III МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

"ІНФОРМАЦІЙНА БЕЗПЕКА ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ"

INFOSEC & COMPTECH

м. Кропивницький, 19-20 квітня 2018 року

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ

МЕХАНІКО-ТЕХНОЛОГІЧНИЙ ФАКУЛЬТЕТ

КАФЕДРА КІБЕРБЕЗПЕКИ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

ІІІ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

"ІНФОРМАЦІЙНА БЕЗПЕКА ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ"

INFOSEC & COMPTECH

19-20 квітня 2018 року

м. Кропивницький

УДК 004

Інформаційна безпека та комп'ютерні технології: Збірник тез доповідей ІІІ Міжнародної науково-практичної конференції, 19-20 квітня 2018 року, м. Кропивницький: ЦНТУ, 2018. – 336 с.

Збірник містить тези доповідей за матеріалами ІІІ Міжнародної науково-практичної конференції "Інформаційна безпека та комп'ютерні технології", що відбулась 19-20 квітня 2018 року на базі кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Голова – **Левченко О.М.**, д.е.н., професор, проректор з наукової роботи Центральноукраїнського національного технічного університету.

Заступники голови:
Смірнов О.А., д.т.н., професор, завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету;
Мелешко Є.В., к.т.н., доцент, доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

Члени оргкомітету:
Карпінський М.П., д.т.н., професор (м. Бельсько-Бяла, Польща).
Сєйлова Н.А., к.т.н., доцент (м. Алмати, Казахстан).
Охрименко С.А., д.е.н., професор (м. Кишинів, Республіка Молдова).
Корченко О.Г., д.т.н., професор (Національний авіаційний університет, м. Київ).
Бурячок В.Л., д.т.н., професор, с.н.с. (Київський Університет імені Бориса Грінченка, м. Київ).
Лахно В.А., д.т.н., професор (Європейський університет, м. Київ).
Кузнецов О.О., д.т.н., професор (Харківський національний університет імені В.Н. Каразіна, м. Харків).
Семенов С.Г., д.т.н., доцент, с.н.с. (Національний технічний університет «Харківський політехнічний інститут», м. Харків).
Павленко М.А., д.т.н., доцент (Харківський національний університет Повітряних Сил імені Івана Кожедуба, м. Харків).
Рудницький В.М., д.т.н., професор (Черкаський державний технологічний університет, м. Черкаси).
Стасєв Ю.В., д.т.н., професор (Харківський національний університет Повітряних Сил імені Івана Кожедуба, м. Харків)
Кавун С.В., д.е.н., к.т.н., професор (ХННІ ДВНЗ «Університет банківської

Адреса редакційної колегії:
25030, м. Кропивницький, пр. Університетський, 8,
Центральноукраїнський національний технічний університет,
тел.: (0522)390-449.

Відповідальна за випуск: Мелешко Є.В.

ЗМІСТ

Секція 1.
Інформаційна безпека держави, суспільства та особистості

Секція 2.
Програмування та інформаційно-комунікаційні технології

Секція 3.
Інтелектуальні системи та штучний інтелект

UDC 004.056.53

Investigation of the properties of hybrid crypt-code constructions

Bilodid I.V., graduate student,
Evseev S.P., Ph.D., assistant professor
Simon Kuznets Kharkiv National University of Economics, Kharkiv

Damaged text is the text obtained by further deformation of non-existent letter codes. Thus, a necessary and sufficient condition for the damage of text with loss of meaning is the shortening of the lengths of the code symbols of the text beyond their redundancy [1]. As a consequence, the damaged text has a length shorter than the length of the source text, and there is no sense in the source text [3].

The theoretical basis for building damaged texts is to remove the ordering of the symbols of the source text and, as a consequence, to reduce the redundancy of the language symbols in the damaged text. In this case, the amount of information expressing this ordering will be equal to the decrease in the entropy of the text in comparison with the maximum possible entropy value corresponding to the lack of ordering in the text in general, i.e. equiprobable appearance of any letter after any previous letter. The methods of computing information proposed by K. Shannon allow us to determine the ratio of the amount of predictable information (ie, formed according to certain rules) and the amount of that unexpected information that can not be predicted in advance.

To restore the original sequence, there is no need to know the intermediate faulty sequences. It is necessary to know only the last flawed sequence (the last flawed text after all the cycles) and all the damages with the rules for their application.

Cryptographic damaged texts are texts obtained by the following methods [3]: damage to the source text with subsequent encryption of the damaged text and / or its damage; damage to the ciphertext; damage to the cipher text of the defective text and / or ciphertext of the damage. In work [1] methods of constructing the HCCSDC based on MCCS McEliece on MEC are considered.

The length of the information sequence (in bits) arriving at the input of the cryptosystem from the SC is determined by the following expression: for HCCSDC on shortened codes: $l_I = l_z^c + l_z^f$, where $l_z^c = K_c \times L + \frac{1}{K_f} \times s$ – length of damaged text; $l_z^f = L + u \times s$ – length of damage; $s = \left[\frac{L_0 - L_{DT}}{L_{DT}} \right]$ – number of segments of the damaged text, $K_C = 1 - K_f \approx 0{,}758$ – compression ratio of the

remainder (damaged text) (at u = 8, v = 3, z = 5); $K_f = \frac{2-2^{v-u+1}}{u} \approx 0{,}242$ – coefficient of compression of the flag (damage) (at u = 8, v = 3, z = 5); $z = \frac{log(u \times L) - 7}{log(1/K_C)}$ – necessary for the randomization of the cipher MV2, the number of permissible conversion rounds. For HCCSDC on extended MEC: $l_I = 1/2k \times m + l_z^c + l_z^f$.

The length of the public key (in bits) is determined by the sum of the elements of the matrix G_X^{EC} and is given by the expressions: for HCCSDC on truncated MEC: $l_K = 1/2k \times \left(2\sqrt{q} + q + 1 - 1/2k\right) \times m$; for HCCSDC on extended MEC: $l_K = 1/2k \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times m$. *The length of the private key* (in bits) is determined by the sum of the matrix elements *X, P, D* (in bits) and is given by expressions: for HCCSDC on shortened codes: $l_{K_+} = 1/2k \left\lceil \log_2 \left(2\sqrt{q} + q + 1\right) \right\rceil + \left|F_u^v\right|$, where $\left|F_u^v\right| = 2^u!$ – the cardinality of the set of substitution transformations; for HCCSDC on extended codes: $l_{K_+} = \left(1/2k - 1/2k\right) \left\lceil \log_2 \left(2\sqrt{q} + q + 1\right) \right\rceil + \left|F_u^v\right|$.

Conclusions. Considered methods for constructing hybrid crypto-code constructions with defective codes (HCCSDC) based on the synthesis of modified non-symmetric crypto-code systems McEliece (MNCCS) on elliptic codes (EC) with multi-channel cryptographic systems on damaged codes, exchange protocols for securing confidentiality in IP networks. Theoretical bases of decrease in 2 - 3 times power capacity of MCCS McEliece with EC and hybrid structures of MCCS with damaged codes due to reduction of power of the Galois field. The required level of cryptographic strength of the hybrid cryptosystem whole is provided for their software implementation.

Literature

1. Evseev S., Korol O., Rzaev H., Smanova Z. Development of a modified asymmetric McEliece crypto-code system on shortened elliptic codes // Eastern-European Journal of Enterprise Technologies. – 2016. – P. 18-26.

2. Mishchenko V., Vilansky Y. Damaged texts and multichannel cryptography. – Minsk: Encyclopedics, 2007. – 292 p.

3. Evseev S., Korol O., Koc G. Building hybrid security systems based on crypto-code structures and damaged codes. // Eastern-European Journal of Eenterprise Technologies. – 2017. – P. 4-22.

UDC 004.9

Technical methods for enhancing hotel information systems security

Borisov T.T., PhD Student
D. A. Tsenov Academy of Economics, Svishtov, Bulgaria

Abstract: *The major contributor to the growth of tourism is the improvements in the methods and mechanisms used to collect, process, analyse, store and use information. The well-known computer systems, video systems, teleconferencing systems and electronic systems have led to the complete automation and widespread use of electronic equipment. The creation of computer systems facilitates accommodation and transport reservations; entertainment services before purchasing the tourist product; the availability and accessibility study of different types of tourism and routes, the tourism potential of countries and regions.*

Key words*: tourism in Bulgaria, mobile technologies, modern types of tourism, e-business, information technologies, payment methods.*

1. Introduction.

In the 21st century, information and communication technologies are constantly present in people's daily routine, both personally and professionally. There is a trend in the development of information technology, associated with the widespread use of small-sized, efficient and easy-to-use devices. Compared to desktop machines, mobile devices provide a more accessible way to connect to the Internet at any time and from anywhere.

The tourism industry, as a key industry where accessing information to customers and partners at the right time and at the right place is of importance, is an environment that has a strong potential for deploying and using mobile devices and technologies. Using these innovative tools facilitates:

- making consumer bookings for accommodation and transport;
- sightseeing and entertainment services, before purchasing the tourist product;
- availability and accessibility study of different types of tourism and routes, the tourism potential of countries and regions.

Mobile information technologies allow transactions through wireless communication networks, regardless of the location of the participants. Mobile devices, mobile phones, laptops, tablet computers, hybrid phones, smart phones, personal digital assistants or handheld computers, etc., are perceived as mobile devices.

Modern mobile information technologies are developing every year to make tourism more attractive and accessible to consumers. Online reservations or online targeting is becoming increasingly popular in Bulgaria. The Bulgarian user participates in online tourism by reviewing reservations, virtual maps of

geographic regions, using online payments, etc.

2. Essence of hotel information systems

The spread of information technologies in the tourism industry is an indisputable fact. At this point, it is impossible to imagine working in any tourist enterprise (object, company, economic organization) without the use of e-mail, Internet access to various services or booking systems.

The introduction of modern information and communication technologies in the tourism industry is a key factor for the prosperity of every tourist enterprise in the conditions of constantly increasing domestic and international competition. The creation of fully functional and Internet-connected computerized information systems for accommodation, transport, sightseeing, etc. is not only a recommendation to managers, but also a necessity imposed by the evolutionary processes in the modern information society and the new forms of marketing and advertising in the tourist business.

In general, **the information system of a tourism company** can be defined as *"a set of technical and software assurance, data, communications, personnel and collecting procedures, processing, storing and transmitting activity data and business process data, both within and outside the company"* (Kraeva, 2012, p. 179). It must be consistent with the management model, information infrastructure and business strategy of the tourism company. Its primary task is to provide complete, on time and reliable information about the realization of the management functions and processes in the tourist site.

The efficient use of these measures realizes in the conditions of their universal application by all the subjects in the tourism industry. Usually, each of the technologies integrates vertically, horizontally and diagonally systemically with others so that it can be used in the activities of various territorial subdivisions of the tourist enterprise.

The management of tourist information is frequently done by using the following **technical and programming means**:

- ***computer reservation systems (reservation platforms)*** **-** the most important information systems in tourism. Representatives of this type are the Saber, Apollo, SystemOne, WorldSpan, Amadeus and Galileo systems;
- ***hotel reservation systems and car rental*** **-** unlike the previous ones, this type of information systems cannot be used directly by travel agents, but only through a booking platform or by telephone. The Sheraton Hotels chain uses such a system. Similar examples are Confirm and Ultrawitch systems;
- ***video texting systems*** **–** they answer the direct questions of tourists about the sale of excursions, reduce the load of communication lines during the peak days of searching for tickets and travel services, coordinate the quantity and timeliness of tourist information;
- ***telemarketing systems*** **–** allow making of pre-programmed calls to customers in order to offer new services and collect feedback from them;

• ***office maintenance systems*** **-** designed to operationally collect and manage customer information.

The implementation of modern information and communication technologies in tourism information systems requires knowledge of the characteristics of the Global Network so that they can be applied to automate the activity of the tourist enterprise.

3. Types of attacks against hotel information systems

Threats against hotel information systems can be targeted against their various modules (information module, data module, and administrative input module). The threats that can harm hotel information systems can be classified into four levels:

First level - detects the modules for receiving and transmitting information in hotel information systems, as well as types of functions working on the processing of information to the database.

Second level - detects the predicted opportunities for creating and running their own type of programs with multiple levels of information processing functionality.

Third level - covers all possible management methods for each function of the hotel information system, which can influence the basic and programmatic insurance of the system.

Fourth level - detects all possible operators (persons having access to the system through a username and a password), working on the design, development, implementation and the use of the hotel information system. This kind of attack is the most dangerous, but it is hardly noticeable.

Most attacks can be categorized into one of the following six classes (Valentina Voinohovska, 2014):

• Malware: This is a basic term for software, designed for malicious purposes. It includes virus attacks, worms, adware, Trojan horses, and a spyware. These are the most common dangers for a computer system.

• Security Breakthrough: This group of attacks includes any attempted unauthorized access to the system. This includes passwords disclosure, rights overrun, server intrusion, all activities that most commonly associate with the term "hacking."

• DoS: a type of attack that causes a service loss or a failure of the network to function.

• Web Attacks: any attack that attempts to break or change a web site. Two of the most common attacks of this type are SQL injection (SQLi) and XSS (cross-site scripting). The first one is a web attack method by which the hacker can deploy and execute SQL commands on the site's database. The XSS attack uses the vulnerability of the application to "insert" an unwanted code being executed in the end user's browser.

- HTTP ‘Hijacking session’: these attacks allow malicious users to access other data belonging to a user by hijacking their session’s identifier. DNS poisoning is another type of attack, which compromises the DNS server so that users can be redirected to malicious websites, including phishing websites.
- Phishing attacks are the most common form of Internet fraud. This is a widely used technique by computer criminals for obtaining important information. They aim to trick people into providing important personal information, most notably credit card details and bank accounts.

4. **Decisions to overcome cyber-attacks against hotel information systems.**

The implementation and operation of a hotel information system leads to a serious risk for the information security collected in it, both to the company and the user. Like any other system, the hotel system also has vulnerabilities that can cause malicious attacks.

Every year, hotel information systems collect more and more information for both their customers and their partners. Addressing security issues will give more security and reliability to the information in it.

According to ESET specialists, the first step of protection relates mainly to the users attention - the use of licensed paid security solutions that regularly update the operating systems and applications used. Last but not least, users have to pay much attention to suspicious emails or social media links.

Other specialists (PCWorld.bg, 2014) suggest:

- downloading apps only from official sources;
- avoiding jailbreaking techniques for breaking devices;
- updating your mobile software to the latest version.

Blue Coat experts (Blue Coat, 2015) recommend:

- to invest money in an application, created by a reliable provider which will clearly display what happens to the device;
- to stop downloading apps from unofficial sources;
- to stop searching for jailbroken or phony versions of well-known applications;
- to stop searching for pornographic materials;
- to stop performing jailbreaks/roots, which cut out the incorporated in the device security mechanisms;
- to pay more attention to connecting to insecure wireless networks;
- to verify the genuine reference of the links.

Mcfee specialists recommend (Snell, 2016):

- to turn off the automatic MMS retrieval;
- to regularly and correctly update devices;
- to stop opening anonymous messages;
- to use an integral protection software;
- to download apps only from official app-stores;

- to be constantly on alert while surfing the network;
- to review the apps reputation report.

5. Conclusion

In conclusion, we can summarize that mobile technology used in tourism brings together many services by offering its users easier access and saving time and resources. They are constantly evolving and improving, and this trend will continue in the future. Technical innovations have paved the way for mobile devices to penetrate the workplace. Many tourist managers choose to use mobile information technology, often without taking into account the risk or business management implications associated with these devices. Losing, stealing, or infecting sensitive data, malware that can affect not only the mobile device itself, but also the corporate network, and the way workers use the devices are just some of the risks associated with this type of technology.

The managers of tourist sites should estimate the benefits and take into account the additional risks when considering the use of mobile computing devices in their environment. Following the awareness of the benefits and the risks, it is appropriate to use an effective management system to ensure that processes and the course of conduct are in place, implement, and understand the suitable levels of security to avoid loss of data.

The progress in information technology, and in particular in mobile technologies, undoubtedly has its positive and negative aspects. Apparently, the regular and widespread use of mobile information technologies solves the safety problem of mobile technologies in tourism, gives the tourism industry a boost to grow and to become even more accessible.

UDC 004.896

Applying agent-based technologies to malicious software simulation

Chumachenko K. I.[1], student, Chumachenko D. I.[2], Associate Professor, PhD, Candidate of Engineering Sciences
[1]South-Eastern Finland University of Applied Sciences, Mikkeli, Finland
[2]National Aerospace University, Kharkiv, Ukraine

Annual losses of hundreds of millions of dollars from cyberattacks confirm the danger of epidemics of the malware. Penetrating into hundreds of thousands of computers around the world, malware destroy a huge amount of important information, literally paralyzing the work of the largest commercial and government organizations. In modern conditions, the computer infrastructure is more vulnerable than ever before, because the rate of development of technology is much higher than the speed of development of protective measures.

In order to protect from attacks of possible worms in the future, it is important to understand their various properties: patterns of propagation throughout the life cycle; development of patches; userawareness and other human factors; network topology, etc. The development of an accurate model of the Internet worm will give an idea of its behavior. This will identify weaknesses in the dynamics of the network worm, as well as create a forecast of its distribution in order to assess damage from the activity of the worm.

Analysis of traditional deterministic models have shown that they do not take into account the stochastic nature of the behavior of malicious software. To eliminate these shortcomings, the development of multi-agent imitation modeling, which allows to consider a large number of factors affecting the distribution of malicious software is needed. The adequacy of the simulation model depends to the large extent on the number of agents in the system. Using large populations and detailed properties of agents leads to the need to use the most advanced information tools and technologies, in particular, algorithms that are optimal in the number of machine operations performed.

The proposed method of multi-agent simulation was implemented using the example of the distribution of the Code Red II network worm. Analysis of the developed agent-based model showed that there are two factors that affect the spread of network worms: the dynamic countermeasures taken by the ISP and users, and the slowing down of the spread of the network worm, as the rapid proliferation of malicious software causes slowdowns and problems with some routers. Given the dynamic aspects of human countermeasures and the variable rate of infection, we obtained a more accurate model of network worm spread, in comparison with deterministic analytical models. The results of the simulation, as well as a numerical solution, show that the constructed agent-based model coincides to a high degree with the observed real data of the Code Red II worm.

UDC 004.056.55.003.26

Security intruder model in quantum cryptography systems

Gnatyuk S.[1], DSc, Associate Professor,
Zhmurko T.[1], PhD, Associate Professor,
Kinzeryavyy V.[1], PhD, Associate Professor,
Yubuzova K.[2], Tutor, PhD Student
[1]*National Aviation University, Kyiv, Ukraine*
[2]*Satbayev University, Almaty, Kazakhstan*

Quantum cryptography (QC) systems become increasingly popular, taking into account the rapid development of information technologies and the emergence of new threats associated with it (cyberthreats). The main advantages of QC methods are: ability to accurately identify intruder and, in some cases, information-theoretic security. But along with the QC and others quantum technologies development, new cyberattacks on them are appearing regularly. Since QC is new direction enough, there is currently no model of a security intruder. So, taking into account the subject relevance intruder's model in quantum systems is developed in this work. The main and primary task of the intruder is unauthorized access to information and communication system (ICS) resources for different purposes. An exception is the case when an intruder accidentally implements unauthorized access (Fig. 1) – in this case, he is an accidental infringer, but not an intruder (attacker). Especially dangerous can be intruders who are under the influence of criminal organizations, businesses, political organizations, security services, etc. Permissible actions for such violators may be the desire to obtain certain data for further use, modification or destruction in order to achieve certain conditions for themselves or the structures under whose influence they are.

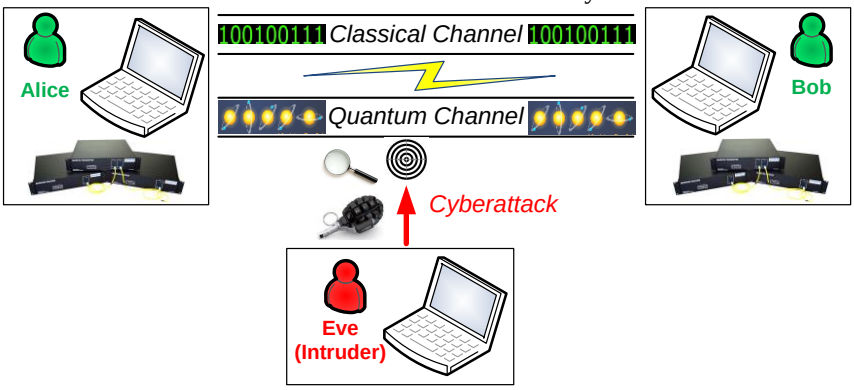


Figure 1 – Scheme of cyberattack on quantum cryptography system

It is also worth noting that the intruder can be either internal (from the

number of employees, for example) or external (located outside the controlled area of the ICS or penetrated it in by unauthorized way). The intruder's qualification is a set of certain knowledge and his abilities, which he uses for unauthorized access implementation to ICS resources. Several types of intruder's qualifications can be noted, which will allow to successfully implement threats to particular quantum systems, so intruders has: 1) information about functional features of quantum systems in general, know how to use regular means of appropriate ICS; 2) high level of knowledge and experience in the maintenance of similar ICS or quantum systems; 3) high level of knowledge in the field of computer technology (cryptography, theory of algorithms, parallel computing, etc) and programming for quantum systems or their analogues; 4) knowledge about quantum physics, quantum optics, etc., as well as the skills of working with the equipment used in such systems; 5) access to global computer networks, a supercomputer or a quantum computer, which can, for example, carry out a power cyberattack.

Possibilities of intruder concerning his influence on quantum systems can be represented in the form of such hierarchical classification – intruder has ability to: 1) launch a limited set of software that implements certain functions for processing classical or quantum information; 2) create his own software and modify the existing, which will create new functions for processing the classical and quantum information to further receive some necessary information; 3) control the functioning of quantum system, that is, directly affect the software, the composition and configuration of ICS technical support; 4) like legitimate users (all the capabilities) – can develop and implement the technical means of ICS, as well as integrate his own technical means in order to further obtain useful information for himself.

It should be emphasized that the theoretical analysis of the quantum protocols security, as a rule, is based on the fact that the intruder has technical capabilities, limited only by the quantum mechanics laws, and not by current level of technology development. The intruder's goals in quantum systems are the creation of new and improved existing methods of cryptanalysis (classical and quantum). The basis for the targeted implementation of unauthorized access to ICS are often selfish motives, although sometimes there is a desire for self-expression or moral harm to legitimate users. Intruder may use a combination of relevant knowledge, skills and abilities, for example knowledge of:

– *mathematical apparatus* will allow him to create new cryptanalysis methods in accordance with the current level of security;

– *programming (coding) languages* will allow the infringer to implement established cryptanalysis methods, as well as modify the existing software of legitimate users;

– *quantum physics* will make it possible to select appropriate interception methods and to obtain useful information;

– *social engineering* can allow the intruder without thorough knowledge of mathematics, physics and programming to easily bypass the information

security system, both classical and quantum.

By the nature of intruders' actions, they can be classified as follows:

1) Accidental Intruder, who mistakenly, unintentionally and unknowingly violated the ICS security policy;

2) Patient Intruder, who violated the security policy of a particular segment or whole ICS consciously, deliberately, but without decisive action, masking and selecting access attributes of legitimate users to overcome access controls;

3) Decisive Intruder – his purpose is to break one of the ICS information resources characteristics. He seeks to overcome all existing access restrictions and to have direct access to ICS resources in order to intervene in the system, modify or destroy information (classical or quantum), obtain necessary data etc;

4) Remote Intruder, analyzes technical channels of information leakage, affects remotely with the help of special means on local and distributed ICS, including quantum and classical channels.

For a more detailed security intruder model building, based on a specific ICS, it is also recommended to classify intruders by the following features: preparation for overcoming of ICS physical protection, nature of behavior, the level of awareness about the cyberattack object, methods and means used, place of implementation of the cyberattack etc.

Conclusions. The developed model of intruder in QC systems allows to determine a set of various measures that need to be further implemented to provide reliable security with the help of specific QC systems.

References

1. Korchenko O. Quantum Secure Telecommunication Systems / Korchenko O., Vasiliu Ye., Gnatyuk S. et al. // Telecommunications Networks – Current Status and Future Trends (ed. by J.H. Ortiz). – InTech, 2012. – P. 211-236.

2. Методы перехвата информации в информационно-коммуникационных системах на основе квантових технологий / А.Г. Корченко, Е.В. Василиу, Т.А. Жмурко, С.А. Гнатюк // Информационные технологии и системы в управлении, образовании, науке: Монография [под. ред. В.С. Пономаренко]. – Х.: Цифрова друкарня № 1, 2013. – С. 98-110.

3. Василиу Е.В. Безопасные системы передачи конфиденциальной информации на основе протоколов квантовой криптографии : монография / Е.В. Василиу, В.Я. Мильчевич, С.В. Николаенко, А.В. Мильчевич. – Харьков: Цифровая типография № 1, 2013.– 168 с.

4. Розширена класифікація квантових методів безпечної комунікації / С.О Гнатюк, Т.О. Жмурко, Ю.Я. Поліщук, Н.А. Сєйлова // Наукоемкие технологи в инфокоммуникациях: обработка информации, кибер-безопасность, информационная борьба: Монография [под. ред. В.М. Безрука, В.В. Баранника]. – Х. : Лидер, 2017. – С. 467-482.

UDC 004.451

Meltdown and Spectre vulnerabilities

Pashinskikh V.V., student of 3rd course
Scientific supervisor – Konoplitska-Slobodeniuk O.K., teacher
Central Ukrainian National Technical University, Kropyvnytskyi

Meltdown and Spectre (CVE-2017-5754, CVE-2017-5753, CVE-2017-5715) are hardware-related vulnerabilities in most of modern processors. They are really so serious vulnerabilities that they had to come up with their own "brands" to facilitate the promotion and dissemination of information about them. At the moment, they are the most serious problems in the field of information security.

Meltdown (CVE-2017-5754) exploits uses effect of out-of-order execution on modern processors to read kernel memory, that may contain confidential information, encryption keys, passwords, etc.

Spectre (CVE-2017-5753 and CVE-2017-5715) is very similar to Meltdown: it also works with cache and the mechanism for transitions predicting. But, unlike Meltdown, Spectre is more difficult to implement. This vulnerability can force any process to share the contents of its own memory. By other words, Spectre can get into the memory of another process with a similar set of instruction sequences, “erasing the line” between isolated applications.

What devices are affected?

Potentially vulnerable almost all computers, laptops (and their predecessors - netbooks, chromebooks, etc.), tablets, smartphones, NAS or DAS, and even modern smart TVs, as well as servers and a bunch of other equipment. Vulnerable may be almost all the technique that surrounds us.

For example, all devices with Intel processors (Core, Xeon, Celeron and Pentium), processors with newest ARM Cortex-A75 cores and all devices running iOS with ARM processors are vulnerable to these vulnerabilities.

But according to the representatives of AMD, the company's processors are almost unaffected by Spectre attacks through gadgets. Experts believe that this is most likely due to the special implementation of the architecture of speculative execution of instructions.

How it works?

Researchers from Google Project Zero managed to discover three mechanisms of attacks, effectively working in different conditions. All of them have one goal: to give the process with the usual user privileges the ability to read data from the protected parts of the kernel memory containing sensitive information such as cryptographic encryption keys, passwords, etc. Tests have shown that attacks can be successfully performed from the virtual machine to physical memory of host computer, and other virtual machines hosted on the same device.

The Meltdown attack uses exception handling or suppression to run a sequence of instructions. They obtain a secret value and change the microarchitectural state of the processor, based on this value. It forms the sending part of a microarchitectural covert channel. Then, receiving side reads the microarchitectural state, makes it architectural and after that - recovers the secret value.

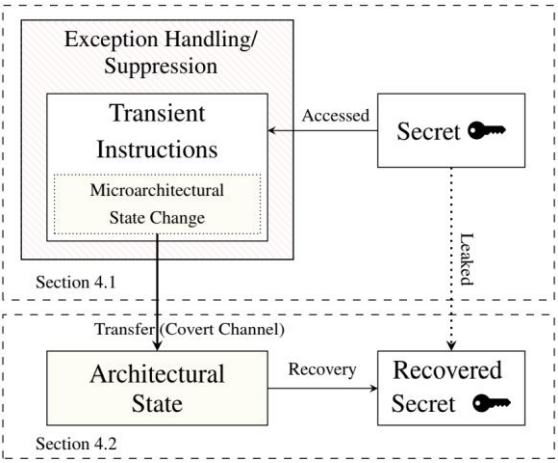


Image 1. The Meltdown attack uses exception handling, to run a sequence of instructions.

The biggest danger of vulnerability is almost complete independence from the operating system: antivirus cannot detect such malicious code. Also Meltdown leaves no traces in the system, which complicates the task of finding malware that has already managed to cause damage.

Conclusions

We examined here Meltdown and Spectre vulnerabilities, which is currently the biggest vulnerabilities of all devices surrounding us. Using them a hacker can access sensitive information such as passwords and encryption keys without requiring any software vulnerability and independent of the operating system.

References

1. Meltdown / Lipp M., Schwarz M., Gruss D. [et al.]. [Electronic resource]. – Access mode: https://meltdownattack.com/meltdown.pdf

2. Spectre / Kocher P., Genkin D., Gruss D. [et al.]. [Electronic resource]. – Access mode: https://spectreattack.com/spectre.pdf

3. Horn J. Reading privileged memory with a side-channel / Project Zero at Google. [Electronic resource]. – Access mode: https://googleprojectzero. blogspot.co.at/2018/01/reading-privileged-memory-with-side.html

UDC 621.391

Security information system based on chaotic system

Rusyn V.[1], Pribylova L.[2], Dimitriu D.[3], Guzan M.[4]
[1] *Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine*
[2] *Masaryk University, Brno, Czech Republic*
[3] *Alexandru Ioan Cuza University, Iasi, Romania*
[4] *Technical University of Kosice, Kosice, Slovakia*

Chaotic systems allow masking information carrier for a certain chaotic law. Since mathematical models describing the work of transmitting-receiving units of modern chaotic information systems have become more complex, modeling of information properties of deterministic chaos is becoming more topical.

Rossler chaotic system is one of chaotic systems used for security of the information carrier, and described by three nonlinear differential equations:

$$\begin{aligned} \frac{dx}{dt} &= -y - z, \\ \frac{dy}{dt} &= x + ay, \\ \frac{dz}{dt} &= b + z(x - c), \end{aligned} \qquad (1)$$

where x, y, z – dynamic variables that determine the phase space,

a, b, c – system parameters [1-3].

The software has been created in one of the most modern system LabView (LabVIEW 2015 (64 bit) for Windows). Figure 1 and figure 2 shows program interfaces for transmitting and receiving of masking signal based LabView with using TCP/IP protocol.

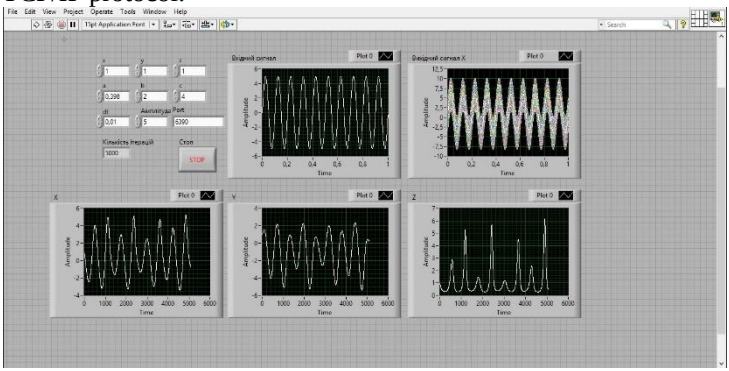


Figure 1 – Program interface that realise transmitting masking signal

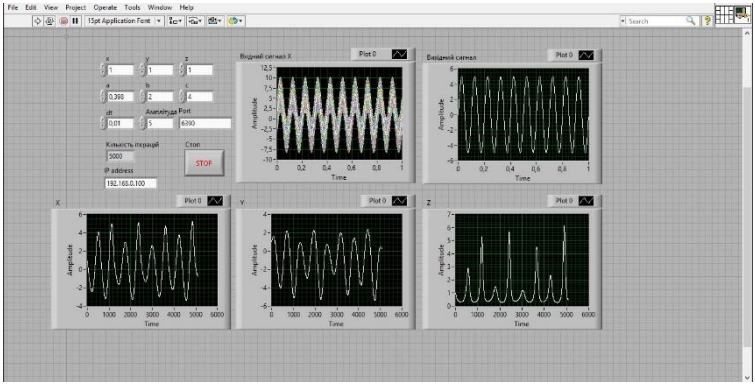


Figure 2 – Program interface that realise receiving masking signal

Chaotic masking of the information carrier is provided by blending chaotic signal with the information. As an information (input) signal was used a sinusoidal signal (useful signal) with amplitude of 1 V and parameters $x = y = z = 1$, $a = 0{,}398, b = 2, c = 4$. Dynamic variables and system parameters are the keys for the masking information.

The principle of the work is as follows: one computer serves as a server for transmitting a disguised information signal, which records the initial conditions, system parameters, port of the channel. Another computer is a client, that is to receive and restore information where identical initial conditions, system parameters are entered, and the IP address of the server is specified.

Conclusions. The develop scheme in LabView programming environment allows the software to generate a chaotic attractor can be used in modern systems transmitting and receiving information. The software interface demonstrates masking and decryption of information carrier of the chaotic Rossler system.

References

1. Aceng Sambas, Mada Sanjaya, Mustafa Mamat & Halimatussadiyah (2013). Design and analysis bidirectional chaotic synchronization of Rossler circuit and its application for secure communication. *Appl. Math. Sci.*, 7(1-4), 11-21.

2. Aceng Sambas, Mada Sanjaya WS & Halimatussadiyah (2012). Unidirectional Chaotic Synchronization of Rossler Circuit and Its Application for Secure Communication. *WSEAS Transactions on Systems*, 11 (9), 506-515.

3. Rössler O.E. (1976). An equation for continuous chaos. *Physics Letters A*, 57 (5), 397-398.

УДК 004.056.5

Секторальные интелектуализированные экспертные системы поддержки решений по кибербезопасности

Ахметов Б.С.[1], д.т.н., профессор,
Лахно В.А.[2], д.т.н., профессор,
Картбаев Т.С.[3], PhD, доцент,
Досжанова А.А.[3], PhD, доцент
[1]*Казахский национальный педагогический университет имени Абая, г. Алматы, Казахстан*
[2]*Европейский университет, г. Киев, Украина*
[3]*Алматинский университет энергетики и связи, г. Алматы, Казахстан*

Аннотация. В работе рассматривается возможность интеграции различных локальных экспертных и систем поддержки принятия решений для задач защиты информации (ЗИ) и обеспечения кибербезопасности для разных объектов информатизации. Анализируется возможность секторального объединения и совместного использования баз знаний подобных интелектуализированных систем. Описана модель подсистемы управления выводом знаний в секторальных экспертных и системах поддержки решений для задач киберзащиты объектов информатизации.

1. Введение

На начальном этапе практического использования систем поддержки принятия решений (СППР) [1, 2] и экспертных систем (ЭС) [3], в частности адаптивных [4], в задачах защиты информации (ЗИ) и кибербезопасности (КБ), их архитектуры соответствовали классическому варианту [1, 2, 5]. По мере усложнения задач, связанных с обеспечением КБ, появились проблемы, которые уже невозможно разрешить в рамках классических локальных СППР и ЭС (СППРЭС) по ЗИ. Например, когда в процессе логического вывода возникает необходимость интегрировать заключения локальных СППР или ЭС. Если СППРЭС изначально разрабатывались только для решения узкопрофильных задач, как например, поддержка решений по выбору аппаратно-совместимых рациональных вариантов комплексных систем защиты информации (КСЗИ) [3] или задач экспертного анализа сложных признаков, выявленных в процессе целевой атаки [4], расширить диапазон решений (для отличных от начальных вариантов) не представляется возможным.

Актуальность настоящего исследования определяется, прежде всего, состоянием проблематики комплексного внедрения в контуры ЗИ и КБ критически важных компьютерных систем (КВКС) СППРЭС, объединённых в секторы (кластеры [6]). Это обуславливает необходимость дальнейшего развития методологического аппарата, и принципов создания секторальных интеллектуализированных СППРЭС

для задач ЗИ и КБ КВКС.

2. Анализ литературных данных и постановка проблемы

Увеличивающаяся сложность кибератак, прежде всего целевых, на КВКС, вызвала интерес к разработке интеллектуализированных СППРЭС в области КБ [7, 8]. Необходимость оперативного принятия решений, связанных с обеспечением КБ КВКС, сделала перспективными исследования по развитию секторальных СППРЭС, способных интегрировать свои запасы познаний в рамках решения поставленных задач [7].

В работах [9, 10] был проанализирован опыт применения ЭС и СППР в задачах оценки рисков для КБ КВКС. Область применения базы знаний (БЗ) данных систем ограничилась только оценкой рисков. В работах [11, 12] описаны СППР, используемые для принятия решений в недостаточно структурированных ситуациях оценки КБ КВКС. Пока исследования [12] не доведены до аппаратно-программной реализации. Опыт применения интелектуализированных СППР и ЭС в задачах менеджмента ЗИ и КБ на отдельных предприятиях представлен в [13, 14]. Область применения данных систем ограничилась только задачами управления ИБ. В работах [15, 16] проанализирован опыт внедрения коммерческих СППР и ЭС по ЗИ и КБ. Авторы отмечают, что коммерческие системы имеют закрытый характер, и их приобретение отдельными предприятиями связано со значительными финансовыми затратами. В показано [17], что проблематика внедрения СППРЭС в контексте их многозадачности, системно не рассматривались.

При этом остается нерассмотренной проблематика теоретического обоснования методологии создания и применения секторальных интелектуализированных СППРЭС в задачах КБ КВКС.

3. Цель и задачи исследований

Цель работы – развитие методологии создания секторальных интелектуализированных СППРЭС для задач ЗИ и КБ КВКС.

4. Модели и методы

В секторальных СППРЭС сектор (кластер) рассматривается как информационная единица. Сектор интегрирует возможности нескольких самостоятельных (т.е. локальных) ЭС или СППР, рис. 1. Будем полагать, что узлы сектора могут обмениваться специфической информацией, относящейся к разным задачам ЗИ и КБ. Но конечному пользователю, например, аналитику по ИБ, кластер доступен как один ресурс. Таким образом, задачей секторальной системы является распределение запросов пользователей и их преобразование для конкретных локальных СППР или ЭС по ЗИ и КБ.

Рис. 1. Структурная схема секторальной (кластерной) платформы для объединения локальных СППР и ЭС по кибербезопасности

Введем следующие обозначения: исходные (входные) данные – X; результирующие (выходные) данные – Y; W – представление множеств входных переменных во множество результирующих данных. Т.е. $X = \langle x_1,..., x_m \rangle, Y = \langle y_1,..., y_n \rangle, W = \langle w_1,..., w_n \rangle$. При этом $X \cap Y = \varnothing$.

Секторальную СППРЭС будем полагать результативной, если выполняются следующие требования:

1) $Y = w\langle X \rangle$.

2) $(\forall x_i \in X)(\exists q_1 \in x_1,..., q_i \in x_i, q_i \in x_i,..., q_m \in x_m) \times$

$\times [w(q_1,..., q_i,..., q_m) \neq w(q_1,..., q_i,..., q_m)]$.

На первом этапе обработки запроса к секторальной СППРЭС задается

набор переменных – $x_i = f_i(x_1,\ldots, x_n)$. Значения x_i необходимо получить в ходе реализации $Y^r = \langle y_1^r,\ldots,y_n^r\rangle$.

Следовательно, $y_i^r = z_i(x_{i1},\ldots,x_{im})$.

Множество функций $Z^1 = \langle z_1,\ldots,z_m\rangle$ формируют представление перечня $X^1 = \bigcup_{i=1}^{m} x_i$ в результирующий список $Y^r = Z^1(X^1)$, где X^1 – перечень переменных конечного ранга функционального структурного модуля секторальной СППРЭС. Т.е. $u = (X, Y, W)$: $X^1 = X^{u1} \bigcup Y^1$, где $X^{u1} \bigcap Y^1 = \varnothing$.

Полагаем, что X^1 содержит переменные, являющиеся исходными данными для модуля U^1. В список Y^1 включаются параметры, подлежащие вычислению в процессе работы модуля U^1.

Перечень Y^1 отображается через новый список. Например, так:

$$Y^1 = Z^2\left(X^2\right), \text{ где } X^2 = X^{u2} \bigcup Y^2,\ X^{u2} \bigcap Y^2 = \varnothing.$$

Операции продолжаются до тех пор, пока список переменных, не принадлежащих к X^1, для ранга k не исчерпан.

Описанная модель может быть представлена в виде графа переменных $x_i = f_i(x_1,\ldots, x_n)$, рис. 2. Вершины графа, обозначенные красными точками, соответствуют результирующим переменным.

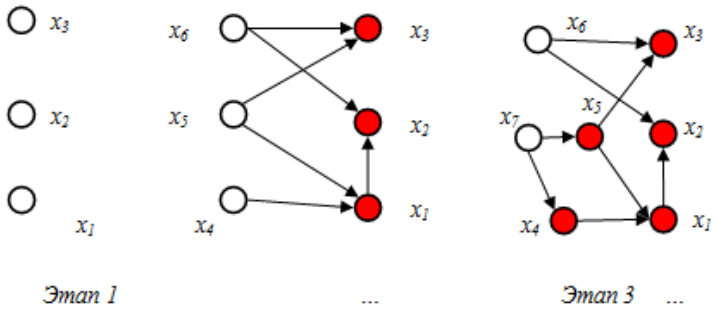


Рис. 2. Этапы решения

На этапах решения т.е. каждом шаге построения графа к неисходным вершинам проводят стрелки. Полагаем процесс законченным в случае, когда все неисходные вершины соединены стрелками. Корректным полагаем исход, если в результирующем графе отсутствуют циклы. Предлагаемый подход дает возможность увязывать знания из локальных СППР и ЭС для смежных задач и предметных областей (например, кибербезопасность, выбор технических средств защиты, стоимость СЗИ, оценивание рисков для ИБ и т.п.). Кроме того, существует возможность составление дерева логического вывода для секторальной СППР или ЭС

по ЗИ и КБ КВКС.

