВОК», разработанный на основе ISO 16484 (*Building Automation and Control Systems*), определяет три уровня автоматизации управления, которые способны обеспечить:

- взаимодействие между системой и персоналом с помощью человеко-машинного интерфейса;
- управление инженерными системами посредством контроллеров;
- управление периферийными устройствами.

Для управления оборудованием в системе «умный дом» используется стандартное оборудование, открытые протоколы передачи данных и распределенная база знаний с дистанционным управлением.

В настоящее время технические характеристики современных портативных устройств позволяют решать большое количество задач управления. Для управления системой портативных устройств может использоваться облачный сервер, обеспечивающий сохранение данных о состоянии датчиков и устройств в базе данных и их обработку с целью организации рациональных режимов их совместного функционирования.

Интеллектуальная система способна варьировать конфигурацией образующих компонентов, собирать и анализировать данные, а также настраивать их параметры в зависимости от состояния внешней среды.

Интеллектуальным является здание, оснащенное средствами автоматического контроля, обеспечивающее эффективное использование рабочего

пространства за счет оптимизации основных элементов, а именно: структуры, систем, служб и управления. Комплекс жизнеобеспечения интеллектуального здания в свою очередь образуют следующие компоненты [1]:

- подсистема защиты от проникновения, включающая в себя: средства защиты периметра и контроля доступа в здание (кодовые замки, домофоны, сенсоры);
- подсистема внешнего и внутреннего видеонаблюдения (видеокамеры, видеосерверы);
- подсистема противопожарной безопасности (пожарные датчики, автоматические разбрызгиватели и т. д.);
- подсистема контроля за расходом воды и электроэнергии (управляемые счетчики);
- информационная подсистема (обеспечивает доступ к внутренним и внешним сетевым ресурсам);
- подсистема управления силовым оборудованием и системой освещения;
- подсистема климатического контроля и вентиляции;
- подсистема связи;
- иные подсистемы, не влияющие на безопасность и функционирование здания (например, электронные табло курсов валют и световая реклама).

Первые системы интеллектуального здания имели централизованное управление, они строились на базе основного контроллера, который получал сигналы с пульта, панели, внешних датчиков и различных сенсоров, после чего направлял необходимую команду соответствующему устройству. В централизованной системе контроллер является сложно-техническим устройством от которого зависят все процессы.

В последнее время появилась альтернатива централизованному управлению, идея которой заключается в разделении систем на подсистемы. Задача автоматизации в данном случае разбивается на отдельные составляющие, что позволяет локализовать их решение, а также уменьшить количество связей между подсистемами.

Рассматривая централизованные и распределенные системы интеллектуального здания, необходимо брать во внимание отличия в построении и управлении подсистемами, а также учитывать специфику решаемых задач.

Достоинствами распределенных систем являются:

- высокая производительность за счет объединения ресурсов обработки данных, которая не может быть достигнута на централизованном компьютере;
- надежность;
- нарастающая производительность.

К основным недостатка распределенных систем можно отнести:

- трудности при проектировании;
- сложность оценки их свойств;
- непредсказуемая реакция систем на некоторые события, которая зависит от полной загрузки системы, организации и сетевой нагрузки. Так как величина нагрузки непостоянна и изменяется с течением времени как в меньшую, так и в большую сторону, то время ответа на запрос постоянно варьируется.

К критериям выбора распределенных систем можно отнести: необходимость разделения данных, гибкость использования вычислительных машин на различных операционных системах с целью распределения нагрузки, упрощение модернизации за счет замены элементов.

Основными требованиями, предъявляемыми к распределенным систем, являются: прозрачность, открытость, безопасность, масштабируемость и надежность.

Прозрачность местоположения заключается в скрытии от пользователя физического расположения сетевых ресурсов. Местоположение может изменяться в процессе использования, например, в случае отказа одного ресурса, данные будут перенаправлены на другой, при этом пользователь или приложение ничего не заметят. Распределенная система должна восприниматься как однородная система, а не набор подсистем, взаимодействующих друг с другом.

Масштабируемость – одна из важнейших характеристик систем, которая заключается в способности распределенной системы увеличивать производительность путем добавления оборудования в существующую инфраструктуру.

Переходя к проблемам, стоит отметить существенные недостатки распределенных систем по сравнению с централизованными, а именно:

- проблемы администрирования, которые включают в себя проблемы балансирования нагрузки на узлах, проблемы восстановления данных при возникновении ошибок и сбоев системы, трудности сбора статистики, а также автоматического обновления программного обеспечения.
- проблемы переноса программного обеспечения, заключающиеся в невозможности запуска созданного приложения на различных архитектурах, так как для того, чтобы объединить подсистемы необходимо разработать приложение для каждого компонента с учетом его архитектуры и операционной системы.

В процессе разработки распределенных систем учитываются положения CAP-теоремы, применимой к распределенным системам [2]. CAP (*Consistency Availability Partition*) – это эвристическая теорема о распреде-

ленных вычислениях, определяющая, что в любой сетевой системе, обеспечивающей хранение совместно доступных данных, одновременно могут поддерживаться только два из трех свойств (рис.).

Consistency (согласованность, целостность данных) – при записи данных в распределенное хранилище любой пользователь при обращении может получить последние актуальные данные.

Availability (доступность) – запрос, который направляется к системе должен быть мгновенно обработан. Доступность считается непостоянной, когда обработка запроса происходит не сразу, а спустя некоторое время.

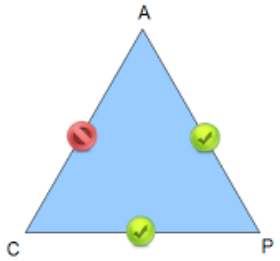


Рисунок. CAP-теорема

Partition tolerance (устойчивость к разделению системы) – потеря сообщений между компонентами системы, а также выход какого-либо компонента из строя не должны никак отражаться на работоспособности системы в целом.

Согласно теореме при построении распределенной системы можно удовлетворить только два из вышеупомянутых свойств, то есть всегда необходимо жертвовать одним из свойств. Однако сразу возникает вопрос об отказе от свойства Partition Tolerance. При отсутствии данного свойства система перестает функционировать, таким образом, формулируется следующее определение CAP-теоремы: при построении распределенной системы, которая способна существовать при отказе ее некоторых компонентов, необходимо жертвовать доступностью или согласованностью.

Изначально понятие Partition Tolerance было введено в теорему потому как не существует такой системы, в которой бы не было проблем отказа сети или не могла случиться ошибка программного обеспечения, или не было проблем с оборудованием. По CAP-теореме существует три возможных подхода к проектированию систем: CP, AP, и AC.

AC-системы гарантируют высокую доступность и целостность до тех пор, пока не происходит сбой в сети. Использование данного типа систем имеет смысл, если оценивается риск, на который можно идти в случае потери сети. Получается так, что можно стремиться к целостности и потерять доступность, либо – к доступности, но потерять целостность.

В рамках разработки проектов, как правило, выбор приходится на CP- или AP-системы.

Несмотря на существующие проблемы, распределенные системы имеют множество преимуществ перед централизованными системами. Каждый процесс обрабатывается конкретным алгоритмом, при этом нет необходимости согласовывать действие с центральным узлом, следовательно, быстродействие системы повышается. Выход из строя одного устройства не вызывает сбой в работе всего комплекса. Распределенные варианты более

мобильны, гибки и унифицированы, что позволяет упросить подбор необходимого оборудования в каждом конкретном случае.

Список используемых источников

1. Игнатов М. С., Немолочнов О. Ф. Интеллектуальные системы поддержки принятия решения // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2008. № 46. С. 14–18.

2. Цветков В. Я., Алпатов А. Н. Проблемы распределенных систем // Перспективы науки и образования. 2014. № 6 (12). С. 31–36.

УДК 654.078
ГРНТИ 49.46.33

СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ОПТИЧЕСКИХ СЕТЕЙ ДОСТУПА

А. С. Дюбов, А. П. Коваленко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Сегодня оптические сети доступа являются наиболее динамично развивающимся сегментом рынка инфотелекоммуникаций. Одним из характерных признаков постоянного развития рынка инфотелекоммуникаций является из года в год совершенствующиеся технологии передачи данных и построения сетей, призванные удовлетворить растущие потребности пользователей. Если на транспортных сетях связи (магистральных линиях связи) переход на оптическое волокно идет полным ходом, то в оптических сетях доступа переход на оптическое волокно становится все ближе и ближе к конечному пользователю.

PON, FTTx, Active Ethernet, Micro SDH, перспективы развития оптических сетей доступа.

Современные оптические сети доступа

На сегодняшний день смело можно заявить, что оптические сети доступа, находясь на начальном этапе своего развития, являются привлекательными и вызывают огромный интерес как со стороны операторов связи, так и со стороны пользователей.

Архитектура построения оптических сетей доступа характеризуется степенью приближения оптического сетевого терминала к пользователю. Международный Союз Электросвязи дает следующую классификацию архитектуры построения оптических сетей доступа, показанной на рис. 1.

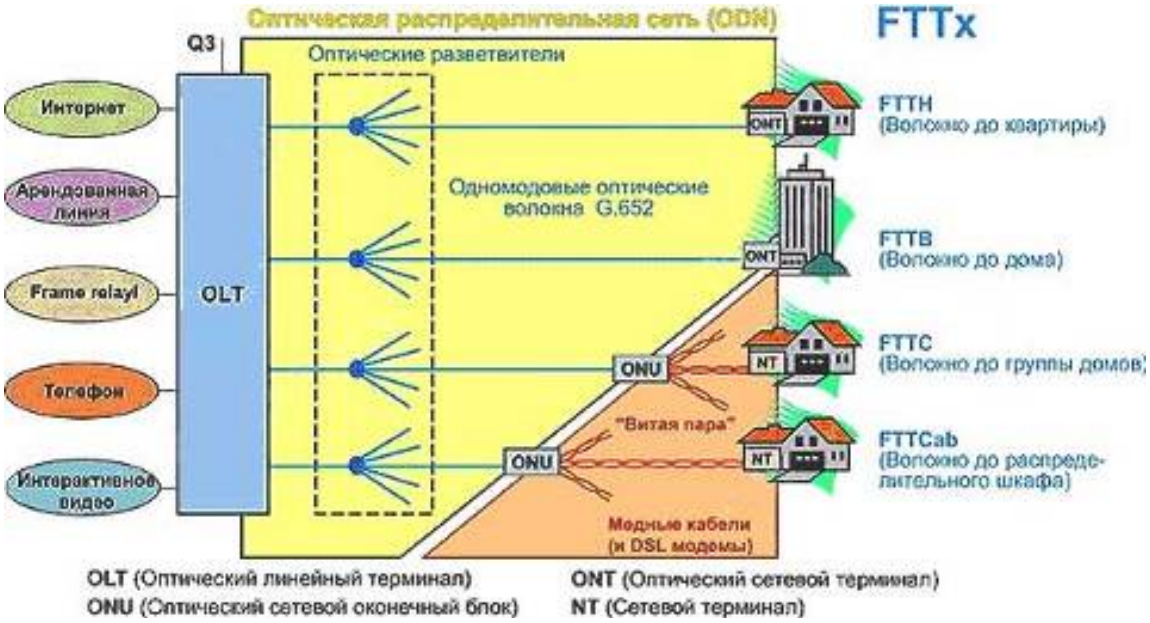


Рис. 1. Архитектуры построения оптических сетей доступа

При выборе архитектуры построения будущей сети следует учитывает достаточно много факторов, одним из главных является – плотность размещения абонентов на проектируемом участке сети. Например, на рис. 1, все архитектуры построения оптических сетей доступа, характеризуются наличием распределительного участка с использованием медного кабеля. Следующим по значимости фактором является и использование конкретной базовой оптической технологии построения сети [1].

В последнее время в оптических сетях доступа наиболее часто используются три интегральные технологии, которые уже успели себя зарекомендовать с лучшей стороны:

– микросеть SDH (*Micro SDH*);
– активные сети Ethernet (*Active Ethernet*, AE);
– пассивные оптические *сети* (*Passive Optical Network*, PON).

Прогнозы потребностей скоростей и объемов трафика на абонентском участке

Современные оптические сети доступа развиваются по трем основным направлениям [2]:

1) увеличение пропускной способности одного канала;
2) увеличение протяженности регенерационного участка сети;
3) увеличение общей емкости систем передачи с помощью различных методов уплотнения каналов (например, благодаря спектральному уплотнению каналов).

Согласно исследованиям компании Cisco, в 2016 году трафик в мобильных сетях в сравнении с предшествующим годом вырос на 63 %. Переходя к абсолютным значениям, то, можно сказать, что в последнем квартале 2016 года. он достиг уровня 7.2 эксабайт в месяц (в последнем квартале 2015 года эта цифра составляла 4.4 эксабайта). Справочно, 1 эксабайт (Эбайт, ЭБ) равен 10^{18} Байт, что соответствует одному миллиарду гигабайт (ГБ) или одному миллиону терабайт. Специалисты из Калифорнийского университета утверждают, что человечеству потребовалось 300 тыс. лет, чтобы создать первые 12 эксабайт информации, зато вторые 12 эксабайт были созданы всего за несколько лет, начиная с 2005 года.

Значительный рост трафика в ближайшие годы обусловлен передачей ультравысококачественных (UHD) 4K видеопотоков. Битрейт для такого видеопотока составляет примерно 18 Мбит/с, что более чем в два раза больше битрейта высококачественного (HD) видео – 1 280 на 720 точек – и в девять раз больше битрейта видеопотока стандартного разрешения (*SD)* – 720 на 576 точек. Прогнозируется, что к 2020 году, 40 % установленных ЖК-телевизоров будут поддерживать UHD – 4 096 точек на 2 160 (рис. 2).

Передача колоссальных видеопотоков высокого качества и появление смартфонов и устройств, поддерживающих воспроизведение такого видео, является также основной причиной роста трафика в мобильных сетях. В 2021 год из 49 эксабайт данных, проходящих через мобильную сеть каждый месяц, 38 эксабайт принадлежат видеоконтенту. Начиная с 2012 года видеопотоки составляют более половины мирового трафика в мобильных сетях.

Как видно из приведенных результатов, трафик в ближайшие годы будет только лишь увеличиваться довольно быстрыми темпами.

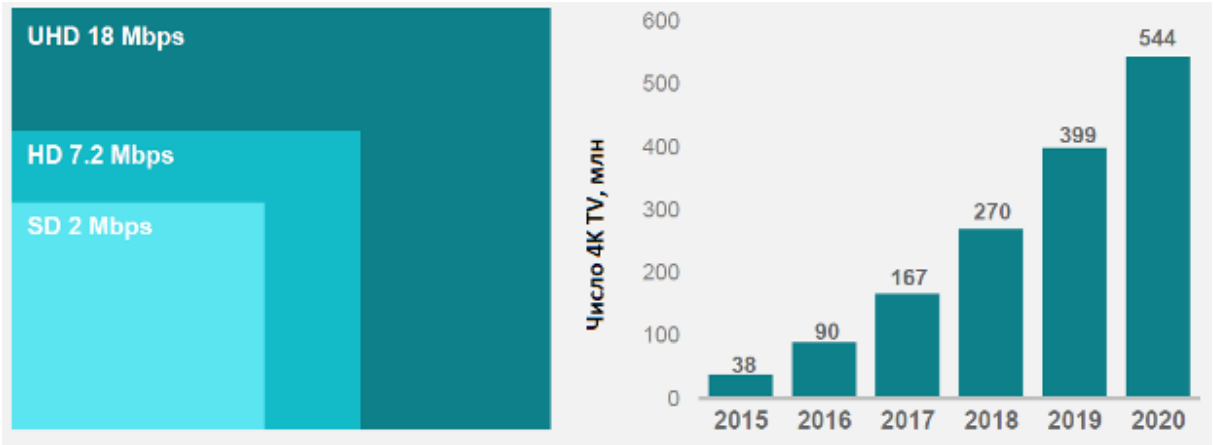


Рис. 2. Увеличение устройств с поддержкой видео 4К

Возможные варианты дальнейшего развития

Одной из главных движущих сил, развивающих инфотелекоммуникации, стала возможность предоставления услуг по передаче видеоконтента самыми разными способами [3].

Рынок инфокоммуникаций, является относительно молодыми огромные инвестиции, вложенные в отрасль, начинают трансформировать мировую инфраструктуру, как в проводной, так и в беспроводной области. Аналитическая компания Insight Research попыталась спрогнозировать дальнейшее развитие событий и описала три возможных варианта преобразований, ожидающих индустрию инфокоммуникаций:

1. Сети продолжают развиваться равномерно, ни одна из технологий связи не уходит с рынка.

2. Сети глобально и повсеместно преобразуются к использованию решений на базе интернет.

3. Сети, в основной своей массе, становятся беспроводными и тотально всеохватывающими.

Перспективные решения развития волоконно-оптических сетей доступа

Дальнейшее развитие волоконно-оптических сетей доступа, по мнению специалистов, будет происходить по двум основным, магистральным, направлениям.

Первое – разработка и внедрение в сетях различного назначения новых волоконно-оптических технологий, направленных на повышение эффективности ВОСП. На магистральных линиях связи основное внимание по-прежнему будет уделяться повышению скорости передачи информации, пропускной способности одного канала, увеличению длины регенерационных участков и повышению надежности. Широкое распространение получат промежуточные оптические усилители и методы волнового мультиплексирования. Доминирующей особенностью развития волоконно-оптических технологий в местных и локальных сетях будет приближение оптического волокна к конечному пользователю сети (абоненту).

Рост потребности в новых видах информационного обслуживания индивидуальных абонентов, а также совершенствование и постоянное снижение стоимости аппаратуры и средств коммутационной техники готовят окончательный переход сетей доступа на оптическое волокно. Локомотивом преобразований и главная роль по скорейшему внедрению оптических сетей доступа принадлежит ГИС Internet. По оценкам специалистов средний объем потока данных в расчете на одного пользователя сети увеличивается ежегодно в восемь раз. Постоянно появляются новые виды услуг. Это выдвигает повышенные требования к скорости передачи информации в сетях

доступа, к пропускной способности одного канала и так далее, удовлетворить которые можно только с помощью все большего и тотального перехода на оптические волокна.

Второе направление развития волоконно-оптических сетей доступа – это создание линий передачи, в которых используются нелинейные свойства оптического волокна, которые позволят обеспечить, так называемый солитонный режим распространения. Импульс лазерного луча состоит из некоторого набора волн, совсем не отличающихся друг от друга по частоте. При распространении этого импульса по оптическому волокну в линейном режиме низкочастотные волны обгоняют высокочастотные, и форма импульса изменяется. В нелинейном режиме работы оптического волокна высокочастотные волны «догоняют» низкочастотные. Происходит формирование оптических солитонов, путем самосжатия импульсов, отличительным свойство которых является распространение в оптическом волокне без изменения формы и длительности. В таких волоконно-оптических сетях доступа можно достичь скорости передачи, равной сотням гигабит в секунду при длине регенерационного участка, достигающего тысячи километров.

Список используемых источников

1. Архитектура оптических сетей доступа FTTH (Fiber-to-the-Home) [Электронный ресурс]. URL: https://www.cisco.com/c/dam/global/ru_ru/assets/downloads/cisco_ftth_architecture.pdf. (дата обращения 22.02.2019).

2. Cisco прогнозирует почти 11-кратный рост мирового трафика мобильной передачи данных с 2013 по 2018 гг. [Электронный ресурс]. URL: https://infocity.az/2014/02/cisco-прогнозирует-почти-11-кратный-рост-мир/ (дата обращения 28.03.2019).

3. Три варианта развития мировых телекоммуникаций [Электронный ресурс]. URL: https://nag.ru/articles/reviews/15578/tri-varianta-razvitiya-mirovyih-telekommunikatsiy.html. (дата обращения 11.01.2019).

УДК 004.925.86
ГРНТИ 20.15.05

ВЛИЯНИЕ ГОЛОСОВЫХ ЗАПРОСОВ НА SEO

К. А. Ефимов, А. А. Шиян

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Интернет становится наиболее популярной площадкой для развития бизнес проектов. Для того, чтобы заработать аудиторию, либо расширить клиентскую базу владельцы сайтов прибегают к различным методам seo продвижения. Одним из таких способов является оптимизация сайта под голосовой поиск, который набирает большую популярность в последнее время.

поисковый запрос, голосовой поиск, seo, оптимизация сайта, интернет продвижение, voice search.

В современном мире интернет становится незаменимой вещью, которая пронизывает все сферы нашей жизни. Все большее количество людей начинают пользоваться всемирной сетью, поэтому постепенно различные компании, от больших до маленьких, делают себе сайты, на которых представлен их ассортимент, газеты и журналы делают виртуальные копии, а телевизионное программы, которые мы могли наблюдать по телевизору, теперь транслируются в интернете и имеют свои новостные порталы. Интернет – это миллионы пользователей, сотни или даже тысячи из которых являются потенциальными клиентами или заинтересованной публикой [1].

Компьютерные технологии развиваются, а вместе с ними и интернет. Такие повседневные задачи как поиск информации, взаимодействие с другими людьми стали намного проще. В связи с большим количеством возможностей – отрасли, связанные с бизнесом и масс-медиа, пытаются использовать данные преимущества для завоевания новой аудитории. Для того, чтобы выделиться компании разрабатывают дорогие сайты с богатым функционалом и красивым дизайном, но этого может быть недостаточно, и сайт может запросто затеряться среди сотни других сайтов, тогда же владельцы этих сайтов и обращаются к инструментам продвижения сайта.

Продвижение сайта – это комплекс мер по обеспечению посещаемости сайта целевыми посетителями. Целевые посетители – это потенциальные потребители, которые заинтересованы в приобретении товаров или услуг, представленных на продвигаемом сайте [2]. Одним из важнейших этапов продвижения сайта является поисковая оптимизация, она же SEO (*Search Engine Optimization*, поисковая оптимизация) – комплекс мер по внутренней и внешней оптимизации, для поднятия позиций сайта в результатах выдачи

поисковых систем по определенным запросам пользователей, с целью увеличения трафика (для инфоресурсов) и потенциальных клиентов (для коммерческих ресурсов) и последующей монетизации этого трафика [3]. Но даже если и обратиться к методам оптимизации, то это не гарантирует успех, ведь методов большое множество, а их актуальность меняется со временем, и чтобы прийти к нужному результату необходимо постоянно следить за новинками в этой сфере и выстраивать грамотную стратегию по продвижению. Одним из новых способов продвижения сайта является адаптация его под голосовой поиск.

Голосовой поиск – технология распознавания речи, позволяющая осуществлять перевод речевого запроса пользователя в текстовый вид, который затем передается в стандартную систему поиска по базе данных. У голосового поиска есть свои особенности, которые нужно учитывать при оптимизации сайта, они отличаются от печатных запросов. Во-первых, голосовой запрос чаще более длинный, в сравнении с фразами, которые пользователи вбивают в поисковую строку браузера. Еще одна особенность – это то, что запросы начинаются с вопросительных фраз, потому что люди спрашивают вопрос у голосового помощника, в то время как в печатном запросе сразу пишут суть вопроса. Также нужно учитывать, что стиль голосовых запросов разговорный (рис. 1, 2).

Технология голосового поиска очень удобна, благодаря неё не нужно тратить время и усилия, чтобы ввести запрос, достаточно просто озвучить его голосовому помощнику для того, чтобы он сделал всю работу за вас, что сэкономит время и позволит параллельно заниматься другими делами. По данным Google с 2008 по 2016 годы количество голосовых запросов выросло в 35 раз. В наше время уже все гаджеты поддерживают данную функцию, а также множество компаний трудятся над устройствами управляемые голосовым поиском, что повышает актуальность данной технологии. Также актуальность растет за счет того, что все большее количество людей пользуются мобильными телефонами, ведь данная технология просто идеально подходит для мобильных устройств. По данным исследования Stone Temple Consulting, 56 % поискового трафика сайты получают с мобильных гаджетов и 44 % – с персональных компьютеров. Из мобильного трафика 65 % запросов печатаются вручную, 35 % поступают от голоса. На рис. 1 представлена статистика и прогноз по голосовым запросам.

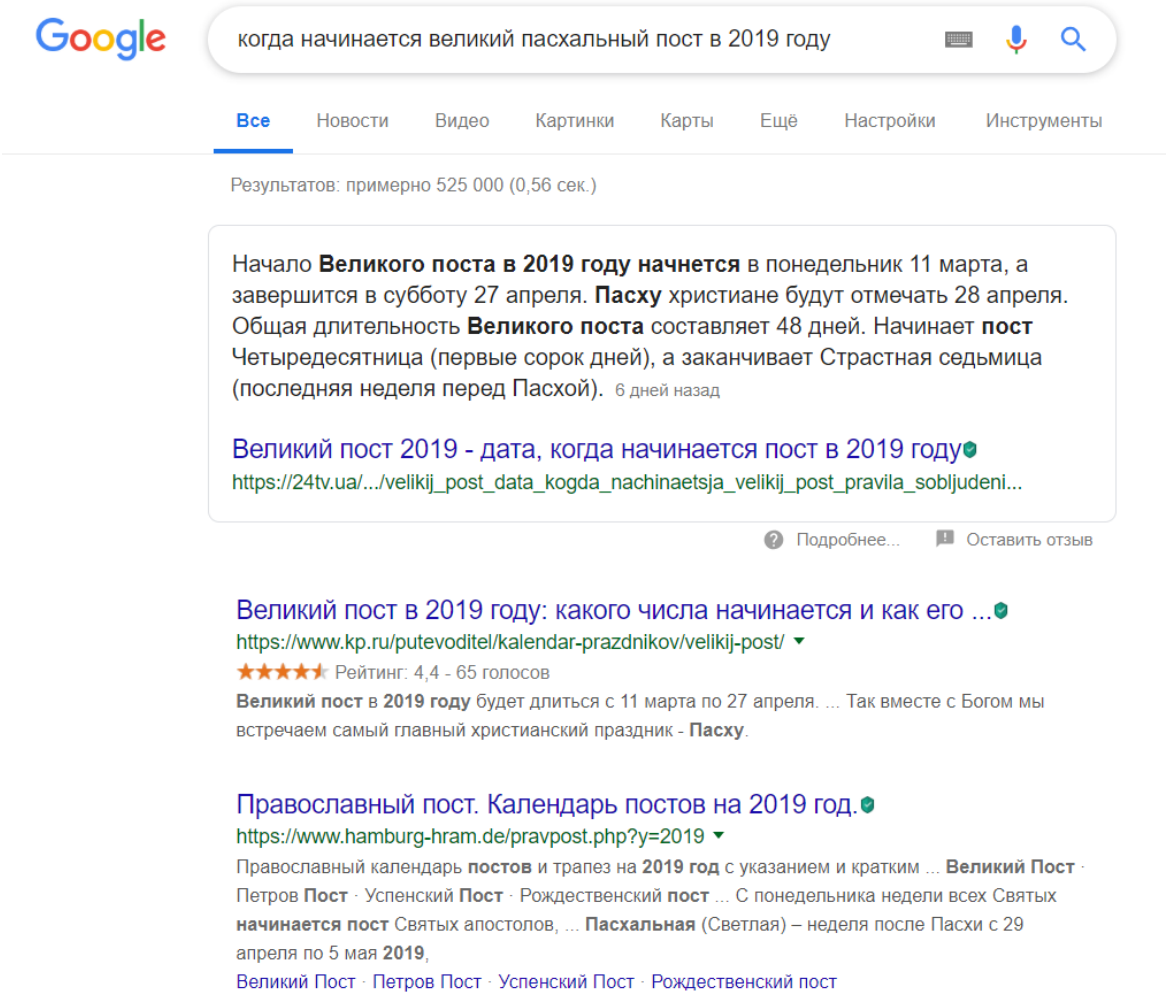


Рис. 1. Пример голосового запроса

Аналитическому агентство We Are Social в своих отчетах указывает на то, что мобильными телефонами в 2018 году пользуются 5,135 млрд человек, то есть, опираясь на эти данные, можно сделать вывод, насколько большая аудитория использует голосовой поиск. Также сейчас набирают популярность умные колонки, такие компании как Amazon, Google, Apple, Яндекс уже создали свои версии гаджета. Умная колонка – это беспроводной динамик со встроенным микрофоном и голосовым помощником, работающим на основе искусственного интеллекта. Микрофоны позволяют помощнику принимать ваши команды и управлять самой умной колонкой, вашими устройствами умного дома и отвечать на справочные вопросы. При этом можно отследить закономерность, что рост и развитие не прекращается, а совершенствование новых технологи и появление новых устройств будет способствовать новым перспективам. Так, согласно прогнозу Comscore, к 2020 году 50 % всех запросов станут голосовыми (рис. 3).

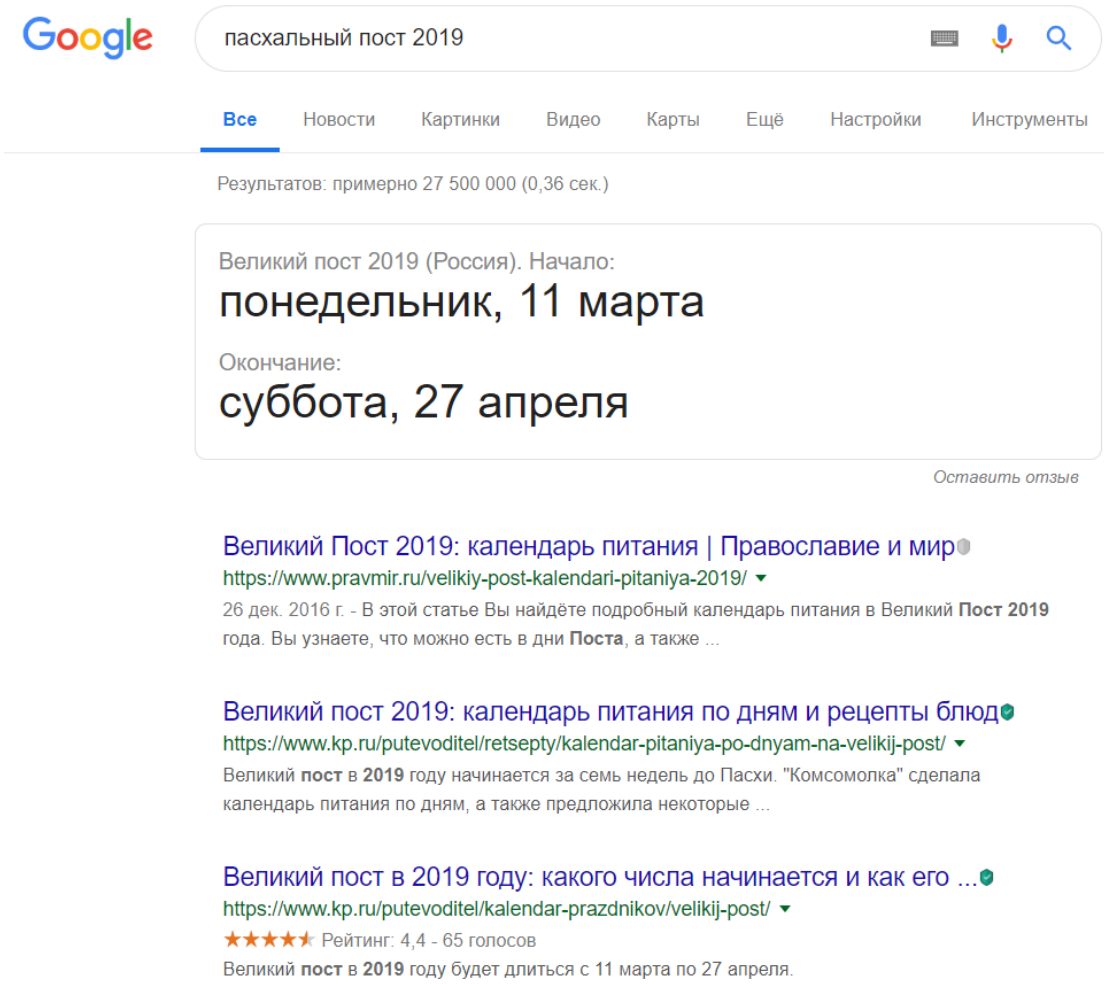


Рис. 2. Пример голосового запроса

Рис. 3. Диаграмма голосовых запросов

В силу того, что голосовые запросы отличаются от печатных, нужно регулярно корректировать семантику ресурса. Подавляющее большинство сделанных с помощью голоса запросов выполнены с мобильных, а значит важно адаптировать ресурс для мобильных устройств. Но наблюдая за стремительным ростом данной технологии можно понять, что данные изменения необходимы и повлекут за собой приток новой аудитории, при том, что полностью перерабатывать сайт не потребуется. Поэтому при оперативном воздействии на свой сайт можно продвинуть его на высокие строки в поисковых системах и тем самым обойти конкурентов.

Список используемых источников

1. Ашманов И. С., Иванов А. А. Оптимизация и продвижение сайта в поисковых системах. Санкт-Петербург, 2012. 132 с.

2. . Бабаев А. Н., Евдокимов С. И., Штарев А. М. Раскрутка: секреты эффективного продвижения сайтов. СПб., 2013. 347 с.

3. Фаустова К. И. Значение SEO для эффективных продаж в интернете // Территория науки. 2015. № 3.

УДК 371.26
ГРНТИ 20.53.19

ФОРМИРОВАНИЕ МОДЕЛИ СИСТЕМЫ КОНТРОЛЯ И ОЦЕНКИ ЗНАНИЙ ОБУЧАЮЩИХСЯ

А. О. Жаранова, М. В. Котлова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обоснована актуальность внедрения автоматизированных систем в современный процесс образования. Проведен анализ современных подходов к учебному процессу и контролю знаний. Определены основные недостатки существующих систем оценки качества знаний обучающихся. Приведены формы и методы проведения контроля и оценки знаний. Предложена модель системы контроля и оценки знаний на базе адаптивного метода. Описаны основные элементы модели. Определены перспективы развития систем контроля и оценки знаний.

контроль знаний, оценка знаний, адаптивный метод, модель системы, обучение, учебный процесс, тестирование.

Контроль знаний – важная часть работы с обучаемыми, своего рода обратная связь. Целью процесса контроля знаний является диагностирование знаний и оценка качества и эффективности проводимого обучения, а также

использование полученных данных для усовершенствования учебной программы и развития навыков обучающихся.

Современный подход к учебному процессу немыслим без автоматизированных систем оценки качества знаний. Однако существующие на сегодняшний день системы контроля знаний имеют ряд недостатков, таких как: узкая применимость, жесткость алгоритмов подсчета итоговых баллов, отсутствие индивидуального подхода к обучающемуся (одного из основных принципов педагогики), сложность выявления причин недостатка знаний [1].

Вследствие этого современное образование ставит перед собой задачу внедрения автоматизированных систем для обеспечения эффективности обучения и повышения знаний и умений обучающихся. Важной составляющей обучения, без которой не может идти речь об эффективности усвоения знаний, является обратная связь. Впоследствии данные, полученные во время контроля знаний обучающих, могут использоваться при корректировке учебного плана и изменении методики преподавания. Таким образом, особую важность приобретают разработка алгоритмов и систем контроля знаний.

Существует множество форм и методов контроля знаний, каждые из которых имеют свои преимущества и недостатки. Универсальной формой является тестовый контроль, который позволяет выявить конкретные пробелы в знаниях обучающихся. Подобная форма контроля знаний имеет ряд преимуществ: возможность использования при самообучении, объективность оценки, дифференциация заданий по уровню сложности, прогнозирование итогов обучения.

Методы контроля знаний можно разделить на три класса: неадаптивные, частично адаптивные, полностью адаптивные [2]. Набор заданий при использовании неадаптивного метода не зависит от индивидуальных особенностей обучающихся и является либо одинаковым для всех, либо случайным, что способствует искажению результатов из-за разного уровня сложности вопросов в двух случайно сформированных тестах. Частично адаптивный метод учитывает некоторые индивидуальные особенности обучающегося перед проведением контроля или же основывается на структуре учебного плана. При использовании адаптивного метода сценарий контроля формируется динамически и зависит от большинства индивидуальных особенностей обучающегося.

Помимо методов контроля существует множество методов оценки знаний, которые по способу вычисления оценки также делятся на три группы: на базе числовых множеств, на базе рассчитываемых вероятностей и на базе классификационных таблиц [2]. Модели на базе числовых множеств представляют собой вычисление некоторой величины с последующим сравнива-

нием ее с заданными заранее граничными значениями (интервалами оценивания), позволяющими представить оценку числом. Самой распространенной моделью данного типа является простейшая модель, где оценкой может служить сумма баллов, полученных при прохождении тестирования. Модели на базе рассчитываемых вероятностей демонстрируют вероятность правильных ответов в зависимости от уровня знаний обучающегося, другими словами, показывает, заслуживает ли обучающийся полученную оценку. Основной идеей модели на базе классификационных таблиц является отнесение обучающегося к одному из заданных классов, используя признаки, определяющие данного учащегося. Для классификации по уровням подготовки используется алгоритм, основанный на вычислении оценок, представляющий собой таблицу с набором признаков (количество заданий, средний балл и другие). Таким образом, существуют разные модели для оценивания и контроля знаний, и выбор конкретной модели или их комбинации зависит от множества факторов: цели контроля, параметров (числа заданий, ответов, попыток прохождения, времени), типов заданий, знаний и навыков обучающихся и других.

Модель адаптивного контроля знаний представлена на рис. 1.

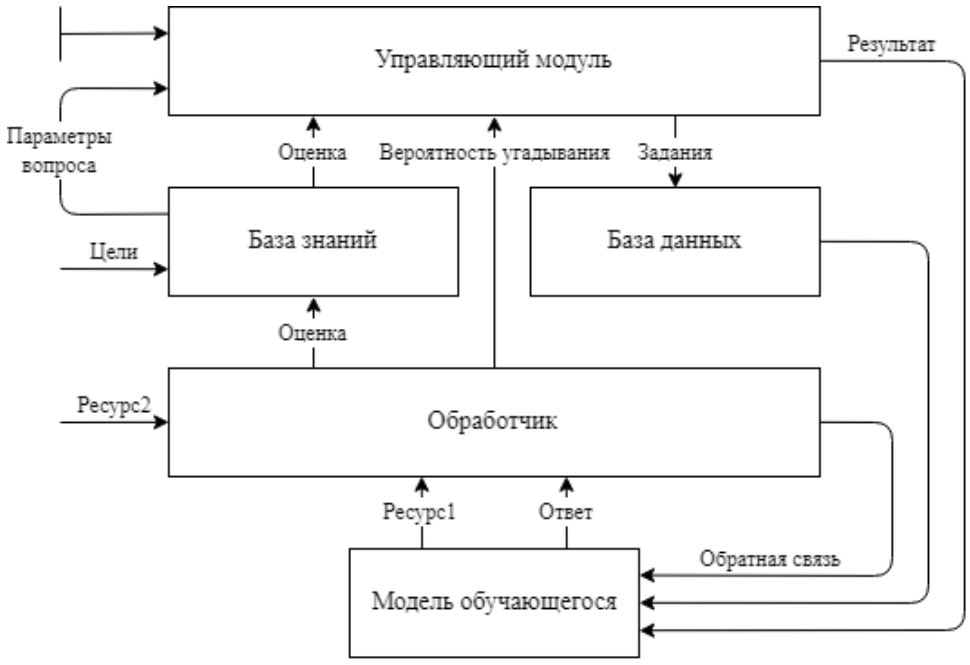


Рис. 1. Модель адаптивного контроля знаний

Алгоритм процесса контроля знаний имеет следующий вид: обучающийся выполняет задание. Результат (ответ, время прохождения, сложность, тип задания и др.) помещается в модель обучающегося, включающую в себя информацию об обучающемся, а затем передается обработчику. Он, в свою очередь, анализирует ответ обучающегося на основе используемого

алгоритма, учитывает внешние (например, система оценивания) и внутренние (например, время контроля) ресурсы, выставляет оценку за выполненное задание. База знаний получает данные об оценке от обработчика и отправляет в управляющий модуль параметры нового вопроса, а также общую оценку с учетом целей контроля. Управляющий модуль выбирает новый вопрос из базы данных на основе полученных параметров. В конце контроля, учитывая погрешности тестирования (вероятность угадывания), отправляет финальную оценку обучающемуся.

Преимуществами данной модели являются: возможность интеграции в любую предметную область, экономия времени при формировании заданий и проверке результатов, точность оценки знаний, помощь при планировании процесса обучения, доступность тестов и результатов в любое время, индивидуальность вариантов заданий.

В системе предлагается два вида тестирования: итоговое по всему курсу и тренировочное на базе адаптивной модели, применяемое для закрепления знаний по дисциплинам [3].

Итоговый тест представляет собой набор из вопросов каждой темы и каждого уровня сложности. Таким образом, тест начинается с простого, среднего и сложного вопросов по первой теме, затем идут три уровня сложности по второй теме и далее до последней темы. По окончании теста выносится итоговый балл по дисциплине. Тест данного типа обучающийся может проходить любое количество раз как в качестве тренировки, так и в качестве действующего итогового теста. Контрольные баллы заносятся в рейтинг обучающегося, где их также может просмотреть преподаватель. Подобная система рейтинга способствует стимулированию деятельности обучающегося, а также помогает спрогнозировать итоговую оценку по дисциплине.

Второй вид контроля – тренировочный тест на базе адаптивной модели (рис. 2).

В модели студента по каждому разделу дисциплины обучающемуся назначается один из трех статусов знаний по дисциплине: «Низкий», «Нормальный» и «Высокий». Во время прохождения первого тестирования у каждого обучающегося по каждому из разделов по умолчанию установлен «Низкий» статус знаний. Это сделано для того, чтобы слабоуспевающие обучающиеся не испытывали беспокойства-тревоги из-за невозможности выполнения более сложных заданий. Это одна из психологических характеристик, которые, в свою очередь, являются важными составляющими адаптивного контроля знаний.

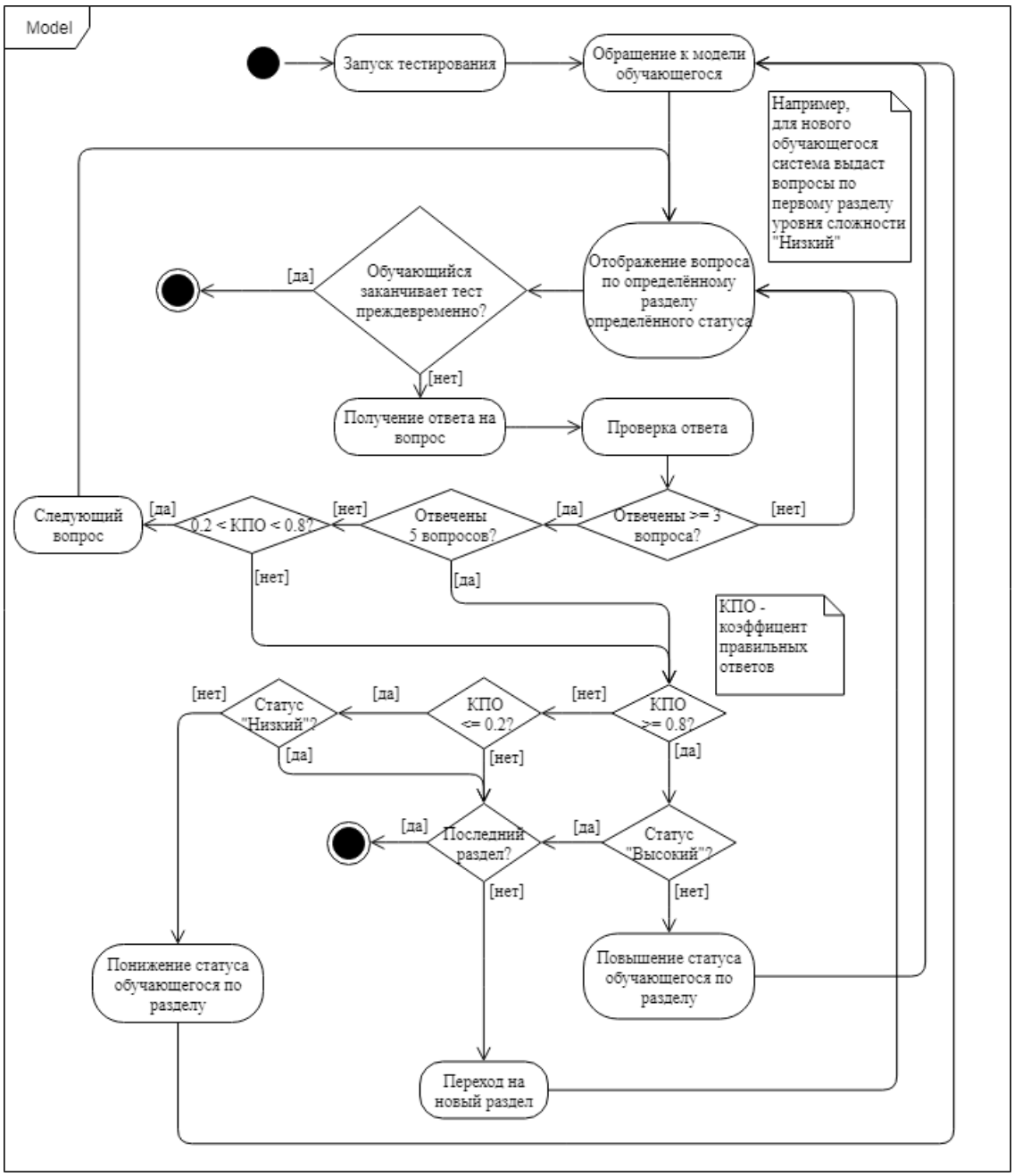


Рис. 2. Диаграмма деятельности прохождения тестирования

Преподаватель устанавливает границу заданий одного уровня сложности одного раздела дисциплины (в рассмотренном случае она равна пяти) и минимальное количество заданий для определения статуса знаний (3), определяет границы коэффициента правильных ответов (далее – КПО), равное отношению числа правильных ответов к общему количеству вопросов, для повышения и понижения статуса знаний. Для повышения статуса знаний по разделу в рассмотренном примере обучающемуся необходимо выполнить следующее условие: КПО не менее 0,8. Понижение статуса знаний проис-

ходит при КПО не более 0,2. В промежутке от 0,2 до 0,8 статус знаний сохраняется и происходит переход к следующему разделу. Если смена статуса знаний произошла, то система запускает тестирование для того же раздела, но со сложностью, соответствующей обновленному статусу знаний. После того, как студент завершает контроль знаний по последнему разделу дисциплины, тестирование завершается, и система выводит уровень подготовленности обучающегося по каждому из разделов в процентах. При повторных прохождениях тестирования вопросы по разделам формируются в зависимости от статуса знаний обучающегося. Если статус знаний в разделе соответствует отметке «Нормальный», то обучающийся получит задания соответствующей сложности.

В перспективах развития представленной работы планируется внедрение более сложных методов оценки знаний обучающихся, а также интеграция модуля автоматической генерации контрольно-измерительных материалов с применением искусственного интеллекта.

Список используемых источников

1. Козлов С. А. Разработка автоматизированной системы контроля знаний на основе интеллектуальных средств // Информатизация образования и науки. 2011. № 2 (10). С. 59–66.

2. Белоус В. В., Домников А. С., Карпенко А. П. Тестовый метод контроля качества обучения и критерии качества образовательных тестов. Обзор [Электронный ресурс] // Наука и образование: электронное научно-техническое издание. 2011. № 4. URL: http://technomag.bmstu.ru/doc/184741.html (дата обращения 27.01.2019).

3. Ворошилова Е. В., Котлова М. В. Модели и средства итогового контроля знаний // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 239–243.

Статья представлена заведующим кафедрой,
доктором технических наук, профессором Л. К. Птицыной.

УДК 658.5
ГРНТИ 50.53.19

АВТОМАТИЗАЦИЯ ПАТЕНТНЫХ ИССЛЕДОВАНИЙ НА ПРЕДПРИЯТИЯХ СВЯЗИ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

К. В. Жолобова, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются пути снижения издержек и повышения качества отчетов о патентных исследованиях на предприятиях связи за счет технологии электронных форм документов в составе подлинников конструкторской документации в условиях цифровой экономики. Предложена интерфейсная среда форм отчетных документов, сведения из которых являются информационной основой для принятия решений по жизненному циклу объектов промышленной собственности, изделий и их составных частей. Использование оригинальных программных решений позволяет обеспечить полноту сведений, имеющих юридическую значимость, например, для ведения патентных формуляров на объекты техники.

автоматизация научных исследований, отчет о патентных исследованиях, патентный формуляр, технология электронных форм документов.

В условиях цифровой экономики возросла роль технологий обработки больших массивов данных, которые широко применяются в обеспечении жизненного цикла продукции, автоматизации научных исследований, например, при разработке различных объектов техники [1]. На рисунке приведен фрагмент процесса разработки изделий, который содержит процедуры систематизации патентной и научно-технической информации (далее – НТИ) с целью определения требуемого технического уровня [2].

В нашей стране, учитывая многоаспектность НТИ и их различную целевую направленность, федеральным органом исполнительной власти, осуществляющим функции по правовой защите интересов государства в процессе экономического и гражданско-правового оборота результатов научно-исследовательских, опытно-конструкторских и технологических работ военного, специального и двойного назначения, регламентированы положения о «патентном ландшафте».

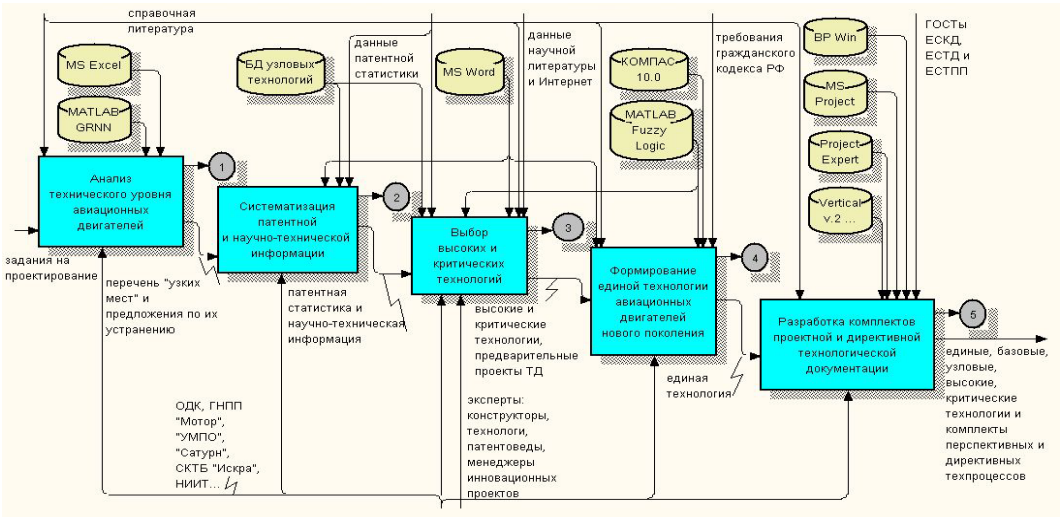


Рисунок. Основные процедуры разработки системотехнических решений

Патентный ландшафт – это информационно-аналитическое исследование патентной документации, показывающее в общем виде патентную ситуацию в определенном технологическом направлении либо в отношении патентной активности субъектов инновационной сферы с учетом временной динамики и территориального признака: страны, региона или в мировом масштабе [3].

Для обработки НТИ создан ряд программных средств, основные характеристики которых представлены в таблице. Программные средства могут использоваться разработчиками как непосредственно на предприятиях, так и в режиме он-лайн посредством услуг различных патентных ведомств в произвольных формах отчетности [4].

ТАБЛИЦА. Программные средства анализа НТИ

Продукт	Разработчик	Назначение (функции)	Источник
PatSearch	АО «АЙ-ТЕКО» (Россия)	Поиск в БД по патентам, сортировка, фильтрация	http://www1.fips.ru/wps/wcm/connect/
LexisNexis PatentSight®	LexisNexis (США)	Поиск в БД по патентам, сортировка, фильтрация, сравнение, анализ, создание отчетов; управление проектами	https://www.lexisnexis.ru
PatBase; PatBase Analytics	Minesoft (Великобритания)	Поиск в БД по патентам, сортировка, фильтрация, сравнение, анализ, создание отчетов;	https://minesoft.com
Patent iNSIGHT Pro; PatSeer	Gridlogics Technologie Pvt Ltd. (Индия)	Поиск в БД по патентам, сортировка, фильтрация, сравнение, анализ, создание отчетов; управление проектами	http://gridlogics.com

Нормативно-техническими документами для целей разработки, постановки продукции на производство и обеспечения последующих этапов ее жизненного цикла предусмотрено использование НТИ [5, 6, 7, 8].

Анализ доступных источников, в части технических заданий предприятий связи на разработку объектов техники, показал включение в их состав требований по проведению патентных исследований, которые регламентированы действующими стандартами. Однако содержание значительной части проанализированных отчетов о патентных исследованиях носит формальный характер: установленные формы представления НТИ не соблюдаются; данные приводятся не системно или неполно.

Повышение качества отчетов о патентных исследованиях на предприятиях связи может быть достигнуто за счет технологии электронных форм документов в составе подлинников конструкторской документации. Прототипы программных средств по некоторым отчетным формам созданы:

− программа преобразования результатов патентного поиска, сохраненного из сети патентной информации Espacenet в RSS-формате, в формат таблицы «В.6.1. Патентная документация» приложения В ГОСТ Р 15.011-96. Программа использует XSLT-процессоры, встроенные в Internet Explorer 7 и выше, Word 2003 и выше [9];

− программа визуализации результатов поиска в сети патентной информации Espacenet в формате таблицы "Количество опубликованных охранных документов по годам (изобретательская активность)" отчета о поиске по ГОСТ Р 15.011-96 [10].

Существенное снижение издержек может быть достигнуто за счет неочевидной взаимосвязи результатов патентных исследований, которые получены на этапе разработки объекта техники, и потенциальными рисками патентной чистоты при эксплуатации изделий, включая ситуации поставок в другие страны. Определенные «гарантии» в таких ситуациях должны быть приведены в «патентном формуляре».

Патентный формуляр предназначен для представления его организациям (органам), решающим вопросы реализации объекта в стране и за рубежом, в том числе возможности и условий экспорта, капитального строительства, продажи лицензий, передачи технической документации за границу, а также экспонирования на международных выставках и ярмарках [11].

Разработка «Патентного формуляра на объект техники», его оформление и содержание регламентированы государственным стандартом [11].

Сведения для заполнения различных разделов «Патентного формуляра» должны поступать на основании результатов патентных исследований.

Положение усугубляется при наличии в объекте технике многочисленных составных частей изделия различных предприятий-разработчиков и их

вложенности по схеме деления. Патентный формуляр составляет или корректирует (если он был ранее составлен) держатель подлинников технической документации на основе отчета о патентных исследованиях, который формируется в этом случае с участием различных предприятий-разработчиков составных частей изделия. Это приводит к значительным сложностям ведения подлинников конструкторской документации, ее актуализации и гармонизации по отношению к результатам деятельности предприятий-разработчиков составных частей изделий в ходе их сопровождения на различных этапах жизненного цикла [12].

При внесении изменений в подлинник патентного формуляра держатель подлинников технической документации сообщает предприятиям (организациям) - держателям учтенных копий патентного формуляра текст изменения, организацию (предприятие)-исполнителя и дату отчета о патентных исследованиях, на основании которого внесены эти изменения [11].

Предлагаемая интерфейсная среда форм отчетных документов патентных исследований содержит документы, которые представлены в приложении А, приложении В (за исключением форм В.6.4-В.6.6), приложении Д (за исключением форм Д.2.1, Д.3) по ГОСТ 15.011-96.

В ходе разработки интерфейсной среды выработана модель автоматизированного ведения форм отчетных документов патентных исследований и информационные модели форм отчетных документов патентных исследований. Представлены в формализованном виде согласно требованиям ЕСПД «Описания постановок задач» для разработки форм отчетных документов патентных исследований. Разработаны блок-схема и макет программы "Интерфейсная модель форм отчетных документов патентных исследований".

Внедрение данного предложения на предприятии связи с реализованными прототипами PDM/PLM, CAD, CAM и ERP систем, например, на основе решений «ЛОЦМАН:PLM АРХИВ»; «1С:PDM Управление инженерными данными 3» для «1С:ERP», приведет к повышению достоверности данных патентного формуляра, об изменениях подлинников документации на изделие, в частности, отчетов о патентных исследованиях, существенному сокращению продолжительности работ по формированию документов при организации и выполнении патентных исследований.

Результаты оценки качества разработанного макета программы, которая проведена с применением методов квалиметрии и подходов по ГОСТ Р ИСО/МЭК 25010-2015, характеризуются существенным приростом показателей качества существенных свойств, интегральных и обобщенного показателя качества по отношению с существующей организации и проведения патентных исследований.

При незначительной доработке макет программы может быть доведен до уровня промышленного изделия.

Таким образом, интерфейсная среда форм отчетных документов, сведения из которых являются информационной основой для принятия решений по жизненному циклу объектов промышленной собственности, изделий и их составных частей, позволяет обеспечить полноту сведений, имеющих юридическую значимость, например, для ведения патентных формуляров на объекты техники.

Список используемых источников

1. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб. : ГУАП, 2016. 325 с.

2. Ахмедзянов Д. А., Поезжалова С. Н., Селиванов С. Г. Концепция совершенствования НИР и НИРС для развития инновационной направленности проектов // Молодой ученый. 2011. № 6. Т. 2. С. 122–136. URL https://moluch.ru/archive/29/3274/ (дата обращения 20.01.2019).

3. Приказ Федеральной службы по интеллектуальной собственности Минэкономразвития России «Об утверждении Методических рекомендаций по подготовке отчетов о патентном обзоре (патентный ландшафт)» от 23.01.2017 № 8.

4. Егармина А. Д. Аналитические возможности патентных исследований // Правовая защита, экономика и управление интеллектуальной собственностью: материалы научно-практической конференции, Екатеринбург, 24 апреля 2014 г. Екатеринбург: УрФУ, 2014. С. 59–69.

5. ГОСТ Р 15.011-96. Система разработки и постановки продукции на производство (СРПП). Патентные исследования. Содержание и порядок проведения.

6. ГОСТ 34.602-89. Техническое задание на создание автоматизированной системы.

7. ГОСТ 15.016-2016. Система разработки и постановки продукции на производство. Техническое задание. Требования к содержанию и оформлению.

8. ГОСТ Р 15.301-2016. Система разработки и постановки продукции на производство (СРПП). Продукция производственно-технического назначения. Порядок разработки и постановки продукции на производство.

9. Свидетельство на программу для ЭВМ № 2014613878 Российская Федерация. Программа визуализации результатов поиска в сети патентной информации Espacenet в формате таблицы "Патентная документация" отчета о поиске по ГОСТ Р 15.011-96 / Холод С.В.; правообладатель Холод С.В. – № 2014611195; заявл. 18.02.2014; опубл. 20.05.2014, Бюл. № 5. – 1 с.

10. Свидетельство на программу для ЭВМ 2016613261 Российская Федерация. Программа визуализации результатов поиска в сети патентной информации Espacenet в формате таблицы «Количество опубликованных охранных документов по годам (изобретательская активность)» отчета о поиске по ГОСТ Р 15.011-96 / Холод С. В.; правообладатель Холод С.В. № 2016610465; зявл. 25.01.2016; опубл. 20.04.2016, Бюл. № 4. 1 с.

11. ГОСТ 15.012-84 Система разработки и постановки продукции на производство (СРПП). Патентный формуляр.

12. Полпудникова Н. В., Шестаков А. В. Предложения об автоматизированном ведении подлинников конструкторской документации предприятия связи на основе технологии распределенных реестров // Актуальные проблемы инфотелекоммуникаций в

науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. Т. 2. С. 535–540.

УДК 004.056.53
ГРНТИ 50.37.23

АДАПТИВНЫЙ ФАЗЗИНГ ВЕБ-ПРИЛОЖЕНИЙ НА ОСНОВЕ МОДЕЛИ ВЕБ-РЕСУРСА

А. А. Зверев, Д. О. Маркин

Академия Федеральной службы охраны Российской Федерации

В работе рассмотрен способ построения автоматизированного тестирования (фаззинга) удаленных веб-ресурсов и веб-приложении на основе построения описательной модели ресурса и с применением сети веб-прокси серверов, реализующих концепцию активных данных. Описана структурная и функциональная модель системы, реализующей адаптивный фаззинг, типовая структурно-логическая схема базы данных. Целью работы является повышение эффективности инструментов фаззинга веб-приложений при поиске уязвимостей.

фаззинг, веб-приложения, активные данные, фаззер, модель веб-ресурса, веб-прокси.

Повсеместное внедрение информационных технологий, развитие цифровой экономики, а также повышение доступности и цифровизация государственных услуг обуславливает потребность в повышенном внимании к информационной безопасности (ИБ) предоставляемых услуг в целом и обеспечении защищенности веб-ресурсов, в частности. Как показывает статистика современные веб-приложения имеют большое число проблем, связанных с обеспечением ИБ, а поиск уязвимостей требует серьезных вычислительных ресурсов и высокой квалификации персонала, отвечающего за вопросы ИБ. В связи с этим актуальной задачей является создание автоматизированных и автоматических средств поиска уязвимостей веб-приложений, позволяющих осуществлять эффективный анализ защищенности веб-ресурсов.

Одним из эффективных способ решения данной задачи является фаззинг веб-приложений [1, 2, 3]. Данный метод тестирования представляет собой тестирование на основе модели «черного» ящика (в условиях отсутствия сведений о приложении) или в отдельных случаях модели «серого» ящика (имеется некоторая информация). Фаззинг может использоваться и в

условиях модели «белого» ящика (при наличии полной информации о приложении) как эффективное средство тестирования корректности обработки входных данных.

На сегодняшний день существует множество фаззеров для веб-приложений: Web Scarab, BurpSuite, Skyfish, SPIKE Proxy, OWASP WSFuzzer (SOAP), Rfuzz, Fuzzops, PowerFuzzer. Однако данные средства имеют ряд недостатков. Существенной проблемой при построении эффективного фаззера веб-приложений является отсутствие средства автоматизированного создания модели веб-ресурса, на основе которой могли бы формироваться исходные данные для фаззинга.

Для эффективного фаззинга необходимо выполнение следующих требований: возможность неоднократного использования; состояние и глубина процесса; отслеживание, покрытие кода и система показателей; определение ошибок; ресурсные ограничения. Схема фаззинга с обратной связью и интеллектуальным формированием входных данных представлена на рис. 1.

Рис. 1. Схема фаззинга с обратной связью при формировании входных данных

Представленный вариант автоматического фаззинга позволяет повысить эффективность анализа объекта тестирования за счет адаптивного формирования входных данных. Для моделирования данного процесса необходимы специальные средства моделирования, способные формализовать все аспекты случайности и предоставить инструменты реализации всех этапов управления тестированием. Байесовские модели имеют широкий потенциал средств для решения перечисленных выше задач тестирования веб-приложений [1]. На рис. 2. приведена концептуальная модель статических и динамических байесовских сетей, предложенная в [3], для моделирования процесса управления тестированием веб-приложений методом фаззинга.

Очевидно, что чем более качественно будут формироваться входные данные для очередной итерации тестирования, тем выше вероятность обнаружения ошибок либо недекларируемых возможностей. В то же время, большинство современных фаззеров построено на основе базы данных известных сигнатур разрушающих программных воздействий и практически

не учитывают актуальную модель исследуемого объекта. Наличие такой модели позволяет учитывать важную информацию при формировании очередной выборки входных данных и, соответственно, повышает результативность фаззинга.

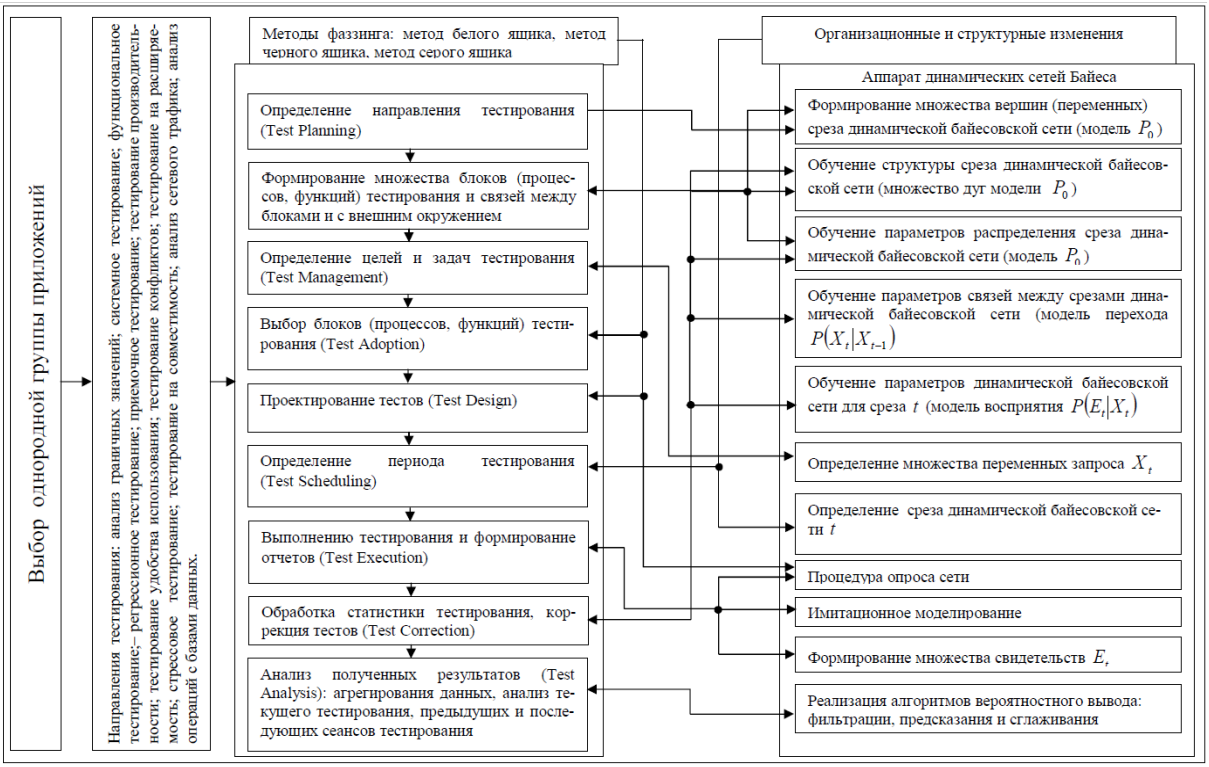


Рис. 2. Концептуальная модель применения аппарата байесовских сетей доверия в процессе управления тестированием веб-приложений

С учетом предложенного подхода схема фаззинга [2] будет выглядеть так, как показано на рис. 3.

В данной схеме для формирования входных данных дополнительно используются данные описания модели веб-ресурса, подготовленные на предварительном этапе средством анализа, которое фактически формирует «индекс» веб-ресурса. Примерная структурно-логическая модель данных описания модели веб-ресурса представлена на рис. 4.

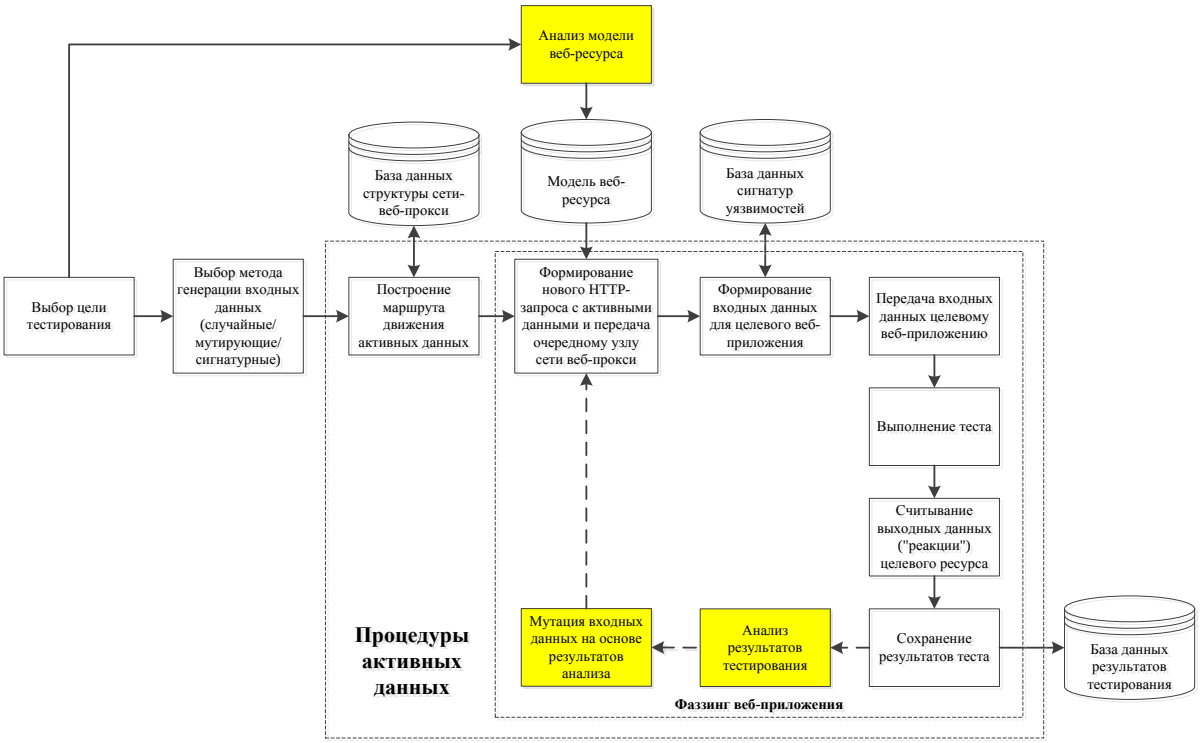


Рис. 3. Схема фаззинга с обратной связью и модель веб-ресурса

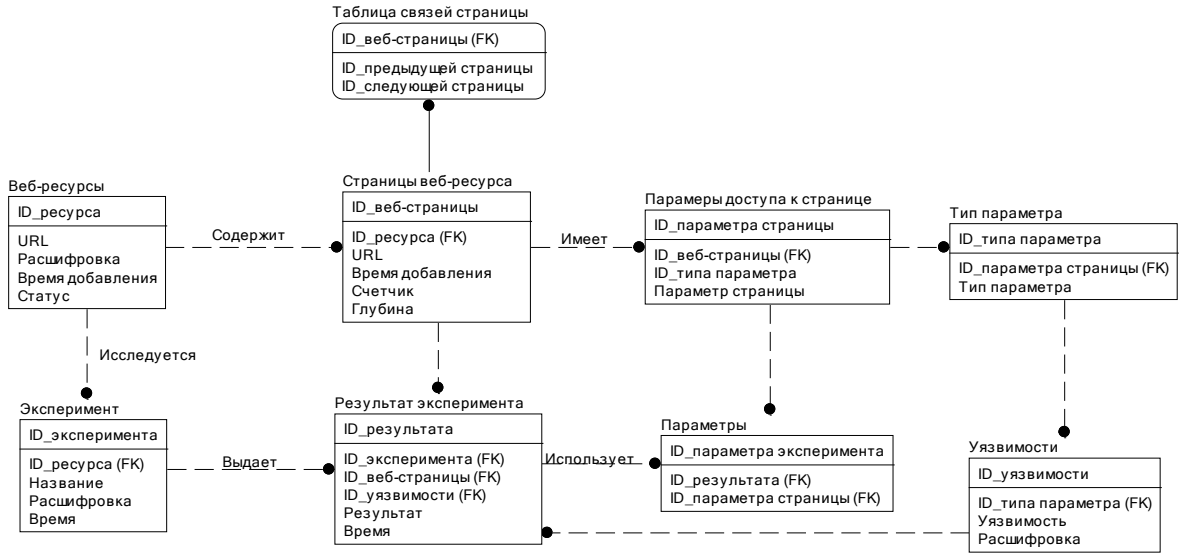


Рис. 4. Структурно-логическая модель данных описания модели веб-ресурса

С учетом представленных схем общая структурная схема адаптивного фаззера на основе сети веб-прокси-серверов [4, 5] может выглядеть так, как показано на рисунке 5.

В состав системы, реализующей адаптивный фаззинг, входят:

− сеть веб-прокси-серверов, обеспечивающих выполнение вычислительных задач (фаззинга);

− комплекс приложений, функционирующих в режиме служб, обеспечивающих выполнение задач управления, анализа структуры удаленного веб-ресурса, доступа к БД, управление вычислительным процессов, взаимодействия с пользовательским интерфейсом;

− веб-ресурс, обеспечивающий взаимодействие с пользователем;

− СУБД и база данных.

Темным цветом на рисунке выделены элементы адаптивного фаззера веб-приложений. Совокупность данных элементов и связи между ними представляет собой автоматизированную системы адаптивного фаззинга веб-приложений, позволяющего анализировать уязвимости целевого тестируемого веб-ресурса с учетом его структуры. Управлением данным средством тестирования может осуществляться через веб-интерфейс за счет изменения конфигурационной информации в базе данных.

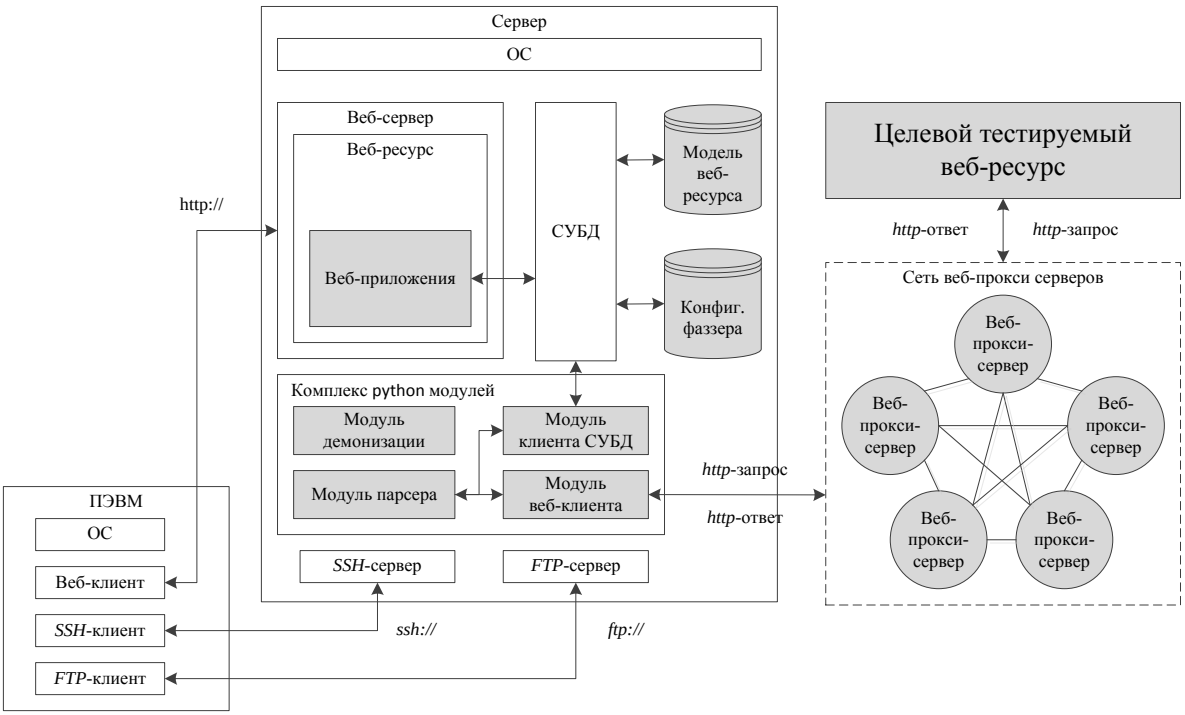


Рис. 5. Структурная схема адаптивного фаззера на основе сети веб-прокси-серверов

Разработка и эксплуатация представленной системы автоматизированного адаптивного фаззинга позволит повысить эффективность поиска и анализа уязвимостей веб-ресурсов с целью выбора и оптимизации средств их защиты от разрушающих программных воздействий.

Список используемых источников

1. Маркин Д. О., Архипов П. А., Галкин А. С. Исследование устойчивости анонимной сети на основе технологий веб-прокси // Вопросы кибербезопасности. 2016. № 2 (15). С. 21–28.

2. Маркин Д. О., Галкин А. С. Распределенное тестирование веб-приложений методом фаззинга на основе технологий веб-прокси и активных данных // Труды Северо-Кавказского филиала Московского технического университета. Ч. 2. Ростов-на-Дону: ПЦ «Университет» СКФ МТУСИ, 2017. 442 с. С. 61–72.

3. Полухин П. В. Байесовские модели и алгоритмы управления процессом тестирования веб-приложений методом фаззинга: дис. … канд. техн. наук: 05.13.18 / Полухин Павел Валерьевич. Воронеж, 2016. 180 с.

4. Маркин Д. О., Галкин А. С., Архипов П. А. Алгоритм распределенного тестирования веб-приложений на основе технологий веб-прокси и активных данных // Информационные системы и технологии. 2018. № 1. (105). С. 93–101.

5. Программный комплекс распределенного тестирования удаленных веб-ресурсов: свидетельство о государственной регистрации программы для ЭВМ № 2017618056 Российская Федерация / Д. О. Маркин, А. С. Галкин, П. А. Архипов, А. А. Юркин, Н. Д. Смирнов; авторы и правообладатели Д. О. Маркин, А. С. Галкин, П. А. Архипов, А. А. Юркин, Н. Д. Смирнов. № 2017613310; заявл. 06.04.2017; зарегистрировано в Реестре программ для ЭВМ 21.07.2017 г.

УДК 004.056.53
ГРНТИ 50.41.25

МЕТОДЫ И СРЕДСТВА АНАЛИЗА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

С. А. Звягинцев, Д. О. Маркин, Д. И. Павлов

Академия Федеральной службы охраны Российской Федерации

В работе представлен обзор основных современных методов и средств анализа программного обеспечения, включая средства статического и динамического анализа, средства автоматизированного анализа, средства динамической бинарной инструментации. Приведена методология исследования программного обеспечения, а также классификация средств и методов анализа программного обеспечения.

обратная разработка, статический анализ, динамический анализ, динамическая бинарная инструментация, дизассемблирование, отладка, эмуляция.

При разработке программных реализаций независимо от их функционального назначения, так или иначе, возникает потребность в защите ее алгоритма. Защита может быть направлена на предотвращение нелегального копирования, на сокрытие критичных с точки зрения функционального назначения функциональных объектов (функций) приложения и других целей. Существующие процессы повсеместного внедрения последних дости-

жений автоматизации, а также «цифровизация» экономики выносят проблему защиты программного обеспечения (ПО) от исследования на первый план и требуют развития, как методов, так и средств защиты.

Наиболее известными средствами исследования ПО являются дизассемблеры и декомпиляторы, отладчики и эмуляторы. Проведенный анализ существующих средств исследования ПО показал, что наиболее распространенными дизассемблерами являются: IDAPro, x64dbg, Radare 2, DeDe, Sourcer, PeExplorer, Cutter, Hopper (OSx Linux), Scratch ABit, Plasma, D3-28, ODA – Online, WinHex, Hiew, DB52ASM, W32DASM, Binary Ninja, Capstone, Zydis, Objconv, HT Editor, distorm 64, Crudasm [1, 2].

Наиболее распространенными отладчиками являются: IDA Pro, OllyDbg, GDB, SoftIce, AQtime, DBX, Dtrace, Electric Fence, GNU Debugger, LLDB, MDB, MS Visual Studio, Immunity Debugger, Dr. Watson, TotalView, WinDbg, FlexTracer, YDbg, x64dbg, Trace replayer, PIN tracer [3].

Эмуляторы: VMware, VirtualBox, QEMU, Nox, Bochs, JVM, Colinux, AlphaVM-Free(-Pro), CHARON-AXP(-VAX), Denali, DOSBox, DOSEMU, Icore virtual accounts, Jail, KVM, OpenVZ, Parallels Workstation, PearPC, Virtual PC, Hyper-V, Virtuozzo, VMware ESX Server, SimNow, Solaris Zones, Xen, z/VM [2–5].

Наиболее распространенными декомпиляторами являются: Boomerang, DCC, RecStudio, Hex-Rays, Cavaj Java Decompiler, JD.

В процессе анализа существующих средств и методов выявилась устойчивая тенденция их развития, направлена на автоматизацию процесса исследования. По сути, в настоящее время проектируются и создаются достаточно эффективные средства статического и динамического исследования ПО, а также сравнительно новое направление – динамическая бинарная инструментация программного кода (DBI).

Среди средств автоматизированного статического анализа известны: АК-ВС 2 (АО «НПО Эшелон»), АИСТ-С (ООО «Центр безопасности информации»), КСАИТ, Project Viewer, «Бурундук», а также AppChecker (АО «НПО Эшелон»), RATS, Yasca, Cppcheck, graudit, Klocwork Insight, SWAAT, PHP Bug Scanner, Pixy, Ounce 6, OWASP Code Crawler, Coverity Prevent Static Analysis [2–4].

К средствам автоматизированного динамического анализа можно отнести: АК-ВС 2 (АО «НПО Эшелон»), EMU, IRIDA, КСАИТ, «Бурундук». Наиболее известные средства динамической бинарной инструментации: frida (http://frida.re), PIN (http://pintool.org), DinamoRIO (http://dynamorio.org), Dyninst (http://dyninst.org), Valgrind (http://valgrind.org) [4, 5].

Как видно из результатов анализа, количество и разнообразие средств исследования ПО достаточно велико. В связи с этим, задача исследования

защитных механизмов ПО является, как правило, вопросом времени, и зависит в большей степени от квалификации исследователя.

Методология исследования программных реализаций с использованием указанных средств анализа обычно выглядит так, как показано на рис. 1. Из анализа представленной методологии видно, что в процессе исследования используется весь спектр средств анализа ПО, включая дизассемблеры, в том числе, интерактивные, отладчики, эмулирующие отладчики, эмуляторы. Дополнительно могут применяться средства мониторинга процессов для перехвата операций ввода-вывода, системных функций, получения характеристик процесса (профилирования), HEX-редакторы и иные средства модификации код, компиляторы, компоновщики и другие вспомогательные средства.

С точки зрения классификации методов исследования ПО известны четыре основных классифицирующих признака: по уровню знаний о ПО и его структуре, по методологии проверок, по степени автоматизации и по способу сбора информации о ПО. Данная классификация представлена на рис. 2.

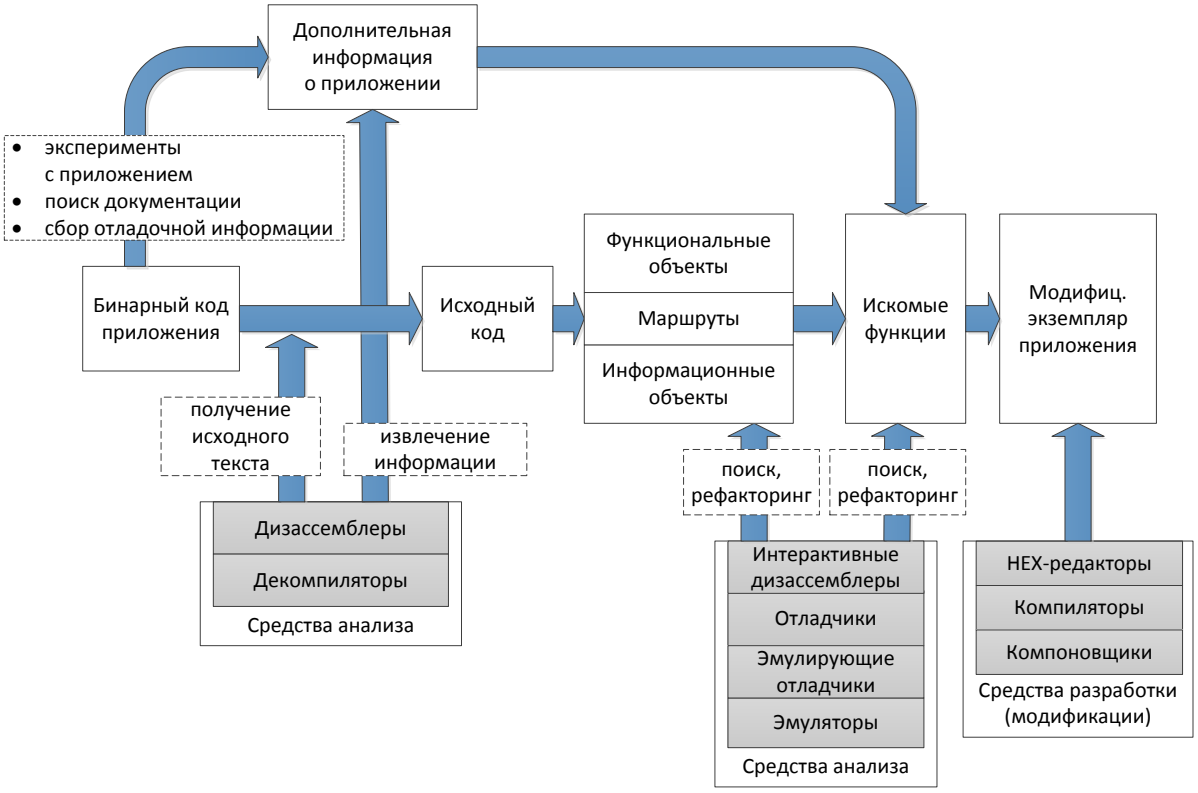


Рис. 1. Методология исследования программного обеспечения

Отдельного внимания заслуживают методы автоматизации исследования ПО, позволяющие осуществлять анализ больших программных реализаций в автоматическом режиме, создавая в результате их анализа отчеты

о проведенном исследовании, на основе которых эксперт способен делать выводы о наличии, расположении и особенностях тех или иных функциональных возможностей исследуемого экземпляра ПО. Классификация методов исследования ПО по степени автоматизации представлена на рис. 3.

Рис. 2. Классификация методов исследования ПО

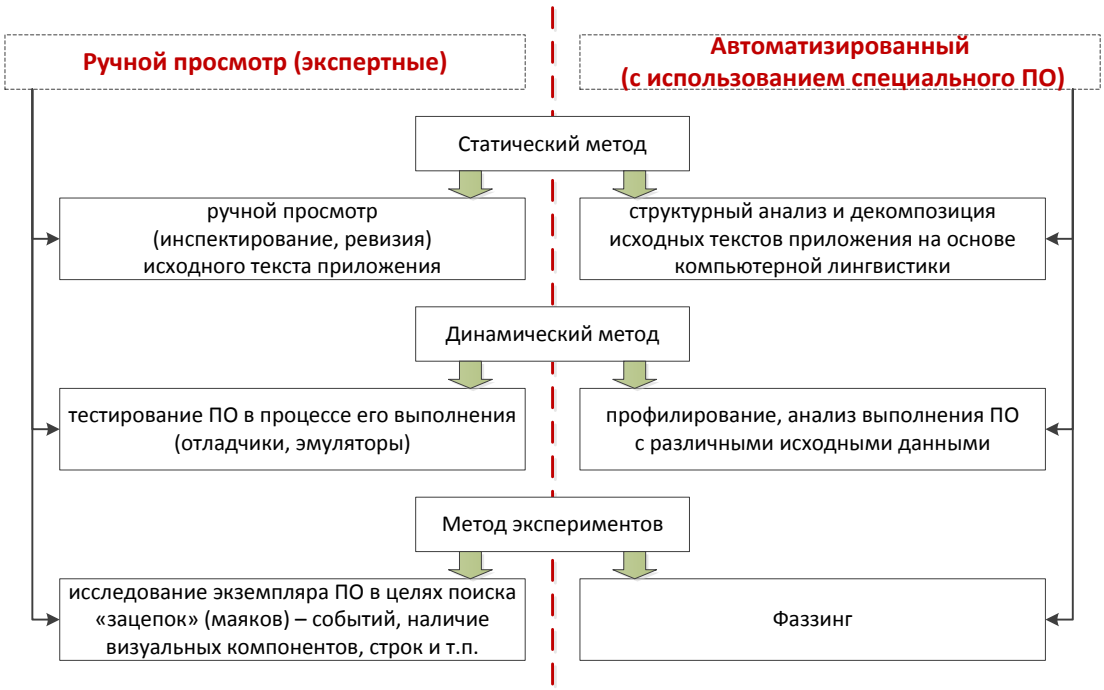


Рис. 3. Классификация методов исследования ПО по степени автоматизации

Среди представленных методов наиболее эффективным, позволяющим оперативно обнаруживать дефекты реализации интерфейсов и иные ошибки некорректных входных данных, является метод фаззинга. Обобщенная схема фаззинга представлена на рис. 4. Для повышения эффективности фаззинга, как правило, используют интеллектуальные методы обработки результатов итераций тестирования, с целью формирования очередной выборки входных данных. Пример такого подхода реализован в работе [6].

Рис. 4. Обобщенная схема тестирования методом фаззинга

Таким образом, проведенный анализ методов и средств исследования ПО показал, что вопросы анализа ПО являются весьма актуальными в настоящее время, методы и средства постоянно развиваются и совершенствуются, а основными тенденциями их дальнейшего развития является их автоматизация, требующая усовершенствования существующих моделей исходного текста, программных реализаций, построения более совершенных схем исполнения ПО и динамического анализа, в том числе, с использованием средств бинарной динамической инструментации.

Список используемых источников

1. Оголюк А. А. Защита приложений от модификации: учебное пособие. СПб.: СПбГУ ИТМО, 2016. 56 с.

2. Мацкевич А. Г., Снигирев С. В., Свечников Д. А. Программно-аппаратные средства обеспечения информационной безопасности. В 2 ч. Ч. 1. Защита от разрушающих программных средств : пособие. Орёл : Академия ФСО России, 2011. 141 с.

3. Касперски К. Искусство дизассемблирования. СПб.: БХВ-Петербург, 2008. 892 с.: ил.

4. Проскурин В. Г. Защита программ и данных: учеб. пособие для студ. учреждений высш. проф. образования. 2-е изд., стер. М.: Академия», 2012. 208 с.

5. Virtual Machines and Abstract Compilers-Towards a Compiler Pattern Language [Электронный ресурс]. URL: https:// www.researchgate.net/publication/221034657_Virtual_Machines_and_Abstract_Compilers_-_Towards_a_Compiler_Pattern_Language (Дата обращения: 04.11.2018).

6. Полухин П. В. Байесовские модели и алгоритмы управления процессом тестирования веб-приложений методом фаззинга: дис. 05.13.18 / Полухин Павел Валерьевич. Воронеж, 2016. 180 с.

УДК 519.7
ГРНТИ 28.15

ПРОБЛЕМЫ СОЗДАНИЯ ПРАКТИЧЕСКИХ СИСТЕМ СТАБИЛИЗАЦИИ СТРУКТУР

О. И. Золотов, Н. Р. Якубова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работах профессора Л. М. Пустыльникова и его соавторов доказана теоретическая возможность использования обратной связи для стабилизации структур объектов любой природы. Практическое решение таких задач наталкивается на ряд серьезных проблем, которые и рассматриваются в данной работе. Приведение этой задачи к классической схеме использования обратной связи требует:

1. Возможности «измерения» структуры, т.е. ее идентификации;

2. Возможности воздействия на структуру с целью ее изменения (некий аналог управляемости);

3. Наличия эталона структуры, возможности сравнения структур и многого другого.

К тому же необходимо определить круг структур, которые можно рассматривать для этих целей.

структура, управление, сохранение, обратная связь

При проектировании систем автоматического регулировании с заданными качественными характеристиками, в том числе и переходных процессов, практически всегда полагают, что уравнения, описывающие объект управления, не изменяются. Однако реально под действием внешних воздействий характеристики объектов управления, а иногда и регуляторов, изменяются. Кроме того, изменение параметров может происходить просто от старения объекта управления в процессе эксплуатации. Это может привести к изменению качественных показателей систем автоматического управления.

Одним из вариантов решения этой проблемы является создание систем стабилизации структур, поддержания уравнений объекта управления.

Впервые идею управления и стабилизации структур предложил А. Г. Бутковский в работе [1]. В работе [2] показано, что теоретически можно создавать системы стабилизации структур, используя универсальный принцип обратной связи. При этом практически нет ограничений на вид операторов, описывающих эти структуры. Реальная система стабилизации структуры, использующая принцип обратной связи, должна выглядеть так: объект управления – это структура, измеритель структуры – это устройство идентификации объекта, устройство сравнения идентифицированной структуры с эталонной и возможность воздействия на структуру.

Рассмотрение этой задачи в такой постановке требует уточнения многих понятий. И первое, что надо уточнить это, что такое структура и какая существует классификация структур и какие классификационные признаки существуют. Необходимо определить понятие сравнения структур и, следовательно, разности структур. И наконец, надо понять, каким образом можно воздействовать на структуру с целью ее изменения.

В данной статье рассмотрена лишь небольшая часть этих вопросов. В основе рассмотрения лежит универсальная, абстрактная теория структур, на основании которой можно представить себе возмущение структуры (приращение структуры), например, в виде аддитивного члена, соответствующего в структурной теории параллельному соединению блоков исходной структуры. Такое представление наводит на мысль, что воздействие на структуру может осуществляться также путем дополнительного блока (блок управления), структура которого формируется так, чтобы компенсировать приращение исходной структуры объекта. Этот блок может быть подсоединен к исходной структуре тоже различными способами.

В работе [2] рассмотрена теоретическая возможность формирования такова блока в виде обратной связи. Приведем несколько примеров рассмотрения структуры, связанных с линейными непрерывными объектами.

Понятия «состояние» и, особенно, «структура», их природа и свойства образуют ёмкую и не до конца изученную область. Ниже предлагается вводное ознакомление, как с содержанием этих понятий, так и с некоторыми их аспектами.

Как известно, одно из представлений решения линейной задачи, записанной в стандартной форме [3], имеет вид:

$$Q(x,t) = \int_0^t \int_D G(x,\xi,t,\tau) w(\xi,\tau) d\xi d\tau. \qquad (1)$$

Здесь, как обычно, x и ξ – пространственные, а t и τ – временные независимые переменные, D – открытая область в некотором многомерном пространстве, $w(x,t)$ – стандартизирующая функция [3], $G\ (x,\xi,t,\tau)$ – функция Грина рассматриваемой задачи.