Развитием данного направления исследований может стать совершенствование взаимодействия алгоритма и программных модулей секторальной СППР “CLSC” с модулями системы «DMSSCIS» [17].

7. Выводы

1. Рассмотрены перспективы интеграции различных экспертных и систем поддержки принятия решений для задач защиты информации и обеспечения кибербезопасности на основе их секторального агрегатирования и совместного использования баз знаний. Предложена модель подсистемы управления выводом знаний в секторальных ЭС и СППР для задач ЗИ и КБ КВКС.

2. Предложена модель и проведены вычислительные эксперименты по исследованию системы управления знаниями существующих локальных СППР и ЭС по ЗИ, интегрируемых в кластер. Проведено тестирование прототипа секторальной (кластерной) системы поддержки решений по обеспечению кибербезопасности КВКС. Выполнена оценка эффективности использования секторальной СППР “CLSC” в сравнении с локальными ЭС и СППР, используемыми в задачах поддержки приятия решений по ЗИ и КБ.

Список литературы

1. Akhmetov, B., Lakhno, V., Boiko, Y., Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity, *Eastern-European Journal of Enterprise Technologies*, 1(2 (85)), 4–15. DOI: 10.15587/1729-4061.2017.90506.

2. Rees, L. P., Deane, J. K., Rakes, T. R., Baker, W. H. (2011). Decision support for Cybersecurity risk planning. *Decision Support Systems*, 51(3), 493–505. DOI: 10.1016/j.dss.2011.02.013.

3. Chang, L. Y., Lee, Z. J. (2013). Applying fuzzy expert system to information security risk Assessment-A case study on an attendance system. *IEEE 2013 International Conference on Fuzzy Theory and Its Applications (iFUZZY)*, 346–351. DOI: 10.1109/iFuzzy.2013.6825462.

4. Lakhno, V., Tkach, Y., Petrenko, T., Zaitsev, S., Bazylevych, V. (2016). Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks. *Eastern-European Journal of Enterprise Technologies*, 6 (9), 32–44. DOI: 10.15587/1729-4061.2016.85600

5. Goztepe, K. (2012). Designing Fuzzy Rule Based Expert System for Cyber Security, *International Journal of Information Security Science*, 1(1), 13–19.

6. Mahmood, T., & Afzal, U. (2013). Security Analytics: Big Data Analytics for cybersecurity: A review of trends, techniques and tools. *In Information assurance (ncia), 2013 2nd national conference on* (pp. 129-134). IEEE.

7. Kim, K., Kim, I., Lim, J. (2017). National cyber security enhancement scheme for intelligent surveillance capacity with public IoT environment, *The Journal of Supercomputing*, 73(3), 1140–1151. DOI: 10.1007/s11227-016-1855-z.

8. Medhat, K., Ramadan, R. A., Talkhan, I. (2017). Security in Mission Critical Communication Systems, Multimedia Services and Applications in Mission Critical Communication Systems, 270. DOI: 10.4018/978-1-5225-2113-6.ch012

9. Radziwill, N., Benton, M. (2017). Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management [Electronic resource] Available at: https://arxiv.org/ftp/arxiv/papers/1707/1707.02653.pdf

10. Jalali, M., Siegel, M., Madnick, S. (2017). Decision Making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment. [Electronic resource]. Available at: https://arxiv.org/ftp/arxiv/papers/1707/1707.01031.pdf.

11. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F. (2016). Decision support approaches for cyber security investment, *Decision Support Systems*, 86, 13–23. DOI:10.1016/j.dss.2016.02.012.

12. Lakhno, V., Petrov, A., & Petrov, A. (2017). Development of a Support System for Managing the Cyber Security of Information and Communication Environment of Transport, *In International Conference on Information Systems Architecture and Technology* (pp. 113–127). Springer, Cham.

13. Benaroch, M. (2017). Real Options Models for Proactive Uncertainty-Reducing Mitigations and Applications in Cybersecurity Investment Decision-Making. *Information Systems Research*. P. 39.

14. Wagner, N., Şahin, C. Ş., Winterrose, M., Riordan, J., Pena, J., Hanson, D., & Streilein, W. W. (2016, December). Towards automated cyber decision support: A case study on network segmentation for security. *Computational Intelligence (SSCI), 2016 IEEE Symposium Series on* (pp. 1–10). IEEE.

15. Atymtayeva, L., Kozhakhmet, K., & Bortsova, G. (2014). Building a knowledge base for expert system in information security. In *Soft computing in artificial intelligence*, 57–76. Springer, Cham.

16. Silva, M. M., de Gusmão, A. P. H., Poleto, T., e Silva, L. C., & Costa, A. P. C. S. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management*, 34(6), 733–740.

17. Tamjidyamcholo, A., Baba, M. S. B., Shuib, N. L. M., & Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security*, 43, 19–34.

18. Lakhno, V., Kozlovskyi, V., Boiko, Y., Mishchenko, A., & Opirskyy, I. (2017). Management of information protection based on the integrated implementation of decision support systems. *Eastern-European Journal of Enterprise Technologies*, 5(9 (89)), 36–42.

19. Lakhno, V., Boiko, Y., Mishchenko, A., Kozlovskii, V., & Pupchenko, O. (2017). Development of the intelligent decision-making support system to manage cyber protection at the object of informatization. *Eastern-European Journal of Enterprise Technologies*, (2 (9)), 53–61.

УДК 004.056.55

Безпека інформації у хмарних сховищах

Берладін В.К., студент 3 курсу
Науковий керівник – Конопліцька О.К., викладач
Центральноукраїнський національний технічний університет, м. Кропивницький

В наш час технології розвиваються дуже швидко, яскравим прикладом цього є хмарні сховища даних. Вони дуже швидко розповсюджуються, адже дозволяють отримати доступ до Ваших даних з будь-якої точки світу, де є доступ в мережу інтернет. Хмарні сховища підтверджують той факт, що час флешок та компакт – дисків минув. В епоху хмарних сховищ збереження безпеки даних є одним з найважливіших аспектів в роботі хмарних сервісів.

Що таке хмарне сховище?

Хмарне сховище – це служба, яка дозволяє зберігати дані шляхом їх передачі по Інтернету або іншої мережі в систему зберігання інформації, що обслуговується третьою стороною. Існує низка відомих постачальників хмарних послуг, найвідоміші з них: iCloud, Google Диск, Dropbox і OneDrive, всі з яких виконують загально аналогічну функцію. Користувач орендує місце зберігання у провайдера, а потім надсилає копії своїх файлів через Інтернет на відповідний сервер даних, який записує інформацію. Для завантаження або зміни інформації на сховищі використовується веб-інтерфейс.

Як і у всіх нових формах зберігання даних, існує ряд переваг та недоліків хмарних сховищ, основними з яких є:

Переваги

1. Поліпшення ефективності: як з точки зору віддаленого доступу, так і більш гнучких робочих умов; користувачі мають доступ до даних з будь-якої точки доступу в Інтернеті без необхідності переміщення фізичного обладнання.

2. Краща співпраця: системи хмарного зберігання інформації дозволяють одним користувачам надавати доступ до своїх даних, тобто можна редагувати документ в режимі реального часу для полегшення співпраці та подальшого підвищення ефективності.

3. Резервне копіювання та відновлення: оскільки всі дані зберігаються в Інтернеті, резервне копіювання та відновлення значно простіше, ніж фізичне зберігання.

Недоліки

1. Залежність: також відома як "lock-in-vendor-in", означає труднощі з переходом від одного постачальника хмарних сховищ до іншої через величезний експорт даних.

2. Інший аспект ризиків: як згадувалося, як хмарний користувач ви відмовляєтеся від повного контролю над вашими даними, які більше не зберігаються виключно на фізичній машині, що знаходиться у вашому розпорядженні.

Захист паролів та конфіденційної інформації

Перш за все, користувачі повинні переконатися, що паролі, які захищають їх облікові записи в хмарі, є належним чином захищені; уникайте очевидних наборів символів, таких як 123456, які продовжують використовувати користувачі, незважаючи на попередження про слабку надійність. На щастя, більшість постачальників хмарних сервісів змушують користувачів дотримуватися певних правил для паролів, таких як «один символ та один великий символ, один номер і щонайменше 8 символів» проте в кількох випадках це все ще дозволяє користувачеві вибирати з численних поширених варіантів, наприклад «Pa55word ». Щоб бути більш захищеними, використовуйте випадкову фразу, яка складається із загальних слів або чисел, які легко запам'ятати, але для машини дуже важко підібрати такі комбінації.

Зрозуміло, що кількість паролів і частин інформації користувачів, що потрібно запам'ятовувати, може виявитись великою. Таким чином, користувачі повинні брати до уваги використання менеджера паролів - програмний додаток, який зберігає та організовує паролі в зашифрованому форматі. Найвідомішими менеджерами паролів є: Robo Form і Last Pass.

Існує очевидна небезпека, пов'язана з використанням менеджерів паролів, тому що зловмисник повинен лише отримати свій основний пароль, щоб отримати доступ до всіх ваших облікових записів і заволодіти ними.

Двофакторна аутентифікація

Інший спосіб покращити безпеку облікового запису – це впровадження або активація додаткових функцій, зокрема двофакторної аутентифікації, що значно ускладнює отримання доступу та викрадення особистих даних особи. Ця додаткова функція безпеки може бути увімкнена у всіх основних постачальників хмарних сервісів. У таких системах повідомлення може бути довгостроково активно або одноразовим, однак останній є більш безпечним, створюючи дуже обмежене вікно, під час якого зловмисник може перехопити і використовувати пароль з СМС.

Висновок. На сьогоднішній день не існує засобу для повного захисту інформації, що зберігається як локально, так і в хмарі. Зловмисники прагнуть отримати доступ до конфіденційної інформації, збільшуючи зусилля та ресурси відповідно до компанії, або людини, інформацією яких хочуть заволодіти. На жаль, існує постійно зростаюча кількість варіантів для "хакерів" для отримання несанкціонованого доступу, при цьому хмарні сховища представляють собою особливу комбінацію ризиків.

Список літератури

1. Захист даних в хмарних технологіях [Електронний ресурс].– Режим доступу: http://conf.vntu.edu.ua/allvntu/2013/inaeksu/txt/tytarchuk.pdf

2. Климентьев И. П. Введение в Облачные вычисления / И. Климентьев, В. Устинов. – М.: УГУ, 2009. – 233 с.

3. Бойко А., Бердник А. Методы защиты виртуальной среды. Программный комплекс для проведения автоматизированного аудита виртуальной среды на предмет наличия ошибок в конфигурации безопасности/ [Електронний ресурс]. – Режим доступу: http://cyberleninka.ru/article/n/metody-zaschity-virtualnoy-sredyprogrammnyy-kompleks-dlya-provedeniya-avtomatizirovannogo-audita-virtualnoy-sredy-na-predmet

УДК 004.04

Применение блокчейн технологии в механизмах аутентификации

Биличенко Д.Г., студент 5 курса, Витюк К.Ю., студентка 5 курса
Харьковский национальный университет радиоэлектроники, г. Харьков

Текущая система аутентификации, построенная на логинах и паролях, довольно неудобна. Люди постоянно забывают пароли – 37% пользователей обращаются за помощью по этому поводу в течении месяца как минимум на одном вебсайте, по данным Deloitte. Для того, чтобы не забывать их, люди стараются использовать максимально простые комбинации одновременно на нескольких сайтах. Поэтому база из 10000 самых популярных паролей дает доступ к 98% всех аккаунтов, при этом средний пользователь использует только 5 разных паролей для доступа к 26 сервисам. Исходя из этой статистики актуальным есть развитие технологий многофакторной аутентификации.

Аутентификация имеет жизненно важное значение для всех форм дистанционного общения. Отсутствие аутентификации открывает дверь к атакам «человек посередине». Один из методов организации многофакторной аутентификации – использование технологии блокчейн.

Модель аутентификации, основанная на технологии блокчейн, позволяет пользователям действительно идентифицировать и подтверждать открытые ключи друг друга. Это исключает угрозу «человек посередине» и попытки манипуляции любого рода как на стороне сервера, так и со стороны третьих лиц.

Блокчейн – это распределенная база данных, в которой хранилища данных не связаны общим процессором. Блокчейн представляет собой список упорядоченных записей, называемых блоками. Каждый последующий блок имеет временную метку и ссылку на предыдущий. Пользователи не могут редактировать части цепочки. Права доступа контролируются при помощи системы шифрования. У каждого пользователя имеется собственный набор приватных ключей, необходимых для записи. Программное обеспечение следит за синхронизацией всех копий распределенной базы данных.

Безопасность технологии блокчейн поддерживают распределенный сервер меток времени и пиринговая сеть. В результате база данных управляется в автономном и децентрализованном режиме. В этом смысле блокчейн отлично подходит для записи событий – транзакций, управления учетными данными и подтверждения происхождения.

Практичность блокчейна неоспорима во всем, что касается хранения данных и подтверждения подлинности. Потенциально эта децентрализованная система данных способна уничтожить коррупцию. В блокчейн можно записывать даты рождения людей, финансовые транзакции, отпечатки пальцев.

УДК 372.862

Особенности процесса преподавания дисциплины «Защита компьютерной информации» студентам экономического профиля подготовки

Богданова В.А., докторант І-го года обучения
Научный руководитель –Кирияк Л.Л., доктор хабилитат, к.ф.-м.н.
Тираспольский Государственный Университет, г.Кишинев, Р. Молдова

В настоящее время на постсоветском пространстве специалисты в области информационной безопасности готовятся по нескольким направлениям подготовки: криптография, компьютерная безопасность, организация и технология защиты информации, комплексная защита объектов информатизации, комплексное обеспечение информационной безопасности автоматизированных систем, информационная безопасность телекоммуникационных систем, противодействие техническим разведкам и т.п.. Получаемая квалификация при этом «Математик» или «Специалист по защите информации». [9]

При этом наиболее значимая необходимость в овладении информационно-коммуникационными компетенциями в области информационной безопасности наблюдается при подготовке специалистов гуманитарного, экономического, юридического профилей, тех, кто в своей профессиональной деятельности имеет непосредственный доступ к информационным системам и информации, требующим защиты.

Несанкционированное воздействие на информационно-коммуникационную сферу современного государства может привести к реализации территориальных, военных, террористических угроз. Особенно остро эта проблема проявляется в области государственного управления, финансово-кредитной, экономической сферах.

Актуальным направлением современного образования является развитие профессиональных компетенций. К одной из них относится компетенция в области информационной безопасности. Сформировать ее у экономистов, управленцев можно:

– в рамках дисциплины «Информационная безопасность» в высшей школе;

– при получении дополнительной квалификации;

– при повышении квалификации в данной области.

Дисциплина «Защита компьютерной информации» включена в вариативную часть учебных программ подготовки бакалавров по направлениям «Экономика», «Менеджмент».

Существенной проблемой преподавания становится отсутствие методической литературы по защите компьютерной информации для

вышеназванных специальностей. Подавляющее большинство учебников, учебных пособий, методических указаний, практикумов предназначены для специалистов в области криптографии либо защиты компьютерной информации [4,5-7].

О противоречиях между востребованностью в специалистах в области информационной безопасности и уровнем их подготовки говорится в работах российских авторов Абиссовой М.А., Боярова Е.Н., Ломаско, Полякова В.П., Тановой Э.В.[1-3,8,10,11]

В работе Тановой Э.В. предложены методы развития компетенций в области защиты информации у школьников. Ломаско П.С. описывает методы подготовки учителей информатики в области информационной безопасности.

Работы Полякова В.П., Абиссовой М.А. посвящены проблемам развития компетенций в области информационной безопасности в вузе у студентов обучающихся по специальностям не входящим в группу специальностей по информационной безопасности.

Поляков В.П. описал методическую систему обучения информационной безопасности как «*сложную открытую динамическую систему, которая должна охватывать все уровни, виды и направления высшего образования. Её содержательное наполнение ... должно предусматривать, помимо специальных дисциплин по основам информационной безопасности, дисперсное включение отдельных вопросов обеспечения информационной безопасности в соответствующие темы информатики, информационных и коммуникационных технологий.* [10]

Поляков В.П. предложил не только ввести обязательную учебную дисциплину «информационная безопасность», но и уделять внимание вопросам защиты информации в рамках всех учебных дисциплин, связанных с информационными технологиями, на всех уровнях подготовки: от школьного до послевузовского образования.

Большинство исследователей считают недостаточность разработанности методологических подходов к обучению основам информационной безопасности.

Существуют следующие проблемы в процессе преподавания дисциплины «Защита компьютерной информации»:

1)у студентов, обучающихся по направлениям подготовки «Экономика» и «Менеджмент», различный начальный уровень владения информационными технологиями;

2)существует много специализированной литературы и материалов, но они достаточно сложны для студентов экономического профиля подготовки;

3)происходят постоянные изменения в информационной отрасли, и знания и навыки быстро теряют свою актуальность.

4)количество аудиторных часов, предусмотренных учебным планом,

составляет 36 часов (8 лекционных и 28 практических).

Решить указанные проблемы помогает активизация самостоятельной работы студентов.

На протяжении 2012-2018 гг. была сформирована программа дисциплины «Защита компьютерной информации» для бакалавров по направлению подготовки «Экономика», «Менеджмент». В ней отражены теоретический материал, тематика лабораторных работ и направления для самостоятельной работы.

Теоретический материал состоит из тем:

– понятие информационной безопасности;

– угрозы информационной безопасности;

– каналы утечки информации;

– организационно-правовые, морально-этические средства защиты информации;

– физические и технические средства защиты информации;

– программные средства защиты информации;

– идентификация и аутентификация;

– криптография;

– электронно-цифровая подпись и алгоритм хеширования.

Предусмотрено выполнение практических работ по темам:

1)оптимизация дискового пространства;

2)политика безопасности Windows;

3)парольная защита;

4)архивация;

5)антивирусная защита информация;

6)защита usb;

7)защита текстового документа;

8)защита электронной таблицы;

Информационные технологии активно развивают социально-экономическую сферу. Проблемы информационной безопасности становятся понятны практически каждому гражданину. Необходимо усовершенствовать систему преподавания предметов связанных с информационной безопасностью студентам, обучающимся по не информационным направлениям. Развивать информационно-коммуникационные компетенции в области защиты компьютерной информации. Развитие компетентности в области информационной безопасности для всех специальностей – ключевой момент повышения безопасности государства.

Список литературы

1. Абиссова, М. А. Сервисы обучения информационной безопасности в теории и методике обучения информатике студентов гуманитарных и социально-экономических специальностей: дис. канд. пед. наук: 13.00.02 / Абиссова Марина Алексеевна. – СПб., 2006. -– 214 с.

2. Бояров, Е. Н. Концептуальные подходы к обучению специалиста информационной безопасности в университете: дис. канд. пед. наук: 13.00.02 / Бояров Евгений Николаевич. – СПб., 2008. – 151 с.

3. Димов, Евгений Дмитриевич, Методика обучения студентов вузов технологиям защиты информации в условиях фундаментализации образования, Место защиты диссертации: Москва, Код специальности ВАК: 13.00.02, Специальность: Теория и методика обучения и воспитания.– М., 2013. – 181 с.

4. Защита компьютерной информации: лаб. практикум для учащихся специальности 2-40 01 01 «Программное обеспечение информационных технологий» / сост. Н. А. Тетерукова, С. А. Апанасевич. – Минск: МГВРК, 2013. – 80 с.

5. Информационная безопасность и защита информации: учеб.пособие для студ. Высш. Учеб. Заведений / В.П. Мельников и др. – М.: «Академия», 2008. – 336 с.

6. Комплексная защита информации в корпоративных системах: учеб. Пособие / В.Ф. Шаньгин. – М.: «Инфра-М», 2010. – 592 с.

7. Коноваленко Д.А., Баженов Р.И. Разработка лабораторно-практических работ по стеганографическим и криптографическим методам защиты информации в курсе «Информационная безопасность» // Современная педагогика. 2014. № 11. [Электронный ресурс]. Режим доступа: http://pedagogika.snauka.ru/2014/11/2935 (дата обращения: 04.03.2018).

8. Ломаско, П. С. Методическая система подготовки учителя информатики в области информационной безопасности: автореф. дис. канд. пед. наук: 13.00.02 / Ломаско Павел Сергеевич. – Красноярск, 2009. – 25 с.

9. Поляков В.П. Аспекты информационной безопасности в информационной подготовке. – М.: ФГБНУ «ИУО РАО», 2016. – 135 с.

10. Поляков, В. П. Методическая система обучения информационной безопасности студентов вузов: автореф. дис. д-ра пед. наук: 13.00.08 / Поляков Виктор Павлович. – Н. Новгород, 2006. – 47 с.

11. Танова, Э. В. Формирование компетентности в области защиты информации у школьников в процессе обучения информатике: дис. . канд. пед. наук: 13.00.02 / Танова Элеонора Владимировна. Челябинск, 2005. – 173 с.

12. Хмидуллин Р.Р., Бригаднов И.А., Морозов А.В. Методы и средства защиты компьютерной информации: Учеб. пособие. – СПб.: СЗТУ, 2005. – 178 с.

УДК 004.056.5

Формалізація методу групового аналізу експертних оцінок при визначені рівня захищеності інформаційно-телекомунікаційної системи від несанкціонованого доступу

Бучик С.С.[1], д.т.н, доцент,
Нетребко Р.В.[2], викладач
[1]Національний авіаційний університет, м. Київ
[2]Житомирський військовий інститут імені С. П. Корольова, м. Житомир

В сучасних умовах, коли проходять динамічні і широкомасштабні зміни у відносинах між державами, однією із першочергових задач для проведення державної політики є захист інформації державних ресурсів. В сьогоднішній ситуації захисту інформації притаманний більш глибокий зміст, розширився спектр вирішуваних при цьому задач, збільшилась кількість складових, що визначають захист інформації. Для оцінки рівня захисту інформації широко використовується експертна оцінка. В процесі експертної оцінки (проведенні експертизи) вирішуються задачі оцінювання, яка полягає в співставленні числа або декількох чисел системі, що розглядається. Методика рішення задач оцінювання основана на використанні експертних процедур тобто визначенні експертної оцінки.

Аналіз існуючих експертиз показує, що у процесі їх побудови можна виділити таку послідовність дій:

1. Вказується множина припустимих оцінок Ω, яка містить шукану оцінку.

2. Визначається множина припустимих оцінок Ω_e, з якої здійснюють вибір експерти.

3. Кожен експерт обирає свою оцінку $a_i = C_i(\Omega_e) \in \Omega_e \quad (i = \overline{1, N})$, тобто вирішує задачу вибору найкращої оцінки з Ω_e. При цьому експерти можуть взаємодіяти між собою.

4. За заздалегідь розробленим алгоритмом (формулою) проводиться обробка отриманої від експертів інформації і розраховується результуюча оцінка з Ω, що є вирішенням вихідної задачі оцінювання.

5. Визначається погодженість думок експертів.

6. Оцінюється надійність обробки результатів.

7. Якщо отримане рішення не задовольняє, можна представити експертам додаткову інформацію, тобто організувати зворотний зв'язок, після чого вони знову вирішують відповідні задачі вибору.

Виділену послідовність дій можна представити схемою експертизи (рис.1).

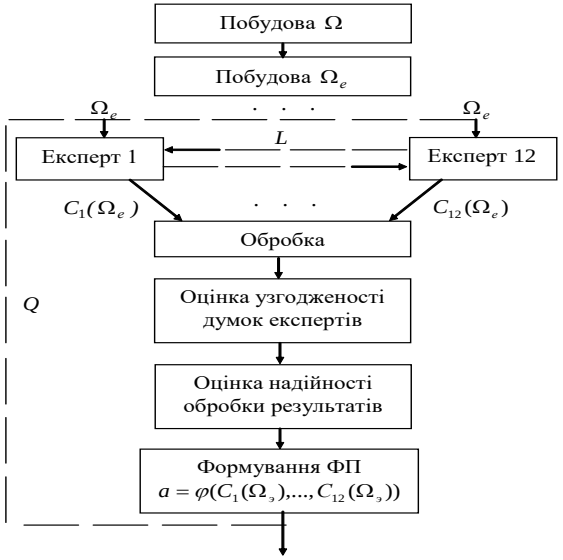


Рисунок 1 – Схема експертизи

1. Складання таблиці опитування експертів у вигляді *анкетування* – припускає відповідь експерта на систему запитань, яка задається розробленою експертною системою (програмний продукт ОФПАС 2.0).

2. Вибір складу експертної комісії в кількості від 5 до 12 чоловік.

3. Визначення профілю захищеності та рівня гарантій програмним продуктом ОФПАС 2.0.

4. За наперед розробленим алгоритмом проводиться обробка експертної інформації.

5. Приймається рішення з урахуванням експертної оцінки та результатів узгодженості думок експертів.

Для обробки експертної інформації було обрано один із методів експертної оцінки – ранжирування, який полягає у зіставленні досліджуваної системи із деякою стандартною.

Висновки. Проаналізовано суть експертизи, визначено за допомогою яких методів проводиться експертиза, кількість експертів, вибрано метод обробки експертної інформації.

Список літератури

1. Теория выбора и принятия решений: Учебное пособие. – М.: Наука. Главная редакция физико-математической литературы, 1982. – 328 с.

2. А. с. 74344 Україна. Комп'ютерна програма. Інформаційна система визначення функціонального профілю захищеності та рівня гарантій автоматизованої системи від несанкціонованого доступу (ОФПАС 2.0) / Бучик С.С., Нетребко Р.В. (Україна). – заявл. 23.10.17; опубл. 26.01.18, Бюл. № 47. – С. 142 – 143.

УДК 004.056.53

Забезпечення захисту даних при передачі інформації через протокол MQTT

Висоцький С. В., аспірант,
Висоцька І. П., аспірант
Науковий керівник – Куницька С. Ю., к.т.н., доцент
Черкаський державний технологічний університет, м. Черкаси

Для створення розумних Інтернет пристроїв, зазвичай використовується протокол обміну даними MQTT, за допомогою якого спрощується взаємодія серверної частини та фізичних пристроїв. Під Інтернет пристроями розуміється технологія IoT (Internet of things), яка допомагає розробникам об'єднувати звичайні пристрої, такі як сигналізації, телевізори та навіть звичайні розетки з Інтернет сервісами.

Message Queue Telemetry Transport або MQTT – це спрощений мережевий протокол, який працює на TCP/IP рівні, що використовується для обміну даними між пристроями за принципом видавець-підписник. Шаблон проектування видавець-підписник часто використовується в програмуванні та представляє собою два елементи – це видавець, або сервіс який зберігає данні та відправляє їх на ініціалізовані клієнти та підписник, це певний елемент ПЗ який ініціалізує з'єднання з сервісом та очікує дані від нього [1]. Таких підписників може бути велика кількість.

Захист інформації, звичайно, є одним з головних елементів правильної роботи будь-якої системи, тож системи IoT також не є виключенням. Для реалізації захисту інформації можна виділити базові принципи технології, які описані в офіційній документації та персональні, які розробники можуть впроваджувати при проектуванні власних систем. Розглянемо базові принципи захисту інформації при використанні протоколу MQTT:

– Аутентифікація клієнта – для того, щоб дозволити новому підписнику підписатися на отримання даних від сервісу потрібно перевірити його аутентифікаційні дані. Зазвичай під аутентифікаційними даними розуміється звичайні ім'я користувача та пароль;

– Авторизація клієнта за допомогою унікального ідентифікатора клієнта, який визначає права доступу до даних сервісу;

– Можливість підключення клієнтів через SSL-з'єднання. SSL – це криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером.

Слід зазначити, що створення SSL з'єднання відбувається за допомогою спеціального сертифікату, який не є безкоштовним та видається на певний період, зазвичай на 1 рік.

Також можна дещо модифікувати дані елементи захисту. Наприклад, аутентифікація за допомогою імені користувача та пароля є застарілою

методологією та не є досить правильною в реалізації систем даного рівня. Більш правильним буде метод використання тимчасового JWT-токену.

JSON Web Token – це стандарт токена доступу на основі JSON, стандартизованого в RFC 7519. Використовується для верифікації даних. Дані в даному стандарті діляться на 3 частини: заголовок, вміст та підпис. Зазвичай в заголовку зберігається службова інформація, така як термін придатності даного токену (так як токен може використовуватися лімітований проміжок часу) [2]. Для отримання токену, клієнт після ініціалізації виконує запит до серверу. Отримавши токен одразу ж можна використовувати його для обміну даними в MQTT-з'єднанні.

Не слід також забувати про самий простий, але необхідний елемент захисту будь-якої системи – це постійний моніторинг існуючої архітектури захисту та моніторинг нових рішень. Прогрес не стоїть на місці та способи захисту інформації постійно змінюються.

Список літератури

1. Paret D., Huon J. Secure Connected Objects. – New York: John Wiley & Sons, 2017. – 129p.

2. Lakshmiraghavan B. Pro ASP.NET Web API Security: Securing ASP.NET Web API. – California: Apress, 2013. – 25 p.

УДК 004.04

Аналіз властивостей механізму автентифікації у блокчейн орієнтованій системі

Вітюк К.Ю., студентка 5 курсу, Біліченко Д.Г., студент 5 курсу
Харківський національний університет радіоелектроніки, м. Харків

Технологія блокчейн лежить в основі біткойна, вона представляє собою децентралізовану базу даних, яка фіксує всі операції з біткойном. Цілісність її постійно перевіряється всією мережею на відміну від центрального органу, такого як банк чи уряд. Таким чином, користувачі не повинні довіряти центральному органу, але безпеку гарантує сила та обчислювальна потужність всієї мережі, яка бере участь у блокчейні.

Цікавий аспект даної технології полягає в тому, що блокчейн може використовуватися для забезпечення автентифікації. Можна автентифікувати користувача у державних службах, банках, аеропортах та інших сервісах лише одним ідентифікатором, використовуючи технологію блокчейн. Використовуючи свою пару ключових слів, користувачі реєструють свій ідентифікатор в блокчейні. Цей зареєстрований ідентифікатор – фрагмент інформації, що містить хеш декількох атрибутів, пов'язаних між особою. Наприклад, ім'я, реєстраційний номер, відбиток пальця, тощо. Після цього такий користувач може перейти до визнаної сторони, яка перевіряє раніше зареєстровані в блокчейні хеші, і нехай сторона, що визнає, "спонсорує" цей фрагмент інформації як істину в блокчейні. Інші сторони, які довіряють одна одній, можуть тепер довіряти ідентифікатору в блокчейні та використовувати його в механізмах автентифікації. Цей сценарій включає проблему, оскільки він все ще вимагає довіри між різними сторонами (спонсорами та сторонами, які визнають їх надійним спонсором), що все ще не є ідеальним.

Іншою проблемою у вищезазначеній концепції є те, що блокчейн вимагає безлічі різних (незалежних) учасників обчислення блоку, щоб переконатися, що він є надійним та незалежним від контролюючих організацій. У випадку біткойна, участь у цих розрахунках нагороджується, сплатою цим учасникам невеликої кількості біткойнів для доставки наступного блоку в ланцюжок. Як це можна мотивувати в блокчейні, який існує лише для служб автентифікації, – це тема, яку слід дослідити.

Останнє, але не менш важливе те, що користувачі можуть втратити свій ідентифікатор (телефон, безпечний флеш-диск або інший носій даних, на якому встановлено приватну ключову частину ідентифікатора). У випадку децентралізованого провайдера аутентифікації, заснованого на технології блокчейн, немає центрального органу, що контролює ідентифікацію, де можна замовити новий ідентифікатор та позначити старий як вкрадений або втрачений.

УДК 004.056.57

Технологія Honeypot для захисту комп'ютерної мережі

Войтович В.С., курсант,
Мандрона М.М., доцент
Львівський державний університет безпеки життєдіяльності, м. Львів

Honeypot – це комп'ютерна система, яка створена для того, щоб заманити кіберзлочинців, а також виявляти, відхиляти або вивчати спроби отримати несанкціонований доступ до інформаційних систем. Як правило, вона складається з комп'ютера, програм та даних, які імітують поведінку реальної системи, яка, як видається, є частиною мережі, але насправді є ізольованою і ретельно контролюється. Всі зв'язки з honeypot вважаються ворожими, оскільки немає підстав для законних користувачів доступу до honeypot. Перегляд та реєстрації даної діяльності дає змогу зрозуміти рівень та типи загрози мережевої інфраструктури, відволікаючи злочинців від активів реальної вартості [1].

На основі їх дизайну та розгортання, honeypots класифікуються як науково-виробничі honeypots. Дослідження honeypots запускаються для точного аналізу активності хакерів і того, як атаки розвиваються та розвиваються, щоб навчитися краще захищати системи від них. Дані, розміщені в honeypot з унікальними ідентифікаційними властивостями, також можуть допомогти аналітикам відслідковувати вкрадені дані та визначати зв'язки між різними учасниками атаки.

Виробничі honeypots розміщуються всередині виробничої мережі з іншими виробничими серверами у ролі приманки в рамках системи виявлення вторгнення в мережу (IDS) [2]. Їхнє призначення є для того, щоб вони відображалися справжніми та містили інформацію або ресурс, за допомогою якого можна залучити хакерів та зайняти їх. Це пов'язує час і ресурси зловмисника, надаючи адміністраторам час для оцінки та пом'якшення будь-яких уразливостей у своїх фактичних системах виробництва. Інформація, зібрана з honeypot також може бути корисною для виявлення та переслідування тих, хто стоїть за атакою. Дослідники підозрюють, що деякі кіберзлочинні особи також використовують honeypots для збору, розвідки про дослідників, виступають в якості дезінформаторів.

Honeypots з високим рівнем взаємодії імітують діяльність виробничої системи та отримують велику інформацію – чисті honeypots є повноцінними виробничими системами, використовуючи екран на посилання honeypot на мережу. Мета honeypots з високою взаємодією, полягає в тому, щоб зловмисник отримував кореневий доступ на машині, а потім вивчав те, що він робить. Зловмисник з кореневим доступом має доступ до всіх команд і файлів у системі, тому цей тип honeypot несе

найбільший ризик, але також має найбільший потенціал для збору інформації. Низькі взаємодії honeypots імітують тільки послуги, які часто націлені зловмисниками, і тому вони менш ризиковані та менш складні для підтримки. Віртуальні машини часто використовуються для розміщення honeypots, щоб honeypot можна було відновити швидше, якщо це скомпрометовано. Два або більше honeypot в мережі утворюють honeynet, а honeypty являє собою централізовану колекцію honeypots та інструменти аналізу.

Honeypots допомагають усвідомлювати загрози мережевим системам, але виробничі honeypots не повинні розглядатися як заміна стандартного IDS. Якщо вони не належним чином налаштовані, вони можуть бути використані для доступу до реальної виробничої системи або використовуватись як стартовий майданчик для атак проти інших систем [3].

Висновок: на сьогоднішній день найбільший інтерес представляють високоінтерактивні динамічні honeypot-системи, так як з завданнями низкоінтерактивних систем справляються інші елементи корпоративної мережі: мережеві сканування успішно запобігають міжмережевими екранами і системами виявлення та запобігання вторгнень, а також правильної конфігурацією елементів мережі, а інформація про конкретні дії зловмисника, вжитих для здійснення доступу в корпоративну мережу, надають набагато більшу цінність, ніж інформація про факт проникнення в мережу, яка також може бути отримана від міжмережевих екранів і засобів виявлення вторгнень.

Динамічні ж honeypot-системи мають великий потенціал розвитку. У таких системах можуть бути застосовані ідеї, зарекомендувавши себе в інших типах систем, а також запропоновані і принципово нові підходи.

Список літератури

1. Intrusion Detection FAQ: What is a Honeypot? [Електронний ресурс]. Режим доступу: https://www.sans.org/security-resources/idfaq/honeypot3.php
2. Dynamic Honeypots [Електронний ресурс]. Режим доступу: http://www.symantec.com/connect/articles/dynamic-honeypots
3. Гіпервізор, віртуалізація і хмара: Про Гіпервізор, віртуалізації систем і про те, як це працює в хмарному середовищі [Електронний ресурс]. Режим доступу: http://www.ibm.com/developerworks/ru/library/cl-hypervisorcompare/
4. The Honeynet Project [Електронний ресурс]. Режим доступу: https://www.honeynet.org

УДК 004.056

Проблеми захисту інформації в IoT

Воронкін І.І., аспірант
Науковий керівник – д.т.н., проф. Семенов С.Г.
Харківський національний університет радіоелектроніки, м. Харків

The given work is devoted to the IoT technology and potential problems of security. IoT devices collect very large amount of personal data. If not properly secured, it may lead to security issues like privacy and confidentiality. Low secure level of IoT devices and the sensitivity of exchanged data makes this technology very attractive for intruders.

Internet of Things (IoT) – це одна з технологій, що досить стрімко розвивається та є об'єктом пильної уваги зі сторони наукових і промислових секторів. Базовою складовою цієї технології є Machine-to-Machine (M2M) взаємодія що відноситься до технології комунікації між компактними і дешевими пристроями що працюють без втручання людини, або з її мінімальним впливом.

В найближчі декілька років очікується швидкий ріст і більш глибоке проникнення даної технології в повсякденне життя. Це допоможе відкрити шлях до масштабного розвитку глобальної мережі де всі девайси взаємодіють без будь-якої участі людини.

До всіх підключених об'єктів, яких уже на сьогоднішній день нараховуються мільярди, висуваються ті ж вимоги безпеки, що і до мобільних телефонів, комп'ютерів і інших електронних пристроїв. Однак у зв'язку з автономністю функціонування, пристроям класу IoT потрібні додаткові заходи безпеки, виходячи з особливостей їхньої взаємодії.

Забезпечення захисту від потенційних загроз є дуже складним завданням. Разом із тим, необхідно враховувати ряд обмежень і вирішувати ряд задач. Серед них розглядають такі:

- розширюваність – здатність до динамічної зміни кількості компонентів мережі;
- неоднорідність пристроїв – різні обчислювальні й енергетичні ресурси компонентів;
- неоднорідність технологій взаємодії (Wi-Fi, Bluetooth, NFC, LAN, Radio та інші);
- затримки в каналах обміну данними;
- обмежена пропускна можливість деяких технологій зв'язку;
- відмовостійкість – вимоги до підвищеної надійності деяких систем.

Очевидно, що приведені задачі роблять реалізацію схеми безпеки доволі складним завданням. Насправді, в більшості випадків не представляється можливим створити універсальне рішення. Тому на

практиці, здебільшого, намагаються задовольнити базові вимоги безпеки, а це: конфіденційність, цілісність і доступність.

Кращий спосіб забезпечити конфіденційність даних – це шифрування з використанням симетричної або асиметричної криптографії. У той час як симетрична криптографія є менш вимогливою до ресурсів системи та відповідає встановленим обмеженням, вона не є досконалою і вимагає, щоб обидві сторони мали загальний секретний ключ (рис. 1). Це ставить питання про те, як безпечно поширювати його.

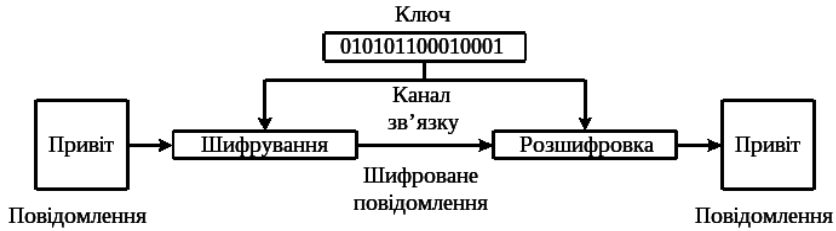


Рисунок 1 – Схематичне зображення симетричного шифрування

Асиметрична криптографія позбавлена цього недоліку. Та з іншого боку, вона забирає багато ресурсів і вимагає прив'язки до пристрою приватного ключа або генератора, з метою забезпечення кожного пристрою його закритим ключем.

Цілісність інформації в IoT системах пропонується забезпечувати за допомогою використання HMAC-функцій. Так як в HMAC повідомлення криптографічно пов'язані, це дозволяє забезпечити захист і від DoS атак, що є елементом реалізації послуги доступності.

Таким чином, IoT системи схильні до тих же загроз безпеки, як і інші комунікаційні системи, проте, чутливість інформації, що обробляється, робить ці атаки більш шкідливими. Вони можуть призвести не тільки до значних фінансових збитків клієнтів, а й навіть поставити під загрозу життя людини. Широка поширеність та недосконалий захист роблять ці системи дуже привабливими для зловмисників. Тому питання захисту інформації стає все актуальнішим і вимагає особливої уваги.

Список літератури

1. D. Evans, "The internet of things, how the next evolution of the internet is changing everything", in Cisco Internet Business Solutions Group (IBSG) white paper, April 2011.

2. Y. Cheng, M. Naslund, G. Selander, and E. Fogelstrom, "Privacy in machine-to-machine communications", in Communication Systems (ICCS), 2012 IEEE International Conference on, pp. 75–79, Nov 2012.