Соотношение (1) может быть так же представлено в краткой символической форме:

$$Q(x,t) = G(x,\xi,t,\tau)\odot w(x,t), \qquad (2)$$

где $\odot$ – символ так называемой пространственно-временной композиции (композиционного умножения) двух связанных этим символом функций – символ, означающий интегрирование (1).

Вид соотношений (1), (2) остаётся таким же и при векторно-матричных обобщениях функций $w(x,t)$, $G(x,\xi,t,\tau)$ и $Q(x,t)$. Но, как мы убедимся, компактная символическая запись (2) оказывается во многих случаях предпочтительнее развёрнутой записи (1). Соотношения (1) и (2) включают в себя также частные случаи отсутствия в них зависимости от пространственной или временной переменных.

Стандартизирующая функция $w(x,t)$ несёт информацию о внешнем входном воздействии и только о нём. Функция же Грина $G(x,\xi,t,\tau)$ представляет собой исчерпывающую функциональную характеристику исключительно собственных (внутренних) свойств изучаемого объекта. Отметим в дополнение, что из принципа причинности физических явлений вытекает, что $G(x,\xi,t,\tau) = 0$ при $t < \tau$. Это соотношение означает, что реакция физической системы не может наступить раньше момента начала возмущения [3].

Таким образом, запись (2) выражает всегда имеющую место смысловую факторизацию решения: $Q(x,t)$ образуется композицией $G(x,\xi,t,\tau)$ и $w(x,t)$.

В кибернетике (теории управления) функцию $Q(x,t)$ (либо функцию $Q(x,t)$ вместе с некоторым числом её производных по времени) называют «состоянием» объекта или системы. Иногда для краткости термин «состояние» применяют к одной только функции $Q(x,t)$, имея (по умолчанию) ввиду оговорку, помещённую в скобках.

В отношении же функции $G(x,\xi,t,\tau)$, дающей полное описание внутренней природы, точнее – внутренней структуры объекта (системы), естественно употреблять для этой функции наравне с другими её названиями также и термин «структура». Вместе с тем, и это существенно, термин «структура» мы будем присваивать не только функции $G(x,\xi,t,\tau)$, но и любому эквивалентному ей математическому объекту (функции, выражению, оператору и др.).

Проиллюстрируем сказанное на простых стационарных (автономных) задачах. Последние инвариантны к временному сдвигу, функция Грина в них $G(x,\xi,t,r)=G(x,\xi,t-\tau)$, т. е. фактически зависит не от четырёх, а только от трёх переменных и может записываться в виде $G(x,\xi,t)$.

Предварительно условимся класс функций, удовлетворяющих начальным, начально-краевым или краевым условиям задачи, записанной в стандартной форме, называть классом Ф.

1. Движение материальной точки:

$$\frac{d^2Q(t)}{dt^2}=w(t), \tag{3}$$

$$Q(o)=0,\ \frac{dQ}{dt}(o)=0,\quad t\geq 0, \tag{4}$$

где $Q(t)$ – координата точки.

В этой задаче пара функций

$$\left(Q(t),\ \frac{dQ(t)}{dt}\right) \tag{5}$$

представляет состояние, а функция Грина

$$G(t)=t \tag{6}$$

– структуру.

Далее, состояние данного объекта (решение задачи (3), (4))

$$Q(t)=G(t)*w(t) \tag{7}$$

(в отсутствии зависимости от пространственных координат композиция превращается в свёртку).

Тогда

$$G^{-1}(t)*Q(t)=w(t). \tag{8}$$

Обратная функция Грина $G^{-1}(t)$ имеет в данном случае вид

$$G^{-1}(t)=\delta''(t), \tag{9}$$

где $\delta(t)$ – дельта-функция.

Действительно, разворачивая левую часть равенства (8) и учитывая (9), сразу же получаем

$$G^{-1}(t) * Q(t) = \int_0^t \delta''(t-\tau)Q(\tau)d\tau = \frac{d^2}{dt^2}Q(t). \qquad (10)$$

Подставляя теперь (10) в (8), возвращаемся в точности к исходному уравнению (3).

Наконец, если

$$L = \frac{d^2}{dt^2} \qquad (11)$$

рассматривать как оператор с областью определения Ф, то такой оператор, обозначаемый далее как L_Φ, оказывается, как видим, эквивалентным $G(t)$ и, потому, наравне с $G(t)$ и $G^{-1}(t)$ также может идентифицироваться (и именоваться) как «структура». Другими словами,

$$G(t) = t,\ G^{-1}(t) = \delta''(t)\ \ и\ \ L_\Phi = \frac{d^2}{dt^2} \qquad (12)$$

выражает одну и туже структуру – структуру объекта, описываемого соотношениями (3), (4).

Список используемых источников

1. Бабичев А. В., Бутковский А. Г., Похьолайнен Сеппо К единой геометрической теории управления. М.: Наука, 2001.

2. Золотов О. И., Пустыльников Л. М. Принципы управления структурами: (монография). СПб.: СПбГУТ, 2018. 406 с.

3. Бутковский А. Г. Структурная теория распределенных систем. М.: Наука, 1977.

УДК 621.396.67
ГРТНИ 47.45.29

ИСПОЛЬЗОВАНИЕ МЕТОДОВ МНОГОКРИТЕРИАЛЬНОГО АНАЛИЗА АРАМИС И ЕЛЕКТРО ДЛЯ ПОИСКА ОПТИМАЛЬНОГО РЕШЕНИЯ ИИ

С. А. Иванов, М. А. Иглов

Военная академия связи им. Маршала Советского Союза С. М. Будённого

Статья посвящена анализу использования методов многокритериального анализа для ИИ. Приводится пример алгоритма действия и анализа ИИ для получения результата. Выделены основные потребности для ИИ в компьютерной игре, и на их основе строиться итоговая ранжированная таблица списка действия и реакций ИИ при определённых событиях.

ИИ, методы многокритериального выбора, самообучающиеся алгоритмы.

Понятие «искусственный интеллект» начали активно использовать в мире с 2016 года, причем внедрение произошло очень быстро и незаметно для многих. Но как работает искусственный интеллект [1]?

Интересен тот факт, что великие умы современного мира до сих пор не могут с точностью сказать, как работает ИИ. Согласно общепринятым представлениям программа «искусственный интеллект» непосредственно ассоциируется с мышлением человека, но при этом наука еще не смогла полностью разобраться, что такое мышление и реальный интеллект. Одним из самых перспективных направлений для развития на данный момент считается создание прикладных нейронных сетей.

В последнее время популярными являются еще нейро-экспертные системы, основа которых – огромная база знаний. В нее включены многочисленные сведения и методы, которые применяются для решения установленных задач. Кроме этого, система имеет самообучающийся алгоритм, опирающийся на полученные данные.

Одним из основных проблем ИИ является принятие решения и обработка результатов. Для решения данной проблемы многие кампании, такие как Google или Яндекс используют различные системы сбора и обработки информации [2]. Но игровой ИИ отличается наличием множества условий и целей.

Возьмем для примера работу ИИ в игре. Перед ним стоят различные игровые ситуации: (встретил врага; нашел новое оружие; заканчиваются боеприпасы; здоровья у врага; здоровья у себя).

Аналитический обзор показал, что задача выбора действия является многовариантной, так как для выбора какого-либо результата можно выбрать некоторое множество действий, удовлетворяющих определенным предпочтениям.

Как правило, при этом необходимо учитывать целый ряд условий: цель миссии, наличие оружия, безопасность пути, информация о противнике и т. д.

Описанная задача относятся к классу задач группового многокритериального выбора, результат решения которого является обоснованием в принятии решения и позволяет лицу, принимающем решение, получить агрегированные оценки всех вариантов. Количество практических задач такого класса достаточно велико, и для повышения эффективности их решения требуется специального методического, математического, алгоритмического и программного обеспечения. Трудоемкость принятия решения возрастает, если необходимо обобщить экспертные мнения, представленные в разной форме (оценки упорядочения вариантов, матрицы парных сравнений).

Для выбора оптимального варианта действия в зависимости от ситуации предлагаем использовать метод АРАМИС (Агрегирование и Ранжирование Альтернатив около Многопризнаковых Идеальных Ситуаций) для коллективного упорядочения многокритериальных вариантов разработан А. Б. Петровским [3]. Метод основан на оценке близости вариантов к наилучшему и к наихудшему из возможных вариантов.

Применим указанный метод для ранжирования действия для различных ситуаций.

В качестве критерии используем: К1 – безопасность пути; К2 – наличие боеприпасов к оружию; К3 – наличие укрытий; К4 – видимость врагом; К5 – цель миссии.

Для примера используем несколько ситуаций:

Стрелять во врага (далее в таблице – вар1);

Отступить на свою базу (вар2);

Мало здоровья у противника (вар3);

Прятаться за укрытием (вар4);

Встретил врага (вар5);

Идти на базу врага (вар6).

В начале, пока у ИИ нет своей базы данных принятых решений необходимо заполнить таблицы решений вручную, воспользуемся услугами 2-х экспертов, которые проранжируют действия по 3-х бальной системе (0, 1, 2).

ТАБЛИЦА 1. Таблица решений, заполненная вручную экспертами

		встретил врага					**нашел новое оружие**					**заканчиваются боеприпасы**					**мало здоровья у врага**					**мало здоровья у себя**				
	Эксперт	К1	К2	К3	К4	К5	К1	К2	К3	К4	К5	К1	К2	К3	К4	К5	К1	К2	К3	К4	К5	К1	К2	К3	К4	К5
Вар1	Первый	0	0	1	1	2	0	0	1	2	2	1	0	1	2	2	2	0	1	2	2	2	0	1	2	2
	Второй	0	0	1	1	2	0	0	1	2	2	1	0	1	2	2	2	0	1	2	2	2	0	1	2	2
Вар2	Первый	1	2	0	2	1	1	2	0	1	1	1	1	0	0	0	2	1	0	0	0	2	0	0	0	0
	Второй	1	2	1	2	1	1	2	0	1	1	1	1	0	0	0	2	1	0	0	0	2	0	0	0	0
Вар3	Первый	2	1	2	1	2	1	1	2	1	2	2	0	1	1	2	2	0	0	1	2	2	0	1	1	2
	Второй	2	1	2	1	2	1	1	2	1	2	2	0	1	1	2	2	0	0	1	2	2	0	1	1	2
Вар4	Первый	1	2	1	1	1	1	2	1	1	1	2	1	1	0	0	2	1	1	0	0	2	0	0	0	0
	Второй	1	2	1	1	1	1	2	1	1	1	2	1	1	0	0	2	1	1	0	0	2	0	0	0	0
Вар5	Первый	1	1	2	2	2	0	1	1	2	2	1	1	1	1	2	2	0	1	1	2	2	0	1	1	2
	Второй	1	1	2	2	2	0	1	1	2	2	1	1	1	1	2	2	0	1	1	2	2	0	1	1	2
Вар6	Первый	1	1	0	1	2	1	2	1	2	2	2	1	0	1	2	2	0	0	0	2	2	0	0	0	2
	Второй	1	1	0	1	2	1	2	1	2	2	2	1	0	1	2	2	0	0	0	2	2	0	0	0	2

По данным таблицы 1 можно рассчитать относительную близость каждого варианта для различных ситуаций к наилучшему варианту

Для каждого варианта Ai задается показатель его относительной близости к наилучшему варианту P1 (см. табл. 2 и 3).

В этом случае упорядочение объектов по предпочтительности строится по возрастанию значения показателя Δ относительной близости объекта Ai к наилучшему варианту P = 20 (в нашем случае, все эксперты поставили максимальный балл по всем пяти критериям), или по убыванию значения показателя относительной близости объекта Ai к наихудшему варианту P2 = 5 (все эксперты поставили минимальный балл по всем критериям). Наилучшим вариантом является вариант максимально близкий к 0 по показателю Δ.

В статье предложен один из возможных подходов к многокритериальному ранжированию вариантов действия ИИ. Варианты оценивались двумя экспертами по пяти критериям. Используя метод АРАМИС для упорядочения многопризнаковых объектов, основанный на теории метрических пространств мультимножеств, были построены ранжировки действий и определены наиболее предпочтительные (см. табл. 4).

Предлагаем в статье метод подбора оптимального действия ИИ в различных ситуациях будет использоваться при разработке компьютерной игры в рамках научного проекта.

ТАБЛИЦА 2. Встретил врага

объект	К1(0)	К1(1)	К1(2)	К2(0)	К2(1)	К2(2)	К3(0)	К3(1)	К3(2)	К4(0)	К4(1)	К4(2)	К5(0)	К5(1)	К5(2)	Δ
Вар1	2	0	0	2	0	0	0	2	0	0	2	0	0	0	2	0.67
Вар2	0	2	0	0	0	2	1	1	0	0	0	2	0	2	0	0.33
Вар3	1	1	0	0	2	0	0	0	2	0	2	0	0	0	2	0.47
Вар4	0	2	0	0	0	2	0	2	0	0	2	0	0	2	0	0.4
Вар5	0	2	0	0	2	0	0	2	0	0	2	0	0	0	2	0.43
Вар6	0	2	0	0	2	0	2	0	0	0	2	0	0	0	2	0.67

ТАБЛИЦА 3. Мало здоровья у противника

объект	К1(0)	К1(1)	К1(2)	К2(0)	К2(1)	К2(2)	К3(0)	К3(1)	К3(2)	К4(0)	К4(1)	К4(2)	К5(0)	К5(1)	К5(2)	Δ
Вар1	2	0	0	2	0	0	0	2	0	0	0	2	0	0	2	0.47
Вар2	0	2	0	0	0	2	2	0	0	0	2	0	0	2	0	0.4
Вар3	0	2	0	0	2	0	0	0	2	0	2	0	0	0	2	0.47
Вар4	0	2	0	0	1	1	0	2	0	0	2	0	0	2	0	0.47
Вар5	2	0	0	0	2	0	0	2	0	0	0	2	0	0	2	0.57
Вар6	0	2	0	0	0	2	0	2	0	0	0	2	0	0	2	0.34

ТАБЛИЦА 4. Ранжировка выбора действия

Действие	Встретил врага	Мало здоровья у врага
Отступить на свою базу	0.33	0.4
Преследовать врага	0.27	0.47
Стрелять во врага	0.67	0.47
Перезарядить оружие	0.32	0.44
Прятаться за укрытием	0.4	0.47
Идти на базу врага	0.47	0.67

Список используемых источников

1. Minh'Chau T. Huynh. A. Numerical and Experimental Investigation of Planar Inverted'F Antennas for Wireless Communication Applications. – In: Master Thesis of Science in Electrical Engineering. Virginia Polytechnic Institute and State University. Blacksburg, Virginia. Oct. 19, 2000. 123 p. URL: http://scholar.lib.vt.edu/theses/available/etd'10242000'22130026/unrestricted.

2. Шихов Е. Варианты реализации искусственного интеллекта [Электронный ресурс ресурс]. URL: http://neural.narod.ru/, 2002 с 125

3. Лотов А. В., Поспелова И. И. Многокритериальные задачи принятия решений. М.: МАКС Пресс, 2008.

УДК 004.415.53
ГРНТИ 50.41.01

АВТОМАТИЗАЦИЯ ПРОЦЕССА ПОДГОТОВКИ ТЕСТОВОЙ СРЕДЫ

И. А. Иевлев, Т. В. Мусаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается задача оптимизации процесса разработки и тестирования ПО с помощью сокращения трудоемкости и временных затрат на подготовку тестовой среды. Рассмотрен опыт разработки и внедрения программного компонента для автоматизации процесса подготовки тестовых стендов биллинговой системы сотового оператора. Предлагается разработанный метод автоматизации процесса подготовки тестового окружения, основанный на полной автоматизации и легкости масштабирования. Приведена структура системы, в которой реализовано решение задачи автоматизации процесса подготовки тестовой среды.

биллинговая система, тестовая среда, автоматизация, тестирование.

В настоящее время сфера разработки программного обеспечения (ПО) стремится к уменьшению времени вывода на рынок (*Time-to-Market*, уменьшение времени от начала проекта до внедрения у заказчика) [1], в связи с этим оптимизируются все этапы жизненного цикла разработки ПО, увеличивается скорость разработки, внедряются новые методологии создания программных средств.

По затратам времени наиболее трудоемким принято считать процесс поиска ошибок в программах (тестирование). Затраты ресурсов на данный процесс может быть равен или даже превосходить совокупные затраты ресурсов на все остальные. Основой данного процесса является подготовка тестовой среды. Каждому тестировщику необходимо свое отдельное и независимое тестовое окружение, которое необходимо поддерживать в актуальном состоянии. Но данный процесс занимает все большее количество времени и традиционный подход к ручной поддержке актуальности тестовой среды уже не может обеспечить быстрое и качественное тестирование современных систем. Увеличение количества времени на подготовительные этапы уменьшает время на тестирование продукта [4].

Таким образом, оптимизация процесса подготовки тестовой среды является актуальной проблемой. В статье предложен метод увеличения качества процесса разработки ПО при значительном уменьшении временных затрат, основанный на автоматизации процесса подготовки тестовых сред [3].

Процесс подготовки тестовой среды

Биллинговая система сотового оператора представлена базой данных под управлением СУБД Oracle, которая содержит множество записей. Бизнес-логика представлена пакетами в базе данных на языке программирования PL/SQL. При разработке новой функциональности данной системы за сутки собирается до 30 версий с различными изменениями в коде системы. В штате работает 10 тестировщиков, каждый из которых имеет свое собственное тестовое окружение. Штат компании продолжает расширяться.

Для установки на тестовую БД последней актуальной версии системы необходимо выполнить следующие шаги:

- заполнить данные о тестовой БД в конфигурационном файле системы;
- остановить все jobы, способные создать блокировку на PL/SQL пакеты;
- отключить все активные сессии на тестовой БД;
- запустить инсталляционный скрипт системы;
- запустить остановленные jobы;

- проверить статус PL/SQL пакетов и текущую версию системы на тестовой БД.

Ниже представлена формула расчета средних временных затрат на подготовку тестовой среды.

$$S = DT\frac{(Pt_1+J(t_2+t_3)+S)}{H},$$

где S – общее затраченное время;

T – количество тестовых БД;

D – количество сборок системы;

P – количество измененных пакетов;

J – количество jobов;

S – время на проверку пакетов и версии системы;

H – количество тестировщиков.

В результате проведенного анализа в предметной области выявлены следующие проблемы:

- отсутствие возможности безболезненного увеличения количества тестовых БД;
- необходимость привлечения большого количества сотрудников для уменьшения количества времени;
- человеческих фактор при проверке успешности установки версии.

Под подготовкой тестовой среды в данной системе подразумевается установка патча системы. Общая структура патча представлена на рис. 1.

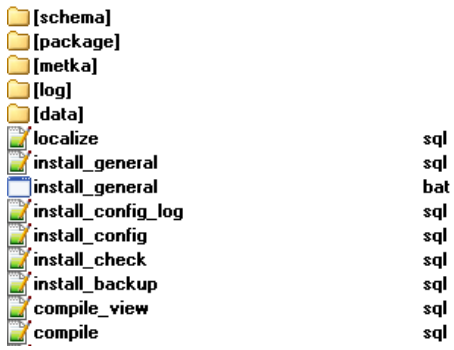


Рис. 1. Общая структура патча

Патч состоит из четырех основных компонентов:

1. Файлы конфигурации, содержащие настроечные параметры (*install_config*, *localize*);
2. Файлы проверки доступности установки патча (*metka*, *install_check*, *install_*backup);
3. Обновленные компоненты системы (*schema*, *package*, *data*);
4. Файлы подготовки системы к эксплуатации (*compile*, *compile_view).*

Анализ существующих решений

Для решения данной задачи используется классический подход контейнеризации на основе Docker и Kubernetes. В его основе лежит выделение тестовой среды в контейнеризованное, обособленное виртуальное окружение. При необходимости создается новое окружение с нуля.

Но данный вариант зачастую бывает слишком трудозатратно внедрить для Legacy систем, не разбитых на отдельные модули и использующих устаревшие технические решения. Основной проблемой внедрения данного варианта в существующую систему является:

- скорость разворачивания нового инстанса БД Oracle;
- патчи не являются накопительными (для проверки последней версии системы на новом окружении необходимо установить все предшествующие патчи);
- большое количество кастомных решений.

Потому для решения данной задачи в Legacy системах, предлагается следующее решение на основе ручного способа:

Необходимо автоматизировать процесс подготовки тестовой среды с помощью скрипта автодеплоя, реализовав все три компонента патча. Для уменьшения количества времени необходимо реализовать запуск данного скрипта при появлении новой сборки системы. Благодаря этому можно увеличивать количество тестовых баз без увеличения времени на их обновление, а автоматическая проверка пакетов и версий будет выполнятся всегда и без учета человеческого фактора (лень, сложность, уверенность в успешной установке. Вариант решения для автоматизации тестовой среды представлен на рис. 2.

Рис. 2. Вариант реализации с использованием Jenkins

Реализация скрипта автодеплоя

Логика установки патча была разделена на основные блоки и реализована на языке Groovy. Скрипт автодеплоя состоит из тех же основных компонентов, что и структура патча. Структура скрипта представлена на рисунке на рис. 3.

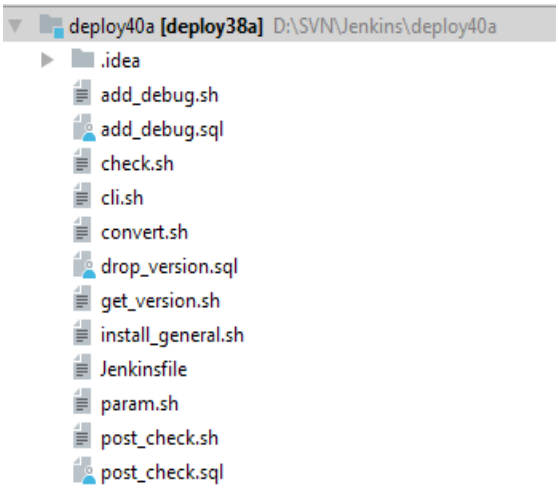


Рис. 3. Структура скрипта автодеплоя

При появлении новой сборки системы происходит вызов скрипта *install_general*, которому передаются нужные параметры. Далее вызывается логика проверки доступности установки патча с помощью компонентов *check.sh*, *get_version*. Если проверка пройдена успешна, то запускается основная часть установки патча в файле *Jenkinsfile*. После выполнения этой части запускается проверка успешности установки и формируется отчет о подготовке тестовой среды. Отчет о подготовке тестовой среды за последние два дня представлен на рис. 4.

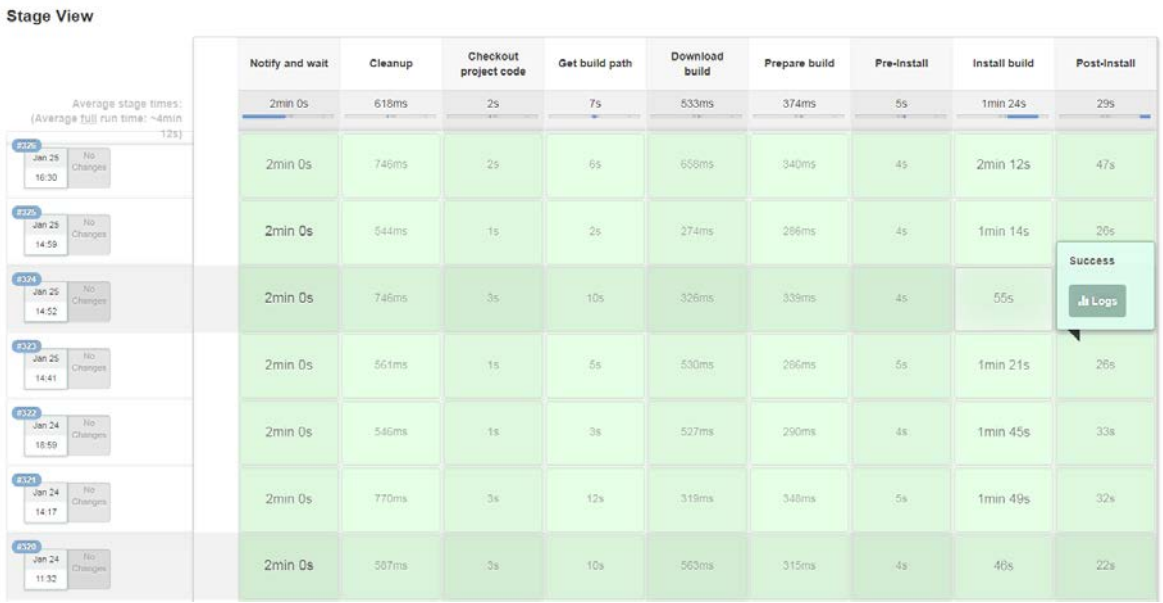


Рис. 4. Пример отчета о подготовке тестового окружения

Заключение

Внедрение предложенного способа автоматизации процесса подготовки тестового окружения позволяет уменьшить влияние человеческого фактора, а выполнение без вмешательства тестировщика дает возможность каскадного увеличения количества тестовых сред для ускорения процесса тестирования.

Таким образом, применение предложенного метода позволяет значительно уменьшить затраты времени, необходимые на весь процесс разработки ПО

Список используемых источников

1. Boosting Time-to-Market by Improving Software Development [Электронный ресурс]. URL: https://devops.com/boosting-time-to-market

2. Возьмите свое тестовое окружение под контроль [Электронный ресурс]. URL: http://www.software-testing.ru/library/testing/general-testing/2424-take-control-of-your-test-environment

3. Готовим тестовое окружение, или сколько тестовых инстансов вам нужно. [Электронный ресурс]. URL: http://www.pvsm.ru/testirovanie/280632

Статья представлена научным руководителем,
доктором технических наук, профессором П. К. Смирновым.

УДК 004.451
ГРНТИ 50.41.15

К ВОПРОСУ О СЕТЕВОЙ БЕЗОПАСНОСТИ И ФИЛЬТРАЦИИ ПАКЕТОВ

О. Б. Ильина[1], О. П. Купчиненко[1], А. В. Скоропад[2]

[1]Военная академия связи им. Маршала Советского Союза С. М. Буденного
[2]Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио»

Iptables в операционной системе Linux представляет собой инструментальный набор для построения эффективных брандмауэров. Он основывается на фильтрации пакетов, проходящих через соединение, и в соответствии с набором правил определяет ту или иную реакцию брандмауэра на эти пакеты. Возможность блокировки входящего трафика, инициированного извне, совместно с функциями трансляции сетевых адресов, дает возможность пользователям свободного выхода в сеть Internet и надежно защищает их от вторжений извне.

операционная система, безопасность информации, межсетевой экран, цепочка, правило, порт, фильтрация пакетов, трафик.

Стремительное развитие и совершенствование информационных технологий, повышение их роли и значимости требуют постоянного внимания к вопросам обеспечения безопасности информации.

Безопасность информации может быть обеспечена лишь при комплексном использовании всех имеющихся средств защиты информации, при котором для защиты информации необходимо использовать не только базовые [1] и дополнительные средства защиты информации [2], но и применять механизмы, пусть и не относящиеся к средствам защиты информации от несанкционированного доступа (НСД), но предотвращающие попытки НСД.

В средства защиты информации фильтрация пакетов не входит, но применяется для защиты информации от НСД в операционной системе (ОС) Linux.

Фильтрацию пакетов производят специальные программные (программно-аппаратные комплексы), называемые файрволами (*firewall*), межсетевыми экранами (МСЭ) или брандмауэрами. МСЭ – средства защиты, устанавливаемые между общедоступной (*Internet*) и внутренней сетью. Межсетевой экран в ОС Linux защищает компьютер как от атак извне, так и от утечки трафика. Основная задача МСЭ – фильтрация и обработка пакетов, проходящих через сеть. При анализе входного пакета файрвол принимает решение о судьбе этого пакета: сбросить пакет (DROP), принять пакет (ACCEPT) или сделать с ним что-то еще [3].

В ОС Linux МСЭ является модулем ядра, называемым netfilter и представляет собой набор хуков (*hooks*) для работы с сетевым стеком. Интерфейсом для модификации правил, по которым файрвол обрабатывает пакеты, служит утилита iptables, которая выполняет фильтрацию пакетов. Данный фильтр позволяет выполнять следующие задачи: фильтрация пакетов – разрешение или запрет передачи пакетов, проходящих через него; трансляция сетевых адресов («маскарадинг») – подмена некоторых параметров в заголовках IP-пакетов; прозрачное проксирование – переадресация пакетов на другой порт компьютера. Всю работу по фильтрации трафика выполняет ядро системы. Iptables не является демоном и не создает новых процессов в системе. Включение или выключение iptables – это всего лишь отправка сигнала в ядро. Большая скорость фильтрации достигается за счёт анализа только заголовков пакетов.

К основным возможностям iptables относятся: фильтрация трафика на основе адресов отправителя и получателя пакетов, номеров портов; перенаправление пакетов по определенным параметрам; организация доступа в сеть Source Network Address Translation (SNAT); проброс портов из глобальной сети в локальную Destination Network Address Translation (DNAT); ограничение числа подключений; установление квот трафика; выполнение правил по расписанию.

Ядро ОС Linux запускается с тремя таблицами: filter, mangle, nat. Каждая из них должна использоваться только в своих целях. Нецелевое использование таблиц может привести к ослаблению защиты МСЭ и сети, находящейся за ним.

В таблице filter содержаться наборы правил для выполнения фильтрации пакетов. Пакеты могут пропускаться далее, либо отвергаться, в зависимости от их содержимого. Таблица filter имеет три встроенных цепочки: FORWARD – для фильтрации пакетов, идущих транзитом через МСЭ;

INPUT – для прохождения пакетов, которые предназначены локальным приложениям; OUTPUT – для фильтрации исходящих пакетов, сгенерированных приложениями самого МСЭ.

Таблица mangle предназначена для внесения изменений в заголовки пакетов. В ней можно устанавливать биты TOS (*Type Of Service*), а так же выполнять действия TTL (*Time To Live*) и MARK.

Действие TOS выполняет установку битов поля Type of Service в пакете. Это поле используется для задания желаемого варианта маршрутизации. Действие TTL используется для установки значения поля TTL пакета. Действие MARK устанавливает специальную метку на пакет, проверяемую другими правилами в iptables или другими программами. С помощью «меток» (MARK) можно управлять маршрутизацией пакетов, ограничивать трафик и т. п.

Таблица mangle имеет пять цепочек: PREROUTING – для внесения изменений в пакеты на входе в МСЭ перед первым принятием решения о маршрутизации; POSTROUTING – для внесения изменений на выходе из МСЭ после последнего принятия решения о маршрутизации; INPUT – для внесения изменений в пакеты перед их передачей локальному приложению внутри МСЭ; OUTPUT – для внесения изменений в пакеты, поступающие от приложений внутри МСЭ; FORWARD – для внесения изменений в транзитные пакеты после первого принятия решения о маршрутизации, но перед последним принятием решения о ней.

Таблица nat используется для выполнения преобразований сетевых адресов NAT (*Network Address Translation*). Только первый пакет из потока проходит через цепочки этой таблицы. Для остальных пакетов в данном соединении автоматически применяются выбранные операции преобразования адресов и номеров портов.

В ОС Linux функции NAT обычно разделяют на SNAT (изменение адреса отправителя в первом пакете) и DNAT (изменение адреса получателя в первом пакете). Маскирование представляет собой частный случай трансляции SNAT, а функции port forwarding (пересылка в другой порт) и transparent proxying (прозрачный proxy) являются частным случаем трансляции DNAT. Все эти функции реализуются в одном блоке NAT.

Для таблицы nat характерны действия DNAT, SNAT и MASQUERADE (маскарадинг).

DNAT производит преобразование адресов назначения в заголовках пакетов, которые после этого перенаправляются на другие адреса, отличные от указанных ранее в заголовках пакетов. SNAT используется для изменения исходных адресов пакетов, что позволяет скрыть структуру локальной сети и разделить единственный внешний IP-адрес между компьютерами локальной сети для выхода в Интернет. MASQUERADE применяется в тех же

целях, что и SNAT, но MASQUERADE производит запрос IP-адреса для указанного в действии сетевого интерфейса, в то время как для SNAT IP-адрес указывается непосредственно. Благодаря такому отличию MASQUERADE может работать в случаях с динамическим IP-адресом, когда подключение к сети осуществляется через PPP или SLIP. Действие MASQUERADE имеет свойство «забывать» соединения при остановке сетевого интерфейса. В случае же SNAT в этой ситуации в таблице трассировщика остаются данные о потерянных соединениях, которые могут храниться в памяти до суток.

При обработке пакетов iptables учитывает следующую информацию: IP-адрес отправителя; IP-адрес получателя; протокол (TCP, UDP, ICMP); номер программного порта отправителя; номер программного порта получателя.

Администратор на основе этой информации задает правила, по которым пакеты будут либо пропускаться через фильтр, либо отбрасываться. Каждое правило – это строка, содержащая в себе критерии, по которым из трафика выбирается пакет, и действие, которое необходимо выполнить в случае удовлетворения критерия. Пребывающий пакет проходит по цепочке правил. Каждое правило содержит условие и цель (действие). Если пакет удовлетворяет условию, то он передается на цель. В противном случае к пакету применяется следующее правило в цепочке. Если пакет не удовлетворил ни одному из условий в цепочке, то к нему применяется действие по умолчанию. Пакеты проходят по цепочке правил последовательно, поэтому порядок добавления правил критичен.

Приходя на МСЭ, входящий пакет сначала попадает на сетевое устройство, перехватывается соответствующим драйвером и передается в ядро. После этот пакет обрабатывается сначала брандмауэром с цепочки PREROUTING в таблице mangle, затем правилами цепочки PREROUTING таблицы nat. На этом этапе проверяется, не требуется ли модификация назначения пакета (DNAT). Важно сменить назначение сейчас, потому что маршрут пакета определяется сразу после того, как он покинет цепочку PREROUTING. После этого он будет отправлен на цепочку INPUT (если целью пакета является этот компьютер) или FORWARD (если его целью является другой компьютер в сети). Пакет проходит несколько этапов прежде, чем он будет передан далее. На каждом из них пакет может быть остановлен.

Если целью пакета является другой компьютер, то пакет фильтруется правилами цепочки FORWARD таблиц mangle и filter, а затем к нему применяются правила цепочки POSTROUTING. На данном этапе можно использовать SNAT/MASQUARADE (подмена источника/маскировка). После этих действий пакет, если он выжил, будет отправлен в сеть.

Если назначением пакета является сам компьютер с брандмауэром, то после маршрутизации он обрабатывается правилами цепочек INPUT таблиц

mangle и filter. В случае прохождения цепочек пакет передается приложению. Когда приложение на машине с МСЭ отвечает на запрос или отправляет собственный пакет, то он обрабатывается цепочкой OUTPUT таблицы filter. Затем к нему применяются правила цепочки OUTPUT таблицы nat для определения необходимости использования DNAT (модификация назначения). Пакет фильтруется цепочкой OUTPUT таблицы filter и выпускается в цепочку POSTROUTING, которая может использовать SNAT и QoS (Quality of Service). В случае успешного прохождения POSTROUTING пакет выходит в сеть.

Поскольку при получении каждого пакета сетевой фильтр просматривает таблицу правил в последовательном порядке, каждое новое правило уменьшает общую производительность маршрутизатора.

Одной из проблем сетевых фильтров является невозможность создания иерархической структуры правил. Сетевые фильтры имеют и ряд других принципиальных недостатков. Так, аутентификация (точнее идентификация) отправителя производится только на основании IP-адреса, подменой которого (IP-spoofing) можно без особых усилий обойти такую преграду. Аутентификация на основании имени и пароля пользователя намного надежнее, но в сетевых фильтрах применить ее не представляется возможным. Сетевой фильтр отслеживает работу сетевых приложений и не контролирует содержимое пакетов транспортного, сеансового и прикладного уровня, поэтому наличие сетевого фильтра не оградит сеть от атак, связанных с фрагментацией пакетов, и от вторжений через сервисы прикладного уровня. Основным достоинством сетевых фильтров является их более высокая производительность, чем у МСЭ сеансового и прикладного уровня.

Несмотря на серьезные недостатки, сетевой фильтр является неотъемлемой частью любого МСЭ и работает в сочетании со шлюзом более высокого уровня иерархии эталонной модели ISO/OSI. В такой схеме сетевой фильтр препятствует прямому общению между внутренней и внешней сетью. Вся же основная фильтрация организуется шлюзом соответствующего вышестоящего уровня OSI.

МСЭ не могут предотвратить атаки внутри локальной сети, но вместе с другими средствами защиты играют важную роль для защиты сетей от вторжения извне. Понимание технологии работы МСЭ позволяет корректно их настроить. С помощью набора расширений для iptables можно строить свои правила, основываясь на анализе содержимого пакетов и диапазона портов, и даже создавать ловушки для злоумышленников.

Iptables в ОС Linux позволяет строить весьма мощные брандмауэры, ничуть не уступающие по своим характеристикам многим коммерческим системам защиты. По своей сути iptables основывается на фильтрации пакетов, проходящих через соединение, и в соответствии с набором правил определяет ту или иную реакцию брандмауэра на эти пакеты.

Простая и очень эффективная возможность блокировки входящего трафика, инициированного извне, вместе с функциями трансляции сетевых адресов дает пользователям возможность свободного выхода в сеть Internet и надежно защищает их от вторжений извне.

Список используемых источников

1. Гринь Д. В., Ильина О. Б., Купчиненко О. П., Скоропад А. В. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность: сб. тр. СПб.: СПОИСУ, 2017. Вып.4. С. 76–78.

2. Ильина О. Б., Купчиненко О. П., Скоропад А. В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т. 2. С. 356–360.

3. Буренин П. В., Девянин П. Н. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition. Учебное пособие / Под редакцией доктора технических наук П. Н. Девянина. М.: Горячая линия – Телеком, 2018. 311 с.

УДК 004.451
ГРНТИ 50.41.15

О ДОПОЛНИТЕЛЬНЫХ ЗАДАЧАХ АДМИНИСТРИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ОПЕРАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

О. Б. Ильина[1], О. П. Купчиненко[1], А. В. Скоропад[2]

[1]Военная академия связи им. Маршала Советского Союза С. М. Буденного
[2]Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио»

В автоматизированных системах, реализованных с использованием операционных систем специального назначения, применение дополнительных функций администрирования операционных систем позволяет построить более гибкую и надежную систему защиты информации от несанкционированного доступа. Для выполнения расширенного контроля целостности файлов широкое распространение получила система AFICK. Для дополнительного ограничения прав пользователей используется режим «Киоск».

автоматизированная система, операционная система специального назначения, защита информации, несанкционированный доступ, контроль целостности.

Непрерывное совершенствование информационных технологий, повышение их роли и значимости, расширение сферы применения автоматизированных систем специального назначения (АС СН) требуют постоянного внимания к вопросам обеспечения безопасности информации.

Функционал операционной системы специального назначения (ОС СН) «Astra Linux SE» расширен комплексом средств защиты (КСЗ) от несанкционированного доступа (НСД), реализующим дополнительные функции администрирования операционных систем (ОС), который работает в составе АС СН [1].

Корректная и полная настройка системы аудита ОС «Astra Linux SE» обеспечивает достаточный контроль над изменениями в объектах файловой системы, в ходе работы с ними множества пользователей. Своевременное оповещение администратора ОС «Astra Linux SE» о событиях несанкционированного (случайного или намеренного) доступа к данным или программам их обрабатывающим позволяет избежать проблем, связанных с потерей данных или нарушением работы прикладных и/или системных программ.

Между тем автоматизированные системы в защищенном исполнении (в том числе и на базе ОС «Astra Linux SE») должны обеспечивать функции контроля целостности (*integrity*) как данных, так и кода обрабатывающих эти данные программ. Подобный контроль позволяет с определенной степенью уверенности констатировать факт отсутствия в ОС и данных, обрабатываемых ее службами информации и функций, обладающих недекларируемыми для данной автоматизированной системы возможностями.

Для решения этой общей задачи контроля целостности в ОС «Astra Linux SE» в состав КСЗ PARSEC включен комплекс средств, решающих частные задачи управления целостностью данных.

В состав этого комплекса входят:

1. Средство подсчета контрольных сумм файлов и оптических дисков;
2. Средство контроля соответствия дистрибутиву;
3. Средство регламентного контроля целостности;
4. Средства создания замкнутой программной среды.

Для решения задач контроля целостности хранимых данных в ОС «Astra Linux SE» реализована библиотека libgost, в которой для вычисления контрольных сумм применяется алгоритм, основанный на хэш-функции по ГОСТ Р 34.11-94.

Контроль соответствия файлов ОС «Astra Linux SE» ее дистрибутиву обеспечивает оценку целостности базовых команд и утилит, копируемых на этапе установки ОС. Это с определенной долей вероятности позволяет судить об отсутствии в коде этих команд и утилит посторонних бинарных вставок, внедренных на этапе эксплуатации ОС.

Однако такая проверка является неэффективной для файлов, состояние которых многократно изменяется в ходе эксплуатации системы, например,

конфигурационных файлов самой ОС СН и прикладных служб, создаваемых пользователями и администратором файлов данных.

Кроме того, контроль целостности на основе контрольной суммы файла не затрагивает таких атрибутов файла, как его метки времени (*timestamps*), дискреционные атрибуты (Minimal ACL и EA ACL), мандатные метки безопасности [2].

Для выполнения расширенного контроля целостности файлов, обеспечивающего проверку указанных выше характеристик файлов, в семействе ОС Linux широкое распространение получила система AFICK (*Another File Integrity Checker*).

Система AFICK совмещает в себе функции контроля целостности файлов и их атрибутов с использованием таких алгоритмов подсчета контрольных сумм, как MD5 и SHA1, с интеграцией с демоном запуска программ по расписанию crond. Это позволяет выполнять периодический (регламентный) контроль целостности ключевых файлов ОС на предмет внесения в них случайных или намеренных изменений. Дополнительно система AFICK имеет возможность настройки правил проверки целостности директорий.

В ОС «Astra Linux SE» используется модифицированный вариант системы AFICK, дополнительно использующий алгоритм подсчета контрольных сумм по ГОСТ Р 34.11-94 и контроля файлов атрибутов подсистемы безопасности PARSEC (мандатные атрибуты и атрибуты подсистемы аудита безопасности) [3]. Система AFICK в ОС «Astra Linux SE» базируется на библиотеке libgost.

Базовым конфигурационным файлом системы AFICK является файл /etc/afick.conf (рис.).

```
#all:    p+d+i+n+u+g+s+b+m+c+md5
#R:      p+d+i+n+u+g+s+m+c+md5
#L:      p+d+i+n+u+g
#P:      p+n+u+g+s+md5
#E:      ''

# action alias may be configured with
# your_alias = another_alias|item[+item][-item]
# all is a pre-defined alias for all items except "a"
DIR=p+i+n+u+g
ETC = p+d+i+u+g+s+md5
Logs = p+n+u+g
MyRule = p+d+i+n+u+g+s+b+md5+m
PARSEConly = e+t
PARSEC = p+d+i+n+u+g+s+b+md5+m+e+t
GOST = p+d+i+n+u+g+s+b+gost+m+e+t
```

Рисунок. Вариант файла afick.conf

Где, например, в правиле PARSEC опции:

p+d+i+n+u+g+s+b+md5+m – слежение за всеми стандартными атрибутами файла и использование хэш-функции MD5 для слежения за целостностью содержимого файлов;

+e+t – контроль расширенных атрибутов: меток безопасности и флагов аудита файлов.

Кроме того, на выбор администратора представлен ряд дополнительных путей с правилами. Соответствующие им строки закомментированы (символ «#») и могут быть активированы удалением символа комментария.

Эталонные значения контрольных сумм и атрибутов файлов хранятся в базе данных системы AFICK – файле с расширением ndbm. База контрольных сумм и атрибутов создается на основании секции files to scan файла afick.conf при помощи опции – i команды afick.

Одним из инструментов ограничения прав пользователей в ОС «Astra Linux SE» является режим «Киоск».

Режим «Киоск» является реализованным в подсистеме PARSEC вариантом маски umask. Отличительной особенностью режима «Киоск» является то, что при использовании команды umask маска на разрешения накладывается только при создании новых объектов файловой системы, а при применении режима «Киоск» маска на разрешения к объектам файловой системы накладывается при любой попытке пользователя получить доступ. Маска режима «Киоск» применяется только к файлам обычного типа. К директориям, сокетам и файлам устройств маска режима «Киоск» не применяется.

Маска режима «Киоск» задается в конфигурационном файле /etc/parsec/kiosk_mask и по умолчанию равна 0000.

При использовании маски 0000 на права доступа пользователя не накладывается никаких ограничений. Типичным значением маски при включенном режиме «Киоск» является 0003. Это значение означает, что для пользователя маскируются операции запись и исполнение ко всем, не принадлежащим ему или группе, в которую он входит, файлам.

Просмотреть текущую маску киоска можно в файле /parsecfs/mode_mask.

Для того, чтобы администратор мог задать разрешения на доступ пользователя к конкретным файлам с использованием режима «Киоск», используется команда mkiosk.

Для автоматизации процесса установки разрешений на доступ для каждого пользователя используется конфигурационный файл, расположенный в директории /etc/parsec/kiosk.

При этом в нем может содержаться как задание разрешений на доступ к конкретным файлам, так и ссылки на другие профили (например, на профили отдельных программ).

Таким образом, если внутри профиля встречается строка с именем другого профиля, то содержимое указанного профиля полностью объединяется с содержимым текущего профиля. Объединение профилей осуществляется рекурсивно. Если строка в файле профиля начинается не с символа «/», то она рассматривается как имя профиля.

Если профиль служит для запуска программы, то он должен содержать права доступа не только к самому исполняемому файлу программы, но и ко всем используемым библиотекам и всем файлам, которые открывает программа в процессе исполнения.

Создаваемый в режиме «Киоск» для каждого пользователя профиль может содержать более сложные действия, чем просто запуск команды с заданными разрешениями на доступ.

Чтобы определить, какие объекты используются отдельными командами или совокупностью команд, выполняемых пользователем, требуется выполнение трассировки хода выполнения команд.

Для решения этой задачи в режиме «Киоск» применяется команда otrace, предназначенная для проведения трассировки выполняющегося процесса относительно использования им системных вызовов.

Синтаксис команды otrace:

otrace – опции команды

Опции команды otrace приведены в таблице.

ТАБЛИЦА. Опции команды otrace

Параметр	**Описание**
-s, --silent	Не выводить информационные сообщения
-o , --output=	Записать результаты трассировки в указанный файл. По умолчанию - stdout
-k , --kiosk-dir=	Указать путь к директории с профилями режима «киоска». По умолчанию используется директория /etc/parsec/kiosk-profiles
-p , --pid=	Трассировать процесс с указанным идентификатором, а также все порожденные им процессы
-u , --user=	Указать имя пользователя. Используется совместно с опциями --audit-trace
-t, --trace	Использовать для трассировки процессов команду strace. Не может быть использована совместно с опцией --audit-trace

Таким образом, базовый функционал средств зашиты информации от НСД в ОС СН «Astra Linux SE» расширен:

− системой AFICK, которая совмещает в себе функции контроля целостности файлов и их атрибутов с использованием таких алгоритмов под-

счета контрольных сумм, как MD5 и SHA1, с интеграцией с демоном запуска программ по расписанию. Дополнительно система AFICK имеет возможность настройки правил проверки целостности директорий.

− режимом «Киоск» (инструментом ограничения прав пользователей в ОС СН). При применении режима «Киоск» маска на разрешения к объектам файловой системы накладывается при любой попытке пользователя получить доступ.

Список используемых источников

1. Гринь Д. В., Ильина О. Б., Купчиненко О. П., Скоропад А. В. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность: сб. тр. СПб.: СПОИСУ, 2017. Вып. 4. С. 76–78.

2. Ильина О. Б., Купчиненко О. П., Скоропад А. В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т. 2. С. 356–360.

3. Буренин П. В., Девянин П. Н. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition. Учебное пособие / Под редакцией доктора технических наук П. Н. Девянина. М.: Горячая линия – Телеком, 2018. 311 с.

УДК 004.056
ГРНТИ 81.93.29

ПРОЦЕДУРЫ ПОСТРОЕНИЯ СИСТЕМЫ КОНТРОЛЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ ОБЪЕКТА СВЯЗИ

Е. А. Исупова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются процедуры построения системы защиты информации и системы контроля защищенности информации от утечки по техническим каналам применительно к различным объектам инфотелекоммуникационной инфраструктуры. Уточняются процедуры классификации объекта и определения уровня защиты, каналов возможных утечек информации. Приведены результаты исследований методического аппарата, используемого для контроля защищенности. Анализируются существующие подходы и технологии к реализации функциональных элементов системы контроля за-

щищенности информации от утечки по техническим каналам. Предлагаются рациональные типовые варианты построения системы контроля защищенности информации от утечки по техническим каналам.

система защиты информации, контроль защищенности информации, утечки по техническим каналам, классификация объекта, уровень защиты, методический аппарат.

Актуальными задачами российского рынка информационной безопасности (ИБ) в равной мере для организаций (учреждений) и предприятий различных форм собственности и видов экономической деятельности, по данным онлайн-опроса Anti-Malware.ru в 2018 году [1], являются создание центров реагирования ИБ или управление безопасностью (SOC, *Security Operation Center*), защита периметра, защита от внутренних угроз, автоматизация процесса управления ИБ.

Основными функциями SOC, которые реализованы на практике [2, 3, 4], являются: администрирование средств защиты информации; выполнение функций компонент ГосСОПКА, поиск уязвимостей в сетевых сервисах, аппаратном и программном обеспечении; сбор и управление событиями ИБ; выявление компьютерных инцидентов, содействие в реагировании на них (локализация и устранения последствий).

Ключевым направлением реализуемости функций SOC для территориально распределенных объектов (сооружения связи) информационно-телекоммуникационной инфраструктуры с учетом [5, 6] (например, базовых станций с совмещенным оборудованием центров обработки данных, объектовых пунктов управления (в том числе и мобильных, при ремонтно-восстановительных работах), call-центров и других объектов согласно требований статей 6 и 7 [7]), которые имеют существенные особенности объектовых систем технической защиты информации (СТЗИ) от утечки по техническим каналам (УТК), является автоматизация процесса децентрализованного управления ИБ совместно со средствами защиты периметра, защиты от внутренних угроз объектов и с обеспечением информационно-логического взаимодействия с SOC (см. рис.).

Модель объектовых СТЗИ от УТК на рисунке не противоречит концепции многоуровневой многопозиционной защиты (ММЗ) [8, 9], описание которой в виде функционирования агрегативной схемы представлено выражением:

$$\vec{U}(t) = F\{\vec{X}(t), \vec{Y}(t), \vec{S}, \vec{P}, \vec{R}, \vec{Z}\}, \quad (1)$$

где X – вектор характеристик опасных событий для объекта защиты;

Y – вектор характеристик среды функционирования системы ММЗ;

S – вектор описания структуры системы ММЗ;

P – вектор требований к результатам ММЗ;

R – вектор требований к процессам, реализуемым в ходе обеспечения ММЗ; *Z* – вектор параметров процедур ММЗ;

U – вектор показателей эффективности ММЗ;

F – функционал, определяющий порядок перехода от векторов *X, Y, S, P, R, Z* к вектору *U*.

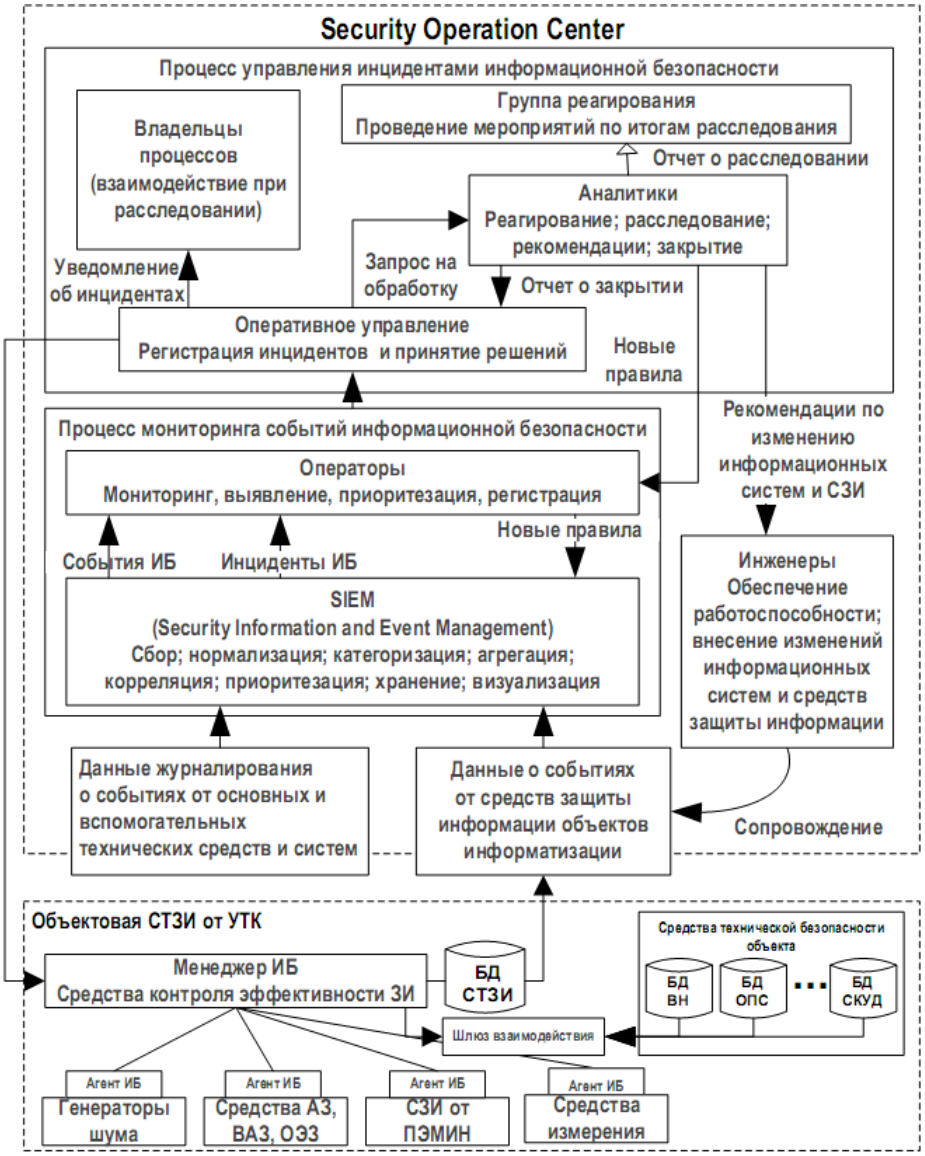


Рисунок. Модель информационно-логического взаимодействия SOC и объектовых СТЗИ

Вырожденная модель согласно формуле (1) рассмотрена в [10] на основе модели канала утечки информации с помощью логико-вероятностной (ЛВ) теории безопасности и риска, где под степенью риска понимается угроза от УТК. Фундаментальными понятиями в ЛВ-теории безопасности и риска являются понятие опасного состояния объекта, которая характеризу-

ется ущербом различного масштаба, и понятие опасности – способности системы переходить в опасное состояние. В каждом конкретном случае необходимо дать аналитическое описание этого опасного состояния объекта. В ЛВ-теории безопасности и риска такое описание начинается с составления сценария опасного состояния, которое осуществляется с помощью конъюнкций и дизъюнкций инициирующих событий и условий.

В многоуровневой декомпозиции событий значительный интерес представляет в выражении (1) вектор X, который содержит вектор b значимости (степени опасности), вектор h вероятностно-временных характеристик опасных событий, вектор g пространственного положения опасных событий с учетом [11] и выражен в виде:

$$\vec{X}(t) = \{\vec{b}(t), \vec{h}(t), \vec{g}(t)\}. \quad (2)$$

Основная цель ММЗ состоит в обеспечении требуемого уровня защищенности от воздействия дестабилизирующих факторов на информационную инфраструктуру объектов управления и связи и информацию, хранимую, обрабатываемую и передаваемую на этих объектах в рамках существующих технологий, с использованием аппаратно-программных средств и способов защиты объектов и информации [9]. На первом уровне ММЗ реализуются административно-организационные, инженерно-технические и программно-логические меры защиты от воздействия дестабилизирующих факторов. На втором – мониторинг событий. На третьем - принятие решений по способу нейтрализации по факту верификации и идентификации событий. На четвертом и пятом – оперативное реагирование и нейтрализация опасных событий.

Состав, структура и функционирование объектовых СТЗИ от УТК в такой иерархической системе различны. Они зависят от категории выделенных помещений объекта информатизации, которая обусловливает для различных категорий объектов ряд альтернативных отечественных средств защиты информации (СЗИ) от УТК. Номенклатура СЗИ от УТК содержит: генераторы акустического шума (ЛГШ-301; ЛГШ-302; ГШ-2500 и другие); средства виброакустической и акустической защиты (Эшелон; ЛГШ-401; Шторм-9 и другие); средства защиты от утечки за счет побочных электромагнитных излучений и наводок на цепи электропитания и заземления (Панцирь-М; Стикс-4; Салют 2000 С и другие), в том числе фильтры сетевые (ФСП-3Ф-15А-ИН; ФП-15МС и другие) [12]. Различные сроки действия сертификатов ФСТЭК России, как и актуальное состояние нормативно-технических документов в сфере защиты информации и СЗИ от УТК обусловливают необходимость их учета как дополнительные риски информационной безопасности.

Способы и технологии построения функциональных элементов системы контроля защищенности информации от УТК зависят от:

− реализованной управляемости (мониторинга) объектовых СЗИ;

− степени использования дополнительных специальных средств, таких как средства видеонаблюдения, физической защиты, контроля доступа и охранной сигнализации, измерительные приборы и аппаратура для мониторинга СЗИ от УТК;

− защищенности технических средств информационного взаимодействия;

− технического уровня средств контроля эффективности защиты информации (СЗИ для контроля эффективности защиты информации [13]).

В ряде работ [14] уровень управляемости СЗИ при декомпозиции объектовых СЗИ учитывается по наличию обратной связи.

Автоматизированные информационно-измерительные системы для мониторинга СЗИ от УТК незаменимы при рассредоточении объектов измерения, одновременном измерении многих параметров, длительных измерениях, измерениях по сложной программе.

Контроль состояния технической защиты информации включает контроль организации и эффективности защиты. Технический контроль защиты информации от утечки по техническим каналам осуществляется в соответствии со специально разработанными программами и методиками контроля ФСТЭК России.

Типовое построение системы контроля защищенности информации от утечки по техническим каналам основано на информационной технологии "агент-менеджер" при котором менеджер является агрегатором данных о событиях от СЗИ от УТК, средств технической безопасности объекта и данных оперативного управления от SOC в части касающейся конкретного объекта информатизации.

Внедрение изложенного подхода посредством методов совмещения телекоммуникационных, измерительных и управляющих систем объектов связи приведет к повышению эффективности контроля защищенности информации от утечки по техническим каналам.

Список используемых источников

1. Шабанов И. Анализ рынка информационной безопасности в России. Часть 1 [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Market_Analysis/ analysis-information-security-market-russia-part-1 (дата обращения 07.02.2019).

2. Сервис противодействия кибератакам IZ:SOC [Электронный ресурс]. URL: http://izsoc.ru (дата обращения 07.02.2019).

3. Центры реагирования ИБ (SOC) [Электронный ресурс]. URL: https://softline.ru/solutions/security/tsentryi-reagirovaniya-ib-soc (дата обращения 07.02.2019).

4. Организация Security Operation Center (SOC) [Электронный ресурс]. URL: https://www.itsoc.ru/wp-content/uploads/2014/09/4site_SOC.pdf (дата обращения 07.02.2019).

5. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 07.02.2019).

6. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ [Электронный ресурс]. URL: https://base.garant.ru/12148555/ (дата обращения 07.02.2019).

7. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения 07.02.2019).

8. Никифоров О. Г. О научно-методическом подходе к оцениванию эффективности функционирования многоуровневых систем защиты // Вопросы радиоэлектроники. Сер. СОИУ. 2012. Вып. 2. С. 120–123.

9. Никифоров О. Г. О некоторых концептуальных вопросах многоуровневой защиты объектов и информации // T-Comm – Телекоммуникации и Транспорт. 2013. № 6. С. 59–61.

10. Карпов А. В. Модель канала утечки и информации на объекте информатизации // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т. 2. С. 378–382.

11. ГОСТ Р 53109-2008. Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности.

12. Информационное сообщение ФСТЭК России «По вопросу продления сроков действия сертификатов соответствия на средства защиты информации от утечки оп техническим каналам» от 28.12.2016 № 240/24/6312 [Электронный ресурс] URL: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1236-informatsionnoe-soobshchenie-fstek-rossii-ot-28-dekabrya-2016-g-n-240-24-6312 (дата обращения 07.02.2019).

13. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

14. Птицына Л. К., Тарабаров А. В. Анализ методов комплексирования средств защиты информации // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т. 2. С. 541–544.

Статья представлена заведующей кафедрой,
доктором технических наук, профессором Г. В. Верховой.

УДК 004.7:004.422.8
ГРНТИ 20.01.07

РАЗРАБОТКА WEB-СЕРВИСА НА ТЕХНОЛОГИЧЕСКОЙ ПЛАТФОРМЕ

Е. А. Карачинская, Я. С. Маргаритова, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлены объективные основания для развития сервис-ориентированных систем. Рассмотрены причины расширения масштабов востребованности и применения Web-сервисов. Выбрана технологическая платформа для разработки Web-сервисов. Определены основные механизмы организации Web-сервисов на технологической платформе. Описан программный интерфейс Web-сервисов, представленный в формате WSDL. Показаны логические части документа в формате WSDL. Раскрыты основные правила формирования XML файла. Приведены описания основных возможностей использования XDTO-сериализации.

сервис-ориентированная система, технологическая платформа, формат WSDL, XML файл, XDTO-сериализация.

В настоящее время в условиях постоянно меняющегося и развивающегося информационного поля, ужесточения конкуренции между предприятиями, а также компьютеризации торгово-рыночных отношений остро стоит необходимость модернизации технологических продуктов, способных наиболее полно удовлетворить потребности клиентов, предусматривающих возможность оперативного реагирования на изменение стандартов заказчиков, а также повышения уровня качества продуктов.

Основная трудность заключается в необходимости оперативного и гибкого изменения и введения в эксплуатацию новых технологических средств в зависимости от постоянно изменяющихся рыночных отношений. Подобная проблема разрешается посредством применения сервис-ориентированной архитектуры (*Service Oriented Architecture* – SOA) в процессе разработки программных и технологических продуктов, тем самым помогая быстрее и эффективнее вводить новые сетевые технологии.

Сервис-ориентированная архитектура подразумевает оперативное технологическое обновление в сети. В связи с этим представленное направление является одним из приоритетных в области развития корпоративных информационных систем, что напрямую связано с увеличением конкурентноспособности любой компании на современном рынке [1].

SOA – это парадигма, созданная для разработки и проектирования приложений в виде систем взаимосвязанных сервисов в вычислительной среде. SOA обладает следующими характеристиками:

- улучшает взаимосвязь между архитектурой предприятия и бизнесом;
- позволяет из систем интегрированных сервисов создавать сложные приложения;
- порождает гибкие бизнес-процессы.

В настоящее время главные позиции среди сервисов, соответствующих концепции SOA, занимают Web-сервисы.

Простой протокол доступа к объектам SOAP (*Simple Object Access Protocol* – SOAP) является основной частью технологии Web-сервисов [2]. Он осуществляет перенос данных по сети и обеспечивает доставку данных Web-сервисов.

При передаче сообщений протокол SOAP увеличивает их объём и снижает скорость обработки. В системах, где скорость важна, чаще используется пересылка XML-документов через протокол HTTP напрямую, где параметры запроса передаются как обычные HTTP-параметры.

Для разработки Web-сервисов во многих корпорациях выбирается платформа «1С:Предприятие». Основания такого выбора базируются на ряде преимуществ указанной платформы, необходимых для интеграции различных технологических средств. Прежде всего, это возможность взаимодействия платформы практически с любыми внешними программами и оборудованием за счет общепринятых протоколов передачи данных и стандартов реализации [3].

Механизм Web-сервисов системы «1С:Предприятие» основан на использовании одноименных объектов метаданных, т.е. объектов конфигурации из ветви «Web-сервисы» [4].

Веб-сервис имеет программный интерфейс, представленный в формате WSDL (Web Services Description Language – WSDL), языка описания веб-сервисов и доступа к ним, основанного на языке XML.

Каждый документ WSDL разбивается на логические части:

- определение типов данных (types) – определение вида отправляемых и получаемых сервисом XML-сообщений:

```
<xs:element name="createRequest">
<xs:complexType>
<xs:sequence>
<xs:element name="userID" type="xs:integer"/>
<xs:element name="topic" type="xs:string"/>
<xs:element name="serviceCode" type="xs:string"/>
```

```
<xs:element name="workplaceCode" type="xs:string"/>
<xs:element name="description" type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:element>
```

- элементы данных (message) – сообщения, используемые Web-сервисом:

```
<message name="getWorkplacesResponseMessage">
<part name="parameters" element="tns:getWorkplacesResponse"/>
</message>
```

- абстрактные операции (portType) – список операций, которые могут быть выполнены с сообщениями:

```
<portType name="ktsTechnoParkWebsitePortType">
<operation name="createRequest">
<input message="tns:createRequestRequestMessage"/>
<output message="tns:createRequestResponseMessage"/>
</operation>
</portType>
```

- связывание сервисов (binding) – способ, с помощью которого сообщение будет доставлено:

```
<binding name="ktsTechnoParkWebsiteSoap12Binding" type="tns:ktsTech-
noParkWebsitePortType">
<soap12bind:binding style="document" transport="http://sche-
mas.xmlsoap.org/soap/http"/>
</binding>
```

При разработке соблюдаются основные правила формирования XML файла:

- элементы могут быть вложены;
- начало элемента <Имя>, конец – то же имя с добавлением символа «/»;
- внутри элемента могут быть: вложенные элементы и текст;
- у элемента могут быть свойства (атрибуты), у них указывается имя и значение;

- в XML нельзя использовать любые символы, так как некоторые из них зарезервированы собственно для XML, например, «<» и «>».
- XML удобно использовать при обмене со сторонними программами, в том числе в механизме обмена данными 1С.

В заголовке XML может быть определено пространство имен. Определяется пространство имен (namespace) следующим образом:

xmlns:ИмяПространства = “URL”.

Например: targetNamespace = *http://localhost/technopark.*

Одним из процессов преобразования данных формата XML в «1С: Предприятия» является XML-сериализация. Средства XML-сериализации используются для реализации схем обмена данными с помощью простых и сложных типов данных. Простые: число, строка, дата, булево, двоичные данные, Null, уникальный идентификатор, хранилище значения. Сложные: тип, описание типов, все объекты базы данных, удаление объекта.

Для добавления описания XML файла необходим механизм XDTO (XML *Data Transfer Objects* – XDTO) – механизм интеграции с другими системами.

Основные возможности использования XDTO заключаются в следующем:

- описание типов параметров и возвращаемых значений Web-сервисов;
- обмен данными между конфигурациями 1С:Предприятия с существенно разными структурами данных;
- обмен данными на основе схем XML, не привязанных к той или иной конфигурации (например, обмен с информационными системами, построенными не на основе 1С:Предприятия);
- создание собственной системы типов и значений для обработки произвольных данных.

XDTO-сериализация предназначена для сохранения данных объекта в файл XML и создания объекта на основе данных, хранящихся в файле XML (см. рис.).

XDTO-пакеты являются частью механизмы XDTO. Они предназначены для описания в конфигурации системы типов и значений для взаимодействия с внешними источниками данных, таких как Web-сервис.

Использование сервис-ориентированной архитектуры, реализованной с применением платформы «1С:Предприятие», позволяет интегрировать слабосвязанные программные продукты, что в свою очередь помогает повысить их повторное применение для различных ситуаций, тем самым поз-

воляя уменьшить издержки за счет интеграции различных по своему составу и применению информационных систем в технологическую структуру компании.

```
// Получить ссылку на элемент справочника Номенклатура
СсылкаНаЭлементСправочника = Справочники.Номенклатура.НайтиПоКоду("0000001");

// Создать сериализатор XDTO для глобальной фабрики XDTO
НовыйСериализаторXDTO = Новый СериализаторXDTO(ФабрикаXDTO);

// Создать объект записи XML и открыть файл
НоваяЗаписьXML = Новый ЗаписьXML;
НоваяЗаписьXML.ОткрытьФайл("D:/Exchange.xml");
```

Рисунок. XDTO-сериализация

Список используемых источников

1. Птицына Л. К., Смирнов Н. Г. Программное обеспечение компьютерных сетей. Управление крупно-гранулярными процессами на основе языка BPEL : учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2011. 105 с.

2. Птицына Л. К., Смирнов Н. Г. Системно-аналитическая основа интеграции сервис-ориентированных средств // Промышленные АСУ и контроллеры. 2011. № 5. С. 31–36.

3. Бояркин В. Э., Филатов А.И. 1С: Предприятие 8. Конвертация данных: обмен данными между прикладными решениями: учебное пособие. М.: Изд-во 1С-Паблишинг, 2008. С. 25–28.

4. Старыгин А. XML: разработка Web-приложений. СПб.: БХВ-Петербург, 2003. 585 с.

УДК 004.7:004.422.8
ГРНТИ 20.01.07

РАСШИРЕНИЕ СИСТЕМЫ КОРПОРАТИВНЫХ WEB-СЕРВИСОВ

Е. А. Карачинская, Я. С. Маргаритова, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Актуализировано развитие сфер профессиональной деятельности в среде информационных инфраструктур. Показана целесообразность развития сфер профессиональной деятельности посредством расширения системы корпоративных Web-сервисов. Рассмотрены основания для выбора технологической платформы для разработки

Web-сервисов. Представлены основные компоненты процесса построения Web-сервисов на выбранной технологической платформе. Раскрыты ключевые особенности реализации Web-сервисов для организации обмена информацией между клиент-серверным приложением и клиентом.

корпоративная информационная система, сервис-ориентированная архитектура, сервис, протокол.

В настоящее время происходит процесс быстрого развития, а также внедрения компьютерных технологий в различные сферы профессиональной деятельности человека. Особенно это проявляется в таких областях, как экономика, промышленность, образование и медицина. Современный этап развития общества характеризуется постоянным ростом объема информации. В утвержденной 9 мая 2017 г. «Стратегии развития информационного общества в РФ на 2017-2030 годы» отмечено, что «информационные и коммуникационные технологии стали частью современных управленческих систем во всех сферах профессиональной деятельности» [1]. Развитие сфер профессиональной деятельности сопровождается стремительным внедрением информационных инфраструктур, включающих набор базовых информационных сервисов, вычислительных систем, систем хранения и передачи данных, которые являются основой для функционирования Web-сервисов. Информационная инфраструктура образует не только среду для автоматизации уже существующего профиля деятельности, но и поддерживает инновационные технологии, предназначенные для развёртки и сопровождения новых профилей деятельности.

Постоянное развитие информационных систем (ИС) и внедрение Web-технологий привело к созданию корпоративных информационных систем (КИС) в соответствии с принципами организации сервис-ориентированных архитектур (*Service Oriented Architecture* – SOA) [2]. КИС отличается от других ИС расширенным функционалом и классом задач, которые решаются в процессе профессиональной деятельности. В основе построения КИС лежит концепция единого информационного пространства, предусматривающая взаимодействие всех её подсистем с единой базой данных.

Системы корпоративных Web-сервисов на сегодняшний день являются основным фактором повышения эффективности и конкурентоспособности бизнеса любой компаний, а также являются инструментом автоматизации деятельности предприятий. Развитие сфер профессиональной деятельности посредством расширения системы корпоративных веб-сервисов определяется необходимостью разрабатывать новые инструменты и методы эффективного управления общим информационным пространством. Непрерывно проводимая модернизация информационных элементов неизбежно влечет за собой и совершенствование информационной системы в целом.

Процесс создания и разработки корпоративных Web-сервисов требует обоснованного выбора технологической платформы. Необходима современная, надежная платформа с гибкой инфраструктурой. Платформа «1С:Предприятие» как предметно-ориентированная среда разработки корпоративных Web-сервисов имеет определенные преимущества. В термин «1С:Предприятие» входят такие понятия, как платформа и набор прикладных решений и методик. Данная платформа используется не только как средство настройки прикладных решений, которые поставляет Фирма «1С», но и как средство для создания новых прикладных решений. В задачу платформы входит предоставление разработчику необходимого набора инструментов для быстрой разработки, отладки и поддержки прикладного решения для автоматизации процессов. Благодаря гибкости данной платформы продукт «1С:Предприятие» можно использовать в различных областях. Созданные прикладные решения на базе данной платформы позволяют решать задачи различной сложности – от автоматизации одного рабочего места, до создания корпоративной информационной системы, что позволяет отойти от «лоскутных технологий» и перейти к более содержательным и высокоуровневым технологическим решениям. Обеспечение высокой степени согласованности задействованных технологий и инструментов происходит благодаря широкой палитре функциональности средств платформы для решения задач профессиональной деятельности, которые ставят перед разработчиками.

Обмен информацией в платформе 1С может происходить при различных её конфигурациях. При этом поддерживается и взаимодействие со сторонними программами. Web-сервисы широко используются для интеграции различных приложений между собой. В платформу «1С:Предприятие» включены возможности работы с Web-сервисами. При использовании данных сервисов нет необходимости в предоставлении доступа к базе данных 1С, что существенно облегчает решение задачи защиты информации [3]. Сторонние информационные системы получают доступ исключительно к набору функций 1С, которые предоставляют конечный результат обмена данными.

Web-сервисы на выбранной технологической платформе соответствуют концепции сервис-ориентированной системы. Подобная архитектура подразумевает, что приложения на разных платформах взаимодействуют между собой согласно протоколу Simple Object Access Protocol (SOAP). На рисунке представлена архитектура приложения на основе использования протокола SOAP.

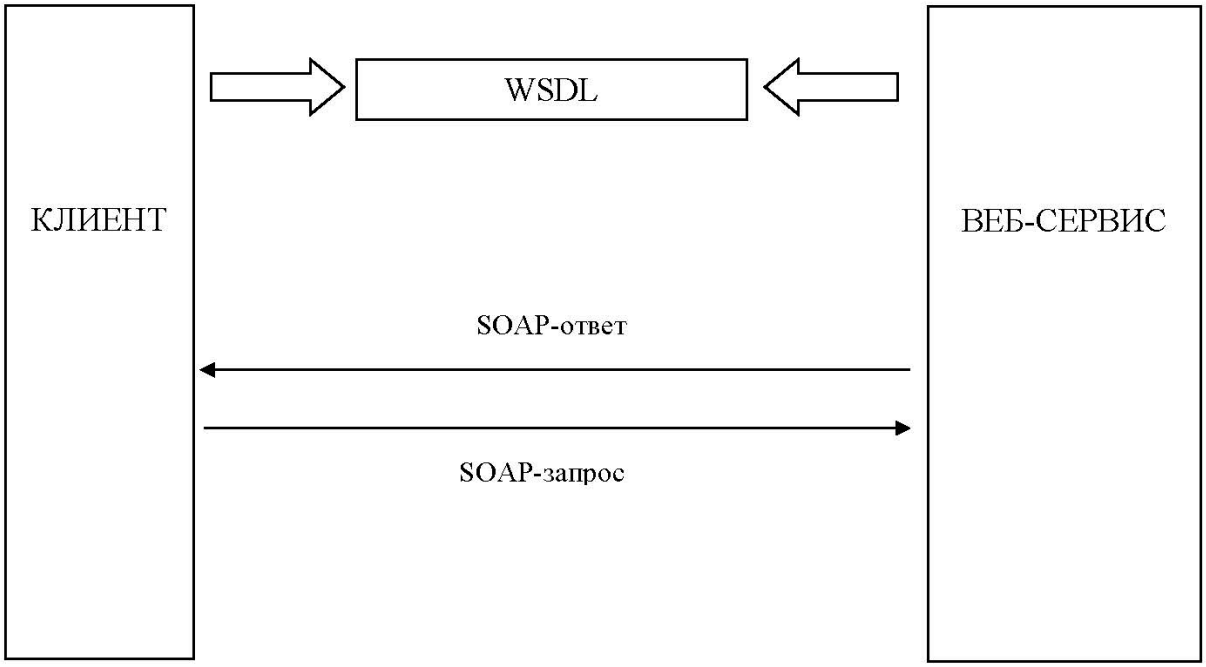


Рисунок. Архитектура приложения на основе протокола SOAP

Протокол SOAP осуществляет перенос данных по сети и обеспечивает доставку Web-сервисов. При передаче сообщений протокол SOAP увеличивает их объем и снижает скорость обработки. В системах, где скорость важна, используется пересылка XML документов на основе протокола HTTP напрямую, где параметры запроса передаются как обычные HTTP параметры. Реализация архитектуры SOA основана на связке специфицируемых консорциумом W3c таких технологических компонентов, как Web-сервисы, протоколы SOAP, языки WSDL (WSDL – *Web Service Definition Language*), WADL (*Web Application Description Language*) и пр., при реализации которых применяется язык XML (*eXtensible Markup Language*), обеспечивающий описание сложной структуры данных в обычном текстовом файле [4]. Благодаря таким технологическим компонентам, прикладное решение «1С:Предприятие» может выступать в роли как поставщика Web-сервисов, так и потребителя Web-сервисов. Сервер «1С:Предприятие» является частью концепции «трехзвенной архитектуры» и выполняет функцию сервера приложений. Подобная схема работы уменьшает зависимость производительности от количества пользователей, а также от объёма базы данных.

Основная нагрузка при выполнении вычислительных операций при сервис-ориентированной архитектуре ложится на Web-сервисы. При выполнении обмена информацией между клиент-серверным приложением и клиентом используются мультиплатформенные технологии. Общий механизм работы Web-сервисов заключается в создании функционала, доступ-

ного для сторонних разработчиков. При публикации на Web-сервере данный функционал будет доступен для интеграции с другими информационными системами в формате WSDL. Данный формат содержит описание методов публикуемого Web-сервиса и типов данных, которые могут передаваться между сервисом и клиент-серверным приложением. Система 1С может экспортировать весь набор функциональности через Web-сервисы. При создании или расширении старых корпоративных Web-сервисов их определения задаются в дереве конфигураций платформы, после чего становятся доступными для других произвольных информационных систем. Для обмена информацией между клиент-серверным приложением и клиентом необходимо выполнить следующие действия:

- Создать в конфигурации платформы необходимое и достаточное количество Web-сервисов (добавить метаданные объекта конфигурации, описать операции, которые будет выполнять действующий Web-сервис, описать параметры операции);
- С помощью специального инструмента конфигуратора опубликовать на Web-сервере созданные Web-сервисы;

В основе сервисной архитектуры находится менеджер сервисов, который выполняет определенные функции:

- управляет пулом соединений с различными информационными базами;
- поддерживает WSDL описание Web-сервиса;
- реализует протокол SOAP.

Механизм корпоративных Web-сервисов, реализованных на платформе «1С:Предприятие», поддерживает определённый ряд стандартов:

- SOAP 1.1;
- SOAP 1.2;
- WSDL 1.1;
- WS-I Basic Profile 1.1;
- HTTP 1.1;
- SSL 3.0/TSL 1.0.

Методологическое обеспечение сервис-ориентированных архитектур, формализованные основы которого представлены в [5, 6], позволяют обеспечить соблюдение гарантий качества информационных услуг в среде корпоративной системы.

Чем интенсивнее развиваются информационные технологии, тем чаще они интегрируются между собой. Выбранная платформа 1С активно развивается в данном направлении, поддерживая большое количество форматов обмена данных, технологий и механизмов для интеграции и обмена данными. Благодаря использованию механизмов Web-сервисов система «1С» выступает как набор сервисов в сложных распределённых и гетерогенных

системах, а также позволяет производить интеграцию с другими информационными системами с помощью сервис-ориентированной архитектуры. При создании или расширении корпоративных Web-сервисов создаются новые приложения, что обеспечивает экономический эффект для бизнеса компаний и предприятий. В ближайшее время Web-сервисы станут незаменимым инструментом для обработки и генерации информации, что будет способствовать реализации новых технологических проектов.

Список используемых источников

1. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы [Электронный ресурс]: указ Президента РФ от 09.05.2017 № 203. URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения 08.01.2019).

2. Сатунина А. Е., Сысоев А. С. Сервис-ориентированный подход к построению и функционированию корпоративной информационной системы // Современные проблемы науки и образования. 2009. № 6-1. URL: http://www.science-education.ru/ru/article/view?id=1295 (дата обращения 10.01.2019).

3. Аунг Аунг Хейн, Щукин Б. А. Обеспечение информационной безопасности при взаимодействии с веб-сервисом // Безопасность информационных технологий, № 1, 2012. С. 124–127.

4. W3 Inc. Официальный сайт спецификации SOAP. [Электронный ресурс]. – URL: http://www.w3.org/TR/2007/REC-soap12-part0-20070427/ (дата обращения 25.01.2011).

5. Птицына Л. К., Смирнов Н. Г. Программное обеспечение компьютерных сетей. Управление крупно-гранулярными процессами на основе языка BPEL: учеб. Пособие. СПб.: Изд-во Политехн. ун-та, 2011. 105 с.

6. Птицына Л. К., Веселов В. О. Анализ интеграции сервис-ориентированных средств в активных инфокоммуникационных средах // Наукоёмкие технологии в космических исследованиях Земли. H&ES RESEARCH. М.: ООО «Издательский Дом Медиа Паблишер». 2015. № 2. С. 42–47.

УДК 004.032
ГРНТИ 20.53.19

АНАЛИЗ ОЦЕНКИ УРОВНЯ ЗНАНИЙ АБИТУРИЕНТОВ С ПРИМЕНЕНИЕМ НЕЙРОННОЙ СЕТИ

Р. Р. Князев, Л. П. Козлова, К. Б. Мурсалимова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С ежегодным увеличением количества абитуриентов возникает необходимость создания автоматизированной системы для анализа и оценки уровня знаний абитуриентов. Данная задача является трудоемкой, которую невозможно решить с помощью

традиционного математического аппарата. В статье рассматривается возможность разработки системы с использованием нейронных сетей.

нейронная сеть, образование, оценка, анализ.

С динамичным развитием информационных технологий появляются новые возможности создания автоматизированных систем для анализа и обработки данных в различных сферах деятельности, в том числе и образовательной. Учебные заведения представляют собой сложный объект, в которых все информационные процессы трудно поддаются формализации. Одной из причин является ежегодный рост числа абитуриентов и увеличивающийся объем информации о них. Применение искусственных нейронных сетей (ИНС) позволяет эффективно решить данную проблему.

Искусственные нейронные сети – это попытка моделирования возможностей обработки информации нервной системой живых организмов [1].

ИНС позволяют воспроизводить чрезвычайно сложные зависимости и справляются с задачами высокой размерности. Они представляют собой математическую структуру, имитирующую некоторые аспекты работы человеческого мозга и демонстрирующие такие его возможности, как способность к неформальному обучению, способность к обобщению и кластеризации неклассифицированной информации, способность самостоятельно строить прогнозы на основе уже предъявленных временных рядов [2].

Составной частью ИНС является искусственный «нейрон» (рис. 1). Он состоит из элементов трех типов: умножителей (синапсов), сумматора и нелинейного преобразователя. Синапсы осуществляют связь между нейронами, умножают входной сигнал на число, характеризующее силу связи (вес синапса). Сумматор выполняет сложение сигналов, поступающих по синаптическим связям от других нейронов, и внешних входных сигналов. Нелинейный преобразователь реализует нелинейную функцию, или функцию активации, одного аргумента – выхода сумматора [3].

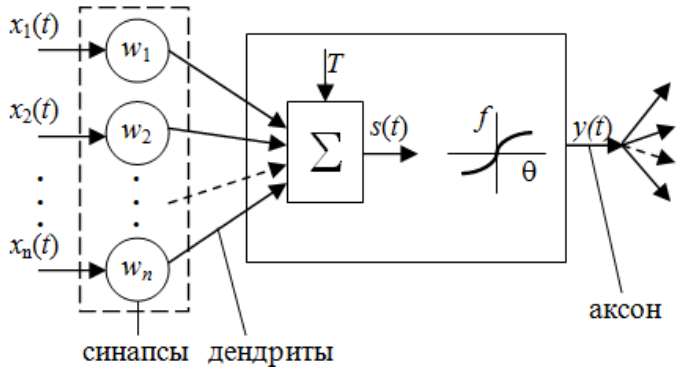


Рис. 1. Схема искусственного нейрона

Вектор **X** образуется совокупностью входных сигналов нейрона, поступающих на вектор весов **W** (совокупность весовых коэффициентов w_i). На блок Σ поступает сигнал полезного отклика *T*, выходом которого является взвешенная сумма входных сигналов $s(t)$, поступающих на нелинейную функцию активации *f*. В результате чего получается выходной сигнал нейрона $y(t)$.

В математическом представлении функционирование нейрона *k* можно описать следующей парой уравнений:

$$u_k = \sum_{j=1}^{m} w_{kj} \cdot x_j ,$$

$$y_k = \varphi(u_k + b_k),$$

где $x_1, x_2, \ldots, x_m$ – входные сигналы; $w_{k1}, w_{k2}, \ldots, w_{km}$ – синаптические веса нейрона *k*; u_k – линейная комбинация входных воздействий; b_k – порог; $\varphi()$ – функция активации; y_k – выходной сигнал нейрона [3].

Рассмотрим некоторые проблемы, решаемые с помощью ИНС:

1. Классификация, то есть распределение данных по параметрам.

2. Поиск зависимостей. ИНС позволяет на основе обучающей выборки построить зависимость одного параметра от других в виде сложной функции.

3. Кластеризация. Алгоритм кластеризации основан на подобии образов и размещает близкие образы в один кластер. Кластеризация позволяет представить неоднородные данные в более наглядном виде и использовать далее для исследования каждого кластера различные методы.

4. Прогнозирование. Нейронные сети широко используются для прогнозирования различных факторов, показателей. Прогноз имеют значительное влияние на принятие решений в бизнесе, науке и технике [1].

Тип задачи, которую может решить нейронная сеть, определяется тем, как она работает и обучается.

Одним из этапов построения нейронной сети является ее обучение. Цель обучения состоит в корректировке весовых коэффициентов. Корректировка выполняется итеративно, пока нейронная сеть не будет производить необходимые выходные сигналы. Нейронная сеть может быть применена на практике только после прохождения обучения.

Для разработки информационной системы на базе ИНС анализа уровня знаний абитуриентов необходимо построить диаграмму потока данных (рис. 2).

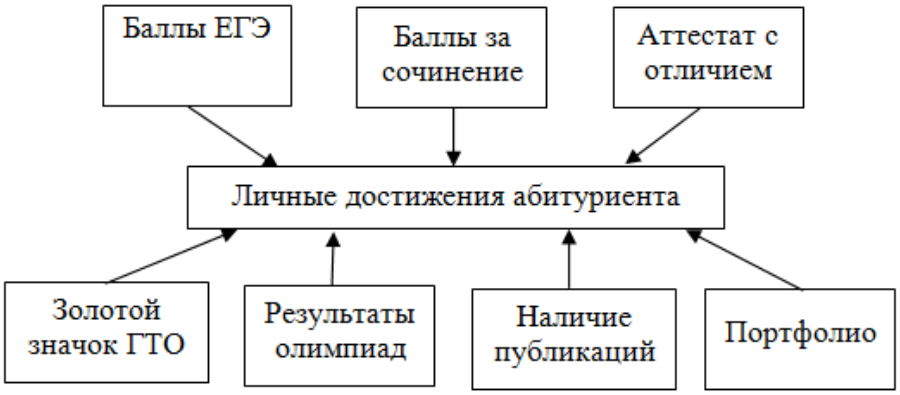


Рис. 2. Диаграмма потока данных абитуриента

В свою очередь база данных (БД) абитуриенты будет взаимодействовать с другими БД учебного заведения.

Таким образом, нейросетевой подход к оценке уровня знаний абитуриентов дает возможность учебному заведению наиболее эффективно проводить анализ получаемых данных, управлять персоналом и набором студентов, а также сократить время при принятии решений.

Создание такой автоматизированной системы является актуальной задачей, имеющей большое значение в управлении и развитии учебного заведения.

Список используемых источников

1. Rojas, R. Neural Networks: A Systematic Introduction. Berlin: Springer-Verlag, 1996. 509 p.

2. Kozlova, L. P., Kozlova, O. A., Belov, A. M. The Use of Neural Networks for Planning the Behavior of Complex Systems // Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). Pp. 902–904. DOI: 10.1109/EIConRus.2018.8317234, ISBN: 9781538643396

3. Круглов В. В., Дли М. И., Голунов Р. Ю. Нечеткая логика и искусственные нейронные сети. М.: Физматлит, 2001. 224 с.

УДК 004.85
ГРНТИ 20.53.19

ПРИМЕНЕНИЕ АНАЛИТИЧЕСКИХ ПРИЛОЖЕНИЙ НА РАЗЛИЧНЫХ ПЛАТФОРМАХ

Р. Р. Князев, Л. П. Козлова, К. Б. Мурсалимова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В информационную эру всё большее значение приобретает обработка и анализ данных. Для реализации оперативных и стратегических решений компании использует аналитику данных, помогающая получить значимые сведения из данных и трансформировать знания в действие. В статье рассматриваются решения, применяемые на различных платформах.

анализ данных, обработка данных, мультиплатформа, аналитические приложения.

С развитием технологий и увеличением числа пользователей мобильных устройств в программном обеспечении возрастает потребность в аналитике.

Аналитика – это использование данных, информационных технологий, статистического анализа, количественных методов, математических и компьютерных моделей для понимания сущности бизнес процессов, и принятия обоснованных решений, основанных на фактах [1].

На данный момент существуют различные аналитические приложения, каждое из которых предлагает свои преимущества, предоставляя информацию по различным метрикам и параметрам, позволяющей узнать актуальность продукта у непосредственных пользователей, их количество и ежедневный прирост.

На основе вышесказанного принимаются решения о выпуске продуктов, их оценивании, потребности ресурсов и о количестве необходимого персонала для поддержания проекта. Их принятие сильно затруднено из-за неопределенности и несовершенности информации, многие из них имеют значительные экономические последствия. Таким образом, эксперты нуждаются в точной информации для принятия важных решений, которые повлияют на их проект и имидж компании. Это одна из причин, по которому аналитика важна в современной деловой среде.

Аналитические приложения принято разделять на три основных категории: количественная, качественная и аналитика сбоев производительности в приложениях.

Количественная аналитика использует числовые данные и помогает измерить успешность программного продукта и проанализировать показатели, используя конкретные данные, предоставляя точную информацию о конверсии, числу переходов между страниц, а также проведенном времени в приложении [2].

Основными количественными метриками, применяемыми в бизнес-среде, являются:

- Customer Retention Rate (CRR) (уровень удержания клиентов), показывающий количество пользователей продолжающих использовать приложение спустя день, неделю, месяц или год с момента первого запуска. Эта метрика имеет решающее значение для успеха приложения, поэтому компании вкладывают средства в продвижение и приобретение новых пользователей. Для расчета коэффициента удержания CRR используется следующая формула:

$$CRR = \frac{N_1 - N_2}{N_1} \cdot 100\%,$$

где N_1 – количество клиентов на конец периода;

N_2 – количество новых клиентов, приобретенных за период.

- Daily Active Users (DAU) – ежедневные активные пользователи. Отвечает на вопрос «Сколько людей считают приложение достаточно полезным, чтобы использовать его каждый день?». Чем быстрее растет это число, тем больше вероятность того, что выручка увеличится. Однако, взятый как отдельный показатель, *DAU* может быть немного обманчивым.
- Monthly Active Users (MAU) – ежемесячное количество активных пользователей. Работает по аналогичному принципу с DAU, но включает в себя большее количество пользователей. Тем самым показывая тех пользователей, которые готовы использовать приложение ни меньше одного раза в месяц.
- Return on Investment (ROI) – доходность инвестированного капитала или коэффициент окупаемости. Применяется для конкретных маркетинговых кампаний, где имеется прямая и измеримая прибыль, например, реклама продукта. Окупаемость инвестиций довольно сложно точно рассчитать из-за существующей погрешности, связанной с усилиями по разработке самого продукта. Для расчета применяется следующая формула:

$$ROI = \frac{\text{сумма прибыли или убытков} - \text{стоимость инвестиций}}{\text{стоимость инвестиций}}.$$

- Cost Per Install (CPI) – стоимость одной установки приложения. Является показателем затрат для привлечения новых пользователей. Чем ниже цена за приобретение, тем более привлекательным для пользователей является разрабатываемое приложение. Для расчета применяется следующая формула:

$$CPI = \frac{\text{затраты на рекламу}}{\text{общее количество установок}}.$$

На рисунке приведен график колебания CPI для iOS и Android в декабре 2018 года, основанный на анализе 13 000 рекламных кампаний.

Рисунок. График колебания CPI для iOS и Android в декабре 2018 года

Однако для определения реальной ценности и определения причин происходящего необходимо также применять и качественные метрики.

Качественная аналитика позволяет разработчикам увидеть приложения глазами пользователя и проанализировать их поведение в различных ситуациях, определить в каких моментах у них возникают проблемы.

Аналитика сбоев производительности фокусируется на сборе и анализе возникающих ошибок и багов в приложении. Возникающие проблемы и неполадки в работе приложения сильно подрывают доверие и удовлетворенность от использования приложения. Данный тип аналитики позволяет автоматически генерировать подробные отчеты об устройстве, статусе батареи, соединении с Wi-Fi, и ориентации в пространстве телефона.

В данный момент существует широкий спектр аналитических инструментов с различными функциями и возможностями для анализа.

Firebase – бесплатная платформа мобильной аналитики от Google . Содержит в себе богатый функционал количественной аналитики и аналитики сбоев производительности. Ее ключевыми особенностями являются деталь-

ные данные о внутренних покупках, глубокая сегментация аудитории, отчёты возникших неполадок и аппаратные данные устройства. Важным функциональным решением является возможность идентифицировать нелетальные ошибки, которые не приводят к закрытию приложения, но вызывают нестабильность его работы.