УДК 621.391.6

Проблеми виникнення каналів витоку інформації за рахунок побічного оптичного випромінювання

Гвоздінський Д.В., курсант
Науковий керівник – Кулініч О.М., к.т.н., доцент
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут ім. Ігоря Сікорського»

Одне з важливих місць у загальному комплексі заходів забезпечення національної безпеки України в інформаційній сфері займає технічний захист інформації (ТЗІ). На даний момент серед визначених реальних та потенційних загроз важливе місце посідає порушення конфіденційності інформації з обмеженим доступом (ІзОД) на об'єктах інформаційної діяльності (ОДІ) та в інформаційно-телекомунікаційних системах (ІТС), особливо захист від витоку інформації технічними каналами.

Для запобігання даним загрозам в Україні на теперішній час функціонує система нормативних документів технічного захисту інформації (ТЗІ), що регламентує порядок захисту інформації від витоку технічними канали та практично весь ряд задач з ТЗІ на ОІД та в ІТС.

На жаль, на даний час в Україні існую брак нормативно-правових актів, які б встановлювали, зокрема, вимоги щодо технічної охорони об'єкту, на якому циркулює ІзОД. Так чинні нормативно-правові акти та відомі праці, як вітчизняних, так і закордонних фахівців сфери ТЗІ визначають перелік технічних каналів витоку інформації (ТКВІ), якими порушується конфіденційність ІзОД.

При побудові комплексу ТЗІ та комплексної системи захисту інформації враховують класифіковані нормативно-правовими актами загрози, утворені ТКВІ. Найбільш загальними ТКВІ виділяють: електромагнітні, акустичні, вібраційні, оптичні та їх підвиди.

Дослідження та аналіз останніх публікацій в сфері інформаційної безпеки дає можливість свідчити про актуальність цілковито нового ТКВІ, який не враховується чинними нормативно правовими документами системи ТЗІ, а саме побічне оптичне випромінювання.

Витік інформації каналами побічного оптичного випромінювання несуть в собі реальну загрозу. Перед нами постає питання – чи може оптичне випромінювання від індикаторів комп'ютерних світлодіодів погіршувати інформаційну безпеку? У статті «Витік інформації оптичним випромінюванням» Джо Лоурі та Девід Умфресс виклали зміст проведених експериментів на різних пристроях зв'язку на яких виявили форми шкідливого випромінювання. Індикатори стану світла на пристроях передачі даних за певних умов демонструють, що вони мають

модульований оптичний сигнал, який суттєво корелює з інформацією, що обробляється пристроєм. Експерименти показали, що можна перехопити дані в реальних умовах на значній відстані. Багато різних пристроїв, зокрема модемів та маршрутизаторів, виявилися вразливими.

Під час дослідів були враховані такі незалежні змінні: 1.Відстань між детектором та випробовуваним пристроєм; 2. Швидкість передачі даних. 3. Умови зовнішнього освітлення в діапазоні випробувань. Залежною змінною була кореляція між отриманим оптичним сигналом і вихідною силою сигналу. Відстань коливалася від 5 м до 38 м (максимальний розмір лабораторії) з кроком 5 м під час випробування. Випробувані умови освітлення враховували в себе умови для роботи денного світла (наприклад, сонячне світло, що проходить через вікна, а також штучне освітлення), звичайне люмінесцентне офісне освітлення, офісне освітлення у нічних умовах (розсіяні флуоресцентні ліхтарі, а також деяке світло, що проникає через вікна з ліхтарі назовні). Всі випробування проводилися в приміщенні.

У дослідженні було виявлено 39 пристроїв, що містять 164 унікальних світлодіодних індикаторів. Вибрані для тестування пристрої були представлені з широкого спектру технологій обробки інформації, включаючи пристрої низькошвидкісного і високошвидкісного зв'язку, пристрої локальної мережі та широкосмугової мережі, персональні комп'ютери та великі комп'ютери та периферійні пристрої.

Висновки

До теперішнього часу не враховувалось виникнення технічного каналу витоку інформації за рахунок побічного оптичного випромінювання, що формувало не цілісну систему захисту інформації.

Необхідно провести дослідження даних ТКВІ і якщо вони підтвердяться то внести зміни та поправки до чинної нормативно-правових бази, що дозволить досягнути значущих цілей при побудові комплексів технічного захисту інформації та комплексних систем захисту інформації

Список літератури

1. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. – [Електронний ресурс]. – Режим доступу до док.: http://www. dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=38934&cat_id=38836.

2. Loughry J. Information Leakage from Optical Emanations/ J. Loughry, D. Umphress. – 2002. – [Electronic resource]. – Access mode: http://applied-math.org/optical_tempest.pdf

УДК 658.52; 681.3

Аналіз порушників та загроз мереж безпровідного типу

Говдун А.В., студент
Науковий керівник – Полотай О.І., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності, м. Львів

З появою в сучасному світі компактних пристроїв для роботи в мережі Інтернет перед розробниками постало нове завдання – забезпечити доступ до мережі в місцях, що знаходяться на віддаленій відстані від кабельної мережі. Саме так і з'явилися мережі, що працюють по радіоканалу і забезпечують доступ до мережевих ресурсів.

Системи бездротового зв'язку використовуються переважно в мережах, побудованих з використанням кабельних систем, і дають можливість ефективно вирішити проблеми, що виникають в процесі проектування і модернізації кабельних мереж. Бездротові засоби зв'язку не є повною заміною кабельних мережах, а лише технологією реалізації окремих сегментів проектованої мережі. Бездротові мережі є новим кроком у розвитку технічних засобів доступу до мережі. Одним з видів мереж, що є бездротового типу та займають перші місця серед популярних, є мережі на основі технології Wi-Fi стандарту IEEE 802.11 [1], які регулюють роботу локальних обчислювальних мереж і мереж, розташованих в мегаполісах.

Однією з основних проблем мереж безпровідного типу є їх безпека. Адже будь-яка особа, з використанням ноутбука з адаптером IEEE 802.11b, не проникаючи в приміщення, в якому є така мережа, може отримати доступ до її ресурсів. Причому факт несанкціонованого доступу буде складно зафіксувати, та й звичний Firewall в даних ситуаціях нічим не допоможе.

Для того, щоб отримати представлення про загрози безпеці мережі безпровідного типу, необхідно здійснити аналіз порушників (табл. 1) та загроз (табл. 2) безпеки даної мережі.

Таблиця 1

Модель порушників [2]

Тип	Характеристика	Рівень шкоди
Зацікав-лені	Вони виконують злом заради свого самоствердження або забави.	Низький
Мисливці за каналами зв'язку	Інтерес цих осіб спрямований на спробу користування чужими мережами для передачі різного контенту в мережу. Найчастіше дані мають не зовсім законний характер.	Середній
Злочинці	Найбільш кваліфіковані та небезпечні особи.	Високий

Під загрозами безпеки мережі безпровідного типу розуміється сукупність атак, що спрямована на систему. Атакою на систему називається дія або сукупність дій порушника, спрямованих на отримання доступу до інформаційної системи, в нашому випадку – до мережі безпровідного типу.

Таблиця 2

Типи атак на мережі безпровідного типу

Загроза	Характеристика
Атака на налаштування параметрів канального рівня в мережах 802.11.	Атака на настройку режиму економії енергії. Зловмисник підміняє пристрій клієнта, яке знаходиться в стані так званого «сплячого» режиму, здійснюючи збір кадрів. Після того як клієнт прийме кадри, точка доступу очистить буфер і, таким чином, клієнт не отримає своїх кадрів.
Dos-атаки	Застосовуються в якості одного із способів проникнення в мережу. Через фізичну природу радіохвиль, як засобу передачі інформації, і конструктивних особливостей протоколів IEEE 802.11 вони не можуть бути захищені від атак на фізичному рівні.
Атаки на систему автентифікації	Атака на фільтрацію MAC-адрес. Для здійснення такої атаки потрібні такі дії з аналізу мережевого трафіку для пошуку MAC-адрес: перевірка наявності в мережі обраного хоста і очікування його виходу з мережі. Іноді зловмисник може відключити хост, на який спрямована атака, застосовуючи спосіб підміни свого MAC-адреси на адресу атакуємого хоста.

Отже, мережі безпровідного типу мають багато вразливостей, і для того, щоб їх усунути необхідно приймати конкретні міри, серед яких зменшення зони покриття, фільтрація MAC-адрес, зміна ідентифікатора мережі, новий пароль адміністратора та ін.

Список літератури

1. Ватаманюк А.И. БЛВС своими руками / А. И. Ватаманюк. – СПб. [и др.]: Питер, Питер пресс, 2006. – 192 с.

2. Носенко А. А. Расчет экономической эффективности инвестиционных проектов: методическое пособие / А. А. Носенко – Мн.: БГУИР, 2003. – 96 с.

УДК 004.056.53

Забезпечення безпеки інформації у хмарних сховищах

Головатій В.І., студентка
Науковий керівник – Конопліцька О.К., викладач
Центральноукраїнський національний технічний університет, м. Кропивницький

З розвитком інформаційних технологій уявити сучасну людину без Інтернету стало неможливо. Так наприклад, в останні роки для зберігання та передачі даних широко використовуються хмарні сховища. Вони дозволяють мати доступ до своїх даних будь-де та з будь-якого пристрою, який має підключення до Інтернету. Це дуже зручно, але більш небезпечно, ніж зберігати дані на персональному комп'ютері, отже важливо забезпечувати захист персональної інформації у хмарних сховищах.

Аналіз забезпечення безпеки в хмарних сховищах

Розглянемо найпопулярніші сховища: Dropbox, iCloud, Google Drive, OneDrive.

Dropbox має три тарифних плани для користуваня. Перший план Basic безкоштовний, дає можливість завантажити даних до 5 ГБ, які в подальшому можна збільшити до 16 ГБ виконавши певні умови. Тарифні плани Pro та Business відрізняються тим, що Pro надає 1Тб пам'яті, а Business необмежений обсяг. Dropbox шифрує дані клієнтів на стороні сервера, але відмовляється від шифрування клієнтської частини програми. Потокова передача з серверів не завжди зашифрована. Таким чином стає можливий витік даних в ході завантаження і вивантаження файлів на сервера. У тарифних планах забезпечено додаткове шифрування при передачі даних, зберігання отримуваних файлів у вигляді зашифрованих блоків, а також роздільне зберігання метаданих і блоків даних. Крім того, у Dropbox є історії інцидентів пов'язаних з безпекою у 2012, 2014 та 2017 роках. Тож Dropbox є не самим надійним хмарним сховищем.

Для користувачів компанії Apple існує хмарне сховище iCloud. В ньому існує 4 тарифних плани: 5 Гб, 50 Гб, 200 ГБ та 2 Тб. Найменший за обсягом є безкоштовним. В 2014 році відбувся великий скандал пов'язаний з масовим зломом акаунтів, згодом в мережу потрапило безліч персональних даних користувачів. Після інциденту компанія серйозно взялася за поліпшення безпеки – зараз інформація шифрується при зберіганні та при передачі, для певних типів конфіденційної інформації Apple використовує наскрізне шифрування, пароль перевіряється на надійність, присутня двухфакторна аутентифікація, використовуються маркери безпеки для аутентифікаці.

У Google Drive також є, як і безкошктовний план на 15 Гб, так і

тарифні плани на 100 ГБ та 1 ТБ. Присутня двухфакторна аутентифікація. Відновлення доступу до акаунту здійснюється за допомогою секретного питання, сам сервіс перевіряє користувачем пароль на надійність і не дозволяє використовувати паролі, які легко зламати. Дані шифруються при передачі, що виключає їх витік в ході завантаження, однак для шифрування даних на сервері знадобляться сторонні програми. Версія для бізнес-акаунтів дозволяє забезпечувати більш високий рівень захисту. У ній, наприклад, існують правила захисту електронної пошти, що примусово включає протокол TLS, а також технології IRM і DLP.

Хмарний сервіс OneDrive має план Basic з простором до 5 ГБ та план Business до 50 ГБ. Продукт забезпечує шифрування переданих між клієнтом і сервером даних, а також присутня двухфакторна авторизація. Крім того, пароль перевіряється на надійність. План Business – сховище зашифрованого контенту має поліпшені функції безпеки. В ній забезпечується безпека центру обробки даних, мережева безпека, безпека доступу, безпека додатків і даних. Типи сховищ, що застосовуються в бізнес версії, фізично розділені, завдяки чому при зломі будь-якого з них можна скомпрометувати інформацію.

Судячи з переліченої інформації, можемо визначити надійність хмарних сховищ. Четверте місце займає Dropbox; третє – Google Drive; друге – iCloud; перше – OneDrive.

Висновки. Хмарні сховища зручні у використанні. Мають свої недоліки та переваги. Проаналізувавши безпеку сховищ, можемо бачити надійність кожного з них. Довіряти свої персональні дані – це особисте рішення кожного, але компанії з кожним роком намагаються збільшити безпеку своїх сховищ.

Список літератури

1. Захист даних в хмарних технологіях. [Електронний ресурс]. – Режим доступу: http://conf.vntu.edu.ua/allvntu/2013/inaeksu/txt/tytarchuk.pdf.

2. Хмарні технології [Електронний ресурс]. – Режим доступу: http://sdo.gtn.lokos.net/mod/book/view.php?id=609&chapterid=264&lang=en.

3. Чи безпечні хмарні сховища даних? [Електронний ресурс]. – Режим доступу: http://mobile-dom.ru/internet/bezopasnyi-li-oblachnyie-hranilishha-dannyih.

УДК 004.056.53

Оцінка ризиків інформаційної безпеки за допомогою апарату штучних нейронних мереж

Грек О. М., студентка 5-го курсу
Науковий керівник – Марчук А. В., к.т.н., старший викладач
Харківський національний університет радіоелектроніки, м. Харків

З часом складність інформаційних систем збільшується, а питання забезпечення інформаційної безпеки (ІБ) стають дедалі більш значимими. Особливу увагу звертають на аналіз та оцінку ризиків ІБ.

Дослідження у сфері аналізу ризиків ІБ проводилися такими вченими як G. Brændeland, A. Papoulis, N.E. Fenton, F.V. Jensen і так далі. Існуючі методи здебільшого відрізняються застосовуваними шкалами: кількісними чи якісними. Виходом алгоритму кількісного підходу є числове значення ризику. В якості вхідних даних звичайно використовують зібрану інформацію про небажані чи несподівані події в системі, котрі можуть поставити від загрозу захист інформації. Однак часта відсутність достатньої кількості статистичних даних призводить до зниження адекватності результатів. Якісні методики більш поширені, однак в них використовуються занадто спрощені шкали, які звичайно містять три рівня оцінки ризику: низький, середній, високий [1].

У зв'язку з перерахованими вище та іншими проблемами в останні роки актуальною задачею є пошук такої методики, яка б була позбавлена таких недоліків як виключно якісний підхід, непристосованість методик до постійних змін стану автоматизованої системи, неперервних поява нових джерел загроз, відсутність можливості прямого повторного застосування старих звітів з оцінки, неадекватність та неактуальність експертних оцінок і тому подібне. Найбільш перспективним напрямком у даній сфері є робота зі штучними нейронними мережами (ШНМ).

Науковою задачею у даній роботі є розробка нового методу оцінки ризиків ІБ, що поєднує в собі якісну та кількісну шкали, позбавленого недоліків та задовольняючого сучасним потребам у процесі оцінки ризиків, шляхом застосування апарату ШНМ.

Так, було розроблено метод, побудований на концепції нечітких нейронних мереж, який поєднує в собі роботу ШНМ та нечіткої логіки.

Розроблений метод оцінки ризиків ІБ було реалізовано у середовищі MATLAB за допомогою вбудованих засобів пакету «Fuzzy Logic Toolbox» із застосуванням редактору FIS та ANFIS.

У роботі використано модель нечіткої ШНМ, яка являє собою багатошаровий перцептрон, в якому шари відповідають за виконання процесів системи нечіткого виводу. Для побудови нейронної мережі було обрано систему, організовану за алгоритмом Такагі-Сугено-Канго. Для

навчання мережі використовувався алгоритм зворотного розповсюдження помилки [2]. Навчальною вибіркою слугували 300 можливих комбінацій якісних рівнів загрози, збитків, вразливості та відповідних якісних рівнів ризиків. У підсумку в кінці навчання величина помилки роботи мережі складала 0.053524.

Вхідними даними для нейронної мережі є кількісні значення рівня загрози, величини збитків та ступеня вразливості для кожного джерела загрози за шкалою від 0 до 1. Виходом є відповідні кількісні значення ризику, які зіставляються із якісною шкалою.

Приклад роботи побудованої ШНМ зображено на рисунку 1 для таких вхідних даних: рівень загрози – 0.95, величина збитків – 0.65, ступінь вразливості – 0.1.

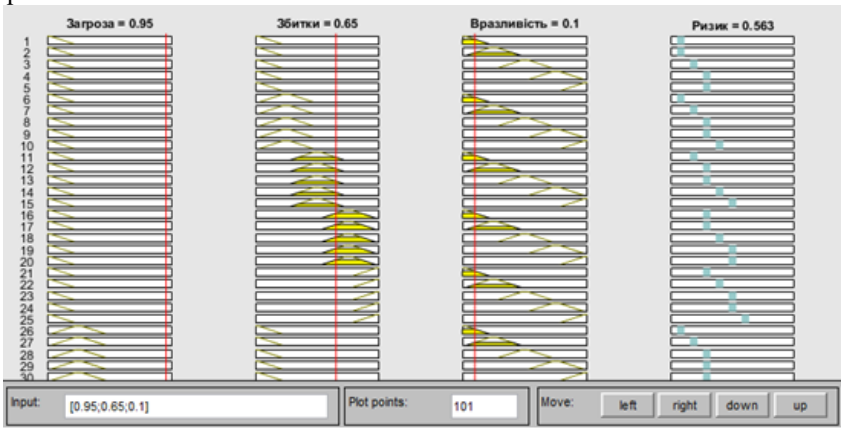


Рисунок 1 – Приклад роботи побудованої ШНМ

Таким чином, як видно на рисунку 1, на виході ШНМ дає величину ризику 0.563, що відповідає його якісному значенню «Середній».

Висновки. Так, було отримано підхід до оцінки ризиків ІБ за допомогою ШНМ, побудованої системою нечіткого виводу.

В подальшому планується розвиток даної теми. Наступним етапом є створення методу оцінки ризиків ІБ за допомогою апарату ШНМ, позбавленого необхідності залучення експертів для оцінки рівнів і ймовірностей загроз, вразливостей та збитків. Ці величини будуть встановлюватися заздалегідь навченою для цього ШНМ.

Список літератури

1. Варфоломеев А. А. Управление информационными рисками: учеб. пособие / А. А. Варфоломеев – М.: РУДН, 2008. – 158 с.

2. Каллан Р. Основные концепции нейронных сетей / Р. Каллан – М.: Издательский дом «Вильямс», 2001. – 287 с.

УДК 681.3

Інформаційна безпека: проблема законодавчого визначення

Гуцу С.Ф., доцент, к.ю.н., доцент
Національний аерокосмічний університет ім. М.Є.Жуковського «ХАІ», м. Харків

25 лютого 2017 року Указом Президента України було затверджено Доктрину інформаційної безпеки України, якою було визначено національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері [1]. Документ є дуже цікавим для аналізу й вивчення, бо в ньому прямо сказано, що інформаційна сфера є ключовою ареною у боротьбі за національну безпеку. А серед актуальних загроз національним інтересам та національній безпеці України названо недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері.

Визначення поняття «національна безпека» містить Закон України «Про основи національної безпеки України» [2]. А саме: «національна безпека – *захищеність життєво важливих інтересів людини і громадянина, суспільства і держави*, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сферах правоохоронної діяльності, боротьби з корупцією, прикордонної діяльності та оборони, міграційної політики, охорони здоров'я, охорони дитинства, освіти та науки, науково-технічної та інноваційної політики, культурного розвитку населення, забезпечення свободи слова та інформаційної безпеки, соціальної політики та пенсійного забезпечення, житлово-комунального господарства, ринку фінансових послуг, захисту прав власності, фондових ринків і обігу цінних паперів, податково-бюджетної та митної політики, торгівлі та підприємницької діяльності, ринку банківських послуг, інвестиційної політики, ревізійної діяльності, монетарної та валютної політики, захисту інформації, ліцензування, промисловості та сільського господарства, транспорту та зв'язку, інформаційних технологій, енергетики та енергозбереження, функціонування природних монополій, використання надр, земельних та водних ресурсів, корисних копалин, захисту екології і навколишнього природного середовища та інших сферах державного управління при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам». Отже, національна безпека полягає у стані «захищеності» суб'єктів, якими визнаються людина, суспільство і держава від реальних та потенційних загроз. А держава забезпечує таку захищеність, визначаючи що саме є загрозою. На мою думку, така позиція може призвести до зловживань і маніпуляцій в сфері прав і свобод

людини, домінанту держави у визначені ступеню небезпеки і необхідності захисту.

Щодо терміну «інформаційна безпека», то вперше його було визначено в Концепції Національної програми інформатизації [3]. Відповідно до цього документу інформаційна безпека – *це комплекс нормативних документів* з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу; комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації; банк засобів діагностики, локалізації та профілактики комп'ютерних вірусів, нові технології захисту інформації з використанням спектральних методів, високонадійні криптографічні методи захисту інформації тощо. Пізніше, було розроблено проект Закону «Про інформаційний суверенітет та інформаційну безпеку України» [4] (ст.3), який має суттєво іншу інтерпретацію цього терміну – інформаційна безпека розглядається як «захищеність життєво важливих інтересів суспільства, держави і особи, якою виключається заподіяння шкоди через неповноту, несвоєчасність, недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок розповсюдження інформації, забороненої для розповсюдження законами України».

Чинне законодавство, а саме Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» визначає інформаційну безпеку теж як «стан захищеності», але саме визначення декілька доповнено: «Інформаційна безпека - стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [5]. На мій погляд таке визначення терміну, знову ж таки, містить право держави визначати яка саме інформація може бути шкідливою не тільки для держави в цілому, а і для конкретної людини, що значно звужує свободу та принцип рівності в інформаційних відносинах.

На жаль, Доктрина інформаційної безпеки України як спеціалізований нормативний акт не містить визначення значення «інформаційна безпека», що спонукає науковців шукати і пропонувати власний суб'єктивний аналіз цього терміну. Маємо низку поглядів, думок і тлумачень, подекуди дуже подібних один до одного, а інколи – кардинально протилежних. Так, ряд авторів [6] у своїх працях беруть за основу визначення терміну, що міститься у чинному законодавстві, інші (Цимбалюк В.С., Кормич Б. А.) категорично не погоджуються з таким визначенням. Як, слушно зазначає В.С. Цимбалюк: «це надмірно

ускладнене формулювання демонструє не лише публічноправове визначення надмірного патерналізму держави. Також у такому формулюванні робиться спроба публічноправовим регулюванням охопити неосяжне: бажання законодавчого закріплення функції держави взяти на себе визначення, яка саме інформація є «достовірною» чи «недостовірною», «зіпсованою», а яку треба заборонити як вияв загрози чи виклик для безпеки. Нами вважається, що держава не може і не повинна мати монополії на всю інформацію. Вона може сприяти плюралізму в інформаційній сфері суспільства на принципі співвідношення потреб та інтересів особи та соціальних утворень.» [7]. Науковець пропонує для обговорення таке розуміння формулювання інформаційної безпеки за правовим змістом – це сфера суспільних відносин щодо підтримки на нормативно визначеному рівні співвідношення прав і обов'язків особи, суспільства, держави в інформаційному просторі від загроз, викликів їх суверенітету.

Підтримуючи таку позицію науковця, вважаю за необхідне зазначити, що сам факт ідентичного трактування «стану захищеності» таких різних суб'єктів інформаційних відносин як держава, суспільство і особа, не може не викликати питань. По-перше, людина як біологічна істота має властивості, які не притаманні таким утворенням як держава і суспільство. На мій погляд, необхідно виокремлювати інформаційну безпеку особи (людини) і інформаційну безпеку суспільства й держави. По-друге, наявне визначення «інформаційна безпека» передбачає досягнення «стану захищеності» не шляхом створення суб'єктам комфортних умов співіснування в інформаційному просторі, а шляхом заборон і цензури з боку держави у цій сфері. В такому вигляді воно перетворюється у механізм державного контролю інформаційного простору. На мою думку визначення поняття і значення «інформаційна безпека» потребує ще неодноразового обговорення науковцями, вироблення єдиної правової позиції, яка б відображала і враховувала інтереси усіх учасників інформаційних відносин.

Список літератури

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року № 47/2017 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/47/2017.

2. Про основи національної безпеки України: Закон України. – К.: «Парламентське видавництво», 2013. – 16 с.

3. Концепція Національної програми інформатизації від 4 лютого 1998 р. № 75/98- ВР) [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua.

4. Про інформаційний суверенітет та інформаційну безпеку України : Проект Закону України від 12 серпня 1999 р. № 1207-d [Електронний

ресурс]. – Режим доступу: http://www.rada.kiev.ua].

5. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/537-16.

6. Інформаційна безпека (соціально-правові аспекти): Підручник / Остроухой Б. В., Петрик Б.М., Прнсяжнюк М. М. та ін. ; за заг. ред. Є. Д. Скулиша. – К.: КНТ, 2010. - 776 с.

7. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. – Київ: Видавничий дім «Гельветика», 2017. – 168 с.

УДК 004.056.53

Автентифікація користувача за його унікальними голосовими характеристиками

Діденко А.І., курсант
Науковий керівник – Кулініч О. М., к.т.н., доцент
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут ім. Ігоря Сікорського»

Основним напрямком систем автентифікації є розвиток біометричних систем. Найбільше зусиль було витрачено на розвиток і вдосконалення засобів, які дозволили б досягти зменшення рівня помилок та досягнути захищеності від інформаційних загроз. Масове виготовлення таких систем дозволить відчутно знизити їх вартість.

Системи розпізнавання можуть бути розділені на текстозалежні і текстонезалежні. При текстозалежному розпізнаванні можуть використані як фіксовані фрази, так і фрази, утворені системою і запропоновані користувачу. Текстонезалежні системи призначені для обробки довільної мови.

Основні переваги такої технології – це можливість дистанційної перевірки користувача на право доступу до інформації. Голос кожної людини, як і відбитки пальців є унікальним. Сама технологія не нова і раніше були спроби використання так званої активної голосової біометрії – коли людині на початку діалогу пропонується назвати свою кодову фразу, яка звірятиметься з еталонною. На зміну їй прийшла технологія пасивної голосової біометрії – коли людина спілкується з роботом або з оператором, і система у фоновому режимі порівнює його голос з еталонним зліпком. Технологія пасивної голосової біометрії має ряд переваг в порівнянні з активною голосовою біометрією.

У зв'язку з розвитком інформаційних технологій в даний час в розпізнаванні диктора, крім державних установ, зацікавлені бізнес-структури і численні категорії користувачів інформаційних послуг. Незважаючи на інтенсивні наукові дослідження, і з'являються час від часу повідомлення про феноменальну ефективність розроблених систем розпізнавання, реальне застосування, за винятком вузьких областей, сильно обмежене, що підтверджується регулярними річними звітами Gartner Group, які констатують, що лише близько 1% обсягу потенційних користувачів задоволено ефективністю комерційних систем розпізнавання диктора.

Автентифікація користувача за голосовими особливостями має суттєві переваги:

- Можливість віддаленої автентифікації користувача (порівняння з

конкретним еталоном) або верифікації (пошуку у базі еталонів) користувачів.

- Мала ймовірність імітування голосу зловмисником за допомогою магнітофона.
- Неможливість автентифікації людини, що знаходиться під загрозою здоров'ю, оскільки емоційний стан користувача має значний вплив на особливості голосу і мови.
- Підвищення рівня надійності автентифікації за рахунок використання технологій автентифікації по голосу і розпізнавання мови (вимовленого паролю).

Висновок: На відміну від автентифікації на основі аналізу сітківки ока або відбитків пальців, автентифікація по голосу не вимагає великої кількості дорогих сканерів, аналіз відбувається на основі телефонного дзвінка, де голос людини звіряється з еталоном на центральному сервері. Аналіз досягнень у сфері розробки і використання біометричних систем показав, що автентифікація за голосовими особливостями – це один з перспективних напрямів наукового дослідження, результати якого можуть ефективно використовуватися не тільки в охоронних системах або системах стеження, але і в експертних системах, що є нагальною потребою сьогодення для криміналістики.

Список літератури

1. Пріорбанк [Електронний ресурс]. – Режим доступу: https://www.priorbank.by/

2. Лебеденко Ю.И. Биометрические системы безопасности. – Тула: Изд-во ТулГУ, 2012. – 160 с.

УДК 007.051:004.5

Генератор мемів для тестування соціальної складової соціотехнічної системи

Дудатьєв А.В., к.т.н., доцент,
Войтович О.П., к.т.н., доцент,
Головенько В.О., студент,
Рудик О.А , студент
Вінницький національний технічний університет, м.Вінниця

Сучасний інформаційний простір, складовою якого є соціальні мережі є специфічною ареною проведення спеціальних інформаційних операцій, зокрема інформаційно-психологічних операцій, що спрямовуються на суспільство. Велика кількість людей по всьому світу вже активно користуються соціальними мережами для спілкування, перегляду новин тощо, проте велика частка користувачів використовують соціальні мережі як інструмент маніпуляції індивідуальною та суспільною свідомістю за допомогою інформаційних вкидів. Одним із джерел розповсюдження інформаційного впливу можуть бути фейкові облікові записи у різноманітних соціальних мережах, ідентифікація яких дозволяє з достатньо високою ймовірністю стверджувати про деструктивність розповсюджуваної інформації. Незалежно від конкретних цілей тих, хто створює фейкові облікові записи, їх використання спрямоване на реалізацію головної мети інформаційного впливу – перепрограмування свідомості соціальної складової соціотехнічної системи (СТС).

У роботі [1] було запропоновано метод реалізації деструктивного інформаційного впливу – мем-програмування, метою якого є оптимізація процесу проведення інформаційно-психологічних операцій. Оскільки, мем, з точки зору еволюції людини, порівнюється з геном, то вирішення проблем пов'язаних із визначенням впливу сформованого мему на соціум, використання змінених мемів за допомогою базових операцій, вплив мемів з декількох каналів впливу (розмноження мемів) і прийняття рішення, щодо стану соціуму та прийняття рішень щодо його захисту є актуальними завданнями.

Для дослідження сформульованих питань було розроблено програмний засіб, для моніторингу стану соціальної складової СТС. Інтерфейс програмного засобу представлений на рис. 1, демонструє можливість створення нового мема або використання готового. Для тестування була обрана соціальна мережа Facebook.

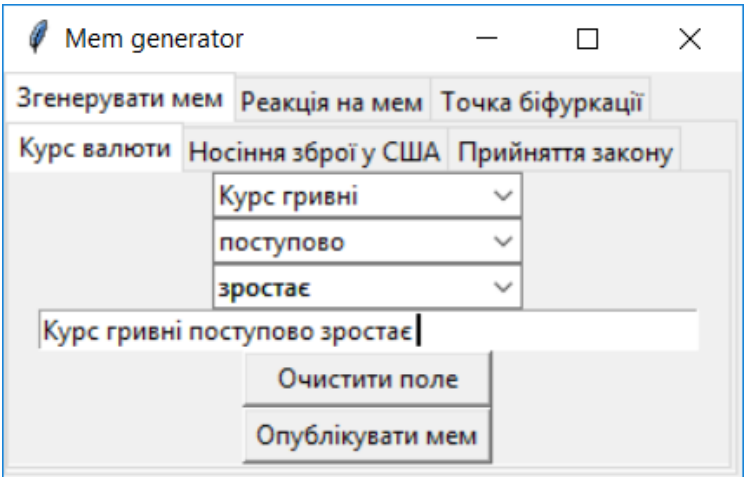


Рисунок 1 – Інтерфейс мем-генератора

Для прикладу був сформований і опублікований мем – “Курс гривні поступово зростає” Після розповсюдження сформованого мема, вирішується одне з базових питань – досліджується реакція відповідного соціуму на відповідну інформацію. Варіант відгуку на розповсюджений мем представлений на рис.2.

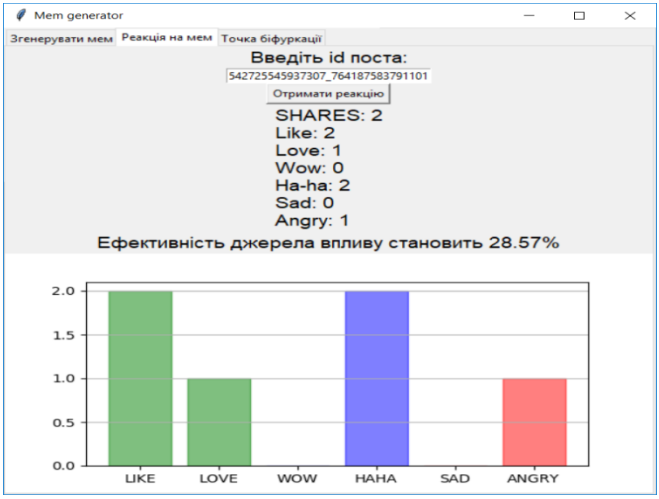


Рисунок 2 – Реакція на розповсюджений мем

Аналіз реакції на розповсюджений мем дозволяє підготувати рішення щодо оцінювання стійкості соціальної складової і всієї системи в цілому [2]. У доповіді наведено приклад моделі інформаційного впливу, а на рис.3 представлена ймовірна динаміка "інфікування" соціуму за допомогою так званої "експоненціальної моделі" інформаційного впливу і визначення точки біфуркації соціуму системи.

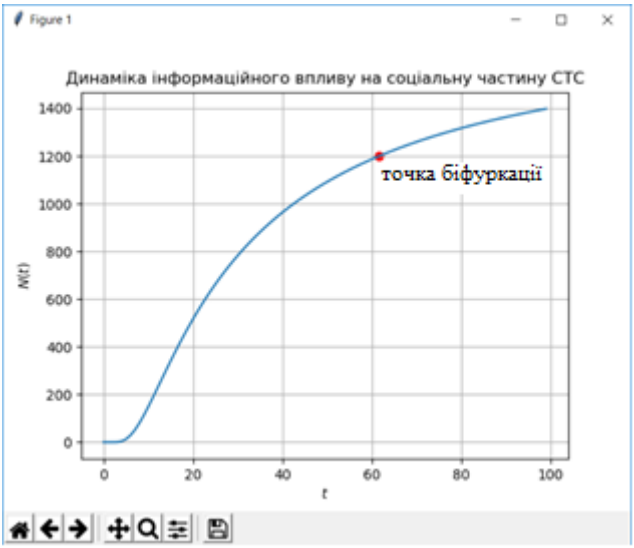


Рисунок 3 – Ймовірна зміна стану соціуму

Висновки. Запропоновано підхід щодо тестування або реакції соціальної складової СТС на спеціально підготовлену і розповсюджену інформацію – мем. Аналіз результатів впливу дозолить прийняти рішення щодо стану соціуму, результатів сприйняття ним тієї чи іншої інформації, як змінити інформацію для досягнення бажаного результату та захисту від деструктивних інформаційних впливів.

Список літератури

1. Дудатьєв А. В. Технологии информационной войны: концепция мем-программирование / А. В. Дудатьєв // Безпека інформації. – 2015. –№ 4–. – С.56-61.

2. Дудатьев А. В. Метод оценки информационной устойчивости социотехнических систем в условиях информационной войны / А. В. Дудатьєв, В. А Лужецкий, Д. А. Коротаев // Восточно-Европейский журнал передовых технологий. – 2016. – № 1. – С.4-11.

УДК 04.056:004.738.5

Усовершенствованый классификатор на основе синергетической модели угроз

Комышан А.С., аспірант,
Евсеев С.П.., к.т.н., с.н.с.
Харьковский национальный экономический университет имени Семена Кузнеца, г. Харьков

Основной задачей исследований в области безопасности организаций банковского сектора (ОБС) является разработка новых и усовершенствование имеющихся методик оценки уязвимости (рисков), нанесения ущерба ОБС в целом или отдельным составляющим компонент автоматизированных банковских систем (АБС). Для построения системы безопасности банковских информационных ресурсов (БИР), как правило используется модель ЦКД (целостность, конфиденциальность, доступность) и соответствующие классификаторы угроз составляющих безопасности БИР: информационной безопасности, кибербезопасности, безопасности информации [1 – 4]. Авторами предложен усовершенствованный классификатор на основе синергетической модели угроз на составляющие безопасности БИР.

Предложенный классификатор формируется из четырех кортежей, соответствующих платформ [2]:

первая платформа – классификация угроз по отношению к составным обеспечения безопасности БИР в АБС ОБС: информационная безопасность (ИБ) (01), безопасность информации (БИ) (02), кибербезопасность (КБр) (03). При этом введем следующие определения:

Безопасность банковской информации (Б БИР) – состояние защищенности банковской информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность аутентичность и доступность БИР при ее обработке в АБС.

Информационная безопасность банковской информации (ИБ БИР) – состояние защищенности информационной среды ОБС, обеспечивающее ее формирование, использование и развитие в интересах граждан и ОБС.

Кибербезопасность банковской информации (КБ БИР) – набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды АБС, ресурсов и пользователей ОБС;

вторая платформа – классификация угроз по характеру

направлений: нормативно-правовое (01), организационное (02), инженерно-техническое (03);

третья платформа – классификация угроз в соответствии с основными особенностями информации: конфиденциальность (01), целостность (02), доступность (03), аутентичность (04);

четвертая платформа – классификация угроз по уровням иерархии инфраструктуры АБС: FL – физический уровень (01), NL – сетевой уровень (02), OSL – уровень операционных систем (ОС) (03), DBL – уровень систем управления базами данных (04), BL – уровень банковских технологических приложений и сервисов (05).

Описание усовершенствованного классификатора угроз состоит из четырех числовых величин: – составная обеспечения безопасности БИР в АБС ОБС: информационная безопасность (ИБ) (01), безопасность информации (БИ) (02), кибербезопасность (КБ) (03); – характер направлений: нормативно-правовое (01), организационное (02), инженерно-техническое (03); – основные особенности информации: конфиденциальность (01), целостность (02), доступность (03), аутентичность (04); – уровни иерархии инфраструктуры АБС: FL – физический уровень (01), NL – сетевой уровень (02), OSL – уровень операционных систем (ОС) (03), DBL – уровень систем управления базами данных (04), BL – уровень банковских технологических приложений и сервисов (05). Такой подход к формированию классификатора позволяет получать синергетическую и гибридную характеристики угроз на составляющие безопасности БИР, формировать обоснованные превентивные меры по использованию технических средств защиты информации.

Список литературы

1. Евсеев С. Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины / С. Евсеев. // Науково-технічний журнал "Безпека інформації". – 2016. – С. 297 – 309.
2. Евсеев С. Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода / С. Евсеев. // Науково-технічний журнал "Інформаційна безпека". – 2017. – С. 110 – 119.
3. Евсеев С. Анализ оценки рисков кибербезопасности банковской информации / С. Евсеев, О. Король, А. Сочнева. // Сборник научных трудов НАУ "Защита информации". – 2016. – С. 109 – 128.
4. Евсеев С. Синергетическая модель оценки безопасности банковской информации / С. Евсеев. // Науково-технічний журнал "Інформаційна безпека". – 2016. – С. 104 – 118.

УДК 32.019.5:351.86

Підхід до виявлення прихованого деструктивного психологічного впливу

Завада А.А.[1] начальник науково-дослідної лабораторії, к.т.н., с.н.с.,
Міхєєв Ю.І.[1], провідний науковий співробітник, к.т.н.,
Рогов П.Д.[2], старший науковий співробітник, к.т.н.
[1]Житомирський військовий інститут ім. С. П. Корольова, м. Житомир
[2]Національний університет оборони України ім. Івана Черняховського, м. Київ

Аналіз світового досвіду ведення війн та воєнних конфліктів підтверджує факт зростання масштабів використання прихованого деструктивного психологічного впливу (ПсВ) спецслужбами провідних країн світу на визначені цільові аудиторії (ЦА) для реалізації своїх воєнно-політичних цілей щодо спричинення масових заворушень та акцій протестів населення проти діючої влади задля її зміни чи блокування.

Враховуючи стрімкий процес інформатизації усіх галузей діяльності людини та держави в цілому, відбулось суттєве зростання ролі інформаційної боротьби, яка в сучасних війнах та конфліктах навіть перевищує збройну боротьбу, протистояння зміщується в інформаційний простір, що призводить до так званої гібридизації війни (конфлікту). Процес ведення гібридної війни ніколи не буває випадковим або відособленим. Він містіть узгоджену діяльність по використанню інформації, як зброї, для ведення бойових дій – будь-то на реальному полі бою, або в економічній, політичній, соціальній та перш за все, інформаційній сфері.

Одним з актуальних завдань, що виникає під час протистояння держав у гібридній війні, є виявлення та своєчасна протидія прихованому деструктивному ПсВ, що в свою чергу передбачає виконання ряду етапів, а саме: моніторингу інформаційного простору; виявлення інформаційних повідомлень з ознаками деструктивного ПсВ; визначення рівня загрози від цих впливів; розроблення пропозицій щодо нейтралізації деструктивних ПсВ та прогнозування подальшого розвитку ситуації.

Не зважаючи на те, що сьогодні в Україні завданню із забезпечення інформаційної безпеки держави приділяється значна увага, одним з проблемних питань залишається формування єдиного підходу щодо своєчасного виявлення та оперативного оцінювання рівня деструктивного ПсВ на ЦА.

У доповіді наведено особливості виконання завдань з виявлення деструктивних ПсВ та оцінювання потенційних можливостей негативного ПсВ на ЦА, що здійснюється за такими етапами: встановлення цілі ПсВ (відомості про ЦА, методи ПсВ, терміни досягнення очікуваних

результатів); вибір способу (критеріїв) оцінювання результатів ПсВ; встановлення оптимального механізму збирання інформації.

Одним з часто вживаних на практиці підходів до оцінювання рівня деструктивного ПсВ є підхід, запропонований С. Катлипом. Згідно з цим підходом оцінювання ПсВ може здійснюватися за трьома етапами:

1. Оцінювання якості підготовки до психологічних заходів, якому підлягає: адекватність початкової інформації загальному задуму; відповідність змісту повідомлення цілі, яку передбачається досягнути за допомогою психологічної акції; якість подання інформації.

2. Оцінювання дій, полягає у вимірюванні кількості: повідомлень, які було поширено; повідомлень, які було отримано ЦА; кількості повідомлень, на які зреагувала ЦА.

3. Оцінювання рівня впливу, який спрямований на зміну переконань, поглядів та поведінки ЦА.

Оцінювання рівня ПсВ на ЦА полягає у визначенні ефекту (рівня), який він спричинив:

– кількість осіб з числа ЦА, які змінили свою думку на іншу або протилежну;

– кількість осіб з числа ЦА, які одноразово виконали дії відповідно до змісту повідомлення;

– кількість осіб з числа ЦА, які слідують поведінці, яка нав'язується повідомленням;

– зміни у соціальній та культурній сферах.

Очевидно, що запропонований підхід частково дозволить забезпечити психологічний захист особового складу Збройних Сил України від деструктивного ПсВ шляхом виявлення певних ознак, що повинні стати засобом для розкриття цілей психологічних операцій (акцій) противника.

Ефективність інформаційно-психологічної протидії досягається тим, що вона планується та здійснюється з урахуванням особливостей деструктивного впливу, реального морально-психологічного стану особового складу і населення та обстановки, що складається, при цьому протидія ведеться безперервно і комплексно.

Метою протидії є нейтралізація деструктивного ПсВ (недопущення деморалізації особового складу військ (сил) військових формувань) та подальша зміна на свою користь співвідношення морально-психологічних стійкостей протиборчих сторін, підтримка цієї стійкості наших сил на рівні, необхідному для успішного виконання покладених (бойових) завдань. Для досягнення поставленої мети необхідно ефективно вирішити наступні завдання:

– аналіз суспільно-політичної обстановки та морально-психологічного стану особового складу військ (сил);

– збір, аналіз та узагальнення даних про можливості здійснювати деструктивний ПсВ противника на місцеве населення;

– аналіз змісту матеріалів засобів масової комунікації, прогнозування

ймовірного характеру та можливих наслідків здійснюваних психологічних операцій (акцій);

– участь у визначенні основних завдань і плануванні заходів з урахуванням особливостей ПсВ;

– участь у проведенні заходів щодо послаблення (нейтралізації, нівелювання, усунення) деструктивного ПсВ противника;

– недопущення поширення дезинформації, проявів паніки, розгубленості серед особового складу військ (сил) та місцевого населення;

– організація взаємодії з можливими союзниками на користь спільної реалізації інформаційно-психологічного протиборства.

Основними засобами інформаційно-психологічної протидії є:

– превентивне регулярне інформування, що передбачає:

а) роз'яснення цілей і завдань психологічних акцій (їх спрямованості, істинних намірах та інтересів);

б) роз'яснення прийомів і техніки ведення психологічних акцій;

в) прогнозування тематики і символіки психологічних акцій з метою попередження дій, зниження їх ефективності або нейтралізації;

– цензорський контроль матеріалів засобів масової комунікації, посилення режиму заходів на теле- і радіостанціях, в редакціях, видавництвах та поліграфічних підприємствах;

– виявлення осіб, що поширюють чутки та домисли, літературу, аудіо- і відеоматеріали, що компрометують владу, ґрунтуючись на національних та релігійних відмінностях;

– контроль громадської думки в умовах деструктивного ПсВ;

– оцінка уразливості масової свідомості від деструктивного ПсВ, прогнозування можливих наслідків.

Інформаційно-психологічне протиборство повинне відповідати певним вимогам:

– активність – досягається визначеністю цілей і завдань, організацією попереджуючих впливів;

– актуальність та конкретність – забезпечується націленістю на найбільш значущі проблеми;

– систематичність – досягається постійним збиранням та аналізом інформації про морально-психологічний стан особового складу й населення, здійсненням протидії відповідно до вирішуваних завдань;

– динамічність і своєчасність – забезпечується оперативним реагуванням на зміну суспільно-політичної, оперативної та бойової обстановки;

– дохідливість – досягається використанням простих і доступних для особового складу аргументів;

– емоційність – забезпечується проведенням емоційно-насичених інформаційних та психологічних заходів, поєднанням раціональних і емоційних начал психіки.

Практика показує, що людина неспроможна захиститися від впливу всіх здійснюваних на нею маніпулятивних впливів. Це пов'язано, по-перше, з тим, що за наявністю великої кількості впливів об'єкт не здатний самостійно оцінювати свій психологічний стан. По-друге, часто адресат сприймає маніпуляцію тільки на підсвідомому рівні, навіть здогадуючись про факт її присутності. У такій ситуації необхідно постійно бути готовим до того що, відбувається маніпуляція. Однак, сильний прояв впливу у деяких випадках усе ж таки можна виявити й не допустити. Саме тому дуже важливо мати навички з виявлення методів впливу. Для цього необхідно розвивати стратагемне та критичне мислення військовослужбовців; проводити роз'яснення суті, цілей, завдань, тематики, форм і методів проведення психологічних операцій.

УДК 004.056.5

Исследование методов авторизации пользователей в информационных системах

Кешку Александр, студент 4 курса
Научный руководитель – Охрименко С.А. д.э.н., профессор
Экономическая Академия Республики Молдова

На сегодняшний день информационные системы разного масштаба стали важной составляющей базисной инфраструктуры страны, коммерции, социума. Все больше защищаемой информации переносится в информационные системы. На данный момент информационные технологии не только предоставляют новые возможности организации бизнеса, ведения гос. и социальной деятельности, но и создают многообещающие потребности в обеспечении безопасности для защиты данных. По некоторым данным, более двадцати пяти процентов злоупотреблений данными в информационных системах совершаются внутренними юзерами и партнерами, имеющими непосредственный доступ к информационной системе. Вплоть до семидесяти процентов из них – эпизоды неразрешенного получения прав, кражи и передачи персональных данных пользователей информационных систем, что становится возможным из-за несовершенства технологий дифференциации доступа и аутентификации юзеров[1]. Усовершенствование способов системы управления доступом и регистрации юзеров является одним из главных течений развития информационных систем. Главными процессами регистрации юзера в информационной системе являются процесс идентификации и аутентификации.

Идентификацию и аутентификацию считают базой программно-технических средств безопасности.

Аутентификация проверяет подлинность предоставленного юзером идентификатора, а идентификация – присваивание юзеру идентификатора под которыми система "узнает" его[2].

Идентификация и аутентификация – это 1-ая линия защиты, "проходная" информационного пространства компании. Идентификация дает возможность субъекту назвать себя. Посредством аутентификации 2-ая сторона удостоверяется, что человек на самом деле тот, за кого себя выдает. Иногда вместо слова "аутентификация" в некоторых случаях применяют сочетание слов "контроль подлинности".

Аутентификация бывает:

- Односторонней. Односторонняя аутентификация устанавливает взаимообмен данными только лишь в 1 направлении;

- Двусторонней. Двусторонняя аутентификация включает данные, в виде ответа для проверяющей стороны с директивами корректности идентификаторов для доказывающей стороны;
- Трёхсторонней. Трехсторонняя аутентификация включает вспомогательную передачу информации от доказывающей стороны проверяющей.

В зависимости от применяемых криптографических алгоритмов, протоколы аутентификации подразделяются на протоколы, основанные: на симметричных алгоритмах шифрования, однонаправленных ключевых хэш-функциях, асимметричных алгоритмах шифрования, алгоритмах цифровой электронной подписи.

Механизм идентификация и аутентификация пользователей включает:

1. Юзер предоставляет индивидуальный идентификатор.
2. Впоследствии система сопоставляет предоставленный идентификатор с остальными находящимися в ее бд идентификаторами.
3. Если пользователь прошел предшествующие пункты успешно, то ему предоставляют доступ к информационной системе. В противном случае появляется сообщение об ошибке и система предлагает повторно ввести идентификатор.

Если же юзер превышает предел допустимых повторов ввода идентификатора, система временно блокируется или же следует другим заданным инструкциям.

Методы аутентификации включают:

- Аутентификация при помощи электронной подписи
- Аутентификация по паролям
- Аутентификация с помощью SMS
- Биометрическая аутентификация
- Аутентификация, основанная на местоположении выхода в интернет

Аутентификация при помощи электронной подписи:

Имеется ряд методик построения цифровой подписи: на основе алгоритмов симметричного шифрования, на основе алгоритмов асимметричного шифрования.

Аутентификация с помощью SMS:

Подтверждение посредством SMS-кодов функционирует достаточно легко. Юзер, вводит личный логин и пароль, уже после чего на его мобильный телефон отправляется SMS с кодом, который необходимо ввести для входа в аккаунт. При следующем входе генерируется уже другой SMS-код, действующий только для текущей сессии.

Биометрическая аутентификация:

Биометрическая система на этапе регистрации вносит образец биометрической черты юзера посредством датчика — к примеру, снимает лицо на камеру. Позже из биометрического образца извлекаются

индивидуальные черты — к примеру, небольшие детали линий пальца. Система хранит извлеченные черты в качестве шаблона в базе вместе с другими идентификаторами (имя, идентификационный номер). Для аутентификации юзер предоставляет считывателю еще один биометрический экземпляр. Черты, извлеченные из него, представляют собой требования, которые система сопоставляет с шаблоном заявленной личности с помощью алгоритма сопоставления [3].

Аутентификация, основанная на местоположении выхода в интернет:

Этот механизм базируется на применении информации о месторасположении серверов, точек доступа wi-fi, посредством которых осуществляется присоединение к сети. Условная легкость взлома заключается в том, что данные о месторасположении можно поменять, применяя так называемые прокси-серверы или системы анонимного доступа.

Аутентификация по уровню информационной безопасности делится на три категории:

- Статическая аутентификация;
- Устойчивая аутентификация;
- Постоянная аутентификация.

1-ая группа гарантирует защиту только от несанкционированных действий в системах, где нарушитель не может во время сеанса прочитать аутентификационные данные. Примером средства статической аутентификации являются обычные пароли. Их результативность зависит от сложности угадывания паролей и, собственно, от того, насколько хорошо они защищены.

Устойчивая аутентификация применяет динамические данные аутентификации, меняющиеся с каждым сеансом работы. Реализациями устойчивой аутентификации являются системы, использующие одноразовые пароли и электронные подписи. Устойчивая аутентификация обеспечивает защиту от атак, где правонарушитель может перехватить аутентификационные данные и применять их в следующих сеансах работы.

Постоянная аутентификация считается более надежной вследствие того, что гарантирует идентификацию каждого блока передаваемой информации, что защищает их от несанкционированного изменения. Примером является применение алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.

Выводы:

Идентификация и аутентификации применяется с целью ограничения доступа случайных и незаконных субъектов информационных систем к ее объектам. Единый метод деятельности подобных концепций состоит в том, чтобы получить от юзера данные, подтверждающие его личность, проверить ее достоверность и предоставить ему возможность работы с

системой. В последнее время получили распространение совмещенные методы идентификации и аутентификации, требующие, кроме наличия пароля, наличие токена — особого устройства, подтверждающего подлинность юзера. В случае успеха авторизации, система обязана определить его полномочия. Это необходимо для последующего контроля и разграничения доступа к ресурсам. Но главным условием как оказалось является цена концепции. Большинство из имеющихся на рынке решений слишком сложны и дороги в реализации и поддержке. Система, требующая наличие токена или отправки кода через SMS на мобильный телефон, делает процесс авторизации более сложным. В любом случае технологии идут вперед и с каждым годом внедряются все больше систем и моделей авторизации, которые обязаны защитить нас и нашу информацию от третьих лиц.

Список литературы

1. Блинов А. Информационная безопасность – СПб.: Издательство «СПбГУЭФ», 2010. – 96 стр.

2. Смит Р.Э. Аутентификация: От паролей до открытых ключей. – М.: Издательство «Вильямс», 2002. – 432 стр.

3. Мельников В.П., Клейменов С.А. Информационная безопасность и защита информации. – М.: Издательский центр «Академия», 2013. – 336 стр.

УДК 004.421.5

Моделювання математичного більярду Сіная для отримання випадкових двійкових послідовностей чисел

Коломієць Д.О. студент 4 курсу
Науковий керівник – Собінов О.Г., викладач
Центральноукраїнський національний технічний університет, м. Кропивницький

Вступ. Як відомо для аналізу криптостійкості алгоритмів шифрування використовують випадкові та псевдопипадкові двійкові послідовності. Випадкові послідовності отримують або за допомогою ірраціональних чисел типу π, е, $\sqrt{2}$ і т.д., або з використанням аналогових систем з природним «шумом». У першому випадку псевдовипадковий числовий ряд (ПВЧР) використовують для аналізу, у другому випадку для шифрування. Але такий тип шифрування не є двостороннім і не може бути повтореним.

В математиці існує розділ, який має назву математичний більярд. За допомогою методів математичного більярду можна отримати ПВЧР безмежної довжини. Відома теорема Колмогорова-Сіная, в якій стверджується, що ентропія динамічної системи це:

$$h(T) = \sup_{\xi} h(T, \xi), \tag{1}$$

де sup береться по всім кінцевим розбиттям ξ.

Як показано в [1], можна створити криптосистему передачі й зберігання даних на основі більярда Сіная.

Викладення основного матеріалу. Для перевірки працездатності і надійності застосування теоретичної системи, розроблено програмне забезпечення, яке моделює поведінку такої системи для подальшого теоретичного аналізу системи.

Математичну модель побудовано на основі тривіальних математичних залежностей з курсу математики за 10-11 клас.

Розроблене програмне забезпечення моделює переміщення математичної точки (кулі) в прямокутній площині mXn, при цьому повинні виконуватися три наступні умови: сторони прямокутника задається взаємо простими числами; кут відбиття дорівнює вхідному куту; на площині знаходиться «шайба», діаметр якої дорівнює половині меншої стороні; при зіткненні кулі з шайбою шайба зміщується на $\Delta x \Delta y$.

В програмному забезпеченні математичної моделі враховують напрямок руху малої кульки та значення кутового коефіцієнту, звідки вибирається одна з можливих точок перетину. Перевірка напрямку

спрощує алгоритм роботи програми. Програмне забезпечення, яке реалізує математичну модель має велику швидкість роботи.

Формування ПВРЧ в даному алгоритмі виконується наступним чином, верхня та права сторона визначається як 1, а нижня та ліва як 0. Згідно з теоремою Сіная через Δt часу траєкторія руху кулі стане хаотичною і, навіть, знаючи поточну координату кулі, неможливо відновити всю її траєкторію, навіть, знаючи початкові координати кулі і шайби.

Висновки. Розроблено математичну модель та програмне забезпечення на її основі, що дозволяє формувати великі двійкові ПВРЧ послідовності, за допомогою яких можна виконувати криптографічне шифрування великих масивів даних. Якщо система використовується для власного вжитку, то ключем для системи є mXn, координата кульки, координата шайби і таймер для встановлення початкових даних - $x_к y_к$, $\Delta x_к \Delta y_к$ $x_ш y_ш$ і дані з RTC для задання цих параметрів. При використанні системи у вигляді Point-Point краще за все використовувати окремі додаткові прилади на основі мікроконтролерів, які забезпечують даний вид шифрування. Таких підхід дозволяє створювати окремі апаратно-захищені модулі, доступ до яких захищений на апаратному рівні (встановлено біт зчитування). У цьому випадку кожна пара приладів має відповідно парно встановлені початкові дані, які при передачі і дешифруванні використовують у якості відкритого ключа дані з RTC. Отримані на практиці масиви ПВРЧ вимагають подальшого вивчення і перевірки двійкових послідовностей методами NIST.

Список літератури

1. Собінов О.Г. Програмно-апаратний генератор псевдовипадкових чисел на основі мікроконтролерів / О.Г. Собінов, Д.О. Коломієць // Актуальні задачі та досягнення у галузі кібербезпеки: матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. / Кіровоград. нац. техн. ун-т, Черкас. держ. технолог. ун-т та ін. – Кропивницький : КНТУ, 2016. – 209 с.

2. Гальперин Г.А. Математические бильярды (бильярдные задачи и смежные вопросы математики и механики) / Г.А. Гальперин., А.Н. Земляков. – М.: Наука. 1990. – 288 с.

3. Земляков А. Математика бильярда / А. Земляков // Квант. – 2002. – №5. – С.17-18.

УДК 004.056.55

Дослідження покращеного багатокрокового 2D RSA шифру та його гістограмно-ентропійних характеристик

Красиленко В.Г., к.т.н., с.н.с., доцент, Нікітович Д.В.
Вінницький національний технічний університет, м. Вінниця

Вступ, аналіз останніх досліджень, публікацій. З кожним роком в епоху масових інформаційно-комунікаційних технологій (ІКТ) зростає частка задач, що стосуються захисту конфіденційної, секретної інформації у вигляді багатовимірних сигналів, різноманітних багато-спектральних, кольорових зображень (З), текстографічних документів (ТГД), 2D, 3D масивів, для яких необхідно виконувати криптографічні перетворення (КП). Це спричинило суттєвий ріст числа публікацій, присвячених КП зображень, і появі робіт [1, 2], що зорієнтовані на матричні моделі (ММ), алгоритми та засоби паралельної обробки, та подальшу активізацію досліджень у цьому напрямку [3-8]. А тому, з урахуванням збільшення сфер застосувань КП З та вимог до них, в тому числі до їх ефективності, криптостійкості, актуальним завданням є як удосконалення ММ, шифрів КП і покращення їх характеристик, так і методів вимірювання, оцінювання останніх. Вперше ММ були запропоновані в [1], модифікації RSA на матричний випадок у [2], які пізніше були використані і для створення електронних цифрових підписів (ЕЦП) для любих ТГД: сліпих ЕЦП на основі матричних афінних шифрів [4], ЕЦП матричного типу на базі модифікацій алгоритму RSA і Ель-Гамаля на 2D випадок [5], де були продемонстровані їх можливості та переваги і введено підклас ММ матричного типу (МТ) або 2D. Результати моделювання таких ММ наводилися, за рідким винятком, лише для невеликих (128×128 ел.) масивів чорно-білих зображень [2, 5], а гістограмно-ентропійним властивостям приділялась мало уваги.

Постановка задачі. Тому метою даної роботи є вивчення функціональних можливостей удосконалених модифікацій 2D RSA для КП З шляхом моделювання у Mathcad на конкретних З, ТГД та оцінювання їх характеристик, переваг на основі ентропійного аналізу та демонстрації криптограм, виду їх гістограм.

Виклад основного матеріалу, результатів дослідження. Ідея узагальнення на 2D випадок класичного скалярного RSA та похідних від нього алгоритмів [2, 5, 9] полягає у виборі в якості ключів не скалярів, а відповідних матричних ключів (МК) матриць K та L з елементами попарно простих чисел k_i,j та l_i,j , таких щоб їх добуток n_i,j трохи перевищував значення елемента масиву, що підлягає КП. Кожен елемент матриць K та L вибирається з множини значень відповідних скалярних ключів e_i,j та d_i,j, тобто значення елементів KEY(E)_i,j та KEY(D)_i,j

публічного МК KEY(E) та приватного МК KEY(D) вибираються з множини чисел взаємно простих з n_i,j (потужність якої визначається за функцією Ейлера від n_i,j). У загальному випадку 2D масив елементів n_i,j є матрицею різних чисел, а потужність множини МК залежить як від потужності множини допустимих значень для кожного елемента так і від кількості елементів у масиві, що забезпечує прийнятні високі для неї значення, наближена оцінка якої ((k-1)*(l-1))^(N*N), де N*N - вимірність масиву. Відомо, що не існує жодного ефективного алгоритму розв'язування задачі обчислення дискретного логарифма за модулем, а тому **розширення** та ускладнення задачі на 2D випадок, особливо за рахунок **збільшення потужностей множин** МК при значних N*N є першим фактором ускладнення розв'язування вище вказаної задачі. Для ще більшого її ускладнення ми пропонуємо так званий **покращений багатокроковий алгоритм**, для якого базову процедуру (у RSA MT) поелементно-матричного піднесення у степінь за відповідними модулями (ПЕМПуСМ), описану в [2, 5], сторони процесу КП **повторюють певну кількість разів**, використовуючи узгоджені публічні та приватні МК. Таке повторення процедур сторонами з утворюваними черговими на попередніх кроках криптограмами чи відновлюваними з них масивами покращує стійкість КП [9]. Але як показали деякі модельні експерименти [5, 9], для специфічних видів З, ТГД, що містять фрагменти з рівними значеннями яскравості елементів, після ПЕМПуСМ у криптограмах залишаються форми та види цих фрагментів, тому **додатково необхідно закривати** З публічним ключем KEY(E) 2-ої сторони перед зашифруванням 1-ою стороною та додатково відкривати цим же ключем після обернених процедур розшифрувань 2-ою стороною. Елементи криптограми CMD для явної матриці T (чи закритої її версії) у RSA MT, обчислюються 1-ою стороною при використанні елементів e_i,j публічного ключа KEYPD 2-ої сторони процедурою за формулою: CMD_i,j ≡ T_i,j^ e_i,j mod n_i,j. Утворену і надіслану CMD 2-а сторона аналогічною процедурою розшифровує, використовуючи свій приватний ключ OKEYD, обчислюючи TV_i,j ≡ CMD_i,j^d_i,j mod n_i,j чи ще й розкриває, якщо T було закрито. На рис.1 показані основні формули з вікон Mathcad, що були взяті для моделювання покращеного багатокрокового 2D RSA шифру, а результати КП ТГД формату A4 (704*572 ел.), представлені на рис.2,3 та підтверджують правильну роботу шифру і потребу у додатковому закритті (рис.3). Протоколи узгодження МК розглядались у роботах [6, 7], а тому, з урахуванням обмежень, тут не розглядаються, а будуть висвітлені та продемонстровані у доповіді.

Результати КП одного кольорового З нашим багатокроковим 2D RSA шифром показані на рис.4. Фрагменти вікон Mathcad з виглядом розроблених програмних модулів для визначення ентропій та побудови гістограм показані на рис.5, з яких видно, що ентропія складових криптограми досягала 7,97-7,98 біт на елемент З (майже 8!), навіть для ТГД з ентропією всього в 1-3 біта.

Рис.1 Програмні модулі (з вікон Mathcad), що використовувались для моделювання 2D RSA алгоритму

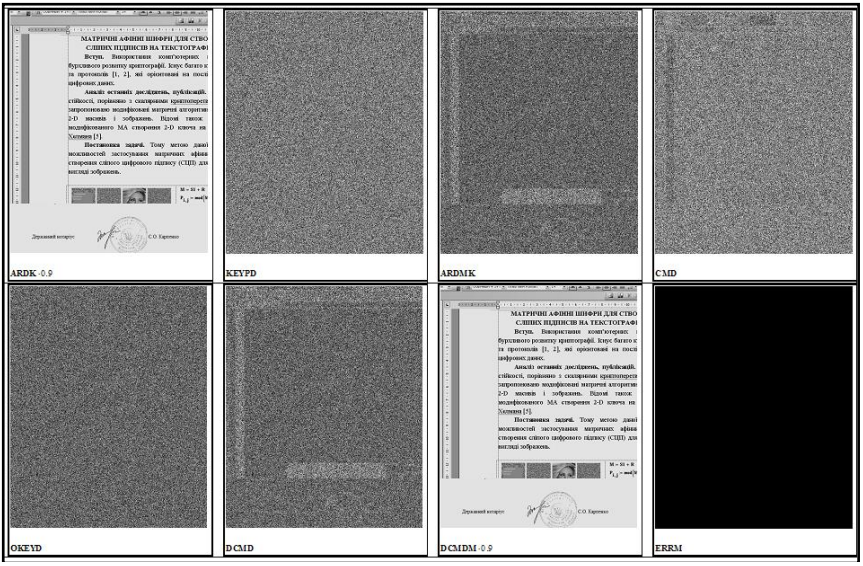


Рис.2 Результати КП ТГД (А4) покращеним 2D RSA алгоритмом. У верхньому ряду зліва направо: скоригований ТГД, публічний МК 2-ої сторони, закритий ним ТГД, криптограма CMD; у нижньому: приватний МК 2-ої сторони, розшифрований ним, додатково розкритий ТГД та його верифікація

Висновки: Запропоновані і промодельовані покращені багатокрокові 2D_RSA моделі та алгоритми КП зображень та текстографічних документів (ТГД), що враховують їх специфіку, адаптуються до різних форматів, мають покращені характеристики. Наведені програмні модулі з вікон Mathcad, формули, описані алгоритмічні кроки процедур КП. Досліджені гістограмно-ентропійні характеристики і показано збільшення ентропії криптограм до 7,98 біт/ел. Низкою модельних експериментів у Mathcad на реальних З, ТГД продемонстровані функціональні можливості та адекватність моделей таких шифрів МТ та криптосистем на їх основі.

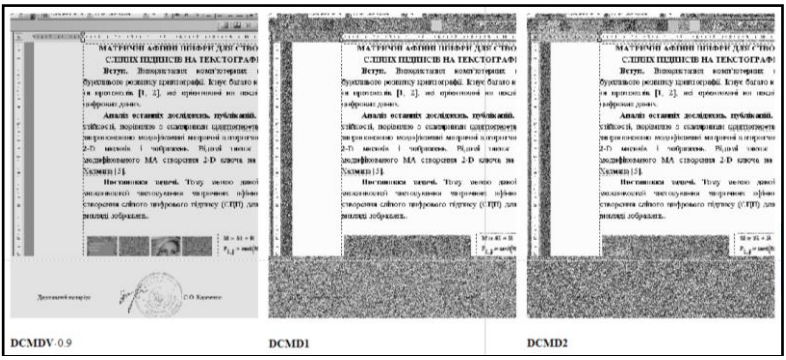


Рис.3 Вигляд розшифрованих ТГД (А4) багатокроковим 2D RSA шифром відповідно після 1-го (DCMD2), 2-го (DCMD1) та 3-го (DCMDV) кроків без додаткових закриття (розкриття) тим же публічним МК.

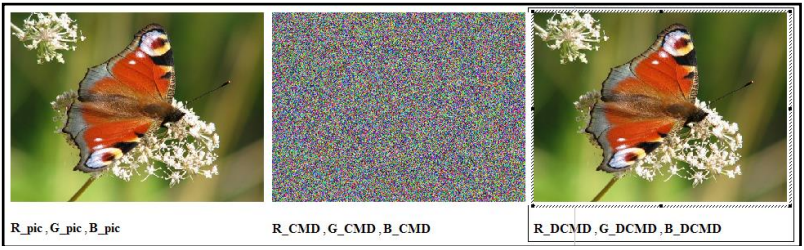


Рис.4 Результати КП кольорового 3 за допомогою 2D RSA алгоритму: явне 3, його криптограма, розшифроване 3

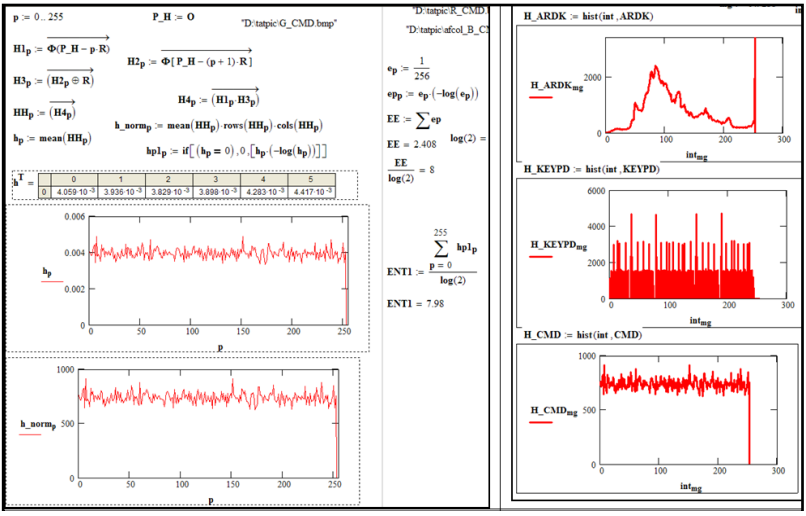


Рис.5 Програмний модуль для визначення ентропії R,G,B складових зображення 3 (ліворуч) та гістограми його G складової, публічного МК, G криптограми

Список літератури

1. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісн. нац. ун-ту "Львів. політехніка". – 2009. – № 658. – С. 59-63.

2. Красиленко В.Г. Модифікації системи RSA для створення на її основі матричних моделей та алгоритмів для зашифрування та розшифрування зображень / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – 2012 . – №8(106).–С.102-106.

3. Красиленко В. Г. Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень / В. Г. Красиленко, С. К. Грабовляк // Системи обробки інформації. – 2012. – Вип. 3(2). – С. 53-61. – Режим доступу: http://nbuv.gov.ua/UJRN/soi_2012_2_3_15

4. Красиленко В.Г. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 7(97). – С. 60 – 63.

5. Красиленко В.Г. Демонстрація процесів створення сліпих електронних цифрових підписів на текстографічну документацію на основі моделей матричного типу / В.Г. Красиленко, Р.О. Яцковська, Ю.М. Тріфонова, // Системи обробки інформації. – 2013. – Вип. 3(110). – Т. 2. – С. 18 – 22.

6. Красиленко В.Г. Моделювання протоколів узгодження секретного матричного ключа для криптографічних перетворень та систем матричного типу / В.Г. Красиленко, Д.В. Нікітович // Системи обробки інформації. – 2017. – Вип. 3 (149). – С 151-157.

7. Красиленко В.Г. "Моделювання багатокрокових та багатоступеневих протоколів узгодження секретних матричних ключів" / В.Г. Красиленко, Д.В. Нікітович // Комп`ютерно-інтегровані технології: освіта, наука, виробництво: науковий журнал. – Луцьк: Луцький національний технічний університет, 2017. – Вип. 26. – С 111-120. - Режим доступу: http://ki.lutsk-ntu.com.ua/node/134

8. Красиленко В.Г. Удосконалення та моделювання матричних афінних шифрів для криптографічних перетворень зображень / В.Г. Красиленко, Д.В. Нікітович // Електроніка та інформаційні технології: збірник наукових праць. – Львів: Львівський національний університет імені Івана Франка, 2017. – Вип. 7. – С 20-42. – Режим доступу: http://elit.lnu.edu.ua/pdf/7_3.pdf

9. Красиленко В.Г. Вдосконалення та моделювання електронних цифрових підписів матричного типу для текстографічних документів / В.Г. Красиленко, Д.В. Нікітович // Матеріали VI міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології» (ІУСТ-Одеса-2017), Одеський національний морський університет, 20-22 вересня 2017р. – Одеса: «ВидавІнформ НУ «ОМА», 2017. – С. 312 -318.

УДК 004.056.55

Дослідження, систематизація та первинний аналіз кодових схем електронного цифрового підпису

Кузнецов О.О., доктор технічних наук, професор кафедри безпеки інформаційних систем і технологій,
Кіян А.С., студентка 4-го курсу,
Деменко Є.Є., студент 1-го курсу
Харківський національний університет ім..В.Н.Каразіна, м. Харків

Уже досить давно теоретично доведено факт того, що квантові обчислення суттєво прискорюють рішення багатьох математичних задач таких, як факторизація, дискретне логарифмування і т.п. На складності вирішення зазначених задач ґрунтується стійкість більшості з існуючих криптографічних алгоритмів [1-3]. Активні роботи в області розробки квантового комп'ютера спонукали Національний інститут стандартів і технологій (NIST) оголосити про початок конкурсу для відбору претендентів на стандарти пост-квантових алгоритмів, рішення щодо яких планується прийняти в 2020-2022 роках [3]. Нині в межах конкурсу представлено 82 проекти, 23 з яких обґрунтовують схеми електронного цифрового підпису (ЕЦП). Роботи у сфері пост-квантової криптографії ведуться у 5 різних напрямках [1-3]. Варто відзначити, що найбільше досліджень зосереджено в області криптографії, заснованої на решітках (всього подано 28 проектів) та на кодах (20 претендентів на стандартизацію) [4]. Особливістю конкурсу, оголошеного NIST, є те, що на нього можуть бути подані алгоритми, які базуються на математичних методах, які є недостатньо випробуваними. Вищезгаданий факт обумовлює актуальність всебічного вивчення представлених проектів, їх порівняльних аналіз, а також оцінку їх захищеності. В межах даної роботи ми обмежимося дослідженням алгоритмів ЕЦП, що засновані на кодах, проведемо їх первинний аналіз та систематизацію. На сьогодні автори представили 3 різних схеми формування та перевірки ЕЦП, алгоритми яких базуються на кодових криптосистемах: pqsigRM, RaCoSS, RankSign. Розглянемо поступово кожну з цих схем.

Схема pqsigRM. Схему pqsigRM було розроблено групою дослідників з Кореї: Wijik Lee, Young-Sik Kim,Yong-Woo Lee та Jong-Seon No. Вона ґрунтується на коді Рида-Мюллера(РМ), покращуючи схему підпису на основі кодів Гоппа , розроблену Courtois, Finiasz та Sendrier (CFS). Перевагами даного алгоритму є контрольований час підписання. У порівнянні з CFS час підпису не залежить від можливості виправлення помилок t. Також час підпису та рівень безпеки контролюється завдяки налаштуванню параметрів. Управління відношенням між часом підпису та

рівнем безпеки здійснюють завдяки змінам параметрів N і w, де N – очікувана кількість ітерацій, w – параметр ваги похибок. Обмеження pqsigRM – це відносно великий розмір відкритого ключа, оскільки код РМ не квазіциклічний, розмір відкритого ключа дорівнює (n - k) × k (n, k-параметри коду) [5].

Схема RacoSS. Назва цього алгоритму розшифровується як Random Code-based Signature Scheme, що в перекладі означає – Випадкова схема підпису, заснована на кодуванні. Вона є результатом спільної роботи японських дослідників (Partha Sarathi Roy, Rui Xu, Kazuhide Fukushima, Shinsaku Kiyomoto, Tsuyoshi Takagi) та вченого з американського університету(Kirill Morozov). Представлено дві версії реалізації цієї схеми: довідкова та оптимізована, перша з яких призначена для покращення розуміння функціонування алгоритму, а друга-для демонстрації продуктивності. Авторами зазначаються такі переваги RacoSS: RaCoSS виявився стійким та екзистенційно непідробним в умовах атаки обраного повідомлення. Підпис має невеликий розмір у порівнянні з іншими схемами підпису на основі кодування, за виключенням схеми підпису CFS з 81 бітовою безпекою. Але, розміри ключів CFS значно більші, ніж потребує RaCoss. Процеси, виконувані у алгоритмі(формування ключів, перевірка та формування підпису) можуть бути легко прискорені паралельними обчисленнями. [4].

Схема RankSign. Розробниками криптосистеми RankSign виступили Nicolas Aragon, Olivier Ruatta, Philipp e Gaborit, Gilles Zémor та Adrien Hauteville. Ця схема підпису заснована на коді в ранговій метриці. Загальною ідеєю є використання коду LRPC як лазівки для обчислення помилки пов’язаної з повідомленням. На конкурс було представлено модифіковану версію RankSign, де додатково відбувається додавання невеликої випадкової помилки до підпису, тобто це дозволяє зменшити спроможність зловмисника розрізнити підписи. Схема підпису має невеликі параметри і є відносно швидкою. Оскільки нам потрібно взяти велике значення q, всі відомі комбінаторні атаки є недієвими для порушення стійкості RankSign. У оцінці безпеки не враховується просторова складність цих алгоритмів, оскільки, зараз не існує квантового прискорення для них, автори очікують, що параметри будуть досить стійкими [4].

Порівняльний аналіз представлених алгоритмів доцільно провести з точки зору їх швидкодії та довжини параметрів. З метою вивчення значень в єдиному форматі дані довжин,що надавалися в бітах, зведені до байт. Продемонструємо дані щодо довжин основних криптографічних парметрів у графічному вигляді (рис.1).

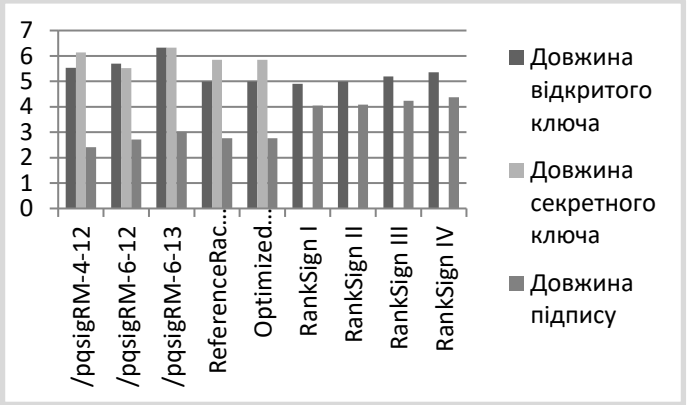


Рис.1. Порівняння довжин параметрів(у байтах) для алгоритмів ЕЦП

Для подальшого дослідження графіки побудовано у логарифмічному масштабі, оскільки значення параметрів для різних алгоритмів різниться в десятки-сотні разів. Порівнюючи отримані дані, варто відзначити, що найбільша довжина шифртексту відповідає алгоритму RankSign і зі зростанням рівня безпеки, що надає ця схема, довжина шифртексту збільшується, як і довжина відкритого ключа. Reference RacoSS та pqsigRM-6-12 продемонстрували найоптимальніші показники за усіма трьома параметрами.

Дані швидкості, що були надані авторами у мілісекундах, зведені до кількості циклів, які потребуються для виконання операцій, з урахуванням особливостей конкретної обчислювальної платформи. Представимо результати за допомогою графічного зображення (рис.2).

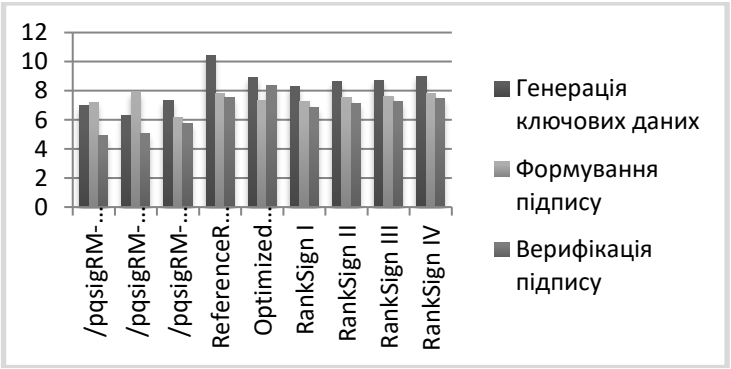


Рис.2. Показники швидкості(у циклах) алгоритмів ЕЦП

Здійснивши порівняльні дослідження алгоритмів формування ЕЦП, з точки зору швидкодіїї очевидно, що більш продуктивним буде той алгоритм, показники для якого більші. Аналізуючи гістограми, бачимо, що оптимізована версія RacoSS(Optimized RacoSS) є найбільш швидкою з усіх представлених алгоритмів. Тоді як схема підпису pqsigRM для різних своїх версій продемонструвала порівняні показники, що є на порядок меншими за швидкість RankSign та RacoSS.

Криптографія, що ґрунтується на виправляючих кодах, нині вважається одним з найперспективніших напрямків. Це підтверджується тим, що з 82 проектів, представлених на конкурс, 20 базуються саме на кодах. У роботі було проведено дослідження та порівняння алгоритмів формування ЕЦП за двома критеріями: довжинами основних криптографічних параметрів та показниками швидкодії, яку забезпечують кожен з алгоритмів. З точки зору швидкості виконання ключових операцій найефективнішим виявився алгоритм формування електронного цифрового підпису RacoSS, що також продемонстрував оптимальні показники довжин основних криптографічних параметрів.

Список літератури

1. Bernstein D., Buchmann J. and Dahmen E. Post-Quantum Cryptography. Springer-Verlag, Berlin-Heidleberg, 2009, 245 p.

2. Koblitz N. and Menezes A.J. A Riddle Wrapped in an Enigma. [Electronic resource]. – Access mode: https://eprint.iacr.org/2015/1018.pdf, Oct. 20, 2015 [Aug. 21, 2016]

3. Moody D. Post-Quntum Cryptography: NIST's Plan for the Future [Electronic resource] // The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016. – Access mode: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf [March 8, 2016].

4. Computer Security Resource Center [Electronic resource]. – Access mode: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions

5. Lee, Young-Sik Kim, Yong-Woo Lee, Jong-Seon No. A modified RM code-based post-quantum digital signature algorithm [Electronic resource]. – Access mode: https://sites.google.com/view/pqsigrm/home

УДК 004.7

Особливості DDOS атак в бездротових мережах

Куций М.О., студент
Науковий керівник – Тесленко О.Е., асистент
Центральноукраїнський національний технічний університет, м. Кропивницький

Аномалія типу "відмова в обслуговуванні" DoS (від англ. Denial of Service) є, як правило, мережевою атакою, проведеною зловмисником щодо мережевого об'єкта, функціонування якого він бажає порушити (наприклад, уповільнити або припинити). Найбільш характерним проявом DoS є "затоплення" або flooding каналу зв'язку або конкретного мережевого пристрою величезною кількістю мережевих пакетів. Залежно від типу пакетів, це може призвести до перевантаження каналу і, як наслідок, неможливість проходження по ньому легітимного трафіку, або до підвищеної завантаженні пристрою (заповнення доступного обсягу оперативної пам'яті і завантаження ресурсів процесора). DoS може бути проведений не тільки шляхом відправки величезного числа пакетів. Можливі ситуації, коли його можна викликати малим числом пакетів. Це можливо в разі наявності специфічної уразливості в програмному або апаратної реалізації пристрою. Виявлення DoS в разі відправки величезного числа пакетів не становить труднощів, на відміну від DoS, проведеного за допомогою незначної кількості пакетів. Необхідно відзначити, що існує ще різновид DoS, так звана розподілена DoS (від англ. Distributed Denial of Service, DDoS). Цей тип DoS характерний участю величезної кількості атакуючих мережевих пристроїв.