Mixpanel – аналитический сервис, совмещающий в себе возможности качественной и количественной аналитики и позволяющий понять путь пользователя в мобильных и Веб приложениях. Данный сервис фокусируется на отчетах о действиях, позволяя отслеживать конкретных пользователей и создавать когортные группы на выбранном промежутке времени. Основными особенностями являются: A/B тестирование, аналитика вовлечения и конверсионные воронки.

Appsee – аналитическая платформа, фокусирующаяся на качественной аналитике. Главным образом выделяется благодаря своим функциям записи сессии пользователя и тепловым картам. Записи сессий пользователя автоматически помечают все пользовательские события и предоставляют исчерпывающую визуализацию взаимодействия каждого пользователя в приложении. Сенсорные тепловые карты предоставляют информацию на совокупном уровне, показывающую, где именно и как пользователи взаимодействуют с каждым экраном, и сталкиваются ли они с какими-либо проблемами пользовательского интерфейса. Помимо этих качественных функций Appsee предлагает воронки преобразования, записи о сбоях и символику, когорты действий.

Таким образом, аналитика помогает лучше понять действия и желания пользователя, а совместное использование количественной и качественной аналитики, отчетах о сбоях позволяет принять необходимые бизнес решения, основанные на точной информации, и внести своевременные изменения и корректировки для развития и продвижения приложения.

Список используемых источников

1. Evans, J. R. Business Analytics: Methods, Models, and Decisions. 2nd. Global Ed. Pearson, 2017. 653 p.

2. Harty, Julian, Aymer, Antoine. The Mobile Analytics Playbook: A Practical Guide to Better Testing. Hewlett Packard Enterprise, 2015. 161 p.

УДК 004.512.4
ГРНТИ 20.53.19

ЧАТ-БОТЫ КАК ИНТЕРФЕЙС ИНФОРМАЦИОННОЙ СИСТЕМЫ

В. А. Ковальчук, М. В. Котлова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрена основная роль социальных сетей в жизни человека. Выявлен набор сервисов, интегрированных в социальную сеть, способных сформировать взаимодействие пользователя с информационной системой стороннего разработчика. Описана технология чат-ботов, определена область применения рассматриваемой технологии. Приведена классификация чат-ботов, рассмотрены достоинства и недостатки эксплуатации технологии. Определены возможности предлагаемого решения в социальных сетях и мессенджерах. Предложено использование технологии чат-бота на примере социальной сети «Вконтакте», как интерфейса информационной системы. Представлены перспективы развития технологии чат-ботов.

социальные сети, мессенджеры, автоматизированная система, python, чат-боты, application programming interface, программирование.

По мере расширения социальных сетей и средств для быстрой передачи сообщений растет и их функциональный потенциал, который позволяет упрощать работу пользователя с сервисами.

На данный момент можно выделить 4 основных вида чат-ботов [1].

1) Справочники – боты, которые позволяют искать необходимую информацию, проводя её первичный анализ. Ярким представителем данной категории является голосовой помощник, разработанный компанией Яндекс – Алиса (в функционал которого входит поиск и анализ информации в интернете, выполнение макросов и простой диалог. Наличие собственного API позволяет совершенствовать и разрабатывать новые «навыки»). Бот-справочник 1NFORM разработан специально для абитуриентов и первокурсников университета СПбГУТ (в рамках проекта 1NFORM). Данное приложение отвечает на часто задаваемые вопросы и помогает найти необходимую аудиторию внутри университета.

2) Консультанты – осуществляют общение с потенциальными или реальными клиентами с целью оказания услуг, от простых менеджеров в интернет-магазинах до медицинских и юридических услуг. Яркими представителями данного класса являются чат-боты банков, выполняющие работу службы поддержки в соответствующем приложении.

3) Развлекательные – реализующие модель виртуального собеседника, отвечающего на вопросы. Например: pbot – простой бот-собеседник, имитирующий беседу реального человека. Возможность оценки каждого ответа на совпадение позволяет улучшить работоспособность приложения.

4) Бизнес-системы – улучшают работу той или иной организации, упрощая взаимодействие между отделами и сокращая бюрократическую деятельность. Например: чат-бот СС СПбГУТ позволяет регистрироваться студентам на мероприятия, подавать жалобы и предложения Студенческому совету СПбГУТ, а также упрощает создание служебных записок внутри университета.

Для создания чат-ботов, в основном, используется технология API (*Application Programming Interface*). API разрабатывается со стороны самих социальных сетей и мессенджеров, в связи с чем, разработка одного чат-бота может различаться в зависимости от площадки размещения. В связи с этим, чаще всего, при разработке этой технологии используется REST API (*Representational State Transfer*), позволяющая упростить интеграцию сервиса с различными платформами. Технология заключается в том, что система размещается на сервере с непрерывным режимом ожидания, а взаимодействие с сервером происходит посредством отправки на него POST-запроса по протоколу HTTP [2].

На рис. 1 представлен процесс технологии чат-бота, применяя API социальной сети «Вконтакте» для разработки «АСУ делопроизводства Студенческого совета СПбГУТ».

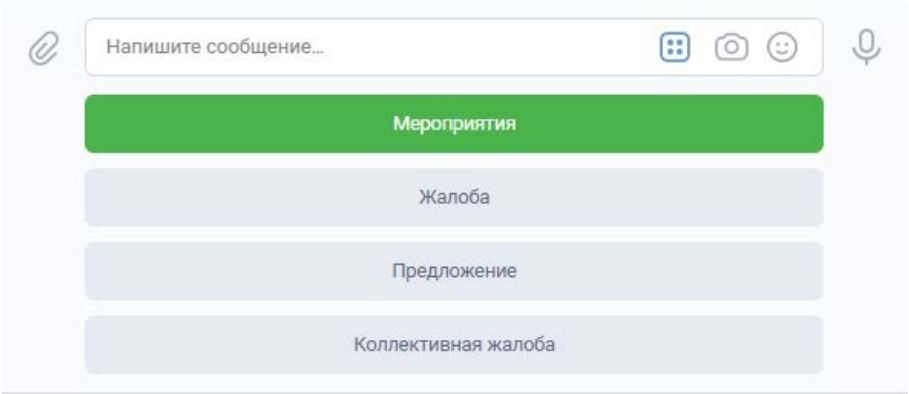


Рис. 1. Интерфейс чат-бота «АСУ делопроизводства Студенческого совета СПбГУТ»

Задача системы заключается в том, чтобы наладить быструю связь студентов со студенческим советом и позволить вести статистику по участникам мероприятий, а также упростить составление служебных записок для членов подразделений СС. Для разработки системы выбран язык программирования Python 3.4, версия API «Вконтакте» – 5.80. Пример реализации

REST API разработанной системы с использованием библиотеки Flask, размещен на рис. 2.

Представленный фрагмент кода описывает инициализацию приложения Flask, которое отвечает за перенаправление запросов к серверу, а также за ответы на эти запросы.

```
1  from flask import Flask, request, json
2  from settings import confirmation_token
3  import messageHandler
4
5  app = Flask(__name__)
6
7
8  @app.route('/', methods=['POST'])
9  def processing():
10     data = json.loads(request.data)
11     if data['type'] == 'confirmation':
12         return confirmation_token
13     elif data['type'] == 'message_new':
14         messageHandler.create_answer(data['object'])
15         return 'ok'
```

Рис. 2. Реализация REST API на Flask

Затем происходит перенаправление POST запроса, инициирующего выполнения определенных действий со стороны сервера. Функция processing производит чтение Json-формата для дальнейшей обработки. В данном случае на сервер могут приходить запросы двух типов: confirmation и message_new. В случае запроса confirmation API «Вконтакте» проверяет сервер на корректность, чтобы в дальнейшем ему можно было отправлять уведомления о новых событиях. Сообщение message_new приходит в случае получения нового сообщения от пользователя, оно обрабатывается, выполняя все необходимые действия и возвращает положительное уведомление в случае успешного завершения.

Следующий скрипт, приведенный на рис. 3, представляет функции, поддерживающие общение с API «Вконтакте» для отправки новых сообщений пользователям.

```
17  def send_private(message):
18      if message.keyboard:
19          print(message.keyboard)
20          return api.messages.send(
21              access_token=token,
22              user_id=message.user_id,
23              message=message.answer_text,
24              attachment=message.attachment,
25              keyboard=message.keyboard
26          )
```

Рис. 3. Реализация общения с VK API для отправки новых сообщений

Функция send_private() выполняет функцию отправки запроса к VK API с определенными задаваемыми параметрами:

- Access token – уникальный токен, необходимый для верификации запроса к API;
- User id – уникальный идентификатор пользователя, которому отправляется сообщение;
- Message – текст сообщения;
- Attachment – прикрепляемые к сообщению документы;
- Keyboard – Json-формат клавиатуры в виде заготовленных макросов, который упрощает взаимодействие пользователя с приложением.

Функция try_send() служит декоратором для send_private, выполняя проверку отправляемого запроса к серверу на возвращение ошибки.

Данное приложение успешно внедрено в работу студенческого совета СПбГУТ. За время его функционирования оно успешно демонстрирует достижение всех поставленных задач, уменьшая издержки и максимально адаптируясь к потребностям студенческой среды.

Технология чат-ботов, а также технологии, применяемые совместно с ней, меняют пользовательский опыт, перенося его на новый уровень.

Список используемых источников

1. Криволапова Е. В., Никонова Е. З. Чат-боты: история технологии и перспективы развития // Современное программирование: сб. науч. тр. / Под ред. Т. Б. Казиахмедова. Нижневартовск: Из-во Нижневарт. гос. ун-та, 2018. С. 100–102.

2. Осадчук П. О. Чат-боты для автоматизации внутренних коммуникаций // Молодой ученый. 2018. № 27 (213). С. 12–16.

Статья представлена заведующим кафедрой,
доктором технических наук, профессором Л. К. Птицыной.

УДК 004.93+004.62
ГРНТИ 81.93.29

О СТАТИСТИЧЕСКИХ СВОЙСТВАХ АЛГОРИТМОВ СЖАТИЯ И ШИФРОВАНИЯ

А. В. Козачок, А. А. Спирин

Академия Федеральной службы охраны Российской Федерации

В работе рассмотрена возможность применения метода тестирования свойств битовых последовательностей как одного из возможных подходов к решению задачи различения алгоритмов сжатия и шифрования. Результаты проведенного анализа позволили сделать вывод о применимости рассмотренного признакового пространства для идентификации алгоритмов сжатия ZIP, RAR, 7-Z *и шифрования* AES, TripleDES*, и возможности их различения с точностью более 0,99.*

идентификация алгоритмов сжатия и шифрования, статистическое тестирование информации.

DLP (Data Loss Prevention) – системы разработаны для предотвращения утечек защищаемой информации. Защита осуществляется путем контроля передаваемой информации и её анализа на наличие сигнатур, маршрута перемещения и некоторой другой служебной информации. Злоумышленниками, с целью обхода DLP-систем, используется шифрование и сжатие передаваемых сообщений.

В настоящее время DLP-системы имеют возможность анализа сжатых файлов, для шифрованных файлов такая возможность отсутствует. С целью предотвращения утечки информации необходимо блокировать передачу шифрованных данных, что обуславливает актуальность решения задачи различения сжатых и шифрованных файлов.

Похожая задача в части обнаружения шифрованного трафика между центром управления и зараженными узлами сети Интернет решалась в работе [1]. Для его идентификации использовалась оценка энтропии, которая возрастает в случае присутствия в нем шифрованных данных. Но высокой энтропией обладают и некоторые типы нешифрованных данных: мультимедиа, исполняемые и сжатые файлы. Таким образом оценка энтропии не позволяет решить задачу различения сжатых и шифрованных данных.

Для построения системы обнаружения передачи шифрованной информации было выбрано признаковое пространство на основе анализа частоты встречаемости битовых последовательностей различной длины N (в битах) [2].

В рамках проводимого исследования были выбраны алгоритмы шифрования AES, Triple DES (параметры по умолчанию, ключ шифрования длиной 18 байт), реализованные в пакете openSSL версии "1.0.2*g* 1 March 2016" [3] и алгоритмы сжатия ZIP, RAR,7-Z (параметры по умолчанию), реализованные в программном обеспечении WinRar [4] и 7-Z File Manager [5].

При проведении эксперимента была подготовлена выборка из 1 000 файлов по 600 Кбайт, содержащая текст на русском языке. Каждый элемент был преобразован каждым алгоритмом сжатия и шифрования. В результате было получено 6 000 файлов.

Для оценки применимости выбранного признакового пространства использовалась кроссвалидация (количество подвыборок было выбрано равным 100) классификаторов машинного обучения с параметрами по умолчанию [6]: классификатор деревьев решений [7, 8, 9], классификатор *K*-ближайших соседей [10], классификатор опорных векторов [10], классификатор на основе случайного леса (КСЛ) [11]. Наилучший результат удалось получить при использовании классификатора на основе случайного леса. Результаты экспериментальной оценки представлены в таблице.

Метрикой для оценки качества классификаторов была выбрана точность (1):

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \quad (1)$$

где TP – количество объектов, верно отнесенных к классу 1,

TN – количество объектов верно отнесенных к классу 0,

FP – количество ложных срабатываний (ошибка первого рода),

FN – количество пропусков цели (ошибка второго рода).

ТАБЛИЦА. Точность различения типов файлов

Тип файлов	Точность алгоритма для последовательности длины							
	$N = 4$	$N = 5$	$N = 6$	$N = 7$	$N = 8$	$N = 9$	$N = 10$	$N = 11$
	Время, затрачиваемое на извлечение признаков, в минутах							
	6	11	15	22	37	69	135	268
AES/7-Z	0,821	0,843	0,834	0,835	0,938	**0,993**	**0,998**	**1,000**
AES/RAR	0,986	**0,992**	**0,994**	**0,992**	**0,991**	**0,997**	**0,993**	**0,993**
AES/ZIP	0,986	**0,992**	0,988	**0,990**	**0,993**	**0,998**	**0,999**	**0,999**
DES/7-Z	0,834	0,846	0,865	0,865	0,947	**0,993**	**0,998**	**1,000**
DES/RAR	0,984	**0,990**	**0,991**	**0,993**	**0,991**	**0,996**	**0,994**	**0,994**
DES/ZIP	**0,991**	0,988	**0,991**	0,989	**0,991**	**0,997**	**0,998**	**0,999**
7-Z/ZIP	0,968	0,974	0,974	0,973	0,971	0,972	0,976	0,978
7-Z/RAR	0,948	0,960	0,964	0,963	0,964	0,983	**0,996**	**0,999**

Тип файлов	Точность алгоритма для последовательности длины							
	N = 4	*N* = 5	*N* = 6	*N* = 7	*N* = 8	*N* = 9	*N* = 10	*N* = 11
	Время, затрачиваемое на извлечение признаков, в минутах							
	6	11	15	22	37	69	135	268
RAR/ZIP	0,840	0,864	0,864	0,863	0,868	0,977	**0,999**	**1,000**
Mean	0,929	0,939	0,941	0,940	0,962	**0,990**	**0,995**	**0,996**

Из анализа результатов, приведенных в таблице 1 можно сделать вывод о том, что КСЛ позволяет различать между собой алгоритмы DES и ZIP при $N = 4$ бита, при среднем значении точности равным 0,929. Но среднее значение точности более 0,990 достигается при $N >= 9$ бит.

Зависимость точности различения типов файлов от длины последовательности представлена на рисунке.

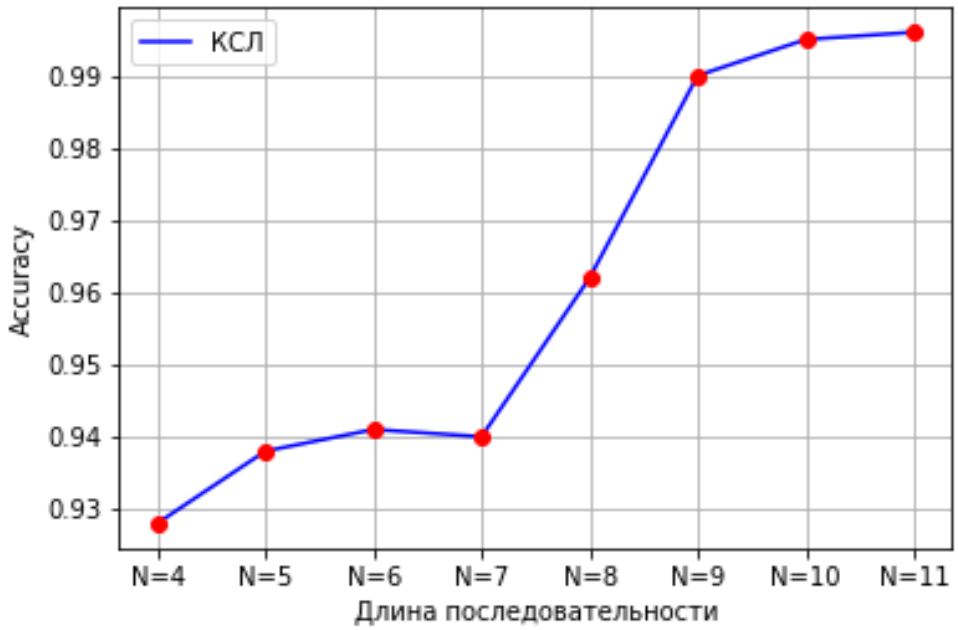


Рисунок. Зависимость точности различения типов файлов от длины последовательности

Для построения подсистемы обнаружения шифрованных файлов для DLP – систем целесообразно принять $N = 9$ бит, среднее значение точности в этом случае равно 0,99. Дальнейшее увеличение длины последовательности N не приводит к существенному увеличению точности, однако значительно увеличивает время, затрачиваемое на выделение признаков.

Таким образом, предложенное признаковое пространство может применятся для решения задачи различения шифрованных и сжатых файлов указанных в работе форматов.

Направлением дальнейших исследований является рассмотрение большего числа алгоритмов сжатия и шифрования, а также выбор и обоснование гиперпараметров классификатора.

Список используемых источников

1. Zhang, H., Papadopoulos, C., Massey, D. Detecting encrypted botnet traffic // 16th IEEE Global Internet Symposium. 2013. 3453 p.

2. Конышев М. Ю., Барабашов А. Ю., Петров К. Е., Двилянский А. А. Формирование распределений вероятностей двоичных векторов источника ошибок марковского дискретного канала связи с памятью с применением метода "группирования вероятностей" векторов ошибок // Промышленные АСУ и контроллеры. 2018. № 3. С. 42–52.

3. Toolkit for the transport layer security and secure sockets layer protocols. URL: http://openssl.org (дата обращения 14.01.2019).

4. Archive manager WinRAR. URL: http://rarlab.com (дата обращения 14.01.2019).

5. Archive manager 7-Z. URL: http://7-zip.org (дата обращения 14.01.2019).

6. Pedregosa F., et al. Scikit-learn: Machine Learning in Python // Journal of Machine Learning Research 12. 2011. Pp. 2825–2830.

7. Breiman, L., Friedman, J., Olshen, R., Stone, C. Classification and Regression Trees // Wadsworth, Belmont, CA. 1984. 368 p. ISBN 9781351460491.

8. Hastie, T., Tibshirani, R., Friedman, J. Elements of Statistical Learning // Springer. 2009. Pp. 587–601. ISBN 978-0387848570.

9. Breiman, L., Cutler, A. Random Forests // URL: https://www.stat.berkeley.edu/~breiman/RandomForests/cc_home.htm (дата обращения 14.01.2019).

10. Рашка С. Python и машинное обучение. М.: ДМК-Пресс. 2017. 418 с. ISBN 978-5-97060-409-0.

11. Breiman, L. Random Forests // Journal Machine Learning. 2001. 45(1). Pp. 5–32.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ СУЩЕСТВУЮЩЕГО ПОЛОЖЕНИЯ ДЕЛ В ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

А. В. Комарова[1], А. Г. Коробейников[2]

[1]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
[2]Санкт-Петербургский филиал ФГБУН Института земного магнетизма, ионосферы и распространения радиоволн им. Н. В. Пушкова РАН

В современном быстроразвивающемся технологическом мире появление квантового компьютера все больше становится реальностью. Появление такого устройства позволит обрабатывать данные на порядок быстрее, чем это делают современные ма-

шины. Для некоторых областей знаний это будет прорывом, но для современной криптографии - угрозой взлома всех существующих криптосистем. В данной статье проведен краткий анализ существующего положения дел в постквантовой криптографии.

квантовый компьютер, постквантовая криптография, изогения эллиптических кривых, теория алгебраического кодирования, теория решеток, эллиптическая кривая, криптосистема McEliec, криптосистема Niederreiter, Shortest Vector Problem, NP-полная задача, квантовая хэш-функция.

Введение

На сегодняшний день актуальной и прорывной темой исследований являются квантовые технологии. Не только в ведущих мировых научных изданиях, но и в средствах массовой информации все чаще появляются статьи, посвященные квантовым вычислениям и созданию квантового компьютера. Так, летом 2017 года группа российских и американских ученых Гарвардского университета под руководством Михаила Лукина смогла связать 51 квантовый кубит [1], а осенью того же года специалистами компании IBM под руководством Dario Jil был создан прототип 50 кубитного квантового процессора [2].

Напомним, что единицей квантовой информации является кубит, который может находиться в единицу времени в двух дискретных состояниях 0 и 1, а система из нескольких кубитов может быть в запутанном состоянии. В данном принципе квантовой суперпозиции (или квантового параллелизма) и заключается преимущество квантовых компьютеров даже над суперкомпьютерами.

По сравнению с классическим компьютером, возможность вычислений квантового компьютера растёт экспоненциально. Таким образом, квантовый компьютер из 50 кубит может за единицу времени выполнять 2^50 ≈ 10^15 шагов. Такой скорости выполнения вполне достаточно, чтобы очень быстро взломать большинство существующих криптоалгоритмов, схем и протоколов, основанных на классической и ассиметричной криптографиях, в том числе отечественные и зарубежные государственные стандарты. Вышеупомянутые ученые намерены реализовать алгоритм Шора [3] на созданных устройствах, тогда схемы, в основе которых лежат задачи факторизации и дискретного логарифмирования, не устоят.

Следует отметить, что Питер Шор предложил свой квантовый алгоритм 1994-м году, а до него, начиная с 1980-х годов, многие советские и иностранные учёные высказывали предположения о возможности реализации квантового компьютера. Мировое криптографическое сообщество быстро отреагировало на пусть даже гипотетическую возможность появления «квантового противника». Была создана новая область криптографии – постквантовая криптография, которая занимается созданием алгоритмов,

противостоящих квантовым вычислениям. Эта область основана на математических задачах, независимых от квантовых вычислений.

Как и в классических криптографических алгоритмах и схемах электронной подписи, трудность взлома которых основывается на сложности вычисления какой-либо «трудной» односторонней математической задачи (функции), в постквантовой криптографии стойкость заключается также в вычислении односторонней функции [4].

В 2016 году национальный институт стандартов и технологий США (NIST) объявил о старте конкурса заявок на создание постквантовых алгоритмов. В данный момент NIST занимается оценкой качества поданных заявок, которые поступают к нему от экспертов в области криптографии. В скором времени институт планирует опубликовать подборку лучших работ, чтобы потом применить их в качестве стандартов шифрования [5].

Постквантовая криптография на данный момент включает в себя следующие основные подходы: изогении эллиптических кривых, теория алгебраического кодирования, теория решеток. Рассмотрим немного подробнее каждый подход и трудные задачи, лежащие в их основе.

Изогении эллиптических кривых

Изогения – это рациональное отображение, переводящее точки одной эллиптической кривой в точки изогенной кривой, оставляя неподвижной бесконечно удаленную точку. Точки эллиптической кривой с абстрактной бесконечно удаленной точкой образуют абелеву группу, а сама бесконечно удаленная точка играет роль нейтрального элемента этой группы [4].

Пусть E_1 и E_2 эллиптические кривые над полем *F*. Изогенией $E_1 \rightarrow E_2$ называется рациональное отображение над *F*:

$$(x,y) \rightarrow \left(\frac{f1(x,y)}{f2(x,y)}, \frac{g1(x,y)}{g2(x,y)}\right)$$, где $f1$, $f2$, $g1$, $g2$ полиномы.

Трудная задача данного подхода заключается в поиске изогении для двух изогенных кривых E_1 и E_2 с разными j-инвариантами.

Основополагающими работами в области изогений эллиптических кривых можно считать [6, 7, 8].

Теория алгебраического кодирования (коды исправления ошибок)

На теории алгебраического кодирования базируются криптосистемы McEliece [9] и Niederreiter [10]. Алгоритмы основаны на сложности декодирования полных линейных кодов.

Общая задача декодирования является NP-сложной, то есть ее можно проверить при наличии некоторых дополнительных сведений (но невозможно быстро решить без наличия этих сведений) на машине Тьюринга за некоторое время, не превосходящее значения некоторого полинома от входных данных [11].

Криптография на решетках

Решетка – это совокупность точек в n-мерном пространстве с периодической структурой. Более точно решетку L можно определить как абелеву подгруппу, заданную в пространстве R^m. Базис решетки – множество линейно независимых векторов ее порождающих.

Пусть базис решетки B = $\{b_1,\ldots, b_n\}$ задан линейно независимыми векторами, тогда под решеткой будем понимать множество целочисленных линейных комбинаций этих векторов

$$\mathrm{L}(b_1,\ldots, b_n) = \{\sum_{j=1}^{n} a_j b_j : (a_1 \ldots a_n) \in Z^n\}.$$

К трудным задачам теории решеток относятся порядка 15 задач, однако самой интересной из них является задача поиска наикратчайшего вектора решетки (*Shortest Vector Problem*) [12], то есть по базису решетки необходимо, найти кратчайший ненулевой вектор. Данная задача является NP-полной задачей, то есть одной из самых сложных задач класса NP.

Квантовая хэш-функция

Данный подход относится к квантовой криптографии, а не к постквантовой, и основан на принципах квантовой физики, но заслуживает того, чтобы быть упомянутым.

В отличие от классического подхода, основанного на классических условно однонаправленных функциях, квантовая криптография при построении хеш-функций основывается на принципах квантовой механики и квантовой теории информации, гарантирующих физическую однонаправленность квантовых хеш-функций [12].

В работах [13, 14] предложены интересные подходы к выполнению квантового хэширования, а в работах [15, 16] предложены схемы электронной подписи на основе квантовых хэш-функций.

Результаты

Актуальность и новизна данного направления исследований не вызывает сомнений, однако вызывают вопросы практическая реализация и применение данных задач в реальных протоколах безопасности.

Постквантовые схемы защиты на коммерческом уровне стали использоваться не так давно, в связи с чем, отсутствуют точные данные о некоторых параметрах схем, вычислительной сложности, длине ключей и т. д. Совсем скоро NIST должен объявить результаты конкурса заявок, но при возможном переходе на постквантовые схемы организациям (банкам, госструктурам, электронным площадкам и т. д.) придется полностью менять всю систему защиты. Для устранения данной проблемы предлагается добавить, так называемый, постквантовый элемент в уже существующие системы. Например, при формировании электронной подписи использовать квантовую хэш-функцию, или создать дополнительный канал связи для распределения ключей с использованием изогений. Таким образом, злоумышленнику сначала придется справиться с постквантовой трудной задачей.

В направлении создания полноценных стойких к квантовым вычислениям схем шифрования, электронной подписи, неоспоримой подписи, коллективной подписи, подписи вслепую, доказательства с нулевым разглашением интересной разработкой будут являться, так называемые, гибридные системы [17]. Такого рода системы предполагают двойную защиту: помимо стандартного ключа шифрования, который повсеместно применяется в современных криптосистемах, предусматривается постквантовая схема защиты.

Выводы

В данное время группа учёных занимается вопросом создания эффективного и стойкого постквантового алгоритма шифрования и протокола электронной подписи, а также квантового распределения ключей, и стандартизации этих алгоритмов для внедрения их в государственные и коммерческие организации, так чтобы это не повлекло за собой огромных финансовых потерь.

Дальнейшие исследования необходимо продолжать в сфере создания алгоритмов и протоколов, основанных одновременно на нескольких трудно вычислительных задачах, одна из которых принадлежит к постквантовой криптографии, а другая – к ассиметричной криптографии.

Список используемых источников

1. 51-кубитный квантовый компьютер Михаила Лукина бьет все рекорды [Электронный ресурс]. URL: https://www.kommersant.ru/doc/3368646. Загл. с экрана. (дата обращения 22.01.2019).

2. Компанией IBM создан самый мощный квантовый компьютер [Электронный ресурс]. Режим доступа: http://news-important.ru/kompaniej-ibm-sozdan-samyj-moshhnyj-kvantovyj-kompyuter. Загл. с экрана. (дата обращения 22.01.2019).

3. Shor, P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Foundations of Computer Science, 1994 // Proceedings., 35th Annual Symposium on IEEE, 1994. Pp. 124–134. ISBN 0-8186-6580-7. doi:10.1109/SFCS.1994.365700.

4. Коробейников А. Г. Математические основы криптографии. Учебное пособие. СПб.: СПб ГИТМО (ТУ), 2002. 41 с.

5. Постквантовая безопасность: время пришло? [Электронный ресурс]. URL: https://www.itweek.ru/security/article/detail.php?ID=202851. – Загл. с экрана. – (дата обращения 22.01.2019).

6. Jao, David and De Feo, Luca. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, PQCrypto, vol. 7071 of Lecture Notes in Computer Science. Pp. 19–34. Springer, 2011.

7. Childs, Andrew, Jao, David, and Soukharev, Vladimir. Constructing elliptic curve isogenies in quantum subexponential time. J. Math. Cryptol, 8(1):1–29, 2014.

8. Sun, Xi, Tian, Haibo, and Wang, Yumin. Toward quantum-resistant strong designated verifier signature from isogenies // In 4th International Conference on Intelligent Networking and Collaborative Systems (INCoS). 2012. Pp. 292–296,

9. McElice, R. J. A Public Key Cryptosystem Based on Algebraic Coding Theory // DSN Progress Report 42–44. Pasadena, CA: Jet Propulsion Lab, 1978. Pp. 114–116.

10. Niederreiter, H. Knapsack-Type Cryptosystem and Algebraic Coding Theory // Probl. Control and Inform. Theory. 1986. V. 15. Pp. 19–34.

11. Коробейников А. Г, Гатчин Ю. А. Математические основы криптологии. Учебное пособие. СПб.: СПб ГУ ИТМО, 2004. 106 с, илл.

12. Комарова А. В., Коробейников А. Г. Применение теории решеток в схемах электронной цифровой подписи // Инженерные кадры – будущее инновационной экономики России: материалы Всероссийской студенческой конференции: в 8 частях. 2015. Т. 4. С. 72–76.

13. Ablayev, F., Ablayev, M., Quantum Hashing via Classical e-universal Hashing Constructions. arXiv:1404.1503v2 [quant-ph]. URL: http://arxiv.org/abs/1404.1503.

14. Ablayev, F., Vasiliev, A. Quantum Hashing, arXiv:1310.4922vl [quant-ph]. URL: http://arxiv.org/abs/1310.4922.

15. Gottesman, Daniel and Chuang, Isaac. Quantum digital signatures. Technical Report arXiv:quant-ph/0105032, Cornell University Library. Nov. 2001.

16. Lu, Xin and Feng, Dengguo. Quantum digital signature based on quantum one way functions // In The 7th International Conference on Advanced Communication Technology. 2005. ICACT 2005. Vol. 1. Pp. 514–517.

17. Комарова А. В., Коробейников А. Г., Менщиков А. А., Кляус Т. К., Негольс А. В., Сергеева А. А. Теоретические возможности комбинирования различных математических примитивов в схеме электронной цифровой подписи // Кибернетика и программирование. 2017. № 3. С. 80–92.

УДК 004.01
ГРНТИ 81.93.29

О ПРОБЛЕМЕ СТАНДАРТИЗАЦИИ В ОБЛАСТИ ИНТЕРНЕТА ВЕЩЕЙ

А. Г. Коробейников[1,2], А. М. Полегенько[2]

[1]Санкт-Петербургский филиал ФГБУН Института земного магнетизма, ионосферы и распространения радиоволн им. Н. В. Пушкова РАН
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Сегодня нас окружает все большее количество «умных» гаджетов, способных обмениваться друг с другом данными с участием пользователя или без него. Учитывая особенности устройств, входящих в сеть Интернета вещей, а также их различную природу, вопросы безопасности сетевого взаимодействия требуют рассмотрения новых аспектов. Ключевую роль в развитии технологий безопасного взаимодействия «умных» гаджетов играет разработка единых стандартов в данной области.

Интернет вещей, информационная безопасность, стандартизация, безопасность сетевого взаимодействия.

Концепция Интернета вещей – активно развивающееся направление сегодня во всех странах, однако отставание российского рынка в этой области пока остается заметным. Долгое время «умные вещи» были дорогостоящими и, соответственно, мало распространёнными. Последние несколько лет наблюдается тенденция развития доступных устройств, способных посредством объединения в сеть, обмениваться друг с другом информацией с участием пользователя или без него. И, если цены на устройства, которые являлись одним из сдерживающих факторов развития Интернета вещей, существенно снижаются, и устройства становятся более доступными, то попрежнему остаётся актуальной другая проблема – отсутствие стандартизации в этой области.

Проблема отсутствия стандартов замедляет общее развитие концепции Интернета вещей как таковой. Это объясняется тем, что в условиях отсутствия стандартов каждая компания вынуждена тратить деньги на проработку одного и того же, и в итоге суммарный эффект в продвижении отрасли получается небольшим. Наличие стандартов позволяет усовершенствовать или использовать иначе то, что уже существует. Кроме этого, конечно же, наличие стандартов позволяет объединять в сеть устройства различных типов и видов, вне зависимости от производителя или форм-фактора.

Можно говорить о том, что все развитые страны участвуют во внедрении протоколов и стандартов Интернета вещей.

Привычной является практика объединения крупных компаний в ассоциации и альянсы, которые призваны решать, в том числе, и проблемы стандартизации.

В настоящие консорциумы входят крупные компании из сферы коммуникаций, разработки программного обеспечения, а также активно включаются компании, представляющие потребительский сектор. Такие компании, в первую очередь, привлекаются в качестве участников испытаний практической применимости разрабатываемых стандартов.

IETF (*Internet Engineering Task Force*) – открытое международное сообщество проектировщиков, учёных, сетевых операторов и провайдеров, которое уже больше десятилетия работает над выработкой спецификаций и документированием ключевых стандартов и рекомендаций в области Интернета вещей. Различные рабочие группы IETF занимаются вопросами адаптации и применимости существующих стандартов и протоколов в специфичных сетях «умных устройств», которые имеют свои ограничения. В последние несколько лет стали создаваться рабочие группы, направленные на проработку, в том числе, и стандартов безопасности в Интернете вещей [1, 2].

В начале 2018 года Американский Национальный институт стандартов и технологий (NIST) представил проект документа «Статус международной стандартизации кибербезопасности Интернета вещей» («*The Status of International Cybersecurity Standardization for IoT*»), призванный помочь разработать международные стандарты безопасности для Интернета вещей. В рамках данного стандарта NIST предлагает разделить устройства Интернета вещей на пять функциональных областей: подключенные устройства, устройства потребительского класса, медицинское оборудование и устройства, используемые в сфере здравоохранения, умные здания, умное производство (в том числе, АСУ ТП) [3].

Исходя из того, что устройства из разных функциональных областей имеют свои особенности и призваны решать разные задачи, стандарты должны быть приняты для каждой из областей. Такой подход имеет ряд недостатков: во-первых – это время, требуемое на разработку, испытания и принятия каждого из стандартов в отдельной функциональной области. Кроме того, подход к стандартизации для разных функциональных областей не решает задачу полной унификации разрабатываемых решений для устройств Интернета вещей.

Возможно, упростить задачу стандартизации можно, используя подход к разделению устройств по ключевым свойствам безопасности, которые должны обеспечивать те или иные устройства.

Известно, что ключевыми свойствами безопасности являются конфиденциальность, целостность и доступность [4]. При этом в Интернете вещей приоритетным, как правило, является обеспечение доступности. Безусловно, можно выделить и класс устройств, для которых на первом месте с точки зрения приоритетов будет находиться конфиденциальность. Однако обеспечение стандартизации по приоритетному свойству безопасности можно предусмотреть на более высоком уровне модели взаимодействия, обеспечив унифицированную стандартизацию на более низких уровнях, таких как, например, физическом, канальном и транспортном.

Такой подход позволил бы принять унифицированный стандарт, регламентирующий разработку устройств Интернета вещей по общепринятым протоколам, адаптированным для данных устройств, а вопросы безопасности решались бы на прикладном уровне, являясь надстройкой в зависимости от назначения устройств.

В России ТК 194 «Кибер-физические системы» (Технический комитет «Кибер-физические системы») является ключевым участником реализации мероприятий в планах по направлению «Нормативное регулирование» программы «Цифровая экономика Российской Федерации» по разработке проектов национальных стандартов в области технологий «Большие данные», «Интернет вещей» и «Промышленный (индустриальный) интернет вещей», «Искусственный интеллект». На сегодняшний день ТК 194 уже разработал стандарт терминологии в сфере Интернета вещей, внедрение которого планируется синхронно с англоязычной версией. Ожидается, что внедрение данного стандарта позволит облегчить коммуникации между заказчиками, исполнителями и потребителями на рынке «интернета вещей», уменьшит вероятность ошибок при составлении технических заданий, проектировании систем и приемке работ.

Также ТК 194 представил проект международного стандарта в области промышленного Интернета вещей (IIoT), который направлен в адрес Международной организации по стандартизации ISO/IEC от имени Российской Федерации для международного голосования. Документ устанавливает единые требования к совместимости различных устройств и систем промышленного Интернета вещей. Принятие стандарта позволит заказчикам технологии IIoT использовать решения и оборудование от различных разработчиков и предприятий-изготовителей, а также проводить корректные испытания решений и оборудования на совместимость [5].

Таким образом, в связи с повсеместным развитием Интернет- технологий и устройств сети Интернета вещей, одной из актуальных проблем становится стандартизация в этой области. Участие стран в разработке, принятии и внедрении стандартов повышает конкурентоспособность и открывает возможности на мировом рынке. Несмотря на то, что развитие Интернета

вещей в России в заметной степени отстает от уровня ведущих стран, на сегодняшний день комитеты по стандартизации в нашей стране ведут активную деятельность и участвуют в реализации проектов на мировом уровне.

Принимаемые стандарты подлежат публичному обсуждению, а также обязательной апробации в условиях функционирующих сетей. Стандартизация является ключевым фактором обеспечения унификации разрабатываемых устройств и поддерживающих их приложений, поэтому принимаемый стандарт должен охватывать как можно больше типов устройств, исключая необходимость принятия огромного количества смежных стандартов.

Список используемых источников

1. Астахов Максим Игоревич. Интернет вещей: роль стандартов [Электронный ресурс] // Техноспецназ, 2017, февраль. URL: техноспецназ.рф/2017/02/28/internet-veshhej-rol-standartov/ (дата обращения 02.12.2018)

2. Бондаренко И. Б., Коробейников А. Г., Прохожев Н. Н., Михайличенко О. В. Принятие технических решений с помощью многоагентных систем // Кибернетика и программирование. 2013. № 1. С. 16–20. DOI: 10.7256/2306-4196.2013.1.8305. URL: http://e-notabene.ru/kp/article_8305.html (дата обращения 17.01.2019)

3. Техника и технологии: [Электронный ресурс] // pro-iot.pro. URL: http://pro-iot.pro/materials/tekhnika-i-tekhnologii/news/nist-predlozhil-printsipy-mezhdunarodnoy-standartizatsii-v-iot-/ (дата обращения 04.12.2018).

4. Коробейников А. Г, Гатчин Ю. А. Математические основы криптологии: учебное пособие. СПб.: СПб ГУ ИТМО, 2004. 106 с, илл.

5. ТК 194 «Кибер-физические системы» [Электронный ресурс]. URL: http://tc194.ru/ (дата обращения 11.12.2018).

УДК 004.7:004.422.8
ГРНТИ 20.01.07

ФОРМИРОВАНИЕ РАСШИРЕННЫХ ОБЪЕКТНО-ОРИЕНТИРОВАННЫХ МОДЕЛЕЙ ПЛАНИРОВЩИКОВ ДЕЙСТВИЙ ИНФОРМАЦИОННЫХ МУЛЬТИАГЕНТНЫХ СИСТЕМ

М. С. Коткина, Л. К. Птицына

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Описаны архитектурные особенности информационных мультиагентных систем. Обоснована актуальность сравнительного анализа планировщиков действий ин-

формационных мультиагентных систем. Представлено современное состояние исследований планировщиков. Поставлена задача расширения знаний о динамических свойствах планировщиков. Предложена методика формирования расширенных объектно-ориентированных моделей планировщиков действий информационных мультиагентных систем. Определена область использования формируемых моделей.

архитектура, мультиагентная система, планировщик действий, динамические свойства, объектно-ориентированные модели.

Современные информационные мультиагентные системы являются одним из приоритетных направлений развития научно-технологических воплощений рационального подхода к созданию искусственного интеллекта, представленного в [1]. Развитие информационных мультиагентных систем обуславливается повышением степени распространённости гетерогенных сетей, в средах которых осуществляется профессиональная, социальная и досуговая деятельность. К основным свойствам мультиагентных систем относятся реактивность, активность, коммуникативность, автономность, рассудительность и обучаемость.

При организации взаимодействия мультиагентных систем с информационными ресурсами решаются типичные задачи, связанные с извлечением информации в ответ на однократные и периодические запросы, мониторингом информационных источников, планированием запросов, диспетчеризацией запросов.

Среди информационных мультиагентных систем выделяются базовые, которые отвечают за взаимодействие с определёнными информационными источниками, и диспетчерские, которые обеспечивают планирование и диспетчеризацию запросов к различным информационным источникам, необходимым для достижения поставленной цели. Для решения задач унифицированного сбора и обработки информации в гетерогенных сетях важнейшей группой функций мультиагентных систем является организация взаимодействия с субагентами. К указанной группе относятся как функции обеспечения обмена информацией или совместного решения задач с другими агентами, которые автономны, обладают гибкой логикой работы и поддерживают высокоуровневое взаимодействие, так и функции обеспечения обмена информацией с различными неинтеллектуальными информационными источниками, которые, как правило, пассивны и имеют жесткую логику работы.

Достижимость цели информационными мультиагентными системами обеспечивается подсистемами планирования их действий, эффективные алгоритмы которых представляются в [2, 3, 4].

Среди известных реализаций мультиагентных систем выделяются три разновидности поведения в гетерогенных сетях: реактивная, проактивная и гибридная. Реактивная модель поведения ориентируется на выполнение

предопределенного набора действий в зависимости от текущего состояния среды. В случае проактивной модели поведения генерация и исполнение плана действий осуществляются на основе имеющихся в распоряжении агентов знаний и поставленной цели. Ведущими факторами, влияющими на функциональность проактивных систем, являются качество модели среды, корректность выбора целей и способность генерировать и исполнять план действий, обеспечивающий достижение поставленной или выбранной цели. При гибридной модели субагенты системы в разные моменты времени демонстрируют как реактивное, так и проактивное поведение. Адекватное использование теории планирования действий агентов повышает эффективность работы мультиагентных систем и существенно расширяет круг решаемых ими задач.

Информационные мультиагентные системы, функционирующие в гетерогенных средах большой размерности и требующие генерации сложных планов действий, характеризуются следующими особенностями:

- организация и использование агентами централизованной универсальной системы выбора алгоритма планирования;
- обеспечение относительной простоты реализации за счет исключения множественных копий системы выбора алгоритма планирования;
- предоставление агентами системе выбора информации о среде, о задаче планирования и возможных вариантах предпочтения;
- обеспечение высокой надежности коммуникаций между агентами и системой выбора алгоритма планирования;
- активизация алгоритма планирования по умолчанию в случае недоступности системы выбора.

Реализации представленных архитектурных особенностей информационных мультиагентных систем нуждаются в формализациях выбора алгоритма планирования. Представленные в [2, 3, 4] исследования известных алгоритмов планирования действий агентов опираются на теоретические разработки и результаты экспериментальных исследований. При этом важнейшие временные профили алгоритмов планирования действий агентов ограничиваются либо предельными оценками, либо экспериментальными оценками, уточняемыми в процессе функционирования действующих систем.

В представленных условиях появляется объективная необходимость разработки новых формализаций, ориентированных на аналитическое определение и оценивание временных профилей алгоритмов планирования действий агентов и мультиагентной системы в целом.

В связи с этим ставится новая научно-техническая задача расширения знаний о динамических свойствах планировщиков действий за счёт разработки методики формирования расширенных объектно- ориентированных

моделей планировщиков действий мультиагентных систем, предусматривающих их последующий анализ с целью аналитического определения и оценивания временных показателей качества.

Современные системы планирования в большинстве своём опираются на алгоритм планирования действий SNLP, характеризующийся системностью, полнотой и корректностью. По этой причине предлагаемая методика раскрывается на примере построения расширенной объектно-ориентированной модели планировщика действий на основе алгоритма SNLP.

Методикой формирования расширенной объектно-ориентированной модели планировщика действий предусматривается выполнение следующих этапов:

1. Определение класса диаграмм деятельности.
2. Представление состава ресурсов информации.
3. Описание видов и статических характеристик действий.
4. Перечисление отношений предшествования для самих действий и их стохастических свойств.
5. Определение специфики сонаправленных действий и вероятностей их выполнения.

Алгоритм SNLP используется при имеющимся наборе целевых предусловий A для обнаружения плана P (рис.).

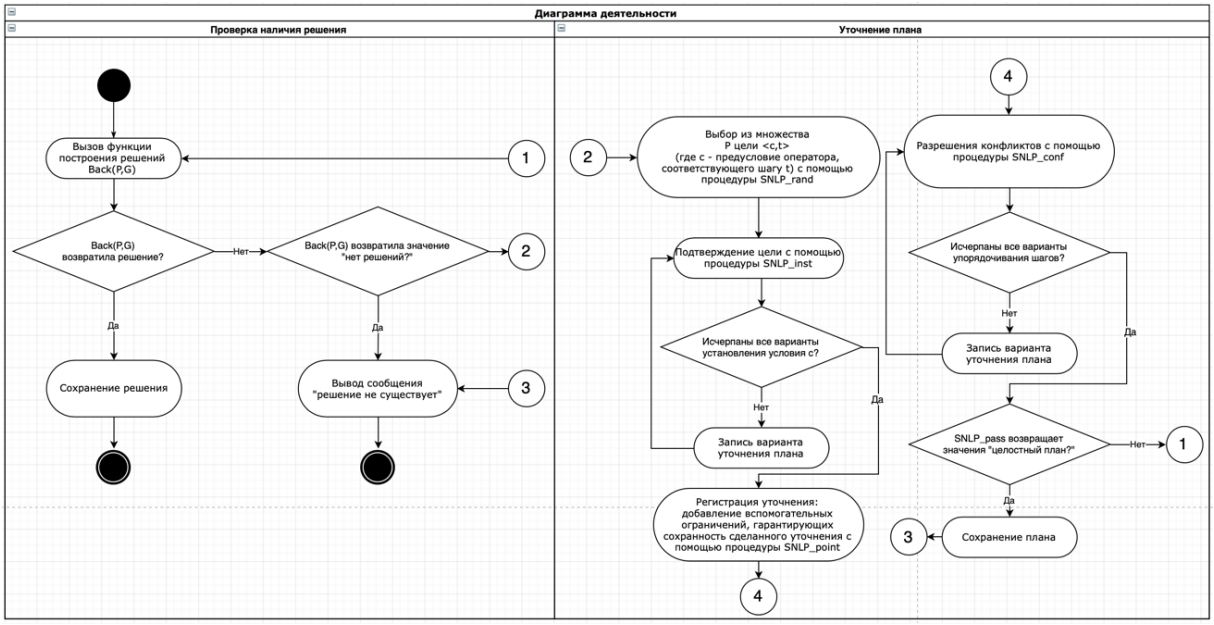


Рисунок. Объектно-ориентированная модель алгоритма SNLP

Функцией SNLP_back(P,G) предусматривается выполнение следующих рассматриваемых действий. В случае, когда множество A пусто, происходит возврат решения. В противном случае происходит возврат значения

«продолжить», но только в случае, если плановая длина не превысила установленное ограничение. В случае, когда множество A не является пустым, но длина плана превысила установленное ограничение, происходит возврат значения «нет решений».

Процедура SNLP_rand позволяет осуществить случайный выбор цели среди целевых предусловий A <c,t> (где c – предусловие оператора, которое соответствует шагу t). При этом возможно исключение цели <c,t> из множества A (A = A – <c,t>).

В процедуре SNLP_inst осуществляется выбор уже существующего шага или выбор нового шага t'для цели (<c,t>). В результате выбранного шага устанавливается условие «c» для шага «t» (в случае если шаг t' отсутствует, как и возможность его добавления, происходит возврат к предшествующей точке).

В процедуре SNLP_point добавляются ограничения, которые являются вспомогательными и гарантирующими то, что выполненное уточнение плана, реализованное при помощи защитной стратегии уточнений, обеспечивающей поиск систематикой, будет сохранено.

Процедура SNLP_conf используется для определения и устранения конфликтов. Каждый из конфликтов подвергается двум уточнениям плана с помощью ограничений.

С помощью функции SNLP_pass выполняются следующие рассматриваемые действия. В случае, когда план не обладает целостностью, происходит возврат значения «нецелостный план», в противном случае возвращается значение «целостный план». В качестве нарушений целостности плана выступают: 1) присутствие циклов в очереди следования операторов, 2) присутствие совместной и несовместной инициализации для двух переменных единовременно.

В ходе планирования реализуется выбор альтернативных вариантов выполнения действий. Для описания возможностей выбора определяется количество узлов решения, номер каждого узла решения, количество вариантов альтернативного выполнения действий после каждого решения и вероятности ветвлений, удовлетворяющих условию полной группы несовместных событий:

$$\sum_{\mathrm{a}=1}^{A_n} p_{n,\mathrm{a}} = 1, \qquad n = 1, 2, \dots, N,$$

где n – номер узла решения,

A_n – количество альтернативных вариантов поведения после решения n,

N – количество узлов решения. В исследуемом случае N=5.

При расширении объектно-ориентированной модели планировщика действий определяются статистические свойства выполняемых действий в виде плотностей распределений вероятностей дискретного времени k_i их реализации $f_i(k_i),\ i = 1, 2, \dots, I$, удовлетворяющих следующему условию

$$\sum_1^{K_i} f_i(k_i) = 1,\ k_i = 1, 2, \dots, K_i,\ i = 1, 2, \dots, I.$$

Для приведенной реализации планировщика i = 15.

Предлагаемая методика формирования расширенных объектно-ориентированных моделей планировщиков действий информационных мультиагентных систем обеспечивает сквозное связывание с методикой анализа, ориентированной на аналитическое определение и оценивание показателей качества их функционирования. Подобное связывание и последующий анализ позволяет решать задачи управления качеством мультиагентных систем по различным профилям как системного, так и прикладного назначения.

Список используемых источников

1. Рассел С., Норвиг П. Искусственный интеллект. Современный подход. 2 изд. М.: Вильямс, 2007. 1408 с.

2. Птицына Л. К., Добрецов С. В. Интеллектуальные технологии и представление знаний. Планирование действий интеллектуальных агентов в информационных сетях: учеб. пособие. СПб. : Изд-во Политехн. ун-та, 2006. 172 с.

3. Птицына Л. К., Шестаков С. М. Информационные сети. Интеллектуальные информационные агенты: учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2008. 210 с.

4. Осипов Г. С. Методы искусственного интеллекта. 2 изд. М.: Физматлит, 2015. 295 с.

УДК 004.056
ГРНТИ 20.53.19

ДИАГНОСТИКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ВЕБ-ПОРТАЛОВ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Д. В. Кривко, Д. А. Свечников, О. А. Степина

Академия Федеральной службы охраны Российской Федерации

В статье представлены основные положения определяющие методы диагностики защищенности информационных ресурсов веб-порталов государственных информационных систем. Описаны основные направления проведения исследований и способы их реализации. Обоснованы методы черного и белого ящика. Предложены способы их применения для выявления уязвимостей компонентов веб-порталов.

информационная система, информационный ресурс, веб-портал, диагностика защищенности

Возрастающая потребность в применении веб-технологий при построении информационных систем обусловливают необходимость решения вопросов обеспечения их информационной безопасности [1]. Несмотря на явные преимущества веб-приложений, наличие в них уязвимостей является одним из наиболее распространенных путей проникновения в защищаемые информационные системы. Это подтверждается исследованиями, которые ежегодно проводятся экспертами компании Positive Technologies и др.

При этом, необходимо отметить, что в области обеспечения ИБ веб-приложений в настоящее время существует большое количество проектов и решений, например, Open Web Application Security Project (OWASP) и др. Однако они характеризуются тем, что являются англоязычными, содержат большое количество разрозненных данных и касаются приложений, функционирующих, как правило, в открытых системах и сетях и не учитывают требования национальных руководящих документов.

Данные обстоятельства подчеркивают необходимость разработки методов диагностики защищенности информационных ресурсов веб-порталов государственных информационных систем, учитывающих требования руководящих документов России [2, 3, 4]:

– выявление (поиск) дефектов безопасности программного обеспечения (*Common Weakness Enumeration*, CWE) на этапах его разработки и обновления (инспекционный контроль). Дефекты безопасности ПО – дефекты,

сбои, ошибки, уязвимости и прочие проблемы реализации кода, проектирования или архитектуры ПО, которые могут сделать веб-портал уязвимым к атакам злоумышленников;

– выявление (поиск) уязвимостей программного обеспечения (*Common Vulnerabilities and Exposures*, CVE), общесистемного, веб-сервера, прикладного, средств защиты информации. Уязвимости – ошибки программы, которые могут быть непосредственно использованы злоумышленником;

– выявление (поиск) неразрешенного ПО (компонентов ПО);

– выявление уязвимостей "нулевого дня", о которых стало известно, но информация о которых еще не включена в сканеры уязвимостей;

– выявление новых уязвимостей, информация о которых еще не опубликована в общедоступных источниках;

– проверку правильности установки и настройки средств защиты информации, технических средств и ПО;

– проверку корректности работы средств защиты информации при их взаимодействии с техническими средствами и ПО;

– проверку своевременности обновлений ПО средств защиты информации, общесистемного и прикладного ПО;

– выявление (поиск) уязвимостей в информационной системе с использованием учетных записей на сканируемых ресурсах;

– тестирование защищенности информационной системы от несанкционированного доступа (НСД).

Диагностика защищенности информационных ресурсов предполагает проведение тестов веб-портала и его компонентов для выявления уязвимостей, которые могут быть использованы злоумышленником для реализации угроз ИБ. Существуют следующие основные методы диагностики защищенности [5]:

– выявление уязвимостей ПО;

– тестирование защищенности веб-портала от НСД (*Penetration Testing*).

Выявление уязвимостей ПО осуществляется в сетевых службах; веб-приложениях.

Уязвимости ПО могут быть диагностированы следующими способами:

– идентификацией версии ПО веб-портала и поиском в базах данных уязвимостей (CWE, CVE и др.);

– запуском программ-тестов (эксплойтов), воспроизводящих в полном объеме или частично выполнение компьютерных атак с использованием уязвимостей.

В зависимости от начальных условий для выявления уязвимостей могут использоваться методы черного ящика и белого ящика.

При применении метода черного ящика исследователю предоставляется доступ к составным частям веб-портала на уровне протокола IP. Предметом исследования являются уязвимости сетевых служб компонентов веб-портала.

При использовании метода белого ящика исследователю предоставляется доступ к операционным системам, телекоммуникационному оборудованию, СУБД и серверам приложений с необходимыми правами доступа. Предметом исследования являются уязвимости программных компонент веб-портала, сведения о которых содержатся в используемой базе данных уязвимостей.

Степень важности выявленных уязвимостей целесообразно определять в соответствии с международной методикой Common Vulnerability Scoring System (CVSS).

Поиск уязвимостей в сетевых службах производится посредством метода черного ящика. Исследование включает:

– идентификацию серверов и рабочих мест по их IP-адресам или именам;

– идентификацию сетевых протоколов, доступных для взаимодействия;

– идентификацию программ, обеспечивающих реализацию указанных сетевых протоколов, с определением их наименований и версий по информации, передаваемой при сетевом взаимодействии;

– поиск идентифицированных уязвимостей в базах данных;

– поиск уязвимостей сетевых служб путем запуска соответствующих им эксплойтов.

Поиск уязвимостей в веб-приложениях осуществляется с помощью метода черного ящика. Определяется уязвимость веб-портала к атакам следующих типов:

– различные виды инъекций: SQL, LDAP, XPath и др.;

– подбор данных аутентификации;

– незащищенная передача данных;

– ошибки при разграничении доступа;

– межсайтовый скриптинг (XSS);

– подделка межсайтовых запросов (CSRF);

– расщепление и перенаправление запроса HTTP;

– идентификация приложений;

– чтение данных;

– переполнение буфера.

Диагностика выполняется путем анализа данных, передаваемых между клиентом и веб-порталом при выполнении тестовых запросов.

Выявление уязвимостей ПО выполняется с использованием метода белого ящика и включает:

– инвентаризацию установленного ПО, идентификацию наименований и версий программ, а также установленных обновлений безопасности;

– поиск уязвимостей в специальных базах данных.

Выявление учетных записей с известными паролями, проводится с использованием методов черного и белого ящика. В методе черного ящика реализуются попытки аутентификации с использованием имен и паролей из специального словаря. В методе белого ящика производится выборка хеш-значений паролей из конфигурационных файлов, таблиц баз данных и сравнение их с хеш-значениями паролей из используемого словаря.

По результатам исследований уязвимостей ПО оформляется отчет, включающий:

– обследованные компоненты веб-портала;

– выявленные уязвимости, оценку степени их критичности для обеспечения ИБ;

– рекомендации по устранению уязвимостей.

Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной системы.

Периодичность проведения диагностики на предмет выявления уязвимостей, информация о которых еще не опубликована в общедоступных источниках, устанавливается заказчиком.

В случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в информационной системе, поиск и анализ уязвимостей осуществляется немедленно.

Контроль проведения диагностики проводится с периодичностью, установленной заказчиком в организационно-распорядительных документах по защите информации и фиксируется в соответствующих журналах.

Разработанные предложения по проведению диагностики защищенности информационных ресурсов веб-порталов позволят комплексно оценить безопасность государственных информационных систем, построенных на основе веб-технологий.

Список используемых источников

1. Свечников Д. А. и др. Предложения по построению комплексной методики анализа защищенности информационных ресурсов веб-порталов [Электронный ресурс] // Информационная безопасность и защита персональных данных. Проблемы и пути их решения : материалы X межрегион. науч. практ. конф., Брянск, 30 апр. 2018 г. Брянск: БГТУ, 2018. С. 157–160. URL: http://mn.tu-bryansk.ru/files/IB2018.pdf (дата обращения 22.01.2019).

2. Приказ ФСТЭК России от 11.2.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3. Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России от 11.02.2014 г.).

4. Изменения, которые вносятся в «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 (утв. ФСТЭК России от 15.2 2017 г. № 27).

5. Рекомендации в области стандартизации Банка России. РС БР ИББС-2.6-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации : ввод в действие с 01.09.14. М.: Банк России, 2014. 34 с.

УДК 004.047
ГРНТИ 50.43.19

МОДЕЛЬ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННЫХ ВОЗДЕЙСТВИЙ И АЛГОРИТМЫ ИХ ОБНАРУЖЕНИЯ

И. В. Кубасов, А. С. Мамончикова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрены предпосылки для моделирования системы защиты информации в автоматизированной системе управления связью. Представлены все направления коррекции целей защиты информации на множестве конкурирующих структур. Показан алгоритм функционирования системы защиты информации (СЗИ) АСУ связью, повышающий ее устойчивость в условиях несанкционированных воздействий.

автоматизированная система управления связью, несанкционированные воздействия, система защиты информации, информационные потоки, коррекция параметров модели, алгоритмы обнаружения.

Информационный конфликт как форма взаимодействия информационных систем характеризуется преднамеренным характером воздействий нарушителя. При этом его объектами становятся как информация, хранимая, обрабатываемая и передаваемая в интересах решения прикладных задач пользователей, так и сами информационно-вычислительные сети, т. е. все доступные для воздействия ее ресурсы [1].

В зависимости от стадии информационного конфликта можно выделить следующие классы программных воздействий: компьютерная разведка, преодоление СЗИ, НСД или программное подавление.

Под компьютерной разведкой будем понимать программное воздействие, реализующее процесс сбора и анализа данных о комплексе средств обработки и СЗИ сети.

Под преодолением СЗИ будем понимать программное воздействие, осуществляющее компрометацию или изменение параметров СЗИ, обеспечивающих эффективность защиты от НСД.

Под НСД будем понимать программное воздействие, непосредственно реализующее одну из угроз нарушения безопасности информации, направленное на проникновение в сеть с последующей реализацией какого- либо несанкционированного воздействия.

Под программным подавлением будем понимать вид несанкционированного воздействия, направленный на снижение эффективности или нарушение работоспособности средств обработки или защиты информации от НСД [2].

Таким образом, первой стадией в информационном противоборстве является компьютерная разведка.

Компьютерная разведка, по сути, это деятельность, направленная на получение информации из электронных баз данных ЭВМ, включенных в компьютерные сети открытого типа, а также информации об особенностях их построения и функционирования.

Целью компьютерной разведки является добывание сведений о предмете, конечных результатах, формах и способах деятельности субъектов, являющихся пользователями информационно-вычислительной сети, и используемом аппаратурном и программном обеспечении, протоколах управления и информационного взаимодействия, используемых средствах и методах защиты информации.

Компьютерная разведка – это новый вид технической разведки. Ее появление связано с развитием концепции информационной войны.

Важнейшая роль в достижении информационного господства отводится виртуальной разведке – разведке, ведущейся в информационных потоках, которые в гигантских количествах производятся всеми государственными и частными организациями, а также отдельными индивидуумами. Она включает в себя три основных направления: разведку в информационно-вычислительных компьютерных сетях, разведку в бумажных и электронных средствах массовой информации, разведку в непериодических изданиях, в том числе, в открытых и так называемых «серых» (т. е. не имеющих грифа секретности, но не предназначенных для массового распространения – отчетах о НИР, аналитических справках, деловой переписке, диссертациях и т. п.).

Виртуальная разведка представляет собой целый комплекс взаимосвязанных действий оперативного и технического характера. Важнейшей тех-

нической компонентой виртуальной разведки является компьютерная разведка (рис.) – целенаправленная деятельность по добыванию с помощью средств вычислительной техники и программного обеспечения информации, обрабатываемой в информационно-вычислительных, сетях и/или отдельных средствах вычислительной техники.

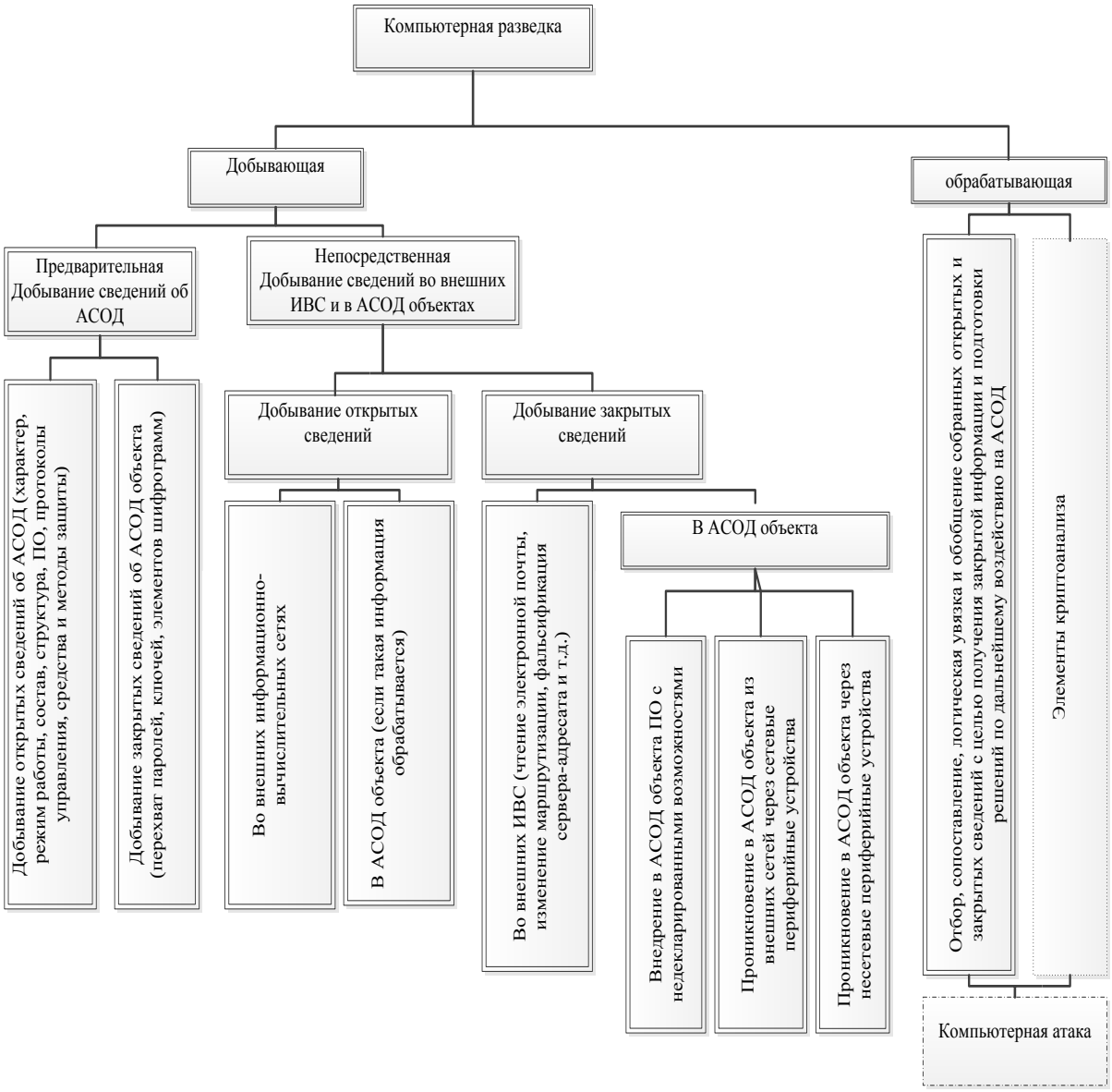


Рисунок. Компьютерная разведка

Изучение информации приводит к формированию знаний (следующий уровень осведомленности), а знания посредством суждения способствуют пониманию (верхний уровень). Задача добывающей разведки состоит в получении данных, а обрабатывающей - в преобразовании данных в информацию и приведение ее в форму, удобную для пользователя.

Добывающая разведка бывает предварительной и непосредственной. Задача предварительной разведки – получение сведений о самой автоматизированной системе обмена данными (АСОД). Цель предварительной разведки – подобрать данные, необходимые для последующего проникновения в АСОД.

Цели предварительной разведки достигаются путем добывания открытых и закрытых сведений. К открытым сведениям можно отнести данные о характере и режиме работы АСОД объекта разведки; квалификации его персонала; составе и структуре самой АСОД, используемом программном обеспечении; протоколах управления и взаимодействия; средствах и методах защиты информации, используемых в АСОД. Для получения этих сведений нет необходимости прибегать к приемам оперативной работы (подкупу персонала, краже документации и т. п.). Эти сведения, как правило, не являются закрытыми и могут быть получены при перехвате сетевого трафика интересующей АСОД либо при попытке установить сетевое соединение непосредственно с самой АСОД, когда по характеру получаемого отклика можно сделать соответствующие выводы.

Добывание закрытых сведений всегда связано с несанкционированным доступом к информации противника и имеет своим следствием утечку информации. Получение закрытых сведений осуществляется как в самой АСОД объекта, так и в информационно-вычислительных сетях, внешних по отношению к АСОД.

Таким образом, компьютерная разведка обладает большими потенциальными возможностями по получению информации, о структуре и принципах функционирования сети, с использованием известных методов и средств разведки.

Список используемых источников

1. Губарев В. А., Крутских П. П. Концептуальная модель конфликта в информационной борьбе // Радиотехника. 1998. № 6. С. 29.

2. Старовойтов А.В. Правительственная связь и актуальные проблемы развития защищенных информационно-коммуникационных систем России // Безопасность информационных технологий. 1994. № 3, 4. С.6–19.

УДК 004.056.5
ГРНТИ 81.93.29

К ВОПРОСУ ИСПОЛЬЗОВАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ АГЕНТОВ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

А. А. Кузькин, М. А. Куцакин, А. Н. Лапко,
Е. В. Лебеденко, В. В. Рябоконь

Академия Федеральной службы охраны Российской Федерации

В статье представлены основные направления и разработки в обеспечении информационной безопасности корпоративных вычислительных систем с использованием интеллектуальных технологий. Освещен вопрос обеспечения информационной безопасности корпоративной информационной системы с облачными вычислениями. Предложена модель безопасности информационной системы с использованием многоагентной технологии. Проанализированы основные проблемы информационной безопасности корпоративных систем, представлены направления для реализации механизмов аутентификации пользователя.

интеллектуальные технологии, информационная безопасность, механизмы аутентификации, облачные вычисления, многоагентный подход.

Рассматривая современные аспекты развития теории и практики поддержки информационных систем стоит выделить с одной стороны усиленное внимание к безопасности объектов, увеличение требований к защите информации, принятие международных стандартов в области информационных взаимодействий, растущие расходы на поддержку высокой защищённости, а с другой – увеличивающийся ущерб, нанесенный владельцам информационных ресурсов, подтвержденный опубликованными данными о результатах хакерских атак [1].

Результатом проведенного анализа в рассматриваемой предметной области является реализация на всех этапах процесса идентификации современных интеллектуальных технологий, которые приобретают все большее распространение. Сбор и обработка данных из Интернета о состоянии, направлении развития и уровне угроз процессов в мировом сообществе, синтез знаний, отраженных в источниках, реализованных на основе их интеллектуальной обработки, дает новое объединенное представление, позволяющее прогнозировать, моделировать и предотвращать развитие рисков безопасности.

Использование интеллектуальных технологий обработки данных дают возможность повысить уровень безопасности различных корпоративных информационных систем и платформ облачных вычислений [2]. При этом развитие технологий и сред облачных вычислений вводит новые источники угроз, которые необходимо учитывать в вопросах информационной безопасности компьютерных систем и сервисов.

Интеллектуальные системы защиты информации, обеспечивающие возможность обнаружения атак, используют нейронные сети как основной инструмент реализации, а также системы нечеткой логики и экспертные системы.

Нейронные сети представлены, как правило, в виде отдельной системы обнаружения атак, и при обработке трафика дают возможность произвести анализ информации о наличии деструктивных воздействий. Случаи с сигналом о наличии атаки перенаправляются к администратору безопасности. Этот подход используется как один из высокоскоростных способов анализа. Однако, основным недостатком использования нейронных сетей является «непрозрачность» формирования результатов анализа [3].

Экспертные системы дополняют нейронные сети. Они располагают некой базой знаний, в которой содержится описание правил классификации для соответствующих профилей легальных пользователей, а также сценарии возможных атак. Основным недостатком интеллектуальных систем защиты информации на основе экспертных систем является то, что они не адаптивны и не всегда могут распознать неизвестные для имеющейся базы знаний атаки.

Использование нейронных сетей в совокупности с экспертными системами повышают чувствительность к возможным атакам, поскольку используются только данные о событиях информационной безопасности, которые считаются подозрительными. Если нейронная сеть в процессе обучения начала выявлять новые атаки, то экспертной системе необходимо будет произвести нужные обновления [3].

Использование гибридных нейроэкспертных или нейронечетких систем позволяет отражать правила нечетких предикатов, которые оправдали себя в процессе обучения нейронной сети внутри системы безопасности. Свойство адаптивности нечетких предикатов нейронной сети позволяет решить отдельно взятые проблемы выявления угроз, сравнения поведения пользователей с имеющимися шаблонами, которые доступны в системе для автоматического создания новых правил в случае изменения состава атаки [3].

Недостатками этих систем являются:

− необходимость наличия высококвалифицированных специалистов;

− трудности реализации, возникающие в случае адаптация методов к потребностям конкретной организации;

− невозможность оценить эффективность конкретного комплекса применяемых средств защиты;

− требование наличия в организации достоверной статистики на инциденты информационной безопасности.

Рассматривая корпоративные информационные системы с точки зрения использования в них облачных вычислений важно отметить, что существуют следующие сервисные технологии: так называемые малые – на основе SaaS; средние – на основе IaaS; большие – на основе PaaS.

Большинство организаций будут работать с использованием гибридной модели, предоставляющей облачные сервисы, которые при необходимости будут интегрированы в функционирующие информационные системы предприятия.

Тогда модель информационных систем, используемых на предприятии, концептуально будет преобразована к следующему виду: вместо установки пакетов приложений на компьютеры организации для получения доступа к широкому спектру облачных сервисов будут использоваться только браузеры.

Направления развития в области защиты информации в интеллектуальных корпоративных информационных системах могут быть определены следующим образом [1]:

− разработка моделей нарушения и защитного действия на основе выбора оптимального варианта реагирования на события безопасности;

− совершенствование архитектуры системы защиты информации для эффективного управления в условиях неопределенности состояния информационной среды;

− совершенствование инструментальных программных комплексов интеллектуальной поддержки принятия решений с помощью исследования эффективности существующих методов, моделей и алгоритмов;

− разработка технологий для реализации мультиагентной системы с целью обнаружения атак, оценки уровня безопасности информации в интеллектуальных корпоративных информационных системах;

− разработка моделей и функций безопасности интеллектуальных корпоративных информационных систем на основе облачной инструментальной платформы с использованием семантических технологий.

Модель противодействия угрозам информационной безопасности корпоративных систем с технологиями облачных вычислений, в которой принимается решение о варианте действий в зависимости от вероятности атаки, оцененной с использованием механизма суетливого логического вывода [4].

Для разработки моделей защиты информации в интеллектуальных корпоративных информационных системах предлагается использовать объектную алгебру [1]. В модели информационной защиты объекты трансформируются в так называемые модели агентов [5].

В общем виде модель идентификатора в интеллектуальных корпоративных информационных системах будет иметь следующий вид (1):

$$M_{ik} = (M_t, M_a, M_s, M_p,), \quad (1)$$

где M_t – модель обнаружения угроз;

M_a – модель аутентификации пользователя;

M_s – модель анализа и оценка программного обеспечения (позволяет получить вывод о наличии или отсутствии разрушительных воздействий в программах);

M_p – модель противодействия угрозам.

Представленная в выражении (1) модель с учетом агентного подхода трансформируется в вид (2):

$$M_{ik} = (A_t, A_a, A_s, A_{sa}, A_p, A_c), \quad (2)$$

где A_t – агенты обнаружения угроз,

A_a – агенты, разграничивающие права доступа,

A_s – агенты анализа и оценки программного обеспечения,

A_{sa} – агенты, определяющие тип атаки,

A_p – агенты, строящие сценарий поведения системы для отражения атаки,

A_c – агенты-координаторы всей мультиагентной системы. Для небольших интеллектуальных корпоративных информационных систем эта модель будет сведена к выражению (3):

$$M_{ik} = (A_a, A_c, A_p, A_c). \quad (3)$$

В [6] описаны необходимые составляющие для обеспечения безопасной работы пользователей в среде облачных вычислений. Участники подобного взаимодействия это: пользователи (в качестве пользователей могут быть люди или организации), правильный аутентификатор, поставщик облачных услуг, цифровая подпись, агент поставщика облачных сервисов.

Краткое описание возможностей каждого из элементов подобного подхода представлено ниже:

− пользователь имеет ограниченный доступ к услугам «облака». Из предлагаемых сервисов он запрашивает облачные ресурсы от поставщика облачных услуг;

− аутентифицированное соединение устанавливает доверительные отношения с агентом аутентификации. Задача такого соединения в облачной среде – предоставить пользователю безопасный доступ к облачным ресурсам через сервис провайдера;

− облачный сервис может динамически масштабироваться для различных совокупностей потребностей пользователей;

− цифровая подпись – это инструмент, который идентифицирует личность отправителя сообщения или подписывает документ и удостоверяет, что содержимое отправленного сообщения или документа не изменялось;

− агенты поставщика облачных услуг способны принимать решения о выполнение заданий от имени пользователей. Они имеют право взаимодействовать с другими агентами путем переговоров с целью сотрудничества и координации. С позиции поставщика облачных услуг агент работает для оказания сервисов, обслуживания переговоров, услуги сотрудничества и их согласования.

Представленные выше составляющие требуют расширения для того, чтобы появилась возможность на основе полученной модели составить алгоритмы аутентификации, описать концепцию архитектуры информационной защиты, основанных на агентном подходе.

На данном этапе работы перечисленные положения являются направлениями дальнейших исследований.

Список используемых источников

1. Vishnyakou, U. A. Information control and safety: methods, models, hardware-software decisions. Monograph, Minsk: MIU, 2014. – 287 p.

2. Molyakov, Ampere-second. Models and a method of counteraction to the hidden threats of information security in the environment of cloud computing/Ampere-second. Abstract PhD thesis. on specialty 05.13.19. SPb, 2014. 17 p.

3. Kalatch, A. V., Nemtin E. S. Intellectual means and simulation of systems of information security the Online magazine «Tekhnologii Tekhnosfernoy Bezopasnosti» Release No. 3 (37). 2011. Pp. 3–11.

4. Машкина И. В. Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий : дис. … д-ра техн. наук / Машкина Ирина Владимировна. Уфа, 2009. 354 с.

5. Швецов А. Н. Агентно-ориентированные системы: от формальных моделей к промышленным приложениям // Всероссийский конкурсный отбор обзорно-аналитических статей по приоритетному направлению «Информационно-телекоммуникационные системы». 2008. 101 с.

6. Vishnyakou, U. A., Gondagh, M. M. Means of authentication of users in enterprise systems of control and the environments of cloud computing. Reports of BGUIR. No. 3. 2016. Pp. 94–97.

УДК 004.75
ГРНТИ 81.93.29

СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

А. А. Кузькин, М. А. Куцакин, В. В. Рябоконь

Академия Федеральной службы охраны Российской Федерации

В статье представлен пример облачной архитектуры с интегрированными средствами обеспечения информационной безопасности. Архитектура базируется на модели «клиент-сервер» с разделением на физический и виртуальный уровни устройств, при этом для повышения безопасности данных предлагается применять узлы виртуальных датчиков. При этом учитываются все направления от модели безопасности, аутентификации и авторизации до конфиденциальности, целостности и защиты данных. Для виртуальных сущностей принципиально проще обеспечить применение мер безопасности, управление и аудит, и проблемой остается лишь организация физического взаимодействия между реальными датчиками и их виртуальным воплощением.

интернет вещей, информационная безопасность, виртуальные объекты.

В течение ближайших лет рынок виртуализации будет расти, что обусловлено спросом на специализированное программное обеспечение и инфраструктуру для работы с большими объемами данных. Растет и популярность мобильных устройств и устройств «Интернета вещей» (IoT – *Internet of Things*). В настоящее время порядка 10 % данных обрабатывается периферийно, поскольку беспилотным летательным аппаратам, автомобилям и роботам требуется очень быстрый обмен информацией, а существенная доля вычислительных ресурсов приходится на конечные устройства. Именно безопасность в итоге станет одним из главных направлений роста инвестиций в облачные технологии (рис. 1).

Существующие решения, такие как: RFID (Radio Frequency Identification), NFC (Near Field Communication), SSO (Single Sign-On), OAuth (Open Authentication) не полностью адаптированы или применимы ко всем аспектам облачных сервисов. Новая модель сети, включающая "интернет вещей", "интернет данных", "интернет сервисов" и "интернет людей" (социальные

сети), подразумевает новую модель безопасности, связывающую все объекты в целостную архитектуру. Исследования и разработка адаптивных моделей для обеспечения защиты данных может стать основой для наиболее общих стандартизованных подходов к обеспечению информационной безопасности облачных технологий.

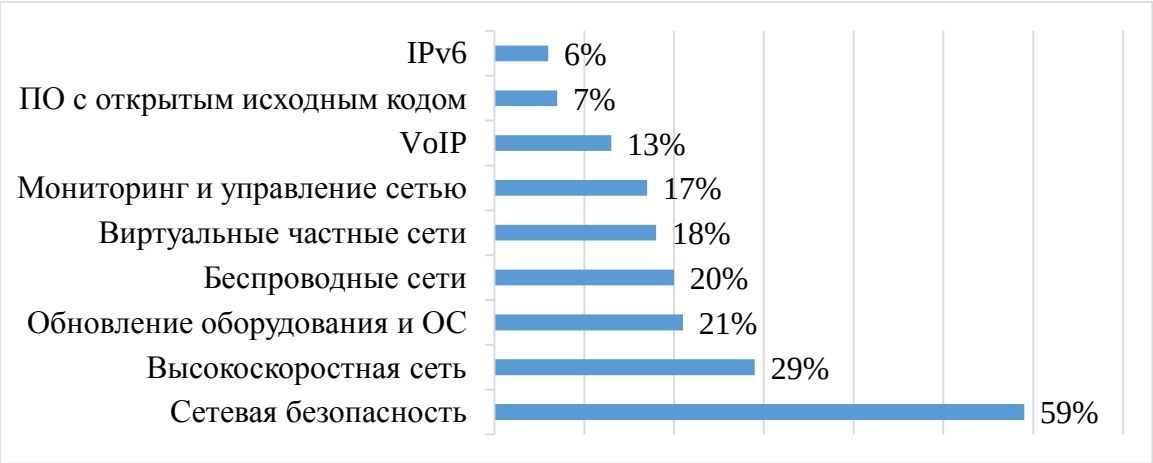


Рис. 1. Приоритеты инвестиций в сетевые технологии

Модели IoT как правило строятся аналогично эталонной модели взаимодействия открытых систем (ЭМВОС) с использованием многоуровневого подхода [1, 2] с отличиями в количестве уровней и их функциональности. Наиболее общими уровнями являются физический (аппаратный), транспортный и прикладной.

Основными задачами аппаратного уровня являются: идентификация устройств, взаимодействие с окружением (датчики и устройства управления), а также подготовка данных. Уровень характеризуется крайне ограниченными ресурсами для вычисления и хранения, а также зависимостью времени автономного функционирования от энергетических ресурсов.

Задачей промежуточного транспортного уровня является надежная и безопасная доставка данных от аппаратного уровня модулям или сервисам обработки данных. Она включает в себя подзадачи управления форматами данных, фильтрации и добавления контекста (значения данных, местоположение, локальные условия, точность, единицы измерения). В общем случае данный уровень может содержать дополнительные уровни абстракции, среди которых часто выделяют уровень «виртуализованного объекта» (VO – *virtualized object*) [3]. Подуровень VO может использоваться для оповещения и представления функций, доступных аппаратному уровню, вышележащим сервисам, а также хранения данных от аппаратного уровня о текущем и предыдущих состояниях физического устройства. Основными преимуществами использования VO в качестве виртуальной копии физического устройства являются: интеграция источников данных для комплексного

анализа, абстрагирование от гетерогенности интерфейсов и коммуникационных протоколов, а также масштабируемость [4]. При этом виртуальные датчики выдают серии данных аналогично физическим датчикам, но могут легко изменять и дополнять содержимое серии для обеспечения совместимости.

Задачей уровня приложений является представление данных и обеспечение сервисами и функциональностью конечных пользователей. Уровень может включать получение, обработку и фильтрацию данных, а также службы представления данных и их статистического анализа.

Обеспечение безопасности IoT как правило основано на применении известных подходов, акцентированных на безопасность сетевого взаимодействия, и включающих контроль доступа по сети, аутентификацию устройств, конфиденциальность и целостность данных. При этом должны быть учтены некоторые факторы, характерные для облачных технологий, такие как:

− безопасная инициализация оборудования, безопасная загрузка и инициализация операционной системы;

− безопасное обновление и изменение конфигурации при администрировании;

− обеспечение доверия между участниками;

− безопасное взаимодействие и контроль доступа;

− защита внутренних данных;

− возможность отказа в обслуживании при пропадании питания;

− обезличивание данных при сохранении их содержимого.

Предполагается, что архитектура IoT должна опираться на три основных кита защиты: доверие, безопасность и конфиденциальность.

Доверие должно основываться на:

− легкореализуемой инфраструктуре открытых ключей (PKI – P*ublic Key Infrastructure*) или децентрализованной самонастраиваемой системе распределения ключей;

− метаданных для обеспечения управления качеством информации;

− методах оценки доверия к пользователям, устройствам и данным;

− политиках управления использованием данных;

− методах контроля использования аппаратной и программной платформы.

Средства безопасности должны обеспечивать надежный и безопасный мониторинг и аудит, интегрироваться в модель используемых данных и обеспечивать защиту от специфических атак типа «отказ в обслуживании» (DoS – *Denial of Service*), специфичных для IoT. Производители оборудования должны обеспечивать возможность безопасного конфигурирования устройств во время всего периода эксплуатации, а также возможность интеллектуального самоконфигурирования в автономных условиях.

Конфиденциальность может основываться на шифровании данных, хотя дополнительно следует минимизировать объем критичных данных на каждом этапе (например, удаление данных местоположения пользователя/устройства при неиспользовании; удаление, обработка и фильтрация информации как можно более локально) и использовать различные идентификаторы для разных приложений и сервисов.

В работе [5] авторы предполагают, что безопасность IoT должна основываться на сети, а не на терминальных устройствах, обладающих ограниченными ресурсами. Предлагается использование программно-конфигурируемых сетей (ПКС, SDN – *Software defined networking*) для динамической адаптации сетевой безопасности к требованиям приложений и содержимого.

На основании описанных преимуществ использования виртуальных устройств для гибкости, масштабируемости и обеспечения информационной безопасности на разных этапах передачи данных от устройств в облако и обратно, предложена архитектура для интеграции облачных технологий и IoT, показанная на рисунке 2.

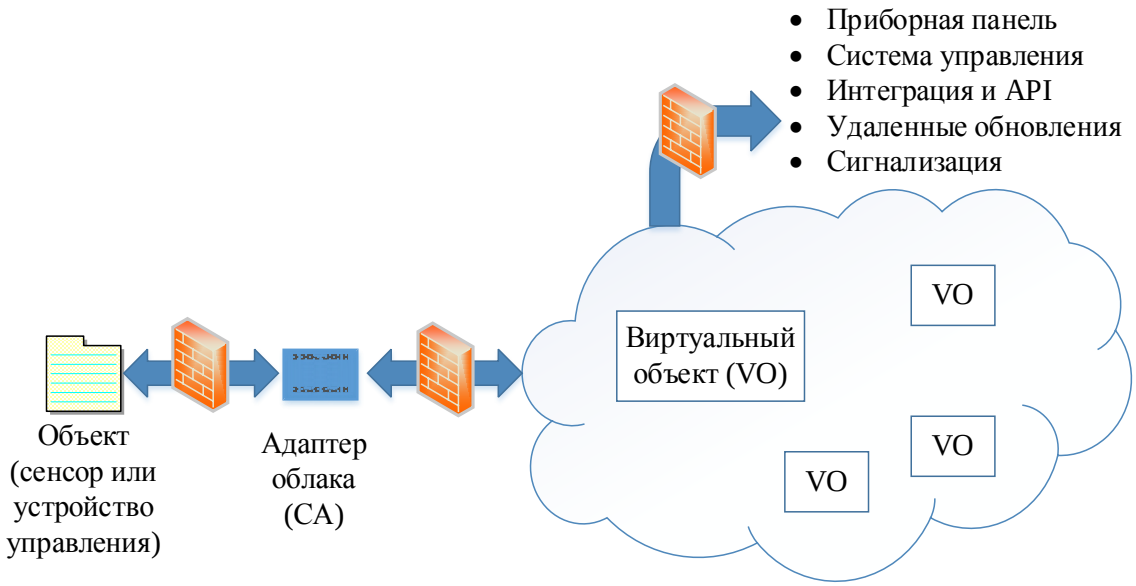


Рис. 2. Архитектура «Объект-облако» с использованием виртуальных объектов

Архитектура «Объект-облако» содержит множество мест, которые должны быть защищены:

− устройства должны быть безопасно спарены с локальным шлюзом (или адаптером облака);

− каждое физическое устройство должно быть безопасно сопряжено со своей виртуальной сущностью;

− взаимодействие устройства со шлюзом должно быть защищено;

− данные в облаке должны храниться с соблюдением требований по конфиденциальности;

− пользователи должны быть аутентифицированы в облаке и их права доступа должны быть определены.

Первый уровень защиты в предложенной архитектуре основан на разделении потоков информационного обмена «пользователь-облако» и «устройство-облако». Это существенно уменьшит атаки типа «низкоуровневый отказ в обслуживании», являющиеся критичными для IoT-объектов, работающих от аккумуляторных батарей. На втором уровне защиты функционирует межсетевой экран (МСЭ), установленный на адаптере шлюза и каждой точке входа в облако. Третий уровень обеспечивает конфиденциальность и безопасность сети устройств за счет аутентификации и шифрования сообщений. Последней частью архитектуры безопасности является упрощение каналов информационного взаимодействия.

Естественно, подобная сложная архитектура не может быть защищена одним-двумя основными протоколами. На каждом уровне архитектуры есть свои требования, которые могут включать: авторизацию, конфиденциальность, целостность, надежность, низкое энергопотребление, низкую вычислительную сложность, маленькую задержку и т. д.

В IoT всегда есть возможность подключения через публичные небезопасные сети, поэтому должны обеспечиваться целостность, конфиденциальность и идентификация оконечного оборудования. Общедоступные каналы связи могут быть защищены такими протоколами, как IPSec, SSL/TLS, а сами сообщения отдельно шифруются на прикладном уровне.

Для обеспечения идентификации оконечного оборудования и определения соответствующих прав доступа могут использоваться системы Kerberos или Radius. В зависимости от приложения, данные прикладного уровня защищаются либо протоколом PGP (*Pretty Good Privacy*), либо S/MIME (*Secure/Multipurpose Internet Mail Extensions*) для обеспечения конфиденциальности и целостности сообщений. При кодировании данных в формате JSON оконечное оборудование может использовать метод JWT (JSON *Web Token*).

В дальнейшем будут проводиться сравнительные эксперименты для выбора протоколов безопасности с учетом их надежности, защищенности и масштабируемости.

Список используемых источников

1. Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., Vasilakos A. V., The quest for privacy in the internet of things // IEEE Cloud Computing. 2016. Vol. 3. No. 2. Pp. 36–45.

2. Wu, M., Lu, T.-J., Ling, F.-Y., Sun, J., Du H.-Y. Research on the architecture of internet of things // 3rd IEEE Int. Conf. on Advanced Computer Theory and Engg. (ICACTE). 2010. Vol. 5. Pp. 484–487.

3. Sarkar, C., Nambi, A. U., Prasad, R. V., Rahim, A., Neisse, R., Baldini, G., DIAT: A scalable distributed architecture for IoT // IEEE Internet of Things Journal. 2015. № 3. Vol. 2. Pp. 230–239.

4. Nitti, M., Pilloni, V., Colistra, G., Atzori, L.The virtual object as a major element of the internet of things: a survey // IEEE Communications Surveys & Tutorials. 2015. Vol. 18. No. 2. Pp. 1228–1240.

5. Yu, T., Sekar, V., Seshan, S., Agarwal, Y., Xu, C., Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things // In Proc. 14th ACM Workshop on Hot Topics in Networks, HotNets-XIV, 2015. Pp. 5:1–5:7.

УДК 621.391
ГРНТИ 49.13.01

К ВОПРОСУ ПРИМЕНЕНИЯ РЕСУРСОСБЕРЕГАЮЩИХ СПОСОБОВ УЛУЧШЕНИЯ ЭКСПЛУАТАЦИОННОЙ НАДЕЖНОСТИ КОМПЛЕКСОВ АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВ

В. И. Курносов, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются пути улучшения эксплуатационной надежности комплексов аппаратно-программных средств, за счет ресурсосберегающих способов эксплуатации применительно к современным сетям, системам и устройствам телекоммуникаций различного назначения. Предложена методика построения таких комплексов. Представлены основные процедуры методического аппарата в виде частных методик и используемых моделей. Использование оригинального подхода позволяет обосновать структуру комплексов минимальной избыточности с обеспечением рационального расхода ресурса при эксплуатации в различных условиях и задачах по связи.

методы, надежность, ресурсосбережение, комплексы средств, телекоммуникации.

Эксплуатационно-экономические показатели телекоммуникационных систем (ТКС) непосредственно зависят от эксплуатационно-технических возможностей комплексов аппаратно-программных средств (КАПС), их образующих. Одним из важнейших показателей КАПС – надежность. Обеспечение безотказности КАПС приобретает особое значение по объективным и

субъективным причинами: возрастания цены отказов; появления у интегрированных комплексов новых свойств, за счет их различной аппаратно-программной реализацией, в том числе базовыми несущими конструкциями (БНК); необходимости обеспечения высокой эффективности ТКС в условиях дестабилизирующих факторов и т. д. [1].

В соответствии с множественным описанием принципов функционирования КАПС в ТКС и разработанным на его основе комплексом аналитических моделей [2] качество обработки информации в информационных направлениях связи (ИНС) ТКС зависит от средней наработки на отказ КАПС, среднего времени их восстановления и вероятности безотказной работы непересекающихся множеств функциональных преобразований (НМФП), которые определяются в том числе их коэффициентом приведения при эксплуатации.

В ряде работ [1, 3, 4], представлена подробная классификация способов обеспечения выполнения требований по эксплуатационной надежности (ЭН) и отказоустойчивости КАПС на всех стадиях их жизненного цикла. Однако техническая реализация при современном состоянии технологий производства телекоммуникационного оборудования не позволяет значительно увеличить (в 10–15 раз) среднюю наработку на отказ КАПС, необходимую для устойчивого функционирования и эффективного управления ТКС [5].