Оскільки середовище передачі в бездротових мережах є загальнодоступним, будь-який з абонентів може зайняти його для ексклюзивного доступу. Ситуація дуже схожа на принцип роботи коаксіального Ethernet, коли в разі виходу з ладу одного з мережевих адаптерів зупинялась вся мережа. В Інтернеті досить просто виявити кілька вільно розповсюджуваних пристроїв, що генерують в діапазоні 2,4 ГГц сигнал достатньої потужності для виведення з ладу Wi-Fi-мережі. Обладнання стандарту IEEE 802.11 використовує неліцензійний спектр частот. Устаткування IEEE 802.11b / g використовує 14 каналів по 5 МГц кожен в діапазоні частот від 2.412 ГГц до 2.484 ГГц. Устаткування IEEE 802.11a використовує вісім каналів по 20 МГц кожен в діапазоні частот від 5.15 ГГц до 5.35 ГГц і чотири канали по 20 МГц в діапазоні частот 5.725 ГГц - 5.825 ГГц. Будь-яка перешкода на ці діапазони частот порушить радіозв'язок між пристроями IEEE 802.11 і призведе до відмови в обслуговуванні. Коли перешкоди виробляються навмисно для порушення зв'язку, це називається радіочастотна перешкода. Це означає,

що джерело перешкод знаходиться в межах поширення і обумовлено двома основними факторами. По-перше, близькість джерела перешкод до приймача, і по-друге потужність передачі (рис. 1).

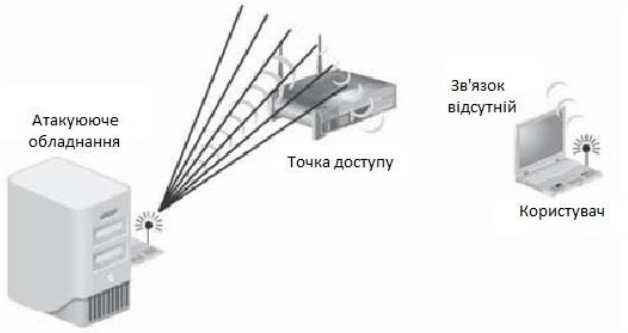


Рисунок 1 – Атака на фізичний рівень

Для успішного проведення атаки, джерело перешкод (або атакуючий) повинен згенерувати сигнал, досить потужний, здатний заглушити основні частоти. При генерації сигналу-завади атакуючий може націлюватися на певну вузьку смугу частот, або якщо дозволяє потужність, більш широку. Сигнал-перешкода може передаватися безперервно або розраховуватися таким чином, щоб впливати в найбільш критичні моменти (наприклад, деякі системи виявлення та запобігання вторгнень в бездротові мережі намагаються запобігти діям зловмисника, виробляючи перевірку підтверджень, що є ефективним запобіганням атак на бездротову мережу). Атакуючий фізично може підслухати або впливати на бездротову мережу:

- Підслуховування - перехоплення і перегляд текстових повідомлень чужими приймачами. Мобільні пристрої та мережі поділяють бездротову мережу. Більшість радіо з'єднань використовує високочастотний спектр і радіопередачу за своєю природою. Віщаючи по радіохвилях сигнали можуть бути легко перехоплені приймачами, налаштованими на відповідну частоту. Таким чином, надіслані повідомлення можуть підслуховувати і підмінювати підробленими повідомленнями.
- Радіо-сигнал може бути заглушений, викликаючи спотворення або втрату переданого повідомлення.

DoS атака проводиться на фізичному рівень при використанні радіообладнання або джерела сильного шуму, здатного заглушити фізичний канал, що в свою чергу ставить під загрозу сервісну доступність. Однак цей вид нападу не поширений, оскільки для цього необхідно спеціалізоване обладнання, яке може бути виявлено радіоаналізатором.

Бездротові мережі сприйнятливі не тільки до атак на фізичному рівні, але і до відсутності захисту цілісності та встановлення автентичності

пакетів управління і контролю протоколу канального рівня MAC.

Атаки на канальному рівні дозволяють атакуючому розривати вибіркові з'єднання з точкою доступу. Найбільш поширені варіанти цих атак - відмови від асоціації і від аутентифікації. При здійсненні даного типу атак зловмисник посилає службові пакети "відмова від асоціації" від MAC-адреси точки доступу до клієнта і навпаки. Оскільки додаткова аутентифікація даних пакетів не потрібна, клієнт розриває поточне з'єднання з точкою доступу. Подібні атаки часто здійснюються як підготовча фаза атак на клієнтів бездротових мереж.

Базовий стандарт 802.11 визначає два типи мереж, що відрізняються конфігурацією: фіксованої і довільної структури. На їх основі будуються різні варіанти топології: "точка-точка", "точка-багато точок", "кожен з кожним", "зірка", "мост' і т. д.. Мережа з фіксованою структурою складається з терміналів (зазвичай комп'ютерів з бездротовим мережним адаптером) і базових станцій. У такій мережі точка доступу виконує роль моста між бездротовою та кабельною мережами, забезпечуючи прийом, накопичення і передачу даних абонентам. До магістральної лінії точки доступу підключаються за допомогою стандартної провідної лінії Ethernet.

Дальність дії приймачів залежить від висоти підйому антени і зазвичай становить від 20 до 500 м. Одна точка доступу забезпечує обслуговування від 15 до 250 абонентів в залежності від конфігурації мережі і технології доступу. Збільшити ємність мережі можна, просто додавши нові точки доступу, при цьому не тільки розширюється зона обслуговування, але і знижується ймовірність перевантаження.

Далі розглянемо атаки на мережевий рівень. Нападаючи на протоколи маршрутизації, атакуючі можуть паралізувати трафік в мережі, проникати в з'єднання між вихідним і кінцевим пристроями, і таким чином керувати транспортним потоком мережі. Транспортні пакети можуть бути перенаправлені по неоптимальному або навіть по неіснуючому шляху, що призведе до істотної затримки або більш того – втрати інформаційного пакета. Атакуючі можуть створити цикли маршрутизації, що призведе до сильної перевантаження в певних областях мережі.

У порівнянні з іншими рівнями прикладний рівень також вразливий з точки зору безпеки. На цьому рівні містяться призначені для користувача дані, які зазвичай підтримувані безліччю протоколів, таких як HTTP, SMTF, TELNET і FTF, які містять безліч уразливостей. Атаки на прикладний рівень привабливі для зловмисників тим, що інформація, що міститься в додатках є основною метою для проведення атаки.

• Атаки за допомогою зловмисних програм (віруси, черв'яки, програми-шпигуни і трояни).

• Атаки відмови: вся або частина комунікаційної системи перестає відповідати на зовнішні запити.

Деякі атаки можуть бути спрямовані на кілька рівнів, замість одного.

Прикладами багаторівневих атак є відмова в обслуговуванні DoS, «людина по середині», а також імітуючі атаки.

• Відмова в обслуговуванні: такі атаки запускаються на декількох рівнях. На фізичному рівні використовується для заглушування сигналу, здатна порушити з'єднання. На канальному рівні, зловмисники можуть перехоплювати канали зв'язку, створюючи перешкоду для доступу інших вузлів каналу.

• Імітуючі атаки: можуть бути запущені з іншого ідентичного вузла з таким же MAC або IP-адресою. Імітують атаки, як правило, є першим кроком більшості нападів, і використовуються для здійснення більш складної атаки.

• Атака «людина посередині»: атакуючий знаходиться між передавачем і приймачем і перехоплює будь-яку інформацію, що передається. У деяких випадках атакуючий виконує роль передавача для з'єднання з приймачем, або роль приймача, щоб відповісти передавачу.

Висновки. Представлений аналіз атак типу відмова в обслуговуванні в широкосмугових бездротових мережах, що надають доступ в Інтернет і супутніх послуг для кінцевих користувачів. Показано, що бездротові мережі, які використовують загальні радіочастоти, часто вразливі від атак цього типу. Бездротові локальні мережі на основі стандартів IEEE 802.11, IEEE 802.16, і WMN не є винятком. Принципи безпеки широкосмугових бездротових мереж варіюються і залежать від відмінностей в топології, мережевих операцій і фізичних установок. Серед різних загроз безпеці атака типу відмова в обслуговуванні є найбільш важкою загрозою, оскільки може порушити доступність і цілісність мережі. У доповненні до атак на фізичний рівень, бездротові мережі уразливі на канальному рівні, вразливість якого може привести до відмови в обслуговуванні. Наводиться огляд різних DoS-атак на бездротові мережі, а також доступні способи виявлення.

Список літератури

1. Gast, Matthew. "Seven Security Problems of 802.11 Wireless" May 24, 2012 [Електронний ресурс]. – Режим доступу: http://www.oreillynet.com/ pub/a/wireless/2002/05/24/ wlan.html?page=1.

2. C He and J. C Mitchell. Security analysis and improvements for IEEE 802.11i. In NDSS. The Internet Society, 2015.

УДК 004.056.53

Дослідження використання більярду Сіная для генерації псевдовипадкових послідовностей

Лисенко І.А., к.т.н., ст. викладач,
Собінов О.Г., викладач
Центральноукраїнський національний технічний університет, м. Кропивницький

Сучасний світ технологій, що стрімко розвиваються потребує все більшого захисту конфіденційних даних. На сьогоднішній день існують сотні різноманітних способів захисту передачі даних: від найпростіших способів шифрування, на кшталт шифру Цезаря, до складних схем, включаючи сучасні стандарти шифрування та стеганографію. Але різноманітні методи шифрування, весь час вдосконалюючись, втрачають у чомусь іншому. Наприклад, при високій криптостійкості, мають значну складність, що збільшує час роботи та призводить до не можливості їх використання для передачі повідомлень в режимі online. Розвиток сучасного Internet-простору та соціальних мереж призводить до необхідності посилення захисту персональних даних користувачів та їх повідомлень під час зв'язку. Популярні месенджери, такі як Viber та WhatsApp, що використовують методи шифрування, постійно піддаються хакерським атакам та регулярно посилюють методи власного захисту.

Таким чином виникає необхідність створення системи передачі даних, котра мала б можливість проводити шифрування та дешифрування даних, не втрачаючи на це багато часу та не використовуючи багато ресурсів системи. Одним з головних питань у цьому напрямку є отримання достатньо криптостійких послідовностей від генератора випадкових чи псевдовипадкових чисел.

Звернемося у запропонованому випадку до математичних методів генерації числових послідовностей. Серед таких методів можливо використати математичний більярд, зокрема, досліджуваний нами математичний більярд Сіная [1-2].

Скористаємось основними принципами математичного більярду, а саме: об'єкт рухається по прямокутній площині, нехтуючи тертям, а значить з однаковою швидкістю і його рух характеризується лише координатами та вектором напрямку. Як показують дослідження, через деякий проміжок часу траєкторія руху об'єкту почне повторюватись, що призведе до втрати хаотичності та є не придатним для генерації послідовностей ключів шифрування.

Але, скориставшись математичним більярдом Сіная, можливо уникнути повторень та отримати випадові, достатньо довгі послідовності чисел. Для отримання послідовностей необхідно задати такі початкові

параметри:

- розміри площини, по якій будуть рухатись об'єкти (кульки радіусів r_1 та r_2, та "шайба" радіусом R, які теж задаються відповідно);

- початкові координати об'єктів (x_1, y_1) та (x_2, y_2) та їх швидкості (dx, dy).

Принцип роботи запропонованого методу наступний. У кожного з абонентів встановлюється невеликий пристрій, що містить мікроконтролер. Особливістю є те, що пристрої повинні бути саме парними, оскільки міститимуть однакові початкові значення. Зрозуміло, що множина початкових значень відповідна розмірності множини дійсних чисел, що в даному випадку достатньо. Одна з можливих систем може бути раелізована з використанням сімейства ARM мікроконтролерів - STM32F405 і STM32F407 та STM32F415 і STM32F417 від фірми STMicroelectronics. Далі на вказані парні пристрої, у яких реалізовано математичний більярд Сіная, через відкритий канал зв'язку будуть передаватись початкові дані про стан системи:

- зміщення координат кульок та шайби на більярдному столі від встановлених у програмній парі мікроконтролерів;
- швидкості (напрямок руху об'єктів (кульок);
- інертність шайби;
- радіуси кульок та шайби.

Відповідно закритий ключ шифрування буде генеруватись локально на кожному з пристроїв та містити унікальну числову послідовність. Розмірність відкритого ключа складатиме $14 \times n$, де n - розрядність мікроконтролера. Для більшої секретності відкритого ключа можна ввести деяке правило, за яким буде передаватись послідовність початкових значень. Таким чином їх комбінація складатиме 14!=871782911200 варіантів.

Висновки. Показано проблему, яка виникає при передачі конфіденційних повідомлень у режимі online. Запропоновано метод генерації псевдовипадкових послідовностей з використанням математичного більярду Сіная.

Список літератури

1. Собінов О.Г. Простий генератор псевдовипадкової послідовності / О.Г. Собінов // Інформаційні технології та комп'ютерна інженерія. - Збірник тез доповідей науково-практичної конференції.- м. Кіровоград, 4 грудня 2014 року. – С.147.

2. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. Учебное пособие. – СПб.: БХВ-Петербург, 2005. – 288 с.

УДК 316.625 (075.8) (043.2)

Сугестивні маніпулятивні технології в Інтернеті

Люля В.С., студентка 4 курсу
Науковий керівник – Присяжнюк М.М., к. т. н., с. н. с.
Національна академія служби безпеки України, м.Київ

Історію людства супроводжує функціонування одного з найбільш універсальних явищ, пов'язаних з психікою людини, – навіювання (сугестія). Цей феномен пронизує багато сфер людського існування: у своїй діяльності, свідомо чи несвідомо, людина піддається впливу цього явища.

Суть сугестії полягає у сприйнятті особою інформації на підсвідомому рівні при вербальній чи невербальній міжособистісній або міжгруповій комунікації.

Сугестивний вплив на відміну від переконання не потребує критичного сприйняття інформації та потреби у її верифікації.

Сучасні новітні інформаційні технології та глобалізаційні процеси у світі сприяють побудові інформаційно-комунікаційного суспільства, яке передбачає безперешкодний доступ до інформації та відсутність інформаційних кордонів і будь-яких рамок комунікації, взаємопроникнення ідей і культур. Проте, при всіх позитивних аспектах інформаційно-комунікаційне суспільство є також ідеальним середовищем для здійснення сугестії. Інтернет дозволив не лише зв'язати людей один з одним і кожного з інформаційними ресурсами всього світу, але й використовувати його комунікаційний потенціал з маніпулятивними цілями.

Виникає соціальна небезпека застосування технологій штучної зміни поведінки людини, впливу на свободу її волевиявлення та на стан здоров'я. З появою Інтернету такі можливості суттєво розширяються. І тепер сугестивний вплив може проявлятися в інтернет-дискурсах різних жанрів. А причинами ефективної сугестії в Інтернеті є:

- висока довіра до неофіційних ресурсів мережі;
- залучення аудиторії до інформації сподіванням розв'язати будь-які проблеми;
- формування мережевих співтовариств на основі емпатії (співчуття).

Для результативного впливу на людину, сугестивні технології в Інтернеті ґрунтуються на важливих мотивах і потребах людини. За А. Маслоу, це початкові потреби – у захищеності, визнанні та задоволенні фізіологічних потреб.

Сугестивні маніпулятивні технології в Інтернеті націлені на масовий результат. Їхнім об'єктом найчастіше виступає певне мережеве співтовариство, або соціальна мережа.

Соціальні мережі в Інтернеті, у порівнянні з традиційними засобами масової інформації щодо здійснення маніпулятивних впливів, мають певні

переваги:

- оперативний обмін інформацією;
- можливість встановлення нових зв'язків;
- двостороння комунікація в режимі реального часу;
- неформальне спілкування;
- полегшений пошук потрібної людини.

Прикладами сучасних сугестивних технологій маніпулятивного впливу в Інтернеті можуть бути: медіавіруси, комп'ютерні ігри, блоги, фейки, тролі, флейми, флуди, спами, кроспостинг, холівари, симулякри тощо.

Так медіавірус (це подія, винахід, система ідей, пісня, візуальний образ, стиль одягу, скандал тощо), циркулюючи у мережах медіапростору, вводить в інфосферу свої концепції у вигляді ідеологічного коду – т. зв. меми, тим самим нав'язуючи їх мережевому співтовариству.

Сугестивний вплив на учасників комп'ютерних ігор ґрунтується на когнітивній підміні у свідомості гравців реальних цінностей на віртуальні. А оскільки найактивнішими користувачами комп'ютерних ігор є підлітки, психіка, тобто, морально-семантичний фільтр яких знаходиться у стані формування, то вони легко піддаються впливу сцен жорстокості й насильства, які надає віртуальний світ комп'ютерних ігор.

Платформою вільного «живого» спілкування людей, зацікавлених певною темою є блогосфера. Головною ж схемою сугестивного впливу в блогах є послідовне використання таких кроків, як: увага – довіра – репутація – вплив.

Фейками, тобто, неправдою, фальсифікацією, підробкою, які часто використовують в Інтернеті для маніпулювання свідомістю, можуть бути фотографії, створені у фотошопі, відеоролики, змонтовані у відеоредакторі, чи зняті зовсім в інший час і в іншому місці, фальшиві новини, сторінки в соціальних мережах, створені від імені інших (як правило, відомих) людей, фішинг сайти, схожі за своїм дизайном на сайти оригінали, тощо.

Ще однією технологією маніпулювання в Інтернеті є розміщення на форумах, в групах новин Usenet, у вікі-проектах і т. п. провокаційних повідомлень з метою виклику флейма, конфлікту між учасниками, пустої говорильні, ображення, тощо, яку називають тролінгом, а особу, що займається тролінгом – тролем.

Обмін повідомленнями на інтернет-форумах і чатах, що представляє собою словесну війну, яка часто не має відношения до причини спору називають флеймом, що також може мати маніпулятивну основу.

З метою комусь дошкулити флудери – особи, що розповсюджують у соціальних мережах флуд – неоднократне повторення непотрібної, однотипної інформації чи однієї фрази, символів, букв, графічних файлів або просто коротких повідомлень, що не мають жодного смислу, на веб-форумах, чатах і блогах.

Для розміщення комерційної, політичної, іншої реклами чи певного виду повідомлень в мережах медіапростору використовується спам – масова розсилка відповідних листів особам, що не мають бажання їх отримувати, нав'язуючи таким чином маніпулятивну інформацію.

З метою залученням нових читачів в Інтернеті часто використовується кроспостинг – автоматичне, напівавтоматичне чи ручне дублювання матеріалів певного блогу на різних блог-сервісах.

Для навіювання певної точки зору на інтернет-форумах і в чатах використовуються холівари – обмін повідомленнями, що представляють дискусії без всякого смислу, наприклад, для доказу переваги однієї з декількох схожих альтернатив.

За допомогою симулякрів, тобто, копій того, що не має оригіналу в дійсності, маскується в Інтернеті відсутність фактичної реальності певних подій, коли необхідно викривити чи спотворити оригінальну інформацію.

Висновки. Глобалізаційні процеси світового інформаційного простору та стрімкий розвиток сучасних інформаційних технологій усе більше сприяють розробці та втіленню нових сугестивних технологій маніпулятивного впливу в Інтернеті.

На сьогодні немає достатніх гарантій захисту людини від загроз маніпулювання їхньою свідомістю. Виникає необхідність забезпечення інформаційно-психологічної безпеки людини, під якою варто розуміти стан захищеності її психіки від деструктивного інформаційного впливу, що призводить до неадекватного сприйняття нею дійсності, порушення її прав та життєво важливих інтересів.

Список літератури

1. Інформаційна безпека держави: підручник / [В. М. Петрик, М. М. Присяжнюк, Д. С. Мельник та ін.]; в 2 т. – / за заг. ред. В. В. Остроухова – К.: ДНУ "Книжкова палата України", 2016. – Т.1 – 264 с., Т.2. – 328 с.

2. Сугестивні технології маніпулятивного впливу: навч. посібн. / В. М. Петрик, М. М. Присяжнюк, Л. Ф. Компанцева, О. Д. Бойко, В. В. Остроухов / за заг. ред. Є. Д. Скулиша. – К.: ВІПОЛ, 2011. – 248 с.

3. Бодрийяр Ж. К критике политической экономике знака. – М., 2007. – С.15.

4. Бодрийяр Ж. Симулякры и симуляция / Перевод О. А. Печенкина. Тула, 2013. – 204 с. [Электронный ресурс] – Режим доступа. – URL: http://simulacrum.p.fl2.fo.ru/file/chunk107/2160178/82514/ Жан%20Бодрийяр%20%20Симулякры%20и%20симуляция.pdf

5. Делез Ж. Логика смысла. – М., 1995. – С.229, 334.

УДК 004.492.3

Програмне забезпечення для виявлення атак на web-сервіси

Майоров Є.О., студент 4 курсу
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Центральноукраїнський національний технічний університет, м. Кропивницький

Сучасний процес розробки програмного забезпечення необхідно проектувати з урахуванням постійних атак на них з боку зловмисників.

Кількість різноманітних атак постійно зростає: особливо це стосується web-сервісів, доступ до яких може мати будь-яка особа, яка має доступ до мережі Інтернет, що призводить до дуже великої кількості атак, порівняно, наприклад, з атаками на десктопні додатки.

Виникає проблема автоматичного виявлення атак на web-сервіси для подальшої її нейтралізації.

Метою даної роботи було розробити програмне забезпечення для виявлення атак на web-сервіси.

Алгоритм роботи розроблюваної системи

Запропоновано метод організації системи, що виконує наступний алгоритм обробки web-трафіку:

1) Перехоплення трафіку web-сервісу.

2) Порівняння трафіку web-сервісу з відомими зловмисними «кейсами» та їх характеристиками.

3) У випадку проходження порівняння, тобто, несхожості з «кейсами», проводити загальний аналіз трафіку web-сервісу на предмет аномалій або невідомих системі зловмисних кейсів.

4) При ідентифікації трафіку атаки на web-сервіс надати повну технічну інформацію про пакет даних і всю інформацію про користувача, яку можна отримати на основі трафіку web-сервісу до адміністратора web-сервісу.

5) При виокремленні виду атаки, надати відповідний сценарій нейтралізації атаки адміністратору.

6) Зберігати трафік web-сервісу для можливих подальших досліджень.

Структура розроблюваної системи

1) Web-сервіс, при отриманні запиту від користувача, отримує базову інформацію про запит з даних протоколу запиту.

2) На сторінках web-сервісу, здійснюється програмний код мови програмування Javascript, що здійснює додатковий збір даних про користувача з браузера до лог-файлу.

3) Зібрана інформація перевіряється з зловмисними «кейсами», які зберігаються в кешованій базі даних Redis.

4) Проводиться базова перевірка трафіку web-сервісу на предмет

аномалій або невідомих системі зловмисних кейсів. При не проходженні перевірки, запит ідентифікується, як зловмисний.

5) При ідентифікації запиту, як атаки на web-сервіс, характеристики запиту зберігаються, як зловмисний «кейс» в кешованій базі даних Redis, і передаються до адміністратора.

6) При виокремленні виду атаки, адміністратору надається відповідний сценарій нейтралізації атаки.

7) При незловмисному запиті, дані про запит зберігається в лог-файлі. Збереження зловмисного трафіку відбувається окремо, взаємодією Redis та лог-файлу. При необхідності, роботу лог-файлу можна оптимізувати, використавши базу даних PostgreSQL.

Висновки. Вектори атак є досить різноманітними і вимагають використання програмного забезпечення широкого профілю, здатного охопити основні сфери атак на web-сервіси.

Була запропонована реалізація вирішення проблеми автоматичного виявлення атак на web-сервіси, у вигляді їх внутрішньої системи аналізу трафіку.

УДК 004.94

Формирование требований к оценке доверия критичных объектов на базе стандартов ISO

Маликов В.В.[1], начальник цикла, канд. техн. наук, доцент,
Лившиц И.И.[2], доцент кафедры, канд. техн. наук
[1]УО «Центр повышения квалификации руководящих работников и специалистов» Департамента охраны МВД Республики Беларусь
[2]Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», Российская Федерация

Замысел доклада появился под впечатлением от документа Организации по безопасности и сотрудничеству в Европе (ОБСЕ) «Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства» (далее – Руководство) [1]. Одна деталь Руководства заставила авторов задуматься о целесообразности дополнения широко используемого в мире информационных технологий (далее – ИТ) понятия актива, еще одной характеристикой – токсичностью. Заметим, что мир финансов, в свое время утративший видение меры и получавший проблемы нестабильных инвестиций, ввел общее понятие «токсичного» актива. Токсичность актива, безусловно, величина относительная, т.е. со временем может изменяться (интересующихся точными примерами классификации и базовыми процессами управления активами просят ознакомиться со стандартами ISO серии 27000) [2–5]. Положительным следствием введения понятия токсичного актива в мире финансов явился вывод ряда активов из некой зоны стыдливого умолчания, организацию их учета и контроля и в целом усиления институционально роли надзора.

Революция в области ИТ, произошедшая в конце XX века за рубежом, имела одно весьма интересное следствие. В ходе революции вопросы информационной безопасности (далее – ИБ) практически полностью утратили самостоятельность и стали органичной и неотъемлемой частью ИТ [6–8]. Данный тезис подтверждается многими фактами из зарубежной практики: это и структура организаций, их процессы, и практика взаимодействий организаций [9, 10]. Поскольку сегодня общее понятие «ИТ» органично включают в себя вопросы ИБ, то далее уместно говорить предметно не только о токсичности активов, но и о влиянии токсичных активов на ИБ.

Документы, датированные 90-ми годами прошлого века, представляются несколько утратившими актуальность. ИТ являются

чрезвычайно динамичной направлением, в котором все меняется быстро и непрерывно. Соответственно, самые актуальные документы – это документация производителей на компоненты систем обработки информации (далее – СОИ). За ними стараются «успеть» международные стандарты и нормативные документы государств, имеющих под своей юрисдикцией развитую индустрию ИТ. В последнее время наблюдается переход к сертификации средств защиты в соответствии с ISO 15408 [11 – 13]. В реальные СОИ вероятность преодоления защиты не равна нулю, и для того чтобы связать вероятность такого события с последующим ущербом давно используют понятия рисков ИБ (например, ранее Guide 73, позже ISO 27005). В мире для организаций уже созданы реестры рисков, например, ISO 31000.

Здесь можно рекомендовать создание технологии, в которой все решения в области ИБ и их компоненты будут изначально разрабатываться в едином безопасном процессе, например Security Development Lifecycle (SDL). Для этого потребуется создать структуру, подобную Configuration Management Database (CMDB), для контроля уровня безопасности, поддержки версионности и отслеживания «родителей» и «потомков» всех оцененных по требованиям ИБ компонент — программных и аппаратных. Финальная «сборка» защищенных ИС возможна только из «доверенных» компонент, прошедших в установленном порядке все положенные тесты ИБ, внесенных в CMDB и позволяющих обеспечивать заданный уровень ИБ. Следующая сложность обеспечения требуемого уровня ИБ — создание полного замкнутого цикла управления ИБ, например, по образцу ЖЦ в NIST (специальные публикации NIST: FIPS 199/SP 800-60 «Информационная безопасность», FIPS 200/SP 800-53 «Меры обеспечения безопасности и приватности для Федеральных информационных систем и организаций»):

1. Категорирование активов (FIPS 199/SP 800-60);
2. Выбор мер безопасности (FIPS 200/SP 800-53);
3. Реализация мер безопасности (SP 800-160);
4. Оценка мер безопасности (SP 800-53A0);
5. Мониторинг мер безопасности (SP 800-137).

Использование вышеперечисленных документов обеспечит единство шкал и методов оценки соответствия с зарубежными центрами компетенций в области ИТ, что позволит объективно, в сопоставимых измеряемых величинах, оценивать степень соответствия ИТ. Доверие к системе, типовым способом формирования которого в настоящее время является «доверие через оценку». Но для того чтобы получать адекватные результаты, нужно понимать, в какой момент времени производить оценку. Мировая практика предусматривает оценку «по мере необходимости». Представляется целесообразным производить оценку безопасности в ИТ в соответствии с требованиями стандартов ISO 15408, а оценку процессов управления — ISO 27001.

Навык распознавания токсичных активов в области ИТ и очистки от них может существенно улучшить показатели устойчивости современной организации. Необходимо признать неизбежность того, что вопросы ИБ должны практически полностью утратить иллюзорную самостоятельность и стать неотъемлемой частью ИТ. Предлагается пересмотреть практикуемое в раздельное «развитие» ИБ и ИТ и обеспечить формирования требований к оценке доверия критичных объектов на базе современных стандартов ISO.

Список литературы

1. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства // osce.org [Электрон. ресурс]. – 2018. – Режим доступа: http://www.osce.org/ru/atu/110472?download=true. – Дата доступа: 21.01.2018.

2. ISO/IEC 27000:2014. Information technology — Security techniques — Information security management systems — Overview and vocabulary, International Organization for Standardization, 2014. – 31 pages.

3. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, 2013. – 23 pages.

4. ISO/IEC 27004:2009. Information technology — Security techniques — Information security management — Measurement, International Organization for Standardization, 2009. – 55 pages.

5. ISO/IEC 27005-2011. Information technology — Security techniques — Information security risk management, International Organization for Standardization, 2011. – 68 pages.

6. Лившиц И.И. Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации: ИСО 27001 и СТО Газпром / Лившиц И.И., Полещук А.В. // Труды СПИИРАН. – 2015. – № 3. – С. 33 – 44.

7. Лившиц И.И. Подходы к решению проблемы учета потерь в интегрированных системах менеджмента // Информатизация и Связь. – 2013, № 1. – С. 57 – 62.

8. Лившиц И.И. Подходы к применению модели интегрированной системы менеджмента для проведения аудитов сложных промышленных объектов – аэропортовых комплексов // Труды СПИИРАН. – 2014, № 6. – С. 72 – 94.

9. Шишкин В.М., Юсупов Р.М. Доктрина информационной безопасности Российской Федерации — опыт количественного моделирования // Труды СПИИРАН. Вып. 1, т. 1. - СПб: СПИИРАН, 2002.

10. Юсупов Р. М., Шишкин В. М. О некоторых противоречиях в решении проблем информационной безопасности // Труды СПИИРАН.

Вып. 6. — СПб.: Наука, 2008, С. 39–59.

11. ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель». 2012.

12. ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности», 2013.

13. ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», 2013.

УДК 004.94

Оценка влияния современных риск-ориентированных стандартов на обеспечение информационной безопасности критичных промышленных объектов

Маликов В.В.[1], начальник цикла, канд. техн. наук, доцент,
Лившиц И.И.[2], доцент кафедры, канд. техн. наук
[1]УО «Центр повышения квалификации руководящих работников и специалистов» Департамента охраны МВД Республики Беларусь
[2]Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», Российская Федерация

В настоящее время проблема формирования требований для обеспечения безопасности сложных промышленных объектов (СлПО) топливно-энергетического комплекса (ТЭК) является актуальной для специалистов в области обеспечения информационной безопасности (ИБ). Для лиц, принимающих решения (ЛПР) важно унифицировать совокупность требований, принятых на законодательном уровне и дополнительно применять современные стандарты ISO, прежде всего ISO серии 27001 и «целевой» стандарт для энергетики ISO 50001, которые совместно формируют методологическую основу обеспечения ИБ для СлПО ТЭК.

Отметим, что в классическом труде Н. Винера по теории кибернетики отмечается: «*Для получения приемлемых результатов в приемлемое время необходимо довести до максимума скорость элементарных процессов и добиться, чтобы течение этих процессов не прерывалось существенно более медленными шагами*». Для выполнения требований нормативных документов и стандартов ISO предлагается далее применять обобщенный термин СлПО, под которым будем понимать «*технический объект, несанкционированное изменение штатного режима функционирования которого, связанное с нарушением свойств ИБ, может привести к угрозе техногенных катастроф с необратимыми последствиями*».

В любой системе менеджмента одним из важнейших вопросов является вопрос корректного выявления перечня активов (в нотации ISO 27000 – "*asset*"), для которых требуют обеспечить защиту от актов незаконного вмешательства. Для ТЭК проблему выявления и защиты критически важных промышленных объектов возможно сопоставить с общей проблемой выявления и защиты ценных для бизнеса активов СлПО в системах менеджмента ИБ (СМИБ) и/или интегрированных системах менеджмента (ИСМ). В стандартах ISO изложена четкая логика данного процесса – выделенная совокупность ценных (критичных) активов,

намеченных ЛПР к защите в составе СМИБ объектов ТЭК, требует определенных ресурсов (временных, технических, персонал) для оценки уязвимостей, анализа соответствующих угроз, формирования файла рисков и плана обработки рисков. Однако на объектах ТЭК требуется принятие решений в режиме, близком к режиму реального времени. Пример явно завышенного времени выполнения процесса показан в работе Л. Кини и Х. Райфа, когда ЛПР для обдумывания различных альтернатив может потребоваться неделя.

На основании сформированного перечня активов, подлежащих защите, на следующем шаге определяется перечень уязвимостей и угроз, для противодействия применяются определенные меры (средства) обеспечения ИБ (в нотации ISO 27000 – "*control*"). Конечной целью применения мер (средств) обеспечения ИБ является снижение потенциального ущерба (потерь) в отношении выбранных активов СлПО ТЭК до приемлемой меры (уровня риска), установленной ЛПР. Для формирования перечня угроз рекомендуется использовать Приложение «В» стандарта ISO 27005. В качестве возможных критериев, используемых для определения ценности актива, могут быть выбраны: исходная (балансовая) стоимость, стоимость замены (воссоздания) актива в случае реализации неблагоприятного сценария акта незаконного вмешательства (события риска ИБ), или дополнительная ценность (например, ценность репутации и политических рисков).

Требования по выполнению проверок (аудитов) активов СлПО ТЭК установлены, соответственно, в п. 9.2 в ISO 27001 и п. 4.6.3 ISO 50001.

Анализ уязвимостей для СлПО проводится в целях оценки возможности преодоления нарушителем системы защиты и нарушения безопасного функционирования за счет реализации угроз безопасности информации. Анализ уязвимостей включает анализ уязвимостей средств защиты информации, технических средств и ПО. Среди методов оценки технических уязвимостей можно отметить методы тестирования ИС, которые применяются для эффективного выявления уязвимостей. Эти методы тестирования включают, например:

- автоматизированные инструментальные средства поиска уязвимостей;
- тестирование и оценка безопасности;
- тестирование на проникновение;
- проверка кодов.

Предложенный методический подход позволяет «мягко» преобразовать существующую систему к требованиям СМИБ и обеспечить результативное проведение различных аудитов и мониторинга состояния СлПО, находящихся под воздействием угроз нарушения ИБ. Методика основана на преобразовании базовой системы и учете требований по идентификации всех групп активов в соответствии с требованиями к СМИБ на базе стандартов ISO серии 27001 и ISO серии

27005. В методике представлена последовательность шагов и набор соответствующих базовых таблиц для преобразования к требованиям СМИБ. Начинается процесс с идентификации активов, их категорирования и первичной оценки со стороны владельцев для принятия решения о включении с область применения (“*scope*”). Например, на этом шаге могут определяться права собственности на помещения, владельцы лицензий ПО, ответственность за процессы СМИБ.

Далее на основании первичного перечня активов выполняются стандартные процедуры оценки рисков, установление критериев принятия рисков и приемлемых уровней рисков, формирование плана обработки рисков. Например, на этом шаге могут быть использованы результаты классификации активов в соответствии с нотацией СОИБ как входные данные и выполнена полная оценка рисков (в том числе и остаточных) в соответствии с требованиями ISO серии 27001. На последующих шагах выполняется выбор мер (средств) обеспечения ИБ, формирование «Заявления о применимости», далее – выполнение внутренних аудитов СМИБ, проведение анализа СМИБ со стороны руководства и определение возможностей для постоянного улучшения СМИБ.

Учет активов в соответствии с требованиями стандарта ISO серии 27001 позволит привнести в СМИБ управляемость по единым целям, измеримых в терминах бизнеса, что позволит выполнять в дальнейшем интеграцию с другими системами менеджмента. Соответственно, для СМИБ могут быть применены соответствующие количественные метрики как доказательства «полезности» для бизнеса.

Различные виды метрик для целей обеспечения ИБ представляется целесообразным сгруппировать следующим образом:

- для оценки основного бизнеса (например, доля на рынке);
- для управления издержками (например, ТСО – совокупная стоимость владения);
- для оптимизации текущей деятельности (например, оптимизация затрат OPEX).

С целью снижения издержек текущей деятельности, могут быть применены метрики, отражающие степень достижения возможного максимума (например, выполнение в срок инфраструктурных проектов). Соответственно, предлагаются различные типы метрик:

- простые метрики (например, количество выявленных инцидентов ИБ);
- сложные метрики (например, отношение стоимости СЗИ к стоимости ИТ активов);
- комплексные метрики (например, число произошедших инцидентов ИБ, приведших к ущербу (вынужденному простою) в АС, определенных как критичные для бизнеса).

Процесс формирования требований к защищенности СлПО ТЭК

рекомендуется реализовать на базе системы современных стандартов ISO серии 27001 и ISO серии 50001. Предлагаемый подход позволит обеспечить необходимый уровень обеспечения безопасности СлПО, в том числе уровень ИБ, адекватный современным требованиям к оценке угроз, анализу уязвимостей и менеджмента рисков на объектах ТЭК.

Список литературы

1. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, 2013. – 23 pages.

2. ISO/IEC 27004:2009. Information technology — Security techniques — Information security management — Measurement, International Organization for Standardization, 2009. – 55 pages.

3. ISO/IEC 27005-2011. Information technology — Security techniques — Information security risk management, International Organization for Standardization, 2011. – 68 pages.

4. Лившиц И.И. Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации: ИСО 27001 и СТО Газпром / Лившиц И.И., Полещук А.В. // Труды СПИИРАН. – 2015. – № 3. – С. 33 – 44.

УДК 511:003.26.09

Прискорення методу квадратичного решета на основі використання розширеної факторної бази та формування достатньої кількості B-гладких чисел

Міська В.М., аспірант
Науковий керівник – Винничук С.Д., д.т.н., старший науковий співробітник відділу автоматизації проектування енергетичних установок
ІПМЕ ім. Г.Е. Пухова НАН України, м. Київ

Метод квадратичного решета (QS) відноситься до найшвидших алгоритмів факторизації [1], який поступається методу решета числового поля. Проте для чисел розміром до 110 десяткових знаків і досі є найкращим. Зниження обчислювальної складності методу квадратичного решета, дасть змогу покращити процес криптоаналізу алгоритму RSA. Тому дослідження нових способів зниження його обчислювальної складності є актуальним.

Алгоритм методу QS працює в два етапи: етап збору даних, де він збирає інформацію, яка може привести до рівності квадратів по модулю N (етап просіювання), та етап обробки даних, де він розміщує всю зібрану інформацію у матрицю та оброблює її для отримання рішення [2].

Найбільш затратною за часом частиною алгоритму квадратичного решета є процес просіювання. Під час просіювання шукають пари чисел (A,B), які задовольняють умові

$$B = A^2 (\text{mod N}), \qquad (1)$$

де число B розкладається на множники, що є елементами факторної бази. Такі числа B називають B-гладкими.

Розмір факторної бази La – це один з ключових параметрів, що визначають ефективність алгоритму просіювання. Невдало обраний інтервал просіювання призведе до втрати рішення або зростання часу роботи алгоритму та об'єму пам'яті який використовується.

Ідея досліджень, результати яких подаються в даній роботі, полягає у використанні початкового розміру факторної бази Lmax > La та визначенні достатнього такого розміру L*, який може виявитися меншим за La.

Метод вибору достатньої кількості B-гладких чисел.

В пропонованому алгоритмі **MLB**, що реалізує вибір достатньої кількості B-гладких чисел при розмірі факторної бази Lmax > La, використовуються два додаткові вектори Ve[Lmax+1] та Vf[Lmax+1], кожен елемент яких співвіднесений відповідному елементу факторної бази. В цих векторах нульовій клітинці відповідає знак B-гладкого числа, а довільній іншій клітинці – відповідний порядковий номер елемента

факторної бази, де елементи факторної бази розміщені в порядку зростання їх значень.

Вектор Ve[Lmax+1] – це інформація про показники степенів отриманого нового B-гладкого числа, де в нульовій клітинці значенню 1 відповідає від'ємне значення B-гладкого числа, а значенню 0 – додатне. В довільній іншій клітинці k вектора Ve вказано показник степеня елемента факторної бази за номером k, що є дільником B-гладкого числа, а інакше нуль.

В кожній клітинці k вектора вектора Vf[Lmax+1] вказано кількість B-гладких чисел, для яких порядковий номер s максимального за значенням елемента факторної бази, що є дільником B-гладкого числа з непарним показником степеня, не перевищує k ($s \le k$).

В пропонованому алгоритмі MLB буде використовуватися також вектор VB[Lmax+2] – в кожній клітинці t якого міститься інформація про значення числа з інтервалу просіювання (-Lb, Lb) на основі якого отримано B-гладке число з номером t, а також вектор VM[Lmax+2]. Клітинці t вектора VM відповідає B-гладке число з номером t, для якого задається порядковий номер s максимального за значенням елемента факторної бази, що є дільником цього B-гладкого числа з непарним показником степеня.

Визначення початкових значень елементів векторів Vf, VM та VB, їх зміни при отриманні нового B-гладкого числа та умови достатності кількості B-гладких чисел представлені нижче кроками алгоритму MLB:

1. Присвоїти довільному k-у елементу вектора Vf значення k + 2, довільному з елементів векторів Ve та VB значення нуль. Лічильнику nb B-гладких чисел присвоїти значення 0.
2. На етапі проріджування при отриманні B-гладкого числа B з номером nb, на основі числа x з інтервалу просіювання, сформувати вектор Ve показників степенів для дільників B та визначити найбільший порядковий номер s ненульового непарного елемента в ньому. Присвоїти nb = nb +1; VB[nb] = x; VM[nb] = s.
3. Для всіх елементів вектора Vf, починаючи з номера s, зменшити їх значення на одиницю.
4. Кроки 2 та 3 продовжувати до тих пір, поки для одного з елементів вектора Vf , наприклад k, не буде виконана умова Vf[k] = 0, або для додатного B всі показники степенів у векторі Ve парні. Якщо для додатного B всі показники степенів у векторі Ve парні, перейти до кроку 5, а при Vf[k] = 0 –до кроку 6.
5. Отримуємо множники N згідно методу факторизації Ферма і завершити роботу алгоритму.
6. Прийняти L* = k . Сформувати матрицю M, що відповідає k + 2 - м B-гладким числам, для кожного з яких з порядковим номером t VM[t] ≤ k. Для формування j – го рядка матриці M необхідно:

a. знайти tj, для якого VM[t] ≤ k;

b. знайти значення B-гладкого числа за формулою , де x =VM[t];

c. сформувати вектор Ve показників степенів елементів факторної бази, дільників B та для непарних їх значень у відповідному стовпчику матриці M записати 1, а в інших випадках 0.

7. Опрацювати матрицю та вияснити чи отримане значення кореня не дорівнює N. Якщо ні, то задача факторизації вирішена, а інакше перейти до кроку 7.

8. Видалити інформацію про B-гладке число, що відповідає рядку j0 з нульовими значеннями елементів перетвореної матриці. Присвоїти:

a. Vf[i] = Vf[i] + 1, де i □ VM[tj0];

b. VM[tj0] = VM[nb]; VM[nb] = 0;

c. Vb[tj0] = Vb[nb]; Vb[nb] = 0;

d. nb = nb – 1.

e. Перейти до кроку 2.

Висновки. У результаті чисельних експериментів було показано, що для найбільш затратного за часом етапу методу квадратичного решета – пошуку B-гладких чисел, - у випадку збільшення факторної бази вдвічі та формуванні достатньої кількості B-гладких:

– в середньому в 2,85 рази зменшилося кількість використаних пробних значень з інтервалу просіювання при збільшенні розміру матриці M в 1.8 рази;

– на 29% зменшився загальний час на просіювання пробних значень та формування достатньої кількості B-гладких для 106 варіантів факторіваних чисел N;

– на 3,96 відсотків від загальної кількості N, що розкладалися на множники, збільшилась кількість вдалих факторизацій по відношенню до базового методу квадратичного решета.

Список літератури

1. Pomerance C. The quadratic sieve factoring algorithm // Advances in Cryptology, Proceedings of Eurocrypt 84. – Paris, 1984. – P. 169–182.

2. Landquist E. The Quadratic Sieve Factoring Algorithm // MATH 488: Cryptographic Algorithms. – 2001.

УДК 004.056.53

Дослідження принципів роботи технологій VPN

Обач В.А., студент 2 курсу
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Центральноукраїнський національний технічний університет, м. Кропивницький

На сьогоднішній день один із популярних та найлегших способів для забезпечення анонімності в Інтернеті це мережа під назвою Virtual Private Network

VPN – загальна назва віртуальної приватної мережі, що створюються поверх інших мереж. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному клієнту бути повноцінним учасником віддаленої мережі і користуватись її сервісами – внутрішніми сайтами, базами, принтерами. Безпека передавання інформації через загальнодоступні мережі реалізується за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. Технологія VPN дозволяє об'єднати декілька географічно віддалених мереж в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

Принцип роботи даної мережі

Рисунок 1 – Схема принципу роботи мережі VPN

VPN-з'єднання завжди складається з каналу типу “точка-точка”, також відомого під назвою “тунель”. Тунель створюється в незахищеній мережі, в якості якої найчастіше виступає Інтернет. З'єднання “точка-точка” має на увазі, що воно завжди встановлюється між двома комп'ютерами, які називаються “вузлами”. Кожен вузол відповідає за шифрування даних до того, як вони потраплять в тунель, і розшифрування цих даних відбудеться після того, як вони покинуть тунель. Після підключення до VPN-сервера всі дані починають передаватися між вашим ПК і сервером в

зашифрованому вигляді. Уже з VPN-сервера всі дані передаються до зовнішніх ресурсів, які були запитані.

Призначення даної мережі

1. Захист від крадіїв. Багато людей люблять відвідувати кафе і сидіти там в Інтернеті через Wi-Fi або часто подорожують і підключаються до відкритих Wi-Fi точок. Злочинець, який сидить за сусіднім столиком, не зможе перехопити дані кредитної карти з CVV кодом, або не вкраде пароль від платіжної системи разом грошима.

2. Захист від спостереження. Якщо людина цінуєте своє приватне життя і їй неприємний той факт, що будь-який системний адміністратор провайдра має доступ до відвіданих вами сайтів, або з яких електронних платіжних системам ви поповнюєте чи знімаєте великі суми грошей. Провайдер більше не буде знати, які сайти ви відвідуєте, а сайти не будуть знати, хто їх відвідав.

3. Кожна людина хоче бачити Інтернет таким, яким він повинен бути – відвідувати сайти без обмежень. Також не рідкість, коли блокуються певні сторінки або розділи, а провайдер не розбираючись блокують весь сайт. Також в список заблокованих сайтів може потрапити ваш улюблений сайт або сервіси які надає привілеї, бонуси, знижки конкретним країнам. За допомогою VPN можна стати резидентом даної країни.

VPN – це теж бізнес, якому потрібні гроші на обладнання, техобслуговування і зарплату співробітникам.

Безкоштовні і дуже популярні сервіси викрили в тому, що вони продають дані своїх користувачів стороннім організаціям. Найчастіше безкоштовні сервіси навіть не приховують передачу інформації третім особам, тому що безкоштовний продукт завжди притупляє пильність користувачів. Такі користувачі скоріше всього не читають умови надання послуги і не ставлять запитань.

Якщо VPN платний тоді зрозуміло де беруться гроші. Платні VPN не зацікавлені в продажу даних, так, як дорожать своїми користувачами і репутацією.

VPN поділяється на такі види:

1. Intranet VPN. Такий варіант дозволяє об'єднати кілька філіалів організації. Передача даних здійснюється по відкритих каналах. Інтернет може використовуватися для звичайних компаній і для мобільних офісів. Але слід мати на увазі, що такий спосіб передбачає установку серверів у всіх офісах.

2. Extranet VPN. Доступ до інформації підприємства надається клієнтам і іншим зовнішнім користувачам. При цьому їх можливості по використанню системи помітно обмежені. Не призначені для абонентів файли надійно захищаються засобами шифрування. Це відповідне рішення для фірм, яким необхідно забезпечити своїм клієнтам доступ до певних відомостей.

3. Remote Access. У цьому випадку створюється захищений канал між

офісом і віддаленим користувачем, що підключаються до ресурсів підприємства з домашнього ПК через Інтернет. Подібні системи прості в побудові, але менш безпечні, ніж їх аналоги, вони використовуються підприємствами з великою кількістю віддалених співробітників.

4. Client / Server. Цей варіант дозволяє обмінюватися даними між декількома вузлами всередині одного сегмента. Він користується найбільшою популярністю у організацій, яким необхідно в рамках однієї фізичної мережі створити кілька логічних, для захисту трафіку під час поділу використовується шифрування.

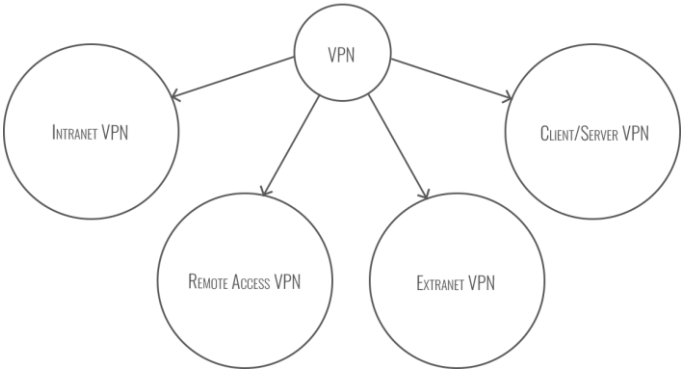


Рисунок 2 – Схема принципу роботи мережі VPN

Висновки. Було досліджено принципи роботи мережі VPN, основне її призначення, види та недоліки даної технології.

Список літератури

1. VPN [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/VPN

2. Принцип роботи мережі VPN [Електронний ресурс]. - Режим доступу: https://blog.themarfa.name/kak-rabotaiet-vpn-i-pochiemu-eto-luchshie-tor-ili-proxy/

3. Міфи про VPN [Електронний ресурс]. – Режим доступу: https://lifehacker.ru/2016/05/12/mify-o-vpn/

4. Що таке VPN [Електронний ресурс]. – Режим доступу: http://tersukr.ru/rizne/8813-shho-take-vpn.html

5. Організація корпоративних мереж [Електронний ресурс]. – Режим доступу: https://www.kp.ru/guide/korporativnaja-set.html

УДК 004.421.5

Проблеми пов'язані з використання генераторів випадкових послідовностей в системах захисту інформації

Павлуник Д.А., курсант
Науковий керівник – Кулініч О.М., к.т.н., доцент
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут ім. Ігоря Сікорського»

Невпевненість у генераторі псевдовипадкових чисел може призвести до серйозної шкоди криптографічним протоколам, і їх вразливості можуть бути використані зловмисниками.

Під «випадковим числом» мається на увазі число, яке є випадковим на практиці (тобто непередбачуваним, і таким, яке повторити неможливо). Може здатися, на перший погляд, досить просто, але набагато складніше це відтворити. Є велика різниця між тим, коли ми говоримо про окреме випадкове число та про випадкову послідовність. Окреме випадкове число є одним з набору можливих значень з рівною ймовірністю, коли у випадку з випадковою послідовністю, коли кожне нове значення повинно бути статистично незалежним одне від одного. Ми говоримо, що А статистично незалежне від В не зважаючи відбулося В, чи ні; і не має значення як часто відбувається А. Статистично незалежне означає, що жодне з них не несе інформації про інше.

У випадку генерування випадкової послідовності, використовуючи комп'ютер, це буде виглядати як «чорний ящик», який всі звикли називати «Генератор випадкових чисел». Можливо розділяти два основні способи генерування випадкових чисел: генератор псевдовипадкових послідовностей (ГПВП) і генератор на основі фізичних явищ. Обидва вони мають свої плюси і мінуси та є корисними в різних ситуаціях.

ГПВП – алгоритм, що виробляє числову послідовність, елементи якої не мають залежності один від одного і підкоряються заданому розподілу, який зазвичай є рівномірним.

Як показує слово "псевдо", вони виглядають випадковими, але не є випадковими, як ми могли б очікувати. Вони використовують деякі математичні формули, такі як лінійна конгруентна формула або деякі попередньо розраховані таблиці для отримання випадкових чисел.

Генератор на основі фізичних явищ використовує деякі зовнішні явища (наприклад, квантовий, тепловий, лавинний шуми) для генерації випадкових чисел і, отже, є більш випадковими, ніж ГПВП.

З ГПВП він, врешті-решт, повторюється і дає відправну точку (зерно), дізнаючись яке можна легко відтворити послідовність. Хоча фізичний генератор буде використовувати деякі апаратні явища або атмосферні

події, такі як поділ клавіатури, переривання, тощо, щоб створити послідовність.

Є багато характерних відмінностей між обома генераторами, що робить їх корисними в різних сценаріях (Табл. 1).

Таблиця 1 – Відмінності між ГПВП та генератором на основі фізичних явищ

	ГПВП	Генератор на основі фізичних явищ
Ефективність (з точки зору генерації більшої кількості за менший час)	Більша	Менша
Періодичність (повторює себе через деякий час)	Так	Ні
Детермінованість (послідовність може бути відтворена пізніше)	Так	Ні
Використання	Симуляція та моделювання додатків	Генерація паролів\ключів, шифрування даних, азартні ігри

Висновок

Отже, для формування ключових послідовностей краще використовувати генератор, що формує послідовність на основі фізичних процесів, оскільки фізичні процеси, на прикладі білого шуму не є детермінованими та дозволять підвищити надійність ключових даних. Та будь-який генератор для підтвердження своєї ефективності повинен пройти низку статистичних тестів таких як, наприклад, DIEHARD або більш популярного NIST.

Список літератури

1. Лифшиц Ю. Курс "Современные задачи криптографии". Лекция 9: Псевдослучайные генераторы [Электр. ресурс]. – Режим доступа: http://yury.name/crypto/09cryptonote.pdf

2. Дональд Э. Кнут. Глава 3. Случайные числа // Искусство программирования — 3-е изд. — М.: Вильямс, 2000. — Т. 2.

УДК 354.42

Комплексний аспект інформаційної безпеки

Панаско О.М., к.т.н., доцент
Черкаський державний технологічний університет, м.Черкаси

Зважаючи на бурхливий розвиток інформаційних технологій, інтенсивне впровадження інформаційно-телекомунікаційних систем в різноманітні сфери діяльності держави, сучасні світові тенденції щодо інформатизації суспільства, виникає необхідність в розгляді поняття та змісту інформаційної безпеки, а також його правового забезпечення з точки зору комплексного підходу до поняття. У зв'язку з тим, що на сьогоднішній день ряд основних загроз інформаційній безпеці держави реалізуються у кібернетичному просторі, окрему увагу слід приділяти поняттю кібернетичної безпеки в якості самостійної складової національної безпеки України по відношенню до сфери інформаційної безпеки.

Інформаційну безпеку доцільно розглядати у контексті комплексу дій, що пов'язаний із забезпеченням прав на захист інформації, а також права власності на інформацію, права на захист від інформації та інформаційних впливів, а також права на інформацію та свободу інформаційної діяльності. З цього приводу, на думку деяких дослідників в сфері інформаційної безпеки, вона представлена трьома структурними компонентами (рис.1):

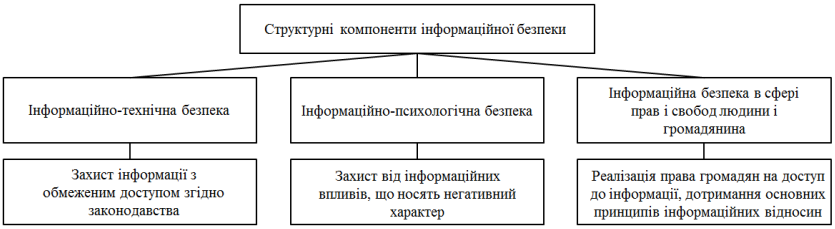


Рисунок 1 – Структурні компоненти інформаційної безпеки

До поняття інформаційної безпеки підходять з точки зору її рівнів, зокрема особистості, суспільства, держави. На державному рівні представлено діяльність державних органів в аспекті інформаційно-аналітичного забезпечення, інформаційне забезпечення міждержавного рівня внутрішньої і зовнішньої політики, система захисту інформації з обмеженим доступом тощо. Суспільний рівень інформаційної безпеки співвідноситься з якістю інформаційно-аналітичного простору, широкими

можливостями отримання інформації. Інформаційна безпека рівня особи характеризується формуванням раціонального, критичного мислення, обумовленого принципами свободи вибору.

На сьогоднішній день з'являються нові виклики – основні загрози інформаційній безпеці держави, зокрема, атаки на інформаційні ресурси держави, поява концепції ведення кібервоєн, створення у збройних силах ряду країн світу спеціальних структур, призначених для ведення такої боротьби, маніпулювання суспільною свідомістю, поява загроз для об'єктів критично важливої інфраструктури держави та суспільства та ряд інших, розгортаються у кібернетичному просторі. Затверджена Указом Президента України від 26.05.15 року нова редакція Стратегії національної безпеки України (№287/2015) [1], вперше виокремлює кібернетичну безпеку в якості самостійної складової національної безпеки України по відношенню до сфери інформаційної безпеки. Проникнення інформаційно-телекомунікаційних технологій в усі без виключення сфери суспільного життя обумовлюють тісний зв'язок кібербезпеки з іншими сферами національної безпеки, зокрема, військовою, оборонною, економічною, науково-технічною, екологічною тощо.

Питання захисту кібернетичного простору постає головним завданням держави, економіки та суспільства як на державному, так і на міжнародному рівнях. Велика увага приділяється нормативно-правовому регулюванню питань кібернетичної безпеки для створення умов та забезпечення безпечного функціонування кіберпростору при реалізації комунікацій та суспільних відносин на основі функціонування об'єднаних комунікаційних систем, а також використання глобальної мережі Інтернет. В цьому напрямку розроблено Стратегію кібербезпеки України, закон України «Про основні засади забезпечення кібербезпеки України» [2].

В цілому слід зазначити, що реалізація інформаційної безпеки проводиться на основі комплексного підходу та здійснюється на державному рівні, установ, організацій, інформаційно-телекомунікаційних систем із дотриманням загальних вимог до інформаційної безпеки, вимог до безпеки інформаційної інфраструктури та вимог до безпеки засобів інформаційних технологій.

Список літератури

1. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» від 26 травня 2015 року № 287/2015 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/287/2015.

2. Про основні засади забезпечення кібербезпеки в Україні: Закон України від 05.10.2017 № 2163-VIII//Відомості Верховної Ради України.– 2017. –№45.– Ст.403.

УДК 004.056

Некоторые аспекты обеспечения информационной безопасности

Поплавская Л.А., доцент, к.ф.-м.н.
Академия МВД Республики Беларусь

Отличительной особенностью современности является стремительное развитие телекоммуникационных и информационных технологий, которые становятся одним из доминирующих факторов в формировании общества XXI века. Постоянно увеличивающееся значение информационной составляющей, являющейся системообразующим фактором жизни общества, оказывает все более активное влияние на состояние социально-экономической, политической, военной и иных сфер национальной безопасности республики. От степени безопасности информационных технологий зависит не только благополучие, но порой и жизнь многих граждан. Информационная безопасность приобретает всё более высокую значимость в общей системе обеспечения национальной безопасности страны. Это предполагает обеспечение сохранности информационных ресурсов государства и защищённость законных прав личности и общества в информационной сфере и влечет за собой правовое регулирование общественных отношений в этой сфере, являющееся приоритетным направлением процесса нормотворчества в республике. Представляя собой сложную, многоаспектную проблему научного характера, информационная безопасность включает в себя технические, технологические, правовые, организационные, психологические и иные аспекты. Государственная политика обеспечения информационной безопасности республики определяет основные направления деятельности органов государственной власти в этой области, порядок закрепления их обязанностей и ответственности за защищённость интересов личности, общества и государства и базируется на соблюдении их баланса.

В процессе реализации своих функций по обеспечению информационной безопасности республики, государством проводится объективный и всесторонний анализ и прогнозирование внешних и внутренних угроз в сфере информационной безопасности, и разрабатываются меры по ее обеспечению. Организуется работа законодательных и исполнительных органов государственной власти республики по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз. Осуществляется контроль над разработкой, созданием, развитием, использованием средств

защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации. Принимаются меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов. Государство способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям, формулирует и реализует государственную информационную политику и способствует интернационализации глобальных информационных сетей и систем, а также вхождению Беларуси в мировое информационное сообщество на условиях равноправного партнёрства.

Государственная политика обеспечения информационной безопасности республики основывается на принципах соблюдения Конституции Республики Беларусь [1], законодательства республики, общепризнанных принципов и норм международного права с приоритетом развития отечественных современных информационных и телекоммуникационных технологий, производства отечественных технических и программных средств в целях соблюдения жизненно важных интересов республики. Первоочередными мероприятиями по реализации данной политики государства являются внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, реализация программ, предусматривающих формирование общедоступных архивов информационных ресурсов органов государственной власти республики, повышение правовой культуры и компьютерной грамотности граждан республики, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства и пресечение всякого рода компьютерной преступности.

Развитие информационных технологий привело к видоизменению старых и появлению новых форм противоправной деятельности, связанных с использованием различных компьютерных систем. Преступления против информационной безопасности приобретают транснациональный, организованный и групповой характер. Расследование преступлений против информационной безопасности имеет свои особенности как в области методики сбора доказательств, так и в оценке последних, а также в квалификации действий виновных лиц, что требует у правоохранителей владения определенными теоретическими и практическими знаниями и умениями в области компьютерных технологий и опыта работы в данной сфере. В республике имеется довольно обширная правовая база, представленная рядом законов, нормативных актов органов власти и управления, правовыми документами и международными соглашениями, а также договорами и контрактами, в которых стороны самостоятельно регламентируют отношения в соответствии с действующим законодательством. Вопросы правового регулирования информационной

безопасности занимают всё более значительное место в законодательстве республики, являются приоритетным направлением процесса нормотворчества в республике, цель которого – обеспечение информационной безопасности государства. 21 декабря 2017 года Президентом страны подписан Декрет №8 «О развитии цифровой экономики», предусматривающий целый ряд преобразований и улучшений в сфере информационных технологий [2], комплексно регулирующий данную сферу отношений и отражающий государственную политику в сфере обеспечения информационной безопасности, меры защиты, виды и источники угроз в сфере информационных технологий и первоочередные мероприятия по ее обеспечению.

Вместе с тем в республике еще недостаточно четко и полно решена проблема правовой защиты информации. В частности, существуют трудности в расследовании уголовных дел, связанных с преступлениями против информационной безопасности, обусловленные сложностью нормативной базы, переполненной узкоспециальными терминами и нормами. Недостаточная степень проработки отдельных правовых норм препятствует формированию единой следственной и судебной практики по делам рассматриваемой категории. Нет опыта в расследовании такого рода преступлений, правоприменительная практика для их исполнения только нарабатывается, нет единого подхода в применении информационных технологий при расследовании. Не хватает подготовленных на достаточно высоком уровне специалистов, существуют затруднения и в наличии современных методик расследования, в современных программных и аппаратных средствах диагностики действий нарушителей.

Информационная безопасность государства – это состояние сохранности ее информационных ресурсов и защищённости законных прав личности и общества в информационной сфере. Современное развитие информационных технологий опережает технологии обеспечения их безопасности. Отставание в своем развитии правоприменительной практики в республике требует постоянной коррекции отдельных правовых норм и внесения изменений в специальное законодательство республики в области информационной безопасности и (либо) принятие новых актов. Наличествует постоянная необходимость в усовершенствовании методик расследования нарушений в данной сфере, базирующихся на анализе потенциальных угроз информации и статистике преступлений, обеспечивающих установление факта нарушения, личности нарушителя, размера ущерба и способа восстановления прав собственника информации. Отставание технологии обеспечения безопасности информационных технологий от современного их развития влечет за собой и запаздывание в коррекции законодательства в их сфере, что создает возможности для манипулирования информацией, негативного воздействия на сознание людей, культуру, нравственные и духовные устои белорусского общества. Огромное внимание уделяется государством

ослаблению уровня зависимости республики от зарубежного программного обеспечения и средств информатизации. В республике форсируется разбработка доступных отечественных высокоэффективных средств, методов и систем защиты информации в общегосударственных информационных и телекоммуникационных системах, а также методов обеспечения надежного и бесперебойного функционирования этих систем. Прогрессирует развитие отечественной промышленности для производства в необходимых объемах современных средств информационной техники, применяемых для создания и развития национальной информационной инфраструктуры, обеспечения деятельности оборонного комплекса, органов государственного управления и наиболее важных предприятий финансовой и деловой сферы. Ведутся научно-исследовательские поиски как по инструментальным средствам защиты информационных ресурсов, так и по их категориальному классификатору информационной безопасности. Проводятся специальные организационно-правовые и воспитательные мероприятия по предотвращению и нейтрализации информационных угроз в духовной сфере жизни общества, по формированию общественного сознания населения страны в направлении активного противодействия этим угрозам.

Таким образом, в условиях становления информационного общества и возрастания скорости движения информации, вектор большинства угроз национальной безопасности страны сдвинулся в сторону информационной сферы. События в Северной Африке и на Ближнем Востоке, введенные США и Европой санкции против Белоруссии продемонстрировали всю силу информационных технологий и необходимость интенсивного развития собственных информационно-телекоммуникационных систем, межбанковской системы передачи информации, программного обеспечения, средств связи и передачи информации, средств защиты белорусского сегмента Интернета и других банков данных. Это повлекло за собой развитие и совершенствование не только самих технологий и ресурсов, но и нормативно-правовой базы и новых подходов к изучению приоритетов и к анализу, своевременному выявлению и оперативному предупреждению и пресечению угроз в информационной сфере республики. Законодательные акты и правоприменительная практика, касающиеся данной проблемы, пока находятся в стадии становления. Поиск новых путей и направлений обеспечения информационной безопасности не прекращается.

Список литературы

1. Конституция Республики Беларусь 1994 года (с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 1996 г. и 17 октября 2004 г.). – Минск: Амалфея, 2010. – 48 с.

2. О развитии цифровой экономики [Электронный ресурс] - Режим доступа: http://president.gov.by/ru/official_documents_ru/view/dekret-8-ot-21-dekabrja-2017-g-17716 (дата обращения: 19.02.2018).

УДК 070.1 (574)

Актуальные вопросы повышения доли отечественного телевизионного контента в контексте обеспечения информационной безопасности Республики Казахстан

Сабитов Р.С., PhD докторант
Евразийский национальный университет имени Л.Н. Гумилева, г. Астана, Казахстан

В условиях глобализации и геополитических вызовов деятельность масс-медиа находится в центре внимания, как зарубежных институтов, так и отдельных исследователей. В данном контексте особое внимание уделяется вопросам информационной безопасности государств. Важное значение приобретают научно-методические подходы к исследованию вопросов, связанных с манипуляциями массовым сознанием с помощью разножанровых телепередач.

Многочисленные теории и концепции тележурналистики отражают особенности существования современного общества и многоплановость научных подходов к анализу предпочтений телепродукции той или иной аудитории. При этом некоторые исследователи часто высказываются о вытеснении Интернетом телевидения в ближайшие 15-20 лет, поскольку Интернет, с применением самых свежих современных интерактивных технологий, дает возможность смотреть понравившуюся передачу без назойливых реклам и без временных ограничений сетки вещания программ.

«Интернет-телевидение – это суточная телесистема оперативного предоставления информации потребителям, живущим в любой точке мира и вместе с тем, способная сохранить архив передач, прошедших в эфире, не только предоставляя различным сегментам аудитории телевизионные контенты разнообразных жанров и форм» - говорит Н. Гегелова [1]. Однако, несмотря на это традиционное телевидение по сегодняшний день играет важную роль в жизни людей. Среди пятисот привычных действий человека, не считая сна, по наблюдениям социологов, первое место занимает время, потраченное на телеканал.

Девять из десяти человек старше четырех лет минимум пять дней в неделю тратит около четырех часов на просмотр телеканалов. Только телевидение, 51% которого составляет киноиндустрия, доводит прямиком до подсознания человека объяснение любого события. Мы, попавшие в поток виртуальных фраз не только не различаем состав, объем и структуру эфира, но даже не замечаем как невольно попадаем под его влияние. Мы не только не думаем, но даже не чувствуем, как нами мастерски управляет телеконтент.

Кроме эфирного телевидения, интенсивное развитие спутникового,

Интернет и мобильного телевидения создает жесткую конкуренцию за аудиторию на отечественном рынке. «Сегодня телевидение превратилось из идеологического института в бизнес» [2], по этой причине любой телеканал, чтобы увеличить поток рекламодателей, в первую очередь, заинтересован предоставить своему зрителю качественный и новый контент. «У телевидения на казахстанском рынке также исчерпаны первоначальные возможности, теперь для того, чтобы его развивать, зарабатывать, вместе с тем, превратить его в важный фактор общественного развития, предельно ясно, что нужно найти свою аудиторию, адаптироваться к его конкретным запросам» [3].

XXI век – эпоха глобализации. Широкое распространение виртуальных отношений отдельно от реальных связей изменило вкусы и требования зрителя к телепродукции. Рост информационного потока, интенсификация культурных связей между народами, более четкая чем прежде сегментация аудитории позволяет ему активно участвовать во всех коммуникационных процессах. Однако, если учесть еще неполную обеспеченность страны компьютерами, что неполностью еще сформирована привычка населения смотреть телепередачи через Интернет, существенную дороговизну высокоскоростного Интернета, недостаточность устойчивой технической поддержки интернет-телевидения, незавершенность технических параметров, предлагаемых передач, если учесть, что не всегда можно найти в сети бесплатный и доступный телеконтент, не говоря уже о прошедших передачах (время сохранения информации в архиве ограничено), ценность традиционных телеканалов пока не меньше, чем у новых средств передачи информации. Одним словом, главный недостаток интернет-телевидения – это ограничение телеконтента, что является основной причиной того, что по сей день зрители отдают приоритет эфирным, традиционным телеканалам. Эксперты говорят: «Список доступных в сети передач еще небольшой. Например, телеканалы считают правильным разместить на сайте лишь одну известную часть телесериала. К тому же срок его демонстрации ограничен лишь несколькими неделями, т.е. через две-три недели передача стирается с архива или чтобы ее посмотреть придется специально подписываться» [4].

Сравнивая телеканал с Интернетом, нельзя недооценивать роль первого в производстве контента. «Телеканал – это не способ вещания, это контентная команда. Хотя отдельный пользователь интернета способен сообщить о фактах, вызывающих беспокойство, написать интересные тексты, загрузить эксклюзивные видео, он не в состоянии создать качественный и содержательный аудиовизуальный контент, который может заинтересовать десятки и сотни миллионов людей. Значительную часть самого посещаемого контента Интернета разрабатывает классический коллектив киностудий, телеканалов и компаний производителей телеконтентов. Это коллективный труд» [5], –

говорит К.Эрнст.

Как бы не сказали, ежедневный эфир показывает, что технологии производства контента на казахстанских телеканалах опираются только на потребительские, рыночные критерии. На сегодняшний день рейтинг «превратился в единственное метасистемное направление в создании отечественного телеконтента» и вопрос о контенте должен иметь не количественную, а качественную форму. Поскольку, под этим понятием в качестве ключа, открывающего содержание и смысл телеканала находится форма. Тем не менее рейтинг – это всего лишь средство измерения, состоящее из количества определенных людей, одновременно включивших телеприемники. Но это не доказывает, что они все смотрят телевизор и воспринимают и принимают контент, идущий в эфире. Так как известно, что «кроме целевого просмотра телевизора, есть виды случайного, дискретного (урывками), фонового (занимаясь другими делами) и звукового (слушание только голоса) просмотра» [6]. Однако руководители всех телеканалов определяют результаты своей работы именно по этому рейтингу, так как в результате этого они добиваются своей основной цели – сверхприбыли. А такие общественно важные цели как личностное и общенациональное развитие, формирование гражданского самосознания, работа, направленная на психологическое здоровье и др. совсем забываются. А это может удовлетворять общество? Соответствует ли разрабатываемая телепродукция спросу аудитории? По мнению мировых профессиональных критиков, капризных зрителей и активных Интернет пользователей, в любой стране имеет место тенденция неудовлетворенности качеством телеконтента.

Коммерческие компании готовы платить огромную сумму для рекламы: так как только телеканалы могут охватить одновременно миллионы потенциальных потребителей. «Известно, что в этом бизнесе стоимость рекламы определяет рейтинг, поэтому любой телеканал прилагает все силы для оправдания доверия аудитории» [7].

Требования сегодняшнего дня показывают, что только динамичный, постоянно меняющийся, обновляющийся эфир может достойно отвечать интересам зрителя. Однако не всякий телеканал может обеспечить такую разновидность, так как сама телеиндустрия требует значительных затрат. По этой причине вся ТВ-индустрия в мире работает в двух направлениях - как операторы, отвечающие за качество распространяемого сигнала и как разработчики телевизионных программ. Таким образом они эффективно используют свои силы и время, оптимально распределяя между собой обязанности.

Казахстанская телевизионная сфера, с момента перехода которой на рыночные отношения прошло четверть века, также работает в этой системе. Некоторые аутсорсинговые компании, готовящие телепрограммы, успели занять свое достойное место на отечественном телерынке. Все телеканалы республиканского уровня, кроме

региональных телеканалов, используют возможности компаний, предлагающих почти готовую продукцию. Но у проблемы есть другая сторона: к сожалению пока «в стране не так много продюсерских центров и телекомпаний, способных предложить качественную продукцию» [8]. Последствия этого сильно отражаются на коммерческих телеканалах, не получающих финансовую помощь от государства.

Проводится ли в Казахстане многоуровневый анализ на контенты наиболее популярных телепередач – новости, ток-шоу, телесериалы? Есть ли спрос на их изучение со стороны власти, политических экспертов, специальных служб или рынка? К сожалению, не секрет, что мы порой затрудняемся ответить на эти вопросы. Несмотря на интенсивное развитие телевидения изо дня в день, в нашей стране до сих пор можно сказать, отсутствуют стратегическая программа развития отечественного телевидения, аналитико-экспертная исследовательская работа, ориентирующая и направляющая отечественный телерынок. По этой причине в отечественных телеканалах не сформировалась единая идеологическая линия, сосредоточенная на общих интересах. Поэтому в будущем, значительная часть огромной работы, которую предстоит выполнить в данном направлении, остается за отечественными учеными.

Сегодня казахстанская телевизионная индустрия адаптировалась к рыночным отношениям и начала подниматься на новую ступень развития. В последние годы на телеэкранах все чаще стали появляться казахстанские сериалы и адаптированные казахские варианты известных мировых телепроектов. Особый интерес у зрителей к национальному продукту способствует росту рейтинга отечественных телеканалов. Это позволяет понимать, что отечественные телепередачи постепенно начали переходить от количества к качеству. Тем не менее, в сфере производства телепередач и телевещания нашей страны есть немало назревших и нерешенных проблем. Накопившиеся в повестке дня проблемы требуют со стороны специалистов и экспертов комплексного анализа и новых подходов.

К сожалению, пока казахстанские зрители отдают предпочтение иностранным продуктам, особенно российским передачам и турецким, индийским, корейским телесериалам. «Одной из причин этому является то, что отечественный телерынок не всегда может предложить качественный продукт и это свободное пространство, пользующееся спросом заполняет иностранный контент» [9]. Например во время прайм-тайм 20-40% программы казахстанских телеканалов занимают иностранные телесериалы [10].

Несбалансированность доли иностранных передач, беспрепятственно распространявшихся на территории Казахстана, долгие годы оказывало свое отрицательное влияние на нашу отечественную телеиндустрию. Во-первых, казахстанские телеканалы, привыкшие к иностранным контентам приспособились к легкому способу заполнения эфира. Готовый продукт

не требует лишних расходов и творческих поисков. В результате чего отечественные телеканалы не смогли сформировать конкурентоспособный иммунитет в современных условиях. Во-вторых, не секрет, что иностранный контент, свободно вошедший в наше информационное пространство, в значительной степени воздействовал на культурные, социально-политические взгляды и мировоззрение местной аудитории, с точки зрения национальной безопасности. В этой связи необходимо отметить, что в нашей стране по сей день не сформирован цензурный механизм, оценивающий и устанавливающий контроль за иностранными передачами.

Конечно, понятно, что хотя отечественные телеканалы заинтересованы в увеличении национального контента, их к этому шагу обязывают требования законодательства, чем зрительский спрос. Особенно для коммерческих телеканалов производство отечественного телепродукта с экономической точки зрения нерентабельно, поэтому во многих случаях они не рискуют снимать телесериалы и мегапроекты, требующие колоссальные средства. Мировая практика доказывает, что для любого телеканала намного дешевле обходится покупка готового контента, чем снятие своего продукта. Например, «если сегодня телеканалы нашей страны за каждую серию турецкого телесериала с высоким рейтингом на рынке, платят по 3000 долларов, то на снятие одной серии отечественного телесериала необходимо потратить минимум 30 000 долларов» [8]. Взамен этого, на коммерческих каналах большую часть национального контента составляют не требующие больших средств новости, ток-шоу и развлекательные программы.

В создании национального контента по сравнению с коммерческими каналами больший потенциал у государственных каналов. Очевидно, что государственный патронаж во многих случаях, вместо создания условий равной конкурентоспособности для игроков рынка, повышает гегемонию государственных каналов. В последние годы коммерческие каналы тоже стали получать государственные заказы. Однако руководители коммерческих каналов говорят, что этих средств недостаточно для полного покрытия эфирных расходов. Со слов бывшего генерального директора телеканала КТК Каната Сахариянова, в 2015 году у КТК хватило возможности снять всего лишь только три сериала, состоящие каждый из трех частей [9]. А телеканал «Қазақстан», имеющий государственный статус «вынес на рынок в последние три года почти 50 сериалов» [10]. Тогда закономерно, что государственные телеканалы лидируют в производстве отечественных телесериалов.

При оценке отечественной телеиндустрии не следует забывать наличие значительного влияния на его развитие геополитических факторов. Невозможно остаться в стороне от влияния соседней России, входящей в десятку мощного европейского телерынка. Не говоря уже о российских телеканалах, свободно вещающих на территории нашей страны, правда,

что Казахстан является вторым рынком для российской теле- и киноиндустрии. Во-первых, куда эффективнее купить качественный продукт с меньшими затратами, чем потратив много средств, снять у себя передачу с низким качеством. Во-вторых, отсутствие языковых барьеров спасает от лишней работы и затрат, таких как перевод, дубляж, изготовление субтитра. В третьих, близость менталитета показывает, что спрос со стороны местных зрителей на российский телеконтент, особенно на сериалы и ток-шоу все еще высок.

Если учесть, что по сравнению с Казахстаном, российский телерынок больше в десять раз, в соответствии с ним и прибыль от реклам также более значительная. Часть прибыли, поступившей от реклам расходуется на большие проекты с высоким рейтингом. В этой связи, понятно, что казахстанские телеканалы с куда более узким рекламным рынком не могут конкурировать с российскими коллегами. К тому же и российские каналы, беспрепятственно вещающие на территории нашей страны, до этого делили отечественный рекламный рынок без всяких обязательств и наносили значительный ущерб национальной телеиндустрии. Только от рекламного рынка иностранные медиаресурсы в Казахстане получали каждый год прибыль свыше четырех миллиардов тенге. Лишь в последние годы работа в этом направлении изменилась в сторону интересов казахстанских телеканалов. В нашей стране в соответствии с внесенными изменениями в Закон «О рекламе», теперь приличная сумма, поступающая от реклам будет использована для производства телепередач.

Закон нашей страны «О телерадиовещании» не ограничивает подготовку местного контента за пределами Казахстана. Эта льгота дает возможность телеканалам снимать передачи за рубежом в целях подготовки качественного продукта и экономии средств. Специалисты телевидения нашей страны говорят, что в Украине и соседней России студия и декорация, техническое оборудование и иные виды услуг намного дешевле и на должном уровне. Тем не менее, несмотря на запоздалость на несколько лет закон, поддерживающий отечественную телеиндустрию, был принят в 2012 году, он установил требования относительно удельного веса иностранного и местного контента, выходящего в эфир. В соответствии с Законом Республики Казахстан «О телерадиовещании» отечественные теле-, радиопередачи в объеме еженедельного телерадиовещания теле-, радиоканалов должны составляють:

1) с 1 января 2014 года – не менее тридцати процентов;

2) с 1 января 2016 года – не менее сорока процентов;

3) с 1 января 2018 года – не менее пятидесяти процентов.

Государственная программа «Информационный Казахстан – 2020» в целях обеспечения конкурентоспособности отечественного информационного пространства предусматривает увеличение в 2020 году

телепродукции в отечественной индустрии до 60%.

Государственная политика в поддержку отечественного продукта незамедлительно начала давать свои плоды. Согласно исследованиям компании «J'son & Partners Consulting», сегодня в структуре телевещания на медиарынке Казахстана национальный контент имеет приоритет и эта тенденция в последние годы остается без изменений. Например, в эфире крупных телевизионных каналов страны доля отечественного контента составляло в 2014 году 53%. Если ссылаться на исследования «J'son & Partners Consulting», среди отечественных телеканалов активно вещают иностранный контент «31 канал» (69,5%), «Астана ТВ» (68,4%) и «Евразия» первый канал» (65%). А на телеканале «Қазақстан» доля иностранного контента составляет лишь 13%. Если на телеканале «Хабар» отечественный продукт составляет 72,3% , то «Седьмой канал» (60,7%) – на следующем месте.

Среди отечественных телеканалов также широко распространяется тенденция приглашения иностранных специалистов. Основная причина обращения за помощью к иностранцам – нехватка в стране профессиональных специалистов, умеющих снимать качественные телепередачи. Дефицит кадров в этой сфере не выполняет одинаковый спрос всех участников телерынка. Генеральный директор «Седьмого канала» Азиза Шожеева рассказывает, что часто приглашает в Казахстан иностранных специалистов и консультантов для обучения своих сотрудников [11]. Казахская телеиндустрия нуждается до сих пор в помощи иностранных креативных агентств, особенно, при разработке адаптаций известных мировых форматов.