С учетом результатов анализа принципов построения инвариантных по каналообразованию сетей и выполненных исследований характера функционирования КАПС на сетях ТКС, решение задачи "качество сетевого ресурса – расход энергетических ресурсов (материальных средств)" целесообразно рассматривать на основе переключающегося критерия, который соответствует концепции адаптивной организации поведения сложных технических систем и описан в [6]:

$$\begin{cases} \max\limits_{\bar{t}\in T} T_0(\bar{t}) \text{ при } K_{\sum \text{тр}} \le K_{\sum} \quad (t), P_{\text{энер.тр.}}(T) \le P_{\sum} \quad (T); \\ \max\limits_{\bar{t}\in T} \overline{K}(T) \text{ при } K_{\sum \text{тр}} \ge K_{\sum} \quad (t), P_{\text{энер.тр.}}(T) > P_{\sum} \quad (T); \\ V \le V_{\text{доп}}, W(t) \ge W_{\text{тр}}. \end{cases} \qquad (1)$$

Критерий (1) отображает целевое предназначение КАПС в ТКС и отвечает системе предпочтений лиц, принимающих решение.

Задача обеспечения максимальной эффективности функционирования КАПС формулируется следующим образом: необходимо обеспечить такое распределение времени использования различного оборудования многофункциональных КАПС при эксплуатации их в ТКС на заданном интервале времени *T*, с учетом количества НМФП в структуре КАПС, которые максимизируют среднюю наработку на отказ комплекса T_0; обслуживание

нагрузки по различным видам услуг с требуемым качеством (при условии, что минимально необходимая производительность комплекса K меньше его возможностей, а энергетические возможности P превышают их требуемое количество), или достижение максимальной средней производительности; выполнение требований по своевременности и достоверности передачи различных видов информации W на заданном периоде эксплуатации оборудования (при условии, что энергетические возможности КАПС используются в полном объеме с задействованием всех ресурсов V, в том числе и при воздействии дестабилизирующих факторов и ограничениях на объем ресурсов).

Задача является сложной, оптимизационной, требует разумного компромисса между путями повышения значений показателей W, K, T_0.

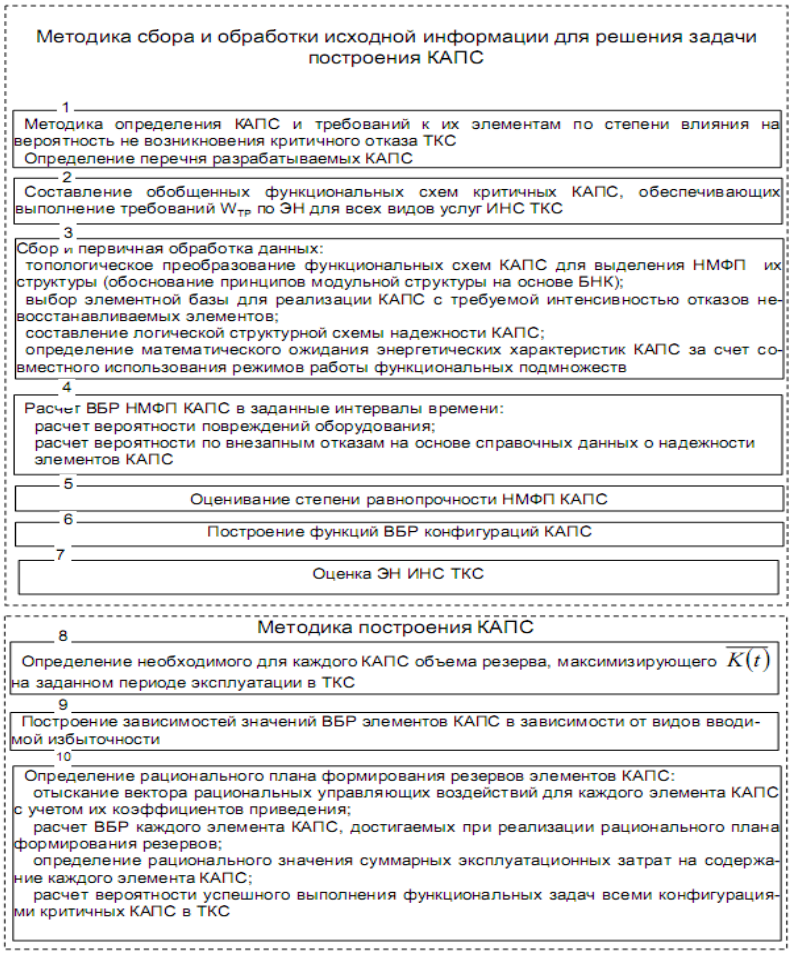


Рис. 1. Методика построения КАПС ТКС

Цель рационального управления ресурсами – достижение желаемого результата в пределах некоторого интервала времени [7] и обеспечение такого распределения времени активной работы между элементами КАПС, при котором их средняя наработка на отказ T_0 максимальна. Достижение второй составляющей указанной цели, в соответствии с критерием (1), осуществляется за пределами часа наибольшей нагрузки (ЧНН) и позволяет получить максимум производительности К за счет использования ресурсосберегающих технологий.

Методика построения КАПС (см. рис. 1) содержит частные методики: «Методику сбора и обработки исходной информации для решения задачи построения ресурсосберегающих КАПС» [6] и «Методику построения ресурсосберегающих КАПС» [2]. Цель второй методики заключается в получении оценок вероятности безотказной работы (ВБР) конфигураций КАПС

от объема различных видов избыточности и режимов эксплуатации, а также разработка алгоритмов реконфигурации структуры, в зависимости от внешних и внутренних условий эксплуатации.

Качество эксплуатации КАПС в значительной мере определяется уровнем организации диагностического обеспечения. Под последним понимают [8] комплекс взаимоувязанных правил, методов, алгоритмов и средств, необходимых для осуществления диагностирования на всех этапах жизненного цикла изделия, например, встроенной системой диагностики (ВСД) и техническим обслуживанием (ТО).

Проведенный анализ процессов эксплуатации и восстановления КАПС показал, что для решения задач по управлению функционированием ТКС важное значение имеет умение оценивать состояние ее элементов (см. рис. 2). События на рис. 2 обозначены цифрами: 1 – повреждение; 2 отказ; 3 – восстановление работоспособности; 4 – восстановление правильности функционирования; 5 – восстановление исправности.

Рис. 2. Схема основных состояний КАПС и событий, характеризующих их смену

Для снижения средних потерь К требуется увеличивать глубину автоматической проверки правильности функционирования НМФП, которая снижает число отказов в неконтролируемой части КАПС. Глубина автоматизации процессов поиска дефектов приводит к усложнению ВСД, безотказность которой влияет на качество применения КАПС [9]. Если исключить возможность участия оператора с помощью системы внешнего контроля в процессе восстановления, то при отказе ВСД возрастет функция потерь. Разделение процессов восстановления на восстановление правильности функционирования, работоспособности и исправности позволяет сократить время простоя комплекса при увеличении общего времени его перевода в исправное состояние.

Для решения этой задачи в общем виде целесообразно использовать модель в обозначениях [8], которая учитывает, что у основного множества ОМ в КАПС есть аварийное множество АМ:

$$\begin{aligned}\overline{\Delta K} = t_{\text{в}} \log_2 L\, \Delta B(y(d_1 P_{\text{ОМ}}^{(\text{C}+\text{a}_1)} Q_{\text{ОМ}} + d_2\left(1 - P_{\text{ОМ}}^{(\text{C}+\text{a}_1)}\right) Q_{\text{ОМ}} - \\ -P_{\text{ОМ}}^{(\text{C}+\alpha_2\text{a}_2)}\left(1 - P_{\text{ОМ}}^{\text{a}_1}\right)(1 - 2P_{\text{ОМ}}^{(1-\alpha_2)}))) + \alpha_2 P_{\text{ОМ}}^{\alpha_2\text{a}_2}(P_{\text{ОМ}}^{C}(2P_{\text{ОМ}}^{(1-\alpha_2)} + \\ +P_{\text{ОМ}}^{\text{a}_1}\left(1 - 2P_{\text{ОМ}}^{(1-\alpha_2)}\right) - P_{\text{ОМ}}) + y(1 - P_{\text{ОМ}}^{C})Q_{\text{ОМ}}) + Z(P_{\text{ОМ}}^{C}(P_{\text{ОМ}}^{\alpha_2\text{a}_2} \times \\ \times\left(P_{\text{ОМ}}^{C} - P_{\text{ОМ}}^{(1-\alpha_2)}\left(3P_{\text{ОМ}}^{\text{a}_1} + \alpha_2\left(1 - 2P_{\text{ОМ}}^{\text{a}_1}\right) - 2\right) - \alpha_2 P_{\text{ОМ}}^{\text{a}_1} + 1{,}5\left(P_{\text{ОМ}}^{\text{a}_1} - 1\right)\right) + \\ +1{,}5Q_{\text{ОМ}}) + y(1 - P_{\text{ОМ}}^{C})(P_{\text{ОМ}}^{\alpha_2\text{a}_2}\left(P_{\text{ОМ}} - P_{\text{ОМ}}^{(1-\alpha_2)}(1 - \alpha_2) - \alpha_2\right) + 1{,}5Q_{\text{ОМ}}))).\end{aligned} \quad (2)$$

Если элементы ОМ зарезервированы, то выражение (2) примет вид:

$$\begin{aligned}\overline{\Delta K_{\text{р}}} = t_{\text{в}} \log_2 L \times B(d_1 P_{\text{ОМ}}^{(\text{C}+\text{a}_1)} Q_{\text{ОМ}} + d_2\left(1 - P_{\text{ОМ}}^{(\text{C}+\text{a}_1)}\right) Q_{\text{ОМ}} + \\ +P_{\text{ОМ}}^{(\text{C}+\alpha_2\text{a}_2)}\left(1 - P_{\text{ОМ}}^{\text{a}_1}\right)(2P_{\text{ОМ}}^{(1-\alpha_2)} - 1)) + (1 - P_{\text{ОМ}}^{C})(P_{\text{ОМ}}^{\alpha_2\text{a}_2}\alpha_2 Q_{\text{ОМ}} + \\ +Z(P_{\text{ОМ}}^{\alpha_2\text{a}_2}\left(P_{\text{ОМ}} - P_{\text{ОМ}}^{(1-\alpha_2)}(1 - \alpha_2) - \alpha_2\right) + 1{,}5Q_{\text{ОМ}}))).\end{aligned} \quad (3)$$

Предложенная методика (рис. 1) позволяет обосновать структуру КАПС, которая обладает минимальной избыточностью и возможностью рационального расхода ресурса в процессе эксплуатации.

Список используемых источников

1. Рябинин И. А. Надежность и безопасность структурно-сложных систем. СПб.: Политехника, 2000. 248 с.

2. Курносов В. И. Методологические основы управления качеством функционирования ведомственных телекоммуникационных систем. СПб.: ФГУП «НИИ "Рубин"», 2007. 412 с.

3. Бакланов И. А. Измерительные технологии в телекоммуникационных системах. М.: Эко-Трендз, 1998. 183 с.

4. Сифоров В. И. О методах расчета надежности работы систем, содержащих большое число элементов // Радиотехника. 1995. № 4–5. С. 147–156.

5. Курносов В. И., Лихачев А. М. Тенденции технического и технологического развития телекоммуникационных сетей. СПб.: Изд-во АБРИС, 1997. 439 с.

6. Курносов В. И., Лихачев А. М. Методология проектных исследований и управление качеством сложных технических систем электросвязи. СПб.: Изд-во ТИРЕКС, 1998. 496 с.

7. Петухов Г. Б. Основы теории эффективности целенаправленных процессов. Ч. 1. Методология, методы, модели. Л.: Изд-во МО, 1989. 660 с.

8. Ксенз С. П., Лихачев А. М., Климентов В. И. Теоретические и прикладные задачи диагностирования средств связи и автоматизации / под ред. С. П. Ксенза. Л.: ВАС, 1990. 227 с.

9. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб.: ГУАП, 2016. 325 с.

УДК 621.391
ГРНТИ 49.01.82

РАЦИОНАЛЬНЫЙ ПОДХОД К РАЗВИТИЮ ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ НА ОСНОВЕ МЕТОДОВ СТРУКТУРНО-ПАРАМЕТРИЧЕСКОГО ПОДОБИЯ

В. И. Курносов, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается подход к развитию действующей телекоммуникационной инфраструктуры посредством методов структурно-параметрического подобия исходного фрагмента на основе положений методологии генотипа телекоммуникаций. Представлены основные процедуры формирования перспективной (итоговой) инфраструктуры для последующего ее поэтапное преобразование в исходный фрагмент, который обладает заданной степенью подобия, обоснованной с применением графовой модели и процедур спарсификации. Использование оригинального подхода позволяет обосновать структуру исходного фрагмента минимальной избыточности с обеспечением рационального расхода ресурсов на его создание и поэтапное развитие в различных условиях и задачах по связи.

граф сети, спарсификация, семплы, структурно-параметрическое подобие, проектирование сетей связи.

Традиционные подходы к построению телекоммуникационной инфраструктуры (ТКИ) с применением средств и комплексов связи и управления связью опираются на эволюционное развитие изделий (средств и комплексов). Их системотехнические решения ориентированы, как правило, на унифицированные платформенные решения коммуникаций, безопасности и управления сетями, узлами, оборудованием связи и техническими средствами [1].

Развитие ТКИ осуществляют в рамках плановых мероприятий и этапности работ, которые реализуют программно-целевые методы:

– развертывание на объектах ТКИ, заблаговременно подготовленных в строительном отношении, перспективных средств и комплексов на базе унифицированных платформенных решений коммуникаций, безопасности и управления для ТКИ;

– комплексную отладку и опытную эксплуатацию в ТКИ пусковых комплексов различной очереди;

– ввод в штатную эксплуатации и последующее наращивание компонент (фрагментов) ТКИ очередного этапа развития с учетом условий в действующей инфраструктуре и ресурсах.

Методологической основой для обоснования системотехнических решений по построению, развитию (модернизации) ТКИ в [2] предложено использовать, в качестве ключевых, исходные фрагменты (опытные районы) перспективной (итоговой) ТКИ.

«Фрагмент» ТКИ в терминах «эволюционного моделирования» можно представить «генотипом» искомой телекоммуникационной инфраструктуры. Для его описания используется геопространственная информация (пространственные данные). Обработка пространственных данных осуществляется на основе известных методов геоинформатики, которые широко применяются в пространственном анализе, в частности, анализе сетей.

Для определения заданной степени подобия «фрагмента» с оригиналом – действующей или искомой ТКИ применяют графовую модель и способы спарсификации графов, которые позволяют получить семплы (графы меньшей размерности), обладающие изоморфизмом по отношению к исходному графу [3].

При спарсификации исходного графа формируется сжимающая последовательность подграфов (геосемплов – с учетом пространственных данных), которые при пошаговой спарсификации отображают фрагменты ТКИ разных этапов развития, в том числе исходный фрагмент ТКИ.

В постановке задачи формирования исходного фрагмента на основе структурно-параметрического построения действующей ТКИ, воспользуемся положениями из [4], с учетом которых она может быть сведена к задаче аппроксимации простого связного неориентированного нагруженного графа $G_0(V_0, E_0, U_0)$, который, в свою очередь, описывает структуру итоговой ТКИ с мощностью множества вершин равной $|V_0| = n$ семплом $G_k(V_k, E_k, U_k)$ меньшей размерности, в котором $|V_k| = n_k$ при выполнении условия:

$$1 \leq n_k < n. \quad (1)$$

В качестве целевой функции аппроксимации предложено использовать минимум максимума разностей расстояний между вершинами исходного графа и соответствующими им вершинами полученного малого графа (семпла).

Введем обозначения:

– метавершины аппроксимирующего графа G_k описываются как:

$$\{v_i^k, i = 1, \dots, n_k\}; \quad (2)$$

– $u_k(v_i, v_j)$ вес ребра между смежными метавершинами графа G_k;

– $m_k(v_i, v_j)$ расстояние между смежными метавершинами графа G_k;

– метавершина графа G_k, аппроксимирующая вершину v_j графа G_0, описывается как:

$$v_{c(i)}^k. \quad (3)$$

Формулировка задачи с учетом введенных обозначений

Дан простой связной неориентированный нагруженный граф $G_0(V_0, E_0, U_0)$, с неотрицательной вещественной весовой функцией U_0 на ребрах E_0, которая принимает значения из диапазона от 0 до ∞, и вещественное число – допустимая погрешность аппроксимации $e_{max} > 0$.

Требуется:

– минимизировать размерность аппроксимирующего графа $G_k(V_k, E_k, U_k)$:

$$|V_k| \to min; \quad (4)$$

– при заданном ограничении на погрешность аппроксимации:

$$A_e \le e_{min}. \quad (5)$$

В терминах [4] – это задача разборки графа с пересчетом матрицы расстояний исходного графа (весов ребер), с сохранением информации о путях исходного графа и минимизации количества вершин аппроксимирующего графа.

Последовательность решения задачи состоит в последовательном «удалении» вершин в исходном графе $G_0(V_0, E_0, U_0)$. Удаляемым вершинам в качестве метавершины ставится в соответствие одна из смежных вершин и выполняется пересчет весов ребер для графа меньшей размерности.

Вершины графа рассматриваются в порядке роста их степеней. Если существуют несколько вершин с одинаковой степенью, выбор осуществляется по росту вносимой погрешности A_e. Если среди них окажется несколько с одинаковой вносимой погрешностью, выбор осуществляется в порядке возрастания номера.

На начальном этапе все значения $A_e = 0$.

Удаление вершины v_i влечет за собой необходимость изменения весов ребер только между смежными с ней вершинами $\{v_i, z = 1, ..., m\}$. Пересчет

весов ребер осуществляется, как предложено в [4] с использованием выражения:

$$u\left(v_{i_j}, v_{i_l}\right) = \begin{cases} u\left(v_{i_j}, v_i\right), \text{если } u\left(v_{i_j}, v_i\right) + u\left(v_i, v_{i_l}\right) < u\left(v_{i_j}, u_{i_l}\right), \\ u\left(v_{i_j}, u_{i_l}\right) \text{иначе} \end{cases}. \quad (6)$$

Для минимизации общей погрешности аппроксимации необходимо поставить в соответствие удаленной вершине v_i такую метавершину $v_{c(i)}$, которая обеспечит как можно меньшим максимум абсолютной разности расстояний между v_i, $v_{c(i)}$ и вершинами исходного графа:

$$\max_i \left| m\left(v_i, v_j\right) - m\left(v_{c(i)}, v_j\right) \right| \to min. \quad (7)$$

В исходном графе расстояния от v_i рассчитываются по формуле:

$$m(v_i, v_j) = \min_z (m(v_i, v_{i_z}) + m(v_{i_z}, v_j)). \quad (8)$$

После удаления v_i расстояние между не удаленными вершинами $m(v_{iz}, v_j)$ не изменилось. В качестве $v_{c(i)}$ необходимо выбирать ближайшую смежную с v_i вершину $v_{c(i)} = v_{ij}$:

$$u(v_i, v_{i_j}) = \min_z u(v_i, v_{i_z}). \quad (9)$$

При этом погрешность аппроксимации увеличится не более чем на вес ребра $u(v_i, v_{ij})$.

Удаление вершины v_i приводит к изменению погрешности аппроксимирующей ее вершины $v_{c(i)}$ по правилу:

$$A_e^{c(i)} \to A_e^{c(i)} + A_e^i + u(v_i, v_{c(i)}). \quad (10)$$

В силу сохранения расстояний между оставшимися вершинами, для выполнения условия

$$A_e \le e_{max} \quad (11)$$

необходимо, чтобы для всех пар оставшихся вершин (v_i, v_j) выполнялось условие:

$$A_e^l + A_e^J \le e_{max}. \quad (12)$$

Условие (12) будет справедливо, если выполняется условие:

$$A_e^J \le \frac{e_{max}}{2},\ \text{для}\ \forall j. \tag{13}$$

Согласно этому условию вершину v_i можно удалять тогда, когда для аппроксимирующей ее вершины $v_{c(i)}$ выполняется условие:

$$A_e^{c(i)} + A_e^i + u(v_i, v_{c(i)}) \le \frac{e_{max}}{2}. \tag{14}$$

Поскольку полученная таким образом аппроксимация не гарантирует связности подграфов

$$G_0(V_j): V_j = \{v_i \in V | c(i) = j\} \tag{15}$$

исходного графа, вершины которых аппроксимируют одной метавершиной, воспользуемся правилом переопределения функции $c(i)$, которое гарантирует связность таких подграфов без увеличения погрешности аппроксимации.

Если для вершины v_i, принадлежащей V_k, отсутствует путь до центра $c(V_k)$ в графе $G_k(V_k)$, то в пути от v_i до $c(V_k)$ в исходном графе G_0 существует вершина v_i, принадлежащая V_l.

В случае, если принадлежность вершины v_i множеству V_l не увиливает радиус $r(V_l)$ и у вершины v_i принадлежность множеству не изменялась, полагаем, что $c(i) = l$.

В противном случае все вершины v_s пути от v_i до v_j в исходном графе G_0 делаем принадлежащими множеству V_k, полагая $c(s) = k$.

После каждого изменения принадлежности множеству какой-либо из вершин, центры и радиусы изменившихся множеств V_k, V_l пересчитываются, и процесс повторяется снова, до тех пор, пока не останется несвязных подграфов, после чего полагают:

$$u\left(c(V_i), c(V_j)\right) = r(V_j), c(i) = c(V_j), \forall i: c(i) = j. \tag{16}$$

Последовательность формирования исходного фрагмента ТКИ (геосемпла $G_k(V_k, E_k, U_k)$) на основе структурно-параметрического подобия итоговой ТКИ (на основе исходного графа $G_0(V_0, E_0, U_0)$) содержит следующие процедуры.

Процедура 1. Ввод исходных данных: множества вершин V_0, множества ветвей E_0; множества весовых функций U_0, требуемой погрешности аппроксимации e_{max}.

Процедура 2. Построение на основе исходных данных: матрицы последовательностей P; матрицы расстояний M; матрицы погрешностей аппроксимации A_e: $= 0$. Подготовка к выбору очередной вершины исходного графа i: = 1.

Процедура 3. Выбор очередной v_i вершины с минимальной степенью.

Процедура 4. Расчет погрешностей смежных с вершиной v_i вершин по правилу (10)

Процедура 5. Выбор для вершины v_i аппроксимирующей вершины $v_{c(i)}$ по правилу (14). При выполнении условия переход на процедуру 6, в ином случае – на процедуру 11.

Процедура 6. Пересчет весов ребер.

Процедура 7. Перерасчет погрешности, вносимой аппроксимирующей вершиной.

Процедура 8. Корректировка графа путем удаления из него вершины v_i.

Процедура 9. Подготовка к выбору очередной вершины с минимальной степенью i: = i + 1.

Процедура 10. Проверка условия $i.(n - 2)$ – все ли вершины исходного графа G_0 рассмотрены? Если нет, переход на процедуру 3, иначе – 11.

Процедура 11. Устранение несвязных подграфов, образуемых метавершинами аппроксимирующего графа, и пересчет параметров.

Процедура 12. Оформление и вывод результатов: G_k, описывающего структуру исходного фрагмента с минимальным количеством узлов связи.

Предложенный подход позволяет обосновать структуру исходного фрагмента минимальной избыточности с обеспечением рационального расхода ресурсов на его создание и поэтапное развитие в различных условиях и задачах по связи.

Список используемых источников

1. Курносов В. И. Методологические основы управления качеством функционирования ведомственных телекоммуникационных систем. СПб.: ФГУП «НИИ "Рубин"», 2007. 412 с.

2. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб.: ГУАП, 2016. 325 с.

3. Шестаков А. В. Метод обоснования структурно-параметрического подобия опытного района действующей системе связи // Автоматизация процессов управления. 2016. № 1 (43). С. 17–25.

4. Тимеряев Т. В. Методы и алгоритмы управления маршрутизацией в транспортных сетях на основе оперативной обработки информации в разреженных графах : дисс. ... канд. техн. наук : 05.13.01 / Тимеряев Тимофей Валерьевич. Уфа, 2015. 203 с.

УДК 004.02
ГРНТИ 28.23.19

СПОСОБ ФОРМИРОВАНИЯ НАБОРА СТРУКТУРНЫХ ИНДИКАТОРОВ В ЗАДАЧЕ РАННЕГО ПРЕДУПРЕЖДЕНИЯ МЕЖНАЦИОНАЛЬНЫХ КОНФЛИКТОВ

А. Н. Лапко

Академия Федеральной службы охраны Российской Федерации

Статья посвящена формированию набора структурных индикаторов, используемых наряду с поведенческими индикаторами при решении задачи раннего предупреждения межнациональных конфликтов. Представлены социально-экономические и политические показатели, на основе которых происходит построение системы структурных индикаторов. Детально описан способ формирования набора структурных индикаторов на основе индуктивного вывода.

межнациональная напряженность, раннее предупреждение межнациональных конфликтов, структурные индикаторы, индуктивный вывод.

Национальное многообразие сопряжено с проявлением напряженности в сфере межнациональных отношений. Конфликтность не свойственна межнациональным отношениям, однако межнациональная напряженность (МНН) способна быстро трансформироваться в конфликт, а затем – в угрозу федеративного устройства государства. В связи с этим одним из важнейших направлений государственного управления в сфере национальной политики является эффективное предупреждение межнациональных конфликтов (МНК) [1].

МНК не возникают неожиданно, а вызревают в течение длительного времени. Их возникновение обусловлено конкретными причинами в условиях конкретной обстановки. Причины МНК многообразны, а их сочетание в каждом случае может изменяться.

Раннее предупреждение МНК предполагает постоянный мониторинг индикаторов повышения МНН. Отслеживаемые в процессе мониторинга индикаторы можно разделить на две группы: структурные (долговременные) и поведенческие (динамические) [2].

Структурные индикаторы представляют собой фоновые условия, которые могут привести к развитию конфликта. Как правило, они характеризуют социально-экономическую и политическую ситуацию в регионе.

Поведенческие индикаторы выступают в роли спускового механизма, после чего конфликт становится открытым и необратимым. Поведенческие индикаторы характеризуют деятельность некоторой политической силы, которая может выступать самостоятельно в роли одной из сторон конфликта в случае, если отстаиваются собственные этноцентристские интересы, либо опосредованно в случае, если отстаивается позиция, навязанная извне, например, специальными службами иностранных государств.

В зависимости от типа индикаторов различают способы их использования. Так структурные индикаторы сигнализируют о наступлении событий в регионе, которые могут привести к проявлению МНН. Они соответствуют предупреждениям, на которые выдаются рекомендации по стабилизации ситуации. Поведенческие индикаторы сигнализируют о возникновении в регионе событий, вызванных деятельностью политических или иных сил и направленных на целенаправленное повышение МНН. Они соответствуют критическим ошибкам, на которые выдаются обязательные для выполнения инструкции по деэскалации конфликта.

Для определения состава структурных индикаторов применяется методология индуктивного вывода на основе прецедентов [3]. Принимается гипотеза о наличии причинно-следственной связи между индикаторами МНН и ее проявлением. В соответствии с принятой гипотезой формулируются утверждения:

– причиной МНН может быть событие или совокупность событий, которые предшествуют ее проявлению;

– если в двух и более случаях проявлению МНН предшествует некоторое событие, то именно это событие следует рассматривать в качестве ее причины.

Исходными данными решаемой задачи являются ретроспективные значения социально-экономических и политических (структурных) показателей, измеренные в равноотстоящие моменты времени $t_k + \Delta t$. Структурных показатели (табл.) могут измеряться в качественной шкале, отражая наличие или отсутствие признака, или в количественной шкале, отражая численное значение показателя.

ТАБЛИЦА. Структурные показатели

Показатель	Обозначение, способ вычисления
представительство в органах местного самоуправления	$p_1 \in \{0, 1\}$, где 0 – представительства нет; 1 – имеется представительство
представительство в органах государственной власти	$p_2 \in \{0, 1\}$, где 0 – представительства нет; 1 – имеется представительство
уровень безработицы	$p_3 \in [0, 100]$ и вычисляется как отношение количества безработного населения этнической группы к

Показатель	Обозначение, способ вычисления
	общей численности экономически активного населения этнической группы
уровень доходов	$p_4 \in [0, +\infty)$ и вычисляется как количество денежных средств, полученных в расчете на каждого представителя этнической группы за временной интервал
доля населения с доходами ниже прожиточного минимума	$p_5 \in [0, 100]$ и вычисляется как отношение населения этнической группы с доходами ниже прожиточного минимума к общей численности населения этнической группы
наличие задолженности по предоставлению жилья	$p_6 \in [0, 100]$ и вычисляется как отношение количества населения этнической группы, признанных нуждающимися в предоставлении жилья, к общей численности населения этнической группы
наличие задолженности по выплате заработной платы	$p_7 \in \{0, 1\}$, где 0 – задолженности нет; 1 – имеется задолженность
наличие задолженности по выплате пенсий	$p_8 \in \{0, 1\}$, где 0 – задолженности нет; 1 – имеется задолженность
наличие задолженности по выплате социальных пособий	$p_9 \in \{0, 1\}$, где 0 – задолженности нет; 1 – имеется задолженность
обеспеченность товарами первой необходимости	$p_{10} \in [0, 100]$ и вычисляется как отношение количества имеющихся в продаже по доступной цене товаров первой необходимости к общему количеству товаров первой необходимости
наличие школ с изучением национального языка	$p_{11} \in \{0, 1\}$, где 0 – школ нет; 1 – имеются школы
наличие теле- и радиоканалов, вещающих на национальном языке	$p_{12} \in \{0, 1\}$, где 0 – теле- и радиоканалов нет; 1 – имеются теле- и радиоканалы
наличие духовно-религиозных учреждений этнической группы	$p_{13} \in \{0, 1\}$, где 0 – учреждений нет; 1 – имеются учреждения
уровень миграции	$p_{14} \in [0, +\infty)$ и вычисляется как отношение прибывших мигрантов к общей численности населения
наличие преступлений, жертвами которых стали представители этнической группы	$p_{15} \in \{0, 1\}$, где 0 – преступлений нет; 1 – имеются преступления

Для определения состава структурных индикаторов из числа соответствующих показателей используется предположение, что проявлению МНН должны предшествовать события, изменяющие в худшую сторону социально-экономическую или политическую ситуацию в регионе. Благоприятная ситуация характеризуется:

– незначительными колебаниями значений структурных показателей, измеряемых в количественной шкале, около некоторого среднего значения,

т. е. отсутствием резких скачков или тренда к увеличению (уменьшению) в значениях структурных показателей;

– отсутствием единиц (нулей) в значениях структурных показателей, измеряемых в качественной шкале.

Способ формирования структурных индикаторов заключается в следующем: в моменты времени, предшествующие проявлению МНН, анализируются значения структурных показателей на наличие тренда или аномальных значений, которые будут являться причиной МНН. Если тренда и аномальных значений выявлено не будет, то причина МНН может быть обусловлена:

– иными социально-экономическими и политическими факторами, которые не описываются имеющимися структурными показателями, это дает основания для расширения признакового пространства;

– исключительно поведенческими факторами в условиях благоприятной социально-экономической и политической ситуации в регионе.

Формирование структурных индикаторов состоит в последовательном выполнении шагов:

1. Выделяется множество временных интервалов $T_k = \{t_{k1}, t_{k2}, \ldots, t_{kq}\}$, в которых было зафиксировано проявление МНН.

2. Задается горизонт поиска r, который определяет длину анализируемого временного ряда, состоящего из значений структурного показателя.

3. Формируется множество $T_{k-1} = \{t_{k1-1}, t_{k2-1}, \ldots, t_{kq-1}\}$, которое содержит временные интервалы, предшествующие на один такт модельного времени повышению МНН в регионе. Аналогично формируются множества T_{k-2}, T_{k-3}, …, T_{k-r}.

4. Из базы данных выбираются значения структурных показателей, соответствующих временным интервалам множеств T_{k-1}, T_{k-2}, T_{k-3} … T_{k-r}. Формируются временные ряды структурных показателей: $S_i(t_{k1}) = (p_i(t_{k1-r}), p_i(t_{k1-r+1}), \ldots, p_i(t_{k1-2})\ p_i(t_{k1-1}))$ и аналогично $S_i(t_{k2})$, $S_i(t_{k3})$, …, $S_i(t_{kq})$.

5. Временные ряды $S_i(t_{k1})$, $S_i(t_{k2})$, $S_i(t_{k3})$, …, $S_i(t_{kq})$, значения которых измеряются в количественной шкале, анализируются на наличие существенных колебаний:

– на основе значений временного ряда строится вспомогательная последовательность нулей и единиц в соответствии с правилом (1):

$$p_i\left(t_j\right) = \begin{cases} 1, \text{если } p_i\left(t_j\right) - p_i\left(t_{j-1}\right) > 0 \\ 0, \text{если } p_i\left(t_j\right) - p_i\left(t_{j-1}\right) < 0 \end{cases}; \quad (1)$$

– для структурных показателей, у которых большее значение является худшим (например, уровень безработицы), анализируется последовательности единиц (восходящие серии): подсчитывается количество и протяженность таких серий;

– для структурных показателей, у которых большее значение является лучшим (например, уровень доходов), анализируется последовательности нулей (нисходящие серии);

– вычисляется выборочное среднее значение m фрагмента временного ряда в соответствии с выражением (2):

$$m = \frac{1}{r} \cdot \sum_{j=1}^{r} p_i\left(t_j\right); \tag{2}$$

– вычисляется выборочное среднеквадратическое отклонение s фрагмента временного ряда в соответствии с выражением (3):

$$s = \sqrt{\frac{1}{r} \cdot \sum_{j=1}^{r} \left(p_i\left(t_j\right) - m\right)^2}\ ; \tag{3}$$

– в случае если хотя бы для одного большего значения восходящей серии выполнится неравенство (4), или для одного меньшего значения нисходящей серии выполнится неравенство (5), то порождается гипотеза h_i о влиянии структурного показателя p_i, значения которого составляют анализируемый временной ряд, на изменение в худшую сторону социально-экономической и политической ситуации в регионе, а сам структурный показатель p_i переходит в разряд индикаторов МНН для данного региона.

$$p_i\left(t_j\right) \geq m + s; \tag{4}$$

$$p_i\left(t_j\right) \leq m - s; \tag{5}$$

6. Фрагменты временных рядов $S_i(t_{k1})$, $S_i(t_{k2})$, $S_i(t_{k3})$, …, $S_i(t_{kq})$, значения которых измеряются в качественной шкале, анализируются на наличие аномальных значений:

– для структурных показателей, у которых единица является лучшим значением (например, представительство в ОГВ), анализируются фрагменты временных рядов на наличие нулей, которые в данном случае являются аномальными значениями;

– для структурных показателей, у которых нуль является лучшим значением (например, наличие преступлений, жертвами которых стали представители этнической группы), анализируются фрагменты временных рядов на наличие единиц;

– при выявлении в фрагментах анализируемых временных рядов аномальных значений порождается гипотеза h_i о влиянии структурного показателя p_i на изменение в худшую сторону социально-экономической и политической ситуации в регионе, а сам структурный показатель p_i переходит в разряд индикаторов МНН для данного региона.

Представленный способ формирования состава структурных индикаторов создает условия для накопления и обобщения информации о социально-экономической и политической ситуации в регионе, своевременного оповещения о нарастании МНН, определения круга проблем, нуждающихся в разрешении. Проведенная оценка адекватности представленного способа подтвердила его непротиворечивость и пригодность к использованию по назначению.

Список используемых источников

1. Стратегия государственной национальной политики Российской Федерации на период до 2025 года: утв. Указом Президента Российской Федерации от 19 декабря 2012 г. № 1666.

2. Лапко А. Н. Подход к совершенствованию информационно-аналитического обеспечения системы раннего предупреждения межнациональных конфликтов // Экономика и менеджмент систем управления. Воронеж: Изд-во Научная книга, 2016. № 2 (20). С. 82–91.

3. Лапко А. Н. Разработка информационно-аналитической системы раннего предупреждения межнациональных конфликтов // Информационные системы и технологии. Орел: ОГУ им. И. С. Тургенева, 2017. № 5 (103). С. 23–32.

УДК 004.03
ГРНТИ 81.93.29

ОСОБЕННОСТИ RFID-МАРКИРОВКИ КАК СРЕДСТВА ИДЕНТИФИКАЦИИ ДЛЯ ОБУВНЫХ ТОВАРОВ

А. А. Лавринович

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В Российской Федерации обувные товары товарных позиций 6401–6405 ТН ВЭД ЕАЭС с 01.07.2019 подлежат обязательной маркировке средствами идентификации. В данной статье на основе результатов проекта по RFID-маркировке изделий из меха выделяются потенциальные особенности RFID-маркировки как средств идентификации обувных товаров. Исходя из этого, определяются угрозы информационной безопасности для системы RFID-маркировки обувных товаров.

маркировка товаров, RFID-технология, информационная безопасность, RFID-маркировка, RFID, маркирование товаров, RFID-метка, средства идентификации, контрафактная продукция, внешняя торговля.

Распоряжением Правительства от 28.04.2018 № 792-р определен перечень товаров, в отношении которых планируется введение маркировки средствами идентификации в целях снижения объемов контрафактной продукции [1]. Данный перечень включает в себя 10 категорий товаров. На сегодняшний день уже имеется успешный опыт внедрения системы маркировки товаров с помощью RFID-технологии – проект по маркировке товаров из меха позволил в разы сократить объемы контрафактной продукции [2]. В данной статье необходимо определить перспективы использования опыта проведения данного проекта в маркировке иных товаров. Каждая из 10 категорий обладает различными характеристиками (тара, конструктивные особенности), что оказывает влияние на то, какими характеристиками могут обладать средства идентификации данных товаров. Данный вопрос будет рассматриваться с позиции обеспечения информационной безопасности системы маркировки товаров в рамках внешнеэкономической деятельности (далее – ВЭД) [3, 4].

Согласно данным таможенной статистики внешней торговли [5], наибольшие объемы импорта в стоимостном выражении наблюдаются обувным товарам (товарные позиции 6401–6405), несмотря на снижение стоимостных объемов импорта на 45,4 % за период 2013–2018 гг. являются лидерами по данному показателю среди рассматриваемых категорий товаров.

В таблице 1 представлены данные по динамике стоимостных объемов импорта данных товаров в РФ за период 2013–2018 гг.

ТАБЛИЦА 1. Статистика по импорту товаров, млн. долл. США

Наименование товара	Код ТН ВЭД ЕАЭС	Период					
		2013	2014	2015	2016	2017	2018
Обувные товары	6401	36,02	25,54	11,80	10,89	15,56	11,80
	6402	1402,23	999,49	639,69	587,24	710,94	575,56
	6403	2155,57	1853,72	1160,01	1103,63	1475,36	1263,54
	6404	649,24	536,27	424,32	503,00	634,02	499,57
	6405	34,75	35,04	18,70	28,64	30,82	27,89
	Итого:	4277,81	3450,06	2254,51	2233,39	2866,71	2378,36

На основе нормативно-правовой информации можно провести сравнение товаров из меха (товарная позиция 4303) и обувных товаров (товарные позиции 6101–6105) в аспекте функционирования системы маркировки товаров (таблица 2).

ТАБЛИЦА 2. Сравнение товарных позиций 4303 и 6101–6105 в аспекте функционирования системы маркировки товаров

Критерий	Товарная позиция 4303	Товарные позиции 6101–6105
Количество классификационных признаков [6]	Малое (вид меха; одежда или принадлежность)	Большое (материал, область использования, конструктивные особенности, наличие отдельных элементов и используемых материалов, длина стельки; обувь является мужской или женской)
Потребительская тара [7, 8, 9, 10]	– Коробки из картона коробочного марок А, Б, В, Г по ГОСТ 7933. – Коробки из гофрированного картона по ГОСТ 7376. – Пакеты из полимерных и комбинированных материалов, из плёнки целлюлозной по ГОСТ 7730. – Пакеты бумажные.	– Коробки из коробочного картона марок А, Б и В по ГОСТ 7933 и картона хром-эрзац по нормативно-технической документации). – Картонные пачки (ГОСТ 12303). – Бумажные пакеты или пакеты из полимерных материалов (ГОСТ 12301).
Варианты маркировки КИЗ	Накладной, вшивной, клеевой. Маркировка наносится на сам товар.	Потенциально маркировка может наноситься на упаковку, так как обувь рассматривается попарно. Предпочтительный вариант маркировки: клеевой

Критерий	Товарная позиция 4303	Товарные позиции 6101–6105
Тип памяти	Write Once Read Many (WORM)	Потенциально маркировка должна быть осуществлена единожды, поэтому предпочтительный тип памяти: WORM
Угрозы информационной безопасности	Уничтожение RFID-метки и КИЗ, создание дубликата RFID-метки, атака «человек-посередине» и фишинговая атака через создание дубликата КИЗ	

Исходя из сравнения, можно сделать следующие выводы.

Во-первых, RFID-метка, которая может применяться в проекте по маркировке обувных товаров, должна содержать больший объем памяти, чтобы не нее можно было записать информацию, которая позволит однозначно сделать вывод о классификационном коде ТН ВЭД ЕАЭС товара, а также о конструктивных особенностях обуви. Больший объем памяти представляется необходимым, так как от кода будет зависеть размер уплачиваемых таможенных платежей. Если в товарной позиции 4303 практически по всем товарам установлена ставка ввозной таможенной пошлины в 10 %, то в товарных позициях 6101–6105 присутствует большее разнообразие ставок, что говорит о больших рисках нарушения информационной безопасности со стороны недобросовестных участников ВЭД. Для их снижения также необходимо использование типа метки Write Once Read Many (WORM).

Отсюда возникает риск заявления недостоверного ТН ВЭД ЕАЭС (декларирование товара прикрытия). В качестве товаров прикрытия могут выступать товары, элементы которых изготовлены из иных материалов, или товары с иными конструктивными особенностями.

Например, товаром группы риска будет Обувь прочая с подошвой из резины, пластмассы, натуральной или композиционной кожи по коду 6405901000 (ставка ввозной таможенной пошлины – 0,34 евро/пар), а товаром прикрытия – Обувь прочая с подошвой из прочих материалов по коду 6405909000 (ставка ввозной таможенной пошлины – 0,28 евро/пар).

Кроме того, существует риск того, что участник ВЭД может недостоверно декларировать обувь как детскую. Тогда ставка НДС будет снижена с 20 % до 10 %. В некоторых случаях установлены ограничения по длине стельки для детской обуви.

Еще один риск – невключение в состав таможенной стоимости, как базы для расчета таможенных платежей, лицензионных платежей за использование товарных знаков. Обувь является одним из наиболее часто подделываемых товаров [11]. В данной области доля распространения контрафактной продукции составляет 30–40 % от всего оборота [12, с. 193, 13, с. 928]. Наиболее часто подделывается обувь известных брендов [14, с. 1117].

Во-вторых, для КИЗ в проекте по маркировке обувных товаров наилучшим образом подходит клеевой вариант нанесения. С одной стороны, клеевой вариант проще заменить или уничтожить, но, с другой стороны, иные варианты нанесения менее целесообразны. Вшивной вариант менее предпочтителен, так как это потребует дублирования КИЗ на каждую обувную единицу. Потенциально может быть использован и накладной (навесной) вариант маркировки, например, таким образом, чтобы он соединял пару вместе. Однако это потребует существенных трудовых затрат при маркировке, а сама маркировка может быть закреплена недостаточно надежно. Можно также отметить, что на КИЗ должен быть расположен QR-код, который позволит потребителям получать информацию о товаре (по аналогии с изделиями из меха).

Таким образом, проект по маркировке изделий из меха полностью не будет совпадать с проектом по маркировке обувных товаров ввиду особенностей потребительской тары обуви, ввиду того, что обувь перемещается парами, а также ввиду того, что для обуви предусматривается большее количество классификационных признаков.

Подведем итоги. Среди товаров, в отношении которых планируется введение обязательной маркировки товаров в 2019 году, особое место занимают товары товарных позиций 6101–6105 или обувные товары. С 01.07.2019 станет обязательной маркировка данных товаров средствами идентификации, которыми могут стать RFID-метки. Однако уже имеющийся опыт по маркировке изделий из меха не может быть полностью перенесен на маркировку обувных товаров.

Тем не менее, для RFID-маркировки обувных товаров также будут актуальны такие угрозы информационной безопасности, как уничтожение RFID-метки и КИЗ, создание дубликата RFID-метки, атака «человек-посередине» и фишинговая атака через создание дубликата КИЗ. С учетом высоких стоимостных объемов импорта обувных товаров, а также с учетом необходимости увеличения объемов памяти метки необходимо проанализировать перспективы применения таких методов защиты метки, как изменение конструкции метки (пластмассовый корпус или *coil-on-chip*), проверку типа памяти метки, шифрование и добавление дополнительных печатных элементов защиты.

Список используемых источников

1. Распоряжение Правительства РФ от 28.04.2018 № 792-р «Перечень отдельных товаров, подлежащих обязательной маркировке средствами идентификации» // СПС «Консультант Плюс».

2. Госдума продлила обязательную маркировку меховых изделий до 2019 года [Электронный ресурс] // Regnum. URL: https://regnum.ru/news/economy/2297160.html (дата обращения 17.01.2019).

3. Лавринович А. А. Подходы к обеспечению информационной безопасности RFID-технологий // Альманах научных работ молодых ученых Университета ИТМО. Т. 1. Университет ИТМО, 2018. С. 16–18.

4. Лавринович А. А., Волошина Н. В. Модель для оценки результатов применения RFID-технологии в области внешнеэкономической деятельности // Конвергенция цифровых и материальных миров: экономика, технологии, образование. Сборник научных статей международной научной конференции. 2018. С. 193–201.

5. База данных «Таможенная статистика внешней торговли Российской Федерации» [Электронный ресурс] // Customsonline. URL: http://customsonline.ru/search_ts.html (дата обращения 18.01.2019).

6. Решение Совета Евразийской экономической комиссии от 16.07.2012 № 54 «Об утверждении единой Товарной номенклатуры внешнеэкономической деятельности Евразийского экономического союза и Единого таможенного тарифа Евразийского экономического союза» // СПС «Консультант Плюс».

7. ГОСТ 7296-81. Обувь. Маркировка, упаковка, транспортирование и хранение // АО «Кодекс».

8. ГОСТ 19878-2014 Меха, меховые и овчинно-шубные изделия. Маркировка, упаковка, транспортирование и хранение // АО «Кодекс».

9. Товароведение и экспертиза в таможенном деле. Т. I. Теоретические основы. Непродовольственные товары: учебник / С. Н. Гамидуллаев [и др.]. СПб.: Троицкий мост, 2014. 480 с.

10. Маркировка, упаковка, транспортирование и хранение обуви [Электронный ресурс] // ЗнайТовар. URL: https://znaytovar.ru/new536.html (дата обращения 18.01.2019).

11. Шахшаева Л. М. Проблемы насыщения рынка контрафактной продукцией и способы борьбы с ней // практика использования концепции маркетинга предприятиями и предпринимательскими структурами. Всероссийская научно-практическая конференция. 2017. С. 169–172.

12. Гаврилин М. С. Некоторые аспекты классификации контрафактной продукции // Научное и образовательное пространство: перспективы развития. Сборник материалов III Международной научно-практической конференции: в 2-х т. 2016. С. 190–193.

13. Шаурина О. С., Савватеева А. С. Актуальные проблемы ввоза контрафактной продукции на территорию Российской Федерации // Аллея науки. 2018. Т. 1. № 5 (21). С. 922–932.

14. Завьялов И. А. Характеристика предмета преступлений в сфере интеллектуальной собственности и потребительского рынка // Научный альманах. 2015. № 7 (9). С. 1116–1118.

Статья представлена научным руководителем,
кандидатом технических наук, доцентом Н. В. Волошиной.

УДК 530.34.013.4
ГРНТИ 28.25

МЕТОД ФУНКЦИОНАЛЬНОГО ТЕСТИРОВАНИЯ ЭЛЕКТРОННЫХ ЦИФРОВЫХ УСТРОЙСТВ И ВЫЯВЛЕНИЯ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ

В. А. Липатников, А. А. Шевченко, А. О. Сазонов

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В данной статье рассматривается подход к решению задач распознавания недекларированных возможностей в интегральных микросхемах электронных устройств на основе теории формальных языков и грамматик, и структурных методов анализа. Раскрываются вопросы функционального тестирования электронных устройств, выбора оптимальной формальной грамматики для создания лингвистического описания исследуемых недекларированных возможностей, а также структура разработанного метода распознавания.

формальные грамматики, методы распознавания, продукционная модель, алгоритм, метод.

В настоящее время в мире интенсивно развивается производство сложных электронных систем и комплексов с использованием интегральных микросхем. Большинство электронных устройств (ЭУ) содержат в себе цифровые модули – части устройства, получающие и обрабатывающие информацию в цифровой форме, в которой сигналы могут принимать конечное множество значений и описываются функцией дискретного времени. В ЭУ могут быть недекларированные возможности (НДВ) (программного обеспечения) – функциональные возможности программного обеспечения, не описанные в документации [1].

Существует противоречие между требованиями стандартов к ЭУ, а с другой стороны обзор релевантных работ [2, 3] показал, что недостатком является малая достоверность распознавания потенциальных неисправностей при уменьшении времени проведения диагностики технических систем.

Постановка задачи – разработать метод функционального тестирования и распознавания НДВ в ЭУ, позволяющий повысить достоверность распознавания потенциальных НДВ при уменьшении времени проведения функционального тестирования технических систем.

Решение

В данной статье предлагается метод распознавания наличия неисправностей и НДВ путем структурно-лингвистического тестирования, на базе которого была создана и успешно апробирована соответствующая система. Разрабатываемый метод распознавания НДВ ЭУ относится к области диагностики технических систем и может быть использован для распознавания ранее сформированных диагностических тестов технических систем (в частности – радиоэлектронной аппаратуры) различной степени сложности, а также создает возможность создания качественных диагностических тестов.

В настоящее время необходима разработка конкретных базовых элементов метода распознавания и определения параметров цифровых сигналов (формальное эталонное описание), способы синтаксического анализа. Поэтому, по существу, необходима разработка нового структурно–лингвистического метода (СЛМ) функционального тестирования, ориентированного на использование формальных грамматик (ФГ), отражающих специфику синтаксической структуры цифровых сигналов и допускающих применение ориентированных на эти подклассы ФГ эффективных методов синтаксического анализа.

В рамках данного исследования предлагается система распознавания, представленная на рис. 1.

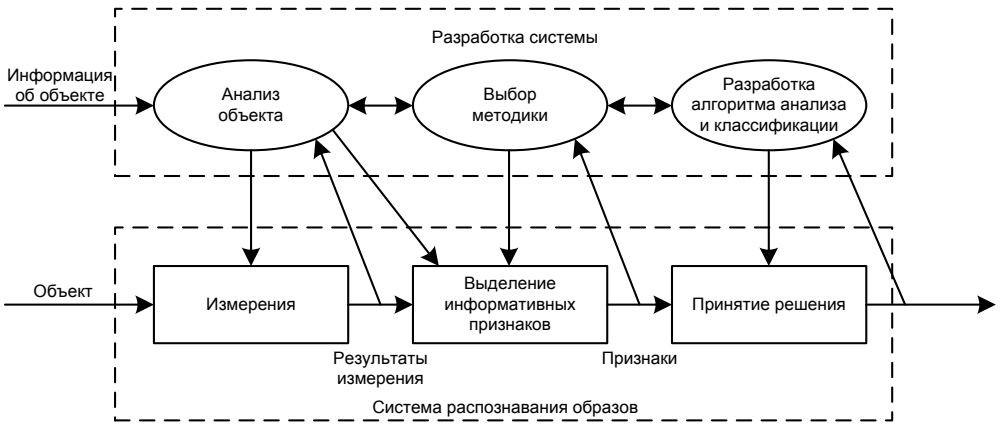


Рис. 1. Структура системы распознавания

Известно, что универсальным средством кодирования семантики информации, а также универсальным средством коммуникации является естественный язык. Этим в основном объясняется то большое внимание, которое уделяется в лингвистике и в кибернетике попыткам построить формальную модель естественного языка.

По определению [4] формальная грамматика – это синтаксическая система, записываемая в виде четверки $G = (V_N, V_T, P, S)$, где V_N – конечное непустое множество нетерминальных символов (нетерминалов); V_T – конечное

непустое множество (алфавит) терминальных символов (терминалов), причем $V_T \cap V_N = \emptyset$ и $V_T \cup V_N = V^*$; P – конечное множество упорядоченных пар (правил подстановки, продукций); S – начальный нетерминал (аксиома), $S \in V_N$. ФГ в компактной продукционной форме описывает возможные цепочки элементов (терминалов), составляющих заданный класс образов, при этом правила подстановки определяют конструктивную схему формирования этих цепочек. Таким образом, ФГ служит средством компактного задания большого числа образов распознаваемого класса сигналов с использованием конечных наборов исходных элементов и правил подстановки.

Алгоритм синтаксического анализа цифрового сигнала представлен на рис. 2.

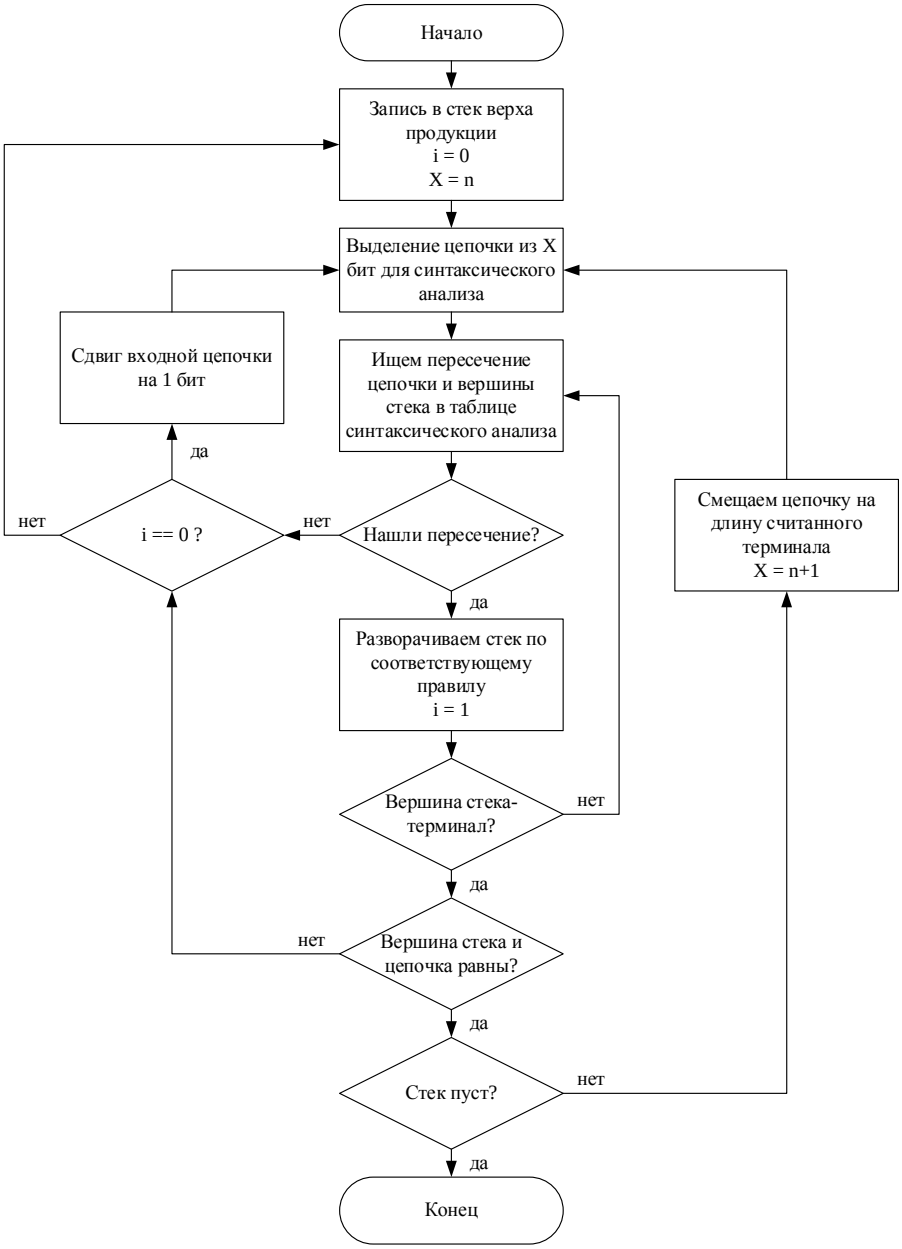


Рис. 2. Алгоритм синтаксического анализа цифрового сигнала

В качестве основных показателей эффективности, в соответствии с общими положениями теории сложности алгоритмов, рассмотрим показатели временной ($O(n)$) и емкостной ($E(n)$) сложности, где n – длина анализируемой цепочки символов. В общем случае, временная сложность предложенных методов синтаксического анализа может быть представлена следующим образом:

$$O(n) \le C_1 \left(\sum_{i=1}^{I} N_i * \left(\sum_{j=1}^{J} C_2 * z_j \right) \right),$$

где C_1 – коэффициент, характеризующий максимальное число шагов, выполняемых при распознавании цифрового сигнала;

C_2 – коэффициент, определяющий максимальное число операций при анализе одного элемента цепочки терминальных символов с использованием КСГ;

N_i – количество терминальных символов в анализируемой цепочке;

z_j – количество терминальных символов, участвующих в грамматическом разборе при анализе одного элемента цепочки.

Данный алгоритм имеет линейную вычислительную сложность, так как при грамматическом разборе применение правила подстановки укорачивает анализируемую цепочку на один терминальный символ, а коэффициенты C_1, C_2 не зависят от длины всей цепочки.

Емкостная сложность алгоритмов синтаксического анализа может быть оценена следующим соотношением:

$$E(n) = L_1 * N_i + L_2 * z_j,$$

где L_1 – коэффициент, задающий максимальное число используемых для синтаксического анализа нетерминальных элементов;

L_2 – коэффициент, определяющий максимальное число элементов, описывающих состояние цифрового сигнала.

В целом, полученные оценки временной и емкостной сложности показывают, что алгоритм синтаксического анализа имеет линейную вычислительную сложность.

Поскольку любая грамматика порождает некоторый язык, то есть множество слов надтерминальным алфавитом, то задача построения грамматик формально сводится к поиску алфавита нетерминальных символов и множества подстановок по множеству «примеров», то есть по множеству слов данного языка.

Степень достижения цели

Технический результат заключается в уменьшении времени проведения диагностики технических систем. На рис. 3 изображена зависимость количества диагностик технических систем от времени (в часах).

Из анализа графиков следует то, что метод с использованием аппарата формальных грамматик показывает наилучший результат (в среднем 2 теста в час). Это связано с тем, что формальные грамматики позволяет в компактной продукционной форме описать структуру диагностируемого модуля (системы). Метод с использованием специализированного языка «ЯСТЕК» требует больших временных затрат из-за громоздкой, хоть и ёмкой системы описания диагностических тестов. Кроме того, формирование тестов на языке «ЯСТЕК» – это длительная, сложная работа, требующая большого внимания, терпения и усидчивости. Метод, основанный на использовании эталонной модели диагностируемого изделия показал самые низкие результаты из-за ограниченной области использования данного метода, невозможности формирования тестов при отсутствии эталонных образцов изделий и недостаточной достоверности формируемых тестов.

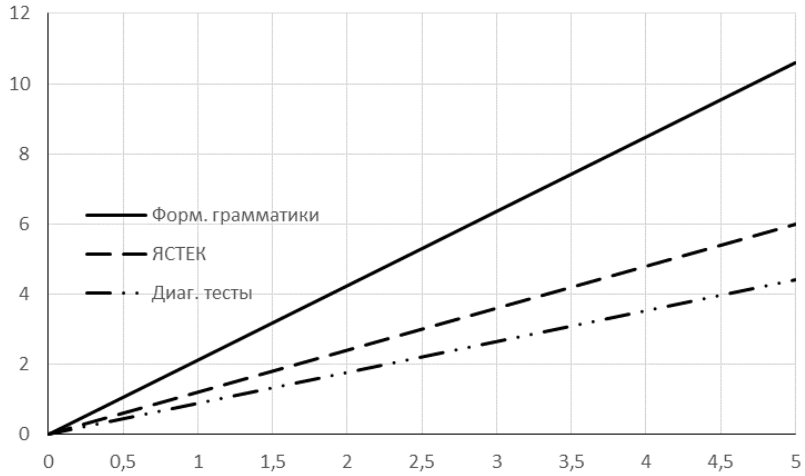


Рис. 3. Результаты проведения диагностики технических систем различными методами

Заключение

Анализ релевантных работ показал, что на данный момент не создано эффективных методик тестирования ИМС ЭУ и выявления НДВ.

Новизна предложенного метода определяется тем, что в отличие от подходов, используемых в отечественных работах, данный метод в полной мере использует порождающую мощность грамматик для описания синтаксиса распознаваемых протоколов обмена данными, что, в свою очередь, позволяет применять эффективные процедуры синтаксического анализа.

Разработка метода распознавания структуры данных цифровых сигналов ориентирована на применение контекстно-свободных грамматик.

Предложенное формальное описание протокола обмена данными на основе контекстно–свободных грамматик является основой разработки методики распознавания структуры временных диаграмм цифровых сигналов, и в целом средств распознавания и обработки рассматриваемого класса сигналов.

Список используемых источников:

1. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М.: Стандартинформ, 2007.

2. Гришкин В. М., Лопаткин Г. С., Михайлов А. Н., Овсянников Д. А. Интерфейсный метод построения моделей входных воздействий для тестирования электронных цифровых модулей // Вопросы радиоэлектроники. 2013. Вып. 1. С. 80–89.

3. Гришкин В. М., Степанов Ю. Л., Лопаткин Г. С., Большаков А. А. Подход к разработке тестов цифровых электронных модулей для автоматического тестового оборудования // Вопросы радиоэлектроники. 2013. Вып. 1. С. 89–99.

4. Хомский Н. Синтаксические структуры. В кн.: Новое в лингвистике. Вып. II. М., 1962.

УДК 004.056
ГРНТИ 81.93.29

МОДЕЛЬ ПРОЦЕССА ПРОАКТИВНОГО УПРАВЛЕНИЯ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТЬЮ СИСТЕМ КРИТИЧЕСКИХ ИНФРАСТРУКТУР СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В. А. Липатников, С. В. Торточаков, В. А. Тихонов

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Рассматривается актуальная проблема обеспечения уровня защищённости кибернетической безопасности критических инфраструктур автоматизированных систем управления и связи специального назначения. Проблема определения факторов, влияющих на уровень кибербезопаности решается путем создания модели процесса проактивного управления с использованием модуля когнитивного моделирования. Целью работы является повышение уровня кибернетической безопасности критических инфраструктур автоматизированных систем управления и связи специального назначения. В статье представлена структура модели процесса проактивного управления кибербезопасностью, реализующей выявление и оценку уязвимостей наряду с прогнозированием рисков.

кибербезопасность, защита информации, оценка рисков, показатель защищённости, проактивное управление, критические инфраструктуры, автоматизированные системы управления.

Защита критических инфраструктур является одной из важнейших проблем для всех стран. Обеспечивая стабильную работу ключевых государственных служб и систем таких, как правительственные органы и крупные производственные предприятия, критические инфраструктуры включают в себя объекты и сети, сбои и затруднения в работе которых несут негативный и непредсказуемый в плане оценки ущерба характер. Тенденция роста киберпреступности – совершения преступлений в сфере высоких технологий – усугубляется цифровой трансформацией современного общества и развитием сети Интернет. Кибербезопасность (КБ) представляет из себя набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей. КБ подразумевает достижение и сохранение свойств безопасности у ресурсов организации или пользователей, направленных против киберугроз.

Целью работы является повышение уровня кибернетической безопасности критических инфраструктур автоматизированных систем управления специального назначения (СН).

Данная информационная система (ИС) представлена моделью процесса проактивного управления, на которую влияет ряд внешних факторов, представляющих из себя возможность реализации компьютерных атак на ИС. Стоит подчеркнуть необходимость соответствия показателя защищённости требуемому значению в целях поддержания приемлемого уровня КБ (рис. 1).

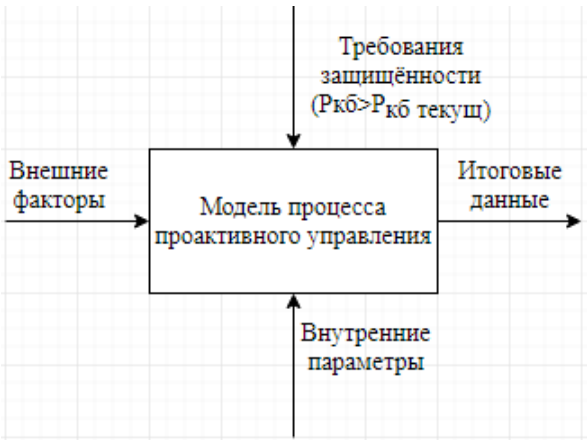


Рис. 1. Структура процесса информационной системы

Предлагается общая структура модели процесса проактивного управления КБ системы критических инфраструктур СН на основе выявления, оценки уязвимостей и прогнозирования рисков с построением когнитивных карт (КК), представленная на рис. 2.

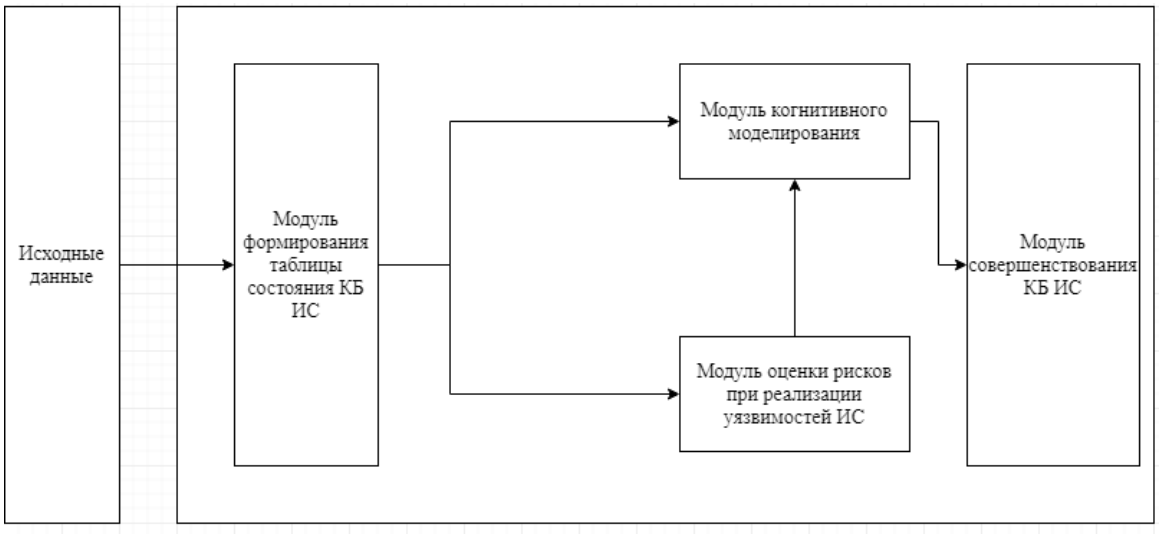


Рис. 2. Общая структура модели процесса проактивного управления КБ

Предлагаемая структура модели представляет собой совокупность процессов, выполняемых конкретными модулями. Каждый процесс происходит независимо друг от друга и выполняет конкретные задачи. Структура отражает взаимосвязь процессов управления КБ с прогнозированием уязвимостей, на основе чего формируются решения по совершенствованию системы защиты информации.

Модель состоит из ряда модулей и выполняет основную функцию повышения КБ ИС на основе анализа уязвимостей. При решении задачи моделирования предполагается, что составными частями модели процесса управления КБ ИС на основе выявления и оценки уязвимостей будут следующие модули, зависимые от аргументов согласно исходным данным:

1. Модуль формирования таблицы состояния КБ ИС $O = \{M, P_{\text{ИБ}}\}$,

2. Модуль оценки рисков при реализации уязвимостей $R = \{M, V, C\}$,

где V – массив показателей оценок уязвимости ресурсов ИС.

3. Модуль совершенствования СЗИ ИС $U = \{P_{\text{ИБ}}, V, R, C\_a\}$.

Кроме того, структура модели процесса проактивного управления КБ также содержит сегмент когнитивного моделирования, задачей которого является реализация итогового прогноза, далее поступающего в упомянутый модуль совершенствования ИС.

На рис. 3 изображен алгоритм построения и функционирования, рассматриваемой ИС. Данный алгоритм включает в себя два параллельных процесса. Первый процесс представляет собой тестирование ИС и выявление уязвимостей [2]. Второй процесс представляет собой анализ цифрового потока (ЦП) с выявлением аномалий и последующим анализом динамики действий нарушителя. На основании динамики действий нарушителя строится

модель угроз и принимаются меры по защите. Данный метод помогает защитить реальную ИС от компьютерных атак (КА), за счёт принятия рациональных мер по защите реальных и возможных уязвимостей в данной сети [3].

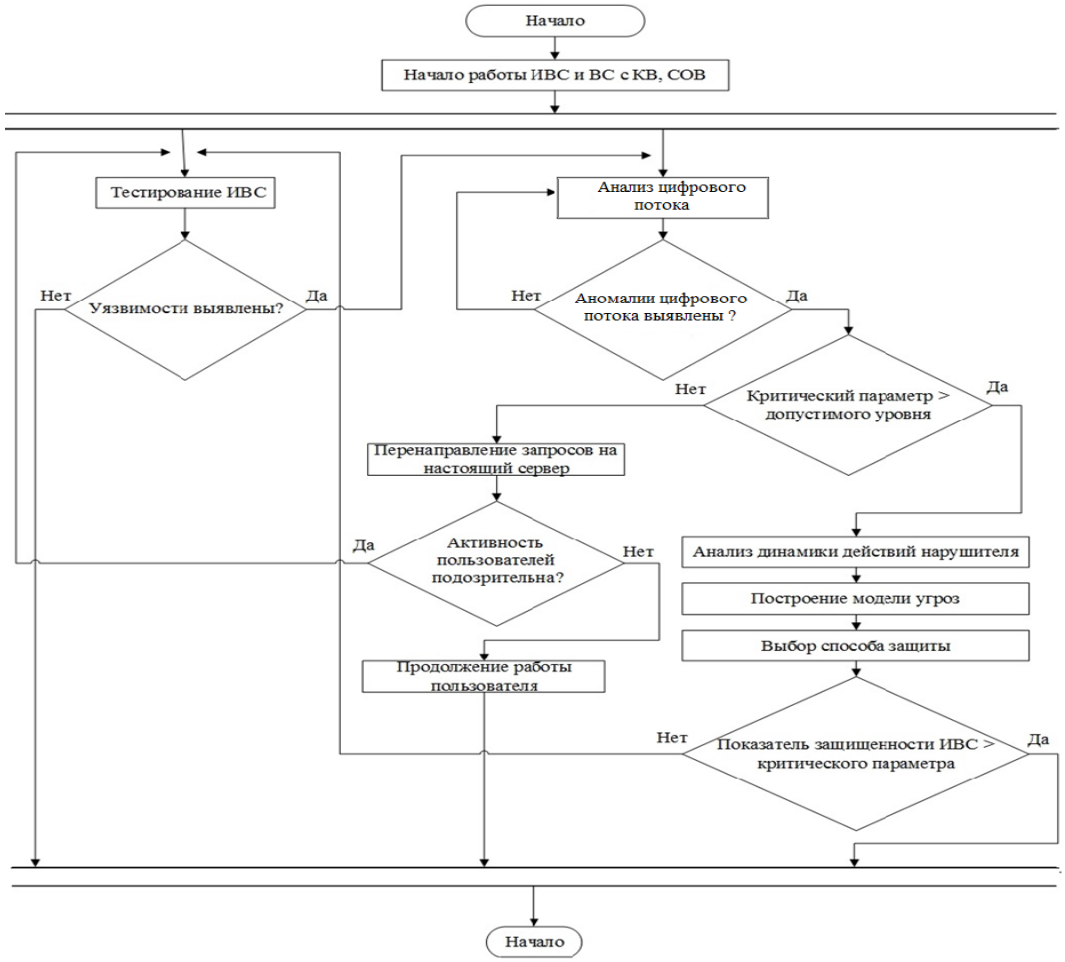


Рис. 3. Обобщенный алгоритм функционирования ИС

В ходе выявления в журнале регистрации аномальных событий действия нарушителя блокируются с оповещением администратора. На рис. 4 изображен граф событий действий нарушителя.

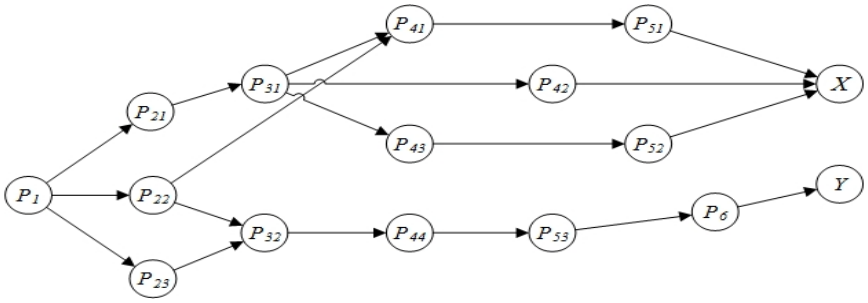


Рис. 4. Граф событий действий нарушителя

В качестве одной из возможных моделей возможно использование представления действия нарушителя как систему с переменной структурой, поведение которой на случайных интервалах времени характеризуется различными структурами и описывается вероятностными законами, при этом переход одной структуры в другую происходит в случайный момент времени в зависимости от значения фазовых координат системы.

Состояние «P_1» соответствует началу действий нарушителя. Состояние «P_{21}» соответствует событию, в котором происходит измерение характеристик ИВС путем внедрения снифера. Состояние «P_{22}» соответствует стадии, в которой проводится тестирование состояния ИС путем анализа запросов. Состояние «P_{23}» соответствует событию анализа «эхо-запросов». Состояние «P_{31}» соответствует событию анализа исходящего цифрового потока.Состояние «P_{32}» соответствует событию выявление хостов. Состояние «P_{41}» соответствует событию выявления паролей. Состояние «P_{42}» соответствует событию дешифрования информации. Состояние «P_{43}» соответствует событию, при котором несанкционированно используется авторизованный IP адрес в сети. Состояние «P_{44}» соответствует событию, при котором происходит сканирование портов. Состояние «P_{51}» соответствует событию подмены пользователя в сети. Состояние «P_{52}» соответствует событию, при которой изменяются целостность, доступность и конфиденциальность информации. Состояние «P_{53}» соответствует событию, при котором происходит анализ характеристик приложений. Состояние «P_6» соответствует режиму осуществления DDoS атак. Состояние «X» соответствует реализации угрозы хищения информации. Состояние «$У$» соответствует реализации отказа в обслуживании. Определим коэффициенты реализуемости событий (элементов графа) для определения динамики действий нарушителя, воспользовавшись методикой [4]:

$$P = \frac{(У_1 + У_2)}{20}, \quad (1)$$

где $У_1$ – коэффициент исходной защищенности;

$У_2$ – коэффициент реализации угрозы.

Время перехода из одного события в другое, зависит от коэффициента реализуемости события:

$$T_i = T_{maxj} - P_i \times T_{\text{исх}ij}, \quad (2)$$

где T_{maxj} –максимальное время реализации j-го события (T_{maxj} = 24 часа);

P_i – коэффициент реализуемости i-го события;

$T_{\text{исх}ij}$ – исходное время перехода из i-го события в j-е событие ($T_{\text{исх}ij}$ от 0 до 24 часа).

Для определения наиболее вероятного пути реализации угроз необходимо рассчитать вероятности наступления каждого из событий в графе. Поэтому воспользуемся формулой расчета вероятности наступления события *X* и *Y* при условии, что событие P_i уже совершено:

$$P = P_{(i)} + P_{(i+1)} - (P_{(i)} \times P_{(i+1)}), \quad (3)$$

где $P_{(i)}$, $P_{(i+1)}$ – вероятность наступления двух последующих событий.

Сложные сетевые конфигурации с требованиями к безопасности и надежности работы сети – в ИС приводит к задачам, которые в дальнейшем примут глобальные масштабы. ИС является высоко масштабной сетью, следовательно, она обладает факторами, которые влияют на КБ ИС. К ним относятся: сложная структура ИС, большое количество разнообразного оборудования, несовместимость платформ, ОС и ПО, отсутствие общей стратегии по применению СЗИ для всех территориально распределенных узлов ИС. Наибольшее влияние на КБ ИС оказывают такие факторы, как различная пропускная способности канала связи и неполное функционирование системы в каждый конкретный момент.

Научная новизна работы состоит в том, что анализ и управление КБ, в отличие от существующих подходов, предложено проводить с помощью построения КК исследуемого объекта.

Практическая значимость

Основная цель взаимосвязанных процессов управления событиями ИС интегрированной организации с прогнозированием уязвимостей – повышение уровня КБ за счёт обеспечения осуществления проактивного управления инцидентами и событиями безопасности. «Проактивный» означает «действующий до того, как ситуация станет критической». Предполагается, что проактивное управление КБ практически основывается на автоматических механизмах, использующих информацию об «истории» анализируемых сетевых событий и прогнозе будущих событий, а также на автоматической подстройке параметров мониторинга событий к текущему состоянию защищаемой системы.

Предложенные алгоритмы анализа и управления КБ, основанные на построении нечетких КК как для систем критических инфраструктур в целом, так и для его структурных подразделений, позволяют определить наиболее уязвимые места системы и выбрать необходимые контрмеры для снижения рисков.

Заключение

Представлена модель процесса проактивного управления КБ систем критических инфраструктур СН, содержащая модуль когнитивного моделирования, обеспечивающий учёт всех факторов влияния на конкретный прогнозируемый показатель. Получаемая когнитивная карта предоставляет результаты прогноза с вероятностью его выполнения. Далее, все данные поступают на финальный модуль, обобщающий информацию и выдающий итоговый прогноз.

Таким образом, благодаря многофункциональному и оперативному характеру работы системы в целом можно убедиться в адекватности и эффективности разработанной модели процесса проактивного управления КБ систем критических инфраструктур СН, способной решать широкий спектр задач в рамках поддержания должного уровня защищённости.

Список используемых источников

1. Котенко И. В., Саенко И. Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. 2012. Вып. 3(22). С. 84–100.

2. Котенко И. В., Саенко И. Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. Вып. 1 (24). С. 21–40.

3. Липатников В. А., Шевченко А. А., Яцкин А. Д. Метод управления безопасностью информационно-вычислительных сетей на основе выделенного сервера с контейнерной виртуализацией // Информационные системы и технологии. 2017. №4 (102). С. 116–126.

4. Кузнецов И. А., Липатников В. А., Шевченко А. А. Способ многофакторного управления безопасностью информационно-телекоммуникационной сети системы менеджмента качества предприятий интегрированных структур. М.: Вопросы радиоэлектроники. 2016. № 6. С. 23–28.

5. Карганов В. В., Костарев С. В., Липатников В. А., Лобашев А. И., Шевченко А. А. Способ защиты информационно-вычислительной сети от несанкционированных воздействий. Патент 2635256 Российская Федерация; заявитель и патентообладатель Военная академия связи имени Маршала Советского Союза С. М. Буденного; заявл. 04.05.2016; опубл. 09.11.2017.

6. Ярушева С. А., Аверкина А. Н., Федотова А. В. Модулярная модель прогнозирования временных рядов на основе нейро-нечетких сетей и когнитивного моделирования // Нечеткие системы и мягкие вычисления. 2017. Т. 12. № 2. С. 159–168. URL: https://doi.org/10.26456/fssc31.

7. Коршунов Г. И., Липатников В. А., Шевченко А. А., Малышев Б. Ю. Метод адаптивного управления защитой информационно-вычислительных сетей на основе анализа динамики действий нарушителя// Информационно-управляющие системы. 2018. № 4. С. 61–72. doi:10.31799/1684-8853-2018-4-61-72.

8. Korshunov, G. I., Lipatnikov, V. A., Tikhonov, V. A., Models and methods of information reliability and data protection // IOP Conference Series: Materials Science and Engi-

neering MIP_2019_4001. International Workshop «Advanced Technologies in Material Science, Mechanical and Automation Engineering». “MIP: Engineering-2019”. Красноярск. Февраль, 2019.

9. Korshunov, G. I., Lipatnikov, V. A., Shevchenko, A. A. Decision support systems for information protection in the management of the information network. //Fuzzy Technologies in the Industry. FTI 2018. 23–25 October, 2018. Ulyanovsk (Russia). Pp. 418–426.

10. Axelrod, R. The Structure of Decision: Cognitive Maps of Political Elites. Princeton. University Press, 1976.

УДК 621.396.969
ГРНТИ 81.93.29

СПОСОБ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНОЙ СИСТЕМЫ РАДИОМОНИТОРИНГА К ВНЕШНИМ И ВНУТРЕННИМ ВОЗДЕЙСТВИЯМ

В. А. Липатников, А. А. Шевченко

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В статье изложен способ повышения устойчивости контрольно-измерительной системы радиомониторинга к внешним и внутренним воздействиям, за счёт мониторинга уязвимостей информационной безопасности и технического состояния системы. Анализ предлагаемого способа показал повышение вероятности устойчивой работы системы и, как следствие, повышение достоверности результатов радиоконтроля.

контрольно-измерительная система радиомониторинга, информационная безопасность, показатель устойчивой работы, стохастическая сеть, преобразование Лапласа-Стилтьеса.

В связи с тем, что в настоящее время радиосвязь является наиболее дешевым видом оперативной связи между объектами, создаются контрольно-измерительной системы (КИС) радиомониторинга (РМ), которые выполняют проверку соблюдения пользователями радиочастотного спектра. [1]

Существует противоречие между требованиями стандартов к КИС РМ, а с другой стороны обзор предложений по разработке КИС РМ [2, 3] показал, что недостатком является относительно низкая достоверность результатов РМ, обусловленная вероятной возможностью появления нарушений технического состояния и защищённости КИС РМ, приводящих к искажению результатов контроля.

Постановка задачи – разработать способ повышения устойчивости КИС РМ к внешним и внутренним воздействиям, позволяющий повысить достоверность результатов РМ.

Решение

В качестве решения предлагается использовать КИС РМ, разработанную на основе [4]. В данном решении дополнительно к основным элементам системы дополнительно введён центрального пункта управления техническим состоянием (ЦПУТС), а также дополнительно в состав каждого стационарного поста мониторинга и в каждый мобильный пост мониторинга предлагается ввести пункты управления техническим состоянием.

Пункты управления техническим состоянием вышеперечисленных объектов и ЦПУТС необходимы для того, чтобы реализовать предлагаемый способ повышения устойчивости КИС РМ к внешним и внутренним воздействиям. Суть способа заключается в том, что данные объекты производят мониторинг уязвимостей информационной безопасности (ИБ) и технического состояния системы, что позволит обеспечить высокую безопасность, производительность, целостность и достоверность результатов РК.

Способ повышения устойчивости КИС РМ к внешним и внутренним воздействиям реализуется в автоматизированной системе управления (АСУ), которая включает в себя модуль планирования задач, базы данных, модуль управления КИС РМ, модуль управления РК, модуль обработки результатов РК, модуля управления техническим состоянием и ИБ, модуль мониторинга технического состояния и ИБ, оперативный модуль управления техническим состоянием и ИБ, а также АСУ мобильных и стационарных постов РК и постов РК на ЛПС. Способ позволяет обеспечить защиту КИС РМ от лиц, которым необходимо скрыть свою деятельность в области использования радиочастотного спектра. Этого удаётся достичь за счет того, что используется способ защиты от несанкционированных воздействий [5]. Алгоритм способа представлен на рис. 1.

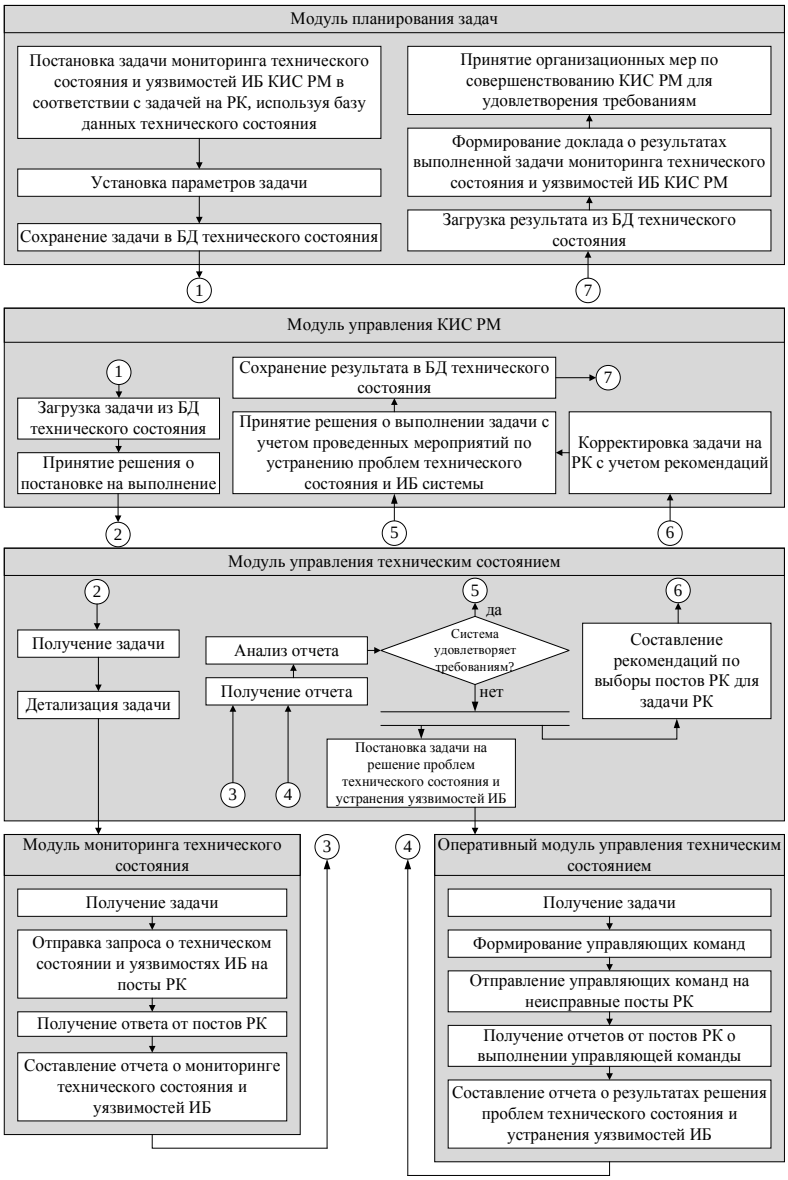


Рис. 1. Алгоритм способа повышения устойчивости КИС РМ к внешним и внутренним воздействиям

Степень достижения цели

Для удобства анализа способа повышения устойчивости КИС РМ к внешним и внутренним воздействиям составляется стохастическая сеть процесса функционирования КИС РМ, представленная на рис. 2. Стохастическая сеть в преобразованиях Лапласа-Стилтьеса позволяет получить эквивалентную функцию $h(s)$, которая равна вероятности устойчивой работы КИС РМ ($P_{раб}$), то есть:

$$P_{раб} = h(s). \quad (1)$$

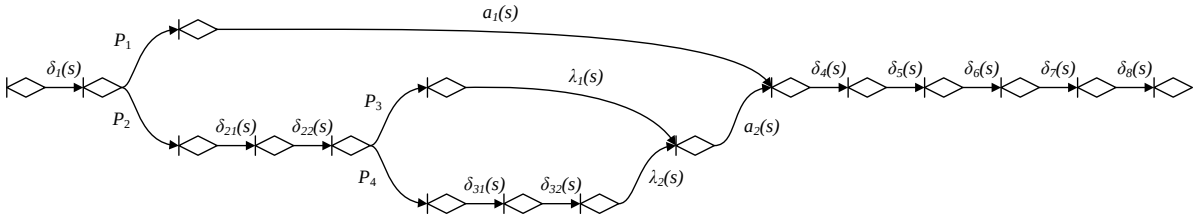


Рис. 2. Стохастическая сеть процесса функционирования КИС РМ

На рис. 2 $\delta_i(s)$ – ПЛС от функции распределения времени *i*-й последовательной операции, $\alpha_j(s)$ и $\lambda_k(s)$ – ПЛС *j*-й и *k*-й параллельных операций, а $P_{j,k}$ – вероятность выбора ветви реализации *j*-й и *k*-й ветвей. Так как предлагаемый процесс разбит на простые операции, то выполнение каждой операции независимо друг от друга во времени будут являться последовательными свершениями одного и того же события, только промежуток времени появления события для каждой операции будут различны. В связи с этим можно сделать вывод, что функции распределения времени имеют экспоненциальный закон распределения, то есть $\delta_i(s)$,$\alpha_j(s)$ и $\lambda_k(s)$ определяются по формулам:

$$\delta_i(s)=\int_0^\infty e^{-st}d[D_i(t)]=\frac{d_i}{d_i+s},\ \ \alpha_j(s)=\int_0^\infty e^{-st}d[A_j(t)]=\frac{a_j}{a_j+s},\ \ \lambda_k(s)=\int_0^\infty e^{-st}d[L_k(t)]=\frac{l_k}{l_k+s}.$$

Эквивалентная функция в ПЛС для последовательного и параллельного выполнения операций будет равна:

$$h(s)=\prod_{i=1}^{n}\delta_i(s)\sum_{j=1}^{m}P_j\alpha_j(s).$$

Стохастическая сеть в преобразованиях Лапласа-Стилтьеса позволяет получить зависимость вероятности устойчивой работы КИС РМ ($P_{\text{раб}}$) от интенсивности проведения мониторинга технического состояния и уязвимостей ИБ КИС РМ и устранения выявленных проблем технической надежности и ИБ (*s*):

$$P_{\text{раб}}(s)=\frac{d_1}{d_1+s}\cdot\left[P_1\cdot\frac{a_1}{a_1+s}+P_2\cdot\frac{d_{21}}{d_{21}+s}\cdot\frac{d_{22}}{d_{22}+s}\cdot\left(P_3\cdot\frac{l_1}{l_1+s}+P_4\cdot\frac{d_{31}}{d_{31}+s}\times\right.\right.$$
$$\left.\left.\times\frac{d_{32}}{d_{32}+s}\cdot\frac{l_2}{l_2+s}\right)\cdot\frac{a_2}{a_2+s}\right]\cdot\frac{d_4}{d_4+s}\cdot\frac{d_5}{d_5+s}\cdot\frac{d_6}{d_6+s}\cdot\frac{d_7}{d_7+s}\cdot\frac{d_8}{d_8+s}.$$

Введены следующие условия моделирования:

1. Построение зависимости $P_{раб}$ от s при вероятностях $P_1 = P_2 = P_3 = P_4 = 1$, то есть идеальный случай работы КИС РМ при бесперебойной работе всех модулей.

2. Построение зависимости $P_{раб}$ от s при вероятностях $P_1 = P_2 = 1$, $P_3 = P_4 = 0{,}5$, то есть работа модулей по устранению выявленных проблем технической надежности и ИБ и составления рекомендаций имеют сбои в работе.

3. Построение зависимости $P_{раб}$ от s при работе КИС РМ без функционирования модулей мониторинга технического состояния и уязвимостей ИБ КИС РМ и устранения выявленных проблем технической надежности и ИБ, то есть $P_2 = 0$.

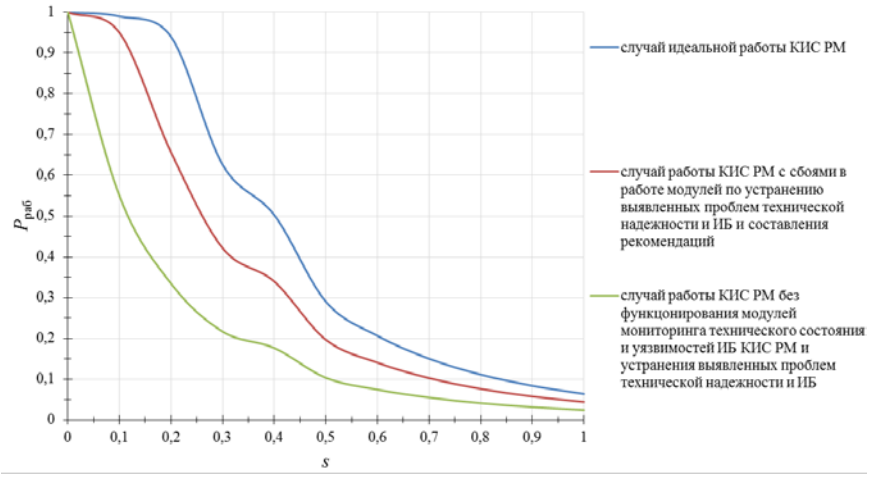


Рис. 3. График зависимости вероятности устойчивой работы КИС РМ ($P_{раб}$) от интенсивности проведения мониторинга технического состояния и уязвимостей ИБ КИС РМ и устранения выявленных проблем технической надежности и ИБ (s)

Из рис. 3 видно, что, используя предложенный способ повышения устойчивости КИС РМ к внешним и внутренним воздействиям, при бесперебойной работе модулей системы вероятность успешной работы системы РК будет выше 0,9, если мониторинг технического состояния и уязвимостей ИБ и устранение выявленных проблем первого и второго рода будут проходить с интенсивностью равной больше 0,2. Это значит, что мониторинг технического состояния и уязвимостей ИБ и устранение выявленных проблем должны проходить каждые 5 часов.

Заключение

Предложенный способ повышения устойчивости КИС РМ к внешним и внутренним воздействиям на основе мониторинга технического состояния и уязвимостей ИБ и устранения выявленных проблем технической надеж-

ности и ИБ в отличие от известных решений обеспечивают повышение достоверности результатов РК и повышают работоспособность системы РК в целом.

Моделирование процесса работы КИС РМ показывает, что использование модулей мониторинга технического состояния и уязвимостей ИБ и устранения выявленных проблем технической надежности и ИБ, повышают работоспособность системы и достоверность результатов РК. Так же исходя из моделирования можно сделать вывод, что процесс мониторинга технического состояния и уязвимостей ИБ и устранения выявленных проблем должен быть цикличным и занимать 5 часов и больше.