В сфере информационной безопасности вопрос развития отечественного телеконтента в количественном и качественном отношении остается в любое время актуальным. Чтобы противостоять непрерывной культурной экспансии развитых стран мира, государство защищая от внешних факторов, должно создавать для всех справедливые и равные условия в соответствии с законом рыночных отношений. Для этого полагаем, что Министерству информации и коммуникаций Республики Казахстан следует внимательно исследовать и изучить следующие пожелания и рекомендации:

- Уменьшить показ иностранных телеканалов в Казахстане;
- Рассмотреть механизмы налогообложения телеканалов, ретранслирующих иностранный контент, согласно хронометража и жанра;
- Создать при Министерстве информации и коммуникаций РК специальную рабочую группу по проверке содержания иностранного контента;
- Предусмотреть налоговые льготы телеканалам для развития индустрии отечественного сериала.

Самое главное, желательно наряду с возложением обязательств в информационной политике уметь правильно применять на

законодательном уровне механизмы стимулирования отечественных телеканалов.

Список литературы

1. Гегелова Н. Интернет-телевидение в России: преимущества и недостатки // Медиальманах, 2011, №5 (46). С.73-77.

2. Полуэхтова И. Динамика Российской телеаудитории // Социологические исследования. 2010, № 1, С. 66-77.

3. Бейсенқұлов А. Қазақстандық бұқаралық ақпарат құралдарының жаңа технология негізінде даму проблемалары. Филол.ғылымд. канд. диссертация. 10.01.10. Әл-Фараби ат. ҚазҰУ. 2001, Алматы, 33 б.

4. Мясникова М. Производство и анализ россиийского телеконтента как научные проблемы // Известия Уральского федерального университета. 2013, серия 1, № 4 (119), С. 74-82.

5. Эрнст К. Запах времени. Новый язык телевидения еще не создан // Искусство и кино, 2012, №4. С. 5-11.

6. Дондурей Д. Граждане против гражданского общества. Телерейтинг как воспитатель нации // Искусство кино, 2013, №4. С.5-15.

7. Толоконникова А. Вещатели и производители программ на российском телевизионном рынке. – Москва, 2009, Полпред Справочники, 68 с.

8. Цай А. Интервью с Генеральным продюсером ТОО «Телекомпания «Эра» Михаилом Дорофеевым: «И седьмые станут третьими» [Электр. ресурс] – 2009. – Режим доступа: http://expertonline.kz/a3630/

9. Веселева О. Интервью с Генеральным директором Первого канала «Евразия» Сергеем Киселевым: «Развивать казахстанский телевизионный контент трудно, но реально [Электр. ресурс– 2012. – Режим доступа: https://kapital.kz/gazeta/9474/sergej-kiselev-razvivat-kazahstanskij-televizionnyj-kontent-trudno-no-realno.html

10. Amos O. Television dependency in independent Kazakhstan: Programming Via Relay, Import and Adaptation // The international journal for communication studies. – 2005. – №67(4), p. 325-337.

11. Бочарова М. Интервью с генеральным директором «Седьмого канала» Азизой Шужеевой: «Государственное финансирование не стимулирует рост телерынка» [Электр. ресурс]. – 2013. – Режим доступа: https://vlast.kz/persona/aziza_shuzheeva_gendirektor_sedmogo_kanala_gosudarstvennoe_finansirovanie_ne_stimuliruet_rost_telerynka-1675.html

УДК 004.056

Огляд статистичних тестів ГВЧ та ГПВЧ стандарту NIST 800-22 Revision 1a

Собінов О.Г., викладач
Центральноукраїнський національний технічний університет, м. Кропивницький

При розробці генераторів випадкових чисел (ГВЧ) і генераторів псевдовипадкових чисел (ГПВЧ), які передбачається використовувати в криптографічних програмних засобах, виникає проблема з оцінки якості отриманих ГВЧ і ГПВЧ. При цьому, поняття якість потребує оцінки, яка може показати розробнику певну метрику для дослідження і порівняльної оцінки отриманих послідовностей.

Як відомо Кнут в визначив такі основні критерії перевірки випадкових спостережень: критерій «хі-квадрат» (χ2-критерій); критерій Колмогорова-Смірнова; критерій рівномірності (критерій частот); критерій серій; критерій інтервалів; покер-критерій (критерій розбиття); критерій збирання купонів; критерій перестановок; критерій монотонності; критерій конфліктів; критерій проміжків між днями народження; критерій серіальної кореляції; критерій послідовностей.

Зрозуміло, що Кнут навів найбільш популярні тести і критерії оцінки випадкових (псевдовипадкових) послідовностей. Існує велика кількість джерел з критичною оцінкою того або іншого тесту чи критерію. Однак, при проведенні тестування ГВЧ і ГПВЧ, як і при проведенні випробувань будь-яких технічних рішень слід орієнтуватися не на суб'єктивні(хоча і математично обгрунтовані) види перевірки, а на прийняті спільнотою розробників методів і критеріїв математичної оцінки (МКМО) об'єкта, що тестується.

Зазвичай такі МКМО називають стандартами і приймають, залежно від важливості об'єкта, який досліджується – національними, державними, міжгалузевими, галузевими і т.д.

На сьогоднішній день одним з кращих стандартів оцінки якості бінарного ГВЧ і ГПВЧ є стандарт NIST SP 800-22 Національного інституту стандартів и технологій(NIST), який був заснований у 1901 році і зараз є частина Міністерства торгівлі США. NIST є однією з найстарішіх фізичних наукових лабораторій Північної Америки.

В наш час використовується версія від 27 квітня 2010 р. NIST SP 800-22rev1a, яка називається – «Статистичний тестовий комплект для перевірки генераторів випадкових чисел і генераторів псевдовипадкових чисел для криптографічних додатків», який описує набір тестів.

Відповідно до заголовку 17 розділу 105 Кодексу США, це програмне забезпечення не підлягає захисту авторських прав і знаходиться в

суспільному використанні. Статистичний тестовий комплект NIST є експериментальною системою.

NIST не несе ніякої відповідальності за її використання іншими сторонами і не дає ніяких гарантій, і не приймає зауважень щодо його якості, надійності або будь-яких інших характеристик оціночного визнання, якщо програмне забезпечення використовується

Було розроблено, реалізовано і оцінено 15 статистичних тестів. В таблиці 1 описується кожен з тестів.

Таблиця. Статистичні тести NIST SP 800-22rev1a

№	Назва	Короткий опис
1	**Тест частотний (монобітний)** Frequency (Monobits) Test	**Тест визначає** – частку нулів і одиниць для всієї послідовності. **Мета тесту** – визначити, чи є це число одиниць і нулів в послідовності приблизно такими ж, як очікувалося б для дійсно випадкової послідовності. **Тест оцінює** – близькість частки одиниць до ½, тобто Число одиниць і нулів в послідовності має бути приблизно однаковим.
2	**Тест на частоту в середині блока** Test For Frequency Within A Block	**Тест визначає** – частку нулів і одиниць в М-бітових блоках. **Мета тесту** – визначити, чи є частота одиниць М-розрядної блоку приблизно рівною М/2. **Тест оцінює** ~ ½ частку одиниць в М-розрядному блоці.
3	**Тест пробігів** Runs Test	**Тест визначає** – загальне число нулів у всій послідовності, де прогін є безперервною послідовністю однакових біт. Прогін довжини k означає, що пробіг складається з рівно k однакових бітів і обмежений до і після бітом з протилежним значенням. **Мета тесту** – визначити, чи є кількість прогонів одиниць і нулів різної довжини очікуваним для випадкової послідовності. **Тест оцінює**, чи є коливання між такими підрядками занадто швидким або занадто повільним.
4	**Тест на самий довгий прохід в блоці** Test For The Longest Run Of Ones In A	**Тест визначає** – найдовший блок з М-бітових блоках. **Мета тесту –** визначити, чи відповідає довжина найдовшого проходу в послідовності, що тестується, довжині найдовшого проходу, який очікувався в випадковій послідовності. **Тест оцінює** нерегулярність довжини найдовшого

	Block	пробігу одиниць. Існує також очікування нерегулярності довжини найдовшого пробігу нулів. Довгі черги нулів не оцінюється окремо для забезпечення статистичної незалежності між тестами.
5	**Тест рангово - матричний** Random Binary Matrix Rank Test	**Тест визначає** – ранг непересічних підматриць всієї послідовності. **Мета тесту** – перевірка лінійної залежності між підрядками постійної довжини у вихідній послідовності. **Тест оцінює** ранги матриць які не перетинаються.
6	**Тест дискретного перетворенн Фурье (спектральний)** Discrete Fourier Transform (Spectral) Test	**Тест визначає** – пікові висоти дискретного швидкого перетворення Фур'є. **Мета тесту** – виявлення періодичних ознак або патернів, що повторюються, і які знаходяться поруч один з одним в послідовності, що тестується. **Тест оцінює** відхилення від припущення про випадковість.
7	**Перевірка шаблонів, що не перекриваються (апереодичність)** Non-Overlapping (Aperiodic) Template Matching Test	**Тест визначає** – кількість входжень заданих підрядків. **Мета тесту** – пошук відхилень послідовностей, які показують занадто багато входжень заданої неперіодичності(апериодичності). Для цього тесту зіставлення перекриття шаблоном і пошуку певного m-бітового шаблону використовується вікно m-bit. Якщо шаблон не знайдений, вікно зрушується на одну бітову позицію. Для цього у тесті, коли шаблон знайдено, вікно повертається в біт після знайденого шаблону, і пошук поновлюється. **Тест оцінює** повторюваність заданих шаблонів у числовому ряді.
8	**Тест перевірки перекриття (періодичного) відповідного шаблону** Overlapping (Periodic) Template Matching Test	**Тест визначає** – кількість попередньо визначених цільових подстрок. **Мета тесту** – відмова від послідовностей, які показують відхилення від очікуваної кількості прогонів певної довжини. Зверніть увагу, що коли є відхилення від очікуваної кількості одиниць заданої довжини, є також відхилення в прогонах нулів. Для цього тесту, коли шаблон знайдений, вікно знову зрушує один біт, і пошук поновлюється. **Тест оцінює** повторюваність завдань шаблонів у числовому ряді

9	**Тест універсальний статистичний Маурера** Maurer's Universal Statistical Test	**Тест визначає** – кількість біт між співпадаючими шаблонами. **Мета тесту** – визначити, чи може послідовність бути значно стиснута без втрати інформації. **Тест оцінює** – якість (щільність) стиснення числової послідовності. Послідовнсть яка сильно стискається вважається невипадковою.
10	**Тест лінійної складності** Linear Complexity Test	**Тест визначає** – довжину генеруючого регістра зворотного зв'язку. **Мета тесту** – визначити, чи достатньо складна послідовність, щоб вважатися випадковою. Випадкові послідовності характеризуються довшим регістром зворотного зв'язку. Короткий регістр зворотного зв'язку має на увазі невипадковість. **Тест оцінює –** оцінює кількість непарних слів і таким чином визначає щільність стискання послідовності.
11	**Тест послідовностей** Serial Test	**Тест визначає** – частота кожного перекривати м-бітового шаблону у всій послідовності. **Мета тесту** – визначити, чи є кількість входжень шаблонів перекриття 2m m-біт приблизно таким же, яка очікувалася для випадкової послідовності. Шаблон може перекриватися. **Тест визначає** з якою ймовірністю з'являється у послідовності кожен шаблон з m-бітів
12	**Тест апроксимуючий ентропійний** Approximate Entropy Test	**Тест визначає** – частоту кожного m–бітового шаблону, який перекривається. **Мета тесту** – порівняння частоти блоків двох послідовних/суміжних довжин (m і m + 1), які перекриваються з очікуваним результатом для випадкової послідовності. **Тест визначає** з якою ймовірністю з'являється у послідовності кожен шаблон з m-бітів.
13	**Тест кумулятивної суми** Cumulative Sum (Cusum) Test	**Тест визначає** – максимальне входження (від нуля) випадкового блукання, що визначається сумарним значенням скоригованих(-1, +1) цифр в послідовності. **Мета тесту** – визначити, чи є сумарна сума часткових послідовностей, що знаходяться в тестованої послідовності, занадто великий або занадто малою щодо очікуваної поведінки цієї сумарної суми для випадкових послідовностей. Цю сукупну суму можна розглядати як випадкові

		блукання. **Тест визначає** те, що для випадкової послідовності випадкове блукання має бути близько нуля. Для невипадкових послідовностей відхилення від цього випадкового відхилення від нуля буде занадто великими.
14	**Тест випадкових перевірок відвідувань** Random Excursions Test	**Тест визначає** – кількість циклів, що мають точно K відвідувань в сумарній сумі випадкового блукання. Кумулятивна сума випадкового блукання визначається, якщо часткові суми послідовності (0,1) коригуються до (-1, +1). Випадкове відвідування випадкового блукання складається з послідовності n кроків одиничної довжини, які беруться випадковим чином, і які починаються з і повертаються в початок координат. **Мета тесту** полягає в тому, щоб визначити, чи перевищує кількість відвідувань стану випадкові блукання випадкової послідовності. **Тест визначає** чи відрізняється кількість відвідувань визначенного стану в середені цикла від аналогічної кількості у випадку абсолютно випадкової вихідної послідовності.
15	**Тест випадкових перевірок варіантів відвідувань** Random Excursions Variant Test	**Тест визначає** – кількість випадків, коли визначений стан відбувається у кумулятивній сумі випадкового блукання. **Мета тесту** – знаходження відхилень від очікуваної кількості входжень різних станів при випадковому блуканні. **Тест визначає** на кожному етапі випадковість вихідної послідовності.

Пакет NIST STS дозволяєть побудувати методики якісного статистичного і структурного аналізу ГВЧ та ГПВЧ послідовностей.

Список літератури

1. Кнут Д. Искусство программирования. Том 2. Получисленные алгоритмы. В 4-х томах. Пер. с англ. – 3-е изд. – М.: Вильямс, 2006. – 682 с.

2. Слеповичев И.И. Генераторы пседослучайных чисел. Учебное пособие. [Електронний ресурс] / Слеповичев И.И. – 2017. – Режим доступу до ресурсу: https://www.sgu.ru/sites/default/files/textdocsfiles/2017/10/04/slepovichev_i.i._generatory_psevdosluchaynyh_chisel_2017.pdf

3. Cybersecurity [Електронний ресурс]. – Режим доступу: https://www.nist.gov/topics/cybersecurity

УДК 623.618.2

Алгоритм захисту радіолінії управління безпілотним літальним апаратом

Стасєв Ю.В. д.т.н., професор, Стасєв С.Ю. к.т.н., Серов С.С.
Харківський національний університет Повітряних Сил імені Івана Кожедуба, м. Харків

Досвіт експлуатації безпілотних літальних апаратів показав, що найбільш слабким ланцюгом системи управління цих апаратів є радіолінія управління, яка може легко бути подавлена засобами радіоелектронної боротьби, або заблокована імітаційними повідомленнями.

Мета роботи – розробка достатніх та необхідних умов реалізації алгоритму захисту радіолінії управління безпілотним літальним апаратом на фізичному рівні.

В доповіді наводяться необхідні та достатні умови функціонування захищеної радіолінії управління безпілотних літальних апаратів на фізичному рівні. Основні з них є:

1. Ймовірність передачі сигнально-кодової конструкції не повинна залежати від переданих інформаційних символів і від передачі попередніх сигнально-кодових конструкцій.

2. Розмір ансамблю використовуваних сигнально-кодових конструкцій має задовольняти вимогам з іміто- і криптостійкості.

3. Надмірність, яка міститься в інформації про множину, що задає алгоритм захисту радіолінії управління безпілотним літальним апаратом на фізичному рівні, повинна прямувати до нуля.

4. Складність і стійкість множини, що задає режим функціонування на фізичному рівні, повинна вибиратися залежно від використовуваного протоколу й вимог до імітозахисту системи.

5. Виконання процедур перетворення має бути формальним. Ці процедури не повинні залежати від довжини повідомлення.

6. Стійкість множини, що задає алгоритм захисту радіолінії управління безпілотним літальним апаратом, не повинна порушуватися навіть у випадку, коли супротивнику відомий алгоритм захисту радіолінії управління безпілотним літальним апаратом.

Таким чином, необхідні й достатні умови визначають шляхи досягнення теоретичної недешифрованності алгоритму захисту радіолінії управління безпілотним літальним апаратом, а їх реалізація дозволяє забезпечити активний завадо- та імітозахист від засобів радіоелектронної розвідки й радіоелектронної боротьби ймовірного противника.

УДК 681.3.06

Підвищення безпеки засобів електронного самоврядування на прикладі електронних петицій

Трифонова А.А., студентка 3 курсу
Науковий керівник – Желдак Т.А., к.т.н., доцент
НТУ «Дніпровська політехніка», м. Дніпро

Перед кожним з нас хоча б один раз поставало питання передачі необхідної інформації адресату потай від інших. Люди стикалися з цим в різний час та з різними цілями і зрозуміли, що практичне вирішення питання захисту інформації лежить в практичній задачі перетворення її, яке унеможливить прочитання цієї інформації іншою особою. Особливо актуальною ця проблема стає в час загальної інформатизації, коли більшість комунікаційних задач покладено на автоматизовані засоби комунікації.

Розглянемо реалістичний приклад, де необхідно застосовувати криптографічні засоби захисту інформації – електронні петиції до Президента України на відповідному сайті.

Сьогодні цей сервіс передбачає наступний функціонал: реєстрація петиції, попередня модерація, підтримка петицій з підтвердженням по e-mail, ідентифікація користувача, моніторинг ходу голосування та розгляду петицій, історії успішних петицій, інтеграція з соціальними мережами [1].

Відповідно до заяв, які поступають від модераторів електронних петицій, стає зрозуміло, що наявний алгоритм ідентифікації користувачів та унеможливлення маніпуляцій волевиявленням громадян віджив своє, тож треба запропонувати більш стійкий та надійний алгоритм подачі петицій та перевірки голосів на їх підтримку.

Сформуємо задачу: є коло осіб – це громадяни України, частина з яких хоче підписати певне повідомлення – в нашому випадку – петицію. Тоді, згідно українського законодавства алгоритм підпису електронної петиції має передбачати наступні функції та обмеження:

- всі підписи мають належати різним особам;
- має бути можливість перевірки належності кожного підписанта до зазначеного кола осіб;
- має бути відсутня можливість перевірки належності підпису конкретній особі;
- кожен підписант може поставити персоналізований або анонімний підпис;
- відсутня можливість перевірки на наявність підпису конкретної особи.

Одним з варіантів такої системи є система з використанням асиметричної криптографії, алгоритмом цифрового підпису та сертифікацією ключів.

Актуальність побудови такої системи обумовлена не якимись штучними чинниками, а українськими реаліями, коли створюються цілі об'єднання в кваліфікованих користувачів, метою яких є спотворення волевиявлення в засобах електронного самоврядування.

Методологія алгоритму полягає в наступному: кожен учасник генерує пару ключів для асиметричного шифрування – методів, в яких використовують пару ключів для кожного учасника протоколу – відкритий для шифрування і таємний для розшифрування, який не може бути обчислений з відкритого ключа за визначений час, використовують сучасні методи шифрування (Схема McEliece, Схема ElGamal, RSA, Алгорит Діффі-Хеллмана) [2].

Математичний апарат державного серверу підтверджує, що ключ дійсний та належить вказаній особі. Цей етап проводиться один раз при реєстрації.

Наступний крок – генерування ще однієї пари ключів. За допомогою цих ключів особа може залишити анонімний або персоналізований голос під петицією. Далі здійснюється перевірка підписанта, яка може бути вибірковою, або повною. Це залежить від кількості підписантів та технічних можливостей [3].

В час, коли країна знаходиться у стані гібридної війни та терпить хакерські атаки з боку ворога, також постає питання захисту та унеможливлення таймінг-атак, необхідно ввести випадкові затримки перед публікацією голосу особи. Також, всі особи, які хочуть проголосувати, мають завчасно кешувати відкриті ключі та сертифікати, щоб почерговість процедури верифікації не можна було встановити по часу звернення до сертифікованого серверу.

Після перевірки ЕЦП верифікацію можна вважати закінченою, та голос можна зараховувати як підпис під петицією.

Такий алгоритм не є панацеєю, в ньому присутні вразливості, які автор розгляне в наступних публікаціях та спробує розробити методи для захисту від них.

Список літератури

1. Електронна демократія // Проекти електронного самоврядування в Україні [Електронний ресурс]. – Режим доступу: http://www.kitsoft.kiev.ua/what-we-do/electronic-democracy/

2. Мінгальова Ю.І. Новітні криптографічні методи захисту інформації / Ю.І. Мингальова, О.М. Спірін // "Науково-дослідна робота молодих учених: стан, проблеми, перспективи". II Всеукр. наук.-практ. конф., присв. 95-річчю ХДУ, 12 – 16 листопада 2012 р., Херсон. – Херсон, 2012.

3. Широчин В.П. Засоби і методи біометричної аутентифікації користувачів в комп'ютерних системах / В.П. Широчин, В.Є. Мухін, А.В. Кулик // Вістник НТУУ «КПІ», Інформатика, управління і обчислювальна техніка. – 1999. – №32. – С. 3-16.

УДК 004.415.53

Програмна модель соціальної мережі та стратегій поширення інформаційно-психологічних впливів

Улічев О.С., аспірант,
Мелешко Є.В., канд. техн. наук, доцент
Центральноукраїнський національний технічний університет, м. Кропивницький

Одним з підходів, в дослідженні соціальних мереж (СМ), є моделювання. Зокрема для дослідження можуть використовуватись програмні моделі, в яких моделюють структуру частини соціальної мережі та інформаційні процеси, що протікають в часі.

Мета роботи полягає у розробці програмного забезпечення для моделювання поширення інформаційних впливів у соціальній мережі та дослідження залежності рівня інформаційно-психологічної безпеки мережі від її структури та властивостей користувачів.

Розроблена програмна модель дозволяє створювати частини мережі з наперед заданою структурою і аналізувати вплив структури на швидкість і динаміку розповсюдження інформаційного впливу.

Пропонується розглядати СМ як набір певних підграфів, і розглядати СМ с точки зору мережевого підходу [1, 2, 4] з урахуванням певних обмежень. Пропонується генерувати мережу на основі комбінацій трьох типів підграфів:

- Група (Г) - граф з таким набором зв'язків, що дозволяє встановити зв'язок між будь-якими двома вузлами графу напряму або використовуючи проміжні вузли. В літературі таку підмножину часто називають – «цілісна мережа» [5].
- Кліка (К) – граф в якому кожен вузол зв'язаний з кожним.
- Лідерська група (ЛГ) – підвид групи з одним або кількома вираженими вузлами, що мають зв'язки з усіма іншими вузлами групи.

Варіативність генерування структури СМ можна досягати за рахунок домішування (або у випадку «К» - вилучення) певної міри випадкових зв'язків. «Пом'якшений» варіант кліки називають К-плекс (поняття введено авторами [3]) – в такій підмножині не всі, але переважна більшість вузлів зв'язані між собою. Такий варіант є ближчим до реальності.

Основним класом моделі є «Користувач» (вузол соціальної мережі). Нижче наведено діаграму класів моделі.

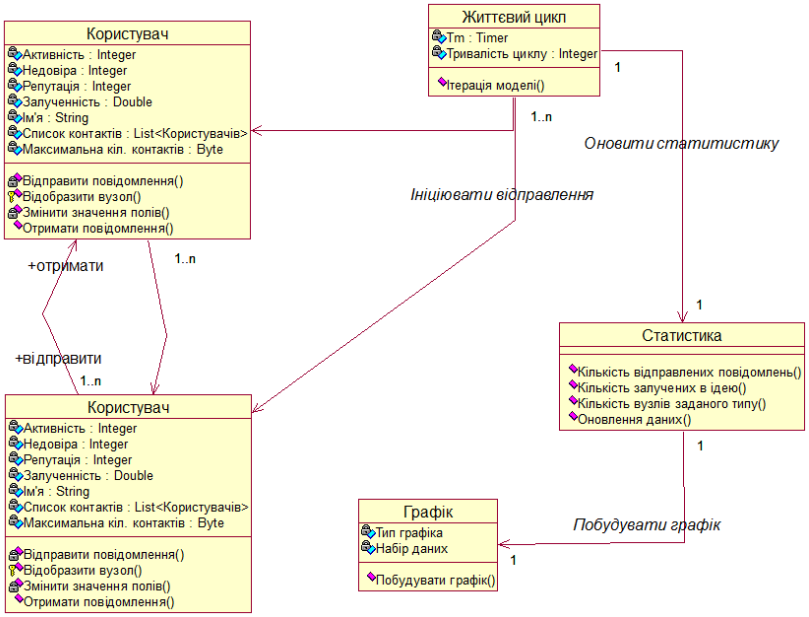


Рисунок 1 - Діаграма основних класів моделі

При аналізі розповсюдження інформаційного впливу пропонується розглядати співвідношення показників: «репутація» атакуючого вузла і «інформаційний спротив» атакованого та адитивний принцип накопичення рівня довіри до ідеї.

Мета введення цих параметрів - наблизити модель до реальності. Адже отримуючи одну і ту ж інформацію від різних адресатів, для кінцевого одержувача вона має різну інформаційну вагу. Чим більше одержувач довіряє відправнику - тим вагомішим для нього є повідомлення. Так як рівень довіри (недовіри) в моделі вже закріплений до конкретної ідеї, то інформаційну вагу (ІВ) пропонується визначати як коефіцієнт, що отримується з відношення:

$$ІВ = Репутація/Недовіра. \quad (1)$$

«Залученість до ідеї» це деяка накопичувальна характеристика - функція від кількості однорідних інформаційних повідомлень, що надійшли до користувача від інших вузлів мережі.

Серед множини вузлів мережі варто виділити генераторів – вузли, що активно пропагують певну ідею (інформаційний посил α). Генератор характеризується абсолютною (непохитною) вірою в ідею α (максимальний рівень залученості), високим рівнем впливу та активності.

Так як в даному дослідженні не розглядається вплив генераторів контр

ідеї, то функція, що визначає рівень «залученості» буде монотонно неспадаючою, а максимальне значення – це рівень генератора ідеї, вузол сам стає генератором і починає розповсюджувати ідею по мережі.

З урахуванням вище сказаного, поведінкова стратегія генератора може бути представлена як:

$$\langle F(P_1 P_2 \dots P_i) | U_g \rangle, \quad (2)$$

де $F(P_1 P_2 \dots P_i)$ – функція, що визначає поведінкову стратегію;

U_g – множина доступних генератору вузлів, тобто – підмножина вузлів всієї мережі, що входить до кола спілкування генератора;

$P_1 P_2 \dots P_i$ – набір поведінкових критеріїв.

Функція $F(P_n)$ може залежати від одного, двох і більше критеріїв.

Поведінка вузла залежить від багатьох чинників:

–мета, що переслідується;

–положення вузла в мережі;

–локальна структура мережі в околі вузла;

–наявність чи відсутність інформаційних соратників \ супротивників та інш.

Розглянемо варіанти поведінок, що базуються лише на виборі вузлів - цілей атаки з свого околу.

В найпростішому випадку вузол (генератор ідеї) веде діалог з випадково обраними вузлами з кола свого спілкування в мережі. При такому варіанті генератор не витрачає часу на аналіз структури чи індивідуальні особливості вузлів – цілей атаки, тому кількість діалогів (інформаційних атак) близька або рівна показнику його активності. Тоді поведінкова стратегія (умовно назвемо її «кущ») може бути описана як:

$$P_{bush} = \{u_i \in U_g | i = random(|U_g|), |u| \leq Act_g\}, \quad (3)$$

де $u_i \in U_g$ – доступні генератору користувачі;

$i = random(|U_g|)$ – випадковий вибір номера користувача для атаки;

$|u| \leq Act_g$ – кількість обраних користувачів не перевищує показника активності генератора.

Можливі і інші поведінки, коли цілі інформаційної атаки обираються не випадково, а з урахуванням певних характеристик. Найпростішою з точки зору аналізу та доступності характеристикою вузла для атаки є кількість його зв'язків (з точки зору соціальної мережі – кількість друзів, активних контактів). Логічно припустити, що вузли з великою кількістю контактів є більш перспективними для атаки і подальшого розповсюдження ідеї. У випадку вдалої атаки і переконання такого вузла канал передачі значно розширюється. Але в цьому випадку генератору необхідно затрачати певний час для аналізу – вибір вузла для атаки, відповідно кількість активних діалогів має бути зменшена по відношенню до поведінки описаної співвідношенням (2). У випадку цієї поведінкової

стратегії (назвемо її умовно «дерево»), вона може бути описана наступним чином:

$$P_{tree} = \{u_i \in U_g \big| |U_{u_i}| \to max, |u| = 2^{l\_g}, |u| \le K * Act_g, u_i \notin G\}, \quad (4)$$

де $u_i \in U_g$ – доступні генератору користувачі;

$|U_{u_i}| \to max$ – кількість вузлів, доступних атакованому вузлу, обирається за ознакою «максимальна з наявних»;

$|u| = 2^{l\_g}$ – кількість вузлів для атаки залежить від рівня генератора (l_g), починаючи від початкового генератора l_g = 0;

$|u| \le K * Act_g$– кількість обраних користувачів не перевищує показника активності генератора з деяким коефіцієнтом, певний час витрачається генератором на аналіз і пошук вузла для атаки. В подальшому моделюванні використовується коефіцієнт К=0.5, тобто половина активності генератора;

$u_i \notin G$ – атака на вузол продовжується до тих пір, поки вузол сам не стане генератором.

Висновки

В ході дослідження запропоновано розглядати формально описані поведінкові стратегії. На програмній моделі проведено експерименти з використанням різних стратегій та різних структур фрагментів мережі.

Ефективність стратегії можна підвищити використовуючи багатокритеріальні функції, багатокритеріальна функція аналізу вузлів дає можливість вибору найбільш вдалого вузла для атаки. Це особливо актуально на ранніх стадіях атаки і дає можливість скоротити час залучення до ідеї і отримання генераторів наступного рівня.

Список літератури

1. Сазанов В.М. Социальные сети как новая общественная сфера. – М.: Лаборатория СВМ, 2010. – 180 с.

2. Хоган Б. Анализ социальных сетей в интернете [Электронный ресурс]. – Режим доступа: https://postnauka.ru/longreads/20259

3. Seidman S. B., Foster B. L. A graph-theoretic generalization of the clique concept // Journal of Mathematical Sociology. – 1978. – Vol. 6. – P. 139–154.

4. Moody J., White, D. R. Structural cohesion and embeddedness // American Sociological Review. – 2003. – Vol. 68(1). – P. 103–128.

5. Connected lives: The project / Wellman, B., Hogan, B., Berg, K. [et al.] // The networked neighborhood / P. Purcell (Ed.). – 2006. – P. 161–216.

6. Батура Т.В. Модели и методы анализа компьютерных социальных сетей // Программные продукты и системы. – 2013. – № 3. – С. 130-137.

УДК 003.26

Особливості використання математичних методів в лінгвістичній стеганографії та стегоаналізі

Федотова-Півень І.М., завідувач кафедри інформаційної безпеки та комп'ютерної інженерії, к.т.н., доцент,
Тарасенко Я.В., аспірант
Черкаський державний технологічний університет, м. Черкаси

На сьогоднішній день, в умовах зростаючої загрози з боку новітніх засобів стеганографії (в тому числі і лінгвістичної), що несуть в собі небезпеку витоку секретної інформації чи незаконного обміну даними між злочинними угрупуваннями, вирішення потребує проблема автоматизації процесу стегоаналізу [1], яка невід'ємно залежить від ефективності автоматизації процесу аналізу тексту, написаного природньою мовою. Інакше кажучи, лінгвістична стеганографія та стегоаналіз потребують покращення та доопрацювання методів машинного розуміння тексту і прикладних комп'ютерних програм аналізу текстових даних.

Перш за все, процес автоматизації лінгвістичного аналізу передбачає використання математичних методів, що потребують адаптації та удосконалення при суміщенні їх із засобами лінгвістичного аналізу. Використання математичних методів при дослідженні тексту, в тому числі і для задач стегоаналізу є тією необхідною умовою, що зумовлює ефективність аналізу тексту в сукупності з класичними методами реферування та лінгвістичного дослідження. Від рівня їх взаємодії залежить результат стегоаналізу та ефективність проведення атаки на стегосистему. Гладкий А.В. в доповіді на Другій міжнародній конференції по моделі «Смисл-Текст» [2] описує можливість використання математичних методів для розвитку лінгвістики, зокрема наголошує, що в математичній лінгвістиці важливу роль відіграє теорія формальних граматик, що близька з математичною логікою і теорією алгоритмів. Автор додає, що до теорії формальних граматик належить теорія синтаксичних структур, а в результаті відповідних трансформацій можна отримати формальний опис деяких традиційних граматичних понять. Сюди автор відносить опис змісту речення за допомогою апарату інтенсіональної логіки [2]. А звідси слідує, що для лінгвістичного дослідження тексту слід користуватися семантикою Монтегю і синтаксичним обчисленням Ламбека [3], що досліджують саме виокремлення змісту з речення. Основою для такого дослідження є формальна логіка, а як відомо саме формальна логіка є інструментом граматичного аналізу [4]. Хоча описані методи відносяться до аналізу мови, їх адаптація для задач стеганографії дозволить проводити ефективний стегоаналіз та навпаки, це необхідна умова розвитку

стеганографії. Отже, використання математичних методів, як теорія множин, методи статистики, теорія імовірності і математичне моделювання не лише можливе в рамках лінгвістичного стегоаналізу, а й необхідна умова для досягнення ефективної протидії методам стеганографії, а апарат інтенсіональної логіки є тією основною особливістю, що зумовлює гармонійне поєднання математичних та лінгвістичних методів в лінгвістичній стаганографії та стегоаналізі.

Список літератури

1. Тарасенко Я. В. Перспективи розвитку автоматизованих програмних засобів та систем текстового стегоаналізу / Я.В. Тарасенко // Матеріали Міжнародної науково-практичної конференції [«Наука у контексті сучасних глобалізаційних процесів»], (19 листопада 2017 р.). – Одеса: Друкарня "Друкарик". – 2017. – С. 75-77.

2. Гладкий А.В. Размышления о взаимодействии лингвистики и математики / А.В. Гладкий // 2-я Международная конференция по модели «Смысл<=>Текст», (22-26 июня 2005 г.). – М.. – 2005 [Электронный ресурс]. – Режим доступу: http://elementy.ru/nauchno-populyarnaya_biblioteka/164549

3. Пентус М. Р. Семантика Монтегю и синтаксическое исчисление Ламбека [Електронний ресурс] – Режим доступу: http://lpcs.math.msu.su/~pentus/ftp/otipl/montak04.pdf

4. Андреев А. В. Формальная логика как инструмент грамматического анализа // Varietas delectans : Сборник статей к 70-летию Николая Леонидовича Сухачева. – СПб.: Нестор-История. – 2012. – С. 34–47.

УДК 004.056

Юридичні аспекти забезпечення безпеки в кіберпросторі

Хлапонін Д.Ю., провідний юрисконсульт
Київський міський центр зайнятості, м. Київ

Розвиток інформаційних послуг вимагає рішення завдань ефективного управління інформаційними ресурсами з одночасним розширенням функціональності інформаційно-телекомунікаційних систем (ІТС).

Одночасно з розвитком технологій постає питання безпеки в інформаційно-телекомунікаційних мережах. З точки зору забезпечення безпеки найбільш важливими властивостями мереж є: конфіденційність (використання інфраструктури або її частини); цілісність (інфраструктури); доступність (служб та сервісів); спостереженість (за використанням інфраструктури або її частини); прихованість (використання та управління інфраструктурою) [1].

Захист інформації це діяльність, яка спрямована на забезпечення безпеки оброблюваної в ІТС інформації та ІТС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз. Основним завданням захисту інформації є протидія порушенню таких властивостей як: конфіденційність **інформації**; цілісність **інформації**; доступність використання ІТС та оброблюваної **інформації**; спостережність **за діями користувачів** та керованість ІТС.

На даний час, відповідно до Закону [3] визначені основні поняття. Кіберпростір – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Закон [3] набуває чинності чинності через шість місяців з дня його опублікування.

Кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем. Кіберзахист – це діяльність, яка спрямована на забезпечення безпеки кіберінфраструктури. Кіберінфраструктура може характеризуватися рядом властивостей. З точки зору забезпечення безпеки найбільш важливими властивостями кіберінфраструктури є: конфіденційність **(використання інфраструктури або її частини);** цілісність **(інфраструктури);** доступність **(служб та сервісів);** спостереженість **(за використанням**

кіберінфраструктури або її частини); прихованість **(використання та управління кіберінфраструктурою).**

Якщо для захисту інформації найбільш важливими заходами є запобігання загрозам конфіденційності та цілісності, то в кіберпросторі основні зусилля повинні бути направлені на запобігання загрозам доступності служб (в кіберпросторі атаки з метою порушення доступності реалізуються простіше) та спостереженість за використанням інфраструктури (або її частини).

При побудові системи захисту інформації властивість "доступність" розглядається насамперед як доступність самої **інформації**, а доступність використання визначеної АС – в контексті захисту конкретної **інформації**. Наприклад, в АС класу 1 ненавмисне або навмисне форматування жорсткого диску призводить до того, що всі дані, які зберігаються на носієві інформації стають недоступними, хоча фізично з носія не видаляються. В кіберпросторі, насамперед в великих розподілених системах, рідко застосовується безпосередній доступ до жорсткого диску віддаленого комп'ютера. Доступ до інформації відбувається шляхом формування та обробки запитів до відповідних служб, які функціонують на різних серверах в цьому кіберпросторі. В питанні запобігання загрозам спостереженості в кіберпросторі, серед визначених задач, найбільш відповідальною та складною є задача взаємної аутентифікації і авторизації користувачів або окремих елементів кіберінфраструктури, до яких визначений користувач намагається отримати доступ.

Таким чином, безпека в кіберпросторі має істотні відмінності від забезпечення безпеки конкретної інформації в будь-якій визначеній системі. На сьогоднішній день, враховуючи необхідність взаємодії та функціональної сумісності окремих структур, задіяних в зоні проведення антитерористичної операції з зовнішніми користувачами (до яких в першу чергу будуть відноситися силові структури), можуть порушуватися окремі лінії зв'язку, можлива втрата боєздатності окремими елементами управління військами, порушення керованості озброєнням та військовою технікою та ін.

Література

1. Хлапонін Ю.І. Загальні характеристики загроз в кіберпросторі / Ю.І. Хлапонін, В.В. Овсянніков, Н.А. Паламарчук – Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення: VI наук.- практ. сем. Військового інституту телекомунікацій та інформатизації НТУУ "КПІ", 20 жовтня 2011 р.: тези доп. – К., 2011. – С. 157.

2. Кіберполіція [Електронний ресурс] – Режим доступу: http://cybercop.in.ua/index.php/naukovi-statti/80-naukovi-statti/176-ponyattya-kiberprostoru-ta-kiberzlochiniv

3. Закон України "Про основні засади забезпечення кібербезпеки України" // Відомості Верховної Ради (ВВР). – № 45. – 2017. – С. 403.

УДК 004.056.53

Формалізація моделі визначення та керування ризиками для інтеграції в автоматизовану систему аудиту інформаційної безпеки

Хох В.Д., аспірант, Сидоренко В.В., ст. викладач
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Центральноукраїнський національний технічний університет, м. Кропивницький

Для ефективного менеджменту ризиків інформаційної безпеки необхідно не лише якісно оцінювати зовнішні та внутрішні контексти, в яких організація досягає своїх цілей, а й адекватно аналізувати інциденти у разі їх виникнення.

Метою даної роботи є формалізація математичної моделі визначення та керування ризиками для інтеграції в автоматизовану систему аудиту інформаційної безпеки основану на продукційній експертній системі.

Важливим показником, який необхідно враховувати під час аналізу інциденту, є його етіологія. У міжнародному стандарті ISO/IEC:27005 походження загроз поділяють на зловмисні, випадкові та екологічні. Кожна з загроз може бути причиною виникнення інциденту, який у свою чергу буде наслідком реалізації певної вразливості. Існують типи загроз з комбінованим походженням, напр., загрози, що призводять до фізичних ушкоджень активів, мають одночасно і зловмисне, і випадкове, і екологічне походження. Відтак, існує ймовірність визначити причину виникнення інциденту некоректно та залишити ризик неопрацьованим.

Якщо припустити, що з самого початку організація вразлива до усіх проявів загроз одночасно, але в певній мірі, напр., загроза – t_i прямує до 0, до того ж, зважаючи на розподіл проявів загроз у стандарті на дві групи – зовнішні і внутрішні, можливо сформувати множину загроз T організації, кожен з елементів якої належить одній з двох підмножин T_{ext} та T_{int}, тоді вразливість можна задати формулою:

$$\mathrm{T} = \{t_1, t_2, t_3, \ldots, t_n\} = T_{ext} \cup T_{int}. \quad (1)$$

Паралельно із тим формується множина можливих вразливостей організації V. Множина V складається з елементів, що були виявлені експертами:

$$V = \{v_1, v_2, v_3, \ldots, v_m\}. \quad (2)$$

Множина вразливостей інформаційної безпеки організації формується на основі множини загроз:

$$t_1 \wedge t_2 \wedge t_3 \wedge t_4 \ldots t_n \rightarrow v_1, v_2 \ldots v_n,\ v_x \in V,\ t_x \in T_{ext} \vee T_{int},\ T_{int} \cap T_{ext}, \quad (3)$$

виходячи з цього:

$$v_n \rightarrow e_n \text{ або } V = \{v_x | v_x \rightarrow e_n\} \rightarrow E = \{e_n | V \rightarrow e_n\}. \quad (4)$$

Кожному елементу множини V ставиться у відповідність певна формула. В розроблюваній математичній моделі вводиться параметр, значення якого відображає рівень можливого зловмисного провокування інцидентів в організації, його розрахунок базується на тому що:

$$t_i = \{t_x | T_{ext} \vee T_{int}\} \exists F = \{N, M, E\}, \quad (5)$$

де F – множина факторів середовища, в якій функціонує організація;

N – фактори, які вважаються незловмисними;

M – фактори, що вважаються зловмисними, тобто такими, що виникають внаслідок навмисних дій;

E – фактори, що вважаються такими, що породжуються природними факторами.