Список используемых источников

1. Липатников В. А., Шевченко А. А. Предложение по разработке контрольно-измерительной системы радиомониторинга на основе сетевых технологий, защищённой от несанкционированных воздействий // Метрология в радиоэлектронике. Материалы XI Всероссийской научно-технической конференции в 2-х т., Менделеево, 19–21 июня 2018 г. Менделеево: ФГУП «ВНИИФТРИ», 2018. Т. 2. С. 143–151.

2. Табунщиков Ю. А. Контрольно-измерительная система радиомониторинга ОВЧ и УВЧ диапазонов «Куница». Пат. 2340914 Российская Федерация; заявитель и патентообладатель Федеральное государственное унитарное предприятие «Радиочастотный центр Дальневосточного федерального округа» (ФГУП «РЧЦ ДФО»). – № 2007126126/09; заявл. 09.07.2007; опубл. 10.12.2008.

3. Божьев А. Н., Елизаров В. В., Наливаев А. В., Смирнов П. Л., Соломатин А. И., Царик Д. В., Шепилов А. М. Контрольно-измерительная система радиомониторинга. Пат. 2459218 Российская Федерация; заявитель и патентообладатель Общество с ограниченной ответственностью «Специальный Технологический Центр». – № 2011125014/07; заявл. 17.06.2011; опубл. 20.08.2012.

4. Земцев И. В., Карганов В. В., Кузин П. И., Липатников В. А. Шевченко А. А. Контрольно-измерительная система мониторинга. Пат. 2662726 Российская Федерация; заявитель и патентообладатель Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С.М. Буденного» Министерства обороны Российской Федерации. – № 2017140340; заявл. 20.11.2017; опубл. 30.07.2018.

5. Карганов В. В., Костарев С. В., Липатников В. А., Лобашев А. И., Шевченко А. А. Способ защиты информационно-вычислительной сети от несанкционированных воздействий. Пат. 2635256 Российская Федерация; заявитель и патентообладатель Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С.М. Буденного» Министерства обороны Российской Федерации. – № 2016117662; заявл. 04.05.2016; опубл. 09.11.2017.

УДК 004.3
ГРНТИ 50.33.03

ИССЛЕДОВАНИЯ МЕТОДОВ ВИРТУАЛИЗАЦИИ И СРАВНИТЕЛЬНЫХ ХАРАКТЕРИСТИК ГИПЕРВИЗОРОВ

В. Л. Литвинов, З. В. Таймазова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Охарактеризовано понятие виртуализации и проанализированы достоинства и недостатки данной технологии. Рассматриваются общие принципы работы с виртуальными серверами. Описаны основные функции гипервизоров. Проведено сравнение основных типов гипервизоров и приведена сравнительная таблица их характеристик.

виртуализация, гипервизоры, VMware, производительность, виртуальные машины.

Существует три способа создания виртуальных серверов: полная виртуализация, паравиртуализация и виртуализация на уровне операционной системы. Физический сервер называется хостом, а виртуальные серверы – гостевыми. Виртуальные серверы ведут себя так же, как и физические машины. Серверная виртуализация позволяет делить ресурсы одной физической вычислительной системы для работы нескольких процессов, каждый из которых использует отведенные ему ресурсы для выполнения своего набора задач.

Полная виртуализация с использованием специального программного обеспечения называется гипервизором. Гипервизор напрямую взаимодействует с центральным процессором и дисковым пространством физического сервера. Он служит платформой для операционных систем – виртуальных серверов. Гипервизор обеспечивает полную независимость и автономность каждого виртуального сервера для других виртуальных серверов, работающих на том же физическом хосте. Каждый гостевой сервер имеет свою собственную операционную систему – может случиться так, что один гостевой сервер работает в Linux, а другой – в Windows.

Гипервизор контролирует ресурсы физического сервера. В процессе применения виртуальных серверов гипервизор распределяет ресурсы физической машины между виртуальными серверами. Для гипервизора требуется обработка данных, что означает, что часть вычислительной мощности физического сервера и связанных ресурсов должна быть зарезервирована для самой программы гипервизора. Это может оказать негативное влияние на общую производительность сервера и замедлить работу приложения.

Существует два типа гипервизоров [1]. Первый тип работает на аппаратных средствах (*bare-metal*), а второй устанавливается поверх уже существующей операционной системы (рис.).

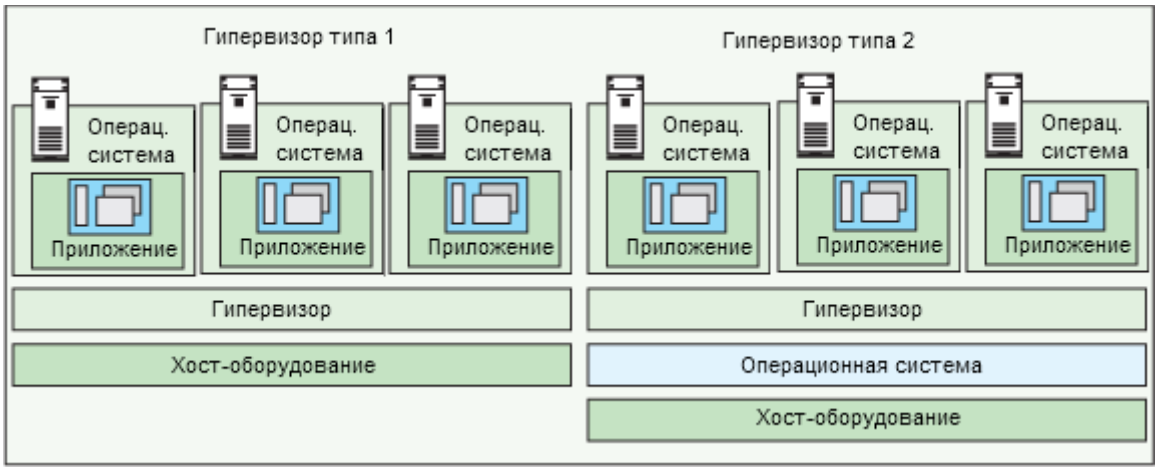


Рисунок. Типы гипервизоров

Несмотря на то, что у данной технологии множество плюсов, она все же обладает некоторыми недостатками. Один из них – дополнительные расходы. Для внедрения гипервизора в уже существующую инфраструктуру придется вкладывать средства в программное обеспечение для виртуализации и дополнительное оборудование.

Помимо дополнительных расходов, понадобятся ресурсы на обучение ИТ-персонала, который будет работать с новой технологией. На стороне пользователя виртуальная среда будет работать аналогично физической среде.

Виртуализация серверов экономит место за счет консолидации. Обычной практикой является выделение каждого сервера для одного приложения. Если несколько приложений используют небольшую вычислительную мощность, сетевой администратор может объединить несколько компьютеров в один сервер, на котором работает несколько виртуальных сред. Для компаний, имеющих сотни или тысячи серверов, потребность в физическом пространстве может значительно снизиться.

Виртуализация серверов позволяет компаниям применять избыточность без приобретения дополнительного оборудования. Резервирование означает запуск одного и того же приложения на нескольких серверах. Это мера безопасности и, если по какой-либо причине происходит сбой сервера, его место может занять другой сервер, на котором работает то же приложение. Это сводит к минимуму любые перерывы в обслуживании. Не имеет смысла создавать два виртуальных сервера, выполняющих одно и то же приложение, на одном физическом сервере. В случае сбоя физического сервера

оба виртуальных сервера также могут выйти из строя. В большинстве случаев сетевые администраторы создают избыточные виртуальные серверы на разных физических машинах.

Одними из самых популярных гипервизоров на данный момент являются VMware ESXi и Microsoft Hyper-V, которые относятся к первому типу гипервизоров и Oracle VirtualBox, который относится ко второму типу [2].

ТАБЛИЦА. Сравнение типов гипервизоров

	VMware ESXi	Oracle VirtualBox
Тип гипервизора	1	2
Хостовый ЦПУ	x86, x86-64	x86, x86-64
Гостевой ЦПУ	x86, x86-64	x86, x86-64 (with Intel VT-x or AMD-V, and VirtualBox 2 or later)
Хостовая ОС	–	Windows, Linux, macOS, Solaris, FreeBSD, eComStation
Гостевая ОС	Windows, Linux, Solaris, FreeBSD, OSx86 (as FreeBSD), virtual appliances, Netware, OS/2, SCO, BeOS, Haiku, Darwin, others: runs arbitrary OS	DOS, Linux, macOS, FreeBSD, Haiku, OS/2, Solaris, Syllable, Windows, and OpenBSD (with Intel VT-x or AMD-V, due to otherwise tolerated incompatibilities in the emulated memory management)
Основные функции	Консолидация серверов, непрерывность обслуживания, разработка/тестирование, облачные вычисления, критически важные для бизнеса приложения	Рабочая станция для бизнеса, консолидация серверов, непрерывность обслуживания, разработчик, любитель

Виртуальные серверы предлагают программистам изолированные, независимые системы, в которых они могут тестировать новые приложения или операционные системы. Вместо того чтобы покупать выделенную физическую машину, сетевой администратор может создать виртуальный сервер на существующем хосте. Поскольку каждый виртуальный сервер независим от всех других серверов, программисты могут запускать программное обеспечение, не беспокоясь о влиянии на другие приложения [3].

Серверное оборудование со временем устареет, и переключение с одной системы на другую может оказаться затруднительным. Чтобы продолжать предлагать услуги, предоставляемые этими устаревшими системами, сетевой администратор может создать виртуальную версию оборудования на современных серверах. С точки зрения приложения ничего не изменилось. Программы работают так, как будто они все еще работают на старом

оборудовании. Это может дать компании время на переход к новым процессам, не беспокоясь о сбоях оборудования, особенно если компания, выпустившая устаревшее оборудование, больше не существует и не может исправить неисправное оборудование.

Новая тенденция в виртуализации серверов называется миграцией. Миграция означает перемещение серверной среды из одного места в другое. С помощью подходящего аппаратного и программного обеспечения можно перемещать виртуальный сервер с одного физического компьютера в сети на другой. Первоначально это было возможно, только если обе физические машины работали на одном оборудовании, операционной системе и процессоре. Теперь возможно перенести виртуальные серверы с одной физической машины на другую, даже если на обеих машинах установлены разные процессоры, но только если процессоры поставляются от одного и того же производителя.

Список используемых источников

1. IBM developerWorks Россия. Гипервизоры, виртуализация и облако. [Электронный ресурс]. URL: https://www.ibm.com/developerworks/ru/library/cl-hypervisorcomparevmwareesx, свободный. Яз. рус. (дата обращения 27.02.2019).

2. Comparison of platform virtualization software [Электронный ресурс] / Википедия – свободная энциклопедия. URL: https://en.wikipedia.org/wiki/Comparison_of_platform_virtualization_software.

3. Джонс, Тим М. Виртуализация для встроенных систем. Архитектура и возможности гипервизоров для встраиваемых устройств [Электронный ресурс] // DeveloperWorks®. URL: http://www.ibm.com/developerworks/ru/library/l-embedded-virtualizion/. (дата обращения 27.02.2019).

УДК 004.942
ГРНТИ 28.17.31

ИССЛЕДОВАНИЕ МЕТОДОВ АНАЛИЗА IT-ИНФРАСТРУКТУРЫ КОМПАНИИ

В. Л. Литвинов, А. В. Фадеева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Проанализированы оценки и перспективы развития мирового и российского рынков информационных технологий. Описаны основные направления развития IT-инфраструктуры компаний. Сформированы решения по взаимодействию IT-компании с клиентами. Предложены идеи для качественной и прибыльной реализации IT-инфраструктуры компании с целью повышения уровня обслуживания клиентов.

информационные технологии, IT-инфраструктура, управление взаимоотношениями с клиентами.

IT-инфраструктура предприятия – это комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации [1]. Ценность информации определяется степенью ее полезности для владельца. Обладание истинной (достоверной) информацией дает ее владельцу определенные преимущества. Информация, искаженно представляющая действительность (недостоверная информация), может нанести владельцу значительный материальный и/или моральный ущерб.

Анализ ИТ-инфраструктуры – это инвентаризация, исследование и оценка всех элементов информационной системы предприятия или организации.

Инициировать анализ может необходимость в модернизации цифровых сетей компании, периферийного оборудования или составных частей структуры безопасности системы.

Наиболее востребован профессиональный анализ ИТ-инфраструктуры предприятия там, где в силу определенных причин необходимо:

- узнать, в какой степени жизнеспособна существующая на конкретный момент времени информационная система;
- понять, как наиболее эффективно использовать существующие ресурсы;
- получить конкретные рекомендации по исправлению существующих ошибок;
- определить план дальнейшей модернизации ИТ инфраструктуры.

Отметим, что анализ или ИТ аудит вычислительной системы – это непременное условие при заключении соглашения между организацией-клиентом и независимой компанией, предоставляющей услуги ИТ аутсорсинга.

Как правило, стандартная IT-инфраструктура состоит из следующих компонентов:

- Аппаратное обеспечение: серверы, компьютеры, центры обработки данных, коммутаторы, концентраторы, маршрутизаторы и другое оборудование.
- Программное обеспечение: планирование ресурсов предприятия (ERP), управление взаимоотношениями с клиентами (CRM), производительность приложений и многое другое.
- Вычислительная сеть: подключение к сети, подключение к Интернету, брандмауэр и безопасность.

• Человеческий ресурс: пользователи-люди, такие как сетевые администраторы (NA), разработчики, дизайнеры и конечные пользователи, имеющие доступ к любому IT-устройству или услуге, также являются частью IT-инфраструктуры, особенно с появлением ориентированной на пользователя разработки IT-услуг.

За последние пять лет наблюдается рост распространенности недорогих альтернатив с открытым исходным кодом. Открытый исходный код стал предпочтительной платформой для разработки новых технологий. В прошлом разработчики программного обеспечения публиковали программное обеспечение с открытым исходным кодом, которое не приносило прибыли, но теперь компании используют программное обеспечение с открытым исходным кодом для увеличения своей значимости и доли на рынке. 78 % компаний используют решения с открытым исходным кодом, а 64 % участвуют в проектах с открытым исходным кодом, что свидетельствует об увеличении числа открытых программных платформ для разработки приложений.

Соединенные Штаты являются крупнейшим рынком технологий в мире, составляя 31 % от общего объема, или примерно 1,6 триллиона долларов США на 2019 год. В США, как и во многих других странах, на сектор технологий приходится значительная часть экономической активности. Несмотря на размер рынка США, большинство расходов на технологии (69 %) происходит за его пределами.

В век новых технологий самый высокий спрос приходится на оборудование, предназначенное для обеспечения высокоскоростной работы пользователя с обработкой данных. Например, используются облачные хранилища, где данные хранятся на многочисленных распределённых в сети серверах. Данные хранятся и обрабатываются в так называемом «облаке», которое представляет собой, с точки зрения пользователя, один большой виртуальный сервер. Чтобы обеспечить работоспособность виртуального сервера, также необходимо наличие физического оборудования с высокими ресурсами производительности.

От потребности использования оборудования растет и спрос на оказание IT-услуг, связанных с установкой, обучением, интеграцией и обслуживанием. Компании поддерживают IT-инфраструктуру как за счет собственных работников, так и прибегают к помощи со стороны аутсорсинга. В связи с чем можно выделить данное направление одним из перспективных в сфере развития мирового и российского рынков IT.

Чтобы пользователь имел возможность взаимодействовать с внедряемым оборудованием, необходимо наличие программного обеспечения (ПО), ежегодный рост которого увеличивается на 6 %. Помимо ПО, больше половины общего объема рынка состоит из приложений для мобильных устройств и средств разработки. Разработка ПО под нужды заказчика ста-

новится более популярной в связи с развитием мобильных технологий, систем аналитики, интернета вещей и искусственного интеллекта. Наиболее быстро развивается категория приложений для организации сотрудничества, в частности, решений для корпоративных социальных сетей и обмена файлами: их объем ежегодно увеличивается более чем на 20 %. Категория решений для управления базами данных и аналитики также динамично развивается с годовым ростом более чем на 8%. Высокий спрос остается на решения для управления ресурсами предприятия и взаимоотношениями с клиентами, а также решениями безопасности.

Оценки агентств, исследующих информацию о рынке IT и его развитии, очень часто отличаются друг от друга. Связано это с тем, что отличаются подходы к анализу и исследованию рынка, а также из-за различий в методологиях проведения расчётов.

Нельзя отрицать тот факт, что обслуживание клиентов важно для малого или среднего бизнеса. Качество этой услуги будет либо повышать, либо снижать лояльность клиентов к бренду и бизнесу. В условиях экономического спада клиенты имеют больше альтернатив, чем когда-либо. Бизнес, который реагирует на вопросы клиентов, жалобы или другие потребности, может получить явное конкурентное преимущество. Вот почему так важно понимать, как новые технологии могут помочь предвидеть потребности клиентов, адаптировать бизнес-процессы для лучшего обслуживания клиентов и, в конечном итоге, повысить эффективность бизнеса – последние, из которых могут снизить затраты.

Существует несколько основных областей, в которых технологии могут помочь обеспечить ключевые преимущества для бизнеса в обеспечении лояльности клиентов за счет улучшения обслуживания:

- *Веб-сайты.*

Предоставление разделов на сайте, где клиенты могут отвечать на свои вопросы или искать ответы от других.

- *Электронный адрес.*

Использование электронной почты, как способ улучшения обслуживания клиентов и более быстрого реагирования на определенные потребности или запросы о помощи.

- *Программного обеспечения.*

Лучшее управление отношениями с клиентами с помощью более сложных инструментов сбора данных, таких как программное обеспечение для управления отношениями с клиентами.

- *Давать клиентам то, что они хотят и когда они этого хотят.*

Целью бизнеса с точки зрения взаимодействия с клиентами является формирование лояльности. Нет лучшего способа сделать это, чем предлагать качественные продукты и услуги и реагировать на запросы клиентов.

Но поскольку на рынке появились новые технологии, облегчающие предоставление услуг клиентам, они также могут увеличить количество каналов, через которые организация взаимодействуете с клиентами, и сложность этих взаимодействий. Организации, которые хотят использовать технологии для повышения качества обслуживания своих клиентов, должны сосредоточиться на следующем:

- *Управление данными и аналитика.*

Использование данных, полученных от клиентов, для анализа их предпочтений.

- *Инсайт-ориентированный маркетинг.*

Получение информации о бизнесе из данных клиентов, для более эффективной ориентации на маркетинг.

- *Автоматизация маркетинга.*

Оптимизация и автоматизация бизнес-процессов для повышения эффективности и снижения затрат.

- *Оптимизация самообслуживания.*

Поиск способов взаимодействия клиентов с вашим бизнесом, когда они захотят.

- *Эффективность рабочей силы.*

Для поощрения сотрудников необходимо использовать новые способы улучшения обслуживания клиентов, предоставляя инструменты и обучение для лучшего обслуживания.

Модели использования информационной системы могут быть разными, поэтому оценка данных и их анализ должны проводиться при помощи различных инструментов. Оценка данных происходит на соответствие стандартам и практикам, среди которых наиболее значимыми являются [2]:

- CobiT и IT Governance;
- Val IT и ITSM;
- ITIL, PMBok и Prince2.

Список используемых источников

1. Аудит IT-инфраструктуры предприятия: цели, задачи, реализация. [Электронный ресурс]. URL: [http://csaa.ru/audit-it-infrastruktury-predprijatija-celi-zadachi]. (дата обращения 27.02.2019).

2. Анализ ИТ и информационной инфраструктуры. [Электронный ресурс]. URL: https://helpit.me/articles/analiz-it-i-informacionnoi-infrastruktury. (дата обращения 27.02.2019).

УДК 67.05
ГРНТИ 28.17.19

МОДЕЛИРОВАНИЕ И ВИЗУАЛИЗАЦИИ ОПЕРАТИВНОЙ ОБСТАНОВКИ

П. В. Макаров, С. А. Иванов

Военная академия связи им. Маршала Советского Союза С. М. Будённого

Моделирование оперативной обстановки востребовано при пользовании интерактивного комплекса для визуализации оперативной обстановки. Данный комплекс позволяет моделировать различные варианты боевых действий с перераспределением целей для подразделений; решать ряд ситуационных задач, в том числе и за противника. Он позволяет планировать развертывание группировок войск, исходя из результатов решения динамических задач.

оперативная обстановка, моделирование, боевые действия.

Оперативная обстановка – это совокупность условий, которые прямо или косвенно влияют на процесс борьбы государственной безопасности с противником, определяют направления этой борьбы и выбор используемых в ходе ее сил, средств и методов.

Оперативная обстановка включает в себя 3 основные группы условий:

1. Деятельность противника (объекты, цели, силы, средства и т. п.);
2. Собственные возможности государства (имеющиеся средства и их готовность к применению);
3. Общие условия для обеих сторон (природные, свойства местности и т. п.).

Для того чтобы показать и визуализировать первые две основные группы условий оперативной обстановки на рельефе местности, где будут проходить действия, необходимо создание и размещение объектов (моделей), которые можно перемещать. Для создания таких моделей необходимо их проектирование в программных продуктах САПР и дальнейшая их печать на 3D принтере.

В 2015 году промышленная 3D печать находилась на переломном этапе, мейнстримом и большой дорогой в будущее.

По мере расширения ассортимента печатаемых материалов будет расти число компаний. Помимо основных пластмасс и фоточувствительных смол, они уже включают керамику, цемент, стекло, многочисленные металлы и металлические сплавы, а также новые термопластичные композиты, насто-

янные на углеродных нанотрубках и волокнах. Прямые затраты на производство товаров с помощью этих новых методов и материалов часто выше, большая гибкость, обеспечиваемая аддитивным производством, означает, что общие затраты могут быть существенно ниже.

С этим революционным сдвигом, менеджеры должны теперь заниматься стратегическими вопросами на трех уровнях:

Во-первых, продавцы материальных продуктов должны спросить, как их *предложения* могут быть улучшены, будь то сами по себе или конкурентами. Изготовление объектного слоя за слоем, согласно цифровому «чертежу», загруженному на принтер, позволяет не только неограниченную настройку, но и более сложные конструкции.

Во-вторых, промышленные предприятия должны пересмотреть свою *деятельность.* Поскольку аддитивное производство создает множество новых вариантов того, как, когда и где изготавливаются продукты и части.

В-третьих, лидеры должны учитывать стратегические последствия, поскольку все коммерческие *экосистемы* начинают формироваться вокруг новых реалий трехмерной печати.

На 2018 год технический прогресс привел к резкому повышению эффективности и расширению применения в самых различных областях. Новые 3D принтеры выпускают продукцию гораздо быстрее и дешевле, а изделия, которые появляются из них, требуют меньше работы, чем ранними 3D-принтерами.

Изготовители могут выбрать от гораздо шире ряда их, включая высокотехнологичные сплавы для частей реактивного двигателя и других продуктов с требовательными требованиями к представлению. Композиты, такие как очень прочные пластмассы, наполненные стекловолокном, углеродным волокном и углеродными нанотрубками, могут заменить металлы во многих случаях.

Новые 3D принтеры могут печатать электронные схемы и компоненты, такие как антенны и датчики, непосредственно на стенах объектов. Это уменьшает потребность для агрегата, освобождает вверх по космосу внутри продукты, и улучшает электронное внедрение всего продукта, уменьшая отход изготавливаемого и увеличивая качество.

Для решения третьего условия создания оперативной обстановки, необходимо создания рельефа местности, для дальнейшего использования его, как оперативную карту и размещения на ней моделей, напечатанных на 3D принтере.

Для создания рельефа местности, необходимо выбрать место оперативной обстановки с помощью базы данных электронных карт (например, ГИС «Панорама») и конвертируем данную местность в матрицу высот рельефа местности.

Матрица высот рельефа местности строится по информации объектов карты, имеющих абсолютную высоту или 3D-метрику. Она используется в таких задачах анализа рельефа, как построение профилей и зон видимости, вычисление длины и площади объектов с учётом рельефа, расчёт объёмов земляных работ, моделирование зон затопления, определение направлений склонов, формирование трёхмерной карты местности и других [1]. Матрица высот рельефа позволяет оценить спектр высот (статистику поверхности) заданного участка местности, получить отмывку рельефа в виде растра [2].

Для построения и анализа поверхностей может использоваться TIN (*Triangulated Irregular Network*). TIN может представлять собой рельеф местности или поверхность, отражающую изменение заданной характеристики. TIN-модель рельефа представляет собой многогранную поверхность – нерегулярную сеть треугольников, вершинами которых являются исходные опорные точки, а также точки метрики структурных линий (хребты, линии водотока, автомагистрали и т. п.) и площадей заполнения постоянным значением (водные поверхности с постоянной высотой). Исходные точки для построения TIN-модели могут располагаться с переменной плотностью в зависимости от изменений формы моделируемой поверхности, что позволяет создать эффективную и точную модель.

Плоское отображение TIN-модели рельефа выполняется с использованием палитры матрицы высот. В схематичном виде TIN-модель отображается рёбрами составляющих её треугольников, при этом простые рёбра, рёбра структурных линий и площадей заполнения имеют разные цвета.

TIN-модель применяется в задачах анализа рельефа местности – построение профилей и зон видимости, вычисление длины и площади объектов с учётом рельефа, расчёт объёмов земляных работ, моделирование зон затопления, определение направлений склонов, формирование трёхмерной карты местности [2].

Для создания рельефа местности используется фрезерный станок с числовым программным управлением (ЧПУ), что позволяет получить точные переходы рельефа местности. Фрезерный ЧПУ станок позволяет существенно увеличить скорость обработки. Показатель производительности увеличивается по причине того, что при ручной обработке оператор тратит много времени на измерения и другие процессы. Повышается показатель точности обработки. При изготовлении современных станков, которые работают под управлением ЧПУ, соблюдается высокая точность позиционирования всех узлов относительно друг друга. За счет этого отклонения размеров составляет всего несколько долей миллиметра [3]. Минимизируется объем выполняемых ручных работ. При модернизации производственных линий или при создании новых установка станков ЧПУ уменьшается количество обслуживающего персонажа. Один оператор сможет обслужить несколько станков, за счет чего существенно снижаются затраты организации.

На подготовку заготовки к обработке требуется намного меньше времени. Современные фрезеровальные станки могут самостоятельно изменять положения заготовки по нескольким осям.

Используемый материал – экструдированный пенополистирол (пеноплекс). Широкое распространение изделий из пеноплекса объясняется не только ценными физическими свойствами, но и лёгкой обработкой резанием (практически без отходов и пыли). Причём резка пеноплекса с успехом может осуществляться как ручным инструментом, так и автоматическими станками. Пеноплекс различают по плотности: чем плотность выше – тем меньше зерна и, как следствие, качество поверхности после обработки.

Такая разработка оперативной обстановки позволяет решать любые оперативные задачи на любом участке рельефа местности с использованием моделирования всех необходимых объектов.

Список используемых источников

1. Геоинформационная система «КАРТ 2005 ВЕРСИЯ 12» (ГИС «Панорама x64»). Руководство оператора. ПАРБ.00046-03 34 01, 2018. 143 с.

2. Геоинформационная система «КАРТА 2008». Обработка матриц и TIN-моделей. Руководство пользователя. Ногинск, 2008. 28 с.

3. Глебов И. Т. Учимся работать на фрезерном станке с ЧПУ: учебное пособие. Екатеринбург: УГЛТУ, 2015. 115 с. : ил. Библиогр.: с. 111–112.

УДК 004.772
ГРНТИ 50.43.19

АКТУАЛЬНЫЕ ВОПРОСЫ АВТОМАТИЗИРОВАННОЙ РАЗРАБОТКИ (ОБРАБОТКИ) ДОКУМЕНТОВ В ОБЩЕМ ПРОЦЕССЕ ПЛАНИРОВАНИЯ СВЯЗИ

А. С. Мамончикова, В. П. Поликанов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается сущность и содержание задач планирования ведомственными службами связи. Обосновывается актуальность вопроса путей совершенствования процесса планирования путём создания системы автоматизированной разработки документов по связи. Формулируются требования к рассматриваемой системе на основе особенностей управления системой и принимаемыми решениями по планированию связи.

планирование связи, автоматизация процессов, система автоматизированной разработки документов по связи.

О месте и роли планирования связи в общем процессе управления связью можно судить из анализа функций управления, которые правомерно рассматривать как относительно однородные по некоторым признакам действия должностных лиц (ДЛ), направленные на достижение частной цели управления. Группирование задач управления связью по периодам функционирования объектов управления и связанной с ними деятельностью ДЛ позволяет определить три основные, относительно самостоятельные, функции управленческой деятельности, соответствующие основным составляющим организации связи (рис. 1).

Рис. 1. Содержание управленческой деятельности должностных лиц по связи

Рис. 1 дает наглядное представление о месте планирования как этапа управления связью. Планирование, как деятельность ДЛ по решению комплекса задач, направленных на определение способов построения и обеспечения функционирования системы связи, разработку необходимых документов по связи, постановку задач, является первым, наиболее сложным, трудоемким и ответственным периодом управленческой деятельности ДЛ. От того, насколько обоснованно будет принято решение на построение и организацию функционирования системы, насколько правильно, точно и полно отработаны документы по связи, определены и своевременно дове-

дены задачи структурным объектам, во многом зависит качество и успешность решения задач обеспечения связи. Этим определяется роль планирования связи во всем комплексе управленческих задач.

В настоящее время вследствие внедрения в системы связи новых сетевых и информационных технологий, усложнения средств, и комплексов связи и автоматизации, увеличения их количества и типажа, а также других факторов возросли объем и сложность информации, необходимой для решения задач управления связью. Следовательно, значительно повысились требования к оперативности управления связью, качеству и обоснованности принимаемых решений. Иными словами, совершенствование системы управления связью, в конечном счете, сводится к сокращению длительности цикла управления с одной стороны, и повышению качества управляющих воздействий с другой. Необходимым условием выполнения этих требований должно быть согласование двух процессов:

- повышение производительности органов управления;
- повышение производительности системы связи по передаче и переработке информации.

Все это в полной мере относится к планированию связи. Из всего вышесказанного очевидно вытекает необходимость автоматизации процесса планирования связи, а, следовательно, создания автоматизированной информационной системы планирования связи.

Информационные потребности различных конечных пользователей пересекаются. Использование локальных массивов приводит к значительному дублированию информации, что существенно снижает уровень ее достоверности, усложняет процедуры обновления данных, приводит к неоправданному увеличению объемов памяти, необходимой для хранения информации.

Функции создания и ведения информационного фонда, предоставления нужной информации пользователям являются общими для разных задач. В настоящее время эти функции не отделены от других функций по обработке данных. Кроме того, желательно обеспечить независимость прикладных программ от изменений состава аппаратурных средств и изменений в информационной базе. В связи с тем, что данные дублируются в разных массивах, затруднено обеспечение требуемого уровня безопасности.

Перечисленные недостатки существующей технологии обработки информации не позволяют выполнить требования по оперативности, адекватности, безопасности и ресурсопотреблению, предъявляемые системой планирования связи.

Решение этой проблемы – создание интегрированной базы данных (БД). БД – многоаспектная идентифицированная совокупность данных, связанных между собой определенным образом и относящихся к некоторой предметной области [1]. В соответствии с принципом этапности автоматизации информационных систем, интегрированная БД может быть создана

для систем автоматизированной разработки документов связи (САРДС), с последующим развитием ее в БД. Место БД в системе планирования связи показано на рис. 2. Прикладные программы системы разработки текстовых и табличных документов по связи (САРТТДС) и системы разработки графических документов по связи (САРГДС) взаимодействуют с БД посредством системы управления базами данных (СУБД) (комплекса программных средств). На нее возлагаются следующие основные функции:

– формирование БД, поддержание ее в актуальном состоянии и постоянной готовности к использованию;

– прием запросов от прикладных программ и ДЛ на выдачу данных из БД и донесений на ее корректировку;

– преобразование данных из БД и донесений на ее корректировку;

– преобразование данных из физического представления в логическое при чтении их из БД и, наоборот, при записи;

– обеспечение целостности БД.

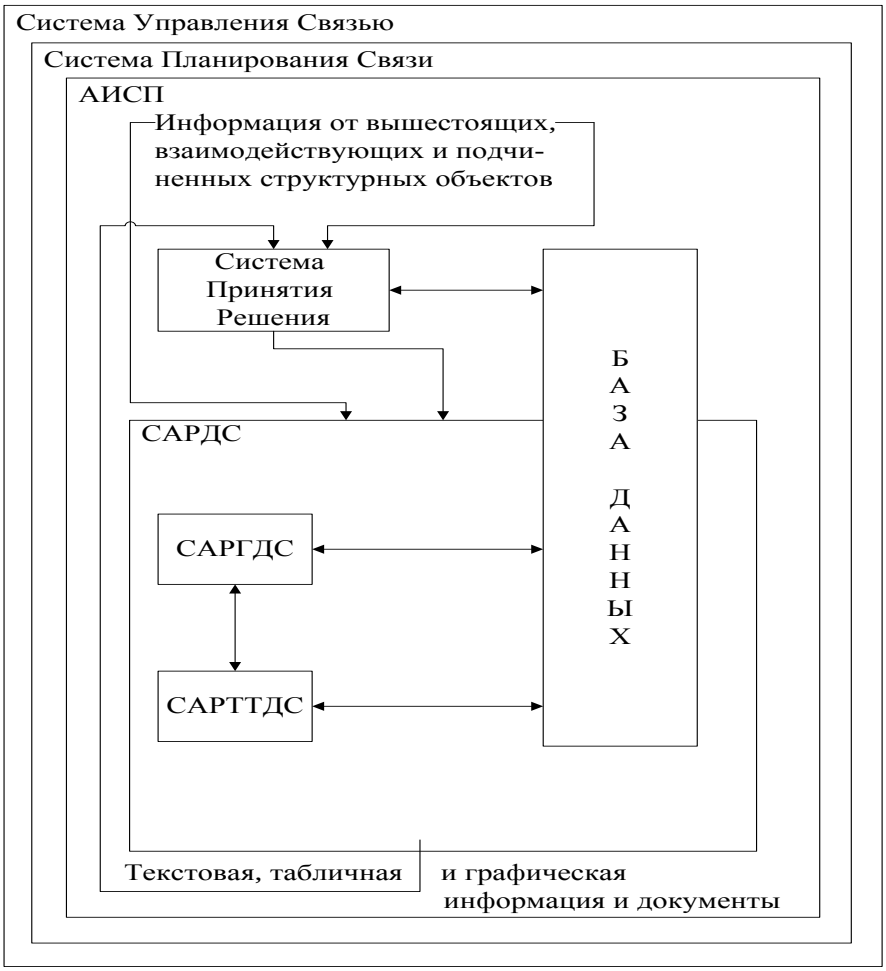


Рис. 2. Место системы автоматизированной разработки документов по связи и базы данных в системе планирования связи

Исходя из требований к САРДС, можно предъявить и требования к разрабатываемой БД. Структура БД, а также процедуры ее ведения должны отвечать требованиям по оперативности, адекватности, безопасности, надежности, удобству пользования.

Оперативность – характеризует процесс преобразования информации во времени.

Для САРДС оперативность характеризуется временем разработки документов, для информационного процесса в БД – это время реакции системы на запросы пользователей, связанных с различными преобразованиями, выполняемыми над данными.

Адекватность – характеризуется полнотой представления предметной области, непротиворечивостью, целостностью и актуальностью данных, правильностью результатов преобразования и хранения информации.

Безопасность – способность защитить информационный процесс и данные, хранящиеся в БД от НСД с целью разрушения БД, ввода в нее ложных данных или утечки информации из БД.

Надежность – способность сохранять во времени значения показателей качества в заданных пределах при частичных отказах комплекса программных и аппаратных средств. Надежность характеризуется безотказностью, долговечностью и восстанавливаемостью [2].

Безотказность – характеризует способность информационного процесса сохранять непрерывность в течении некоторого времени.

Восстанавливаемость – характеризует способность к восстановлению при возникновении нарушений в работе технических и программных средств и неправильных действий ДЛ и администрации системы.

Долговечность характеризуется адаптивностью, расширяемостью и информационной совместимостью. Адаптивность – характеризует приспособляемость информационного процесса к изменению структуры информационной системы. Расширяемость – характеризует возможность БД к наращиванию. Совместимость – характеризует идентичность технологии обработки информации в различных системах.

Разработка базы данных для системы автоматизированной разработки (обработки) документов по планированию связи предполагает решение следующих задач:

– анализ существующего состояния систем автоматизированной разработки документов по планированию связи;

– определение места и роли БД САРДС в системе планирования связи;

– исследование направлений дальнейшего совершенствования БД САРДС;

– определение требований к БД САРДС с точки зрения её предназначения, цели разработки, направления решения практических задач, определения конечных результатов, возможности внедрения в производственную деятельность;

– разработка структуры БД САРДС, отражающей: общую постановку задачи; формирование массива исходных данных; используемые математические модели; разработку рекомендаций по её практическому применению;

– разработка алгоритмов ведения БД САРДС;

– проведение функционального анализа предлагаемых решений.

Конечным результатом разработки темы магистерской диссертации является разработка базы данных для системы автоматизированной разработки документов по планированию связи, включающей в себя:

– разработку инфологической модели БД САРДС;

– построение даталогической модели БД САРДС (на базе выбранной СУБД);

– разработку алгоритмов обработки информации и взаимодействия БД с пользователями САРДС;

– разработку программных средств реализации интерфейса БД с пользователями САРДС;

– оценку эффективности БД САРДС;

– предложения по использованию БД САРДС.

Для решения вышеперечисленных задач предлагается использовать ряд руководящих, нормативных, методических и инженерно-технических материалов, таких как:

– перечень документов по связи (диаграмма «сущность-связь» фрагмента БД САРДС);

– фрагмент описания схемы базы данных;

– программный макет, реализующий алгоритмы конец редактирования поля и перед активацией.

Список используемых источников

1. Когаловский М. Р. Технология баз данных на персональных ЭВМ. М.: Финансы и статистика, 2002.

2. Волкова В. Н., Денисов А. А. Основы теории систем и системного анализа. СПб.: Изд-во СПбГТУ, 2007. 510 с.

Статья представлена заведующей кафедрой,
доктором технических наук, профессором Г. В. Верховой.

УДК 004.047
ГРНТИ 50.43.19

К ВОПРОСУ ИССЛЕДОВАНИЯ МЕТОДОВ УНИЧТОЖЕНИЯ ИНФОРМАЦИИ НА ОБЪЕКТАХ АВТОМАТИЗАЦИИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

А. С. Мамончикова, И. И. Филичкин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается проблема утечки остаточной информации, возникающей вследствие ее недостаточно надежного удаления с накопители на жестком магнитном диске. Предлагаются пути решения частных инженерных задач, направленных на разработку конструктивного алгоритма и методики безопасного уничтожения информации с энергонезависимых носителей на объектах автоматизации телекоммуникационных систем.

автоматизированные информационные системы, несанкционированный доступ к информации, энергонезависимые носители информации, уничтожение конфиденциальной информации.

Индустрия защиты информации (ЗИ) направлена на решение одной задачи – сделать открытую информацию доступной всем пользователям, а грифованную – только тому, кому она предназначена. Как в сфере бизнеса, так и в сфере государственного управления, уже скопились значительные объемы конфиденциальной и секретной информации, хранящиеся в базах данных компьютеров. Эта информация представляет собой реальную ценность, а утечка ее в ряде случаев способна влиять даже на государственную безопасность.

Учитывая специфику способов и средств защиты, общая задача обеспечения информационной безопасности может быть декомпозирована на четыре частные [1]:

- защита от несанкционированного доступа (НСД) к информации (копирование данных или кража носителей информации, удаленный взлом компьютеров, объединенных в сеть, перехват сетевых сообщений, восстановление уничтоженной информации и т. д.);
- защита от разрушения информации (вирусные воздействия на отдельные компьютеры или сети в целом, физическое уничтожение носителей информации и т. д.);

- защита от ввода ложной информации (подмена или модификация файлов, записей баз данных, сетевых сообщений и т. д.);
- защита от блокирования доступа к информации и вычислительным ресурсам (атаки типа «Отказ в обслуживании» (*Denial of Service*) на отдельные компьютеры и сети в целом и т. д.).

В большинстве телекоммуникационных систем на объектах автоматизации (а они как правило базируются на основе ПК) в качестве основного энергонезависимого носителя используется накопитель на жестком магнитном диске (НЖМД). В работе рассматривается один из аспектов защиты от несанкционированного доступа к информации – защита от доступа к информации, удаленной с НЖМД.

Существует ряд методов уничтожения информации, хранимой на НЖМД. Эти методы можно условно разделить по методу воздействия на носитель [3]:

Программные методы – основаны на использовании стандартных команд управления НЖМД;

Аппаратные методы – реализуются с помощью специального оборудования, воздействующего на магнитные диски НЖМД. По способу воздействия аппаратные методы классифицируются на несколько подгрупп:

– методы, перестраивающие доменную структуру магнитного носителя без разрушения его конструкции;

– методы, связанные с разрушением конструкции носителя;

Метод шифрования по известному ключу – основан на использовании эффекта рассеивания блочных шифров для защиты утилизированной информации с НЖМД.

Достоинства программных методов:

– возможность последующего использования носителей;

– низкая стоимость;

– простота использования;

– возможность использование в ходе работы ВС в качестве профилактической меры.

Недостатки программных методов:

– низкая скорость работы. Выполнение многократной перезаписи современного накопителя может потребовать нескольких часов или даже дней;

– низкая универсальность. Программы уничтожения информации могут не поддерживать устаревшие или нестандартные накопители;

– невозможность уничтожения информации с неисправного накопителя;

– отсутствие программного метода, эффективность которого (т. е. невозможность восстановления информации) обоснована теоретически или на практике.

Достоинства аппаратных методов:

– высокая скорость работы – не дольше нескольких минут для любого метода. На базе установок для перемагничивания возможно создание систем мгновенного уничтожения информации в экстренных случаях (при краже, стихийных бедствиях и т. п.);

– высокая универсальность – возможность уничтожения накопителей любого типа, а так же магнитных дисков, магнитных лент. При использовании систем, разрушающих конструкцию накопителя, возможно уничтожение не только магнитных, но и оптических накопителей, а так же микросхем энергонезависимой памяти;

– возможность уничтожения информации с неисправного накопителя;

– наибольшая надежность уничтожения информации.

Недостатки аппаратных методов:

– после уничтожения информации носители не могут быть использованы повторно;

– дороговизна – необходимость закупки специального оборудования, высокие энергозатраты;

– работа с аппаратными системами уничтожения информации требует специальных навыков.

Достоинства метода ШИК:

– возможность последующего использования носителей;

– низкая стоимость;

– простота использования;

– надежность метода обоснована теоретически;

– высокая скорость работы.

Недостатки метода ШИК:

– невозможность уничтожения информации с неисправного накопителя;

– безопасность метода не апробирована практически;

– безопасность метода основана на «искусственном» предположении о идеальных рассеивающих свойствах блочного шифра. Однако для проверки рассеивающих свойств блочных шифров [2] их тестирование целесообразно проводить по методике, предложенной членами Нового Европейского Проекта по созданию базовых примитивов, имея ввиду возможную будущую стандартизацию (NESSIE, *New European Schemes for Signature, Integrity and Encryption*) [4]. Одним из критериев тестирования является среднее число битов выхода, изменяющееся при изменении одного бита входного вектора. Эту проверку проходят не все шифры;

Применение методов уничтожения информации с НЖМД, рассмотренных в этом разделе, в целом решает задачу защиты от утечки утилизированной информации, но подобные решения имеют ряд недостатков, затрудняющих их повсеместное использование. Самый существенный недостаток

программных методов – их потенциальная ненадежность и небольшая скорость. Аппаратные методы выводят очищаемый носитель из строя, что нерационально и неприемлемо с экономической точки зрения. Безопасность метода ШИК оставляет еще много вопросов.

Сказанное позволяет сделать вывод о настоятельной необходимости разработки новых программных методов уничтожения информации с НЖМД, позволяющих с требуемой надежностью и за приемлемое время уничтожать информацию. При этом должна оставаться возможность последующего использования носителя.

Считывание информации, хранимой на НЖМД, может рассматриваться как процесс передачи информации [2]. Восстановление информации, поверх которой была выполнена новая запись, так же может рассматриваться как процесс приема, но с более высоким уровнем зашумления. Эти процессы могут быть интерпретированы как передача-прием информации по двум каналам с произвольным доступом – основному каналу и каналу утечки.

Одним из известных способов защиты информации, передаваемой по каналам перехвата, является кодовое зашумление (КЗ). А. Вайнер [5] предложил следующую модель КЗ. Если основной канал (канал между законными пользователями) не содержит помех, канал утечки – двоичный симметричный канал, Вайнером предложен способ кодирования в смежных классах линейного $(n, n-k)$ кода V, при каждому информационному k-блоку ставится в однозначное соответствие один из смежных классов кода, а для передачи по каналу случайно и равновероятно выбирается слово в этом смежном классе. Декодирование на приеме осуществляется путем определения номера смежного класса, содержащего принятый k-блок. В канале утечки из-за наличия помех наиболее вероятен переход кодового блока в какой-либо другой смежный класс, что при декодировании вызывает дополнительное искажение (зашумление) информационного блока.

Используя коды, преобразующие блоки данных достаточно большого размера, можно получить требуемый уровень защищенности информации в канале перехвата при заданном значении вероятности ошибки в нем.

Научная задача исследования заключается в разработке модели нарушителя, осуществляющего несанкционированный доступ к информации, предназначенной для удаления из энергонезависимой памяти, конструктивного алгоритма и методики оценки безопасности уничтожения информации, хранимой в энергонезависимой памяти на защищаемых УТ ОА исполнительных органов государственной власти Санкт-Петербурга на основе использования метода кодового зашумления (КЗ).

Быстрое устаревание телекоммуникационных и компьютерных технологий, необходимость постоянного обновления аппаратного обеспечения, невысокая надежность НЖМД, особенности проведения их гарантийного

ремонта и повторного использования в сочетании с наличием высокоразвитых технологий восстановления информации с НЖМД обуславливают возможность несанкционированного доступа к секретной и конфиденциальной информации.

Проведенный анализ известных программных и аппаратных методов уничтожения информации с магнитных носителей показал неэффективность и экономическую нецелесообразность их применения для уничтожения информации, хранимой на НЖМД, а также несоответствие нормативной базе.

Список используемых источников

1. Беседин Д. И., Боборыкин С. Н., Рыжиков С. С. Анализ возможностей предотвращения утечки информации, хранящейся в накопителях на жестких магнитных дисках // Специальная техника. 2001. № 1.

2. Инструкция по обеспечению режима секретности в Российской Федерации. М.: Постановление Правительства Российской Федерации от 05.01.2004, № 3-1.

3. Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам. М.: Приказ Гостехкомиссии (ФСТЭК) России от 23.05.2007, № 55.

4. Understanding Data Loss. Ontrack Data Recovery, 2000. URL: http://www.ontrack.com/understandingdataloss.

5. Коржик В.И., Яковлев В.А. Неасимптотические оценки эффективности кодового зашумления одного канала // Проблемы передачи информации. М.: Связь, 1981. Т. 17. № 4. С. 11–18.

Статья представлена заведующей кафедрой,
доктором технических наук, профессором Г. В. Верховой.

УДК 004.056.53
ГРНТИ 20.53.19

МЕТОДИКА ПОИСКА УЯЗВИМОСТЕЙ В СИСТЕМНОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ СЕТЕВОГО ОБОРУДОВАНИЯ СЕМЕЙСТВА CISCO

Д. О. Маркин, И. А. Санников

Академия Федеральной службы охраны Российской Федерации

В работе описана методика исследования защищенности системного программного обеспечения сетевого оборудования семейства Cisco Systems. Описан порядок дизассемблирования системного программного обеспечения с учетом архитектуры процессоров, методика поиска критических с точки зрения реализации процедур аутентификации и авторизации маршрутов потоков управления.

Cisco, поиск уязвимостей, реверс-инжиниринг, дизассемблирование, отладка, системное программное обеспечение.

В настоящее время значительная часть сетевого оборудования, обеспечивающего инфокоммуникационное взаимодействие как в отрытых информационно-телекоммуникационных сетях, так и в защищенных корпоративных, построена на базе программно-аппаратных комплексов иностранного производства, в частности, на телекоммуникационном оборудовании компании Cisco Systems [1]. В связи с этим в случае возникновения острых конфликтов возможны внешние воздействия на данное оборудования в целях эксплуатирования скрытых возможностей данного оборудования и нанесения ущерба экономике страны. Основной для функционирования любого телекоммуникационного оборудования является его программно-аппаратная составляющая и, в частности, системное программное обеспечение (СПО). Таким образом, одной из актуальных задач по обеспечению информационной безопасности в инфокоммуникационных сетях является исследование защищенности СПО телекоммуникационного оборудования [2] иностранного производства на предмет наличия уязвимостей (недекларированных возможностей – НДВ и/или программных закладок).

Для исследования особенностей функционирования СПО сетевого оборудования компании Cisco Systems могут применяться такие классы инструментальных средств анализа программного обеспечения (ПО) как: диззассемблеры, отладчики, средства виртуализации и эмуляторы.

Особенностью СПО сетевого оборудования компании Cisco Systems является архитектура микропроцессоров – PowerPC, на основе которых оно

разработано, что накладывает специфические ограничения на применения указанных средств анализа ПО.

Для анализа системного программного обеспечения телекоммуникационного оборудования компании Cisco System был разработан лабораторный стенд, схема которого представлена на рисунке.

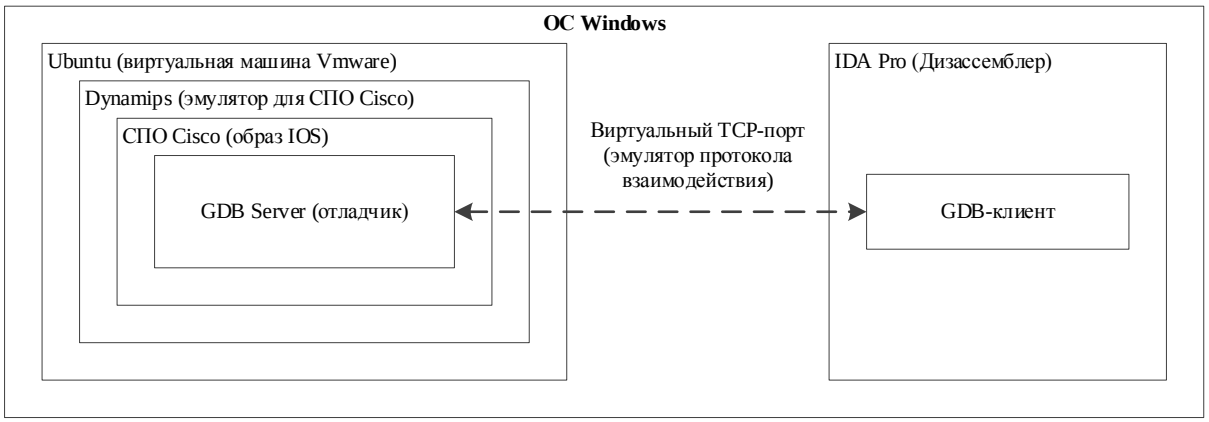


Рисунок. Схема лабораторного стенда

В состав лабораторного стенда входят: виртуальная машина с ОС Ubuntu; dynamips (Эмулятор сетевого оборудования семейства CISCO); IDA Pro (Дизассемблер); образ СПО CISCO.

Подготовка лабораторного стенда на основе виртуальной машины с образом ОС Ubuntu необходимо осуществлять в следующей последовательности:

Создать виртуальную машину на основе ОС Ubuntu. В данной ОС будет осуществляться основная работа.

Загрузить дистрибутивы для дальнейшей разборки, отладки и сборки образа: dymanips, putty, radare2, net-tools, uml-utilities и hexedit.

Войти в систему:

Запустить приложение Terminal. Terminal оповестит об использовании команды sudo, необходимой для исполнения команд от имени супер пользователя.

Для дальнейшей работы необходимо использовать суперпользователя, но в Ubuntu 18.04 изначально он заблокирован.

Чтобы разблокировать суперпользователя, необходимо:

1) задать пароль, использовав следующую последовательность команд:

```
user@ubuntu:~$ sudo passwd root
```

ввести пароль:

```
[sudo] password for user:
```

ввести новый пароль *root*-пользователя:

```
Enter new UNIX password:
```

Подтвердить введенный пароль:

```
Retype new UNIX password:
```

Пароль при вводе не отображается.

После разблокировки суперпользователя необходимо войти в него с помощью команды:

```
user@ubuntu:~$ su
```

Terminal запрашивает ввод пароля:

```
Password:
```

Примечание. При введении пароль не отображается.

Далее работа в Terminal осуществляется с правами суперпользователя:

```
root@ubuntu:/home/user#
```

Осуществить загрузку установочных пакетов (дистрибутивов).

Примечание. Для выполнения данного этапа необходим доступ к хранилищам установочных пакетов (репозиторию) либо используя доступ в сеть Интернет, либо доступ к локальному хранилищу.

Рекомендуемый порядок установки пакетов следующий:

2) установить эмулятор для СПО Cisco Systems – приложение dynamips;

```
root@ubuntu:/home/user# apt install dynamips
```

установить средство доступа к удаленным приложениям с использованием протоколов Telnet, SSH и д. – приложение putty:

```
root@ubuntu:/home/user# apt install putty
```

В процессе загрузки появится запрос на подтверждение продолжения загрузки. Подтвердить его введением команды:

```
Do you want to continue?[Y/n] y
```

установить программное средство настройки сетевой конфигурации – пакет net-tools:

```
root@ubuntu:/home/user# apt install net-tools
```

установить комплекс программных средств настройки виртуального интерфейса для доступа к эмулируемому СПО Cisco Systems – пакеты uml-utilities:

```
root@ubuntu:/home/user# apt install uml-utilities
```

установить дизассемблер radare2:

```
root@ubuntu:/home/user# apt install radare2
```

В процессе загрузки появится запрос на подтверждение продолжения загрузки. Подтвердить его введением команды:

```
Do you want to continue?[Y/n] y
```

установить шестнадцатеричный редактор данных hexedit:

```
root@ubuntu:/home/user# apt install ht hexedit
```

Загрузка установочных пакетов (дистрибутивов) завершена.

Подготовка образа СПО Cisco Systems к дизассемблированию:

3) открыть в панели задач файл менеджер Nautilus;

в открытом файл менеджере необходимо выбрать рабочую папку (например, Documents) и открыть её. В рабочую папку нужно поместить файл образа СПО Cisco.

вернуться в Terminal и перейти в рабочую папку командой:

```
root@ubuntu:/home/user# cd Documents/
```

извлечь образ СПО Cisco для осуществления отладки с помощью команды:

```
root@ubuntu:/home/user/Documents# unzip c2600-bino3s3-mz.123-22.bin
```

В результате разархивирования создается файл C2600-BI.BIN.

Для создания файла для дизассемблирования нужно воспользоваться копированием файла с помощью команды:

```
root@ubuntu:/home/user/Documents# cp C2600-BI.BIN C2600-BI.BIN.ida
```

В результате разархивирования создается файл C2600-BI.BIN.ida.

Открыть файл для дизассемблирования через HEX-редактор командой:

```
root@ubuntu:/home/user/Documents# hte C2600-BI.BIN.ida
```

Примечание. Появляется окно с предупреждение нажать Enter.

нажать F6 для изменения режима отображения;

выбрать режим – elf/header с помощью клавиши Tab, затем Enter;

переместиться стрелками на клавиатуре на строку с именем machine;

нажать F4 изменить значение 002b на 0014. Для сохранения изменений нажать F2. Таким образом изменяется значение архитектуры процессора, которое считывает дизассемблер. Выйти из HEX-редактора кнопкой F10.

извлечь файл для дизассемблирования. Для этого необходимо:

перейти в файл менеджер;

выбрать файл C2600-BI.BIN.ida указателем мыши;

зажав левую кнопку, перетащить файл C2600-BI.BIN.ida на хостовую машину.

Открыть файл для дизассемблирования с помощью IDA Pro.

4) запустить IDA Pro, выбрать на панели программы кнопу New;

5) выбрать файл C2600-BI.BIN.ida и нажать открыть;

6) в окне для задания параметров открытия файла нажать на кнопку *Kernel options 1*. В появившемся окне выбрать все пункты и нажать OK;

7) аналогично повторить для Kernel options 2;

8) завершить настройку параметров, нажать OK;

9) дождаться выполнения дизассемблирования.

В виртуальной машине запустить эмуляцию образа СПО Cisco.

10) в Terminal создать виртуальный интерфейс и настроить его, для подключения по протоколу Telnet, командой:

```
root@ubuntu:/home/user/Documents# tunctl -t tap1
root@ubuntu:/home/user/Documents# ifconfig tap1 up
```

```
root@ubuntu:/home/user/Documents# ifconfig tap1
192.168.23.1/24
```

узнать ip-адрес самой виртуальной машины командой:

```
root@ubuntu:/home/user/Documents# ifconfig
```

запустить эмулятор образа с помощью команды:

```
root@ubuntu:/home/user/Documents# dynamips -T 2003 -j -P 2600
-t 2621 -s 0:0:tap:tap1 C2600-BI.BIN
```

запустить Putty на панели задач;

в поле Host Name ввести 127.0.0.1, в поле Port 2003, в Connection type: выбрать Telnet и нажать кнопу Open.

в открывшемся терминале настройки маршрутизатора осуществить настройку маршрутизатора с помощью команд:

```
Router>enable
Router#configure terminal
Router(config)#interface  f0/0
Router(config-if)#ip address 192.168.23.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#line vty 0 15
Router(config-line)#password 12345
Router(config-line)#login
Router(config-line)#end
Router#wr
```

запустить GDB сервер командой:

```
Router#gdb kernel
```

Настройка стенда завершена.

В исходном коде СПО с использованием функции поиска строк необходимо найти сообщение с текстом, выдаваемым программой при введении некорректного пароля «Bad passwords».

Для нейтрализации подсистемы аутентификации в СПО достаточно осуществить оператора сравнения на противоположное условие либо на безусловный переход, после чего сохранить изменения в новом образе СПО. Установка данного образа СПО в оборудование и осуществление начальных настроек приведет к тому, что доступ к данному оборудованию по протоколу Telnet можно будет получить без ввода пароля.

Список используемых источников

1. CISCO: Сетевое программное обеспечение [Электронный ресурс]. URL: http://www.cisco.com (дата обращения 30.11.2017).

2. Whitepaper: Writing Cisco IOS Rootkits [Электронный ресурс] / Grid32 Security. Newark, 2015. URL: https://grid32.com/cisco_ios_rootkits.pdf (дата обращения 06.04.2018).

3. IDA: About [Электронный ресурс] : [сайт] / Hex-Rays SA. Rue Rennequin Sualem, 2016– . URL: https://www.hex-rays.com/products/ida/ (дата обращения 06.04.2018).

4. Санников И. А., Маркин Д. О., Хомякова А. А. Исследование защищенности системного программного обеспечения сетевого оборудования семейства Cisco // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: материалы X Межрегиональной научно-практической конференции [Электронный ресурс] / под ред. О. М. Голембиовской. Брянск: БГТУ, 2018. 187 с. С. 99–103.

УДК 007:519.2
ГРНТИ 27.43.15

ВЕРОЯТНОСТНЫЕ ХАРАКТЕРИСТИКИ БИНАРНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ. РЕЗЮМЕ

В. А. Медведев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Подводится итог исследованию бинарной последовательности как модели различных её реализаций, в которой дискрета может принимать одно из двух возможных значений. Описан прямой путь определения вероятностей значений отсчетов бинарной последовательности (P-вероятностей) на основе заданных значений вероятностей пачек нулей и единиц (G -вероятностей). Продемонстрирован обратный путь – определение вероятностей пачек нулей и единиц на основе вероятностей независимых отсчетов одной или нескольких позиций бинарной последовательности. Приведены формульные соотношения.

бинарная последовательность, модель, вероятность, вероятностное позиционирование, P-вероятности, G-вероятности.

Когда рассматривают последовательность, то обычно подразумевают какую-то её конкретную реализацию. Для бинарной последовательности это может быть, например:

0 1 1 0 1 0 0 1 0 1 1 1 0 1 …

В ней, как правило, указывается начало (а может быть) и конец, т. е. в реализации последовательности существуют границы. Для исследования последовательностей создаётся модель, которая не является представлением, а выступает как понятие (т. е. не имеет ограничений).

Бинарная последовательность есть двоичное кольцо неопределённого размера; это – модель дискретного случайного процесса с двумя возможными значениями на одной позиции, обозначенными как «0» и «1» и распо-

ложенными в последовательности произвольным образом (рис. 1). Определенная таким образом она выступает как обобщение всевозможных реализаций бинарной последовательности [1].

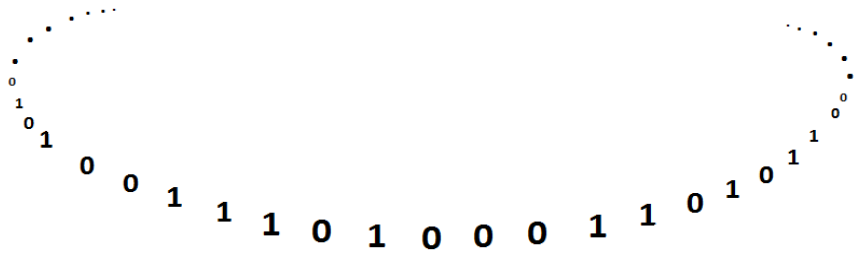


Рис. 1. Бинарная последовательность

Первой характеристикой бинарной последовательности является количественное соотношение между нулями и единицами. Если Q – количество позиций последовательности, а q – общее количество нулей (или единиц) в последовательности, то одна бинарная последовательность отличается от другой своей константой:

$$P(0) \text{ (или } P(1)) = {}^{q}/_{Q}. \quad (1)$$

С вероятностной точки зрения $P(0)$ означает вероятность получения нуля на произвольной позиции последовательности. Очевидно, что

$$P(0) + P(1) = 1. \quad (2)$$

Вторая характеристика бинарной последовательности представляет её «внутреннюю» организацию. Случайное чередование нулей и единиц в последовательности образуют структуру, в которой нули и единицы группируются в унарные случайные серии (пачки). Минимальная пачка включает одну составляющую. Среднее число нулей (единиц) в пачке обозначается как $M_0(M_1)$.

Эта вторая характеристика бинарной последовательности связана с первой характеристикой следующими соотношениями [1]:

$$P(0) = M_0/(M_0 + M_1), \qquad P(1) = M_1/(M_0 + M_1). \quad (3)$$

Таким образом, если производится отсчет одной позиции бинарной последовательности, то вероятность получить нуль или единицу определяется выражениями (3).

При отсчете двух соседних позиций бинарной последовательности (возможные результаты: 00, 01, 10, 11) следует определить связи между результатами на каждой позиции. Исходные соотношения [1]

$$\begin{aligned} P(00) + P(10) &= P(0), \\ P(00) + P(01) &= P(0), \\ P(11) + P(10) &= P(1), \\ P(11) + P(01) &= P(1) \end{aligned} \qquad (4)$$

позволяют установить, что вероятностная природа бинарной последовательности не чувствительна к направлению. Так, вероятность получить нуль на левой позиции отсчета $P(0) = P(00) + P(01)$, а на правой позиции – $P(0) = P(00) + P(10)$. Отсюда получаем:

$$P(01) = P(10). \qquad (5)$$

Вероятности результатов отсчета двух соседних позиций можно выразить через вероятности результатов отсчета одной позиции бинарной последовательности. Например,

$$P(01) = P(0)\,P(0/1), \qquad (6)$$

где $P(0)$ – вероятность нахождения нуля на произвольной позиции бинарной последовательности, $P(0/1)$ – вероятность нахождения единицы на соседней позиции с обнаруженным нулем. Как показано в [1, 2]

$$P(0/1) = 1/M_0, \qquad (7)$$

$$P(1/0) = 1/M_1. \qquad (8)$$

Соответственно:

$$P(0/0) = (M_0 - 1)/M_0, \qquad (9)$$

$$P(1/1) = (M_1 - 1)/M_1, \qquad (10)$$

Тогда (для примера) вероятность отсчета «01» составит:

$$P(01) = 1/(M_0 + M_1), \qquad (11)$$

Третий уровень модели бинарной последовательности предписывает отсчет трех соседних позиций, четвертый уровень – четырёх и т. д. Для их описания требуется введения вероятностей пачек нулей и единиц.

На рис. 2 показаны размеры пачек нулей и обозначение соответствующих им вероятностей. Так, $\mathrm{G}_0(\mathrm{k})$ – вероятность пачки, состоящей из k нулей (для единиц соответственно – $\mathrm{G}_1(\mathrm{k})$).

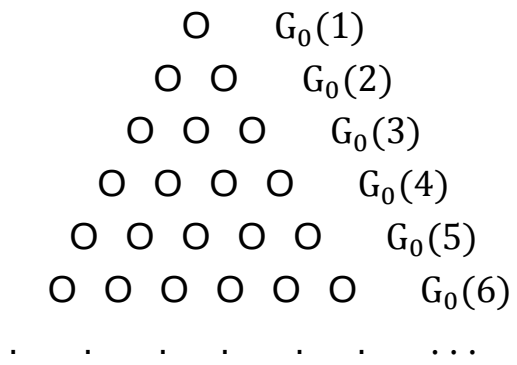


Рис. 2. Размеры пачек нулей и обозначение вероятностей

Используя вероятностное позиционирование [2], можно вычислить условные вероятности модели бинарной последовательности, начиная с третьего уровня. Например, вероятность $P(0/01)$ определится как

$$P(0/01) = \frac{1}{\mathrm{M}_0} \sum_{k=2} \mathrm{G}_0(\mathrm{k}).$$

Применяя связь безусловных вероятностей различных уровней бинарной последовательности, например, как для $P(01)$ [3]:

$$P(01) = P(010) + P(0110) + P(01110) + P(011110) + \ldots, \qquad (12)$$

можно получить условные вероятности различной конфигурации (состава), например, [3]:

$$P(0111/0) = G_1(3) / \sum_{k=3} G_0(k);$$

$$P(0111/1) = \sum_{k=4} G_0(k) / \sum_{k=3} G_0(k).$$

Анализ условных вероятностей различных уровней обнаруживает важное свойство бинарной последовательности, заключающееся в том, что условная вероятность на очередном шаге *не зависит* от предшествующей бинарной конфигурации (точнее – от её части), а определяется только местом события (на очередном шаге) в текущей пачке нулей или единиц [3].

Таким образом, имея G-вероятности пачек нулей и единиц, можно определить P-вероятности для любой конфигурации значений бинарной последовательности. Обратный путь – получение G-вероятностей при исходных P-вероятностях – возможен только для независимых отсчетов.

Независимые отсчеты характеризуются неизменностью вероятностей результатов текущего отсчета от результатов других отсчетов. В частности, например: $P(0/1) = P(1)$ – вероятность нахождения «1» после «0» равна абсолютной вероятности получения «1». Из этого простого равенства с учетом (3) и (7) вытекает основное соотношение для независимых отсчетов:

$$\mathrm{M}_0 + \mathrm{M}_1 = \mathrm{M}_0\mathrm{M}_1. \qquad (13)$$

Далее продолжая приравнивание соответствующих условных и безусловных Р-вероятностей [4], получаем основные соотношения для G-вероятностей:

$$G_0(k) = P(1)P(0)^{k-1}; \qquad G_1(4) = P(0)P(1)^3. \qquad (14)$$

Не трудно заметить, что G-вероятности в отдельности для нулей и единиц являются членами геометрической прогрессии. Вычисление математического ожидания полученных G-вероятностей, например, для пачек нулей, приводит к ожидаемому результату [4]:

$$1 + P(0) + P(0)^2 + P(0)^3 + P(0)^4 + \ldots = \frac{1}{1-P(0)} = \mathrm{M}_0. \qquad (15)$$

Список используемых источников

1. Медведев В. А. Модели бинарной последовательности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2015. Т. 1. С. 538–542.

2. Медведев В. А. Вероятностные характеристики бинарной последовательности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2016. Т. 2. С. 137–140.

3. Медведев В. А. Вероятностные характеристики бинарной последовательности. Продолжение // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2017. Т. 3. С. 329–333.

4. Медведев В. А. Вероятностные характеристики бинарной последовательности. Окончание // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2018. Т. 2. С. 491–494.

УДК 004.056
ГРНТИ 50.01.29

МОДЕЛЬ УГРОЗ И МЕТОДИКА ОЦЕНКИ РИСКА СИСТЕМЫ УПРАВЛЕНИЯ ВОДОСНАБЖЕНИЕМ

А. В. Мелешко[1,2], С. В. Савков[1]

[1]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В работе представлена модель угроз для киберфизической системы управления водоснабжением. Выделены основные события риска для класса объектов по управлению водоснабжением и их взаимосвязи. На основе модели разработана комплексная методика оценки риска. Комплексность методики заключается в оценке событий риска не только исходя из знаний экспертов, но и с применением информации полученной от датчиков объекта. Разработанная модель угроз и методика призваны улучшить качество оценки рисков, что позволяет повысить общий уровень безопасности объекта.

модель угроз, оценка риска, киберфизическая система, система управления водоснабжение.

На сегодняшний день все большое распространение получают узкоспециализированные киберфизические системы (КФС). Такие системы применяются в различных областях деятельности, на транспорте, в здравоохранении и в других областях. Среди объектов внедрения КФС выделяют объекты с критически важной инфраструктурой. Безопасности КФС на таких объектах необходимо уделять особое внимание, так как любые сбои могут приводить к катастрофичным последствиям [1].

В настоящей статье под киберфизической системой управления водоснабжением подразумевается дамба – объект критической инфраструктуры. Особенностью подобного рода систем является то, что в процессе работы происходит взаимодействие с окружающей средой. КФС с помощью датчиков получает данные о состоянии окружающей среды и в дальнейшем реагирует на изменение её параметров. Различные атаки на подобного рода системы могут приводить к негативным и даже катастрофическим последствиям, например, затопление города и т. д. Поэтому для обеспечения безопасности системы необходимо сформировать эффективную систему защиты.

Для построения системы защиты необходимо выделить угрозы и оценить риски их возникновения. Сначала необходимо составить модель угроз, которая включает в себя основные факторы риска системы, а в дальнейшем

оценить их влияние на систему (итоговая оценка рисков). Анализируя итоговые оценки влияния, можно разработать систему защиты, а также проверить её эффективность путем сравнения оценок до применения средств защиты и после.

Дамба является объектом критической инфраструктуры и включает в себя множество датчиков, систем управления, оповещения и других. Поэтому модель угроз должна основываться на имеющемся опыте и рекомендациях в области безопасности дамб и плотин.

В открытых отечественных источниках информации об угрозах и уязвимостях класса объектов по управлению водоснабжением найдено не было. В процессе изучения руководства Министерства внутренней безопасности США по обеспечению безопасности в секторе плотин [2], а так же других иностранных источников [3, 4, 5] были выделены основные события безопасности, на которые необходимо обратить особое внимание при моделировании угроз объектов по управлению водоснабжением. Были выявлены соответствующие угрозы, а так же причины их появления и возможные последствия. Угрозы, используя уязвимости системы, воздействуют на её компоненты. Поэтому были выявлены те самые компоненты системы, а так же источники угроз. Источники угроз, угрозы и компоненты представлены в таблице и пронумерованы следующим образом: *S* – источник, *T* – угроза, *C* – компонент. Так же в таблице указаны взаимосвязи между всеми угрозами, источниками и компонентами.

ТАБЛИЦА. Источники угроз, угрозы, компоненты и их взаимосвязи

№	Источники/угрозы/компоненты	Взаимосвязь (следствия)
1	2	3
S1	Злоумышленник	T1, T2, T4, T7, T8, T10, T11, T14, T16, T17, T18, T21
S2	Персонал	T3, T5, T12, T21, T22
S3	Приборы фото/видео фиксации	T1
S4	«Хакеры»	T1, T6, T8, T9, T11, T12, T13, T15, T18, T20
S5	Подрядные рабочие	T19, T21
S6	Подозрительные новые объекты вблизи КФС	T10
S7	Неизвестные объекты на территории объекта	T22, T27
T1	Несанкционированное наблюдение	T23
T2	Допрос персонала	T3
T3	Разглашение конфиденциальной информации	T24
T4	Проникновение на закрытую территорию	T25, T7, T6
T5	Кража идентификационных карт	T4
T6	Отключение системы охранного наблюдения	C1
T7	Отключение системы обнаружения вторжений	C2
T8	Вмешательство в работу СКУД	C3

№	Источники/угрозы/компоненты	Взаимосвязь (следствия)
1	2	3
T9	Возникновение ложных тревог от систем безопасности	T26
1	2	3
T10	Разрушение ограждений по периметру дамбы	C4
T11	Отключение системы освещения	C4
T12	Кража схем дамбы, карт и прочих материалов по строению дамбы	T26
T13	Несанкционированный доступ к защищенным компьютерам	T28
T14	Кража информации по графику поставок и системах безопасности	T4
T15	Кража паролей	T27
T16	Отключение электроэнергии	C8
T17	Несанкционированный сбор мусора	T28
T18	Кража средств связи	T30, T31
T19	Незапланированная доставка	T4
T20	Оповещение об угрозах из недостоверных источников	T9
T21	Проникновение в систему коммуникаций	T29
T22	Нарушение правил безопасности сотрудниками	C9, C10, C11, C12
T23	Кража видовой информации об объекте	C5, C6, C7
T24	Разглашение информации о системах защиты объекта	C1, C2, C3
T25	Вмешательство в работу затворов дамбы	C6
T26	Поиск уязвимостей в периметре дамбы, а также системе безопасности	C1, C2, C3
T27	Несанкционированный доступ под видом легального пользователя	C1, C2, C3, C11
T28	Кража конфиденциальной информации	C12
T29	Воздействие на систему коммуникации	C9
T30	Подслушивание разговоров сотрудников	C12
T31	Воздействие на локальную сеть сотрудников	C13
C1	Система охранного наблюдения	Z (защищенность системы)
C2	Система обнаружения вторжений	Z
C3	Система контроля доступа	Z
C4	Система освещения	Z
C5	Окрестности дамбы	Z
C6	Затворы дамбы	Z
C7	Периметр дамбы	Z
C8	Система электроснабжения	Z
C9	Система коммуникаций	Z
C10	Система резервного копирования	Z
C11	Система резервного питания	Z
C12	Конфиденциальная информация	Z

№	Источники/угрозы/компоненты	Взаимосвязь (следствия)
1	2	3
C13	Локальная сеть общения сотрудников	Z

Множество факторов риска, состоит из объединения трех непересекающихся подмножеств: M_S – множество источников угроз, M_T – множество угроз, M_C – множество компонентов (рис.).

На итоговом множестве определяется бинарное отношение причинности со свойством транзитивности. Элемент *z* показывает состояние защищенности объекта в целом. На выходе *z* можно фиксировать результирующий поток угроз f_z, интеграл от которого F_T по интервалу времени *T*, показывает степень уязвимости объекта, измеряемой ущербом.

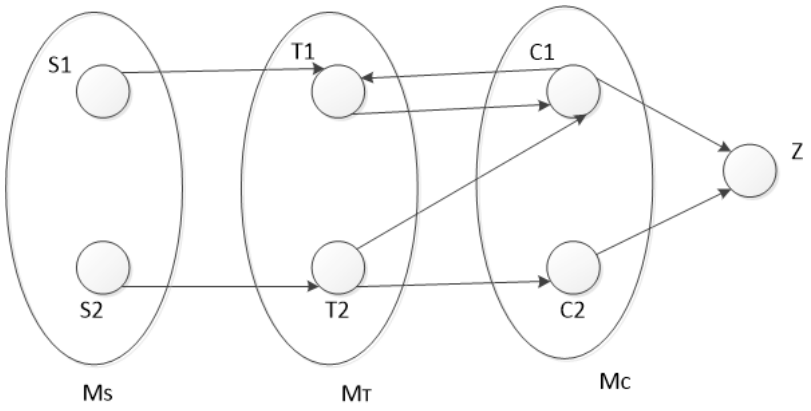


Рисунок. Метамодель риск анализа

Отношение причинности упорядочивает множество и порождает квадратную матрицу отношений W_0. Эта матрица формируется после выявления связей между факторами риска и показывает структуру путей распространения потоков угроз от источника до объекта. Далее формируется матрица V_0, которая показывает удаленное влияние факторов друг на друга, то есть строится с учетом транзитивности.

В количественной интерпретации матрица W_0 представляет собой арифметическую матрицу $W = (W_{ij})$. Элементы матрицы *W* являются весовыми коэффициентами, показывающими меру влияния *i*-го элемента на *j*-й, то есть данная матрица представляет собой матрицу смежности. Коэффициенты W_{ij} рассчитываются по формуле (1).

$$W_{ij} = \frac{F_{ij}}{\sum_i F_{ij}}, \qquad (1)$$

где F_{ij} – оценка влияния фактора i на фактор j, а $\sum_i F_{ij}$ – сумма всех оценок влияния факторов, которые влияют на фактор j.

После формирования матрицы W рассчитываются показатели V_{ij}, которые схожи с показателями W_{ij}, но они учитывают транзитивность отношений. Матрица V и показатели V_{ij} рассчитываются по формуле (2) [6].

$$V = (I - W)^{-1} - I, \quad (2)$$

где I – это квадратная единичная матрица необходимо размерности. Последний столбец матрицы V показывает оценки влияния каждого фактора на защищенность системы (профиль риска).

После формирования модели угроз эксперт оценивает значения весовых коэффициентов влияния и, по вышеописанным формулам, вычисляется профиль риска. Но поскольку КФС функционирует в режиме реального времени и зависит от внешней среды, то для более актуальной оценки риска предлагается так же учитывать постоянно изменяющиеся данные с датчиков. То есть предлагаемый подход предполагает использование экспертных оценок на начальных этапах риск анализа и последующее их уточнение по средствам данных с датчиков КФС. Также эксперт кроме оценок влияния задает граничные значения. Если система зафиксирует выход за эти значения, то модель угроз уточняется. На базе уточненной модели строится актуальный профиль риска, который в дальнейшем будет служить основой для мероприятий по повышению эффективности комплекса СЗИ. Итоговый профиль получается динамическим. Динамическая оценка позволяет оценивать текущий уровень безопасности КФС, что дает возможность оперативно реагировать на события безопасности, не учтенные или некорректно оцененные при первоначальной экспертной оценке.

На данный момент имеется программная реализация предложенной методики оценки рисков безопасности, позволяющая осуществлять следующие действия: ввод факторов риска модели угроз и их взаимосвязей, ввод разнородных экспертных оценок, формирования профиля риска. Так же имеется аппаратный макет дамбы, описанный в статье [1]. В дальнейшем планируется разработка модуля, позволяющего проводить обработку данных с датчиков и автоматическое внесение корректировок с модель угроз, а также формирование динамического профиля риска. Так же планируется провести тестирование разработанной методики на данных, приближенных к реальным. Программная реализация планируется к интеграции с аппаратным макетом КФС.

Список используемых источников

1. Десницкий В. А., Мелешко А. В. Моделирование инцидентов безопасности в системе управления водоснабжением // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. Т. 2. С. 301–306.
2. Dams Sector Security Awareness Guide // A Guide for Owners and Operators – 2007. 20 p.
2. Dams Sector Cybersecurity Guidelines, Washington, D.C.: U.S. // Department of Homeland Security. 2015. 64 p.
3. Massimo Meghella, Ignacio Escuder Bueno, Manuel de Membrillera Ortuño, Armando Serrano Lombillo A European Methodology for the Security Assessment of Dams // DAMSE – Deliverable 3. 2008. V. 02. 93 p.
4. Dams Sector Analysis Tool // Homeland Security. 2012. 2 p.
5. Шишкин В. М., Савков С. В. Автоматизированная система стохастического риск-анализа // Моделирование и Анализ Безопасности и Риска в Сложных Системах Труды Международной Научной Школы МАБР–2015. 2015. С. 61–66.

Статья представлена кандидатом технических наук В. А. Десницким.

УДК 02.026 (681.3)
ГРНТИ 20.53.01

ВАРИАНТ КЛАССИФИКАЦИИ ЭЛЕКТРОННЫХ БИБЛИОТЕК В ИНТЕРЕСАХ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ ИХ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ

Н. В. Михайличенко, И. Б. Паращук, А. В. Чернявский

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Электронные библиотеки приобретают все большую популярность благодаря тому, что они работают в широком спектре информационно-справочных услуг, предоставляют доступ к большому объему информационных ресурсов и их развертывание не требует значительных затрат времени и средств. В статье рассматривается методологический подход к поиску и обоснованию классификационных признаков электронных библиотек в интересах автоматизации управления их информационными ресурсами. Обоснованная классификация таких сложных автоматизированных информационно-справочных систем, как электронные библиотеки, дает свободу достоверного выбора их проектировщику и возможности для экономии различным категориям пользователей электронных библиотек.

электронная библиотека, информационные ресурсы, классификация, данные.

В настоящее время электронные библиотеки являются неотъемлемой частью исследовательской деятельности практически в любой области науки, промышленности, образования.

Влияние электронных (цифровых) библиотек на информационные процессы неуклонно возрастает. Сегодня пользователям предоставляется обширный выбор из быстро растущего числа электронных библиотек (ЭБ) с различными характеристиками. Современные модели (архитектуры) ЭБ развиты от уровня простых контент-провайдеров до уровня сложных поставщиков услуг. Они предлагают широкий спектр информационных услуг в сочетании с возможностями кооперации информационных ресурсов, электронного обучения и различных технологий доступа. Тем не менее, традиционные схемы классификации ЭБ недостаточно учитывают эти особенности, а, зачастую, игнорируют их при формулировке классификационных признаков. Не учитывают аспекты, связанные с задачами автоматизации управления информационными ресурсами ЭБ [1].

Анализ современных подходов к формулировке целей создания и задачам функционирования ЭБ показывает, что электронная библиотека представляет собой не только и столько базу из множества коллекций электронных документов, сколько систему, объединяющую в себе методы (подходы) к производству, хранению и организации информации, с целью ее поиска и анализа, с целью доступа к информационным ресурсам как непосредственно, так и с помощью технологий локальных и глобальных компьютерных сетей [1, 2, 3]. Цели создания и функционирования ЭБ хорошо изучены, их анализ позволяет сформулировать краткое предназначение ЭБ, как совокупности взаимоувязанных множеств информационных ресурсов: обеспечение доступности информационных ресурсов, предоставление которых пользователям затруднено или ограничено (редких изданий книг, фотоальбомов, рукописей, диссертаций, архивов, недоступных большинству библиотек, и т. п.); обеспечение доступа к информационным ресурсам, существующим исключительно в электронной форме; предоставление пользователям качественно новых возможностей работы с большими объемами данных, составляющих содержание информационных ресурсов; обеспечение сохранности печатного материала, первую очередь редких и ценных документов; придание новых свойств печатным и рукописным материалам; рациональная организация информационных ресурсов в виде базы документов [2]. И главное, ключевая цель создания и функционирования ЭБ должна быть безусловно сформулирована, как удовлетворение информационных потребностей пользователей, вне зависимости от того, является ли ЭБ локальной или она представлена в глобальной сети.

Вариант классификации ЭБ в интересах автоматизации управления их информационными ресурсами, среди прочего, должен быть ориентирован и на задачи, возлагаемые на библиотеки, к числу которых современные исследователи и практики относят предоставление пользователям качественно новых возможностей работы с большими объемами электронных данных, организацию фондов информационных ресурсов (документов, данных), существующих исключительно в электронной форме, их каталогизация и обеспечение доступа к ним потребителей информации, а также обеспечение широкого, в идеале – неограниченного доступа к документам, предоставление которых в бумажном виде пользователям затруднено или ограничено [3, 4].

Основные классификационные признаки ЭБ должны быть напрямую связаны с функционалом, возлагаемым на них. При этом, в рамках формирования классов ЭБ в интересах автоматизации управления их информационными ресурсами, предполагается, что информационный функционал направлен на удовлетворение потребностей в информации различных категорий пользователей по всем отраслям знаний либо одной из предметных областей; просветительный функционал ориентирован на вопросы популяризации электронных документов, относящихся к истории и культуре; научно-исследовательский функционал отвечает за содействие глубокому изучения темы (предмета) научными работниками и специалистами, в том числе за счет предоставления полных текстов из удаленных фондов; образовательный функционал направлен на поддержку как базового, так и дополнительного образования (путем предоставления не только мультимедийного учебного материала, но и необходимой литературы); справочный функционал ориентирован на получение достоверных сведений, отраженных в документах определенного вида, а функционал сохранения творческого наследия позволяет сберечь для следующих поколений ресурсы науки и культуры с использованием электронной среды [5].

Для того, чтобы успешно применять ЭБ в научной, культурной, образовательной среде и при любой иной библиотечно-информационной деятельности, следует, прежде всего, попытаться объективно сформулировать классификационные признаки этих систем, попробовать учесть все их современные особенности и условия функционирования, учесть аспекты, связанные с процедурами автоматизации управления их информационными ресурсами. Вариант такой классификации предложен на (см. рис.).

Исходя из способов финансирования при создании ЭБ можно выделить государственные и негосударственные. Государственные финансируются за счет средств бюджета, негосударственные, соответственно, финансируются частными лицами, коммерческими организациями для своих нужд. В зависимости от использования в интерфейсах ЭБ поддержки одного или не-

скольких языков, электронные библиотеки можно разделить по лингвистическому признаку на одноязычные и многоязычные. По стоимости предоставления ресурса ЭБ пользователям, можно выделить: платные – с пользователя взимается плата за пользование ресурсом, и бесплатная – пользователь бесплатно пользуется ресурсом электронных библиотек.

По защищенности ресурса ЭБ можно разделить на защищенные и незащищенные (открытые). Защищенные ЭБ способны противостоять несанкционированному доступу к ресурсам, их копированию, изменению, уничтожению, нарушению целостности [7]. Незащищенные ЭБ предоставляют открытый доступ к своим ресурсам.

По способу использования можно выделить следующие виды ЭБ: частные – ресурс ЭБ используется ограниченным кругом лиц в пределах ограниченного пространства; объединенные – ресурсы различных электронных библиотек, как правило, территориально разнесенных, объединены в общий ресурс и используется определенным кругом лиц; он-лайн, требующие регистрацию пользователей – доступ к ресурсам предоставляется только зарегистрированным пользователям в неограниченном пространстве (Интернет); он-лайн, не требующие регистрацию пользователей – доступ к ресурсам не ограничен ни числом пользователей, ни пространством.

По целевому назначению ЭБ можно разделить по следующим видам: художественная – в качестве ресурса ЭБ выступает художественные литературные произведения; специализированная – в качестве ресурса ЭБ выступают материалы, имеющие узконаправленную специализацию, присущую, как правило, одной отдельной организации в определенной сфере деятельности; учебные – в качестве ресурса ЭБ выступают материалы, ориентированные на образовательный процесс; научные – в качестве ресурса электронной библиотеки выступают научные труды специалистов и научных работников; смешанные – в качестве ресурса электронной библиотеки выступают общие фонды без какого-либо конкретного целевого назначения.

По разграничению доступа к информационным ресурсам ЭБ можно разделить на: ЭБ ограниченного доступа – ресурс библиотек предоставляется строго ограниченному кругу лиц, выделяемых по определенному принципу; ЭБ общего доступа – доступ к ресурсам библиотек имеют все пользователи в равной степени. По формату предоставляемого ресурса ЭБ можно разделить на: текстовые – в качестве ресурса ЭБ выступают текстовые документы; графические – в качестве ресурса ЭБ выступает графическая информация; тексто-графические – в качестве ресурса ЭБ выступает графическая информация, дополненная текстом; мультимедийные – в качестве ресурса ЭБ выступают мультимедийные файлы (звук, видео и т. д.); универсальные – в качестве ресурса ЭБ выступают файлы всех поддерживаемых форматов.

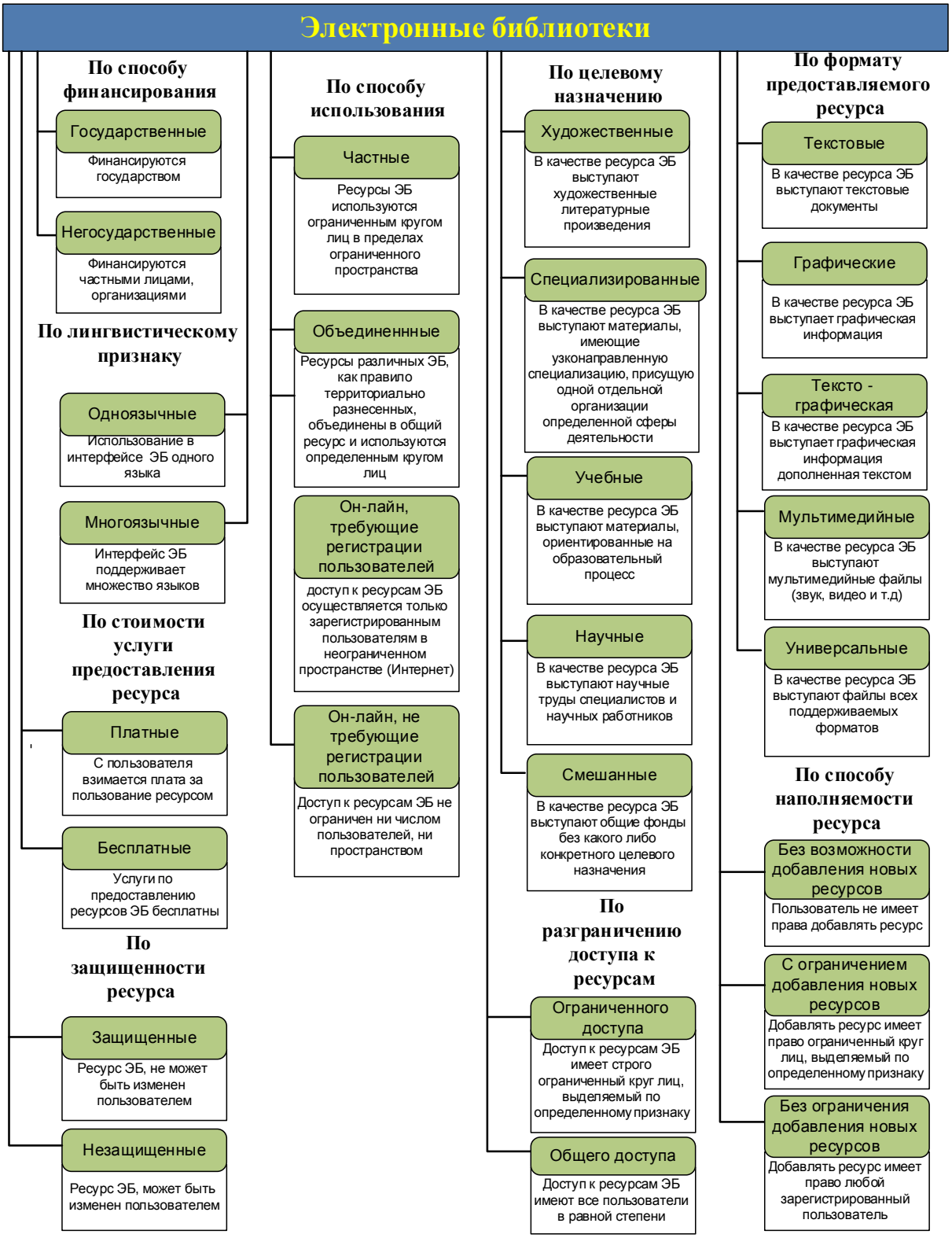


Рисунок. Вариант классификации электронных библиотек

По способу наполняемости информационного ресурса ЭБ можно разделить на следующие виды: ЭБ без возможности добавления новых ресур-

сов – пользователь не имеет права добавлять новый ресурс; ЭБ с ограничением добавления новых ресурсов – добавлять ресурс имеет право ограниченный круг лиц, выделяемый по определенном признаку; ЭБ без ограничения добавления новых ресурсов – добавлять ресурс имеет право любой зарегистрированный пользователь.

Данный подход к классификации цифровых библиотек основан на характеристиках с особым акцентом на эволюцию цифровых библиотек от контента до поставщиков информационных услуг. Он позволит помочь поставщикам более эффективно сообщать преимущества и особенности своих библиотек. Он также поддерживает клиентов при выборе соответствующей цифровой библиотеки [6, 8].

Иными словами, обоснованная классификация таких сложных автоматизированных информационно-справочных систем, как электронные библиотеки, дает свободу достоверного выбора их проектировщику и возможности для экономии различным категориям пользователей электронных библиотек.

Список используемых источников

1. Маркшефель Б., Фишер Д., Стельцер Д. Классификация цифровых библиотек – подход к моделированию на основе электронного бизнеса // Журнал управления цифровой информацией. Ильменау. Германия, 2008. С. 71–80.

2. Земсков А. И., Шрайберг Я. Л. Электронная информация и электронные ресурсы: публикации и документы, фонды и библиотеки. М.: Фаир-Пресс, 2007. 528 с.

2. Дригайло В. Г. Основы организации библиотек вуза: науч.-практ. пособие. М.: Либерея-Бибинформ, 2007. 624 с.

3. Учебные материалы [Электронный ресурс]. URL: http://works.doklad.ru/ view/ kzQThy0-1D8/2.html (дата обращения 16.11.2018).

4. Фур Н., Хансен П., Мабе М., Мисик А., Шельвберг И. Исследования и передовые технологии для цифровых библиотек: Цифровые библиотеки: общая схема классификации и оценки // 5-я Европейская конференция ECDL 2001. Дармштадт, Германия, 2001. С. 187–199.

5. Иванова В. В. Электронная библиотека в системе библиотечного обслуживания // Библиотеки и информационные ресурсы в современном мире науки, культуры, образования и бизнеса: Труды 12-й Межд. конференции «Крым-2005». М., 2005. С. 27–33.

6. Домбровский Я. А., Авраменко В. С., Бобрешов-Шишов Д. И., Саяркин Л. А., Ломанокский И. Г. Совершенствование средств доверенного сеанса работы при эксплуатации автоматизированных систем управления // Естественные и технические науки. 2016. № 11 (101). С. 207–214.

7. Паращук И. Б., Ренсков А. А. Особенности технического обеспечения и этапов процесса создания единой электронной библиотеки в рамках системы «электронного вуза» // III Межвузовская научно-практическая конференция «Проблемы технического обеспечения войск в современных условиях». Труды конференции. Т. 1. СПб.: ВАС, 2018. 378 с., С. 347–351.

УДК 004.416.6
ГРНТИ 50.41.25

ОСНОВНЫЕ КОНЦЕПЦИИ РЕФАКТОРИНГА ИСХОДНОГО КОДА ПРОГРАММНОГО ПРОДУКТА

А. А. Мишин, С. А. Комисаров

Военная академия связи им. Маршала Советского Союза С. М. Будённого

В данной статье обосновывается применение рефакторинга при разработке программного обеспечения. Перечисляются основные недостатки программного кода, сигнализирующие о необходимости рефакторинга. Рассматриваются основные преимущества рефакторинга кода как средства улучшения его композиционной стройности структуры программы и улучшения его читабельности.

архитектура ПО, рефакторинг прогармного кода, оптимизация.

Люди склонны совершать ошибки, по этой причине в разработке так необходим этап обзора и совершенствования проделанной работы. Таким образом, конечный продукт приобретает качество, соответствующее нашим требованиям. В разработке программного обеспечения, данный этап носит название **рефакторинг** [1].

Рефакторинг – это процесс изменения внутренней структуры программы, не затрагивающий её внешнего поведения и имеющий целью облегчить понимание её работы [2].

Одной из самых важных черт хорошего программного продукта является возможность его расширения и улучшения в будущем. Достигая этого, разработчики тратят немало времени в процессе проектирования системы. Однако, процесс разработки неизбежно подвержен ошибкам, поэтому так важно после реализации продукта оставлять время для улучшения системы.

На основе множества статей, можно с уверенностью утверждать, что рефакторинг – это очень важный этап в процессе разработки и часто используемая практика в так называемых гибких методологиях [3].

Как правило, говорят о необходимости проведения рефакторинга при обнаружении в программном коде следующих недостатков:

Повторение кода.

Как следует из названия, этот случай характеризуется дублированием участков программы. **Правило трех** утверждает, что необходимо переработать код, когда мы копируем какой-либо участок дважды. Одна копия зача-

стую является допустимой, однако при периодическом повторении процесса стоит провести анализ кода. Целесообразно включить дублирующийся код в функцию или метод с последующим вызовом.

Комплексный метод.

Данный недостаток характеризуется наличием метода, который состоит из нескольких неявных методов. Комплексный метод обрабатывает множество различных процессов, как правило, относящихся к разному функционалу. Рекомендуется декомпозировать метод, разделив его на простые.

Большой класс.

Аналогично предыдущему недостатку, данный случай возникает при чрезмерном усложнении, но уже класса. Принцип единственной ответственности утверждает, что каждый класс представляет собой единую сущность, имеющую только одну ответственность. Нарушение данного принципа приводит к образованию классов, содержащих в себе методы, относящихся к различным сущностям. Исправление недостатка производится декомпозицией или разбиением класса на подклассы, каждый из которых будет отвечать выше приведенному принципу.

Многие специалисты рекомендуют не прекращать рефакторинг на протяжении всей разработки: периодически анализировать код на предмет наличие перечисленных недостатков и по возможности устранять их. Эффективность разработки при этом значительно выше, чем в случае, когда для рефакторинга выделяется специально отведенное время.

Рефакторинг как таковой не устраняет все недостатки программного продукта, но однозначно помогает улучшить некоторые аспекты программы.

Улучшение системной архитектуры.

Иметь плохо спроектированную программу может быть достаточным в случае коротких сроков, однако в долгосрочной перспективе, неизбежно проявляется так называемый эффект «технического долга». Эффект заключается в проблемах, возникших в результате принятия простых и быстрых технических решений вместо лучших практик. Если брать в качестве аналогии мытье посуду, то техническим долгом будет гора немытых тарелок, возникшая в результате регулярного пренебрежения мытьем. Рефакторинг позволяет нам поддерживать программу в чистоте.

Упрощение понимания системы.

Рефакторинг повышает читабельность программы, позволяя другим проще понимать наш код.

Позволяет быстрее находить баги.

Логично предположить, что понимание кода позволяет проще находить баги. Таким образом, рефакторинг также позволяет нам быстрее находить

ошибки. Даже в том случае, если мы не слишком хороши в поиске багов, имея в привычках рефакторинг, мы достигаем лучших результатов.

Увеличение скорости разработки.

Наиболее ощутимая польза от рефакторинга заключается в увеличении скорости разработки ПО. Данное утверждение может показаться спорным ввиду того, что сам рефакторинг является время затратной процедурой, однако все не так, как может показаться на первый взгляд. Когда рефакторинг является неотъемлемой и постоянной частью работы, шанс столкновения с упомянутым техническим долгом стремится к нулю. Время работы не расходуется на устранение ошибок, возникших в результате принятия упрощенных технических решений.

Использование методов рефакторинга носит довольно общий характер и, следовательно, освоение подобной практики должно быть актуально для любого программиста вне зависимости от используемого в работе языка программирования. Применение методов рефакторинга программного кода и смежных технологических достижений в коммерческих целях позволит создавать качественные программные продукты в установленные сроки и в рамках заявленного бюджета.

Список используемых источников

1. Martin, R., Clean Code: A Handbook of Agile Software Craftmanship, Prentice Hall, 1st ed., 200 p.

2. Фаулер М., Бек К., Брант Д. и др. Рефакторинг: улучшение существующего кода. Спб: Символ-Плюс, 2009. 432 с.

3. John, F.; Cynthia, K. Toward an Understanding of Job Satisfaction on Agile Teams: Agile Development as Work Redesign // Hawaii International Conference on System Sciences // Waikoloa, HI, USA. 10 March 2014. Pp. 3993–4002.

УДК 004.4’2
ГРНТИ 50.41.25

СРАВНЕНИЕ И АНАЛИЗ ПРОГРАММНЫХ ПРОДУКТОВ, КОТОРЫЕ ПОЗВОЛЯЮТ РЕАЛИЗОВЫВАТЬ ИНТЕРАКТИВНЫЕ 3D–ПРИЛОЖЕНИЯ

И. В. Москвичев, Е. Т. Сыса

Военная академия связи им. Маршала Советского Союза С. М. Будённого

В статье дан обзор наиболее распространённых игровых движков для разработки 3D-приложений. Рассмотрены наиболее важные функции и возможности движков, такие как: поддерживаемые языки программирования, возможность взаимодействия с другими программными средствами, а также стоимость использования программных продуктов. Для анализа приведена сравнительная таблица для соотношения игровых движков.

игровые движки, разработка 3D-приложений, сравнительный анализ.

В настоящее время невозможно представить работу на сложном оборудовании без соответствующей подготовки. Однако проводить обучение на реальных прототипах является нецелесообразным, поскольку вероятность ошибок, которые могут привести к отказу системы, высока. Для таких случаев применяется моделирование системы, на которой будет проводиться подготовка.

В процессе разработки программно-аппаратного комплекса, позволяющего визуализировать и моделировать боевые действия и нанесения оперативной обстановки актуальным вопросом встаёт выбор программных продуктов, которые позволят реализовать модель необходимой аппаратуры.

Игровой движок Unity имеет много функций и понятный интерфейс. Его основное преимущество – кросс-платформенность. Языками программирования в Unity являются: C#, C++ и собственный язык Unity – UnityScript, что обеспечивает низкий порог вхождения для создания проектов. Движок поддерживает активы из основных 3D-приложений, таких как 3ds Max, Maya, Softimage, CINEMA 4D, Blender и т. д. Это означает, что реальных ограничений на поддерживаемые форматы файлов нет. Хотя Unity поддерживает интеграцию практически с любым 3D-приложением, его внутренний редактор недостаточно развит. Unity не имеет реальных функций для моделирования или построения вне нескольких примитивных форм, поэтому все нужно будет создавать в стороннем 3D-приложении. Однако

движок имеет большую библиотеку активов, в которой можно бесплатно загружать или приобретать их за деньги. В Unity 5 создатели попытались расширить возможности движка. Произошло значительное увеличение графических возможностей: физически точный шейдинг, глобальное освещение в реальном времени.

Достоинства:

1. Постоянные обновления и исправления обнаруженных другими разработчиками ошибок;

2. Возможность создания проектов без необходимости вникать в сложные технические особенности;

3. Возможность использовать движок на большинстве распространенных в настоящее платформ;

4. Оплата лицензии производится только если доход студии выше 100 000$;

5. Малое ресурсопотребление.

Недостатки:

1. Отсутствие исходного кода;

2. Нет возможности достичь наилучшей графики.

UE4 или Unreal Engine 4 – это движок, выпущенный в Epic Games, он является преемником UDK (Unreal Development Kit). В UE4 расширены возможности динамического освещения, новая система частиц может обрабатывать до миллиона частиц в одной сцене. Заметное изменение внесено в языке сценариев для UE4. Unreal Engine всегда запускает UnrealScript. Скрипт в UE4 теперь полностью заменен C ++, а Kismet – более интуитивно понятной системой Blueprint.

Достоинства:

1. Большое количество инструментов, для освоения большинства из которых не нужно быть узкоспециализированным специалистом;

2. Отзывчивая и грамотная служба технической поддержки;

3. Совместимость с такими основными платформами, как Windows, iOS, Mac и Android;

4. Добавление новых инструментов почти в каждом обновлении;

5. Имеет низкий порог вхождения, что позволяет легко освоиться новичкам.

Недостатки:

1. Стоимость лицензии, которая предполагает подписку стоимостью 19 долларов (вносится ежемесячно) и последующая оплата в размере 5 % от прибыли с продукта;

2. Высокое ресурсопотребление.

CryENGINE – чрезвычайно мощный движок, разработанный компанией Crytek. Графические возможности CryENGINE превосходят Unity и

находятся на одном уровне с Unreal Engine 4. Для работы доступны продвинутые инструменты создания освещения, реалистичной физики, усовершенствованные системы анимации. Таким образом, движок необходимо использовать в случаях, когда самым важным аспектом в разработке 3D-приложения является визуальная составляющая. Интерфейс CryENGINE обладает интуитивно понятными и мощными инструментами. Для того, чтобы начать работать с движком – потребуется время на обучение, если нет опыта работы с подобными программными продуктами.

На данный момент доступ к CryENGINE является абсолютно бесплатным, однако это ограничивает доступ к обучающим материалам, консультациям разработчиков и другим дополнительным материалам.

Достоинства:

1. Возможность быстро освоить и применять UI даже при низком уровне подготовки пользователя;
2. Упрощенная работа с графикой благодаря встроенной функции Flowgraph;
3. Упрощен процесс работы с искусственным интеллектом;
4. Возможность расширенной работы со звуковым сопровождением посредством набора инструментов Fmod.

Недостатки:

1. Высокое ресурсопотребление;
2. Высокий порог вхождения по сравнению с другими аналогичными компонентами.

Сравнение программных продуктов

Для проведения сравнительного анализа используем сводную таблицу (табл.).

ТАБЛИЦА. Сравнительный анализ игровых движков

	Unity 5.5.0f3	Unreal Engine 4	CryENGINE 3
Языки программирования	C#, C++, UnityScript	C++, UnrealScript	C++, Flowgraph
Интеграция файлов из других приложений	+	+	+
Возможность создавать приложения для разных платформ	+	+	+
Порог вхождения	Низкий	Низкий	Высокий
Стоимость ПО	Бесплатно	Платная подписка	Бесплатно
Ресурсопотребление	Низкое	Высокое	Высокое

Список используемых источников

1. Shah, Ryan. Mastering of Art of Unreak Engine 4 – Blueprints. June 15, 2014. 122 p.
2. Pearce-Authers, Ruan; Lundgren, Filip. Cryengine Game Programming with C++, C#, and Lua. Nov. 22, 2013. 276.
3. Лукосек Грег. Изучение C#, разрабатывая компьютерные игры, 2016. 210 с.

УДК 004.415.53
ГРНТИ 50.41.25

ОДНОСТРАНИЧНЫЕ WEB-ПРИЛОЖЕНИЯ АВТОМАТИЗИРОВАННЫХ ПРЕДПРИЯТИЙ СВЯЗИ

А. Д. Напалкова, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Освещаются вопросы разработки лендингов и квиз-лендингов, как одностраничных WEB-приложений, бизнес-процессов управления маркетингом и предложением продукта, взаимоотношениями с клиентами, знаниями организации и исследованиями предприятия связи, которые соответствуют требованиям ГОСТ Р 53633.0. Рассмотрена модель качества при использовании программных средств согласно ГОСТ Р ИСО/МЭК 25010 применительно к одностраничным WEB-приложений с позиции пользователя. Уточнена совокупность метрик, по которым должны быть получены количественные значения в ходе функционального, usability и A/B тестирования лендингов и квиз-лендингов.

лендинг, квиз-лендинг, модель качества при использовании, тестирование программного обеспечения, функциональное тестирование, usability тестирование.

Одностраничные WEB-приложения в формате одностраничных сайтов на одном URL-адресе (*Uniform Resource Locator*) называются «лендинг» (*landing page*, посадочная страница) [1]. Формат сайтов не предусматривает разветвленной структуры и обеспечивает просмотр информации «вверх» или «вниз» при помощи скролинга.

«Лендинг» предприятия связи создается под конкретную акцию или мероприятие с целью мотивации определенных групп потенциальных поль-

зователей и побуждения к выполнению ожидаемых действий. Примеры одностраничных WEB-приложений предприятий связи, размещенных на Интернет-ресурсах[1], представлены на рис. 1.

Анализ известных примеров «лендингов» показывает, что для достижения целей одностраничного сайта «лендинг» должен иметь:

– незначительную стоимость и сроки разработки;

– адаптивный дизайн под различное клиентское мобильное оборудование (планшеты, смартфоны и т. д.);

– уникальность и оригинальность структуризации разнородной информации;

– упрощенный вид информации и максимальную информативность представленных сведений;

– иллюстративность и образность представленных сведений для формирования побудительных мотивов;

– высокую эстетичность и зрелищность целевой информации для мотивации ожидаемых действий.

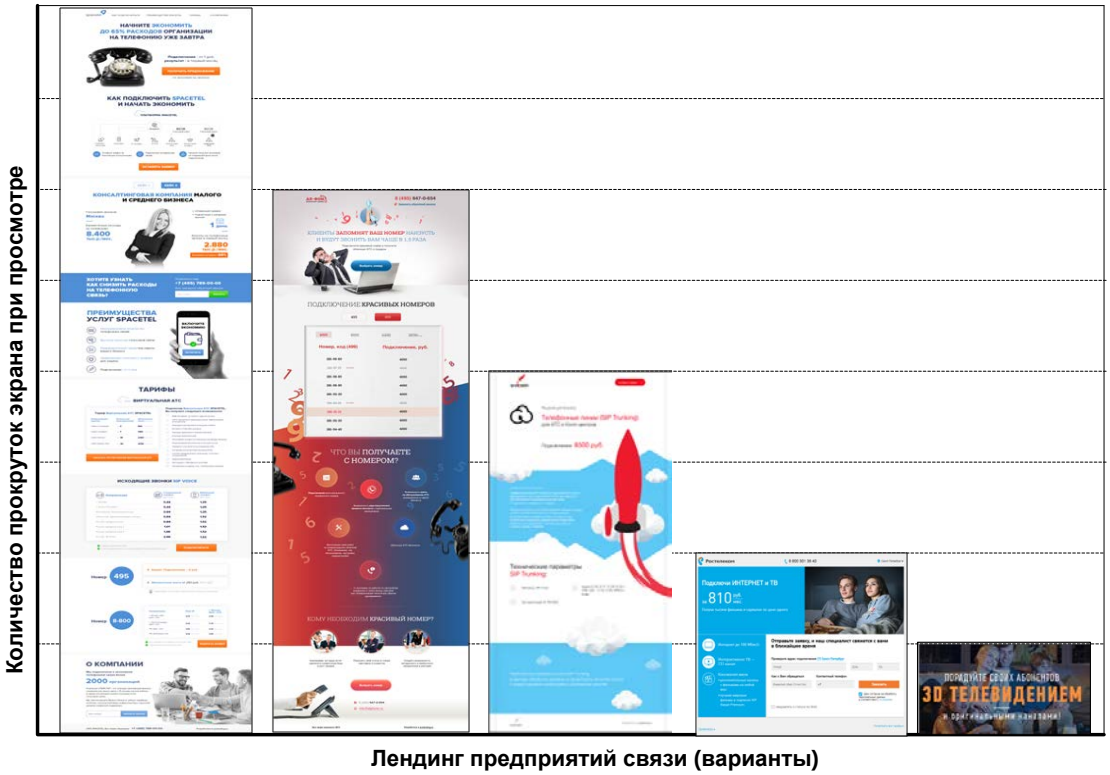


Рис. 1. Одностраничные WEB-приложения услуг предприятий связи

Результативность применения предприятиями связи «лендинга», как программного обеспечения, оценивается в процессе тестирования [2]:

1 Электронные ресурсы: http://pozovi.b-concept.ru; http://prolanding.ru/portfolio-katalog.

- «A/B/n-тестирование» – это сборка и сравнение двух или более вариантов одного и того же элемента «лендинга»;
- «сплит-тестирование» – организация тестирования за счет перенаправления трафика пользователей на один или несколько URL-адресов однотипного «лендинга» с различными вариантами реализации;
- «многовариантное тестирование», которое заключается в применении тестовых комбинаций изменений элементов «лендинга» для определения характеристик их взаимодействия;
- «испытание воронкой» – организация постоянного отображения изменений «лендинга» на нескольких страницах.

Методы и технологии тестирования «лендинга» реализуются в таких системах как платформа LP; VWO (*Visual Website Optimizer*); Googl Analytics; LPgenerator; LPmotor; Abtest; Flexbe; Unbounce; Content Experiments; Landerapp; Convert; Clickthroo; Ioninteractive; En.abtasty. Характеристики инструментальных средств тестирования VWO, LPmotor и En.abtasty приведены в таблице 1.

ТАБЛИЦА 1. Обобщенные данные средств тестирования «лендинга»

Характеристики	Инструментальные средства		
	VWO	LPmotor	En.abtasty
Методы тестирования	A/B/n-тестирование. Сплит-тестирование. Многовариантное тестирование. Испытание воронкой.	A/B-тестирование.	A/B/n-тестирование. Сплит-тестирование. Многовариантное тестирование. Испытание воронкой.
Дополнительные функции	Индикатор контроля страниц. Тепловая карта. Обработка данных опроса.	Конструктор сайтов и лендингов. Среда CRM-системы. Платежная система. Аналитическая система.	Контроль курсора. Индикатор контроля страниц. Тепловая карта. Обработка данных опроса.
Стоимость использования	В зависимости от функций.	Ежемесячно, в зависимости от функций	В зависимости от функций.
Владелец средства	Paras, Индия.	ООО "ЛПМОТОР", Россия.	AB Tasty, Франция.
Источник	https://vwo.com.	http://lpmotor.ru/	www.abtasty.com.

Развитием WEB-приложений предприятий связи для более глубокой вовлеченности пользователей в потребность потенциальных услуг и сервисов является «квиз» (англ. *quiz*, опрос), который использует опросы, игровые методы и реализуемые стимулы (например, скидки) [3].

«Квиз» – это способ детализации потребностей пользователей через формализованные варианты ответов (например, калькуляционные формы) и сбор результатов (ответов, лидов[2], заявок) по результатам опроса.

По технологии «квиз» реализуют как стандартный формализованный опрос, либо целевой опрос оператором в режиме он-лайн, либо опрос с градацией стимула в зависимости от целенаправленного участия пользователя во взаимодействии.

По форме «квиз» реализуют в виде «квиз-лендинга», «квиз-сайта» или «квиз-виджета» на сайте («лендинге»).

Примеры «квиз-лендинга», размещенные на Интернет-ресурсах[3], представлены на рис. 2.

Реализация функциональных возможностей «квиз» обусловлена применяемыми средствами разработки, характеристики которых представлены в таблице 2.

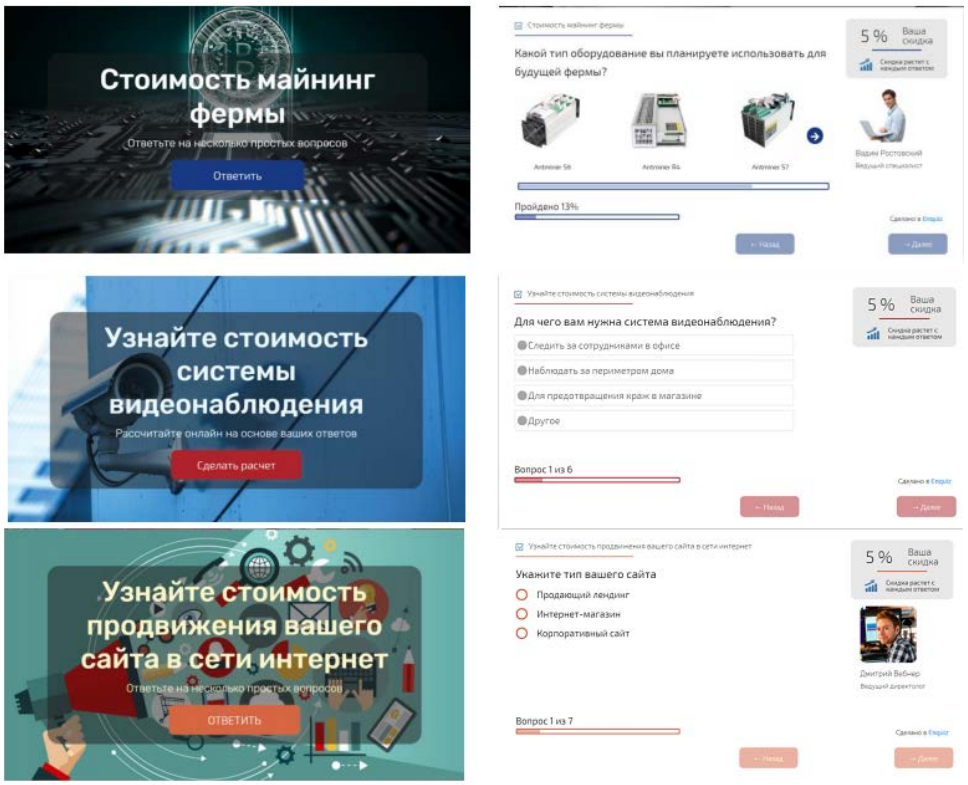


Рис. 2. Квиз-лендинг услуг предприятий связи

2 Лид-фиксация положительного интереса потенциального клиента на взаимодействие.
3 https://enquiz.io/templates

ТАБЛИЦА 2. Конструктор «квиз-лендингов»

Наименование средства	Владелец (лицензиар)	Результат разработки	Форма/обратная связь	Интернет-адрес
ENQUIZ.IO		Квиз-лендинг	Лендинг / SMS, mail, WhatsApp, Telegram, Viber, Skype	https://enquiz.io
Платформа LP	ИП Демкин М.В.	Квиз-лендинг	Лендинг / mail, SMS, Telegram	http://platformalp.ru
EnvyQuiz.io	ООО "Энвибокс"	Квиз	Виджет / mail, SMS, Telegram	https://envybox.io
Marquiz.ru	ИП Балачков Г. А.	Маркетинговый квиз	Виджет / mail, Telegram, Albato	https://www.marquiz.ru
Quizab	ИП Бакланов Д. С.	Квиз-сайт Квиз-лендинг Квиз	Лендинг, виджет/ mail, SMS,	https://quizab.com
Хамелеон для 1С-Битрикс	web-агентство «Концепт»	Квиз-сайт Квиз-лендинг Квиз	Лендинг, виджет / mail	http://quiz360.ru
«ЛПмотор» (Конструктор LPmotor)	ИП Старолат А. Ю.	Лендинг	Лендинг / mail, SMS	https://lpmotor.ru
Сервис Moclients	ИП Новицкий С. В.	Квиз	Виджет / SMS, mail	moclients.com
Конверсус	ИП Семенова В. В.	Лендинг	Лендинг / mail	https://conversus.pro

В сфере информационной технологии совместными усилиями международных организаций, таких как Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК), проведены работы по гармонизации и единству методик тестирования программных средств с подходами Института инженеров по электротехнике и радиоэлектронике (ИИЭР) [4], по результатам которых приняты стандарты ИСО/МЭК/ИИЭР 29119 [5] и [6].

Качество при использовании одностраничного WEB-приложения – степень, с которой WEB-приложение может быть применено некоторыми интернет-пользователями для удовлетворения их требований в достижении целей эффективности (в том числе и экономической), избежать риски, удовлетворенности и охвата контекста в заданных условиях использования. Такое определение обусловливает необходимость проведения оценки этой «степени», то есть проведения «валидации».

Однако реализация процедур обработки и оценки данных тестирования применительно к одностраничным WEB-приложениям («лендингу», «квиз-лендингу») предприятий связи требует детализации.

Существующие методики тестирования WEB-приложений [7], ориентированные на оценку внутренних характеристик существенных свойств программных средств, не содержат процедуры оценки с позиции целевого использования «лендинга», «квиз-лендинга» и «квиз-виджета».

Несмотря на стройную систему декомпозиции характеристик существенных свойств программных средств, которая регламентирована требованиями [6], не проработаны вопросы адаптации или уточнения под-характеристик, суб-характеристик и их метрик для проведения валидации «лендинга», «квиз-лендинга» и «квиз-виджета».

Список используемых источников

1. Петроченков А., Новиков Е. Идеальный Landing Page. Создаем продающие вебстраницы. СПб.: Питер, 2017. 320 с.

2. Блэк Р. Ключевые процессы тестирования / пер. М. Павлов. М.: Лори, 2011. 544с.

3. Жестков Н. Квиз сайт: «новое поколение лендингов». URL https://in-scale.ru/blog/kviz-sajt-novoe-pokolenie-lendingov.html (дата обращения 26.01.2019).

4. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб. : ГУАП, 2016. 325 с.

5. ГОСТ Р 56920-2016/ISO/IEC/IEEE 29119-1:2013. Системная и программная инженерия. Тестирование программного обеспечения. Часть 1. Понятия и определения.

6. ГОСТ Р ИСО/МЭК 25010-2015. Информационные технологии (ИТ). Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов. М.: Стандартинформ, 2015. 30 с.

7. Напалкова А. Д. Методика тестирования при валидации одностраничных WEB-приложений автоматизированных предприятий связи // 72-я региональная научно-техническую конференция студентов, аспирантов и молодых ученых «СТУДЕНЧЕСКАЯ ВЕСНА – 2018»: сб. ст. СПб.: СПбГУТ, 2018.

УДК 621.396.67
ГРТНИ 47.45.29

СОЗДАНИЕ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА СПЕЦИАЛИСТА УПРАВЛЕНИЯ МИНИСТЕРСТВА ЮСТИЦИИ ПО РЕСПУБЛИКЕ ХАКАСИЯ

Д. А. Никулин, С. А. Комисаров

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Данная статья представляет собой описание процесса создания информационной подсистемы «Реестр адвокатов», которая служит для редактирования данных об адвокатах и формирования отчетов на их основе. Продукт разработан для сотрудников отдела по контролю и надзору в сфере адвокатуры, нотариата, государственной регистрации актов гражданского состояния Управления Министерства юстиции.

информационные системы, базы данных, концептуальная модель.

Роль информатизации в современном мире очевидна. Предприятия стремятся автоматизировать различные области своей деятельности, поскольку от уровня автоматизации зависит производительность работы организации в целом. Для этого внедряются различные программные комплексы, которые в совокупности образуют информационную систему предприятия. Информационная система (по законодательству Российской Федерации) представляет собой организационно упорядоченную совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы. Большое внимание при создании подобных систем уделяется функциональности, надежности и защищенности от взлома.

Актуальность данной работы обуславливается тем, что сегодня как в России в целом, так и в Республике Хакасия в частности, активными темпами идет процесс автоматизации в различных областях деятельности. Од-

ним из основных направлений автоматизации является разработка информационных систем, поддерживающих различные виды деятельности организации и корректно выполняющих поставленные перед ней задачи. ИС даже частично не удовлетворяющие своим основным задачам способны не только понизить производительность работы в области их применения, но и привести к различным проблемам в деятельности организации. Учитывая темпы развития аппаратных и программных средств, информационные системы нуждаются в периодической модернизации, что позволяет добиться как повышения производительности работы организации, так и исключить риск возникновения критических ситуаций в будущем.

Для исследования рассматриваемой области применялись следующие методы:

– анализ организационных материалов;
– консультации у сотрудников организации;
– анализ используемых программных и аппаратных средств;
– анализ информационных потоков внутри организации.

Полная модернизация информационной подсистемы «Реестр адвокатов» приведет к росту производительности отдела по контролю и надзору в сфере адвокатуры, нотариата, государственной регистрации актов гражданского состояния Минюст и значительному уменьшению шанса возникновения критических ситуаций при работе с данными из реестра.

Проектирование программного продукта

Первым шагом проектирования информационной подсистемы «Реестр адвокатов» является построение моделей описания информационных потоков. Для данного проекта наиболее предпочтительным является построение концептуальной, логической, функциональной моделей и модели данных. В комплексе данные модели позволяют определить общую структуру подсистемы.

Концептуальная модель

В концептуальной модели в качестве пользователя выступает сотрудник отдела по контролю и надзору в сфере адвокатуры, нотариата, государственной регистрации актов гражданского состояния. Сотрудник имеет полный доступ к данным, а также имеет возможность распечатывать отчеты на основе данных, находящихся в базе.

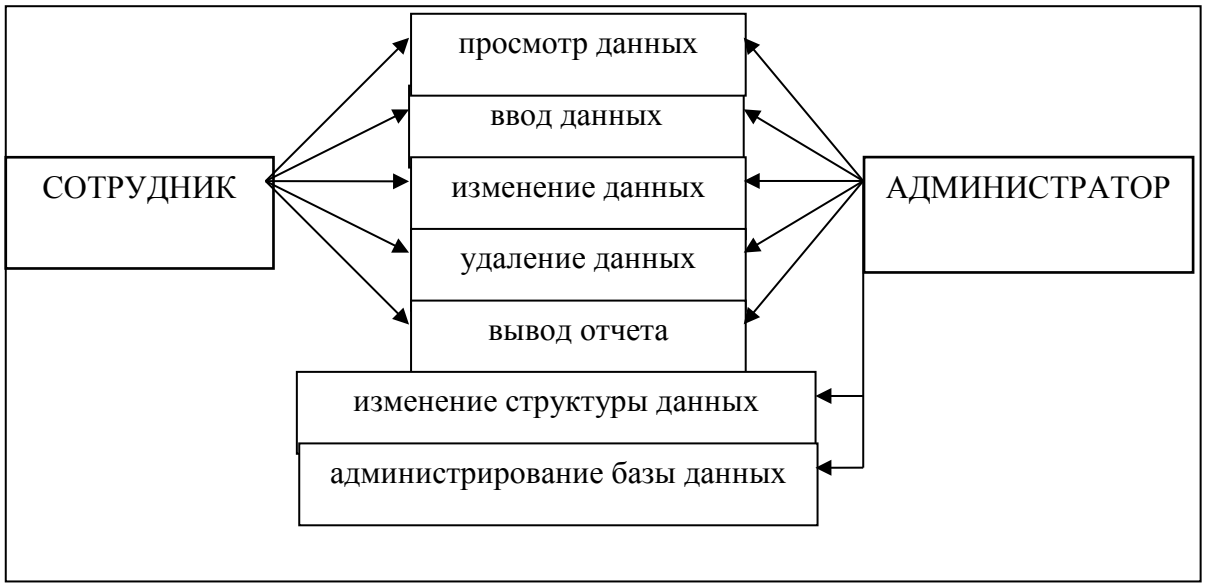


Рис. 1. Концептуальная модель

Модель данных

Модель данных представлена в виде ER-диаграммы. Модель показывает предварительную структуру проектируемой базы данных. Как видно из схемы, главной таблицей будет блок «Адвокаты». Таблицы базы данных приведены к третьей нормальной формы, дабы избавиться от избыточности данных.

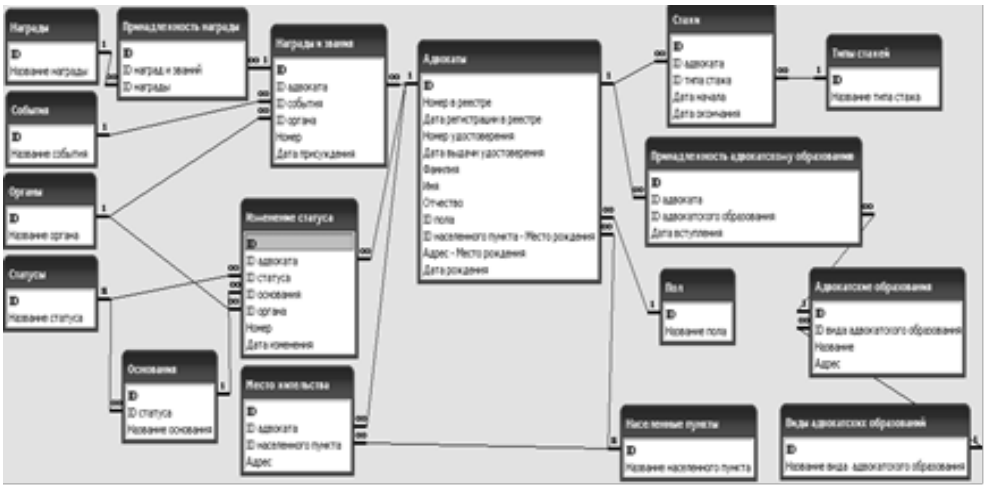


Рис. 2. Модель данных

Как уже отмечалось, целью проекта является разработка модифицированной информационной подсистемы «Реестр адвокатов». Система будет сетевой и централизованной, следовательно, будет состоять из двух частей: серверная и клиентская.

В качестве сервера баз данных системы «Реестр адвокатов» используется Microsoft SQL Server 2012, потому как данная СУБД приобретена Минюстом и используется в деятельности Управления.

Не последнюю роль играет опыт создания приложений в данных языках и личное предпочтение. В результате проведенного анализа сред разработки, наиболее предпочтительным для реализации данного проекта стал продукт Embarcadero RAD Studio XE2.

Проведенный анализ предметной области позволил выявить узкие места в работе Управления Министерства юстиции по Республике Хакасия. Рассмотрение аппаратной части позволило выявить моменты, не имеющие большого значения сегодня, но которые приведут к определенным неудобствам в будущем при увеличении размеров сети. Что касается программной оснащенности, то в этой области были обнаружены недостатки в информационной системе сотрудников отдела по контролю и надзору в сфере адвокатуры, нотариата, государственной регистрации актов гражданского состояния. В качестве решения данной проблемы предложено создать новую систему, в которой будут устранены погрешности существующей.

В качестве первого шага в проектировании автоматизированного рабочего места сотрудника вышеописанного отдела были построены концептуальная и логическая модели, которые отображают структуру планируемого проекта. Заключительным шагом был выбор средств разработки проекта. В качестве оптимального решения будет использование средств Embarcadero RAD Studio XE2 и Microsoft SQL Server 2012.

Разработана информационная система «Реестр адвокатов», состоящая из двух основных частей: серверной и клиентской. Серверная часть реализована в среде Microsoft SQL Server 2012 и представляет собой структуры базы данных. Все таблицы в данной базе приведены к третьей нормальной форме, что исключает избыточность информации. Клиентская часть реализована в среде Embarcadero RAD Studio XE2 и представляет собой клиент к базе данных на сервере. Система разработана с учетом всех пожеланий сотрудников отдела Минюст. Работа приложения основана на интерфейсе доступа к данным ADO и языке запросов SQL. Все требования технического задания были выполнены. Таким образом, создана информационная система, автоматизирующая работу сотрудников отдела по контролю и надзору в сфере адвокатуры, нотариата, государственной регистрации актов гражданского состояния Управления Министерства юстиции по Республике Хакасия.

На основе тестов информационной системы был проведен анализ качества. Анализ проводился по характеристикам, имеющим наибольшее значение для данной системы: функциональность, надежность, безопасность информации и удобство работы. Анализ показал достаточный уровень качества продукта. элементов, использованию различных панелей, горячих

клавиш и т. д. Необходимо отметить, что затраты на разработку указанной информационной подсистемы «Реестр адвокатов» оказались весьма незначительны, а внедрение данной системы не предполагает каких-либо изменений в работе аппаратного обеспечения организации.

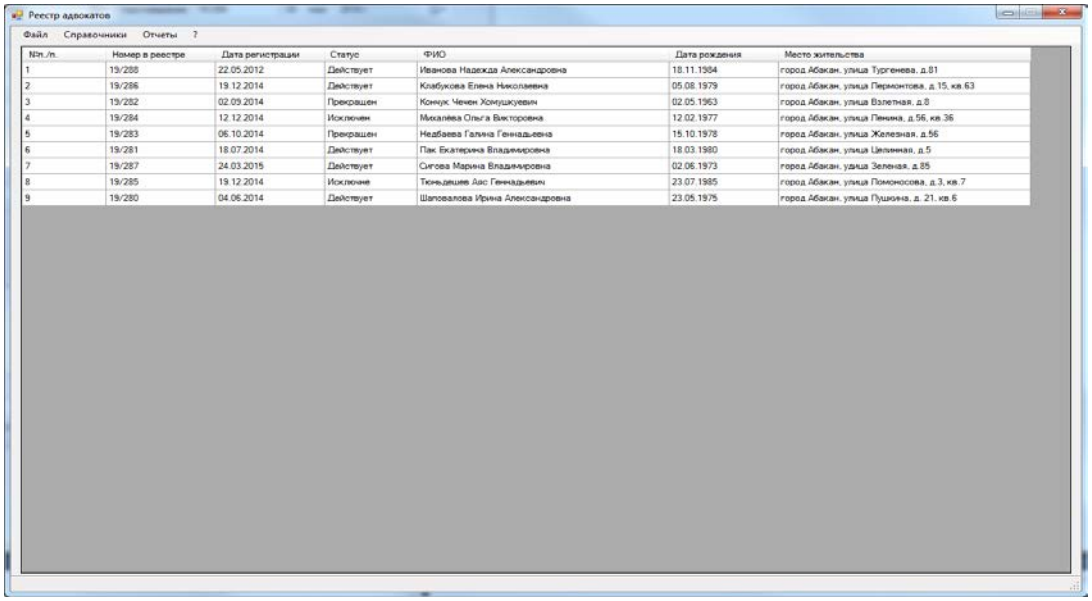


Рис. 3. Главное окно программы «Реестр адвокатов»

Список используемых источников

1. Коннолли Т., Бегг К. Базы данных: проектирование, реализация и сопровождение. М.: Диалектика, 2000. 713 с.

2. Буч Г. Объектно-ориентированное проектирование с примерами применения. М.: Конкорд, 1992. 356 с.

3. Абрамян М. Э. Delphi 7. Карманный справочник с примерами. М.: Кудиц-Образ, 2010. 233 с.

4. Пирогов В. Н. MS SQL SERVER 2012: Управление и программирование. СПб.: Питер, 2002. 686 с.

5. Борисок В. В., Корвель Ю. И., Чиртик А. Н. Delphi. Трюки и эффекты. СПб.: Питер, 2006. 356 с.

6. Луис Д. Проектирование баз данных на SQL Server 2012. М.: Бином, 2014. 510 с.

7. Мамаев Е., Шкарина Л. Microsoft Server 2000 для профессионалов. СПб.: Питер, 2001. 1085 с.

8. Мандел Т. Разработка пользовательского интерфейса. М.: ДМК Пресс, 2015. 383 с.

УДК 004.056.5
ГРНТИ 81.93.29

ОБОБЩЕННЫЙ АЛГОРИТМ УСТРАНЕНИЯ НЕОПРЕДЕЛЕННОСТИ ОЦЕНКИ И КАТЕГОРИЗАЦИИ СМЫСЛОВОГО НАПОЛНЕНИЯ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ В ИНТЕРЕСАХ ОБНАРУЖЕНИЯ И ПРОТИВОДЕЙСТВИЯ НЕЖЕЛАТЕЛЬНОЙ ИНФОРМАЦИИ

И. Б. Паращук[1,2], И. Б. Саенко[1,2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Проведен анализ современных методологических подходов, частных моделей и методов преодоления неопределенности исходных данных, необходимых для решения задач анализа цифрового сетевого контента. Детально рассмотрены особенности синтеза достоверного пространства признаков нежелательной информации в различных условиях неопределенности. Предложена схема поэтапной обработки информации при решении таких задач синтеза, при этом учитывается, что неопределенность признаков нежелательной информации может иметь характер недостоверности (неполноты) и неоднозначности (нечеткости). Сформулированы этапы обобщенного алгоритма устранения неопределенности оценки и категоризации смыслового наполнения информационных объектов в интересах обнаружения и противодействия нежелательной информации.

неопределенность, контент, синтез, признак, нежелательная информация, пространство, информационный объект, недостоверность, нечеткость

Многоаспектная оценка и категоризация смыслового наполнения информационных объектов, по сути, является многокритериальным контент-анализом. Иными словами, это анализ содержания и смысла, набор средств и методики исследования, предметом анализа которых является содержание и смысл текстовых, графических, речевых и видео массивов, а также иных продуктов коммуникативной корреспонденции. Принято считать, что компонентами оценки и категоризации смыслового наполнения информационных объектов являются компоненты сбора, предварительной обработки и хранения информационных объектов, семантического анализа вредоносных информационных объектов, выявления источников

нежелательной информации и целевой аудитории воздействия, анализа каналов распространения вредоносных информационных объектов и комплексного распознавания элементов воздействия.

При этом, в рамках перспективной интеллектуальной системы (ИС) аналитической обработки (АО) цифрового сетевого контента (ЦСК), вместе с компонентами многоаспектной оценки и категоризации смыслового наполнения должны быть размещены компоненты устранения неопределенности исходных данных, и, как следствие, неопределенности результатов этих процессов – процессов оценки и категоризации [1, 2]. Действительно, практический опыт в области контент-анализа, объективная, достоверная оценка номенклатуры и содержания цифрового сетевого контента показывает, что объективный анализ этого контента (смыслового наполнения) информационных объектов невозможны без обработки данных и, соответственно, получаемых на их основе выводов и знаний, в условиях неопределенности, без привлечения алгоритмов анализа противоречивых и динамичных (изменяющихся) знаний. Исследования показывают, что большинство задач интеллектуальной обработки данных для обнаружения и противодействия нежелательной информации приходится решать в условиях различного рода неопределенности, привлекая нечеткие множества (НМ) [3] или искусственные нейронные сети (ИНС) [4].

Именно поэтому необходимо обеспечить способность ИС АО ЦСК при оценке и категоризации учитывать одновременно два ключевых вида неопределенности: неоднозначность (нечеткость) и недостоверность (недостаточность, неполноту, противоречивость) исходной информации – анализируемых признаков нежелательной информации (ПНИ). Известны методы и частные алгоритмы устранения неопределенности разнообразных данных – параметров (признаков) анализируемой информации в интересах задач выявления и противодействия вредоносным воздействиям в различных условиях, т. е. алгоритмы синтеза достоверного пространства ПНИ, оценки которых необходимы администратору безопасности как лицу, принимающему решения (ЛПР), или системе принятия решений (СПР) в конкретных условиях. Данные методы и алгоритмы способны решать частные задачи синтеза достоверного пространства ПНИ в различных условиях неопределенности. Однако необходим механизм выбора (адаптации), позволяющий использовать для конкретных условий адекватный метод (алгоритм) синтеза, либо комплекс методов (алгоритмов) синтеза достоверного пространства ПНИ. Необходимость разработки обобщенной алгоритмической структуры устранения неопределенности оценки и категоризации смыслового наполнения информационных объектов в интересах обнаружения и противодействия нежелательной информации, обобщенного алгоритма синтеза достоверного пространства ПНИ обусловлена тем, что имеющиеся отдель-

ные, частные алгоритмы синтеза предназначены для решения узких локальных задач в различных условиях неопределенности. Критериями выбора того или иного метода (алгоритма) синтеза достоверного пространства ПНИ служит вид (уровень) целевой, природной и поведенческой неопределенности исходной информации, характеризующей изменяющиеся задачи выявления и противодействия нежелательной информации и обуславливаемой различного рода воздействиями, имеющими место в процессе технической эволюции (ТЭ), жизненного цикла (ЖЦ) и эксплуатации ИС АО ЦСК в конкретной обстановке.

Иллюстрацией общего подхода, определяющего ключевые этапы алгоритма (обобщенной алгоритмической структуры) устранения неопределенности оценки и категоризации смыслового наполнения информационных объектов в интересах обнаружения и противодействия нежелательной информации, может служить схема поэтапной обработки информации при решении задачи формулировки достоверного (полного), операционного, декомпозированного, безызбыточного, минимального и измеримого пространства ПНИ (рис.).

Схема, представленная на рисунке ниже, показывает, что решение задачи формулировки достоверного пространства ПНИ в интересах оценки и категоризации смыслового наполнения информационных объектов для обнаружения и противодействия нежелательной информации может быть получено на основе методов предобработки и с учетом двух ключевых видов неопределенности: неоднозначности (нечеткости) и недостоверности (недостаточности, неполноты, противоречивости) исходной информации (анализируемых ПНИ), обусловленных тремя основными источниками: (1) наличием целенаправленного противодействия со стороны источников и распространителей нежелательной информации, способы действия которых неизвестны (поведенческая неопределенность); (2) недостаточной изученностью некоторых явлений, сопровождающих процессы, реализуемые в рамках функционирования ИС АО ЦСК (природная неопределенность) и (3) недостаточно четким представлением цели, общей задачи функционирования ИС АО ЦСК (целевая неопределенность). Опираясь на этапы обработки информации при решении задачи синтеза достоверного пространства ПНИ, можно описать обобщенную алгоритмическую структуру устранения неопределенности оценки и категоризации. В рамках описания реализуется совместная поэтапная процедура предобработки, а также синтеза достоверного пространства ПНИ в условиях неоднозначности (нечеткости) и недостаточности (неполноты) исходной информации, обусловленных поведенческой, природной и целевой неопределенностью, присущей реальным процессам обнаружения ПНИ и противодействия информации такого класса.

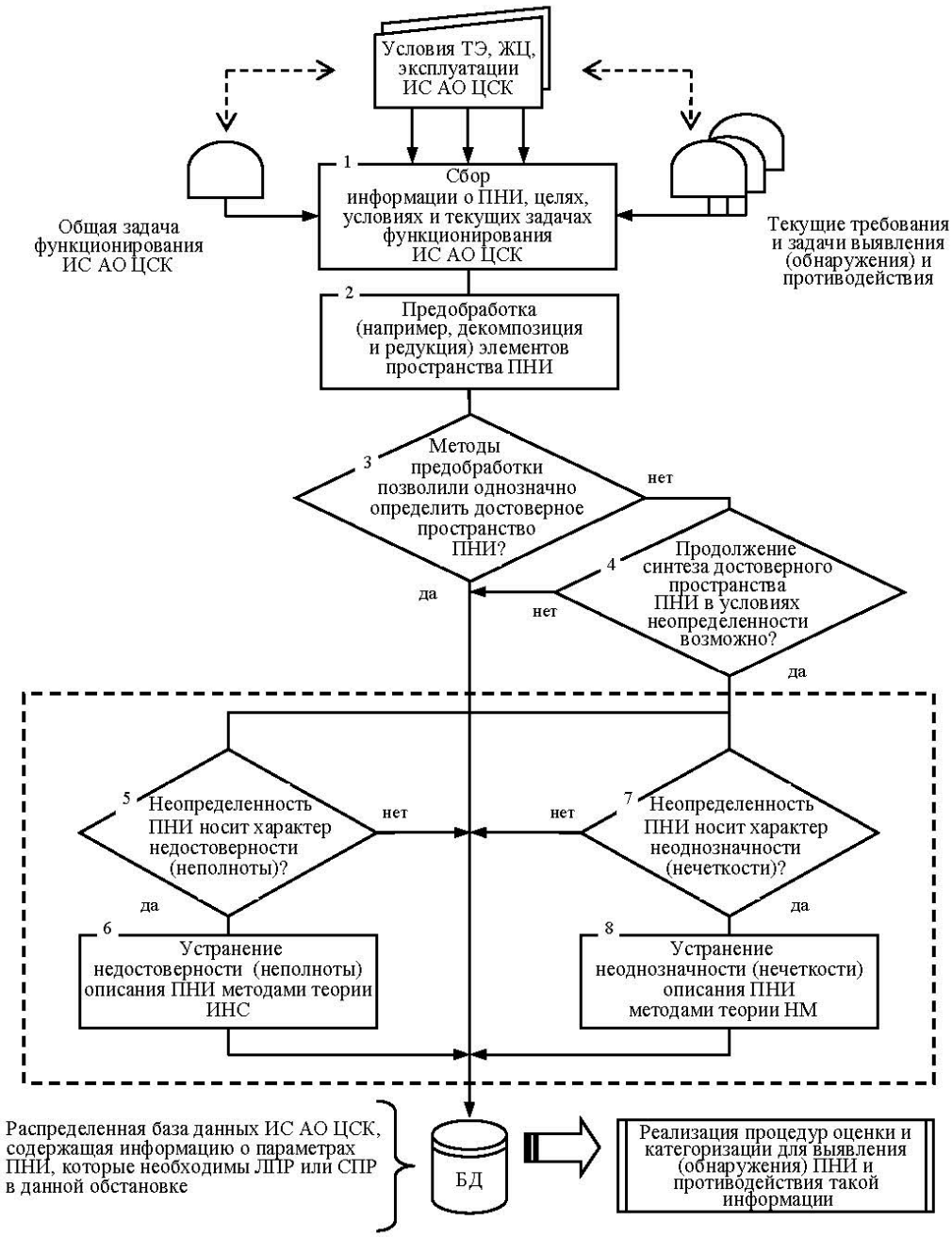


Рисунок. Схема поэтапной обработки информации при решении задачи синтеза достоверного пространства ПНИ в интересах оценки и категоризации

Использование в рамках этой структуры как апробированных подходов к предварительной обработке информации, так и новых подходов к решению задачи синтеза достоверного пространства ПНИ в условиях неопределенности, позволяет, сохраняя достоинства (математическую корректность, учет корреляционных связей ПНИ и т. д.) алгоритмов предобработки, учесть как объективную (объекты и процессы), так и субъективную (ЛПР) неопре-

деленность, возникающую при принятии решений о том, являются ли анализируемые признаки информационных объектов признаками нежелательной информации. Данный подход обладает рядом достоинств по сравнению с традиционными методами многокритериального контент-анализа. Существующие методы позволяют отчасти решить проблему минимизации перечней анализируемых параметров (признаков) ЦСК. Актуальность этой проблемы не вызывает сомнений. С одной стороны, ИС АО ЦСК призвана анализировать сетевой трафик с общим числом параметров (признаков) превышающим иногда сотни и тысячи. С другой стороны, только незначительная их часть несет признаки именно нежелательной информации, которую действительно необходимо выявлять в конкретных условиях обстановки.

Вместе с тем, обобщенная алгоритмическая структура синтеза достоверного пространства ПНИ позволяет решать эту проблему с учетом различного вида неопределенности, позволяя выполнять требования по полноте, оперативности, декомпозированности, безызбыточности, минимальной размерности и измеримости параметров (признаков) нежелательной информации. Таким образом, компоненты устранения неопределенности оценки и категоризации в рамках архитектуры ИС АО ЦСК отвечают за [5]: устранение неоднозначности (нечеткости) исходных данных для многоаспектной оценки и категоризации смыслового наполнения информационных объектов; устранение недостоверности (недостаточности, неполноты, противоречивости) этих исходных данных.

Применение рассмотренных методов и алгоритмов обработки неполных, противоречивых и нечетких знаний позволяет повысить достоверность оценивания и категоризации смыслового наполнения, а значит, в конечном итоге, повысить обоснованность принимаемых решений по обнаружению и противодействию нежелательной, сомнительной и вредоносной информации.

Работа выполнена при финансовой поддержке РНФ (проект 18-11-00302).

Список используемых источников

1. Котенко И. В., Паращук И. Б. Общая архитектура интеллектуальной системы аналитической обработки цифрового сетевого контента в интересах защиты от нежелательной информации // Материалы конференции «Информационные технологии в управлении» (ИТУ-2018). СПб.: АО «Концерн «ЦНИИ «Электроприбор», 2018. 742 с., С. 501–505.

2. Котенко И. В., Саенко И. Б., Чечулин А. А. Защита от нежелательной и вредоносной информации в глобальных информационных сетях // Информационно-психологическая и когнитивная безопасность. Коллективная монография / Под ред. И. Ф. Кефели, Р. М. Юсупова. СПб.: Изд-во «Петрополис», 2017. 300 с. С. 175–194.

3. Авраменко В. С., Беденков В. Н., Бобрешов-Шишов Д. И., Маликов А. В. Определение актуальных угроз безопасности информации в инфокоммуникационных системах на основе аппарата нечеткой логики. // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. В 4-х т. СПб.: СПбГУТ, 2017. Т. 3. 535 с. С. 13–18.

4. Паращук И. Б., Дойникова Е. В., Котенко И. В. Подход к выработке требований по устранению неполноты и противоречивости оценки и категоризации смыслового наполнения информационных объектов // Региональная информатика (РИ-2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». Санкт-Петербург, 24–26 октября 2018 г.: Материалы конференции. СПб.: СПОИСУ, 2018. 631 с., С. 162–164.

5. Котенко И. В., Саенко И. Б., Паращук И. Б., Чечулин А. А. Ключевые архитектурные решения по построению интеллектуальной системы аналитической обработки цифрового сетевого контента в интересах защиты от нежелательной информации // Региональная информатика (РИ-2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». Санкт-Петербург, 24–26 октября 2018 г.: Материалы конференции. СПб.: СПОИСУ, 2018. 631 с., С. 151–153.

УДК 658.8.012.12
ГРНТИ 28.29.15

ОПТИМИЗАЦИЯ УПРАВЛЕНИЯ МАРКЕТИНГОМ ПРЕДПРИЯТИЯ НА ОСНОВЕ ПРИМЕНЕНИЯ МЕТОДОВ ИССЛЕДОВАНИЯ ОПЕРАЦИЙ

Э. Б. Песиков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается один из возможных подходов к построению аналитического инструментария управления маркетингом предприятия, предназначенного для выбора оптимальных ассортимента, объемов продаж, сегментов рынка и цен на продукцию и основанного на применении математических методов исследования операций. Предлагается модель нелинейного частично-целочисленного программирования с переменными непрерывного и булевого типа, применение которой позволяет планировать производство как ранее выпускаемой, так и новой продукции. Для анализа оптимизационной модели предлагается использовать эвристический алгоритм, основанный на итерационном увеличении цен на продукцию и решении на каждом шаге изменения цен задачи линейного частично-целочисленного программирования методом Лэнда и Дойга.

предприятие, маркетинг, оптимизация, исследование операций, целевой сегмент, объем продаж, цена продукта.

Введение

Актуальность темы исследования обусловлена необходимостью формирования эффективной маркетинговой стратегии предприятия в условиях высокой динамики изменений параметров рынка, высокой остроты конкуренции и ограниченности производственных ресурсов [1].

Целью работы является разработка аналитического инструментария оптимального планирования товарной, сбытовой и ценовой стратегий предприятия, основанного на эвристических методах и моделях математического программирования. В основу предлагаемого инструментария положена математическая модель выбора оптимального ассортимента, объемов продаж, сегментов рынка и цен на продукцию за плановый период [2]. С помощью предлагаемой оптимизационной модели представляется возможным планировать производство и реализацию как ранее производимой, так и новой продукции.

Постановка задачи

Пусть предприятие работает со своими продуктами на определенных рынках (или сегментах рынка). В товарном портфеле предприятия имеются также виды продукции, с которыми предприятие еще не выходило на рынок и по которым необходимо принимать решение о целесообразности их производства и вывода на рынок. Проведенные маркетинговые исследования позволили оценить емкости рынков сегментов, на которых предприятие уже работает или предполагает выходить со своими продуктами. Маркетологи определили также по каждому сегменту рынка предельные значения цен, по которым потребитель согласен приобрести продукты. Руководство предприятия ставит перед собой задачу достичь в планируемом периоде определенных значений таких целевых показателей как прибыль от реализации продукции и доля рынка, контролируемая предприятием. Ожидаемые уровни наличных производственных ресурсов (материалы, оборудование и трудовые ресурсы) в планируемом периоде определены и используются при планировании в качестве ограничивающих факторов. Предполагаются заданными нормы расхода ресурсов на единицу каждого вида продукта; затраты на реализацию (транспортные и торговые издержки, затраты на рекламу) единицы продукта для каждого сегмента рынка; цены единицы каждого вида ресурса.

Требуется определить на какие сегменты рынка, с какими продуктами, объемами предложения и ценами следует выходить предприятию на рынок при условии, что будут реализованы цели предприятия, учтены ограничения по спросу и производственным ресурсам и при этом ожидаемая прибыль от

производства и реализации продукции достигнет своего максимального значения.

Математическая модель задачи

Формализация процесса выбора сегментов рынка, ассортимента продукции, объемов предложения и цен на продукцию проводится в терминах математического программирования. При построении математической модели случайные параметры модели (например, спрос на продукты на различных сегментах рынка) заменяются их математическими ожиданиями. Построение математической модели проводится для фиксированного временного интервала, т. е. процесс планирования исследуется в статической постановке. При необходимости построения динамической модели, т. е. рассмотрения процесса планирования в динамике, следует задавать временную определенность всем переменным и параметрам рассматриваемой математической модели.

Рассмотрим компоненты предлагаемой оптимизационной модели.

Управляемыми переменными в модели являются:

x_{jf} – объем продаж продукта j на сегменте f; причем $j \in J_1$ *и* $j \in J_2$,

где J_1 – множество продуктов j, с которыми предприятие уже работает на рынке;

J_2 – множество продуктов j, по которым предприятие должно принимать решение о выходе на рынок;

$f \in F$, где F – множество сегментов f, на которых предприятие может работать со своими продуктами;

w_{jf} – булевые переменные, управляющие включением в план производства и реализации «новых», ранее разработанных товаров (показатели целесообразности выхода на рынок с определенным товаром); причем переменные w_{jf} такие, что $w_{jf} = 1$, если продукт j будет реализовываться на сегменте рынка f и $w_{jf} = 0$ – в противном случае;

g_{jf} – цена единицы продукта j, по которой продукт будет реализоваться на сегменте f;

k_{jf} – булевые переменные, отслеживающие факт превышения расчетных цен g_{jf} заданных предельных цен $q_{jf}^{\text{пр}}$ для сегмента f;

Переменные k_{jf} такие, что $k_{jf} = 1$, если $g_{jf} \le q_{jf}^{\text{пр}}$ и $k_{jf} = 0$, если $g_{jf} > q_{jf}^{\text{пр}}$.

Рассмотрим систему ограничений на значения управляемых переменных, описывающую условия функционирования исследуемой производственной системы.

Ограничение, гарантирующее предприятию достижение в планируемом периоде заданного уровня прибыли от производства и реализации продукции, имеет вид

$$P(x,w,g,k)=\left[\sum_{j\in J}\left(\sum_{f\in F}g_{jf}k_{jf}x_{jf}-\sum_{f\in F}S_{jf}x_{jf}-\sum_{l\in L}\tilde{q}_l m_{jl}\sum_{f\in F}x_{jf}\right)\right]\geq P_0,$$

где *sjf* – затраты на реализацию единицы продукта *j* на сегменте *f*;

$\tilde{q}_l$ – цена единицы ресурса *l*;

m_{jl} – норма расхода ресурса *l* на единицу продукта *j*;

L – множество наименований производственных ресурсов «*l*» ;

P_o – желаемое значение прибыли предприятия от реализации продукции за планируемый период;

$$k_{jf}=\begin{cases}1, \text{ если } q_{jf}\leq q_{jf}^{\text{пр}};\\ 0, \text{ если } q_{jf}>q_{jf}^{\text{пр}}.\end{cases}$$

Ограничения, гарантирующие предприятию достижение заданного значения доли рынка для каждого исследуемого сегмента, сводятся к системе неравенств вида:

$$\sum_{j\in J_1}x_{jf}+\sum_{j\in J_2}x_{jf}\geq b_f E_f,\ f\in F,$$

где b_f – желаемое значение доли рынка *f*-го сегмента;

E_f – емкость рынка сегмента *f*'.

Ограничения на значения объемов предложения продукции на различных сегментах рынка имеют вид:

$$\underline{a}_{jf}\leq x_{jf}\leq \bar{a}_{jf},\ j\in J_1;\ f\in F,$$
$$\underline{a}_{jf}w_{jf}\leq x_{jf}\leq \bar{a}_{jf}w_{jf},\ j\in J_2;\ f\in F,$$
$$0\leq w_{jf}\leq 1;$$
$$w_{jf}\ -\text{целые},$$

где $\underline{a}_{jf}$, $\bar{a}_{jf}$ – соответственно нижняя и верхняя границы объема предложения продукта *j* на сегменте *f* ($\underline{a}_{jf}$, – обязательная часть объема производства продукта *j* для реализации его на сегменте *f*;

$\bar{a}_{jf}$ – платежеспособный спрос на продукт j на сегменте f).

Ограничения по производственным ресурсам, гарантирующие не превышение расчетной потребности в ресурсах уровней наличных ресурсов, сводятся к следующим неравенствам:

$$\sum_{j \in J} m_{jl} x_{jf} \le M_1, \ \ l \in L,$$

где M_l – уровень наличных ресурсов вида l в планируемом периоде.

Ограничения на значения цен продуктов записываются следующим образом:

$$q_{jf} \le g_{jf} \le q_{jf}^{np}, \ j \in J_1; \ f \in F$$
$$q_{jf} w_{jf} \le g_{jf} \le q_{jf}^{np}, \ j \in J_2, \ f \in F$$

где q_{jf} – нижняя граница цены единицы продукта j на сегменте f (например, себестоимость продукта).

$q_{jf}^{\text{пр}}$ – предельная цена продукта j на сегменте f.

Критерием оптимальности (целевой функцией) задачи является максимизация ожидаемой прибыли от реализации продукции за планируемый период:

$$\max_{x,w,g,k} P\left(x, w, g, k\right).$$

В итоге получаем следующую формулировку задачи: требуется найти такие значения $x^*=||x^*_{jf}||$, $w^*=||w^*_{jf}||$, $g^*=||q^*_{jf}||$ и $k^*=||k^*_{jf}||$ управляемых переменных, которые удовлетворяли бы системе ограничений и при этом доставляли бы максимум целевой функции $P(x, w, q, k)$.

Оптимизационная модель относится к классу моделей нелинейного программирования с управляемыми переменными целого (булевого) и непрерывного типа [3, 4].

Для анализа модели предлагается применять эвристический алгоритм, основанный на поэтапном увеличении значений цен продуктов и решении на каждом этапе соответствующей задачи частично-целочисленного программирования методом ветвей и границ (методом Лэнда и Дойга). При итерационном увеличении цен (начиная с себестоимости продуктов) ожидаемая прибыль вначале должна расти за счет роста объема выручки. В дальнейшем отдельные виды продуктов, для которых текущие значения цен будут превышать предельные цены для сегментов, начнут “выпадать” из сегментов. В результате рост прибыли должен замедлиться и начиная с

определенной итерации прибыль будет уменьшаться. Значения объемов предложения и цен на продукты, а также множество оставшихся сегментов на определенном шаге итерационного процесса, при котором достигается максимальная прибыль предприятия, будут соответствовать оптимальному решению задачи (см. рис.).

В результате решения задачи представляется возможным оптимизировать выбор целевых сегментов, ассортимента и объемов продаж продукции, а также цен на продукты на каждом сегменте; наиболее полно учесть потребительский спрос; максимизировать ожидаемую прибыль от продаж продукции и эффективность использования производственных ресурсов.

Рисунок. График зависимости прибыли от номера итерации изменения цен

Для решения исследуемой задачи использовался оптимизационный пакет прикладных программ «Lindo», предназначенный для решения задач линейного и частично-целочисленного программирования [5].

Заключение

Анализ результатов вычислительных экспериментов на ПК позволяет сделать вывод о корректности принятых допущений и ограничений исследуемой математической модели поведения предприятия на рынке и работоспособности предлагаемого метода решения задачи.

Применение методов исследования операций при формировании маркетинговой стратегии предприятия позволяет существенно повысить эффективность принимаемых маркетинговых решений. Предложенный в работе вычислительный алгоритм может быть положен в основу компьютерных систем поддержки принятия решений при стратегическом управлении маркетингом предприятия.

В дальнейшем для повышения адекватности моделирования предполагается применить стохастический подход, основанный на построении одноэтапной модели стохастического программирования с вероятностными ограничениями и последующим переходом с заданным уровнем риска к ее детерминированному эквиваленту.

Список используемых источников

1. Котлер Ф. Основы маркетинга; пер. с англ. Е. М. Пенькова. М.: Прогресс, 2008.
2. Песиков Э. Б. Стратегическое планирование. Решение задачи выбора оптимальных сегментов рынка, ассортимента, объёмов предложения и цен изданий // «Print & Publishing». 2001. № 46. С. 48–50.
3. Вентцель Е. С. Исследование операций: задачи, принципы, методология. М.: Дрофа, 2004.
4. Зайченко Ю. П. Исследование операций. Учебник. 6-е изд. Киев: Слово, 2003.
5. LindoSystems Inc / сайт разработчика программной системы «Lindo». URL: http://www.lindo.com/.

УДК 65.011.56, 004.624, 004.622
ГРНТИ 49.01.85, 50.01.85

К ВОПРОСУ О МНОГОЦЕЛЕВОЙ ТРАНСФОРМАЦИИ АВТОМАТИЗИРОВАННОГО УЧЕТА ПРЕДПРИЯТИЯ СВЯЗИ

Я. А. Плетнев, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Значительные успехи в трансформации цифровых платформ бизнес-процессов различных областей деятельности оператора связи согласно концепции NGOSS обусловили возможность продвижения мобильного сервиса учетных задач предприятия связи применительно к материальным активам с особым правовым (юридическим) статусом и спецификой инвентаризации, учета и ведения, например, экспонатов, музейных предметов и коллекций. Предлагаемые технические решения усовершенствованного мобильного сервиса учетных задач позволяют расширить его использование различными организациями (учреждениями, предприятиями) в условиях цифровой экономики.

многоцелевая трансформация, учет, NGOSS, облачные вычисления.

Информационные технологии с каждым годом оказывают все большее влияние как на экономику, так и на повседневную жизнь людей и их развитие является одним из важнейших факторов, способствующих решению ключевых задач государственной политики Российской Федерации.

Одним из ожидаемых результатов реализации государственной программы Российской Федерации «Информационное общество (2011–2020 годы)», является обеспечение развития сервисов на основе информационно-телекоммуникационных технологий, в том числе в сферах культуры, образования, науки и здравоохранения [1].

Дальнейшее развитие этого направления предусмотрено в национальной программе «Цифровая экономика Российской Федерации» до 2024 года, в частности, национальных проектах «Информационная инфраструктура», «Цифровая технология» и «Цифровое государственное управление» [2].

Программными мероприятиями предусмотрено стимулирование развития отрасли связи посредством развития сетей связи и инфраструктуры хранения и обработки данных, которые позволят повысить эффективность реализации текущих и перспективных инфраструктурных проектов государства, государственных компаний, а также компаний с государственным участием.

Достаточно актуальным в условиях цифровой экономики является трансформация автоматизированных задач учета бизнес-процессов оператора связи (предприятий и организаций – в терминах [3]) под особенности организации учетных задач субъектов хозяйственной деятельности в различных отраслях экономики, а также предоставление доступных и соответствующих им «облачных» сервисов [4]).

Автоматизированный учет оператора связи (предприятия, организации) предназначен для обеспечения выполнения учетных задач в бизнес-процессах (производственных процессах), как представлено на рис. 1, определены моделью Enhanced Telecom Operations Map (eTOM) и регламентированы нормативно-техническими документами России [5, 6].

Перечни учетных задач в зависимости от областей бизнес-процессов модели eTOM можно представить в виде трех обобщенных групп:

- стратегического менеджмента;
- операционной деятельности оператора (предприятия) связи;
- управления организацией.

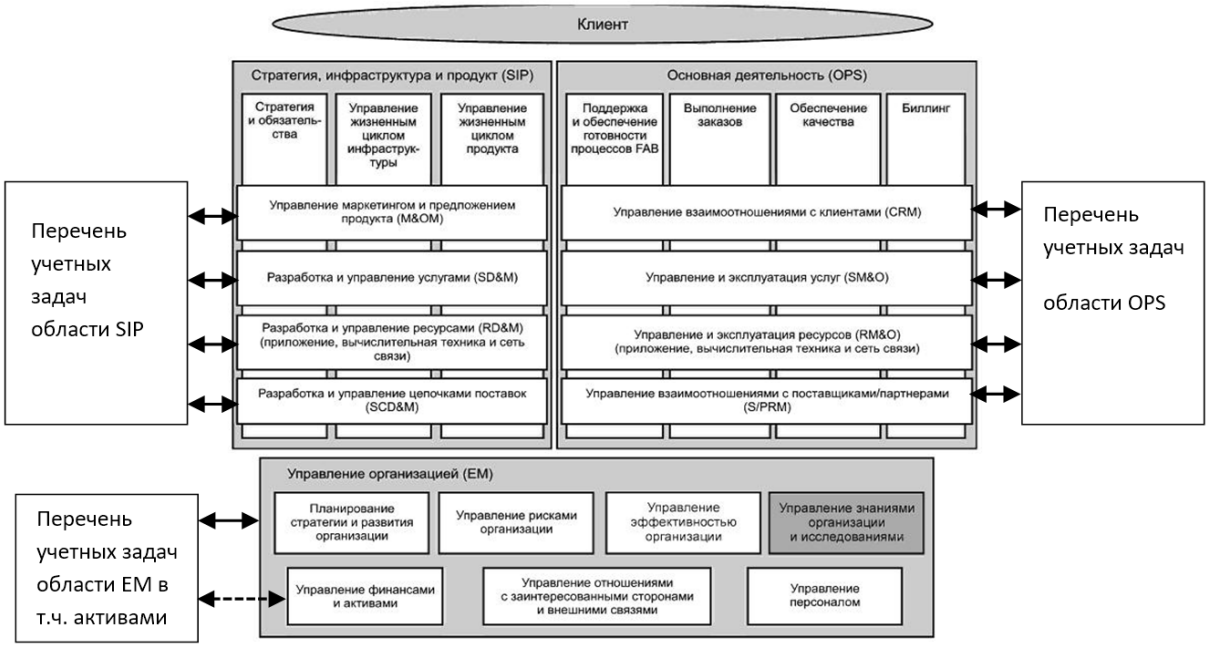


Рис. 1. Учетные задачи eTOM

Автоматизация учетных задач реализуется как отдельными программными средствами, так и в комплексах задач по отдельным областям или совокупности областей многофункциональными автоматизированными комплексами.

При этом, применение высокотехнологичных перспективных автоматизированных систем отрасли «Связь» в организациях (предприятиях, учреждениях) других отраслей экономики как «прямой перенос» технологических процедур автоматизации на полную совокупность задач, в том числе и учетные, является проблематичным, из-за различий в «сущностях» материальных и нематериальных активов, в особенностях организации и обеспечения учетных задач активов. К таким «материальным активам» относятся, например, «музейные объекты» или «музейные предметы», которые также могут являться объектами учета в структурных подразделениях или самостоятельных организациях, предприятиях или учреждениях связи.

Автоматизированные системы учета музейных объектов и предметов на примере отечественных разработок: «1С: Музей 8»; «1С:Музейный каталог»; ФГИС «Госкаталог музейного фонда Российской Федерации» («Государственный каталог Музейного фонда Российской Федерации»); АС «Музей-3».

Многоцелевая трансформация автоматизированного учета и отрасли связи в другие отрасли экономики возможна путем реализации заданной функции агрегирования данных (атрибутов) о соответствующих активах и предоставления их в виде регламентированном пользователем. Процедуры агрегирования данных включают процедуры сбора (импорта) данных

от отдельных информационных каналов, обработки и формирования данных и атрибутов, возможно слоев (в соответствии с внутренней или внешней базой моделей учетных задач), представления данных и атрибутов (в соответствии с установленными шаблонами или заданными пользователем) и хранения (экспорта) данных в требуемых форматах.

Практические реализации таких функций, при обеспечении минимальных затрат, программных и аппаратных ресурсов, исходя из анализа открытых и доступных сведений, в настоящее время, отсутствуют.

Многоцелевая трансформация может осуществляться посредством программного «агрегатора учетных данных» с применением веб-технологий (рис. 2).

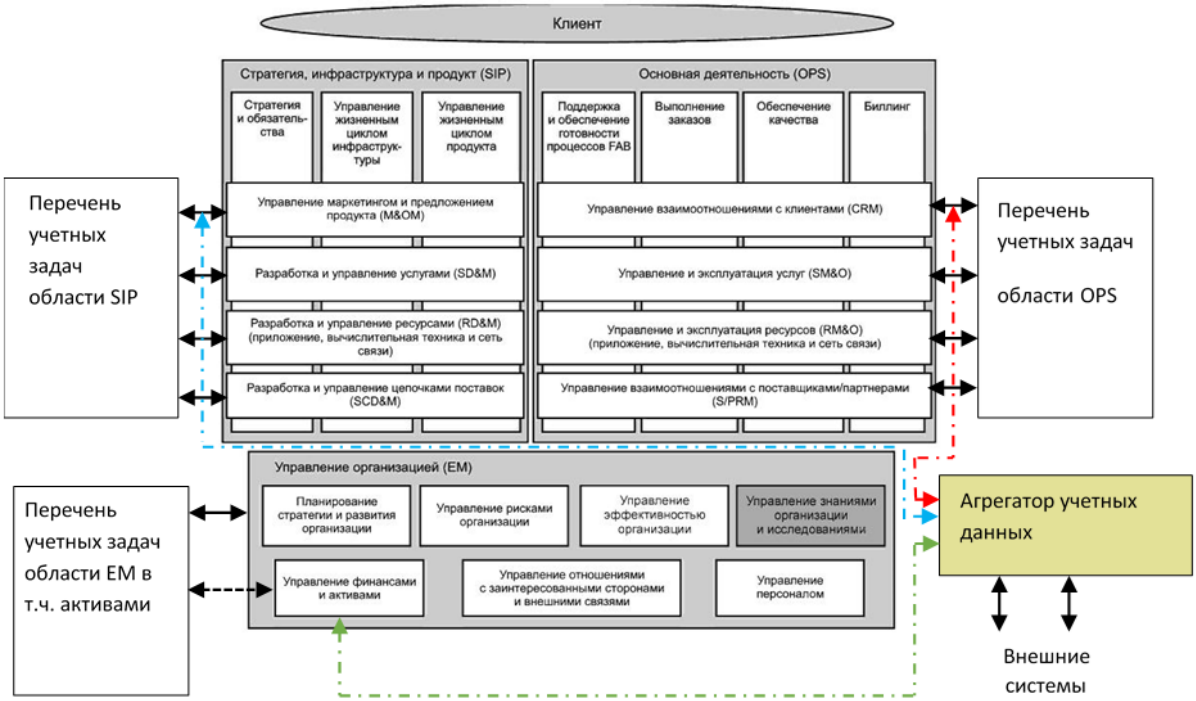


Рис. 2. Агрегатор учетных данных

«Агрегатор учетных данных» – программа для ЭВМ (далее – ПО), которая предназначена для формирования информационного ресурса о материальных активах порядок учета которых регламентирован специальными нормативными и правовыми актами. Программа реализует процедуры сбора, агрегирования и предоставления информации от различных источников (систем) по формам установленным пользователем. При этом хранение информации может осуществляться при непосредственном взаимодействии с базой данных «Агрегатора учетных данных» или с базами данных внешних источников (систем).

Техническая реализация ПО «Агрегатор учетных данных» должна соответствовать требованиям развивающейся технологии сервисов и услуг

«облачных вычислений», то есть соответствовать модели SaaS (*software as a service*) [7].

Модель SaaS – программное обеспечение как услуга – это категория служб облачных вычислений, в которой потребителю службы облачных вычислений предоставляется следующий тип возможностей облака: тип возможностей приложений (далее – Сервис).

Использование модели SaaS в Сервисе позволит поддерживать его версию в актуальном состоянии, исправлять удаленно ошибки в ПО, которые будут обнаружены в процессе эксплуатации.

Сервис должен иметь многоуровневую архитектуру аналогично Эталонной архитектуре облачных вычислений (ЭАОВ) [8] (см. рис. 3):

– уровень пользователя;
– уровень доступа;
– уровень службы;
– уровень ресурсов.

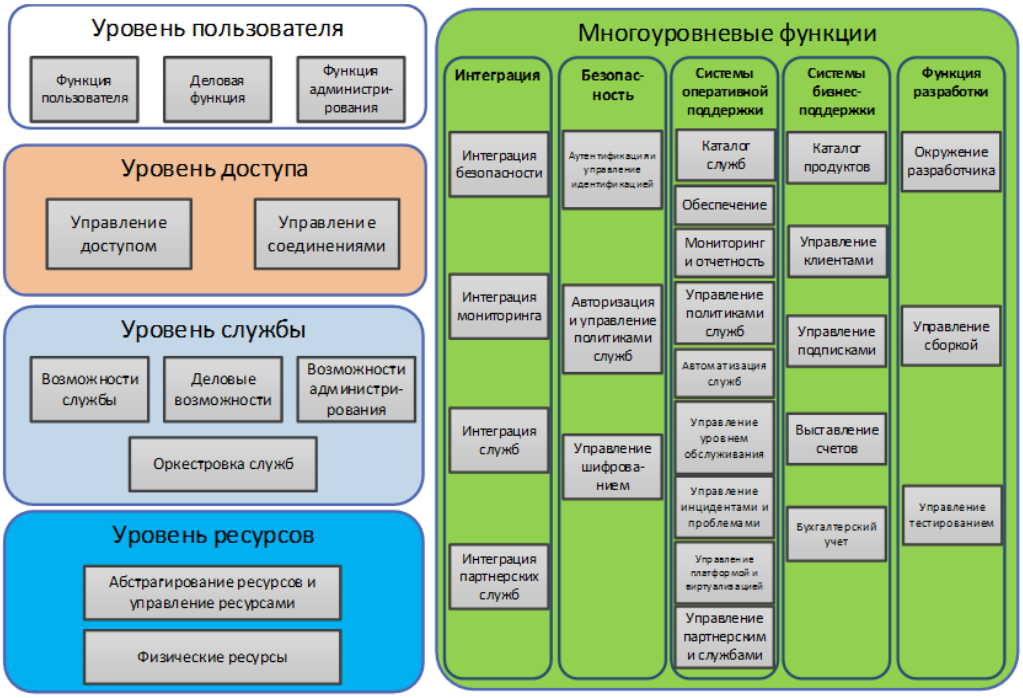


Рис. 3. Функциональные компоненты ЭАОВ

Функциональная структура «Агрегатора учетных данных» содержит следующие функциональные блоки:

– агрегирования учетных данных;

– экспорта/импорта данных (атрибутов) от автоматизированных средств учета организации (предприятия, учреждения), например, бухгалтерии, архива, локальной БД;

– экспорта/импорта данных (атрибутов) от внешних систем (источников данных): пространственных данных (геоинформационных систем); технических систем безопасности; систем контроля и управления доступа; систем телевизионного наблюдения;

– ввода информации с бумажных носителей (с применением средств и технологий голосового ввода, например, Web Speech API, распознавания голоса);

– ввода информации посредством Web-интерфейса;

– вывода информации на визуализатор (в том числе с применением средств и технологий голосового вывода, например, Web Speech API, синтеза голоса);

– сопряжения с базой данных «агрегатора учетных данных»;

– конфигуратора программного средства.

Предложенное техническое решение мобильного сервиса учетных задач позволяют расширить его использование различными организациями (учреждениями, предприятиями) в условиях цифровой экономики.

Список используемых источников

1. Программа «Цифровая экономика Российской Федерации» [Электронный ресурс]. URL: http://government.ru/rugovclassifier/ 614/events/ (дата обращения 05.04.2019).

2. Паспорт национальной программы «Цифровая экономика Российской Федерации» [Электронный ресурс]. URL: http://static.government.ru/ (дата обращения 05.04.2019).

3. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения 05.04.2019).

4. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб.: ГУАП, 2016. 325 с.

5. ГОСТ Р 53633.0-2009. Информационные технологии (ИТ). Сеть управления электросвязью. Расширенная схема деятельности организации связи (eTOM). Общая структура бизнес-процессов.

6. ГОСТ Р 53633.12-2016. Информационные технологии. Сеть управления электросвязью. Расширенная схема деятельности организации связи (eTOM). Декомпозиция и описания процессов. Процессы уровня 2 eTOM. Управление организацией. Управление знаниями организации и исследованиями.

7. ГОСТ ISO/IEC 17788-2016. Информационные технологии (ИТ). Облачные вычисления. Общие положения и терминология. М.: Стандартинформ.

8. ГОСТ Р ИСО/МЭК 17789. Информационные технологии. Облачные вычисления. Эталонная архитектура.

УДК 65.011.56
ГРНТИ 81.14.01

ТЕХНОЛОГИИ АВТОМАТИЗИРОВАННОГО ВЕДЕНИЯ ПОДЛИННИКОВ КОНСТРУКТОРСКОЙ ДОКУМЕНТАЦИИ ПРЕДПРИЯТИЯ СВЯЗИ

Н. В. Полпудникова, А. В. Шестаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются вопросы ведения подлинников конструкторской документации предприятия-разработчика средств связи на различных этапах жизненного цикла продукции. С целью обеспечения интегрированных подходов в условиях изменения и развития технологий в делопроизводстве и документообороте электронными документами и повышения защищенности информации подлинников конструкторской документации исследуются технологии распределенных реестров с учетом находящихся в эксплуатации программных и аппаратно-программных средств PDM/PLM систем.

электронная конструкторская документация, управление данными об изделии, управление инженерными данными, жизненный цикл продукции, ведение подлинников электронной документации.

Переход в рамках программы «Цифровая экономика Российской Федерации» предприятий различных сфер экономической деятельности (включая отрасль «Связь») к новым технологиям при разработке (проектировании), производстве, поставке и сопровождении продукции [1] характеризуется использованием электронных моделей изделий и актуализацией их атрибутов [2] посредством ведения подлинников документации в ходе жизненного цикла с учетом пространственных данных об их размещении и эксплуатации [3] на объектах заказчика.

Ведение подлинников документации (конструкторской – КД; технологической – ТД; программной – ПД) – важный бизнес-процесс организаций (предприятий) связи в жизненном цикле промышленной продукции (изделия), систем, сетей и оборудования связи. Данное обстоятельство является определяющим для организаций-держателей подлинников документации. Основой для поддержания в актуальном состоянии подлинников документации являются требования единой системы конструкторской документации (ЕСКД), единой системы технологической документации (ЕСТД), единой системы программной документации (ЕСПД) и других нормативно-технических документов (НТД). Комплексная регламентация всех аспектов документов, проводимая над подлинниками, устанавливает взаимосвязанные

правила, требования и нормы по разработке, оформлению и обращению документации, перечень которой представлен на рис. 1.

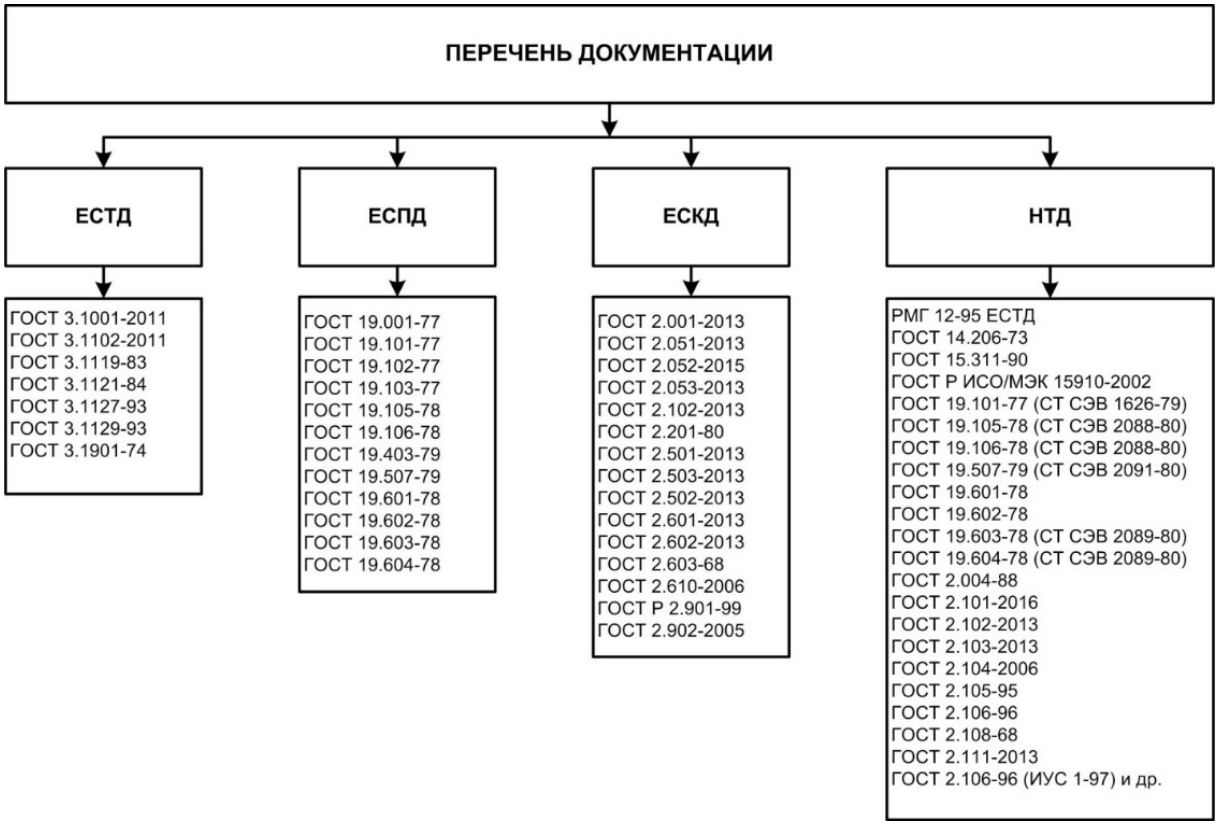


Рис. 1. Взаимоувязанность требований НТД к документации на изделия

Переиздание КД (ПД, ТД), то есть выпуск новых подлинников, и передача её в другую организацию влечет обязательность учета изменений. В случае использования ранее разработанной КД (ПД, ТД) в новых разработках обусловливает необходимость внесения в такую документацию изменений, которые реализует предприятие-разработчик (организация-держатель подлинников). При передаче другому предприятию дубликатов или учтённых копий КД (ПД, ТД) вопрос о внесении в подлинники, а также в дубликаты и учтённые копии, изменений связанных с внедрением новых, пересмотренных и изменённых документов, решается по согласованию между предприятием, передающим документы, и предприятием принимающей их.

Продолжительность и качество процедур в автоматизированной системе ведения и учёта подлинников КД (ПД, ТД) предприятия связи определяются в соответствии с [4, 5]. На них влияют:

− существующая регламентация процедур внесения изменений в документы и реестры (разработка предложения об изменении; выпуск предварительного извещения об изменении; дополнительного извещения об изменении извещения об изменении);

− потребный объём изменений, вносимых в комплект КД и реестры;

− необходимость разработки нового комплекта КД и изменение реестра (если изменения документа для одного изделия окажутся неприемлемыми, то на изменяемое изделие должен быть выпущен новый документ с внесёнными обозначениями);

− ведение системы реестров смешанного учёта бумажной и электронной КД в организации-держателе подлинников.

Реализованные прототипы автоматизированного ведения подлинников документации относятся либо к средствам управления инженерными данными (*Engineering Data Management,* EDM) – опциям систем управления данными об изделии (*Product Data Management*, PDM), либо к совмещенным средствам, альтернативным PDM-системам, либо ориентированным на ведение изменений данных об объекте (например, при строительстве):

− опция «OrCAD®EDM» от ООО «ПСБ СОФТ» (г. Москва), дистрибьютора компании «CADENCE Design Systems» (США), обеспечивает среду взаимодействия для пользователей схемного редактора OrCAD Capture (координация командной работы над документами; фиксация неподтвержденных данных; прослеживание и коммуникации в реальном времени; хранение полной истории версий каждого загруженного изменения на странице или на уровне проекта) [6];

− приложение «AutoManager Meridian» компании «Cyco Software» является совмещенной EDM-системой и организации документооборота интегрирующее основные функции PDM/PLM-систем [7];

− комплекс «Управление инженерными данными» компании «LMP Project Group» на основе «SmartPlantFoundation» (Интерграфу) и «ENOVIA» (*Dassault Systemes*) предоставляет сервисы электронной системы, которая содержит основные параметры конструкции, связи между ними, историю внесенных изменений и другую важную информацию [8]. Единая информационная база позволяет упростить поиск данных и их быструю координацию. В результате такого подхода обеспечивается экономия ресурсов, эффективная организация бизнес-процессов и снижение рисков.

Как показывают результаты проведенного анализа ряда предприятий связи (организаций-держателей подлинников документации) существующая операционная деятельность по ведению ими подлинников конструкторской документации имеет определенные недостатки:

− низкую оперативность внесения изменений при валидации по требованиям службы эксплуатации и заказчика в условиях стремительно развивающихся телекоммуникационных и информационных технологий;

− сложность контроля со стороны заказчика и кооперационного взаимодействия предприятий-разработчиков и предприятий-изготовителей СЧ изделия при значительном количестве СЧ изделия;

− риски изменений целостности данных в реестрах о проведенных изменениях в документах как СЧ изделия, так и на изделие в целом;

− проблематичность обеспеченности ресурсами стадий и этапов жизненного цикла изделий при реализации принятых изменений.

Для разрешения сложившихся противоречий целесообразно использовать интегрированную информационную среду, технологию и регламентацию распределённых реестров и блокчейн как системную технологию оптимизации затрат и повышения операционной эффективности взаимосвязанных бизнес-систем.

Интегрированная информационная среда (ИИС) является базой для процессов обращения бумажной и электронной КД (ПД, ТД). При переходе от бумажной КД (ПД, ТД) к совместному использованию с электронной КД (ПД, ТД) актуальным является ведения документации различных видов.

Процессы обращения в ИИС бумажной и электронной КД (ПД, ТД) представлены на рис. 2 (где: СПВП – общесистемный справочник продукции внешней поставки; БД КТИ – общесистемный справочник база данных конструкторско-технологической информации; АИПС УДИ – автоматизированная информационно-поисковая система утверждённой документации на изделия; КИУС – корпоративная информационно-управляющая система).

В основу технологии распределенных реестров легли различные криптографические методы и инструменты. Формирование цепей блоков происходит на основе технологии блокчейна и с использованием механизмов хеширования. Распределённая база данных представляется как цепочка последовательных блоков, каждый из которых содержит в себе хеш предыдущего блока и свой порядковый номер. Каждый новый блок подтверждает содержащиеся в нём транзакции, в дополнение к этому подтверждает транзакции во всех предыдущих блоках цепочки, за счет этого достигается неизменность хранимой информации, после чего корректировка информации внутри цепи без нарушения целостности становится невозможна.

Для обеспечения неизменности и подлинности транзакции подписываются электронной подписью. Проверка электронной подписи осуществляется на основе открытого ключа отправителя транзакции. Значение хеш-функции от открытого ключа отправителя используется в качестве идентификатора отправителя – служит механизмом идентификации участников сети. В итоге, криптографию можно использовать для обеспечения процесса достижения консенсуса, так как большинство алгоритмов консенсуса используют хеширование.

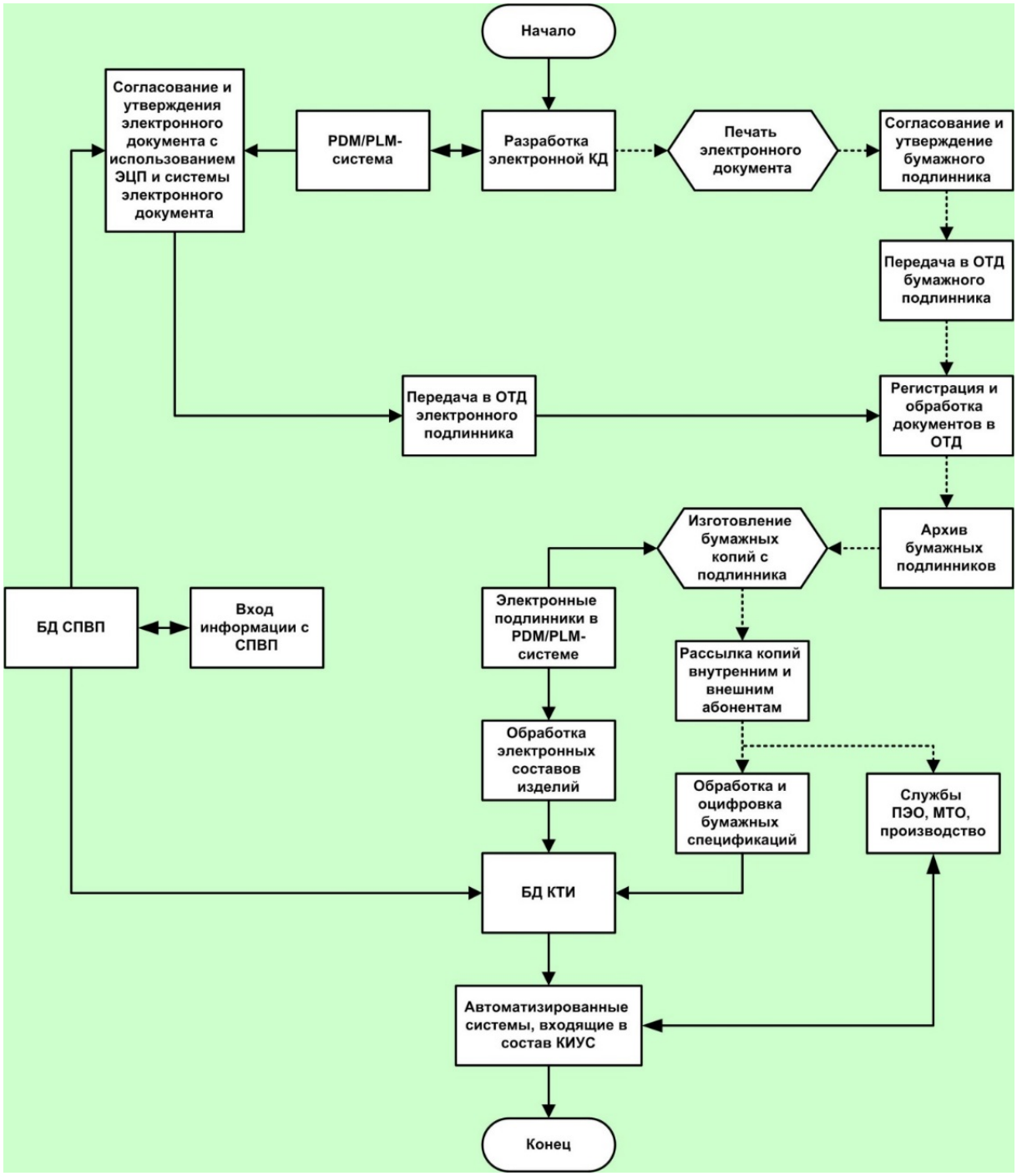


Рис. 2. Процессы обращения в ИИС бумажной и электронной документации

Список используемых источников

1. Акимов С. В., Верхова Г. В., Полпудникова Н. В.Автоматизированная система мониторинга вычислительной техники // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 2. С. 21–25.

2. Полпудникова Н. В., Шестаков А. В. Предложения об автоматизированном ведении подлинников конструкторской документации предприятия связи на основе технологии распределенных реестров // Актуальные проблемы инфотелекоммуникаций в науке

и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. Т. 2. С. 535–540.

3. Шестаков А. В. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций. СПб.: ГУАП, 2016. 325 с.

4. ГОСТ 2.501–2013. Единая система конструкторской документации. Правила учета и хранения. М.: Стандартинформ, 2014. III, 19 с. : ил.

5. ГОСТ 2.503–2013. Единая система конструкторской документации. Правила внесения изменений. М.: Стандартинформ, 2014. III, 27 с. : ил.

6. OrCAD EDM [Электронный ресурс]. URL: https://www.pcbsoft.ru/orcad-edm (дата обращения 12.02.2019).

7. AutoManager Meridian – система управления инженерными данными и организации документооборота от компании Cyco Software как разумная альтернатива PDM-системам [Электронный ресурс]. URL: https://sapr.ru/article/7525#О%20компании%20Cyco%20Software (дата обращения 12.02.2019).

8. Управление инженерными данными от LMP Project Group [Электронный ресурс]. URL: http://lmp-project.com/ru/services/upravlenie-inzhenernyimi-dannyimi-proekta/ (дата обращения 12.02.2019).

УДК 519.688
ГРНТИ 27.43.51

МНОГОШАГОВЫЙ АЛГОРИТМ ОБНАРУЖЕНИЯ ЭПИЗОДОВ ИШЕМИИ ПРИ АНАЛИЗЕ ЭКГ

Г. А. Портнов, П. А. Тимошенко, М. З. Лещук, А. Ф. Янак

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Синтезирование многошагового алгоритма обнаружения эпизодов ишемии и его апробация на основе тестового сигнала, максимально близко имитирующего фрагмент кардиосигнала при развитии эпизода ишемии.

ишемическая болезнь сердца, ST-сегмент, критерий Неймана-Пирсона, вероятность ложной тревоги, вероятность правильного обнаружения, отношение сигнал/шум, электрокардиограмма.

При обследовании пациентов с целью выявления у них патологий в работе ССС (сердечно-сосудистой системы), специалисты практически всегда прибегают к анализу электрокардиосигнала, как наиболее информативного биологического сигнала. Однако зачастую, выявлению заболеваний препятствует присутствие в сигнале помех различной физической природы.

Таким образом, появляется потребность в необходимости разработки новых подходов и методов выявления сердечных заболеваний, нового высокоэффективного и сравнительно недорогого оборудования, а также программных средств и алгоритмов, позволяющих автоматизировать процесс выявления данных заболеваний.

Одним из наиболее важных медико-технических направлений исследования представляется создание методов автоматизированного выявления такой болезни сердца как ишемия миокарда.

Перед обнаружением эпизодов ишемии и дальнейшей постановки диагноза необходимо провести предварительную фильтрацию сигнала ЭКГ, а также устранение дрейфа изоэлектрической линии:

- Исходная дискретная ЭКГ пропускается через фильтр нижних частот (ФНЧ) с частотой дискретизации;
- Вокруг каждой точки отфильтрованного сигнала, отсчеты которого также берутся с интервалом дискретизации, выбирается окно шириной 1,3 секунды;
- Все значения отфильтрованного сигнала в этом окне ранжируются;
- Выбираются 50 % центральных значений. Считается среднее арифметическое этих 50 %. Данное значение и будет значением изолинии в искомой точке.

На рис. 1 представлена блок схема, реализующая предварительную обработку ЭКГ.

Рис. 1. Блок-схема алгоритма устранения дрейфа изолинии

При использовании многошагового алгоритма обнаружения эпизодов ишемии используется два порога, которые делят область принятия решений

(в данном случае ось q – отношение сигнал-шум) на три интервала. Главное отличие предложенного многошагового алгоритма обнаружения ишемии от метода, предложенного Вальдом, заключается в том, что обработка принятой реализации осуществляется в окне, в котором сосредоточен определенный фрагмент наблюдаемого кардиосигнала, при этом ширина окна на каждом шаге наблюдения не увеличивается.

1. Когда значение корреляционной суммы меньше или равна значению нижнего порога, $z \leq Z_{\text{ПН}}$ – принимается решение об отсутствии сигнала и как следствие отсутствие ишемии;

2. Когда значение корреляционной суммы больше или равна значению верхнего порога, $z \geq Z_{\text{ПВ}}$ – принимается решение о наличии сигнала, и в данном случае наличие ишемии;

3. Когда значение корреляционной суммы лежит в интервале между значениями нижнего и верхнего порога, $Z_{\text{ПН}} \geq z \geq Z_{\text{ПВ}}$ – принимается решение о продолжении наблюдений, т. е. z попало в зону неопределенности и продолжается накопление выборки.

Ширина области неопределенности зависит от значений порогов $Z_{\text{ПН}}$ и $Z_{\text{ПВ}}$. Эти пороги зависят от величины вероятности ложной тревоги и пропуска сигнала, которыми мы задаемся изначально.

Моделью тестового сигнала, описывающих элевацию (депрессию) ST-сегментов является последовательность прямоугольных импульсов, на которую наложен шум с нарастающей дисперсией. Ее рост обусловлен физической нагрузкой, которую может претерпевает пациент при не выявлении ишемии в состоянии покоя, т. к. при физической или аэробной нагрузке более отчетливо прослеживается наличие ишемии.

На рис. 2 представлена аддитивная смесь модели сигнала *ST*-сегмента ЭКГ с ишемией и шума.

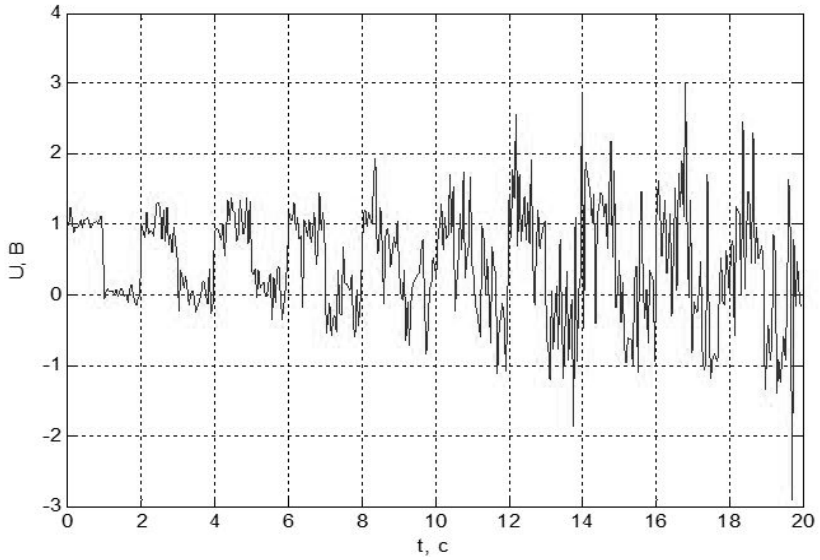


Рис. 2. Аддитивная смесь полезного сигнала и шума

Алгоритм обнаружения построен на основе корреляционного приемника, и разбивается в несколько этапов:

1. При поступлении сигнала ЭЭГ производится произведение опорного сигнала s_{oni}, который является точной копией полезного сигнала s_i и наблюдаемой реализации y_i по формуле (1), приведенной на рис. 1:

$$z_i = y_i s_{oni}. \quad (1)$$

2. Суммирование отсчетов z_i согласно формуле (2):

$$Z_j = \sum_{i=1}^{M} z_i, \quad (2)$$

где M – количество отсчетов одного периода последовательности;

Z_j – значения корреляционной суммы, где дисперсия шума имеет постоянное значение (дисперсия шума имеет постоянное значение в течении одного периода сигнала, и возрастает ступенчато при наступлении следующего).

3. Имея массив значений корреляционной суммы Z_j, каждое ее значение умножается на коэффициент равный обратному значению дисперсии шума действующем на данном периоде сигнала и по формуле (3) сравнивается с пороговым значением:

$$\frac{1}{\sigma_1^2} Z_1 + \frac{1}{\sigma_2^2} Z_2 + ... + \frac{1}{\sigma_{10}^2} Z_{10} \underset{\overset{\wedge}{H_0}}{\overset{\wedge}{H_1}}{\gtrless} Z_{\text{П}} \quad (3)$$

где $\frac{1}{\sigma_1^2}, \frac{1}{\sigma_2^2}, ..., \frac{1}{\sigma_{10}^2}$ – весовые коэффициенты на каждом периоде сигнала;

H_0, H_1 – гипотезы отсутствия или наличия сигнала ишемии на ЭКГ;

Z_Σ – итоговое значение корреляционной суммы.

4. После того как получено итоговое значение корреляционной суммы (Z_Σ), необходимо определиться со значением порога $Z_{\text{П}}$. Зададимся фиксированным значением вероятности пропуска сигнала (ВПС) $\beta = 0{,}01$. Далее производится расчет нормированного порога по формуле (4):

$$h = q + \Phi^{-1}(\beta), \quad (4)$$

где h – нормированный порог;

q – отношение сигнал шум.

Вероятность ложной тревоги можно рассчитать по формуле (5):

$$\alpha = 1 - \Phi(h). \quad (5)$$

Тогда пороговое значение рассчитывается по формуле (6):

$$Z_{\text{П}} = h\sigma_z, \quad (6)$$

где $\sigma_z = \sqrt{\sum_{i=1}^{N} \frac{1}{\sigma_i^2} E_i}$ – значение СКО z;

σ_i – значение СКО шума на отдельном участке сигнала;

$E_i = \sum_{j=1}^{M} s_{ij}^2$ – значение энергии полезного сигнала на данном участке (т. е. энергия одного импульса);

M – количество отсчетов.

5. Таким образом сравнивая порог со значением корреляционной суммы получим решающее правило: $Z \underset{\overset{\wedge}{H_0}}{\overset{\wedge}{H_1}} Z_{П}$.

Был синтезирован алгоритм обнаружения эпизодов ишемии, в результате работы которого имеем решение о наличии или отсутствии эпизода ишемии на ЭКГ. В качестве исследуемого сигнала использовалась последовательность импульсов, имитирующих элевацию ST-сегмента с амплитудой, превышающей норму на ЭКГ.

Таким образом, автоматизировав процесс выявления ишемической болезни сердца можно приобрести несколько крайне важных плюсов. К подобным можно отнести возможность повышения достоверности выносимого диагноза врачом-кардиологом.

Список используемых источников

1. Гришин Ю. П., Ипатов В. П., Казаринов Ю. М., Коломенский Ю. А., Ульяницкий Ю. Д. Радиотехнические системы. М.: Академия, 2008. 592 с.

2. Рангайян Р. Анализ биомедицинских сигналов. М.: ФИЗМАТЛИТ, 2007. 516 с.

3. Сергиенко А. Б. Цифровая обработка сигналов. СПб.: Питер, 2013. 750 с.

4. Duck, H. L., Jun, W. P., Jeasoon, C., Ahmed, R., Reza, F. Automatic Detection of Electrocardiogram ST Segment: Application in Ischemic Disease Diagnosis // International Journal of Advanced Computer Science and Applications. 2014. Vol. 4. No. 2.

5. De Gaetano, A., Panunzi, S., Rinaldi, F., Risi, A., Sciandrone, M. // Applied Mathematics and Computation // Elsevier Inc. Journal. 2017.

6. Красичков А. С. Методологическое обеспечение автоматизированной системы тревожной сигнализации при развитии ишемии миокарда: дис. … д-ра. мед. наук: 02.17 / Красичков Александр Сергеевич. Санкт-Петербург. 2016. 299 с.

7. Леман Э. Проверка статистических гипотез. М.: Наука, 1979. 408 с.

8. Хэмптон Д. Основы ЭКГ. М.: Мед. лит., 2006. 224 с.

9. Барановский А. Л., Калиниченко А. Н., Манило Л. А. Кардиомониторы аппаратура непрерывного контроля ЭКГ. М.: Радио и связь, 1993. 243 с.

10. Бакулев П. А. Радиолокационные системы. М.: Радиотехника, 2004. 320 с.

11. Зайчик А. Ш., Чурилов Л. П. Патохимия (эндокринно-метаболические нарушения). СПб.: ЭЛБИ-СПб, 2016. 768 с.

12. Duck, H. L., Jun, W. P., Jeasoon, C., Ahmed, R., Reza, F. Automatic Detection of Electrocardiogram ST Segment: Application in Ischemic Disease Diagnosis // International Journal of Advanced Computer Science and Applications. 2015. Vol. 4. No. 2.

УДК 004.946
ГРНТИ 50.10.47

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ДОПОЛНЕННОЙ И ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ В ОБРАЗОВАТЕЛЬНОЙ СФЕРЕ

Д. В. Прокудин, Е. Т. Сыса

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Сегодня технологии дополненной и виртуальной реальности развиваются стремительными темпами и набирают всё большую популярность. В современных школах и университетах всё чаще можно встретить устройства, использующие данные технологии. Ещё несколько лет назад использование данных технологий в обучающем процессе могло показаться футуристической сказкой, однако вероятно уже совсем скоро образовательные учреждения будет невозможно представить без устройств на основе технологий дополненной и виртуальной реальности.

AR, VR, дополненная реальность, виртуальная реальность, образование.

В современном мире искусственный интеллект постепенно начинает изменять вид привычной для нас системы образования. Этот процесс также делает систему более гибкой. Комбинация технологий дополненной и виртуальной реальности позволяет обучающимся фокусироваться на конкретных областях, в которых они имеют более высокий потенциал для развития,

а также продвигаться вперёд ученикам, быстрее усваивающим материал, вместо ожидания своих ещё навёрстывающих материал коллег. Доступ к технологиям искусственного интеллекта также оказывает помощь в подготовке обучающихся к их дальнейшей трудовой деятельности, так как работодатели в настоящее время активно внедряют данные технологии в рабочий процесс. Возможности для разработки практически безграничны.

Что такое дополненная реальность (AR)

Говоря простым языком, данная технология позволяет накладывать различные звуки, изображения и текст на реальные объекты, наблюдаемые через экраны электронных устройств (таких как смартфоны, планшеты, очки дополненной реальности). Примерами приложений использующих эту технологию могут послужить такие игры, как Pokemon Go, Ingress, Harry Potter: Wizrds Unite, фильтры в Instagram, добавляющие различные элементы к вашим фотографиям. По существу, дополненная реальность – это когда вы, смотря через экран телефона (AR-очки, камеру и т. д.), в реальном времени видите вещи, которых на самом деле нет. Практическое применение AR-технологии в наши дни можно увидеть, например, в аэропортах, где технология используется операторами, для контроля передвижения самолётов и пассажиров вплоть до того, сколько человек находится у конкретного пункта досмотра, и сколько товара было продано в Duty Free [1]. Мебельные магазины позволяют вам видеть, как элементы фурнитуры будут смотреться у вас дома, хирурги используют AR для создания плана перед началом операции.

Что такое виртуальная реальность (VR)

В отличие от дополненной реальности, эта технология использует окружение и сцены, полностью сгенерированные компьютером и основанные на реалистичных скриптах. Вместо изображений, наложенных на реальные объекты, пользователям предоставляется возможность исследовать сгенерированные трёхмерные пространства, и, так как они полностью погружены в искусственную среду, их восприятие легко обманывается, и пользователь начинает ощущать себя находящимся внутри сгенерированного пространства. Уже в настоящее время вы можете исследовать музеи, находящиеся в других городах и странах так, как будто вы на самом деле находитесь там. Технология используется в самых разных форматах: от видеоигр и кино, до архитектуры и обучения. В частности, архитекторы часто используют технологию для проверки качества конструкции в симулированном окружении перед её применением в реальной жизни.

Дополненная реальность и образование

Масштабы разработки мобильных приложений с применением технологий дополненной реальности продолжают расти с каждым днём. Одним из наиболее интересных достоинств этой технологии в образовательной сфере деятельности является обеспечение преподавателей возможностью индивидуализировать обучающий процесс. Программы, использующие данную технологию, могут оценить уровень понимания предмета обучаемым, что позволяет преподавателю создавать учебные планы, принимая во внимание индивидуальные проблемы ученика, вместо повторения материала в областях, где ребёнок уже отлично всё понимает. Благодаря данной технологии методика преподавания также становится более привлекательной, повышая интерес ребёнка к, например, домашним заданиям, они становятся интерактивными, а, следовательно, более увлекательными.

Виртуальная реальность и образование

Виртуальная реальность – это ещё один способ превратить обучающий процесс во что-то занимательное и увлекательное. Обучающимся предоставляется возможность мгновенно перемещаться в любую точку мира, вместо того, чтобы заниматься только в своих аудиториях. Множеству детей удобнее воспринимать информацию визуально, следовательно, преподаватели могут использовать эту технологию, для более детального раскрытия сути предметов [2]. Если дети смогут увидеть воочию определённые исторические события, они будут более склонны к впитыванию и пониманию информации, более увлечённо изучать необходимые разделы. Технология также может быть использована для развития интереса к иностранным языкам: ученик может быть помещён в виртуальное пространство, где языком обмена информации является, например, английский, испанский или любой другой. Возможности данной технологии имеют поистине безграничный потенциал. Применение её в обучающем процессе уже продемонстрировало её полезность.

Применение искусственного интеллекта в разработке программ продолжает наращивать обороты, и вхождение этой технологии в каждую сферу нашей жизнедеятельности неминуемо, так как количество цифровых устройств в наших домах значительно возрастает с каждым месяцем [3]. Технологии дополненной и виртуальной реальности – это только начало, и как преподаватели, так и обучаемые школ и университетов, находящихся в любой точке земного шара, могут извлечь существенную пользу из использования приложений, в основе которых эти технологии лежат.

Список используемых источников

1. Иванова А. Технологии виртуальной и дополненной реальности: возможности и препятствия применения // Стратегические решения и риск-менеджмент. 2018. Вып. 3 (108). ISSN 2618-947X.
2. Касатиков А. Д., Лейбов А. М., Осокина О. М. Современные информационные технологии в педагогическом процессе технологических факультетов педагогических вузов // Современное машиностроение. Наука и образование. СПб.: Изд-во политехнического университета. 2014. С. 60–67.
3. Галкин Д. В., Сербин В. А. Эволюция пользовательских интерфейсов: от терминала к дополненной реальности. 2013. С. 35–49.

УДК 004.439
ГРНТИ 50.05.09

HTML5 РАЗРАБОТКА: ЧТО ЭТО ЗНАЧИТ ДЛЯ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ И РАЗРАБОТЧИКА

Д. В. Прокудин, С. А. Комисаров, И. С. Якшибаев

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В статье рассмотрена технология разработки HTML5, определены преимущества и недостатки языка разметки, а также рассмотрены позиции разработчика и конечного пользователя об HTML5.

HTML5, веб-сайт, разработчик, пользователь, разработка, Adobe Flash.

Сегодня, когда дело подходит к чёткому определению языка HTML5, осознанию его преимуществ и созданию интерактивного опыта, который люди ассоциируют с новыми инновационными веб-сайтами, между разработчиками и конечными пользователями возникает масса недопонимания.

HTML5 – это технологический стандарт, расширяющий возможности веб-приложений и существенно упрощающий их разработку [2].

Поскольку HTML5 решает ряд важных практических проблем, производители браузеров ведут активную работу по внедрению новых возможностей, и это несмотря на то, что до выпуска окончательного варианта спецификации еще очень далеко. В свою очередь, апробация спецификации в

эксплуатируемых браузерах служит источником ценной информации, которая используется для улучшения самой спецификации. HTML5 быстро развивается, шагая в ногу со все возрастающими требованиями к веб-платформам [3].

HTML5 – неформал. Его придумала группа вольнодумцев, которые не входили в группу, отвечавшую за официальный стандарт HTML. В стандарте HTML5 разрешаются методы написания страниц, которые были запрещены десять лет тому назад. В нем подробно изложены инструкции браузерам, как обрабатывать ошибки в разметке страниц, чтобы попытаться отобразить эти страницы, вместо того чтобы сразу же забраковывать их [1].

Он, наконец, позволяет воспроизводить видео, не прибегая к помощи модулей расширения браузера, таких как, например, Flash. Также в этом стандарте вводится лавина функциональностей, движимых JavaScript, которые могут придать веб-страницам определенные расширенные, интерактивные возможности, встречаемые в программном обеспечении для настольных компьютеров.

Последние несколько лет HTML5 был весьма распространённым словом в отраслях издательской деятельности и веб-разработке. Так как язык прошёл путь от прозвища «убийца flash» до таких основанных на нём веб-сайтов как Google Wave, Facebook Mobile, и Financial Times, существует пласт недопонимания между разработчиками и конечными пользователями относительно того, что из себя представляет разработка на HTML5, какие выгоды приносит его использование, и что требуется для разработки того, что люди будут ассоциировать с новыми интерактивными веб-сайтами [1].

Что видит конечный пользователь

Когда конечные пользователи обсуждают создание веб-сайтов на HTML5, у большинства возникают следующие предположения:

1) Веб-сайт будет выглядеть графически богато. Современные веб-сайты имеют такие броские анимированные объекты, как плавные переходы, выдвигающиеся объекты, тени. Все это — элементы добавляющие красоты картинки.

2) Веб-сайт не будет использовать Adobe Flash. В момент выпуска iPhone в 2007-м году, произошел толчок веб-сайтов к использованию технологии, таких как JavaScript и MPEG-4, чтобы уменьшить зависимость от Flash в целях разработки визуально более богатых страниц.

3) Веб-сайт будет доступен для телефона. Клиент предполагает, что весь контент, в том числе интерактивный, например, видео будет доступен на мобильных устройствах.

Что видит разработчик

Множество разработчиков видят HTML5 не так, как это делают конечные пользователи. Одними термин “HTML5” воспринимается более буквально, чем то, что подразумевается конечным пользователем. Для них HTML5 является средством для структурирования и отображения контента. В то время как множеством веб-сайтов используются все преимущества медиа-контента такого как видео, объекты и canvas, для некоторых сайтов это не обязательно. Разработчики видят следующие проблемы при внедрении HTML5:

1) HTML 4.01 и XHTML 1.1 структурировали ту же информацию надлежащим образом не хуже, чем HTML5. Все, что структурировано при использовании тэгов на XHTML 1.1 работает также и на HTML5. Так в чем же преимущество HTML5.

2) То, что требуют клиенты – это не HTML5. На самом деле им нужен HTML с CSS3 и JavaScript. Вс– это — не HTML5.

Уроки

Обе стороны могут извлечь полезные и важные уроки из этих разногласий.

Для конечного пользователя

Важно точно сформулировать какой пользовательский опыт необходим посетителям сайта, по мнению заказчика. Важно также осознавать все преимущества использования HTML5 и понимать нужны ли они в конкретном проекте. Большинство новшеств, на которые были обращены взгляды всех рядовых пользователей являются комбинацией большого количества разных технологий. Таким образом четкое объяснение того, чего вы хотите разработчику – это ключ к успеху. В дополнение у браузеров существуют некоторые ограничения, к спецификации HTML5 все еще в разработке, а значит она будет развиваться со временем.

Для разработчиков

Следует понимать, что, когда конечные пользователи говорят об HTML5, требуется некоторая интерпретация уже их ожиданий. Клиенты не всегда понимают, что они хотят до того, как они это увидят. Ожидание клиента от HTML5 сформирована благодаря богатым графически примерам, который были созданы при помощи набора технологий таких как JavaScript, CSS3, HTML5. Необходимо проводить с клиентом работу, направленную на уточнение необходимых требований с целью угодить заказчику.

Одно из обстоятельств, повышающих интерес к разработке веб-интерфейса, заключается в работе в условиях быстрых перемен. Всегда есть что-то новое для изучения, и веб-сообщество всегда придумывает способы, как при решении тех или иных задач все улучшить, ускорить и сделать намного эффективнее [2].

Аналогично этому не так давно Flexbox еще только мерещился тем, кто создавал спецификацию. И даже по мере развития спецификации ее реализация давалась с большим трудом до тех пор, пока Андрей Ситник и такие же умные, как он, ребята из Evil Martians не создали Autoprefixer, после чего мы смогли с относительной простотой воспользоваться кросс-браузерным кодом [4].

Есть также Web Components – коллекция стандартов, составленная из Shadow DOM, Custom Elements и HTML Imports, которая позволяет создавать полностью предсказуемые и многократно используемые компоненты [2].

В будущем нам предстоит осваивать еще более захватывающие возможности.

Список используемых источников

1. Дронов В. А. HTML 5, CSS 3 и Web 2.0. Разработка современных Web-сайтов. СПб.: БХВ-Петербург, 2011. 416 с

2. Лоусон Б., Шарп Р. Изучаем HTML5. Библиотека специалиста. 2-е изд. СПб.: Питер, 2012. 304 с.

3. Макфарланд Д. Большая книга CSS3. 3-е изд. СПб.: Питер, 2014. 608 с.

4. Фримен Э., Робсон Э. Изучаем программирование на HTML5. СПб.: Питер, 2013. 640 с.

УДК 004.7:004.422.8
ГРНТИ 20.01.07

АНАЛИЗ ВЛИЯНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА КАЧЕСТВО ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Л. К. Птицына, А. В. Тарабаров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрены причины расширения методических основ анализа влияния систем защиты информации на качество функционирования информационных систем, описаны ключевые составляющие расширений, представлены модели и методы рассматриваемого анализа.

угроза, защита информации, модель, метод, качество, показатели.

Масштабы и сферы использования информационных инфраструктур в условиях развития цифровой экономики предопределяют необходимость обеспечения не только их надёжности, устойчивости, но и защиты информации от несанкционированного доступа. Защита информации является неотъемлемой составляющей информационной безопасности, относящейся к основным инфраструктурным элементам цифровой экономики.

На современном этапе развития платформ информатизации, входящих в информационные инфраструктуры, большинство их операционных систем сопровождается встроенными средствами защиты. При этом наблюдается общая тенденция усиления роли данных механизмов. Однако даже при использовании последних версий операционных систем и соответствующего прикладного программного обеспечения не гарантируется полная защищённость от несанкционированного доступа.

Подавляющее большинство проводимых исследований, связанных с повышением защищённости от воздействия появляющихся угроз, ориентируется на исследование возможных методов комплексирования средств защиты информации с позиции профилирования их собственного качества. Однако с позиции системного подхода к организации сложных комплексов введение дополнительных средств, сказывается и на профилях качества защищаемых объектов. Подобный контекст исследований характеризуется фрагментарностью и частным характером рассматриваемых объектов. В связи с этим актуализируется разработка методической основы оценки

влияния систем защиты информации на качество функционирования информационных систем.

Представляемые методические основы ориентируются на развитие методического сопровождения жизненного цикла комплексных систем защиты информации.

При расширении методических основ предусматривается:

− формирование информационного обеспечения системы представления знаний о комплексировании средств защиты информации;

− определение требований к анализу влияния средств защиты информации от несанкционированного доступа на показатели качества функционирования объектов защиты;

− формальные описания методов комплексирования средств защиты информации;

− формирование методик построения моделей процессов функционирования объектов защиты информации;

− формирование методик построения моделей процессов функционирования комплексных систем защиты информации;

− формирование методик построения моделей процессов совместного функционирования объектов защиты информации и комплексных систем защиты информации;

− формирование базиса методов анализа моделей процессов совместного функционирования объектов защиты информации и комплексных систем защиты информации;

− формирование методик определения и оценки показателей качества функционирования объектов защиты при подключении комплексной системы защиты информации;

− формирование методики анализа влияния комплексной системы защиты информации на показатели качества функционирования объектов защиты;

− формирование методики разработки рекомендаций для выбора способов организации комплексной системы защиты информации и рационального сочетания параметров, определяющих режим соблюдения необходимых требований к качеству функционирования объектов защиты.

При формировании информационного обеспечения системы представления знаний о комплексировании средств защиты информации учитываются все классы защищённости, соответствующие нормативной документации, и известные способы совершенствования комплексных программных систем защиты информации. Среди известных способов выделяются опорные и расширенные. К опорным способам относятся: комплексирование аппаратных средств и заявка комплексирование аппаратно-программных средств, а к расширенным – комплексирование виртуальных средств, ком-

плексирование аппаратных с обратной связью, комплексирование аппаратно-программных средств с обратной связью, комплексирование виртуальных средств с обратной связью.

Наряду с указанными способами организации комплексных систем защиты информации, анализируются и архитектуры, предусматривающие их интеллектуализацию с помощью агентных технологий [1].

При формировании информационного обеспечения системы представления знаний о комплексировании интеллектуальных средств защиты информации описываются архитектуры с агентами-контролёрами. В подобных архитектурах выделяются следующие способы комплексирования [2]:

− комплексирование аппаратных средств с агентом-контроллером в обратной связи;

− комплексирование аппаратно-программных средств с агентом-контролёром в обратной связи;

− комплексирование виртуальных средств с агентом-контролёром в обратной связи.

Методики построения моделей процессов функционирования объектов защиты информации ориентируются на разные ситуации в поведении инфокоммуникационной среды. Среди возможных ситуаций различаются две основные группы. К первой группе относятся ситуации пассивного поведения, а ко второй группе – активного поведения инфокоммуникационной среды.

Методики построения моделей представленных процессов формируются на основе определений моделей в классах марковских цепей, марковских процессов, полумарковских процессов, диаграмм деятельности, процессов функционирования систем массового облуживания и сетей систем массового обслуживания. Задействованные классы моделей связываются сквозными переходами между их параметрами и характеристиками.

В базис методов анализа моделей процессов совместного функционирования объектов защиты и комплексных систем защиты информации вводятся методы теории конечных цепей Маркова, методы теории марковских и полумарковских процессов, методы анализа логических моделей, модифицированный метод свёртки, модифицированный метод отыскания групп совместных вершин, методы анализа расширенных объектно-ориентированных моделей [3, 4], методы теории систем массового обслуживания и сетей систем массового облуживания, методы анализа агентных технологий [1]. Перечисленные методы используются для определения показателей качества функционирования комплексных систем защиты информации, а также объектов при отсутствии и наличии комплексных систем защиты информации.

Благодаря обширному составу методов, в формируемые методики вводятся процедуры подтверждения корректности результатов определения

и оценивания показателей качества функционирования комплексных систем защиты информации и объектов информационных инфраструктур.

Исследования, проведённые согласно представленным методикам, показывают, что введение комплексных систем защиты информации в информационную инфраструктуру сопровождается увеличением нагрузки процессорного поля и снижением риска срыва решения прикладных задач в поле окружающих угроз.

Научная новизна заключается в сквозном связывании технологий моделирования информационных инфраструктур и технологий информационной безопасности на основе системного подхода к анализу качества функционирования распределённых систем с целью обеспечения требуемого качества функционирования информационных систем в поле окружающих угроз.

Список используемых источников

1. Птицына Л. К., Птицын А. В. Обеспечение информационной безопасности на основе методологического базиса агентных технологий // Вестник Брянского государственного технического университета. 2017. № 2 (55). С. 146–154.

2. Птицын А. В. Методологический базис агентных технологий для обеспечения информационной защищённости // Наукоемкие технологии в космических исследованиях Земли. Т. 7. № 1. 2015. С. 50–55.

3. Птицын А. В., Птицына. Л. К. Генерация системно-аналитического ядра безопасных информационных технологий. СПб.: Изд-во Политехн. ун-та, 2011. 263 с.

4. Птицын А. В., Птицына Л. К. Аналитическое моделирование комплексных систем защиты информации. Гамбург. Saarbrucken: LAP LAMBERT Academic Publishing, 2012. 293 с.

УДК 004.7:004.422.8
ГРНТИ 20.01.07

ДИНАМИЧЕСКИЙ ПРОФИЛЬ СЕРВИС-ОРИЕНТИРОВАННЫХ СИСТЕМ С АДАПТИВНЫМ УПРАВЛЕНИЕМ ИХ КАЧЕСТВОМ

Л. К. Птицына, Н. Эль Сабаяр Шевченко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Описаны причины повышения требований к качеству сервис-ориентированных систем. Выбраны показатели качества сервис-ориентированных систем. Проанализированы возможные подходы к управлению их качеством. Детализированы представления

об адаптивном управлении качеством сервис-ориентированных систем. Построена расширенная объектно-ориентированная модель сервис-ориентированной системы с адаптивным управлением её качеством. Предложен метод определения динамического профиля сервис-ориентированных систем с адаптивным управлением их качеством.

сервис-ориентированные системы, адаптивное управление качеством, объектно-ориентированная модель деятельности, динамический временной профиль.

При переходе к цифровой экономике, с ужесточением конкуренции, ростом автоматизации промышленности и экспоненциальным увеличением больших данных актуализируется интеллектуализация сервис-ориентированных средств с адаптивным управлением их качеством, являющихся архитектурной основой корпораций, крупных кластеров и различных распределенных систем, взаимодействующих со сложной средой с априорной неопределенностью [1]. В связи с этим возникает объективная необходимость обеспечения быстрой и своевременной адаптации с целью обеспечения постоянного обмена опытом, технологиями и осуществления совместного использования возможностей, в том числе, и различных сервисов [2].

Важным механизмом качественной адаптации сервис-ориентированной системы к резким изменениям в окружающей среде является управление временной разверткой. В этой связи целесообразно оценивать статистические временные характеристики с помощью плотности распределения вероятностей $u(k_{1,2,\ldots,i,\ldots,I})$ дискретного времени выполнения деятельности интегрируемых сервис-ориентированных систем [3]. Исходя из этого, выделяются следующие показатели качества:

– $E[k_{0,1,\ldots,i,\ldots,I}]$ и $D[k_{0,1,\ldots,i,\ldots,I}]$ – соответственно математическое ожидание и дисперсия дискретного времени $k_{0,1,\ldots,i,\ldots,I}$ выполнения деятельности,

– $R(k_{0,1,\ldots,i,\ldots,I} > C)$ – риск срыва временного регламента или вероятность невыполнения деятельности по установленному временному регламенту C (верхняя граница допустимого времени).

Основные этапы оценки выбранных показателей качества подробно раскрываются в работе [3].

Благодаря возможностям оценивания выбранных показателей качества расширяются представления о возможных вариантах адаптивности сервис-ориентированной системы, что повышает предсказуемость поведения задействованных сервисных компонентов и их управляемость по отношению к резким переменам в среде ее развертывания. На рисунке представлено взаимодействие компонентов модулей интеллектуального ядра, на которые возлагается адаптивное управление показателями качества сервис-ориенти-

рованных систем. Статистический временной профиль, генерируемый модельно-аналитическим интеллектом, позволяет анализировать спланированную композицию действий бизнес-процессов.

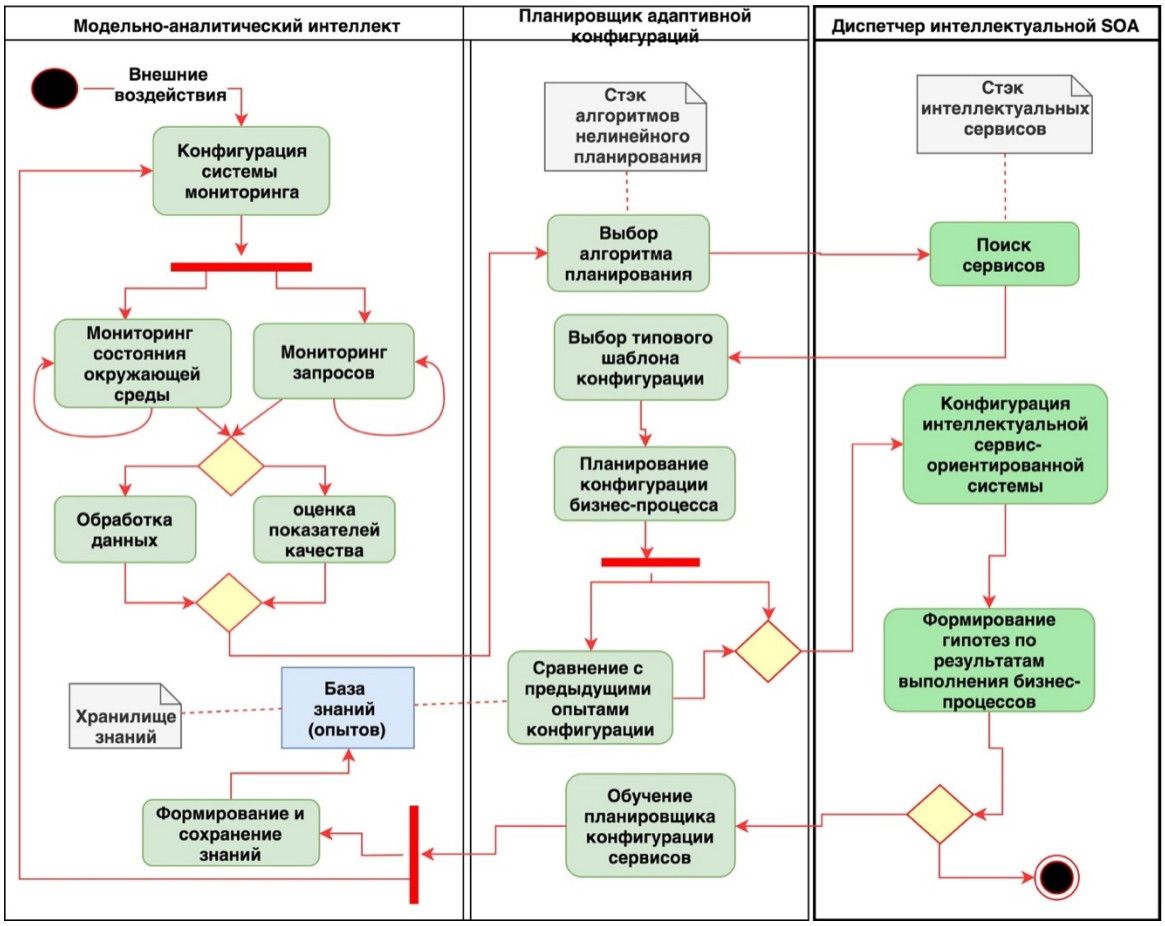


Рисунок. Объектно-ориентированная модель деятельности сервис-ориентированных систем с адаптивным управлением их качеством на основе многокомпонентного интеллектуального ядра

В представленной на рисунке объектно-ориентированной модели деятельности интеллектуального ядра адаптивного управления качеством планировщик или сервис планирования отвечает за построение моделей интеграции сервис-ориентированных средств с учётом предусловий и постусловий сервисов [4]. Модельно-аналитический интеллект отвечает за мониторинг статистических характеристик и оценивание качества спланированной интеграции [1, 3, 5]. Диспетчер отвечает за организацию сервис-ориентированной деятельности.

Интеллектуальные профили сервис-ориентированных систем [5] определяются взаимодействием системных компонентов, представленных на ри-

сунке. В зависимости от сложности задачи и достигаемой цели может осуществляться сочетание тех или иных системных компонентов, формирующих интеллектуальный динамический профиль.

Для определения динамического профиля предлагается метод анализа оцениваемых результатов качества на основе проверки статистической гипотезы с применением системы кривых Пирсона для формирования новых знаний и изучения адаптивности сервис-ориентированной системы. Перед применением метода необходимо выполнить следующие этапы:

1. Определение диспетчером типового шаблона интеграции для последующей композиции бизнес-процессов сервис-ориентированной системы;

2. Выбор алгоритма планирования действий. Данный шаг возлагается на сервис планирования действий с учетом предусловий и постусловий, которыми описывается каждый сервис [4]. Интеграция подразумевает типовые шаблоны в порядке последовательных, условных (альтернативных), параллельных и распределенных действий [3, 5]. Допустимо сочетание двух или нескольких типовых шаблонов в зависимости от сложности среды, что облегчает процесс адаптивного управления в режиме реального времени.

3. Вычисление временных характеристик типового шаблона интеграции и оценка его качества при условий выполнения деятельности в рамках установленного временного регламента.

4. Выполнение деятельности, связанной с управлением бизнес-процессов.

Далее, с целью определения динамического профиля, необходимо вычислить дополнительные показатели качества асимметрии и эксцесса, представляющие собой координаты на карте кривых Пирсона, с помощью которой подтверждается принадлежность временного профиля к некоторому распределению:

$$As = \frac{m_3}{\sigma^3},$$

$$Ek = \frac{m_4}{\sigma^4},$$

где As – показатель асимметрии,

Ek – показатель эксцесса,

σ – среднеквадратическое отклонение, которое оценивается по формуле:

$$\sigma = \sqrt{m_2}.$$

Второй, третий и четвертый центральные моменты вычисляются по формулам:

$$m_2 = D[k_{0,1,\ldots,i,\ldots,I}],$$

$$m_3 = \sum_{k_i}^{K_i} (k_i - E[k_{0,1,\ldots,i,\ldots,I}])^3 u(k_{0,1,\ldots,i,\ldots,I}),$$

$$m_4 = \sum_{k_i}^{K_i} (k_i - E[k_{0,1,\ldots,i,\ldots,I}])^4 u(k_{0,1,\ldots,i,\ldots,I});$$

где m_2, m_3 и m_4 соответственно второй, третий и четвертый центральные моменты случайной величины.

По успешному завершению фиксируется реальное полученное количество единиц дискретного времени, за которое выполнилась деятельность, и присваивается соответствующая вероятность из сформированной модельно-аналитическим интеллектом плотности распределения вероятностей. Выполненная деятельность описывается в виде объекта из признаков результатов и показателей качества следующей формулой:

$$BP_n^{(q)} = \langle E_n, D_n, C_n, As_n, Ek_n, RDT_n, probRDT_n \rangle,$$

где $BP_n^{(q)}$ – *n*-я сервис-ориентированная деятельность, принадлежащая *q*-классу, по которому классифицируются различные виды деятельности и значения их показателей качества, варьируемые в зависимости от предусловий и постусловий, которыми описывается каждый сервис, а также от состояния окружающей среды;

E_n – математическое ожидание *n*-го динамического профиля деятельности;

D_n – дисперсия *n*-го динамического профиля деятельности;

C_n – максимальное допустимое количество единиц дискретного времени выполнения *n-ой* деятельности динамического профиля;

As_n – асимметрия распределения вероятностей временного профиля *n*-ой деятельности;

Ek_n – эксцесс распределения вероятностей временного профиля *n*-ой деятельности

RDT_n и $probRDT_n$ – соответственно итоговое дискретное время выполненной деятельности и его вероятность из плотности распределения вероятностей $u(k_{1,2,\ldots,i,\ldots,I})$. Данные признаки являются результатом работы системы мониторинга модельно-аналитического интеллекта (рис.) и фиксируются в качестве временных характеристик по завершению сервис-ориентированной деятельности.

Таким образом, при длительном наблюдении и анализе поведения сервис-ориентированной системы открывается возможность изучить динамику её адаптивности при условии соблюдения установленного временного регламента по определенным классам вида деятельности.

Представленные формализации позволяют аналитически профилировать адаптивную эволюцию интеллектуальных сервис-ориентированных систем и входят в опорный методологический базис развития адаптивного управления их качеством в контексте самосовершенствования.

Список используемых источников

1. Птицына Л. К., Эль Сабаяр Шевченко Н. Н., Белов М. П. Моделирование сервис-ориентированных систем в условиях неопределённости // Международная конференция по мягким вычислениям и измерениям. 2018. № Секция 2. С. 291–294.

2. Птицына Л. К., Эль Сабаяр Шевченко Н. Интеллектуальная интеграция кластерных сегментов сервис-ориентированных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т. 3. С. 544–549.

3. Птицына Л. К., Смирнов Н. Г. Программное обеспечение компьютерных сетей. Управление крупно-гранулярными процессами на основе языка BPEL: учебное пособие; Федеральное агентство по образованию ; СПбГПУ. СПб.: Изд-во Политехнического ун-та, 2011. 106 с.

2. Птицына Л. К., Кондратьев Д. А., Эль Сабаяр Шевченко Н. Выбор алгоритма планирования для интеллектуальных сервис-ориентированных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2017. Т. 3. С. 277–282.

3. Птицына Л. К., Кондратьев Д. А., Эль Сабаяр Шевченко Н. Н. Интеллектуальные профили сервис-ориентированных архитектур // 70-я региональная научно-техническая конференция студентов, аспирантов и молодых учёных «Студенческая весна – 2016». СПб.: СПбГУТ, 2016. С. 340–344.

УДК 004.654
ГРНТИ 20.53.17

ОЦЕНКА И ВЫБОР ВАРИАНТОВ РАЗМЕЩЕНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ В ЕДИНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

И. Б. Саенко, И. Н. Фабияновский

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Рассматривается проблема размещения информационных ресурсов в зависимости от воздействия внешних угроз на элементы единого информационного пространства. Приводится сравнительная оценка различных вариантов. Обсуждается постановка задачи оптимизации размещения информационных ресурсов в едином информационном пространстве.

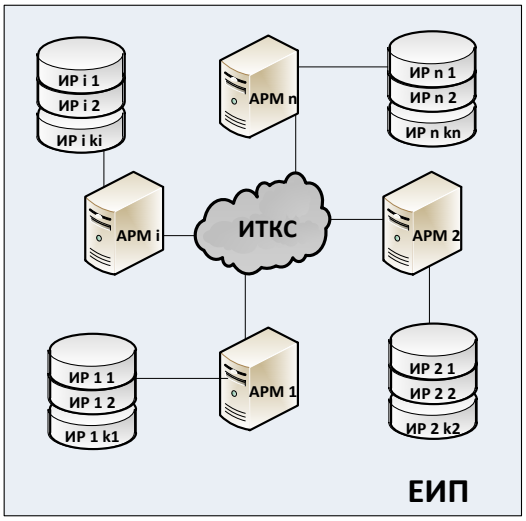
единое информационное пространство, информационный ресурс.

В настоящее время создание единого информационного пространства является весьма актуальной задачей, решение которой может быть эффективным только в том случае если она синтезирована на основе сочетания различных технологий, обеспечивающих оперативный и устойчивый доступ к информационным ресурсам [1, 2].

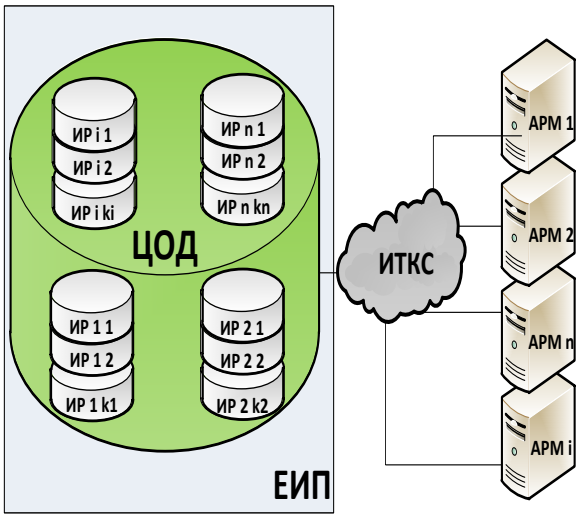
Единое информационное пространство (ЕИП) представляет собой совокупность баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных сетей (ИТКС), функционирующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей. ЕИП складывается из следующих главных компонентов [3]:

- информационные ресурсы (ИР), содержащие данные, сведения и знания, зафиксированные на соответствующих носителях информации;
- организационные структуры, обеспечивающие функционирование и развитие единого информационного пространства, в частности, сбор, обработку, хранение, распространение, поиск и передачу информации;
- средства информационного взаимодействия граждан и организаций, в том числе программно-технические средства и организационно-нормативные документы, обеспечивающие доступ к информационным ресурсам на основе соответствующих информационных технологий.

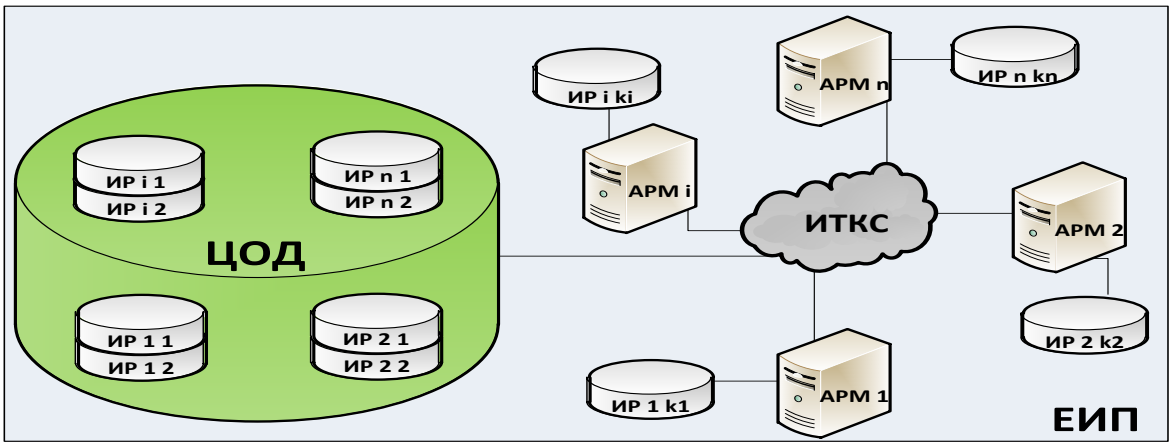
Информационные ресурсы являются важнейшими компонентами ЕИП. От варианта их размещения зависит эффективность информационного взаимодействия между пользователями. Возможны следующие три варианта размещения ИР в ЕИП: децентрализованный, централизованный и смешанный (рис.).



а) децентрализованный вариант



б) централизованный вариант



в) смешанный вариант

Рисунок. Варианты размещения ИР в ЕИП

Децентрализованный вариант размещения ИР в ЕИП (рис. а) предполагает, что ИР территориально разнесены и подключены к серверам или автоматизированному рабочему месту (АРМ). Связь между ИР обеспечивается с помощью ИТКС. К достоинствам этого варианта можно отнести высокую оперативность доступа к своим ИР (данным, сохраненным на своем устройстве хранения), а также высокую устойчивость при воздействии на ИР

внешних угроз. Недостатком является низкая оперативность доступа при работе с чужими ИР (данными, сохраненными на чужих устройствах хранения).

Централизованный вариант размещения ИР в ЕИП (рис. б) предполагает, что все ИР размещены в центре обработке данных (ЦОД). Связь между ИР и АРМ обеспечивается с помощью ИТКС. Таким образом, оперативность доступа к ИР оценивается как средняя. Недостатком этого варианта является сравнительно низкая устойчивость при воздействии внешних угроз на ЦОД.

Смешанный вариант размещения ИР в ЕИП (рис. в) предполагает, что часть ИР территориально разнесены и подключены к серверам или АРМ, а часть ИР размещается в ЦОД. Достоинствам этого варианта является как высокая оперативность доступа ко всем ИР, так и высокая устойчивость при воздействии внешних угроз на ЦОД и АРМ [4].

Результаты сравнительной оценки вариантов размещения ИР в ЕИП приведены в таблице. Их анализ показывает, что смешанный вариант способен обеспечить как достаточно высокую устойчивость ЕИП, так и высокую оперативность работы с ИР. Однако для достижения этой цели необходимо решить задачу оптимизации размещения ИР в ЕИП.

ТАБЛИЦА. Сравнительная оценка варианта размещения ИР в ЕИП

Показатель	Децентрализованный вариант	Централизованный вариант	Смешанный вариант
Устойчивость	Высокая	низкая	требуемая
Оперативность	высокая – к своим ИР/ низкая – к чужим ИР	средняя	требуемая

Суть задачи оптимизации размещения ИР в ЕИП заключается в том, чтобы, исходя из параметров, характеризующих ИР, ИТКС и внешние воздействия, найти (выбрать) вариант размещения ИР в ЕИП, отвечающий предъявляемым требованиям по оперативности и устойчивости.

Дальнейшие исследования планируется проводить в области практической реализации методов решения рассмотренной выше оптимизационной задачи и экспериментальной оценки вариантов размещения ИР в ЕИП, получаемых в ходе решения задачи.

Список используемых источников

1. Бирюков М. А., Брунилин А. А., Саенко И. Б. Имитационный подход к моделированию системы разграничения доступа к единому информационному пространству // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 78–83.

2. Саенко И. Б., Бирюков М. А., Ясинский С. А., Грязев А. Н. Реализация критериев безопасности при построении единой системы разграничения доступа к информационным ресурсам в облачных инфраструктурах // Информация и космос. 2018. № 1. С. 81–85.

3. Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов: Межотрасл. информ. служба. М.: Маркетинг, 1995. № 3. С. 3–8.

4. Котенко И. В., Саенко И. Б., Полубелова О. В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. 2013. № 2 (25). С. 113–134.

УДК 004.052.42+ 004.056.2
ГРНТИ 28.21.19; 28.21.15

АЛГОРИТМ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДЛЯ ЗАЩИТЫ NAND ФЛЕШ ПАМЯТИ

С. В. Таранов, С. В. Хорошенко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются коды, обнаруживающие алгебраические манипуляции, как решение для проблемы обеспечения целостности в средствах хранения информации, использующих технологию NAND флеш. Описываются две модификации алгоритма с применением вейвлет преобразований и без их использования. Дополнительное использование вейвлет преобразований позволяет снизить максимальное значение вероятности маскировки при этом добавляет в алгоритм банк вейвлет-коэффициентов.

целостность, теория кодирования, надежные коды, вейвлет-преобразование, NAND флеш память.

Вероятность ошибок растет с ростом сложности программно-аппаратной реализации современных средств хранения, обработки и передачи информации. Сложность влияет на кратность ошибки, ее характер, возможное распространение в кодовом слове. Для решения поставленной проблемы естественным решением является применение кодов, обнаруживающих и исправляющих ошибки. Помехоустойчивые коды широко используются в NAND флеш памяти, которая является одним из важнейших составляющих современных средств обеспечения целостности. Различают многоуровневую (MLC) и трехуровневую (TLC) NAND типы флеш памяти, оба типа хра-

нят более одного бита в каждой ячейке. Подобная структура памяти чувствительна к ошибкам высокой кратности, в связи с чем для нее необходимы алгоритмы, способные обнаруживать ошибки любой кратности.

Рассмотрим примеры программно-аппаратных средств хранения информации, в которых используется технология NAND флеш. Для каждого примера приведем базовые ошибки и применяемые методы обеспечения целостности.

NAND флеш является энергонезависимой памятью, основными составными элементами которой являются транзисторы с плавающими затворами, которые способны сохранять информацию даже при отсутствии питания. Преимуществами NAND флеш памяти можно назвать энергонезависимость, низкую стоимость, высокую плотность записи, быстрые операции записи и удаления. Среди недостатков многоуровневой NAND флеш памяти отдельно выделяют проблему обеспечения целостности информации, в частности, решению которой посвящена данная статья.

В настоящее время применение технологии NAND флеш памяти можно встретить в таких программно-аппаратных средствах, как:

- *Смартфоны, телефоны, ноутбуки и другие переносные устройства.* Технология NAND флеш памяти позволяет добиться высокой скорости записи и удаления информации, что является критичной для мобильных устройств;
- *Твердотельные носители (SSD диски)*. Области применения SSD дисков постоянно растут, они постепенно заменяют HDD благодаря лучшим показателями скорости, однако уступают последним по объему хранимых данных. Но уже в настоящее время SSD носители твердо заняли нишу на современном рынке средств хранения информации, преимущественно как кэш для HDD;
- *Центры обработки данных*. В центрах обработки данных применяется широкий спектр средств хранения информации, различающихся по сложности реализации, по требованиям к эксплуатации и многим другим параметрам.

Все перечисленные системы и программно-аппаратные средства крайне требовательны к высокому уровню обеспечения целостности.

Среди компаний-производителей средств хранения информации, использующих технологию NAND флеш, есть такие крупные, как Samsung, Toshiba, Micron, Intel. Производители NAND флеш памяти нацелены на дальнейшее увеличение плотности записи, в связи с чем создание новых алгоритмов обнаружения ошибок для данного типа устройств является актуальной задачей.

В данной статье рассматривается применение вейвлетных AMD кодов для защиты NAND флеш памяти. Аналогами для предлагаемого в данной работе метода являются:

- *Коды проверки на четность/Коды Хэмминга.* Обнаруживают две ошибки и исправляет одну ошибку. Эффективное решение для малой кратности ошибки, однако для NAND флеш памяти крайне важна устойчивость к ошибкам любой кратности;
- *Коды Боуза – Чоудхури – Хоквингема или коды БЧХ*. Примеры алгоритмов обеспечения целостности на основе кодов БЧХ можно найти в [1, 2]. Данный класс известен тем, что в нем можно задать требуемое минимальное кодовое расстояние, что непосредственно влияет на исправляющую способность кода. Но средства на основе технологии NAND флеш используют помехоустойчивые коды преимущественно как обнаруживающий искажения механизм;
- *Коды Рида-Соломона*. Линейные блочные коды, являющиеся подклассом БЧХ кодов, также используются в некоторых схемах NAND флеш памяти [3, 4]. Используются для исправления последовательностей ошибок, что может быть полезно в совокупности с другими помехоустойчивыми методами.

Последние исследования в области применения линейных кодов для защиты средств хранения информации, использующих технологию NAND флеш памяти [5, 6], показали недостатки данного класса. Линейные коды не минимизируют максимальную вероятность обнаружения ошибок и имеют по умолчанию множество необнаруживаемых ошибок. С учетом данных исследований, в качестве механизма защиты NAND флеш памяти предлагается использовать нелинейные коды, обнаруживающие алгебраические манипуляции. Предлагаемый механизм по определению обнаруживает все возможные аддитивные ошибки, что позволяет надежно защититься от искажений, характерных для многоуровневой (MLC) и трехуровневой (TLC) NAND флеш памяти.

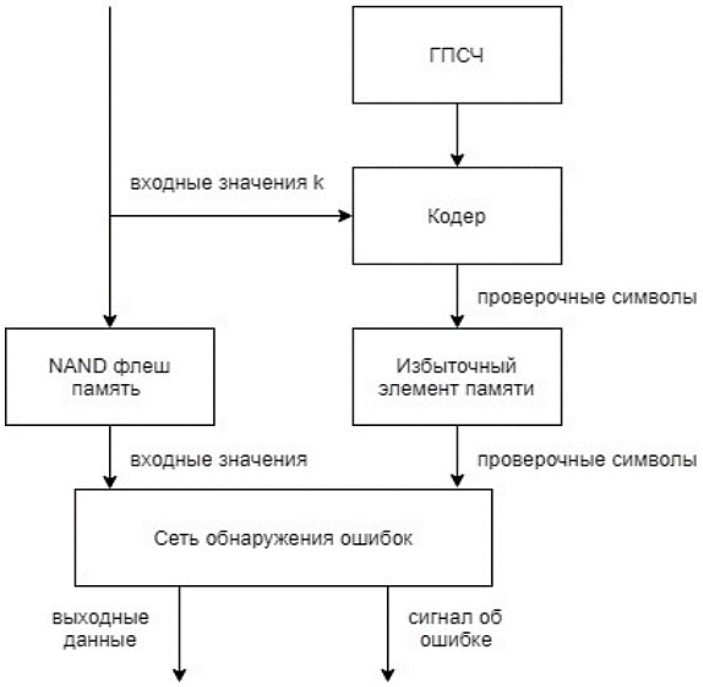


Рис. 1. Схема использования AMD кода для защиты NAND флеш памяти

Алгоритм защиты NAND флеш памяти, использующий нелинейный AMD код показан на рис. 1. Алгоритм представляет собой схему одновременного обнаружения ошибок, состоящую из оригинального устройства

хранения, избыточного элемента памяти, кодера AMD кода и генератора псевдослучайных чисел (ГПСЧ), который используется для усиления обнаруживающих характеристик алгоритма. Последним составляющим элементом является сеть обнаружения ошибок, выполняющая проверку целостности информации, выгружаемой из NAND флеш памяти.

Опишем общий принцип работы алгоритма. При записи информации на устройство хранения с технологией NAND флеш, кодер генерирует избыточные биты и сохраняет кодовое слово в блок памяти. При чтении информации из памяти, сеть обнаружения ошибок генерирует проверочные биты заново на основе информационной части кодового слова и сравнивает их с выгруженными из памяти избыточными битами. В результате работы алгоритма мы получаем сигнал об ошибке, который может передаваться далее на механизм исправления ошибок или процедуру восстановления.

Использование вейвлет-преобразования совместно с AMD конструкцией позволяет добиться высокой производительности в случае работы в системах с рассчитанными вейвлет-коэффициентами. В таком случае целесообразным будет использовать алгоритм, представленный на рис. 2.

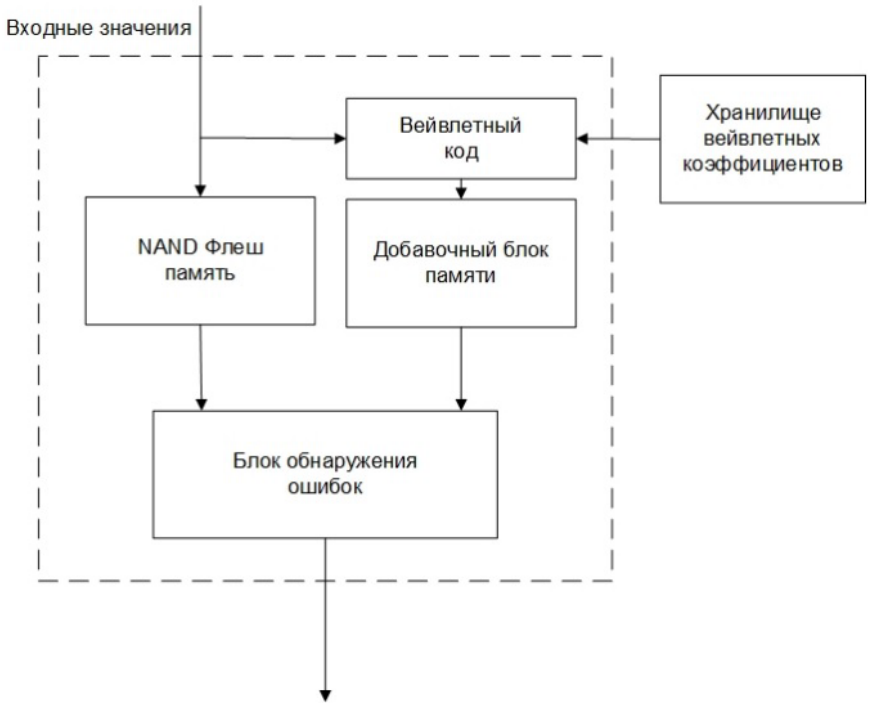


Рис. 2. Структура системы обеспечения целостности на основе вейвлетных AMD кодов для защиты NAND флеш памяти

Опишем алгоритм генерации кодовых слов для вейвлетного AMD кода. Обозначим исходную информационную часть как $x = (x_1, x_2, \dots, x_N)$. Кодовое слово, получившееся после преобразования, обозначим $c = (v, r)$, где

$v = (v_1, v_2, \dots, v_{N/2})$ – информационная часть, а $r = (r_1, r_2, \dots, r_{N/2})$ избыточная часть.

При выполнении вышеописанных условий, множество всех кодовых слов линейного вейвлетного кода может быть задано с помощью порождающей матрицы, которая имеет вид:

$$c = x(H^T + aG^T J),$$

тогда проверочная матрица вейвлетного кода будет иметь вид:

$$c(\overline{H}^T + bJ^T \bar{G}^T) = 0,$$

где a, b некоторые вектора, принадлежащие полю $GF(q)$ и удовлетворяющие условию $ab = (p-1)\ mod\ p, p \in GF(q), J = cir(0,1,0,\dots,0)$ – матрица размерности $N/2 \times N/2$.

Нелинейный AMD код, показанный на рис. 2, представляет собой функцию кодирования следующего вида

$$F(x, y) = (x_1 * y_1, x_2 * y_2, \dots, x_N * y_N),$$

где x, y две равные части информационного сообщений, рассматриваются как элементы поля $GF(q)$, соответственно $x_1 * y_1 \in GF(q)$.

Вейвлетный AMD код, показанный на рис. 2, также является нелинейным как и предыдущая конструкция (рис. 1). В основе содержит ту же функцию кодирования, однако функция применятся к результату вейвлет преобразования информационного потока представляет собой функцию кодирования следующего вида

$$F(v, r) = (v_1 * r_1, v_2 * r_2, \dots, v_N * r_N),$$

где v, r основной и вейвлет поток после вейвлет преобразования, соответственно $v_1 * r_1 \in GF(q)$.

Более подробное описание методов обеспечения целостности на основе вейвлетных разложений можно найти в работах [7, 8, 9].

Таблица содержит сравнительную характеристику предлагаемого в диссертации метода кодирования на основе вейвлетов и аналогов.

Вейвлетные AMD коды позволяют обнаруживать ошибки любой кратности, они устойчивы к изменениям в распределении входных кодовых слов. Данные свойства являются наиважнейшими для NAND флеш памяти. Но стоит заметить, что оба предложенных в данной статье алгоритма, представленные на рис. 1 и 2, являются нелинейными кодовыми конструкциями.

И как видно из таблицы, программно-аппаратная реализация схемы кодирования для предложенным методов будет сложнее по сравнению с линейными кодовыми конструкциями.

ТАБЛИЦА. Сравнительная характеристика методов обеспечения целостности, применяемых в NAND флеш

	Хэмминга	РС	БЧХ	AMD	Вейвлетный AMD код
Тип устройства хранения	SLC	MLC	MLS/TLS	MLS/TLS	MLS/TLS
Тип ошибки	одиночные	группа	одиночные	Любая кратность	Любая кратность
Площадь схемы кодирования	Малая	Средняя	Средняя	Большая	Большая
Потребление мощности	Низкое	Высокое	Высокое	Высокое	Высокое

Заключение

В статье предлагается алгоритм на основе AMD кодов в качестве механизма обеспечения целостности для NAND флеш памяти. Предложены две модификации алгоритма – первая с использованием PN функции, вторая на основе вейвлет преобразований в конечных пространствах. Обе модификации минимизируют максимальное значение вероятности маскировки ошибки, а также обнаруживают ошибки любой кратности. Данные критерии имеют первостепенное значение для систем и средств хранения информации, использующих технологию NAND флеш.

Список используемых источников

1. Ge, S. Wang, Z. Karpovsky, M. Secure memories resistant to both random errors and fault injection attacks using nonlinear error correction codes // Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy / ACM. 2013. P. 5.

2. Ge, S. Wang, Z. Karpovsky, M. G. Reliable and Secure Memories Based on Algebraic Manipulation Detection Codes and Robust Error Correction // Proc. Int. Depend Symp / Citeseer. 2013.

3. Luo, P. Wang, Z. Karpovsky, M. G. Secure nand flash architecture resilient to strong fault-injection attacks using algebraic manipulation detection code // Proceedings of the International Conference on Security and Management (SAM) / The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). 2013. P. 1.

2. Karpovsky, M. G. Nagvajam, P. Optimal codes for the minimax criteria on error detection // IEEE Trans on Information Theory. 1989. Vol. 35. No. 6. Pp. 1299–1305.

3. Karpovsky, M. G. Kulilowski, K. J., Taubin, A. Robust protection against faultinjection attack on smart cards implemention the Advanced Encryption standard // Proceeding of Dependeable Systems and Networks. 2004. Pp. 93–101.

4. Kulikowski, K. J., Karpovsky, M. G. Robust correction of repeating Errors in by Non-linear Codes // IET Communications. 2011. Vol. 5. No. 16. Pp. 2317–2327.

5. Levina, A. Taranov, S. Creation of codes based on wavelet transformation and its application in ADV612 chips // International Journal of Wavelets, Multiresolution and Information Processing. 2017. Vol. 15. No. 2. P. 1750014.

6. Levina, A. B. Taranov, S. V. Algorithms of constructing linear and robust codes based on wavelet decomposition and its appllication // Lecture Notes in Computer Science. 2015. — Vol. 9084. Pp. 247–258.

7. Levina, A. B. Taranov, S. V. New Construction of Algebraic Manipulation Detection Codes Based on Wavelet Transform // Proceedings of the 18th Conference of Open Innovations Association FRUCT. 2016. Pp. 187–192.

УДК 004.7
ГРНТИ 50.39

ВОПРОСЫ МОДЕЛИРОВАНИЯ И АНАЛИЗА ХАРАКТЕРИСТИК МУЛЬТИМЕДИЙНОГО ТРАФИКА В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

В. А. Тарасов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются современные методы анализа мультимедийного трафика с учётом помехозащищённости и предотвращения перегрузок для обеспечения надлежащего качества обслуживания в сетях с интеграцией служб. Проводится обзор подходов к оценке производительности инфотелекоммуникационных инфраструктур, оценка влияния внешних и внутренних факторов на вероятностно-временные характеристики и иные показатели качества обслуживания. Осуществляется анализ перспектив разработки, модернизации, внедрения и расширения коммуникационных услуг и мультимедийных аппаратно-программных комплексов для решения различных задач.

Triple Play, IPTV, средства виртуальной реальности.

В настоящее время традиционные средства коммуникаций постепенно уступают место системам с интеграцией служб, и, по-видимому, в недалёком будущем вытеснят их. Современные поставщики информационных услуг разного масштаба активно предлагают абонентам в дополнение к Интернет-доступу в рамках одного пакета или отдельно доступ к набору телевизионных каналов, а также IP-телефонию, что в совокупности принято именовать термином «Triple Play», и другие услуги.

Несмотря на рост технологического уровня приёмо-передающих средств, остаётся актуальной проблема обеспечения защиты от перегрузок.

Основные методы исследования трафика современных телекоммуникационных сетей базируются на анализе трафиковых трасс (зависимости числа пакетов от времени). Данные исследования показали, что современный телекоммуникационный трафик, который можно рассматривать как локально-стационарный случайный процесс, обладает свойствами самоподобия. Установлены характерные законы распределений для интенсивности трафика. Однако исследование трафика методами теории массового обслуживания требует использования таких параметров как интервалы времени между пакетами и длительности пакетов.

Для получения наиболее полной информации о статистических свойствах трафика мультимедийных приложений необходимо исследовать характеристики потоков, передаваемых на различных уровнях мультисервисной сети, что позволит проследить влияние объединения потоков на уровне агрегации на свойства трафика.

Исследования показали, что трафик уровня агрегации (суммарный и выделенный IPTV) в меньшей степени обладает самоподобными свойствами, чем трафик уровня доступа. Схожесть законов распределений случайных интервалов времени между пакетами и длин пакетов трафика общего и IPTV указывает на большое влияние телевизионного трафика на трафик уровня агрегации. Это можно объяснить преобладанием видеотрафика IPTV в суммарном информационном потоке [1].

Перегрузки наблюдаются в сетях SIP-серверов при отсутствии достаточного ресурса производительности для обработки получаемых сигнальных сообщений. Одним из способов управления перегрузками в сетях SIP-серверов является механизм просеивания нагрузки. Существует имитационная модель контроля перегрузок, основанная на гистерезисном управлении нагрузкой и механизме контроля перегрузок RBOC (Rate-based Overload Control). Механизм работает таким образом, что в случае наступления перегрузки сервер сообщает вышележащим серверам, сколько запросов в единицу времени он готов принять от каждого из них. Данный механизм гарантирует, что нижележащий сервер не получит объём трафика больший, чем он сможет обработать [2].

Одной из наиболее важных задач мультисервисных сетей NGN/IMS с использованием SIP-серверов является поддержка качества обслуживания мультимедийного трафика, минимизация временных характеристик задержек доступа к услугам.

Эффективность использования подсистем мультимедийной связи IMS в значительной степени зависит от пропускной способности сетей NGN/IMS с использованием SIP-серверов и сетевого оборудования системы управления сеансами CSCF. Для гарантированного обслуживания таких нагрузок

необходимы максимальная пропускная способность сети NGN/IMS, минимальные средние задержки в системе IMS, повышенные коэффициенты эффективного использования ресурсов SIP-серверов и т. д.

Исследования показали, что оценки и анализ показателей платформы мультимедийной связи IMS как средней длины очереди СМО, так и среднего времени задержки передачи трафика в функции загрузки являются весьма важными при изучении мультисервисных сетей с учётом самоподобия служебного и полезного трафиков. Предложены математические модели в виде СМО общего вида с очередями и получены аналитические выражения, позволяющие оценить показатели эффективности NGN/IMS с учётом свойств самоподобия мультимедийного трафика, обеспечивающего гарантированное качество услуг, регламентируемых рекомендациями ITU-T [3].

Средства виртуальной реальности (VR), являясь одной из составляющих мультимедийных систем, расширяют сферу своего распространения, интегрируясь с телекоммуникационными системами.

Развитие телекоммуникационной отрасли не может ограничиваться только совершенствованием уже применяемых технологий и программно-аппаратных средств. В контексте ожидаемых масштабных преобразований в функционировании социальных институтов и экономических субъектов для сферы телекоммуникаций необходим поиск направлений опережающего развития, результатом которого должно являться заблаговременное формирование новых, но востребованных в будущем сегментов рынка телекоммуникационных сервисов и входящих в их состав услуг. С точки зрения экономической эффективности предлагать новые телекоммуникационные сервисы и услуги целесообразно в наибольших сегментах существующего рынка, отвечающих наиболее предпочтительным целевым аудиториям: доступ в Интернет и мобильная (сотовая) связь [4].

В нынешних условиях сотовая связь и мобильный Интернет являются общедоступными в большинстве стран мира, а география областей покрытия и аудитория абонентов данных телекоммуникационных сервисов стабильно расширяются. Любой абонент оператора сотовой связи может быть идентифицирован по номеру телефона, и дополнительная телекоммуникационная услуга на основе технологий виртуальной реальности оказывается ему посредством использования уже подключенных услуг мобильного Интернета. Ниже представлена концепция реализации такой дополнительной услуги на основе типовой телекоммуникационной системы (ТКС) сотовой связи.

1. На современных мобильных телефонах и смартфонах выполняются VR-приложения; данные устройства используются в качестве экранов для специальных шлемов, то есть выполняют основную функцию оконечных устройств ТКС.

2. Интерактивное взаимодействие с выполняемым приложением VR обеспечивается использованием контроллеров, которые дополняют функционал оконечных устройств ТКС.

3. Сети приемо-передающих устройств для подключения абонентов к услуге обеспечиваются уже используемым оборудованием операторов сотовой связи – базовыми станциями, линиями связи, коммутационными центрами и т. д.

4. Для коммутации потребителей дополнительной услуги требуется дополнить типовую ТКС сотовой связи сервером, обеспечивающим синхронизацию абонентов в процессе использования конкретного приложения VR. Данный сервер сможет обеспечить также работу абонентов, использующих любые способы доступа в Интернет.

В общем виде структура сервиса телекоммуникационных услуг в средах виртуальной реальности приведена на рис. 1.

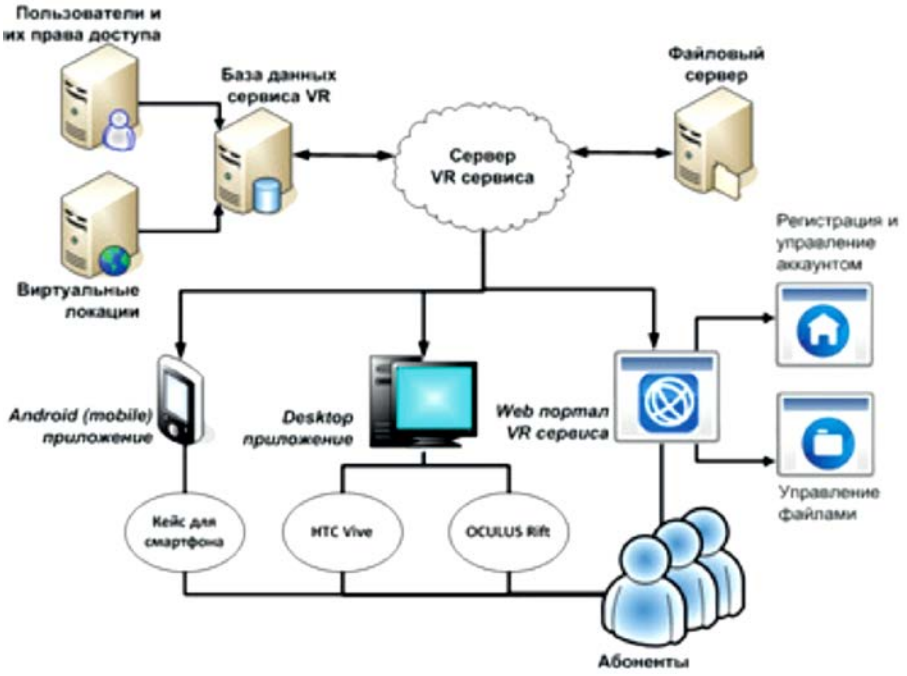


Рис. 1. Общий вид структуры сервиса в средах виртуальной реальности

Структура сервера VR-сервиса в общем виде представлена на рис. 2.

Фактически оператор сотовой связи автоматически предоставляет свою ТКС и мобильный Интернет как техническое обеспечение для рассматриваемой дополнительной услуги. При этом основания для взимания оплаты с её потребителя и/или оператора (провайдера) у него отсутствуют. Помимо мобильных телефонов и смартфонов в качестве оконечных устройств могут использоваться специализированные устройства виртуальной реальности, такие как шлемы HTC Vive и Oculus Rift.

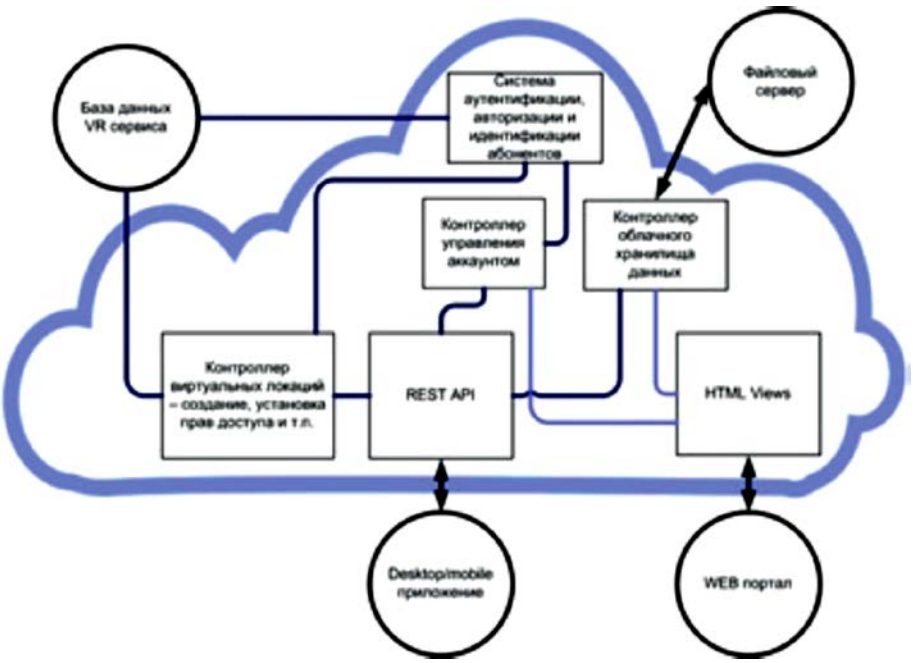


Рис. 2. Общий вид структуры сервера VR-сервиса

Основными задачами, требующими решения для реализации рассматриваемых телекоммуникационных сервисов и услуг, являются:

− обеспечение достаточных вычислительных мощностей оконечных устройств;

− быстрая передача и обработка больших объемов мультимедийной информации.

Данные задачи в среднесрочной перспективе могут иметь комплексное решение с учетом тенденций развития технологий передачи и обработки информации.

Список используемых источников

1. Буранова М. А., Карташевский В. Г., Самойлов М. С. Анализ статистических характеристик мультимедийного трафика узла агрегации в мультисервисной сети // Радиотехнические и телекоммуникационные системы. 2014. № 4 (16). С. 63–69.

2. Самуйлов К. Е., Павлоцкий О. Э. Имитационная модель механизма снижения скорости передачи при управлении перегрузками сервера протокола установления сессий // T-Comm: Телекоммуникации и транспорт. 2016. Том 10. № 3. С. 44–48.

3. Ибрагимов Б. Г., Гасанов А. Г. Исследование и оценка эффективности мультисервисных сетей NGN/ IMS при передаче мультимедийных трафиков // T-Comm: Телекоммуникации и транспорт. 2017. Том 11. № 2. С. 15–18.

4. Зуев А. С., Болбаков Р. Г. О телекоммуникационных сервисах на основе технологий виртуальной реальности // Российский технологический журнал. 2017. Т. 5. № 6 (20). С. 3–10.

Статья представлена заведующим кафедрой,
доктором технических наук, профессором Л. К. Птицыной.

УДК 378.146
ГРНТИ 14.35

ПРИМЕНЕНИЕ ИННОВАЦИОННОГО ПОДХОДА ПРИ ПРОВЕДЕНИИ АТТЕСТАЦИИ В РАМКАХ ТЕХНИЧЕСКИХ ДИСЦИПЛИН

В. А. Тарасов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Предлагается подход к организации промежуточной и итоговой аттестации, где в качестве альтернативы традиционным средствам контроля выступает взаимодействие между обучающимися, ставящими и решающими прикладные задачи, используя как знания, полученные в рамках дисциплины, так и аналитические способности. Данный подход призван обеспечить привнесение в образовательный процесс как соревновательной составляющей, так и потребности в коллективном решении задач. Тем самым появляется некий игровой компонент, мотивирующий обучающихся к профессиональному обучению, а также к развитию навыков работы в коллективе.

инновационные подходы, технические дисциплины, конкуренция.

Образование во все времена является одной из основ развития цивилизации. Качество образования непосредственно влияет на качество жизни как лица его получившего, так и общества в целом. В свою очередь, качество образования определяется во многом теми приёмами, средствами, технологиями, которые лежат в его основе.

Под инновационным подходом в системе образования понимаются процессы совершенствования педагогических технологий, совокупности методов, приёмов и средств обучения [1].

Инноватика как теория и практика всей жизни в настоящее время является одной из самых острых и актуальных тем общества в целом, образования и воспитания в частности.

В настоящее время инновационная педагогическая деятельность является одним из существенных компонентов образовательной деятельности любых учебных заведений и организаций. Ведь именно инновационная деятельность создаёт основу для создания конкурентоспособных кадров, определяет направления профессионального роста преподавателя. Творческий подход педагога становится сегодня важной характеристикой деятельности образования и означает переход на более высокую ступень организации образовательного процесса.

Инновации в образовании – это использование новых, повышающих эффективность способов, средств:

− подачи информации;

− представления знаний;

− обучения самостоятельному поиску нужной информации, проверки её адекватности;

− повышения интереса к новому материалу;

− контроля усвоения информации и знания.

Применяя инновационные подходы, важно создать такие психолого-педагогические условия, в которых обучающийся сможет занять активную личностную позицию и в полной мере проявить себя как субъект учебной деятельности. Дидактический принцип активности личности в обучении и профессиональном самоопределении обусловливает систему требований к учебной деятельности обучающегося и педагогической деятельности преподавателя в едином образовательном процессе. В эту систему входят внешние и внутренние факторы, потребности и мотивы конкретных форм и методов обучения. Многое зависит от того, как преподаватель пользуется тем или иным методом.

В системе обучения студентов в вузах инженерно-технического профиля наблюдаются следующие противоречия: между объективной востребованностью общества в высококвалифицированных инженерно-технических кадрах, имеющих сформированную установку на постоянное развитие деятельностных и личностных качеств, которые отвечают потребностям сегодняшнего дня, и недостаточной проработкой методологии процесса оптимизации профессионального обучения; между необходимостью формирования требуемых профессиональных компетенций в процессе обучения будущих инженеров и жестким определением критериев оптимизации обучения необходимым дисциплинам в вузе; между требованиями современных промышленных и инженерно-технических предприятий к инженерным кадрам и несоответствием уровня компетентности педагогических кадров вузов [2].

Такая постановка вопроса свидетельствует об актуальности осмысления теоретических основ и практических путей совершенствования системы подготовки компетентных специалистов в вузах инженерно-технического профиля.

Ученые справедливо обращают внимание на то, что в настоящее время процесс подготовки научно-технических кадров должен выстраиваться в соответствии с новыми требованиями, связанными с установкой на инновационное образование, интегрированное с интенсивной научно-исследовательской деятельностью как студентов, так и педагогов.

При определении инновационной составляющей современного российского образования, ориентированного на международный уровень предприятий, прежде всего, необходимо определиться с перечнем знаний и навыков, которыми должен обладать специалист, чтобы быть востребованным этими предприятиями. В результате анализа можно выделить следующее. Выпускник вуза должен:

− безусловно, быть специалистом в своей области;

− владеть набором необходимых знаний экономики и юриспруденции;

− владеть иностранным языком;

− знать принципы постановки задачи и организации ведения научно-исследовательских и опытно-конструкторских работ (НИОКР);

− обладать знаниями основных принципов коммерциализации результатов НИОКР;

− уметь принимать нестандартные решения или решать нестандартные задачи.

Важно также учитывать, что в настоящее время функционал будущей профессиональной деятельности специалистов, работающих согласно должностным инструкциям на инженерных должностях на предприятиях и в организациях той или иной отрасли, является достаточно обширным. В контексте решаемых задач выделяются следующие группы инженеров по выполняемым ими функциям:

− инженеры-организаторы (менеджеры) – занимаются организацией работы на производстве и принимают управленческие решения (начальник цеха, отдела, лаборатории, директор предприятия и т. п.);

− инженеры-конструкторы – занимаются проектированием машин, приборов, оборудования, различных устройств;

− инженеры-технологи – участвуют в проектировании и внедрении технологических процессов;

− инженеры-эксплуатационники − обеспечивают функционирование производственных процессов на заданном уровне (механики, энергетики, технологи и т. д.);

− инженеры-исследователи – занимаются научно-исследовательской работой в заводских лабораториях или в научно-исследовательских организациях;

− инженеры прочих функциональных подразделений (информационно-вычислительные центры, отделы научно-технической информации, материально-технического снабжения, патентные бюро и др.) – обеспечивают функционирование производства.

В образовании выделяются следующие тенденции, которые будут проявляться в разной степени в ближайшем будущем:

− осознание каждого уровня образования как органической составной части системы непрерывного образования;

− индустриализация обучения, т. е. его компьютеризация и сопровождающая её технологизация, что позволяет действенно усилить интеллектуальную деятельность современного студента;

− переход от преимущественно информационных форм к активным методам и формам обучения, т. е. обучению проблемному, с широким использованием резервов самостоятельной работы обучающихся.

Важно подчеркнуть, что мышление инженера представляет собой процесс, имеющий сложную структуру. Этот процесс содержательно включает экологический, эргономический, экономический, эстетический, управленческий и коммуникативный компоненты. Процесс мышления функционально выражен в логических, научных, практических, творческих и образно-интуитивных формах мышления. Чтобы сформировать гармонично развитого специалиста, обладающего системным мышлением, преподаватели технического вуза должны преодолевать узкоспециальный взгляд на задачи обучения и особую роль своей учебной дисциплины.

Современные образовательные технологии должны удовлетворять целому ряду требований. Они должны обеспечивать лёгкость восприятия, высокую усвояемость, способность анализировать и принимать приемлемые решения, занимая при этом минимум временного ресурса. Не последнюю роль играет и уровень остаточных знаний.

Однако высокое качество усвоения материала зачастую является не единственной целью осуществления образовательного процесса. Важными являются воспитательная и социализирующая его составляющие, которые проще реализовать в крупных коллективах.

Технические дисциплины занимают особую нишу в системе образования. Они, как правило, характеризуются большим объёмом разнородной информации, необходимостью творческого подхода и использования логического мышления, а зачастую предполагают и необходимость коллективного выполнения задач. Прежде всего, это относится к таким формам обучения как лабораторные и практические занятия.

При проведении аттестации по дисциплине для лучшего выявления уровня её освоения, а также для придания контролю знаний увлекательного характера, представляется целесообразным следующий подход.

Прежде всего, необходимо подготовить лабораторно-техническую базу (например, небольшую компьютерную сеть, компоненты которой осваивались обучающимися в рамках данной дисциплины – аппаратные и программные средства и, при необходимости, вспомогательный инструментарий).

Далее из обучающихся либо по желанию, либо случайным образом формируется пара – «нарушитель» и «администратор». Для получения положительной оценки один из них должен одержать верх в соревновании с другим.

Задача «нарушителя» – за ограниченное время (например, 1 минуту) вывести лабораторную систему из стабильного состояния (например, путём изменения настроек протокола). При этом его действия не должны привести к порче оборудования или потенциальной возможности его порчи.

«Администратору» надлежит за ограниченное время, превышающее время данное «нарушителю» (например, 5 минут), вернуть систему в работоспособное состояние.

Если «администратор» выполняет свою задачу, то получает положительную оценку, в противном случае аттестуется «нарушитель». Не получивший положительную оценку включается в состав другой пары. Последний обучающийся, оставшийся без пары, аттестуется по усмотрению преподавателя.

Данный подход привносит в процесс освоения дисциплин конкурентную составляющую, которая мотивирует к более глубокому освоению дисциплины, способствует повышению навыков решения практических задач и, за счёт конкуренции, их сложности, а также потенциально стимулирует развитие навыков социальной коммуникации.

В дальнейшем значение новых подходов к реализации образовательной деятельности будет расти, как и конкуренция в их разработке.

Список используемых источников

1. Шайдулина А. А., Мамадалиев О. О. О применении инновационных подходов в процессе обучения // Молодой ученый. 2016. № 6 (110). С. 839–841.

2. Хомичева В. Е., Федоркина А. П. Особенности профессионального обучения студентов в вузах инженерно-технического профиля // Вестник Сибирского государственного индустриального университета. 2013. № 2 (4). С. 55–60.

Статья представлена заведующим кафедрой,
доктором технических наук, профессором Л. К. Птицыной.

УДК 004.056.53
ГРНТИ 81.93.29

МЕТОДИКА БЫСТРОЙ ОБФУСКАЦИИ CLASS-ФАЙЛОВ JAVA-ПРИЛОЖЕНИЯ С МИНИМАЛЬНЫМ ИСПОЛЬЗОВАНИЕМ РЕСУРСОВ

П. И. Шариков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Защита программного обеспечения является актуальной задачей. В статье объясняется необходимость защиты байт-код java-приложения с помощью обфуцирования предложенных методов. На основе полученных результатов работы декомпиляторов и java-компилятора предлагается методика обфуцированная java-кода с целью усложнения реверс-инженеринга class-файлов java. Сделан вывод о возможности использования исследуемого метода для защиты java-приложения.

Java, bytecode, байт-код, методы защиты байт-кода, digital watermark, стеганография, исполняемые файлы, obfuscator, обфуцирование, запутывание, obfucation.

Технологии развиваются стремительно. На текущий момент, самый популярный язык программирования – Java.

Именно на этом языке написано множество приложений, которые используются в самых разных сферах, начиная от касс в супермаркетах и заканчивая банковской сферой. Следствием этого является повышенный интерес недобросовестных пользователей к программам, частям различных проектов, которые написаны на Java или работают на JVM.

Программы на Java кроссплатформенны, также существует много сайтов использующих Java-апплеты, логику клиент-сервер. Таким образом, данный язык покрывает все сферы IT, будь то бесконтактные карты, роутеры или оборудование компании cisco [1].

Разумеется, такая популярность языка дает о себе знать. Java-файлы легко анализируются [2]. Грамотному специалисту, практически не составит труда, получить исходный код, имея на руках class-файл вашей Java-программы, об этом говорилось в предыдущих статьях [3].

Шифратор, на английском – obfuscator, – это программа, которая в большей или меньшей мере изменяет байт-код или исходный код Java [4] приложения. Исходный код Java-программ преобразуется в байт-код после компиляции. Естественно, возможен и обратный процесс – декомпиляция. Существует огромное количество декомпиляторов, которые могут извлечь исходный код приложения в довольно хорошем качестве. Все это ставит под

угрозу интеллектуальную собственность автора программ и алгоритмов. Поэтому необходимо усложнять reverse engineering.

Программные обфускаторы используются для преобразования кода, таким образом, что его становится труднее понять. Запутывание Java-программ особенно важно, поскольку двоичная форма Java, байт-код Java[5-6], является относительно высокоуровневым и подвержен качественной декомпиляции. В данной статье представлено три вида методов запутывания, которые:

1. Скрывают действия кода на операционном уровне;
2. Запутывают структуру программы, усложнение потока управления и запутанный объектно-ориентированный дизайн;
3. Использование семантический разрыв между тем, что разрешено на уровне исходного кода Java, и тем, что разрешено на уровне байт-кода.

Самый быстрый и простой способ обфускации кода изменяет структуру программы следующими способами:

- переименованием идентификаторов;
- удалением информации отладчика.

При компиляции java классов компилятор может сохранять отладочную информацию [7], которую можно использовать, например, для удаленной отладки приложения. По-умолчанию javac сохраняет информацию о номерах строк исходного файла и самом исходном файле, а имена локальных переменных не сохраняются [8].

Отключить сохранение debug информации можно с помощью опции -g:none. Пример в листинге.

ЛИСТИНГ. Отключение отладочной информации

```
javac -g:none MyClass.java
```

Возможно, также одно из самых простых, но очень эффективных средств преобразования – переименование идентификаторов. Байт-код Java сохраняет имена классов, полей и методов, и эти имена часто очень полезны для reverse engineering. Например, метод с именем getDate, с типом возврата Date является довольно явным и однозначным. Некоторые из этих имен не могут быть затронуты, потому что они могут быть определены в библиотеках, упомянуты посредством отражения или как точки входа в приложение. Тем не менее, для остальных случаев поля, методы и классы могут быть переименованы [9].

Была разработана методика для выбора имен идентификаторов. Смысл ее работы заключается в том, что в коде создаются случайные строки с использованием символов, которые трудно различить визуально. Таким образом, мы случайным образом создаем действительные идентификаторы из

алфавитов {*S*, 5 $}, {l, 1, I} и {_}. В этом случае декомпилированный код будет включать идентификаторы, такие как *I1l, Ill,* ____, _____, *S5S$* или *SS5$*. Эти идентификаторы явно будут искажены для реверс-инженеров, и, хотя какой-либо инструмент может заменить их с менее визуально запутанными идентификаторами, это не простой процесс создания семантически значимых имен для подобного рода инструментов.

Вторая составляющая методики – заимствовать имена из других частей приложения или стандартных библиотек. В этом случае getDate может быть переименован в getFirstName. Эта замена не так очевидна для реверс-инженера или инструмента и передает неверную семантическая информацию.

Третья часть методики – упаковка локальных переменных в битовые поля (PLVB). Чтобы использовать обфускацию в локальных переменных типов (Boolean, char, byte integer) можно произвести объединение некоторых переменных и упаковать их в одну переменную, которая имеет больший размер, например, long. Для реализации более сложного алгоритма обфускации, рекомендуется выбирать случайным образом диапазон битов для каждой локальной переменной. Например, переменная с целым числом может быть упакована в биты с 9 по 43. Поскольку каждое чтение или запись исходной переменной может быть заменено на операцию упаковки и распаковки, то при использовании обфуцированного кода таким образом, возможно незначительное замедление работы приложения.

Четвертая часть методики – Добавление операторов переключения неиспользуемого / «мертвого» кода (ADSS) [10].

Конструкция switch-case в байт-коде java предлагает полезный инструмент для обфускации потока управления программой. Это единственный естественный способ (отличный от структуры try-catch) для создания графа потока управления приложением, который имеет один входной узел, с числом приемников более, чем два. Данная структура может значительно увеличить сложность метода.

В данном блоке предлагается добавлять дополнительные ребра в граф потока управления приложением, посредством добавления переключателя switch-case. Также, необходимо «обернуть» всю конструкцию неявный предикат, для убеждения в том, что данный метод никогда не будет выполнен.

Все инструкции байт-кода имеющие нулевой приоритет в стеке – потенциально безопасны для прыжков от цели к цели в коммутаторе [11]. Рекомендуется выбор случайного набора целей (case) для switch. Данное обфуцирование увеличивает связность кода и общую сложность метода. Декомпилятор не сможет удалить данную конструкцию, даже несмотря на то, что она вроде бы «мертвый» код. Это достигается за счет «обертки» конструкции switch-case в неявный предикат, потому что декомпилятор не статическим анализом определить значение непрозрачного предиката.

Список используемых источников

1. Красов А. В., Шариков П. И., Методика защиты байт-кода java-программы от декомпиляции и хищения исходного кода злоумышленником // Вестник СПбГУТД. 2017. № 1. С. 47–50.

2. Шариков П. И., Красов А. В., Исследование уязвимости сериализации и десериализации данных в Java // Региональная информатика и информационная безопасность. Сборник научных трудов. Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. Труды РИИБ 2017. 3 выпуск.

3. Shterenberg, S. I., Krasov, A. V., Ushakov, I. A. Analysis of using equivalent instructions at the hidden embedding of information into the executable files // Journal of Theoretical and Applied Information Technology. (ISSN19928645-Pakistan-Scopus) 2015. Т. 80. No. 1. Pp. 28–34.

4. Шариков П. И. Методика нахождение величины наиболее выгодного контейнера в форматах исполняемых файлов // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 58–62.

5. Sharikov, P. I., Krasov, A. V., Shterenberg, S. I. Method of creation and attachments digital watermark into an executable Java file by means of substitutions opcode // T-Comm. 2017. Vol. 11. No. 3. Pp. 66–70.

6. Шариков П. И., Красов А. В., Штеренберг С. И. Методика создания и вложения цифрового водяного знака в исполняемые java файлы на основе замен опкодов // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 3. С. 66–70.

7. Krasov, Andrey Vladimirovich, Arshinov, Aleksander Sergeevich and Ushakov, Igor Aleksandrovich. Embedding the hidden information into java byte code based on operands' interchanging // ARPN Journal of Engineering and Applied Sciences. April 2018. Vol. 13. No. 8.

8. Красов А. В., Штеренберг С. И. Разработка методов защиты от копирования ПО на основе цифровых водяных знаков внедряемых в исполняемые и библиотечные файлы // Актуальные проблемы инфотелекоммуникаций в науке и образовании. II Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2013. С. 847–852.

9. Шариков П. И., Красов А. В., Иванов А. В. Исследование возможностей методики скрытого вложения цифрового водяного знака в class-файлы на виртуализированных платформах с отличающейся архитектурой // Вестник СПб университета ГПС МЧС России. 2018. № 2. С. 79–88.

10. Красов А. В., Верещагин А. С., Цветков А. Ю. Аутентификация программного обеспечения при помощи вложения цифровых водяных знаков в исполняемый код // Телекоммуникации. 2013. № S7. С. 27–29.

11. Хомяков И. Н., Красов А. В. Возможность скрытого вложения информации в байт-код java // Информационные технологии моделирования и управления. 2014. № 2 (86). С. 185–191.

12. Коржик В. И., Небаева К. А., Герлинг Е. Ю., Догиль П. С., Федянин И. А. Цифровая стеганография и цифровые водяные знаки / Под общей редакцией профессора В. И. Коржика. СПб.: СПбГУТ. 2016. 226 с.

Статья представлена научным руководителем кандидатом технических наук, доцентом А. В. Красовым.

A N N O T A T I O N S

INFORMATION SYSTEMS AND TECHNOLOGIES

Nuraliev F., Giyosov U. Design of Virtual Reality for Education System. – PP. 5–14.
One of the main problems with virtual reality as a learning tool is that there are hardly any theories or models upon which to found and justify the application development. This paper presents a model that defends the metaphorical design of educational virtual reality systems. The results reached with the use of the developed software show the attributes that make the ideal Virtual Reality for situations of research and learning taking the discipline as a reference of the classroom to the computer labs and making more interesting to the student, making the learning easy. This paper reviews how virtual reality and augmented reality has been used in education, discusses the advantages and disadvantages of using these technologies in the classroom, and describes how virtual reality and augmented reality technologies can be used to enhance teaching at the Samarkand branch of the Tashkent university of information technologies named after Muhammad al-Khwarizmi.
Key words: virtual reality for education, visualization of knowledge; design of virtual reality systems, Smart classes, E-learning, sensors and interactive communication technology, 3D, Blender, VRML, virtual laboratory.

Avramenko V., Malikov A. Diagnosis of Security Infringements in Infocommunication Systems Based on a Combined Artificial Neural Network. – PP. 14–19.
Computer incidents detected in infocommunication systems must be diagnosed in order to obtain information to make an informed decision on the response.
Under the diagnosis refers to the process of determining the values of the characteristics of security violations, such as the type, purpose, sources, causes, results, etc.Given the large amount of heterogeneous diagnostic features used in the analysis stage, as well as high requirements for the efficiency and reliability of diagnosing computer incidents, it is proposed to use artificial neural networks as a base for building a model, in particular the Hopfield network and the perceptron.
Combined diagnostic neural network allows you to share the advantages of certain types of artificial neural networks and improve the efficiency of the diagnosis process. Due to the fact that the calculation of the values of the characteristics of security violations by the artificial neural network is carried out quickly enough, the proposed approach allows for rapid diagnosis of the characteristics of security violations with the required reliability of the result.
Key words: computer incident, security infringements of information, artificial neural networks, analysis, means of protection.

Avramenko V., Tarasov A. Forecasting Information Security in Authomated Systems Special Appointments. – PP. 19–24.
Protection of information in modern automated systems characterized by you with the inertia of measures to maintain or restore the required level of protection of information from unauthorized access and computer attacks. One of ways to solve the problem of inertia of the information security system in conditions of uncertainly threats is the implementation of the function of forecasting protection information security. This article presents a statistical model of missile defense forecasting indicators of information security.
Key words: the system of information protection, security threat, forecasting model, forecasting methods.

Agapov E., Ptitsyna L. Model-Analytical Intelligence Service High-Performance Computing Systems. – PP. 25–28.
The intellectualization of the task launch process in geographically distributed computing systems is updated. The reasons for the heterogeneity of high-performance computing systems and the heterogeneity of the tasks launched in geographically distributed systems are described. Innovative techniques for intellectualizing the process of launching tasks in geographically distributed computing systems are proposed. The content of innovative methods of intellectualization is disclosed.
Key words: intellectualization, computing system, launch tasks, monitoring system, neural network.

Akimov S., Verkhova G., Khoder H. Analysis and Formalizing the Problem of Structural-Parametric Synthesis of Bus-Modular Systems. – PP. 28–33.
The modular principle in design of modern systems is becoming more widespread due to the flexibility and the ability to quickly aggregate systems from standardized modules. In this regard, this paper presents an analysis of the problem of synthesis of bus-modular systems. It is also indicated that the automation of structural-parametric synthesis requires special multi-aspect models. The mathematical formulation of synthesis of bus-modular systems is considered.
Key words: bus-modular systems, complex systems, automation, structural-parametric synthesis, multi-aspect modeling, universal model, complex model.

Akimov S., Verkhova G. The Concept of Integrated Automation Management of Educational Programs. – PP. 33–36.
The concept of integrated automation of management of the educational program of a higher educational institution at all stages of the life cycle is presented. The system of automated management of the educational program is based on a multi-aspect model reflecting various aspects of the educational program. The multidimensional model ensures the consistency of all the resources and processes involved in the design and implementation of the educational program. The introduction of an integrated automation system for managing the educational program will significantly reduce the time spent on preparing and maintaining the current status of the accompanying documentation, minimizing human error.
Key words: multi-aspect model, educational program, work curriculum, work program, fund of evaluation tools, interactive educational and methodical complex, life cycle.

Akimov S., Verkhova G. Digital Twin Technology in Monitoring and Control. – PP. 36–41.
The concept of digital twins and their application in monitoring and managing complex technical systems are presented. The digital twin is a virtual image of an object, synchronized with the object being represented by means of physical quantity sensors and actuators. Digital counterparts take monitoring and control processes to a new level. The use of digital twins will enable the creation of a global cyber environment of monitoring and control, ensuring the integration of individual cyber-physical systems into a single system. The formation of such an environment is the primary task facing the post-industrial society.
Key words: digital twin, monitoring, management, multidimensional models, cyber environment, post-industrial society, information society.

Akimov S., Davletshina E., Popova M. Program Module for Automatic Generation of Documents for Graduate Qualification Works in MS Word Format. – PP. 42–46.
The report presents the development of a prototype of the module for automatic generation of documents for graduate works. Objective of the project is automatic generation of documents for graduate works in Microsoft Word format. The module is designed for the work within the system of complex automation of a higher educational institution, integration into the cyber environment of EJ-IK (Education Job International Keeper).
Key words: automatic generation, automation, report generation, C#, Office Open XML.

Almaev T., Lepeshkin O. Methods of Checking an Object-Oriented System in the Availability of Unauthorized Access. – PP. 46–51.
Today, the possibility of unauthorized access to data is one of the main problems of ensuring the security of information. To solve this problem, it is customary to analyze a computer system based on a discretionary security model. In this connection, there is a need to develop a methodology for checking object-oriented systems for the possibility of leakage of access rights.
Key words: object-oriented system, security model, unauthorized access, methods.

Andreev D., Vaganov A. To a Question of Application of Programmable Discrete and Analog Integrated Schemes in Modern Automated Control Systems. – PP. 52–57.
In article possibility of use of the field-programmable analog array (FPAA) in modern automated control systems is considered. Relevance of application of this class of chips is shown, and also comparison of their parameters with characteristics modern analog and digital by ERIE, the systems of processing of signals applied to construction is made. Recommendations to use of mathematical models for the description of similar systems are made.
Key words: integrated scheme, FPAA, analog signal, digital signal.

Antonov V. To the Question about Development of a Single Adaptive Education on-line Space. – PP. 58–61.
The issues of developing a software information system that implements distance education on the basis of a "single educational space" and "learning scenarios" are considered. The system adapts the learning process to the level of knowledge of a particular student.
Key words: educational space, learning scenarios, adaptive learning.

Achilova F., Kodirov F. Effective Software Tools for 3D Modeling. – PP. 61–65.
3D technologies are advanced technologies that fill modern human life. The basis of 3D technology is 3D modeling. Today it is difficult to imagine the work of a designer, designer, multiplier without the use of 3D models built using a computer. 3D modeling has become even more widespread due to the proliferation of 3D printers. Now 3D models are used in all branches of science, engineering, medicine, architecture and design.
Key words: 3d modeling, three-dimensional graphics, 3D-models.

Bayazitov E., Sysa E. Tolerance Interval for Regression with Heteroskedasticity Residues and Censored Observations. – PP. 65–71.
The article deals with the technique of point and interval estimation of distribution parameters on the example of samples obtained during mechanical fatigue tests. The samples obtained in such tests are characterized by the following features: heteroskedasticity of the regression model residues and the presence of censored observations. Taking into account the designated features of mechanical tests significantly improves the accuracy of determining the characteristics of durability. The characteristic of durability is used to justify the evaluation of the guaranteed resource, normalized by the lower confidence limit of the durability quantile.
Key words: fatigue test, endurance, tolerant intervals, differential evolution, method of maximum likelihood, censored sample, heteroscedasticity.

Bayazitov E., Dmitriev V., Timoshenko P., Portnov G. Study of Image Compression Methods. – PP. 71–77.
A digital image is a two-dimensional image represented in digital form. Depending on the description method, the image may be raster or vector. Images are very important documents today, to work with them in various applications requires image compression. Compression more or less depends on the purpose of the application. Image compression plays a very important role in the transmission and storage of image data as a result of limitations and storage. The main purpose of image compression should be to represent it in the least number of bits without losing important information on the contents of the original image. The aim of the work is to consider various methods of image compression. Based on the analysis of various image compression methods, the article presents a review of existing research. In this paper, we analyze various types of existing image compression methods.
Key words: image compression, DCT, DWT, OCR, run-length coding.

Belous K., Davydova E., Pilikina E., Shabanov A. Portable Streaming Player. – PP. 77–80.
A prototype of a portable streaming audio player based on the popular software hardware codec VS1053 is proposed. The player allows you to listen to streaming audio in mp3, aac, ogg formats. Control can be carried out using the IR remote control or buttons located on the front panel of the device. The player is equipped with a screen on which basic information is displayed – the name of the radio station, the song being played and the volume level.
Key words: streaming player, codecs, Internet radio, ES-32, portable.

Belotsvetov D., Kozin N., Lebedev D., Leschchuk M. An Algorithm for Nonlinear Filteration Based on the Baysevsk Approach to Solving the Task of Evaluation for Systems with a Discrete Time. – PP. 80–84.

In practice, nonlinear estimation algorithms are used, but mainly limited to the simplest options, such as the advanced Kalman filter. More powerful algorithms exist, but are rarely used, since they require large computational costs.

But the constant pace of development and increase in computing power of modern equipment stimulates the development of more powerful and high-precision algorithms.

Below is considered one of the variants of nonlinear filtering algorithms based on the Bayesian approach to solving the estimation problem for systems with discrete time. The main idea of the algorithm is to represent the a posteriori distribution density of the estimated state vector as an ensemble of weighted points, regularly distributed in a certain area of the phase space.

Key words: extended Kalman filter, nonlinear filtering, anscent filter, Gaussian distribution.

Belotsvetov D., Komashinsky V. Architecture and Functioning Algorithms of cognitive computing systems. – PP. 84–89.

Any intellectual system is designed to conduct certain activities that, taken together, make up its functionality. The central question that confronts the developer of a cognitive architecture is how to provide agents with access to various sources of knowledge. For example, environmental knowledge comes through sensation, knowledge of the consequences of the current situation comes through planning, reasoning and predictions, knowledge from other agents comes through communication, and knowledge from the past comes through memorization and training. The more such capabilities the architecture supports, the more knowledge sources it can access to inform about its behavior.

Another key question is whether the cognitive architecture supports any capability directly using built-in processes, or instead, it provides ways to realize this capability in terms of knowledge. Design decisions of this kind affect what the agent can learn from their own experience, what developers can optimize at the very beginning, and what functionality can be obtained from specialized concepts and mechanisms.

Key words: Architecture and algorithms, cognitive systems, computing systems.

Belyaev V., Komarov I., Laskus E. Information Security in Mobile Wireless Networks Using Active Data. – PP. 89–93.

The article discusses possible vulnerabilities and threats in mobile wireless networks built using active data technology, as well as the use of this technology in order to eliminate existing information security problems.

Key words: wireless networks, MANET, Active data, Information security.

Bovykin E., Hvostov M., Chebykin V. Development of the Analytic and Mobile Monitoring System for Android OS. – PP. 93–96.

This article presents the results of the development of the mobile monitoring and the technological process quality control system. The system takes advantage of the machine learning algorithms and positively differs from its analogs by avoiding their common limitations and disadvantages. The system can be used in the production organization in many industries.

Key words: android, Kotlin, machine learning, math modeling.

Botyakov V., Shestakov A. Monitoring Technologies Enterprise Communications Topologies Slopes of Lines. – PP. 97–102.
The questions of the existing order and the organization of the regulated account of fiber-optic communication lines are considered. With regard to the current objective conditions of the transition to the digital economy of the country developed organizational and organizational and technical proposals for the input, processing and maintenance in the current state of spatial data on communication lines, as well as their feasibility with a slight change in the currently involved resource and means of the enterprise.
Key words: communication operator, fixed assets, radio frequency label, radio frequency identification, spatial data, automation of spatiotemporal data accounting.

Bochkarev D., Vakalyuk A., Pantiuhin O. The Choice of Metric for Quality Control of Special Purpose Software Systems. – PP. 102–105.
Quality control of special purpose software systems is a complex process based on the selection of quality metric. A special feature of the development of special purpose software is the need for strict compliance with state standards in the field of software quality and in the development of special purpose systems.
Key words: software, quality control, state standard, software quality metric.

Buneev I., Lukyanchik V. Online Learning System Development. – PP. 105–110.
Online educational courses are gaining popularity among those who want to improve their skills or learn a new profession. The nascent industry of distance learning platforms allows you to get a quality education when it comes to introducing beginners to the profession, or to gain additional knowledge. The article discusses the process of developing a web system for the provision of services in the field of online learning, as well as the design of a web system using UML.
Key words: online training, design, UML, idef0, use case diagram, activity diagram, web development, web programming.

Burlov V., Lepeshkin M. Formalization of the System of Management Technosphere Safety in the Region. – PP. 110–116.
Management of social and economic systems, ensuring the technosphere security of the region uses models based on the analysis. The use of such models does not provide a guarantee of achieving the goal of forming processes with specified properties. The control model based on the synthesis and the law of preservation of object integrity allows to solve the inverse problem of management and to formulate conditions of application of program-target management.
Key words: *technosphere safety, management model, law of conservation of integrity of the object model* based on synthesis.

Vaganov A., Lebedev S. Alarm System at Hazardous Industries. – PP. 116–121.
The article discusses ways to create a warning system for the personnel of enterprises, which are based on dangerous technological processes, about the occurrence of an emergency situation. The urgency of the development of such systems for a wide range of productions is shown, the general concepts of their construction are considered. The structure of an intelligent adaptive alarm system (IASAS) has been developed, which implies an assessment of the degree of

threat to humans and adapts to changes in environmental conditions. Recommendations are given to the choice of the system structure, the choice of the element base, and also mathematical models for describing the individual elements of the system are given.
An algorithm has been deprotveloped that allows the IASAS to provide the required parameters for reliable detection of an emergency, reducing the likelihood of false alarms.
Key words: alarm system, security, production.

Vaganov A., Nazarov K. Elimination of Influence of interference on Electronic Parts, Blocks and Devices in Automated Control Systems. – PP. 121–127.
The article discusses the theory of electromagnetic compatibility of various devices of electronic equipment used in systems of automated control of enterprises. A review of the main sources and causes of electromagnetic interference in the circuits of preliminary and main signal processing was made. Analytical dependencies are given to evaluate the effect of various sources of interference on the primary signal processing path.
Practical recommendations for the design of primary and secondary power supply systems, analog and digital data transmission and processing channels are given. The options for the design of the devices and the placement of blocks in them are considered to minimize the effect of interference on the electronic systems of the automated control system.
Key words: electromagnetic compatibility, source of interference, impact assessment and interference minimization.

Vazhenin I., Ptitsyna L. Simulation of Quantum Cryptographic Processes. – PP. 128–133.
The system of initial assumptions that allow analytical modeling of the processes of functioning of quantum crypto protection is defined. The selected quality profiles of the functioning of quantum cryptographic protection. The description of the models of quantum crypto protection is given. The method of determining the quality indicators of the functioning of quantum crypto protection is disclosed.
Key words: quantum crypto protection, resources, model, quality profile, analysis.

Vanchakova N., Vitkova L., Kotenko I., Krasilnikova N., Strah L., Tishkov A., Chechulin A. Signs and Criteria of Personality Destructiveness and Destructive Impact Based on Internet Content and the Behavior of Subjects in Social Networks. – PP. 133–138.
Networking is the most important communication tool in the modern world. Many young people behave openly and even carelessly, especially students who only recently left their parental home. Often, young people leave enough content in social networks, through which it is possible to detect the emerging and trace the dynamics of the developing destructive elements of behavior. The most dangerous behavior in the network is extremism. This paper proposes a seven-step scale for assessing destructive behavior and its connection with ten signs of extremism in the network, based on Federal Law No. 114-FL "On Countering Extremist Activities".
Key words: destructive behavior, social networks, extremism.

Verkhova G., Kotelnikov M. Augmented Reality Marker Detectors. – PP. 139–144.
One of the most important functions in augmented reality technology is the detection of augmented reality marker. Such detection is performed on the key points of the augmented reality marker. The main detectors of augmented reality markers and the algorithms used in these

detectors are considered. The requirements for key points of augmented reality markers are given. Algorithms of Moravec, Harris and Stephen detectors, as well as FAST and SURF detectors are considered. The features of these detectors, their advantages and disadvantages are indicated.
Key words: augmented reality marker detector, augmented reality marker, augmented reality key point, key point detection algorithms, Moravec detector, Harris and Stefan detector, FAST detector, SURF detector.

Verkhova G., Makarenko E. Adaptive Systems. – PP. 144–148.
External disturbances can lead not only to changes in coordinates, but also to system parameters. Changes in the parameters that go beyond the prescribed limits may lead to errors, deterioration of the functioning or complete loss of system performance. This article discusses the concept of adaptive systems, the reasons for applying the principles of adaptation. Considered how the adaptation, as well as the shortcomings of the use of adaptive systems.
Key words: adaptive systems, adaptation problems, adaptation properties, implementation of adaptive control.

Viharev A., Markin D. The Method of Software Protection from Analysis Based on the Use of Byte-Code Interpreters. – PP. 148–153.
The article describes a software protection method from analysis based on the use of virtual machines with unknown architecture and byte-code alphabet. The algorithms of bytecode and virtual machine generation are presented. The work presents justification of virtual machine based obfuscation method effectiveness. The proposed protection method is described. It is to create conditions for forcing the program analysis using unknown command codes.
Key words: virtual machine, obfuscation, interpreter, bytecode, reverse engineering, disassembly, debugging.

Vlasenko M., Dmitriev V., Ivanov D., Mamadzhanova Sh., Khokhlacheva E. Protection of Information in Promising Radio Networks Based on a Time Stamp. – PP. 153–157.
Today, the problem of protecting information from unauthorized access is more urgent than ever. This is due to the huge constantly growing number of computer attacks on a daily basis, the increase in outbreaks of malware, the increase in the number of attacks sponsored by states, and the requirements for the highest level of security for military objects to keep information containing military secrets secret.
Key words: hashing, timestamp, program, interface.

Voloshenenko D., Komarova L., Litvinov V. Analysis of Methods of Modeling Business Processes in Problems of Assessment of Efficiency of Modernization of Information Infrastructure of the Enterprise. – PP. 157–162.
The article discusses the methods of modeling business processes in the problems of assessing the effectiveness of modernization of the information infrastructure of the enterprise. The analysis of existing methods of modeling business processes and methods of evaluating the effectiveness of information technology in business. The necessity of joint use of business process modeling methods and methods of evaluating the effectiveness of modernization of the information infrastructure of the enterprise is revealed and justified. On the basis of the study, the authors propose to identify a joint method for evaluating the effectiveness of the modeling of business processes as an auxiliary tool.

Key words: efficiency assessment, information infrastructure, functional and cost analysis, business process modeling methods.

Voloshinov D., Zaitseva A., Lysenko A., Sosnovskikh A. Methods for Building an Effective Topology of Game Characters Through the Retopology of High-Poly Models. – PP. 163–168.
Currently, there are many programs and tools for creating well-detailed three-dimensional objects using both the method of sculpting and photogrammetry. But in both cases, the result of the work is a very dense polygonal mesh with an almost chaotic topology. Such an object is not used for gaming purposes, since not every computer can cope with the animation of a huge number of polygons in real time, which will have different characteristics depending on the user who uses this product. The way out of this problem is to reduce the number of polygons and build a more efficient and correct topology of the 3D model using various tools for retopology.
Key words: polygonal mesh, 3D models, retopology.

Volynkin P., Kapurov N. Problems of Interaction of Ion Streams with a Solid Surface. – PP. 169–173.
In the manufacture of a number of products of nano and microelectronics there are increased requirements for the reproducibility of the surface geometry obtained by ion processing. In the bombardment of the surface generated by heavy ions have three main processes: erosion is the main ion flow, erosion reflected from the walls of the mask and the forming of the walls in the sample, as well as redeposition – deposition only that the pulverized material of the mask and the sample on the surface of the product. To find methods of automated control of the product forming process requires the development of a mathematical model of the process.
Key words: microelectronics, technology, ion etching, erosion, reflection, redeposition, mathematical model.

Volynkin P., Savinov A. Simulation of Erosion of Solid Surface During Ion Etching. – PP. 173–179.
In the microelectronic industry over the years, it becomes increasingly important to obtain an accurate profile of the solid surface.
A number of microelectronics products are manufactured using ion etching technology (ion-beam, ion-plasma). In the course of removal from the open part of the product material there are three main processes: surface erosion by the main ion flow, erosion by the ion flows reflected from the side walls of the mask and the formed surface, re - deposition-dusting of the newly removed mask material and the product material itself. When forming sufficiently thin elements of products, the influence of the relative error of the profile of the formed surface on the qualitative characteristics of the product (for example, on the frequency of the piezoelectric resonator with the inverse Mesa structure) significantly increases.
In this regard, there is a need to study the method of mathematical and computer modeling of these processes in order to find factors for the operational management of the formed profile.
Key words: microelectronics, technology, ion etching, erosion, reflection, redeposition, mathematical model.

Vostrukh A. Comparative Analysis of Methods for Evaluating Human-Machine Interfaces. – PP. 179–185.
Constantly growing information needs of the modern user of various systems not always find reflection in the existing program environment. The interface as the intermediary between a system and the person, now mostly is at the level of art and an intuition that leads to negative effects, beginning from personal discomfort of the user and finishing with severe accidents and accidents. Today the question is particularly acute: "By means of what and how it is possible to measure compliance of an information system to needs of users more effectively?" In work the relevance of the matter is shown, described parameters of assessment of compliance of interfaces of the human-oriented approaches, carried out contrastive analysis of the existing valuation methods of the interfaces considering these parameters.
Key words: human-machine interfaces, information demand, information opportunities, efficiency evaluation.

Vyshlov O., Dovgiy S. About Preparation and use of Resources of the Unified Telecommunication Network of Russia for Ensuring Functioning of the Protected Objects of Critical Information Infrastructure. – PP. 185–190.
Threats in the area of information security, including the use of information and telecommunication technologies for the application of economic and other loss, including through the provision of the destructive effects on the objects of critical information infrastructure, necessitate a scientific approach to the normative-technical regulation of activities in the field of protection of the information contained in critical processes.
Key words: critical information infrastructure, critical process, regulatory and technical regulation, information security.

Gatchin Yu., Korobeynikov A., Menshchikov A. Detecting Web-Crawler Based on the Analysis of the Graph of Visits. – PP. 190–194.
Modern research suggests that robotic traffic on web resources in terms of volume and intensity prevails over the user. Web-crawler threaten data privacy, copyright, and affect performance, security, and distort visitor statistics. There was a need to detect and counter such means. Existing methods involve the use of syntactic and analytical processing of web server logs to detect web-crawler. In this article we propose to analyze the graph of visits to web-crawler, taking into account the time, subject, and the connectivity of the visited pages. The analysis of performance, accuracy and completeness of detection, as well as comparison with the results of existing approaches.
Key words: web-crawler, the graph of visits, parsing, crawling, countering parsing, collection of information, information security, web resource protection.

Gatchin Yu., Yumasheva E. Practical Features of Building Centers for the State Service on the Basis of Regulatory Requirements. – PP. 195–200.
The article discusses the stages of development of the regulatory framework governing the security of the critical information infrastructure. And also some practical features of the construction of the State Department for the Development of State Service for the Administration of State Administration for the Development of Important Information and Important Objects of Critical Information Infrastructure are considered.

Key words: critical information infrastructure, state system for detection and prevention of computer attacks, security of objects.

Graschenko L., Revyakin A., Scurnovich A. The System of Recognizing of the Compressed Stationary Graphical Message (SGM) in JPEG Format, Containing the Text Documents. – PP. 201–206.

The article describes the system of recognition of graphic messages in JPEG format for the presence of electronic copies of text documents in the image. The proposed solution is based on the principle of majority decision-making based on the results of three two-class classifiers. The working dictionary of features is formed by a full search of 10 normalized statistical indicators reflecting the frequency features of the image. The results of preliminary tests show that the proposed recognition system operates with a precision of 0.98 and a recall of 0.95.

Key words: stationary compressed graphical message of the JPEG format, text content, frequency region picture messages.

Grigorenko K., Kozlova L. Interface Design Methods for Educational Platform Based On UX and UI Design. – PP. 207–210.

In case of human interaction, user interface is the key point of communication between the user and computer software. The result of this interaction depends on the design of the user interface, especially essential in the development of educational software. The principles and concepts of interface design should be considered in conjunction with the design of user experience.

Key words: user interface, user experience, user interface design, educational platform interface.

Gruzdeva L. Comparative Analysis of Existing Methods of Approximation in the Study of Light Scattering in a Heterogeneous Medium. – PP. 211–216.

The application of approximation methods for solving the transport equation for media with different anisotropy parameters is considered. Strict methods for solving the transport equation. A less accurate method, Monte-Carlo. Single scattering approximation. Double scattering approximation. The diffuse approximation for the cases of isotropic media. Small-angle approximation for homogeneous media. Propagation of a short bounded pulse in an inhomogeneous medium (small-angle approximation).

Key word: transport equation, single scattering, the double scattering, the diffuse approximation.

Grushevaya E., Makeev S. Design the Layout and Methods of Configuring the Intelligent Module Big Data Processing on the Basis of Free Software. – PP. 216–220.

The paper considers the result of the work on the development of the layout and methods of configuration of the module of intellectual processing of big data on the basis of free software. A block diagram of the layout is presented, as well as a sequence of actions to configure the module for intelligent processing of big data, which allows to reduce the number of errors in the configuration.

Key words: big data, Apache Spark, Apache Hadoop cluster, configuration technique.

Gubin A., Litvinov V., Filippov F. Measuring the Kolmogorov complexity of binary strings on the basis of autoencoders. – PP. 221–224.
Autoencoder are popular learning models because they are conceptually simple, easy to learn and provide efficient code. This paper shows how you can get a meaningful estimate of some set of data in the form of binary strings, which measures how well an autoencoder can represent this data.
Key words: autoencoder, Kolmogorov complexity, neural networks, learning models.

Gubin A., Litvinov V., Filippov F. Information Aspects of Digital Smoothing of Random Signals. – PP. 224–228.
The possibilities of informational evaluation of the processes of smoothing of random signals by digital filters using the concept of entropy potential are considered. The value of the entropy potential is defined as half the range of the uniform distribution, having the same entropy as the distribution law of the observed parameter.
Key words: digital smoothing of signals, entropy, entropy potential.

Gubin A., Litvinov V., Filippov F. The Study of Ontology Control Methods Information and Communication Structures. – PP. 228–232.
The concept of semantic markup for the formalization of information resources leads to the possibility of structural universalization of the control model. Specification of any information structure is possible on the basis of ontology of the relevant subject area. The fundamental scientific objective is to develop universal methods of control of information and communication structures obtained with the use of formalized procedures for structuring information resources specified by the ontology.
Key words: ontology, information and communication structures, fault-tolerant system.

Guryeva T., Sharabaeva L. Tasks of Management of Information-Technological Architecture in Higher Education Institution. – PP. 232–237.
The article is devoted to architectural approach of management of information-technological infrastructure in higher education institution for achievement of strategic objectives. The main area of improvement in this sphere consists of such problems as sharing of the general data, an exception of business functions duplication, coordination management, monitoring of users activity and providing of information security due to improvements in management of a complex of applied systems.
Key words: Enterprise Architecture, information and technological infrastructure, IT- management, SLA, BISL, COBIT, ITIL.

Danilova E., Kribel A., Rakitsky S., Rakitsky D. Approach to the Protection Channel Management Robotic Systems. – PP. 237–244.
To date, research in the field of robotics is very relevant. Robotic systems can significantly increase productivity without making mistakes due to the "human" factor. Such complexes are referred to cyberphysical systems. An integral part of cyberphysical systems is the control system. This system, like any information channel, must be protected from computer attacks to avoid interception of cyber-physical systems by attackers. In the article the developed robotic system and a system that allows to manage this complex and robust cryptographically secure

connection. The main element of this system is a cryptographic chip stm32f415. It allows you to reduce the load on the CPU to perform control algorithms, freeing it from cryptographic operations, thereby ensuring a gain in time.
Key words: control channel, cyberphysical systems, robotic systems, cryptographic algorithms.

Demidov A., Denisov E., Nikishina T. Automated System for the Time-Domain Impedance Spectroscopy Excitation Signal Generation. – PP. 244–249.
The wide distribution of lithium batteries and other electrochemical energy sources leads to the emergence of the need to develop new diagnostic methods that provide sufficient accuracy and speed at low cost. Electrochemical impedance spectroscopy in the time domain has good prospects here. This method allows to use the energy of an electrochemical energy source to generate an input signal, which, in turn, reduces the complexity, weight, size and cost of measuring equipment. The proposed system consists of two main parts: 1) control circuit of operating modes and 2) controlled load. The system also allows to generate any input signal. The control circuit of operating modes uses information about the current voltage and current of the electrochemical energy source under study. The system uses a PID controller, in whose memory a set of coefficients is entered, which are selected depending on the current voltage of the electrochemical source.
Key words: electrochemical energy sources, lithium batteries, electrochemical impedance spectroscopy.

Dovjik A., Ivanov V., Kobelev A., Lavrov A. The Challenge of Organization of Operative-Technical Services in Communication Centers. – PP. 249–254.
The article discusses the automation concept of processes of operational and technical service on the example of creating a hardware-software complex of the organization of documents formation on communication nodes. The purpose, structure, capabilities and operating principle of the complex are considered.
Key words: electronic documentation, ECM systems, operative-technical data, client and server application, Web server.

Doynikova E., Parashchuk I. Requirements to Processes and Components of Elimination of Uncertainty of the Analysis of Semantic Filling of Information Objects for the Benefit of Detection and Counteraction of Harmful Information. – PP. 254–259.
The paper offers an approach to the wording of basic requirements to components of elimination of uncertainty of assessment and categorization of semantic filling of the information objects making the content of the services provided by the Internet. The approach takes into account results of the analysis of modern requirements to processes and elements of control systems of digital network content. This approach is implemented considering the fact that elimination of uncertainty of assessment and categorization of semantic filling of information objects will be carried out with use of methods of processing of incomplete, contradictory and indistinct knowledge. Implementation of these requirements will allow intelligent scanners (qualifiers) quickly, authentically and adequately to reveal signs and to counteract harmful (undesirable, doubtful) information in digital network content.
Key words: requirements, uncertainty, content, information object, component, harmful information, semantic filling, assessment.

Dolgun V., Kazakov D., Russia V., Schvidkiy A. Methods and Means for Ensuring Information Security of 1C Databases: Enterprises. – PP. 259–263.
Currently, modern 1C systems have drawbacks related to the problems of ensuring the integrity, confidentiality and security of financial documents. It is proposed to consider the most common case of using the 1C system. The 1C system consists of an application server, a SQL database server and user workstations. It is necessary to develop a methodology that ensures the protection of data stored and processed in 1C systems.
Key words: Data protection, 1C:Enterprise, SQL, databases, integrity.

Dolgun V., Ptitsyna L. Architecture of Distributed Intelligent Management Systems of a Smart House. – PP. 264–268.
Updated development of smart home control systems. A systematic presentation of knowledge about smart home control systems. The advantages of distributed intelligent smart home control systems are described. The problems of distributed systems are considered. The basis of architectures of smart home control systems has been formed. The features of building smart home control systems are described.
Key words: smart home, intelligent systems, methods.

Dyubov A., Kovalenko A. The Current State and Prospects of Development of Optical Access Networks. – PP. 268–272.
Recently, optical access networks are the most dynamically developing segment of the telecommunications market. One of the characteristic signs of the continuous development of the access network market is from year to year improved data transmission and networking technologies designed to meet the growing needs of users. If on transport networks (trunk lines), the transition to an optical fiber is in full swing, then on optical access networks, the transition to an optical fiber is getting closer and closer to the end user.
Key words: PON, FTTx, Active Ethernet, Micro SDH, network development prospects.

Efimov K., Shiyan A. Impact of Voice Requests on Seo. – PP. 273–277.
The Internet is becoming the most popular platform for the development of business projects. In order to earn an audience, or to expand the client base, site owners resort to various methods of seo promotion. One of these ways is to optimize the site for voice search, which is gaining great popularity recently.
Key words: search query, voice search, seo, website optimization, internet promotion, voice search.

Zharanova A., Kotlova M. Formation of the Model for the Knowledge Monitoring and Assessment System for Students. – PP. 277–282.
Justification of relevance for the automated system introduction into the modern education process. The analysis was conducted on modern approaches to education process and knowledge monitoring. Identification of the main disadvantages of the existing systems for assessing the quality of students' knowledge. Forms and methods of the implementation of knowledge monitoring and assessment. The proposed model for the knowledge monitoring and assessment system based on the adaptive method. Description of the main elements of the model. Identification of prospects for the development of the knowledge monitoring and assessment systems.

Key words: knowledge monitoring, knowledge assessment, adaptive method, model of the system, education, education process, testing.

Zholobova K., Shestakov A. Automation of Patent Research at Communication Enterprises in the Digital Economy. – PP. 283–288.
The ways to reduce costs and improve the quality of reports on patent research in the communications industry due to the technology of electronic forms of documents as part of the original design documentation in the digital economy. The interface environment of forms of reporting documents, information from which is the information basis for decision-making on the life cycle of industrial property, products and their components, is proposed. The use of original software allows to ensure the completeness of information of legal significance, for example, for the maintenance of patent forms on the objects of technology.
Key words: the report on patent research, patent form, the technology of electronic forms of documents.

Zverev A., Markin D. Adaptive Web Application Fuzzing Based on Web Resource Model. – PP. 288–293.
The work contains description of web application fuzzing method based on web resource model and web-proxy server network. The web-proxy server network allows to execute fuzzing using active data technology. Structure and functional model are described, database logical scheme is showed. The works` aim is to improve web application fuzzing tools effectiveness for finding vulnerabilities.
Key words: fuzzing, web application, active data, fuzzier, web resource model, web-proxy server.

Zvyagincev S., Markin D., Pavlov D. Methods and Tools Used for Software Analysis. – PP. 293–298.
The work contains description of methods and tools used for software analysis. The authors present the methodology of reverse engineering used for software analysis and tools for it. The work contains classification of Methods and tools used for software analysis. The automated software analysis methods classification is described.
Key words: reverse engineering, static analysis, dynamic analysis, dynamic binary instrumentation, fuzzing, debugger, emulator.

Zolotov O., Yakubov N. Problems of Creation of Practical Systems of Stabilization of Structures. – PP. 298–302.
In the works of Professor Pustylnikov L. M. and his co-authors proved the theoretical possibility of using feedback to stabilize the structures of objects of any nature. The practical solution of such problems is faced with a number of serious problems, which are considered in this work. Bringing this problem to the classical scheme of using feedback requires:
1. The possibility of "measuring" the structure, i. e. its identification;
2. Opportunities to influence the structure to its changes (an analogue of the controllability);
3. The presence of the standard structure, the possibility of comparing structures and much more.

In addition, it is necessary to determine the range of structures that can be considered for these purposes.
Key words: structure, management, preservation, feedback.

Ivanov S., Iglov M. Using the Methods of Multi Criteria Analysis of Aramis and Electro to Search for an Optimal Solution of AI. – PP. 303–308.
The article is devoted to the analysis of the use of multi-criteria analysis methods for AI. An example of the algorithm of action and analysis of AI for obtaining the result is given. The basic needs for AI in a computer game are highlighted, and on their basis a final ranked table of the list of AI actions and reactions for certain events is built.
Key words: AI, multicriteria selection methods, self-learning algorithms.

Ievlev I., Musaeva T. Automate the Preparation of the Test Environment. – PP. 308–313.
The article deals with the task of optimizing the process of developing and testing software by reducing the complexity and time spent on preparing a test environment. The experience of the development and implementation of a software component to automate the process of preparing test benches of the billing system of a cellular operator is considered. A developed method of automating the process of preparing a test environment based on full automation and ease of scaling is proposed.
Key words: billing system, test environment, automation, testing.

Ilina O., Kupchinenko O., Skoropad A. To the Question of Network Security and Filtration of Packages. – PP. 313–318.
Iptables in the Linux operating system is a set of instruments for building effective firewalls. It is based on filtering packets passing through a connection, and according to a set of rules determines a particular firewall reaction to these packets. The ability to block incoming traffic initiated from the outside, together with the functions of network address translation, allows users to freely access the Internet and reliably protect them from influence of outside.
Key words: operating system, information security, firewall, chain, rule, port, filtration of packages, traffic.

Ilina O., Kupchinenko O., Skoropad A. About Additional Goals of Administrated Sets of Protection Information in Operating Systems of Special Purpose. – PP. 318–323.
Automated systems which realized with using operating systems of a special purpose, can use additional functions of administering operating systems. It allows you to build a more flexible and reliable system for protecting information from unauthorized access. AFICK system has a huge popularity for controlling of file integrity. «Kiosk» mode is used for additional restriction of user rights.
Key words: automated system, operating system of a special purpose, information security, unauthorized access, integrity control.

Isupova E. Procedures for Building a System for Monitoring Information Security Against Leakage Through Technical Channels of a Communication Facility. – PP. 323–328.
The procedures for building an information protection system and a system for monitoring information security against leakage through technical channels in relation to various objects of

information and telecommunications infrastructure are considered. The procedures for classifying an object and determining the level of protection, channels of possible information leaks are specified. The results of studies of the methodological apparatus used to control security are given. The existing approaches and technologies to the implementation of the functional elements of the information security control system against leakage through technical channels are analyzed. Offered rational typical options for building a system for monitoring information security against leakage through technical channels.
Key words: information protection system, information security control, technical channel leakage, object classification, level of protection, methodological apparatus.

Karachinskaya E., Margaritova J, Ptitsyna L. Web Service Development on a Technology Platform. – PP. 329–333.
Presented objective grounds for the development of service-oriented systems. The reasons for increasing the scale of demand and the use of Web services are considered. A technology platform has been selected for developing Web services. The basic mechanisms for organizing Web services on a technology platform are defined. A Web services programming interface described in the WSDL format is described. Shows the logical parts of the document in WSDL format. The basic rules for the formation of an XML file are disclosed. Descriptions of the main features of using XDTO-serialization.
Key words: service oriented system, technology platform, format WSDL, XML file, XDTO serialization.

Karachinskaya E., Margaritova J, Ptitsyna L. Extending Enterprise Web-services. – PP. 333–338.
The development of professional activities in the information infrastructure environment has been updated. The feasibility of the development of professional activities through the expansion of corporate Web-services. Considered the basis for the choice of technology platform for the development of Web-services. Presents the main components of the process of building Web-services on the selected technology platform. Revealed the key features of the implementation of Web-services for the organization of information exchange between the client-server application and the client.
Key words: corporate information system, service oriented architecture, service, protocol.

Knyazev R., Kozlova L., Mursalimova K. Analysis of the Assessment of the Level of Knowledge of the Entrancers with the Application of the Neural Network. – PP. 338–341.
With the annual increase in the number of applicants, it becomes necessary to create an automated system for analyzing and evaluating the level of knowledge of applicants. This task is laborious, which is not possible to solve with the help of traditional mathematical apparatus. The article discusses the possibility of developing a system using neural networks.
Key words: neural network, education, evaluation, analysis.

Knyazev R., Kozlova L., Mursalimova K. Application of Analytical Applications on Different Platforms. – PP. 342–345.
In the information age, the processing and analysis of data is becoming increasingly important. For the implementation of operational and strategic decisions of the company uses data analytics, which helps to obtain meaningful information from the data and transform knowledge into action. The article discusses solutions used on different platforms.
Key words: data analysis, data processing, multiplatform, analytical applications.

Kovalchuk V., Kotlova M. Chat-Bots as Information System Interface. – PP. 346–349.
Considered the main role of social networks in human life. Identified a set of services integrated into a social network that can form user interaction with a third-party information system. The chatbots technology is described, the scope of the technology in question is defined. The classification of chat bots is given, the advantages and disadvantages of operating the technology are considered. The possibilities of the proposed solution in social networks and instant messengers are defined. The use of chatbot technology was suggested using the example of the Vkontakte social network as an information system interface. The prospects for the development of chatbots technology are presented.
Key words: social networks, messengers, automated system, python, chat bots, application programming interface, programming.

Kozachok A., Spirin A. About Some Statistical Properties of Compression and Encryption Algorithms. – PP. 350–353.
The paper considers the possibility of using the method of testing the properties of bit sequences as one of the possible approaches to solving the problem of differentiation of compression and encryption algorithms the results of the analysis made it possible to draw a conclusion about the applicability of the considered method for the identification of zip, rar, 7-z compression algorithms and AES, triple DES encryption algorithms and the possibility of their distinction with an accuracy of more than 0.99.
Key words: algorithms of compression and encryption identification, statistical information testing.

Komarova A., Korobeynikov A. Analysis of the Existing Affairs in Post-Quantum Cryptography. – PP. 353–358.
In today's fast-growing technological world, the emergence of a quantum computer is increasingly becoming a reality. The emergence of such a device will allow to process data an order of magnitude faster than modern machines do. For some areas of knowledge this will be a breakthrough, but for modern cryptography – the threat of hacking into all existing cryptosystems. This article provides a brief analysis of the current state of affairs in post-quantum cryptography.
Key words: quantum computer, post-quantum cryptography, elliptic curve isogeny, algebraic coding theory, lattice theory, elliptic curve, McEliec cryptosystem, Niederreiter cryptosystem, Shortest Vector Problem, NP-complete problem, quantum hash function.

Korobeynikov A., Polegenko A. IoT Standardization Issues. – PP. 359–362.
Today we are surrounded by an increasing number of smart gadgets that can communicate to each other with the user or without him. The information security issues require consideration of new aspects because of the specificity of the devices, as well as their limited capability and different nature. A key role in the development of technologies for smart gadgets communication is the implementation of common standards in this area.
Key words: internet of things, information security, smart gadgets, network communication, standardization.

Kotkina M., Ptitsyna L. Formation of Extended Object-Oriented Models of Action Planners of Information Multi-Agent Systems. – PP. 362–367.
The architectural features of informational multi-agent systems are described. The relevance of a comparative analysis of action planners of information multi-agent systems is grounded. Presents the current state of research planners. The task is to expand knowledge of the dynamic properties of planners. A method for the formation of extended object-oriented models of action planners information multi-agent systems. The scope of use of the generated models is determined.
Key words: architecture, multi-agent system, action planner, dynamic properties, object-oriented models.

Krivko D., Svechnikov D., Stepina O. Diagnostics of Information Resources Security of the Government Web Portals. – PP. 368–372.
The article describes the diagnostics methods of state information systems web portals information resources security. The work contains description of vulnerability identifying methods implementation based on black and white boxes models.
Key words: information system, information resource, web portal, security diagnostics.

Kubasov I., Mamonchikova A. Model of Information Security System from Unauthorized Influences and Algorithms of their Detection. – PP. 372–375.
Prerequisites for modeling of information security system in the automated control system for communication are considered. All directions of correction of the information security purposes on a set of the competing structures are presented. The functioning algorithm of information security system of ACS communication increasing its stability in the conditions of unauthorized influences is shown.
Key words: automated control system for communication, unauthorized influences, information security system, information flows, correction of model parameters, detection algorithms.

Kuzkin A., Kutsakin M., Lapko A., Lebedenko E., Ryabokon V. To the Question of the Use of Intellectual Agents to Ensure the Information Security of the Corporate Information System. – PP. 376–381.
The article presents the main directions and developments in ensuring information security of corporate computing systems using intelligent technologies. The question of ensuring the information security of a corporate information system with cloud computing is covered. A security model for an information system using multi-agent technology is proposed. Analyzed the main

problems of information security of corporate systems, presented directions for the implementation of user authentication mechanisms.
Key words: intellectual technologies, information security, authentication mechanisms, cloud computing, multi-agent approach.

Kuzkin A., Kutsakin M., Ryabokon V. Information Security Methods for IoT-Based Devices. – PP. 381–386.
This paper presents an example of cloud architecture with integrated information security methods. It is based on the client-server model with separation of physical and virtual instances of IoT-based devices, proposing the application of virtualised sensor nodes for increasing data protection. It concerns all security vectors: from secure association, authentication and authorization to privacy and data integrity and protection. Securing the virtual instances is easier to implement, manage and audit and the only problem is the physical interaction between real sensor and its virtual instance.
Key words: IoT, information security, virtual objects.

Kurnosov V., Shestakov A. To the Application of Resource-Saving Methods of Improving the Operational Reliability of the Complexes of Hardware and Software. – PP. 386–391.
The ways of improving the operational reliability of hardware and software systems due to resource-saving methods of operation in relation to modern systems, networks and telecommunications devices for various purposes are considered. The technique of construction of such complexes is offered. The main procedures of the proposed methodical apparatus in the form of private techniques and models used are presented. The use of the original approach allows us to justify the structure of the complexes of minimum redundancy with the provision of rational resource consumption during operation in various conditions and communication tasks.
Key words: methods, reliability, resource saving, software and hardware complexes, telecommunications.

Kurnosov V., Shestakov A. A Rational Approach to the Development of Telecommunications Infrastructure Based on the Methods of Structural and Parametric Similarity. – PP. 391–396.
An approach to the development of the existing telecommunications infrastructure through the methods of structural-parametric similarity of the original fragment based on the provisions of the methodology of the telecommunications genotype is considered. The main procedures of formation of perspective (final) infrastructure for its subsequent step-by-step transformation into the initial fragment, which has a given degree of similarity, justified with the use of graph model and sparsification procedures, are presented. The use of the original approach allows us to justify the structure of the initial fragment of minimal redundancy with the provision of rational consumption of resources for its creation and gradual development in various conditions and communication tasks.
Key words: network graph, samples, structural and parametric similarity, the design of communication networks.

Lapko A. The Structural Indicators Building Method in the Task of Ethnic Conflict Early Warning. – PP. 397–402.
The article is devoted to the building the set of structural indicators used along with behavioral indicators in solving the problem of ethnic conflict early warning. The social-economic and political parameters used in the building of the structural indicators system are presented. Described in detail the structural indicators building method based on inductive inference.
Key words: ethnic tension, ethnic conflict early warning, structural indicators, inductive inference.

Lavrinovich A. Features of RFID-Marking as a Means of Identification for Shoe Goods. – PP. 403–407.
Shoe products of commodity items 6401–6405 of FEACN UUE are subject to mandatory labeling with identification tools from 01.07.2019 in the Russian Federation. In this article based on the results of the project on RFID-marking of fur products, the potential features of RFID marking as a means of identifying shoe products are highlighted. Based on this, author identified information security threats for the RFID-labeling system for shoe products.
Key words: product labeling, RFID-technology, information security, RFID-labeling, RFID, product marking, RFID-tag, identification tools, counterfeit products, foreign trade.

Lipatnikov V., Sazonov A., Shevchenko A. Method of Functional Testing of Electronic Digital Devices and Detection of Undocumented Features. – PP. 408–413.
This article describes an approach of solving recognition tasks of undocumented features in integrated circuits of electronic devices based on theory of formal languages and grammars and structural linguistic analysis methods. The article deals with questions of functional testing of electronic devices, the choice of the optimal formal grammar to create a linguistic description of the investigated undocumented features, as well as the structure of the developed method of recognition.
Key words: formal grammars, recognition methods, production model, algorithm, method.

Lipatnikov V., Tortochakov S., Tikhonov V. Types of Crossovers are for Finding the Optimal Routes of Delivery of Messages of Nerworks with Genetic Algorithm on the Model of Whitley. – PP. 413–420.
The actual problem of ensuring the level of cyber security security of critical infrastructures of automated control systems and special-purpose communications is considered. The problem of determining the factors affecting the level of cybersecurity is solved by creating a model of the proactive control process using the cognitive modeling module. The aim is to increase the level of cyber security of critical infrastructures of automated control systems and communications for special purposes. The article presents the structure of the proactive cybersecurity management process model that implements the identification and assessment of vulnerabilities along with risk prediction.
Key words: cyber security, information security, risk assessment, security indicator, proactive management, critical infrastructures, automated control systems.

Lipatnikov V., Shevchenko A. Method of rising rigidity of control-measurement radiomonitoring system to external and internal actions. – PP. 420–425.
In this article exposed method of rising rigidity of control-measurement radiomonitoring system to external and internal actions, by monitoring of information sensibilities and technical system state. Investigation of available method shows rising of system working probability and, as a result, rising radiocontrol results authenticity.
Key words: control-measurement radiomonitoring system, information security, stable operation index, stochastic network, Laplace-Stieltjes transform.

Litvinov V., Taymazova Z. Researches of Virtualization Methods and Comparative Characteristics of Hypervisors. – PP. 426–429.
The concept of virtualization is characterized and the advantages and disadvantages of this technology are analyzed. We consider the general principles of working with virtual servers. The main functions of hypervisors are described. A comparison of the main types of hypervisors is carried out and a comparative table of their characteristics is given.
Key words: virtualization, hypervisors, VMware, performance, virtual machines.

Litvinov V., Fadeeva A. Research Methods for the Analysis of the IT-Infrastructure of the Company. – PP. 429–433.
Estimates and prospects of development of the world and Russian markets of information technologies are analyzed. The main directions of development of IT-infrastructure of the companies are described. Solutions for IT-company interaction with customers have been formed. The ideas for high-quality and profitable implementation of IT-infrastructure of the company in order to improve the level of customer service.
Key words: information technology, IT-infrastructure, customer relationship management.

Makarov P., Ivanov S. Modeling and Visualization of an Operational Environment. – PP. 434–437.
Modeling of an operational situation is demanded when using the interactive system for the visualization of an operational environment. This complex allows you to simulate different variants of combat operations with the redistribution of goals for units; to solve a number of situational problems, including such for the enemy. It allows you to plan the deployment of groups of troops, based on the results of dynamic tasks.
Key words: operational environment, simulation, combat.

Mamonchikova A., Polikanov V. Topical Issues of the Automated Documents Development (Processing) in the General Process of Communication Planning. – PP. 437–442.
The entity and the maintenance of planning problems by the departmental communication services is considered. The relevance of a question of planning process improvement ways by creation of the system of the automated development of communication documents is proved. Requirements to the considered system on the basis of management system features and the made communication planning decisions are formulated.
Key words: communication planning, process automation, the system of the automated development of communication documents.

Mamonchikova A., Filichkin I. To the Question of Information Destruction Methods Research on Objects of Automation Telecommunication Systems. – PP. 443–447.
The leak problem of the residual information arising owing to its insufficiently reliable removal about hard disk drives is considered. Solutions of the private engineering tasks directed to development of a constructive algorithm and technique of safe information destruction from non-volatile carriers on objects of telecommunication systems automation are offered.
Key words: the automated information systems, unauthorized access to information, non-volatile data carriers, confidential information destruction.

Markin D., Sannikov I. The Method of Detecting Vulnerabilities in Cisco System Software. – PP. 448–453.
The paper describes a method of detecting vulnerabilities in Cisco system software. The procedure for disassembly system software based on the processors architecture is described. The method of critical procedures such as authentication and authorization is presented. The work contains detailed description of presented method of detecting vulnerabilities in Cisco system software and description of the software environment model used for analyzing.
Key words: Cisco, vulnerability search, reverse engineering, disassembly, debugging, system software.

Medvedev V. Probabilistic Characteristics of Binary Sequence. Summary. – PP. 453–457.
Summarizes study of binary sequence as models of various its implementations in which the value can be one of two possible values. Described in a direct way of determining the probability of importances of binary counts sequence (P) probabilities based on probabilities reams of zeros and ones (G -probabilities). Shown way back-the definition of probability reams of zeros and ones based on the probabilities of independent samples of one or several positions of the binary sequence. Shows the formula ratio.
Key words: the binary sequence, model, probability, probabilistic positioning, (P)-probability (G)-probability.

Meleshko A., Savkov S. Threat Model and Risk Assessment Methodology for a Water Supply Management System. – PP. 458–463.
The paper presents a threat model for the cyberphysical water supply management system. The main risk events for the class of water supply management objects and their interrelations are allocated. Based on the model, a comprehensive risk assessment methodology was developed. The complexity of the methodology consists in the assessment of risk events not only on the basis of expert knowledge, but also using information obtained from the object's sensors. The developed threat model and methodology are designed to improve the quality of risk assessment, which allows increasing the overall security level of an object.
Key words: threat model, risk assessment, cyber-physical system, water supply management system.

Mikhailichenko N., Parashchuk I., Chernyavsky A. Option of Classification of Electronic Libraries for the Benefit of Automation of Management of Their Information Resources. – PP. 463–468.
Electronic libraries gain the increasing popularity thanks to the fact that they work in a wide range of directory services, provide access to the large volume of information resources and their expansion does not demand considerable expenses of time and means. In article methodological approach to search and justification of classification signs of electronic libraries for the benefit of automation of management of their information resources is considered. Reasonable classification of such complex automated directory systems as electronic libraries, gives freedom of the reliable choice to their designer and an opportunity for economy to various categories of users of electronic libraries.
Key words: electronic library, information resources, classification, data.

Mihin A., Komisarov S. Basic Concepts of Source Code Refactoring. – PP. 469–471.
The article justifies the application of refactoring in the software development. The paper considers code flaws that signal of the need to refactor. The main advantages of code refactoring as a means of improving its compositional structure and increasing its readability are considered.
Key words: software architecture, source code refactoring, optimization.

Moskvichev I., Sysa E. Comparison and Analysis of Software Products that Allow to Realize Interactive 3D-Applications. – PP. 472–475.
The article provides an overview of the most common game engines for developing 3D applications. The most important functions and capabilities of engines, such as: supported programming languages, the ability to interact with other software, as well as the cost of using software products, are considered. For analysis, a comparative table for the ratio of game engines is given.
Key words: shading, crossplatform.

Napalkova F., Shestakov A. Single-Page Web Applications of Automated Communication Enterprises. – PP. 475–481.
The issues of development of landing pages and quizzes as single-page WEB-applications, business processes of marketing and product offer management, customer relations, knowledge of the organization and research of the communication enterprise that meet the requirements of GOST R 53633.0 are covered. The quality model is considered when using software according to GOST R ISO / IEC 25010 in relation to single-page WEB-applications from the user's point of view. The set of metrics on which quantitative values should be obtained in the course of functional testing of landing pages and quizzes is specified.
Key words: the landing pages and quizzes, *model is considered when using software*

Nikulin D., Komisarov S. Creating an Automated Workplace Office of the MINISTRY of Justice on Republic of Khakasia. – PP. 481–485.
The given work represents the all process description of creation of an information subsystem «The Register of the Lawyers», which serves for editing information about the lawyers and

formation of the reports on their basis. The product is developed for the employees of a department of Management of a Minjust on Khakasia Republic.
Key words: table, report, applications development, software, information system, The Register of the Lawyers, Embarcadero RAD Studio XE2, Microsoft SQL Server 2012.

Parashchuk I., Saenko I. The Generalized Algorithm of Elimination of Uncertainty of Assessment and Categorization of Semantic Filling of Information Objects for the Benefit of Detection and Counteraction of Undesirable Information. – PP. 486–491.
The analysis of modern methodological approaches, private models and methods of overcoming uncertainty of the basic data necessary for the solution of tasks of the analysis of digital network content is carried out. Features of synthesis of reliable space of signs of undesirable information in various conditions of uncertainty are in details considered. The scheme of stage-by-stage processing of information at the solution of such problems of synthesis is offered, at the same time it is considered that uncertainty of signs of undesirable information can have the nature of unauthenticity (incompleteness) and ambiguity (illegibility). Stages of the generalized algorithm of elimination of uncertainty of assessment and a categorization of semantic filling of information objects for the benefit of detection and counteraction of undesirable information are formulated.
Key words: uncertainty, content, synthesis, sign, undesirable information, space, information object, unauthenticity, illegibility.

Pesikov E. Optimization of Marketing Management Enterprise on the Basis of Application of Methods Operation Research. – PP. 491–497.
We consider one of the possible approaches to the construction of analytical tools for enterprise marketing management, designed to select the optimal range, sales volumes, market segments and product prices and based on the use of mathematical methods of operations research. A model of nonlinear partial-integer programming with variables of continuous and Boolean type is proposed, the use of which allows to plan the production of both previously produced and new products. To analyze the optimization model, it is proposed to use a heuristic algorithm based on the iterative increase in product prices and the solution at each step of the price change of the linear partially integer programming problem by the Land and Doig method.
Key words: enterprise, marketing, optimization, operations research, target segment, sales volume, product price.

Pletnev Y., Shestakov A. To the Issue of Multi-Purpose Transformation Automated Accounting Enterprise. – PP. 497–502.
Significant progress in the transformation of digital platforms of business processes in various areas of the operator's activity according to the NGOSS concept led to the possibility of promoting the mobile service of accounting tasks of the communication enterprise in relation to tangible assets with a special legal status and specifics of inventory, accounting and maintenance, for example, exhibits, Museum objects and collections. The proposed technical solutions of the improved mobile service of accounting tasks allow to expand its use by various organizations (institutions, enterprises) in the digital economy.
Key words: multi-purpose transformation, accounting, NGOSS, cloud computing.

Polpudnikova N., Shestakov A. Technologies for the Automated Management of the Original Design Documentation of the Enterprise Communications. – PP. 503–508.
Questions of maintenance of originals of design documentation of the enterprise developer of means of communication at various stages of a product life cycle are considered. In order to provide integrated approaches in the conditions of change and development of technologies in the office and document management of electronic documents and improve the security of information of the originals of design documentation, the technologies of distributed registers are studied, taking into account the software and hardware-software PDM/PLM systems in operation.
Key words: electronic design documentation, product data management, engineering data management, product life cycle, maintenance of original electronic documentation.

Portnov G., Timoshenko P., Leshchuk M., Yanak A. Multi-Step Detection Algorithm of Ischemia Episodes at ECG Analysis. – PP. 508–513.
Synthesizing a multi-step algorithm for detecting ischemia episodes and testing it on the basis of a test signal which simulates a fragment of a cardio signal as closely as possible during the development of an ischemia episode.
Key words: coronary heart disease, electrocardiogram, ST-segment, Neumann-Pearson criterion, false alarm probability, probability of correct detection, signal-noise ratio.

Prokudin D., Sysa E. Use of AR and VR Technologies in the Educational Sphere. – PP. 513–516.
Nowadays AR and VR technologies develop rapidly and gain more and more popularity. It becomes common to come across devices based on these technologies in modern schools and universities. Just a few years ago implementation of such technologies may have seemed like a futuristic fantasy, however it is most likely that in the forseeable future we will not be able to imagine an educational institution without such devices.
Key words: AR, VR, virtual reality, augmented reality, education.

Prokudin D., Komisarov S., Yakshibaev I. HTML5 Development: What it Means to the End User and Developer. – PP. 516–519.
This article overviews HTML5 development technology, identifies pros and cons of the markup language, and also considers end user's and developer's view on HTML5,
Key words: HTML5, website, developer, end user, development, Adobe Flash.

Ptitsyna L., Tarabarov A. Analysis of the Impact of Information Security Systems on the Performance of Information Systems. – PP. 520–523.
The reasons for the expansion of the methodological foundations of the analysis of the influence of information protection systems on the quality of information systems functioning are considered, describes the key components of the extensions, the models and methods of the analyzed analysis are presented.
Key words: threat, protection of information, model, method, quality, indicators.

Ptitsyna L., El Sabayar Shevchenko N. Dynamic Profile Service-Oriented Systems with Adaptive Management of Their Quality. – PP. 523–528.
The reasons of the increasing demands on the quality of service-oriented systems are described. Quality indicators of service-oriented systems are selected. An possible approaches to managing their quality are analyzed. The ideas about adaptive quality management of service-oriented systems are detailed. An extended object-oriented model of a service-oriented system with adaptive management of its quality has been built. A method for determining the dynamic profile of service-oriented systems with adaptive management of their quality is proposed.
Key words: service-oriented systems, adaptive quality management, object-oriented activity model, dynamic time profile.

Fabiyanovsky I., Saenko I. Assessment and the Choice of Options for Locating Information Resources in a Common Information Space. – PP. 529–532.
The problem of locating information resources depending on the impact of external threats on elements of a common information space is considered. A comparative assessment of various options is given. A problem statement of optimization of information resources placement in a common information space is discussed.
Key words: common information space, information resource.

Horoshenko S., Taranov S. Integrity Ensuring Algorithm for Protecting NAND Flash Memory. – PP. 532–538.
The article describes algebraic manipulation detection codes as a solution to the problem of ensuring integrity in information storage media device using the NAND flash technology. Two modifications of the algorithm are described using wavelet transforms and without it. The additional use of wavelet transforms allows to reduce the maximum of error masking probability while adding a bank of wavelet coefficients to the algorithm.
Key words: integrity, coding theory, robust codes, wavelet transform, NAND flash memory.

Tarasov V. Modeling and Performance Analysis of Multimedia Traffic in Infocommunication Systems. – PP. 538–542.
Modern methods of multimedia traffic analysis with regard to noise immunity and overload prevention to ensure proper quality of service in networks with the integration of services are considered. The review of approaches to the performance evaluation of infotelecommunication infrastructures, evaluation of the impact of external and internal factors on the probability-time characteristics and other indicators of service quality. The analysis of prospects of development, modernization, introduction and expansion of communication services and multimedia hardware and software systems for solving various problems is carried out.
Key words: Triple Play, IPTV, virtual reality.

Tarasov V. Application of Innovative Approach in Evaluating the Technical Disciplines. – PP. 543–547.
The approach to the organization of intermediate and final certification, where as an alternative to the traditional means of control is the interaction between students, setting and solving applied problems, using both the knowledge gained within the discipline and analytical skills.

This approach is designed to ensure the introduction of the educational process as a competitive component, and the need for collective problem solving. Thus, there is a game component that motivates students to professional training, as well as to the development of skills in the team.
Key words: innovative approaches, technical disciplines, competition.

Sharikov P. A Methodic for Quickly Obfuscating Java-Application Class Files with Minimal Use of Resources. – PP. 548–551.
Software protection is an important task. The article explains the need to protect bytecode java-application using obfucirovaniya proposed methods. On the basis of the results obtained by the work of decompilers and java-compiler, a technique obfuscated java-code is proposed in order to complicate the reverse engineering of java class files. The conclusion is made about the possibility of using the investigated method to protect the java-application.
Key words: Java, bytecode, bytecode, bytecode protection methods, digital watermark, steganography, executable files, obfuscator, obfucation, obfuscation, obfucation.

АВТОРЫ СТАТЕЙ

АВРАМЕНКО
Владимир Семенович — кандидат технических наук, доцент, профессор кафедры Автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, vsavr@yandex.ru

АГАПОВ
Ефим Вячеславович — студент группы ИСМ-61з кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, agapovefim@gmail.com

АКИМОВ
Сергей Викторович — кандидат технических наук, доцент кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akimov-sv@yandex.ru

АЛМАЕВ
Тимур Юрьевич — курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, almaevtimur@mail.ru

АНДРЕЕВ
Дмитрий Сергеевич — студент группы ИСТ-741М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, twer11@mail.ru

АНТОНОВ
Валерий Валентинович — старший преподаватель кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, antonler@rambler.ru

АЧИЛОВА
Фируза Курбановна — старший преподаватель факультеты Компьютерный инжиниринг кафедры «Информационные технологии» Каршинский филиал Ташкентского университета информационных технологий имени Мухаммада аль-Хорезми, Farishta18@mail.ru

БАЯЗИТОВ
Евгений Гасанович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, kolosnicynEvgeny@yandex.ru

БЕЛОУС Константин Владимирович — кандидат технических наук, доцент кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kostos2@yandex.ru

БЕЛОЦВЕТОВ Денис Андреевич — рядовой, оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, belotsvetov.denis@yandex.ru

БЕЛЯЕВ Владислав Владиславович — студент факультета Безопасности информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, vladikbelyaew@yandex.ru

БОВЫКИН Евгений Александрович — студент группы ИСТ-541 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rebovykin@gmail.com

БОТЯКОВ Вячеслав Витальевич — магистрант кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, wiseboy@yandex.ru

БОЧКАРЕВ Дмитрий Александрович — слушатель Военной академии связи им. Маршала Советского Союза С. М. Буденного, p_oleg99@mail.ru

БУНЕЕВ Иван Романович — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, buneev_ivan_r@mail.ru

БУРЛОВ Вячеслав Георгиевич — доктор технических наук, профессор, заведующий кафедрой Информационных технологий и систем безопасности Российского государственного гидрометеорологического университета, burlovvg@mail.ru

ВАГАНОВ Александр Валерьевич — старший преподаватель кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sut-ispiu@mail.ru

ВАЖЕНИН Иван Андреевич — студент группы ИСМ-61з кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, ptitsina_lk@inbox.ru

ВАКАЛЮК Андрей Игоревич — слушатель Военной академии связи им. Маршала Советского Союза С. М. Буденного, p_oleg99@mail.ru

ВАНЧАКОВА Нина Павловна — доктор психологических наук, заведующая кафедрой педагогики и психологии факультета последипломного образования Первого Санкт-Петербургского государственного медицинского университета им. И. П. Павлова, nvanchakova@gmail.com

ВЕРХОВА Галина Викторовна — доктор технических наук, профессор, заведующая кафедрой Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича galina500@inbox.ru

ВИТКОВА Лидия Андреевна — научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, старший преподаватель Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lidia@glorystory.ru

ВИХАРЕВ Антон Николаевич — сотрудник Академии Федеральной службы охраны Российской Федерации, jereeko5@gmail.com

ВЛАСЕНКО Максим Андреевич — курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, vlasenko199@yandex.ru

ВОЛОШЕНЕНКО Дарья Владимировна — студентка группы ИСТ-811м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dasha.voloshenenko@gmail.com

ВОЛОШИНОВ Денис Вячеславович — доктор технических наук, заведующий кафедрой Информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, voloshinov@pochta.ru

ВОЛЫНКИН Павел Александрович — кандидат технических наук, доцент кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pavelas@mail.ru

ВОСТРЫХ Алексей Владимирович — аспирант кафедры Безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.vostrykh@list.ru

ВЫШЛОВ Олег Валерьевич — аспирант кафедры Защищенных сетей связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ov@it-telecom.ru

ГАТЧИН Юрий Арменакович — доктор технических наук, профессор факультета Безопасности информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, Gatchin@mail.ifmo.ru

ГИЯСОВ Улугбек Эшпулутович — старший преподаватель кафедры «Программный инжиниринг» Самаркандского филиала Ташкентского университет информационных технологий им. Мухаммада Ал-Хорезми, bek99989@gmail.com

ГРАЩЕНКО Леонид Александрович — кандидат физико-математических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, graschenko@mail.ru

ГРИГОРЕНКО Ксения Владимировна — студентка группы ИСТ-711м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, xeniakorsakova@gmail.com

ГРУЗДЕВА Людмила Авенировна — старший преподаватель кафедры Информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gruzdeva.18@bk.ru

ГРУШЕВАЯ Екатерина Васильевна — сотрудник Академии Федеральной службы охраны Российской Федерации, leshinsckaya.kat@yandex.ru

ГУБИН Александр Николаевич — кандидат технических наук, доцент, доцент кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gan50_60@mail.ru

ГУРЬЕВА Татьяна Николаевна — кандидат педагогических наук, доцент кафедры Бизнес-информатики Северо-Западного института управления РАНХ и ГС, tguryeva@yandex.ru

ДАВЛЕТШИНА Элеонора Ринатовна — студент 4 курса кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, eleonora.davletshina@mail.ru

ДАВЫДОВА Екатерина Викторовна — старший преподаватель кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, k_davidova@bk.ru

ДАНИЛОВА Елена Ивановна — преподаватель кафедры Информационных технологий Военно-морского (политехнического) института ВУНЦ ВМФ «Военно-морская академия», danilova-ei@mail.ru

ДЕМИДОВ Андрей Михаилович — студент группы 5185 Казанского Национального Исследовательского Технического Университета им. А. Н. Туполева – КАИ, shugary.shu@gmail.com

ДЕНИСОВ Евгений Сергеевич — кандидат технических наук, Ph.D., доцент кафедры Радиоэлектроники и информационно-измерительной техники Казанского Национального Исследовательского Технического Университета им. А. Н. Туполева - КАИ genia-denisov@yandex.ru

ДМИТРИЕВ В. И. — доктор технических наук, доцент Военной академии связи им. Маршала Советского Союза С. М. Будённого

ДОВГИЙ Сергей Сергеевич — аспирант кафедры Защищенных сетей связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dss1307@mail.ru

ДОВЖИК Антон Викторович — ефрейтор, старший оператор 7-й научной роты Военной академии связи им. Маршала Советского Союза С.М. Будённого

ДОЙНИКОВА Елена Владимировна — кандидат технических наук, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук; старший научный сотрудник Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, doynikova@comsec.spb.ru

ДОЛГУН Владислав Олегович — аспирант кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Dolgun@spbgut.ru

ДЮБОВ Андрей Сергеевич — кандидат технических наук, доцент кафедры Фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, blip@bk.ru

ЕФИМОВ Кирилл Анатольевич — студент группы ИСТ-712М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, heykirill@gmail.com

ЖАРАНОВА Анастасия Олеговна — студент группы ИСТ-511 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zharanovaan@gmail.com

ЖОЛОБОВА Кристина Владимировна — студент кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Dnitreva97@yandex.ru

ЗАЙЦЕВА Алиса Сергеевна — студент группы Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alicewithalex25@gmail.com

ЗВЕРЕВ Артем Александрович — сотрудник Академии Федеральной службы охраны Российской Федерации, zverevartyom@yandex.ru

ЗВЯГИНЦЕВ Станислав Александрович — сотрудник Академии Федеральной службы охраны Российской Федерации, endrkray@gmail.com

ЗОЛОТОВ Олег Иванович — кандидат технических наук, профессор, доцент кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Oleg_1938@mail.ru

ИВАНОВ Василий Геннадьевич — полковник, кандидат военных наук, доцент кафедры Организации связи Военной академии связи им. Маршала Советского Союза С. М. Будённого, wasj2006@yandex.ru

ИВАНОВ Денис Александрович — адъюнкт кафедры Безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, prosto_deniss@mail.ru

ИВАНОВ С. А. — кандидат военных наук, доцент Военной академии связи им. Маршала Советского Союза С. М. Буденного

ИГЛОВ Михаил Алексеевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, may_devil@inbox.ru

ИЕВЛЕВ Иван Алексеевич — студент группы ИСТ-712М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivlyan_363@mail.ru

ИЛЬИНА Ольга Борисовна — кандидат географических наук, доцент, старший преподаватель кафедры Автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, nastik94@yandex.ru

ИСУПОВА Екатерина Анатольевна — старший преподаватель кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kat_isupova@list.ru

КАЗАКОВ Дмитрий Борисович — аспирант кафедры Защищенных сетей связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dkazakov@spbgut.ru

КАПУРОВ Николай Александрович — магистрант кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kapnik95@rambler.ru

КАРАЧИНСКАЯ Елизавета Анатольевна — студентка группы ИСТ-711м кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elizavetakarachinskayaa@gmail.com

КНЯЗЕВ Ренат Радикович — магистр группы ИСТ-811м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, renatknyazev@gmail.com

КОБЕЛЕВ Александр Сергеевич — рядовой, оператор 7й научной роты Военной академии связи им. Маршала Советского Союза С. М. Будённого

КОВАЛЕНКО Алексей Павлович — студент группы ИКМ-72 з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alesha-kovalenko@mail.ru

КОВАЛЬЧУК Владислав Андреевич — студент группы ИСТ-612 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dobro322@yandex.ru

КОДИРОВ Фаррух Эргаш угли — бакалавр факультеты Компьютерный инжиниринг кафедры «Информационные технологии» Каршинский филиала Ташкентского университета информационных технологий имени Мухаммада аль-Хорезми, Farruxbek0209@mail.ru

КОЗАЧОК Александр Васильевич — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, totrin@list.ru

КОЗИН Никита Сергеевич — рядовой, оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Будённого, nekozinanikita@yandex.ru

КОЗЛОВА Людмила Петровна — кандидат технических наук, доцент, доцент кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tigrenok59@mail.ru

КОМАРОВ Игорь Иванович — кандидат физико-математических наук, доцент факультета Безопасности информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, komarov@cit.ifmo.ru

КОМАРОВА Антонина Владиславовна — аспирант факультета Безопасности информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, piter-ton@mail.ru

КОМАРОВА Лидия Дмитриевна — студентка группы ИСТ-811м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lidia.comarowa@yandex.ru

КОМАШИНСКИЙ Владимир Ильич — доктор технических наук, доцент, заместитель директора по научной работе Института проблем транспорта им. Н. С. Соломенко Российской академии наук, kama54@rambler.ru

КОМИСАРОВ С. А. — кандидат технических наук, доцент Военной академии связи им. Маршала Советского Союза С. М. Будённого

КОРОБЕЙНИКОВ Анатолий Григорьевич — доктор технических наук, профессор, заместитель директора по науке Санкт-Петербургского филиала Федерального государственного бюджетного учреждения науки Института земного магнетизма, ионосферы и распространения радиоволн им. Н. В. Пушкова Российской академии наук; профессор факультета Безопасности информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, Korobeynikov_a_g@mail.ru

КОТЕЛЬНИКОВ Максим Михайлович — магистрант кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, max.kat.ru@mail.ru

КОТЕНКО Игорь Витальевич — доктор технических наук, профессор, заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, профессор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, ivkote@comsec.spb.ru

КОТКИНА Мария Сергеевна — студентка группы ИСТ-812м кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maria.kotkina@yandex.ru

КОТЛОВА Мария Владимировна — старший преподаватель кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mkotlova@gmail.com

КРАСИЛЬНИКОВА Наталья Валерьевна — кандидат психологических наук, доцент кафедры Педагогики и психологии факультета Последипломного образования Первого Санкт-Петербургского государственного медицинского университета им. И. П. Павлова, NataljaKrasilnikova@yandex.ru

КРИБЕЛЬ Александр Михайлович — адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, s15136@mail.ru

КРИВКО Дмитрий Витальевич — сотрудник Академии Федеральной службы охраны Российской Федерации

КУБАСОВ Игорь Вячеславович — магистр, инженер кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

КУЗЬКИН Александр Александрович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, kuzmich313@mail.ru

КУПЧИНЕНКО Ольга Павловна — преподаватель кафедры Автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, k-olga102@yandex.ru

КУРНОСОВ Валерий Игоревич — доктор технических наук, профессор кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vi-Kurnosov@mail.ru

КУЦАКИН Максим Алексеевич — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, max_kooks@mail.ru

КХОДЕР Хабиб Мухссен — аспирант кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, h.khoder@list.ru

ЛАВРИНОВИЧ Александр Андреевич — инженер кафедры Безопасности информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, lavrinovich@corp.ifmo.ru

ЛАВРОВ Антон Владимирович — рядовой, оператор 7й научной роты Военной академии связи им. Маршала Советского Союза С. М. Будённого

ЛАПКО Александр Николаевич — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, lan46@mail.ru

ЛАСКУС Евгений Олегович — студент факультета Безопасности информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики

ЛЕБЕДЕВ Дмитрий Сергеевич — ефрейтор, старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, 715702@gmail.com

ЛЕБЕДЕВ Сергей Игоревич — студент кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sergi-spb@yandex.ru

ЛЕБЕДЕНКО Евгений Викторович — кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, lev@academ.msk.rsnet.ru

ЛЕПЕШКИН Михаил Олегович — аспирант Санкт-Петербургского Политехнического университета имени Петра Великого, Высшая школа техносферной безопасности, misha.lepeshckin@yandex.ru

ЛЕПЕШКИН Олег Михайлович — доктор технических наук, доцент, доцент кафедры Безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, lepechkin1@yandex.ru

ЛЕЩУК М. З. — кандидат технических наук, доцент Военной академии связи им. Маршала Советского Союза С. М. Буденного

ЛИПАТНИКОВ Валерий Алексеевич — доктор технических наук, профессор, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, lipatnikovanl@mail.ru

ЛИТВИНОВ Владислав Леонидович — кандидат технических наук, доцент, доцент кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vlad.litvinov61@gmail.com

ЛУКЬЯНЧИК Валентин Николаевич — кандидат военных наук, доцент, сотрудник первого научного отдела научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного

ЛЫСЕНКО Александр Михайлович — студент группы Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alicewithalex25@gmail.com

МАКАРЕНКО Екатерина Андреевна — студент группы ИСТ-742М Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, makarenko-94@mail.ru

МАКАРОВ Павел Владимирович — оператор научной роты Военной академии связи имени Маршала Советского Союза С. М. Буденного, pav5722862@yandex.ru

МАКЕЕВ Сергей Михайлович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, maksm57@yandex.ru

МАЛИКОВ Альберт Валерьянович — адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, mkv.vas@yandex.ru

МАМАДЖАНОВА Шахло Вахобжоновна — курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, mamadzhanowashahlo@gmail.com

МАМОНЧИКОВА Алина Сергеевна — старший инженер кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mamonchikova@rubin-spb.ru

МАРГАРИТОВА Яна Сергеевна — студентка группы ИСТ-711м кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, margaritova.yana@yandex.ru

МАРКИН Дмитрий Олегович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, admin@nikitka.net

МЕДВЕДЕВ Валерий Александрович — кандидат технических наук, доцент кафедры Безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, medvedev.spb@list.ru

МЕЛЕШКО Алексей Викторович — студент 2 курса магистратуры Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, младший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, lexa.0710@gmail.com

МЕНЩИКОВ Александр Алексеевич — аспирант факультета Безопасности информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, Menshikov@corp.ifmo.ru

МИХАЙЛИЧЕНКО Николай Валерьевич — адъюнкт кафедры Автоматизированных систем Военной академии связи им. Маршала Советского Союза С. М. Буденного, 23esn2008@rambler.ru

МИШИН Алексей Александрович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, mishin-lex@mail.ru

МОСКВИЧЕВ Илья Вячеславович — оператор научной роты Военной Академии Связи им. Маршала Советского Союза С. М. Буденного, ilya-moskvichev@yandex.ru

МУРСАЛИМОВА Камила Болатовна — магистр группы ИСТ-811м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mursalimovi@mail.ru

МУСАЕВА Татьяна Вагифовна — кандидат технических наук, доцент кафедры Информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, neli_6868@mail.ru

НАЗАРОВ Кирилл Всеволодович — студент группы ИСТ-741М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nazarov1995@icloud.com

НАПАЛКОВА Алена Дмитриевна — магистрант кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alleho4ka@gmail.com

НИКИШИНА Гузель Венеровна — аспирант кафедры Радиоэлектроники и информационно-измерительной техники Казанского Национального Исследовательского Технического Университета им. А. Н. Туполева – КАИ, time-guzel-v@yandex.ru

НИКУЛИН Денис Александрович — оператор научной роты Военной Академии Связи им. Маршала Советского Союза С. М. Буденного, nikulinarmy@yandex.ru

НУРАЛИЕВ Фахриддин Муродиллаевич — доктор технических наук, доцент кафедры Аудиовизуальные технологии, декан факультета Телевизионные технологии Ташкентского университета информационных технологий им. Мухаммада Ал-Хорезми, nuraliev2001@mail.ru

ПАВЛОВ Дмитрий Игоревич — сотрудник Академии Федеральной службы охраны Российской Федерации, chupa5598@gmail.com

ПАНТЮХИН Олег Игоревич — кандидат технических наук, доцент, доцент кафедры, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, p_oleg99@mail.ru

ПАРАЩУК Игорь Борисович — доктор технических наук, профессор, Заслуженный изобретатель РФ, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук; инженер лаборатории Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики; профессор кафедры автоматизированных систем Военной академии связи им. Маршала Советского Союза С. М. Буденного, shchuk@rambler.ru

ПЕСИКОВ Эдуард Борисович — доктор технических наук, профессор, профессор кафедры Автоматизации предприятий связи Санкт - Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ed_pesikov@mail.ru

ПИЛИКИНА Елена Анатольевна — старший преподаватель кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, helenarh@yandex.ru

ПЛЕТНЕВ Ярослав Андреевич — магистрант кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pletnevyaroslav@gmail.com

ПОЛЕГЕНЬКО Анастасия Михайловна — аспирант факультета Безопасности информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, ведущий специалист по защите информации ЗАО «ТЕЛРОС», ассистент кафедры вычислительных систем и программирования Санкт-Петербургского государственного экономического университета, p.a.m.92@mail.ru

ПОЛИКАНОВ Владимир Павлович — магистр кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

ПОЛПУДНИКОВА Наталья Викторовна — магистрант кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, santpetesburg521@yandex.ru

ПОПОВА Марина Николаевна — студент 4 курса кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, marinapopova14@ya.ru

ПОРТНОВ Георгий Александрович — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, portnov-georgii@mail.ru

ПРОКУДИН Даниил Владимирович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, prokodile@yandex.ru

ПТИЦЫНА Лариса Константиновна — доктор технических наук, профессор, заведующая кафедрой Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ptitsina_lk@inbox.ru

РАКИЦКИЙ Дмитрий Станиславович — адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, s15136@mail.ru

РАКИЦКИЙ Станислав Николаевич — кандидат военных наук, доцент, доцент кафедры Военной академии связи им. Маршала Советского Союза С. М. Буденного, s15136@mail.ru

РЕВЯКИН Андрей Михайлович — адъюнкт Академии Федеральной службы охраны Российской Федерации, dronrev@mail.ru

РУССИЯ Вахтанг Сергеевич — студент кафедры Программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, russiya.vs@spbgut.ru

РЯБОКОНЬ Владимир Владимирович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, mimicria@mail.ru

САВИНОВ Артем Андреевич — дипломник кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Artemrm21@yandex.ru

САВКОВ Сергей Витальевич — преподаватель факультета Безопасности информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, sergsavkov@gmail.com

САЕНКО Игорь Борисович — доктор технических наук, профессор, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук; ведущий научный сотрудник лаборатории Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики; профессор Военной академии связи им. Маршала Советского Союза С. М. Будённого, ibsaen@mail.ru

САЗОНОВ Антон Олегович — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, ant-sazon@yandex.ru

САННИКОВ Иван Алексеевич — сотрудник Академии Федеральной службы охраны Российской Федерации, syadoy@yandex.ru

СВЕЧНИКОВ Дмитрий Александрович — кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, mhm57@yandex.ru

СКОРОПАД Александр Витальевич — ведущий инженер-электроник НИЛ № 4231, НИО № 423, НТЦ № 42 Санкт-Петербургского филиала «Ленинградское отделение научно-исследовательского института радио», sav01236@yandex.ru

СКУРНОВИЧ Алексей Валентинович — кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, alekseymail2010@mail.ru

СОСНОВСКИХ Александр Михайлович — ассистент, аспирант кафедры Информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sosnovskikh.am@yandex.ru

СПИРИН Андрей Андреевич — сотрудник Академии Федеральной службы охраны Российской Федерации, spirin_aa@bk.ru

СТЕПИНА Олеся Александровна — сотрудник Академии Федеральной службы охраны Российской Федерации

СТРАХ Любовь Владимировна — студентка 6 курса лечебного факультета Первого Санкт-Петербургского государственного медицинского университета им. И. П. Павлова, lubovstrah@gmail.com

СЫСА Е. Т. — кандидат военных наук, доцент Военной академии связи им. Маршала Советского Союза С. М. Буденного

ТАЙМАЗОВА Зарина Валерьевна — студентка группы ИСТ-812м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zarinataymazova@gmail.com

ТАРАБАРОВ Андрей Викторович — студент группы ИСМ-61з кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, antar94@bk.ru

ТАРАНОВ Сергей Владимирович — ассистент кафедры Безопасности информационных систем факультета Информационных систем и технологий Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, serg.tvc@gmail.com

ТАРАСОВ Андрей Владимирович — курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, ringhton555@gmail.com

ТАРАСОВ Владимир Анатольевич — старший преподаватель кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича», vat-liquidator@bk.ru

ТИМОШЕНКО Павел Анатольевич — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, progrims@gmail.com

ТИХОНОВ Валерий Александрович — оператор научной роты Военной Академии Связи им. Маршала Советского Союза С. М. Будённого, valery_tikhonov@mail.ru

ТИШКОВ Артем Валерьевич — кандидат физико-математических наук заведующий кафедрой физики, математики и информатики Первого Санкт-Петербургского государственного медицинского университета им. И. П. Павлова, artem.tishkov@gmail.com

ТОРТОЧАКОВ Сергей Владиславович — оператор научной роты Военной Академии Связи им. Маршала Советского Союза С. М. Будённого, de.loire@yandex.ru

ФАБИЯНОВСКИЙ Игорь Николаевич — адъюнкт Военной Академии Связи Маршала Советского Союза им. С.М. Будённого, fabik-spb@yandex.ru

ФАДЕЕВА Александра Викторовна — студентка группы ИСТ-812м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fadeevasash@gmail.com

ФИЛИППОВ Феликс Васильевич — кандидат технических наук, старший научный сотрудник, доцент кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 9000096@mail.ru

ФИЛИЧКИН Илья Игоревич — магистр, инженер кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

ХВОСТОВ Максим Алексеевич — студент группы ИСТ-541 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mkliverout@gmail.com

ХОРОШЕНКО Сергей Викторович — кандидат технических наук, доцент, заведующий кафедрой Безопасность информационных систем факультета Информационных систем и технологий Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, khoroshenko@sut.ru

ХОХЛАЧЕВА Екатерина Александровна — курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, katplotnikova82@mail.ru

ЧЕБЫКИН Василий Александрович — кандидат технических наук, доцент кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bazil.chebykin@yandex.ru

ЧЕРНЯВСКИЙ Андрей Владимирович — магистрант Военной академии связи им. Маршала Советского Союза С. М. Буденного, zxcdewqa@mail.ru

ЧЕЧУЛИН Андрей Алексеевич — кандидат технических наук, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института автоматизации и информатики Российской академии наук, старший преподаватель Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chechulin@comsec.spb.ru

ШАБАНОВ Александр Павлович — студент кафедры Автоматизации предприятий связи факультета Информационных систем и технологий Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, saxa1997@mail.ru

ШАРАБАЕВА Любовь Юрьевна — кандидат физико-математических наук, доцент кафедры Бизнес-информатики Северо-Западного института управления РАНХ и ГС, shar_lu@mail.ru

ШАРИКОВ Павел Иванович — аспирант кафедры Защищённые системы связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sharikov.pavel@ro.ru

ШВИДКИЙ Артем Александрович — аспирант кафедры Защищенных сетей связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shvidkiy@sut.ru

ШЕВЧЕНКО Александр Александрович — младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, alex_pavel1991@mail.ru

ШЕСТАКОВ Александр Викторович — доктор технических наук, старший научный сотрудник, профессор кафедры Автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexandr.shestakov01@yandex.ru

ШИЯН Андрей Анатольевич — кандидат педагогических наук, доцент кафедры Информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mnea@mail.ru

ЭЛЬ САБАЯР ШЕВЧЕНКО Нидал — аспирант кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nzs.vus@gmail.com

ЮМАШЕВА Елена Сергеевна — бакалавр, магистр факультета Безопасности информационных технологий Санкт-Петербургского национально исследовательского университета информационных технологий, механики и оптики, yumasheva.lena@list.ru

ЯКУБОВА Наиля Равильевна — старший преподаватель кафедры Информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nel123@yandex.ru

ЯКШИБАЕВ
Ильдар Салаватович
оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного,
dvyglazzik@mail.ru

ЯНАК
Александр Федорович
старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного,
ya6ik1@list.ru

АВТОРСКИЙ УКАЗАТЕЛЬ

СПбГУТ)))