Згідно моделі можна сказати, що множини, які містять фактори різного типу, можуть перетинатися, тобто $N \cap M \cap E$, тоді $F = \{f_i | N \oplus M \oplus E\}$.

Після формування множини F необхідно побудувати нечітку множину $\tilde{A}$ рівня m, де $m \in [0; 1]$:

$$\tilde{A}_m = \{x \in F | \mu_{\tilde{A}} > z\} \quad (6)$$

Тоді функція $\mu_{\tilde{A}}(x)$ – ступінь належності x до множини $\tilde{A}$, де z – допустимий рівень припущення, щодо належності елементу x до множини M.

Таким чином, можливо формувати перелік факторів необхідних для оцінки ризику, враховуючи не лише ті, що однозначно визначені як зловмисні. Якщо значення z базується на статистичних даних і може використовуватись в організації для корегування списку факторів, що необхідно врахувати при майбутній переоцінці ризику, а значення $|\tilde{A}|$ можна використовувати як індикатор для визначення необхідності переоцінки ризику.

Список літератури

1. Information technology — Security techniques – Information security risk Magement : ISO/IEC 27005: 2008.

2. Shapiro A.F. Risk Assessment Applications of Fuzzy Logic / A.F. Shapiro, M. Koissi. – Ottawa: Casualty Actuarial Society, 2015. – 89 с.

3. Козлов А. Промышленные стандарты беспроводной передачи данных // Chip News Украина. – 2008. – №7. – С. 18-21.

4. Корченко А. Г. Построение систем защиты информации на нечётких множествах / А. Г. Корченко. – Київ: МК-Пресс, 2006. – 320 с.

УДК 004.056.53

Система контролю та управління доступом з використанням двохфакторної автентифікації на основі платформи Arduino

Хутченко І. В., студент
Науковий керівник – Куперштейн Л. М., к.т.н., доцент
Вінницький національний технічний університет, м. Вінниця

Забезпечення безпеки, запобігання витоку інформації і контроль ефективності роботи персоналу є одними з найбільш важливих і значних проблем на багатьох підприємствах. Традиційні методи персональної ідентифікації, засновані на застосуванні паролів або матеріальних носіїв, таких як перепустка, паспорт, бейджі, не завжди відповідають сучасним вимогам безпеки [1]. Широкого застосування набувають біометричні технології, перевагою яких є найвища надійність. І дійсно, відомо, що двох людей з однаковими відбитками пальців у природі просто не існує [2].

Існуючі системи контролю та управління доступом (СКУД) на ринку України не вирішують проблему комплексної автентифікації, тому рішенням цієї проблеми може бути розробка системи, яка об'єднує застосування радіочастотної та біометричної автентифікації, а також поєднує функції охоронної сигналізації.

Під час проведення аналізу існуючих СКУД на ринку України, було виділено 3 найбільш популярних з різними параметрами та ціновою категорією: Tecsar Trek, Fr-02, CnM Secure Gate. В таблиці 1 наведено порівняльну характеристику, відповідно технічним характеристикам вказаних виробником [3, 4, 5].

Таблиця 1 - Порівняльна характеристика існуючих СКУД

Параметр порівняння	Tecsar Trek	Fr-02	CnM Secure Gate
Частота зчитування RFID-карт, кГц	125		
Кількість RFID-карт в пам'яті, шт	6	1364	1364
Запірна сила електромагнітного замка, кг	180	200	200
Живлення, В	12	12	100-240
Кнопка виходу	+		
ПЗ обліку робочого часу	-	+	+
Додаткові можливості	Підсвітка клавіатури	Ведення БД, індикація	Індикація, внутрішня пам'ять, фотозйомка
Вартість, грн	3180	9880	10660

Проаналізувавши найпопулярніші на ринку системи контролю доступу, можна зробити висновок, що вони не гарантують достатньо

високого рівня захисту, адже RFID-карти можна підробити чи клонувати. Розроблена СКУД враховує ці вразливості та передбачає додаткові методи автентифікації, охоронну систему, що реагує на рух, а також система оповіщення, для надійного захисту від спроб несанкціонованого проникнення в приміщення.

Система контролю та управління доступом побудована так, щоб працівники могли пройти автентифікацію найефективнішим способом, для зменшення витрат робочого часу. Однак, процес автентифікації необхідно оптимізований так, щоб він не був обтяжливим великою кількістю та об'ємом речей для цього, не займає занадто багато часу, однак він також унеможливлює несанкціонований доступ до приміщення.

Для виконання поставлених задач був обраний мікроконтролер фірми Atmel ATmega 328P на базі платформи Arduino UNO R3. Вибір даного мікроконтролера обумовлений технічною відповідністю поставленому завданню: забезпечується необхідна кількість входів, простота використання та програмування.

Структурна схема засобу контролю та управління доступом. Відповідно рисунку 1, на структурній схемі пунктиром позначені елементи, що кріпляться з внутрішньої сторони стіни. Усі кабелі зібрані в короб, усі елементи занесені у щит електричний, що закривається ключем.

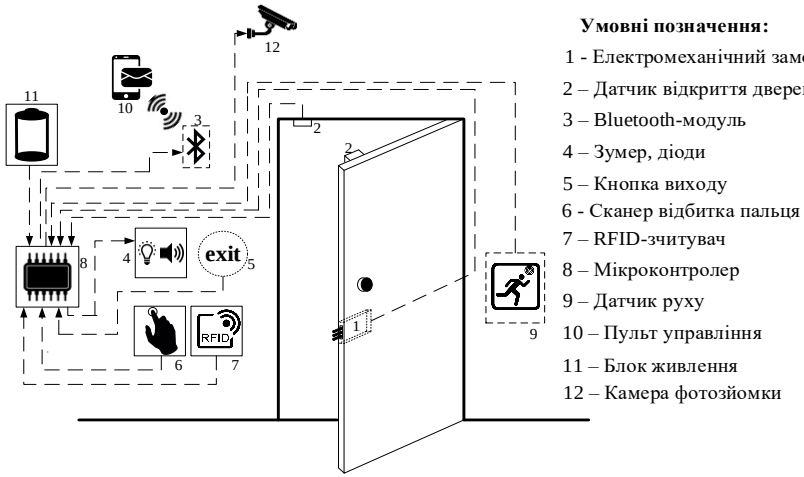


Рисунок 1 – Структурна схема системи контролю та управління доступом

В розробленій системі контролю та управління доступом реалізовано різні режими роботи: режим штатного функціонування (при якому користувач проходить ідентифікацію спочатку за допомогою RFID-карти (7), а потім – сканера відбитка пальця (6)), режим охорони (цей режим активується охоронцем після закінчення робочого дня, при якому вмикатиметься датчик руху (9) і камера фотозйомки (12)) та режим додавання нових користувачів в пам'ять системи (6).

Активувати дані режими роботи можна за допомогою дистанційного пульта управління (10), функції якого виконує мобільний телефон із встановленим, будь яким, додатком Bluetooth-терміналу. Обмін даними між пультом управління та контролером СКУД здійснюється за допомогою Bluetooth-модуля (3).

Усі дії користувача супроводжуються звуковою та світловою індикацією, за допомогою зумера та світлодіодів (4). Запірним елементом в розробленому засобі слугує електромеханічний засув (1), управління яким здійснюється за допомогою сервоприводу. Контроль за станом відкриття дверей проводиться за допомогою датчика відкриття дверей (2). Кнопкою виходу (5) слугує для безперешкодного виходу з приміщення, яка розміщена на внутрішній стіні поблизу дверей.

Після ініціалізації вхідних даних, система працює у режимі «Користувач»: активується зчитувач карток. Отриманий номер картки ідентифікується, якщо це картка охоронця, то далі система очікує на код, відправлений на Bluetooth-приймач, за допомогою додатку, який встановлений на мобільний пристрій. Якщо отриманий код дорівнює «2» – система переходить в режим «Додавання нових користувачів», а якщо код дорівнює «3» – встановлюється режим «Охорона».

При більше трьох невдалих спробах ідентифікації карти активується режим «Тривога», який супроводжується звуковою та світловою сигналізацією, вимкнути який можна відправивши код «1».

У випадку, коли це карта користувача, а не охоронця, система, після успішної автентифікації карти користувача, активує сканер відбитка пальця. Після успішної біометричної автентифікації, двері розблоковуються, що супроводжується загорянням зеленого світлодіоду та звуковою сигналізацією. Індикація продовжується до того часу, доки двері залишатимуться відкритими. Контроль за станом відкриття дверей здійснюється за допомогою геркону. Після того як двері будуть зачинені, система автоматично закриває їх на замок та переходить до сканування карти наступного користувача.

В режимі «Охорона» активується ультразвуковий датчик відстані HC-SR04, що виконує функцію датчика руху. При потраплянні людини чи предмету в поле зору датчика відстань стає відмінною від еталонної (відстань до протилежної стіни), тому надсилається сигнал тривоги і камера робить 10 фотознімків з інтервалом в 1 секунду. Використання даного типу датчика дало змогу зменшити загальну вартість засобу.

Висновки. Під час проведення тестування розробленого засобу контролю та управління доступом виявилось, що існує ряд недоліків:

- різні мобільні додатки Bluetooth-терміналу не відображають вихідні повідомлення з монітора послідовного порту плати Arduino UNO. Для зручності і зрозумілості роботи необхідно розробити власний додаток для виведення повідомлень або ж додати до засобу LED-екран, хоча це не є технічно можливим через брак вільних портів на платі;

- електромеханічний засув не є надійним запірним засобом. Для вирішення цієї проблеми, краще використати електромеханічний засув, але для його функціонування також потрібне окреме джерело живлення або реле напруги, що значно підвищить кінцеву вартість створеного засобу.

- камера для фотозйомки має малу роздільну здатність, тому краще використовувати відеозйомку із високою роздільною здатністю, але для вирішення цієї проблеми потрібно додатково підключити flash-накопичувач для буферизації відеопотоку.

Вирішення даних проблем, виявлених під час проведення тестування створеної системи контролю та управління доступом з використанням двохфакторної автентифікації на основі платформи Arduino, планується вирішити в процесі подальшої модернізації системи.

Список літератури

1. Волковицкий В.Д. Системы контроля и управления доступом. / В.Д.Волковицкий, В.В. Волхонский – М.: Экополис и культура, 2007. – 66 с.

2. Идентификация по отпечаткам пальцев. Часть 1 [Електронний ресурс]: Прогноз финансовых рисков 2000 – 2009. / В. Задорожный // PC Magazine / Russian Edition №2, 2004. – Режим доступу: http://www.bre.ru/security/20994.html

3. Автономный комплект Tecsar Trek SA-TS22/Flash EM [Електронний ресурс]. – Режим доступу: https://secur.ua/kk/komplekty-skud/avtonomnyj-komplekt-sa-ts22-flash-em.html

4. Комплект СКУД для офиса с учетом рабочего времени, для одной двери Fr-02 [Електронний ресурс]. – Режим доступу: https://secur.ua/kk/komplekty-skud/avtonomnyj-komplekt-sa-ts22-flash-em.html

5. СКУД CnM Secure Gate [Електронний ресурс]. – Режим доступу: https://secur.ua/kk/komplekty-skud/komplekt-setevogo-skud-cnm-secur-gate-4-dveri-schityvatel-knopka.html

УДК 004.056:005.7

Дослідження особистості сучасного менеджера у сфері інформаційної безпеки

Шаумян О.Г., канд. психол. наук, доцент кафедри психології та педагогіки
Кропивницький інститут Приватного вищого навчального закладу «Університету сучасних знань», м. Кропивницький

Розвиток цивілізації, науково-технічний прогрес приводять сучасного менеджера до потреби у розвитку заходів щодо інформаційної безпеки. У професійній діяльності передусім, це пов'язано з усвідомленням внеску в діяльність як потрібної і корисної для суспільства в цілому. Сучасний менеджер має приділяти увагу ризикам інформаційного суспільства. Можна виокремити домінуючі інформаційні ризики, як заміщення духовної культури вузькоспеціалізованими знаннями, витіснення реального спілкування, зміна характеру людського спілкування від людського до формалізованого мислення, деформація дозвілля, орієнтація на розваги.

Так, швидкість суспільства завжди є вищою за швидкість розвитку окремої особистості, особистість змушена постійно бути в курсі подій і внутрішньо готова до прийняття цих змін. Ця готовність проявляється у часі, котрий пов'язаний із сприйняттям та засвоєнням нової інформації, прийняттям нових установок, зміною власних моделей поведінки, використанням нових ролей [3].

Важливу роль у розвитку наукової думки з окресленої проблеми відіграли дослідження американських антропологів А. Крьобера і К. Клакхона, які вважали, що «культура складається із внутрішніх цінностей і норм, що виявляються зовні... за допомогою символів; вона виникає в результаті діяльності людей, включаючи її втілення в матеріальних засобах. Сутнісне ядро культури становлять традиційні (історично сформовані) ідеї, насамперед ті, яким приписується особлива цінність. Культурні системи можуть розглядатися, з одного боку, як результати діяльності людей, а з іншого, – як її регулятори». У даному визначенні культура є наслідком діяльності людей; стереотипи поведінки та їхні особливості посідають істотне місце в дослідженні культур [2; 6].

Розгальмуваня (дезінгібіція) як термін Інтернет-користувачів позначається субкультурним виразом (флейм) може призводити до послаблення стримуючої дії соціальних норм, соціальних санкцій і заборон.

Крім того, ефект дезінгібіції є не єдиним фактором, що визначає, наскільки людина розкривається чи реагує у кіберпросторі. Сила латентних почуттів, потреб, цінностей, мотивів має значний вплив на людей. Особистості можуть відрізнятися за силою захисних механізмів психіки та схильністю до інгібіції чи експресії. Ефект онлайн-дезінгібіції взаємодіє з цими особистісними змінними, у деяких випадках

проявляються у незначних відхиленнях від базового поведінкового патерну (офлайнового), а у деяких – спричиняють значні, драматичні зміни [3].

Менеджери в організації визначають напрям її діяльності і безпосередньо несуть відповідальність за досягнення поставлених перед нею задач шляхом ефективного використання ресурсів. Рушійні сили і поведінка менеджера сприяють вирішенню ним завдань та проблем у діяльності організації. Без врахування особистості керівника у процесі життєдіяльності організації неможливо досягти поставлених цілей.

Залежно від ситуації та обстановки, що складається, від роботи механізму цілепокладання свідомості формується образ потреби. Зовнішній образ потреби пов'язаний з абстрагуванням, зі стратегічними цілями керівника, внутрішній — з конкретним періодом життя, із щоденною тактикою.

З точки зору Дж. Міда, розвиток ідентичності відбувається від неусвідомленої ідентичності до усвідомленої. Аспекти «I» та «Me» позначають співіснування принципів соціальності та індивідуальності. Тобто, з одного боку, суспільство визначає ідентичність людини, задаючи норми та закони її існування, а з іншого боку, індивід створює власне оточення в процесі вибору, мети, цінностей, потреб. Разом з тим є автори, які доповнюють особистісну та соціальну ідентичності такою підструктурою, як ціннісна ідентичність. Ціннісна ідентичність відображає індивідуальні цінності такими, які вони є, і такими, якими б індивіду їх хотілось бачити. Так, англійським соціолог К. Камільєрі уточнює, що ці два виміри більшою мірою співпадають, але завжди мають дискретний характер. Відповідно, індивід згідно з його підходом, саме взаємодія цих процесів формує як особистісну, так і соціальну ідентичності.

Англійський психолог Г. Теджфел вважав, що особистісна та рольова ідентичності є двома полюсами ставлення особистості до себе як до представника суспільства. На одному полюсі – поведінка особистості, що повністю визначається особистісними самоідентифікаціями, а на другому – поведінка, яка повністю обумовлена впливом середовища і визначається специфікою функціонування рольової самоідентифікації. Виходячи із вищевикладеного, в основі самоідентифікації як психологічного механізму формування ідентичності відбувається:

а) відбір нових особистісних та соціальних цінностей у структурі ідентичності;

б) переструктурування ідентичності відповідно до особливостей нових елементів, що увійшли до її структури;

в) визначення індивідом значення та цінності нових елементів ідентичності та співставлення їх із попередніми соціальними цінностями, що також входять до структури ідентичності.

Крім того, воля суб'єкта як складова ідентичності особистості є

здатністю підтверджувати соціальне самовизначення в діяльності, у спілкуванні, забезпечувати постановку цілей, формулювання завдань, визначення норм. Воля керівника визначає, як він діє — використовує старі норми чи модернізує їх, зберігаючи намічені цілі. Воля є відносною щодо соціальної норми, принципу, цілі, які були прийняті людиною в процесі соціалізації. Розвиток волі пов'язаний із соціалізацією використовуваних способів мислення, з розвитком рефлексивно-критичних здібностей, зі свідомістю і самосвідомістю суб'єкта.

Для використання внутрішнього потенціалу менеджерові необхідно:

- створити відповідні умови у внутрішньому і зовнішньому середовищах, активізуючи об'єктивні закони організації праці менеджера як біосоціальної та духовної системи, що дає можливість використовувати механізми дії законів управління для розвитку;

- здійснювати цілеспрямовану самоуправлінську діяльність з використанням відповідних методів самоуправління, технологій, впливаючи на інформаційні та енергетичні потоки, що циркулюють в організмі й забезпечують гармонізацію життєдіяльності та «пробудження» психофізіологічних резервів;

- плануючи реалізацію стратегічних життєвих цілей, враховувати наявність генетичної, настановної і свідомої програми життя;

- здійснювати стратегічну, повсякденну організацію діяльності менеджера;

- виявити професійну, особисту і духовну складові, визначити їх відповідності обраному шляхові і розвитку [1; 4].

Так, у ролі регуляторів культури поведінки людини виступають норми моралі, права, а також зразки поведінки. Норма характеризує не лише вже досягнуте суспільством, а й те, що має статус загальної вимоги. Взірець (вище, найкраще) – це те, що досягнуто передовими людьми суспільства, найбільш наближене до ідеалу. З розвитком людства певні зразки поступово перетворюються на загальну норму поведінки, згодом їм на зміну приходять нові, досконаліші [7].

Важливим є звернення до сутнісного підходу, в основі якого розгляд особистості як певної цілісності. Сутнісний підхід задекларував радянський психолог С. Рубінштейн (1889-1960) у своєму відомому постулаті цілісності особистості: «У психічному складі особистості виділяються різні сфери або області рис, що характеризують різні сторони особистості; однак, попри всю свою різноманітність, відмінність і суперечливість, основні властивості особистості взаємодіють одна з одною в конкретній діяльності людини і, взаємопроникаючи одна в одну, сходяться все ж у реальній єдності особистості. Тому однаково неправильні як та точка зору, для якої єдність особистості виявляється в аморфній цілісності, що перетворює її психічний склад на безформну туманність, так і інша, протилежна до неї, яка бачить в особистості лише окремі риси». Сьогодні цілісність трактують як стійку систему

самосвідомості, волі, характеру, що реалізуються у соціальному способі життя, суспільних відносинах і певним чином впливають на них. Стрижнем цілісності особистості є світогляд як система поглядів на об'єктивний світ і місце людини в ньому, ставлення людини до себе та навколишньої дійсності [7].

О. Скібіцький вважає, що самозміна є частиною життєвого плану (програми). Вона може перетворитися на саморозвиток за умови примусового переходу з одного типу діяльності та рівня здібностей до інших. Саморозвиток і самозміна в планах особистого самовизначення створюють феномен вільної людини. Від неї залежать якісні та кількісні характеристики саморозвитку, що передбачає розвиток діяльності, організму, здібностей, особистості та мислення.

У повсякденній життєдіяльності це часто призводить до таких наслідків:

- сформована ситуація може бути сприйнята як проблема, хоча вона не є такою. У результаті витрачаються життєві сили, час на боротьбу з вигаданими «велетнями»;

- у людей на більшість типових життєвих ситуацій у підсвідомості сформовано підпрограми дій, установки. Це призводить до автоматичної реакції організму при потраплянні у відповідну (вашій моделі світу) ситуацію;

- результатом вищезгаданого є неадекватність реагування на процес розвитку подальших подій [4].

Отже, у сучасному світі дослідження інформаційної безпеки є перспективним напрямом діяльності психолога.

Список літератури

1. Колпаков В.М. Організація праці менеджера: [навч. посібник для студ. вищ. навч. закладів] / В.М. Колпаков. – К.: ДП Вид. дім «Персонал», 2008. – 432 с.

2. Культурология: дайджест / (Теория и история культуры). - [редкол.: И.Л. Галинская (гл. ред.) и др.]. - М.: РАН ИНИОН, 2001. - 215 с.

3. Немеш О.М. Практична психологія віртуальної реальності: монографія / О.М. Немеш. – К.: Видавничий Дім «Слово», 2015. – 320 с.

4. Скібіцька Л.І. Тайм – менеджмент: [навч. посібник для студ. екон. вузів] / Л.І. Скібіцька. – К.: Кондор, 2009. – 528 с.

4. Соціологічна енциклопедія / уклад. В.Г. Городяненко. – К.: Академвидав, 2008. – 456 с.

6. Parasuraman A., Zeithaml V.A., Berry L.L. A conceptual model of service quality and some implications for future research // Journal of marketing. - 1985. - № 49. – P. 41 – 50.

7. Турен А. Возвращение человека действующего: очерк социологии / Ален Турен; [пер. с фр. Е.А. Самарской; ред. пер. М.Н. Грецкий]. – М.: Научный мир, 1998. – 204 с.

УДК 004.056

Автоматизовані системи управління ризиками інформаційної безпеки

Шевченко О.О., студент 1 курсу
Науковий керівник – Хох В.Д., аспірант
Центральноукраїнський національний технічний університет, м. Кропивницький

Сучасний світ характеризується великою кількістю інформаційних загроз, які можуть нести загрозу як звичайним людям, так і підприємствам та навіть державі. Саме тому використання систем управління ризиками інформаційної безпеки є обов'язковим, адже це дозволяє не тільки вирахувати потенційні ризики, а й захиститися від них.

Методи оцінки ризику поділяються на кількісні і якісні. Кожен з них має свою спеціалізацію, тому найбільш ефективними автоматизованими системами управління ризиками є ті, що використовують обидва типа методик. До них належать такі системи управління ризиками інформаційної безпеки, як CRAMM [1].

У загальному випадку можна виділити такі складові управління ризиками: моніторинг та оцінювання організаційних ризиків функціонування системи; моніторинг та оцінювання ризиків технічних засобів; прийняття рішення з управління ризиками на основі наявних оцінок; проведення безпосередньої роботи з управління ризиками [2].

Умовно проблематику аналізу ризиків можна поділити на дві групи.

До першої належить розроблення наукових методів аналізу ризиків на основі відомих теорій та вимог стандартів щодо створення системи управління інформаційної безпеки (СУІБ). Друга група містить спеціалізовані програмні продукти, які, зазвичай базуються на методах першої групи, але мають більшу практичну спрямованість і краще враховують специфіку об'єкта захисту.

У галузі оцінки та управління інформаційними ризиками в ІТС на даний момент переважають інструментальні засоби їх оцінки такі, як CRAMM, Risk Watch, ГРИФ 2006, NIST, COBRA, OCTAVE [3].

AlienVault: Open Source Security Information Management (OSSIM) [4]

Open Source Security Information and Event Management (OSSIM) від компанії AlienVault має такі можливості: виявлення переваг, оцінка вразливостей, виявлення вторгнення, моніторинг дій, співвідношення подій управління інформаційною безпекою та подіями безпеки. OSSIM використовує можливості AlienVault® Open Threat Exchange® (OTX ™), даючи можливість користувачам вносити та отримувати інформацію про шкідливі хости в режимі реального часу.

До переваг можна внести те, що данний продукт постійно оновлюється та вдосконалюється та те, що він є безкоштовним.

Основним його недоліком є те, що він є основою для платного продукту розробників та, відповідно, має ряд обмежених та відсутніх функцій.

Risk Watch [5]

Наступним програмним забезпеченням є експертна система Risk Watch розроблена компанією Risk Watch. RiskWatch являє собою сімейство програмних продуктів (SecureWatch, CyberWatch, ComplianceWatch), побудованих на загальному програмному ядрі, які призначені для управління різними видами ризиків та підтримки великого різновиду стандартів.

До можливостей даної системи можна віднести: виявлення вразливостей; візуалізація (побудова різних діаграм, графіків) ризиків для більшої інформативності та зрозумілості; кількісна оцінка ризиків; автоматизований збір даних, їх аналіз та створення звітів;

Перевагами даної системи є: можливість адаптації до будь-яких галузей; кросплатформеність (веб), гнучкість для налаштувань запитань та співвідношень; детально налаштовані шаблони оцінки; аналіз (не)використовуваних дій за допомогою комбінації фільтрів.

До недоліків Risk Watch можна віднести: метод ефективний лише при проведенні аналізу ризиків на програмно-технічному рівні захисту без урахування організаційних і адміністративних чинників; дане програмне забезпечення англомовне; висока вартість ліцензії – $ 15000.

Данна система може стати основою для вітчизняних розробників, щоб створювати свої профілі, які будуть відтворювати місцеві реалії інформаційної безпеки.

ГРИФ 2006 [6]

Данне ПЗ дозволяє створювати автоматизовану систему керування ризиками. Програма складається з декількох модулів, які виконують окремі функції такі як: аналіз конфігурації системи автоматизації професійної діяльності (SAP); пошук вразливостей та перевірка систем захисту; функція аналізу програмного коду на наявність вразливостей нульового дня (java, ABAP), програмних закладок, критичних викликів та застарівших виразів; функція розподілення обов'язків між працівниками (аналіз критичних привілеїв, аналіз конфліктів повноважень, оптимізація ролей); оцінка ризиків.

Перевагами методу ГРИФ 2006 є: просте в використанні програмне рішення оцінки рівня ризиків в ІТС; можливість здійснення оцінки ризиків по різним інформаційним ресурсам; ефективність управління ризиками за допомогою вибору контрзаходів; не потребує спеціальних знань у сфері інформаційної безпеки.

До недоліків ГРИФ 2006 можна віднести: відсутність прив'язки до бізнес-процесів; відсутня можливість зрівнювання звітності на різних етапах втілення комплексу мір із забезпечення захищеності інформації.

COBRA [7]

Метод COBRA (Consultative Objective and BiFunctional Risk Analysis, developer – C & A Systems Security Ltd, Велика Британія) орієнтований на підтримку вимог стандарту ISO 17799. В комплект програмного забезпечення (ПЗ) входять модулі COBRA ISO 17799 Security Consultant, COBRA Policy Compliance Analyst и COBRA Data Protection Consultant, а також менеджер модуля COBRA, який призначений для налаштування та зміни наявної бази знань. Цей метод дозволяє виконати в автоматизованому режимі найпростіший варіант оцінювання інформаційних ризиків будь-якого підприємства. Він оцінює відносну важливість усіх загроз і вразливостей, генерує відповідні рішення та рекомендації.

Переваги методу COBRA: простота у використанні і відносно прийнятна вартість (усе залежить від бюджету, виділеного на ІБ) – $ 895 і $ 1995 за систему з модулем аналізу ризиків базового рівня.

До недоліків COBRA можна віднести: знання спеціальних електронних баз знань та процедур логічного виводу; застарілий, не дуже зручний для користувача інтерфейс; не визначається рівень ризиків, а лише базовий рівень безпеки; відсутність підтримки української та російської мов; виникають проблеми з генерацією звіту.

nCircle: IP360 [8]

IP360 від компанії nCircle має такі можливості: ідентифікація вразливостей; керування конфігурацією системи; створення сканування вразливостей та планування сканувань; співвідношення знаходження сканувань в режимі тертя.

До переваг системи можна віднести: високу масштабованість; інтуїтивно зрозумілий інтерфейс; близька інтеграція з Cisco; детальність звітів.

Недоліками є: інтерфейс (погано підходить для цільового сканування вразливостей; вразливості не організовані, а також не визначені операційною системою або програмою).

Система легко встановлюється в корпоративних мережах, забезпечує низьку вартість експлуатації та дозволяє сфокусувати обмежені ресурси системи безпеки тільки на реальні загрози, знижуючи ризик мережевої безпеки. Дана система є життєздатним вибором для великих організацій, яким доводиться стикатися з проблемою отримання контролю над власними процесами безпеки, особливо з інвестиціями в безпеку Cisco.

Висновки

Були розглянуті найбільш популярні автоматизовані системи управління ризиками інформаційної безпеки. Одні більш підходять для дрібних підприємств, другі – для середніх, а інші – для великих. Це простежується в функціоналі даних систем та в ціні за їх придбання. Загалом, кожна система має свої можливості, недоліки та переваги,

відштовхуючись від яких потрібно вибирати для себе СУІБ. Наприклад система RiskWatch підходить для будь-якої галузі, а в системі ГРИФ 2006 є модуль, який оптимізує кадрові взаємодії зі сторони ІБ.

Визначення основних недоліків, які присутні в цих засобах дає можливість для розробки та впровадження в Україні власного інструментального засобу оцінювання ризиків ІБ, оптимального за якістю та ціною і який би не суперечив міжнародним стандартам.

З проведеного аналізу можна навести такі рекомендації щодо вибору систем оцінки ризиків інформаційної безпеки: для невеликих підприємств доцільно використовувати систему Open Source Security Information and Event Management (OSSIM), для середніх – RiskWatch, а для великих – IP360.

Список літератури

1. Білоконь Д.С., Федулова І.В. Процес управління ризиками інформаційної безпеки // Наукові праці НУХТ. – 2016. – Т. 22, № 6. – С. 84-91.

2. Бучик С. С., Мельник С. В. Методика оцінювання інформаційних ризиків в автоматизованій системі // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. – Житомир: ЖВІ ДУТ, 2015. – Вип. 11. – С. 33–43.

3. Бучик С. С., Шалаєв В. О. Аналіз інструментальних методів визначення ризиків інформаційної безпеки інформаційно-телекомунікаційних систем // Наукоємні технології. – 2017. – № 3 (35). – С. 215-225.

4. AlienVault: Open Source Security Information Management (OSSIM) [Електронний ресурс]. – Режим доступу: https://www.alienvault.com/

5. Risk Watch [Електронний ресурс]. – Режим доступу: https://www.riskwatch.com/

6. ГРИФ 2006 [Електронний ресурс]. – Режим доступу: https://dsec.ru/

7. COBRA [Електронний ресурс]. – Режим доступу: http://www.riskworld.net/

8. IP360 [Електронний ресурс]. – Режим доступу: https://searchsecurity.techtarget.com/magazineContent/nCircles-IP360-Vulnerability-Management-System-product-review

УДК 004.056.55

Забезпечення цілісності даних шляхом використання стеганографічних методів

Шеханін К.Ю., аспірант кафедри безпеки інформаційних систем і технологій,
Колгатін А.О., інженер кафедри безпеки інформаційних систем і технологій,
Кузнецов О.О., доктор технічних наук, професор кафедри безпеки інформаційних систем і технологій
Харківський національний університет імені В.Н. Каразіна, м. Харків

Інформаційні технології визначають процеси передачі і розповсюдження, зберігання та обробки інформації, а також її використання у певних цілях. Інколи, факт виконання цих процесів повинен бути прихований від сторонніх осіб. Цим і займається галузь науки цифрова стеганографія.

Окремим розділом сучасної цифрової стеганографії, що вивчає методи і засоби вбудовування та вилучення інформаційних повідомлень в різні цифрові контейнери з використанням технічних особливостей зберігання, передачі і відображення даних, є технічна стеганографія [1-5].

На даний час відомо декілька напрямків розвитку технічної стеганографії: прихована передача інформації у мережевому трафіку [1]; приховування інформації у модель під час 3D-друку [2]; методи технічної стеганографії, що базуються на структурній особливості файлових систем у носіях інформації [3-5]. У даній роботі розглянуто спосіб забезпечення цілісності даних на носії інформації шляхом використання третього напрямку технічної стеганографії, наприклад, перемішування кластерів певних покрівельних файлів (англ. Cover File) [5].

Нехай маємо набір даних, який складається із файлів F_i, цілісність яких необхідно забезпечити, та носій інформації, на якому дані файли містяться. Для забезпечення цілісності необхідно взяти геш-значення від файлів F_i, та вбудувати геш-значення у структуру файлової системи, використовуючи один з методів [3-5].

$$M = Hash(F_0|F_1|\dots|F_i|\dots|F_n) \quad (1)$$

$$FS^* = Hide(FS, F_i, M) \quad (2)$$

де: $Hash$ – геш-функція;

n – загальна кількість файлів, цілісність яких необхідно забезпечити;

FS – структура файлової системи;

$Hide$ – метод приховування даних [3-5], вхідними даними є структура файлової системи, ключова інформація та повідомлення, яке необхідно

приховати;

FS^* – змінена структура файлової системи, відповідно до [3-5].

Носій інформації, наприклад: флеш-накопичувач, компакт-диск, жорсткий диск, із структурою файлової системи FS^*, та файлами F_i, може бути передано по незахищеному каналу. Ключову інформацію, для перевірки цілісності, передавати необхідно лише захищеним каналом.

Отримувач, маючи носій інформації та ключову інформацію, може перевірити цілісність даних файлів F_i. Для цього необхідно вилучити зі структури FS^* повідомлення та порівняти його із геш-значенням від файлів F_i. Якщо значення співпадають, то отримані дані дійсні.

$$M^* = Extr(FS^*, F_i) \tag{3}$$

$$Valid(M^*, M) \tag{4}$$

де: F_i– ключова інформація для вилучення повідомлення;

FS^* – змінена структура файлової системи;

$Extr$ – відповідний метод вилучення даних [3-5], вхідними даними є структура файлової системи, ключова інформація, вихідними даними є вилучене повідомлення – M^*;

$Valid$ – функція перевірки співвідношення повідомлень, якщо M^* співпадає із M, то можна стверджувати, що файли F_i – є валідними.

Для подальшого аналізу роздивимось певний приклад. Нехай, для приховування повідомлення використовується базовий метод перемішування кластерів покрівельних файлів [5], флеш-накопичувач із файловою системою сімейства FAT та набір файлів цілісність яких необхідно забезпечити.

Сутність методу [5] полягає у тому, що приховування даних відбувається за рахунок зміни порядку кластерів даних покрівельних файлів у FAT-таблиці. Ключовою інформацією даного методу є кількість покрівельних файлів та їх порядок задання. Повідомлення, яке необхідно приховати, розбивається на стеганоблоки, розміром по $m = \log_2(p)$ біт кожен, де p – загальна кількість покрівельних файлів. Таким чином, накладається обмеження на ключову інформацію, а саме: кількість покрівельних файлів може біти лише степенем двійки – $p = 2^n$, $n \in N$. Кожен стеганоблок відповідає порядку задання певного покрівельного файлу. Безпосередньо, приховування даних відбувається за рахунок зміни порядку кластерів у FAT-таблиці, відповідно до набору стеганоблоків.

Для прикладу, якщо використовується два покрівельних файли ($p = 2$) то значення кожного блоку стеганограми може бути «0» або «1», де «0» відповідає кластеру, що належить до першого покрівельного файлу, а «1» – до другого. Нехай покрівельні файли мають назви $A.txt$ та $B.txt$ і кожен з них займає по 10 кластерів у структурі файлової системи. Припустимо, що кластери цих файлів дефрагментовані, ланцюги кластерів файлів мають такі значення:

–для файлу $A.txt$ маємо послідовність $\{3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$;

–для файлу $B.txt$ – $\{13, 14, 15, 16, 17, 18, 19, 20, 21, 22\}$.

Нехай повідомлення, яке треба приховати, дорівнює 0x47. Розбивши це повідомлення на відповідні стеганоблоки отримаємо двійковий масив $M = \{0, 1, 0, 0, 0, 1, 1, 1\}$. Отже виконавши етап перемішування кластерів у ланцюгах із відповідністю до масиву із стеганоблоків, отримаємо відповідні ланцюги кластерів:

–для файлу $A.txt$ маємо $\{3, 5, 6, 7, 11, 12, 13, 14, 15, 16\}$;

–для файлу $B.txt$ – $\{4, 8, 9, 10, 17, 18, 19, 20, 21, 22\}$;

Отже приховане повідомлення міститься у зміненій нумерації окремих кластерів покрівельних файлів $A.txt$ та $B.txt$, структуру файлової системи у спрощеному вигляді до та після приховування базовим методом наведено на рисунку 1.

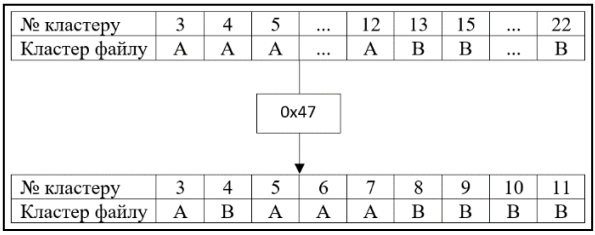


Рис. 1 – Приклад приховування повідомлення 0x47 методом [5]

Вилучення повідомлення відбувається за рахунок зчитування порядку кластерів покрівельних файлів із FAT-таблиці структури файлової системи. Вилучене повідомлення може бути більшим за розміром та не дорівнювати тому повідомленню, що вбудовувалось. Але отримувач, знаючи структуру приховуваної інформації, зможе з легкістю виділити корисну.

$$M^* = M|SI \tag{5}$$

де: SI – надлишкова інформація у ході вилучення повідомлення;

Слід відмітити переваги розглянутого методу. Перш за все це надійність приховування:

–обсяг інформації, що зберігається на носії не змінюється;

–не змінюється кількість вільних чи помилкових кластерів.

Тобто, для користувача структури файлових систем до приховування та після приховування будуть ідентичні.

Таким чином, файли, які потребують забезпечення цілісності, є покрівельними файлами, а геш-значенням від цих файлів є повідомлення, яке необхідно приховати. Значне обмеження накладає можливий розмір приховуваного повідомлення, який залежить від кількості та розмірів

покрівельних файлів, й від розміру одного кластеру у структурі файлової системи.

Для кількісної оцінки, роздивимось структуру файлової системи FAT, яка дозволяє приховати максимальну кількість байт (параметри структури залежать від виробника та від року виробництва носія інформації), тобто, розмір одного кластеру дорівнює 2048 байт, та будем змінювати кількість покрівельних файлів. Необхідні мінімальні розміри покрівельних файлів, для приховування геш-значень, у залежності від обраної геш-функції зазначені у таб. 1.

Таблиця 1 – Мінімальний розмір покрівельного файлу (байт) у залежності від кількості файлів та обраного алгоритму гешування

Кількість покрівельних файлів	2	4	8	16
MD5 (128 біт)	131072	32768	10923	4096
SHA-1 (160 біт)	163840	40960	13654	5120
SHA-2 (256 біт)	262144	65536	21846	8192
SHA-2 (512 біт)	524288	131072	43691	16384

Можна зробити висновок, що даний спосіб забезпечення цілісності інформації є доцільним для файлів відносно великого розміру. Та використання одного файлу-документа, сертифіката, не рекомендується, необхідно використовувати набір файлів. Даний напрям технічної стеганографії потребує подальших розробок та досліджень, щодо практичного використання та забезпечення функцій захисту інформації.

Список літератури

1. Пескова О.Ю., Халабурда Г.Ю. Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам интернет // Информационные системы для научных исследований (IMS-2012): Труды XV Всероссийской объединенной конференции "Интернет и современное общество" (IMS-2012). – СПб.: МПСС, 2012 – С. 348-354.

2. Кузнецов А.А., Коваленко О.Ю. Стеганографическая защита информации с использованием 3D-печати // Інформаційна безпека держави, суспільства та особистості: Збірник тез доповідей. – Кіровоград: КНТУ. – 2015. – 91-92 с.

3. Khan H., Javed M., Khayam S.A., Mirza F.. Designing a cluster-based covert channel to evade disk investigation and forensics // Computers & Security. – Vol. 30, N1, January 2011.

4. Khan H., Javed M., Mirza F. Evading Disk Investigation and Forensics using a Cluster-Based Covert Channel. National University of Science & Technology (NUST), Islamabad 44000, Pakistan.

5. Morkevičius N., Petraitis G., Venčkauskas A., Čeponis J.. Covert Channel for Cluster-based File Systems Using Multiple Cover Files // Information Technology and Control. – 2013. – Vol.42, No.3. – P. 32.

УДК 004.056.55

Криптография в облачных вычислениях

Щепилов Е.А., студент 6 курса
Научный руководитель – Гунченко Ю.А., д.т.н., профессор
Одесский национальный морской университет, г. Одесса

Облачные вычисления – одна из наиболее популярных современных технологий, связанных с развитием Интернета, который задумывался доступным и всеохватывающим, но никак не абсолютно безопасным. Распределенные приложения, подобные этим, весьма подвержены атакам. Поэтому проблемы конфиденциальности данных в облачных вычислениях, с целью недопущения раскрытия информации, хранимой в облаке и передачи ее третьим лицам, исключительно важны. Для этого данные должны быть надлежащим образом зашифрованы и включать такие криптоалгоритмы как AES, RSA, DES и 3DES. Облачная безопасность может быть обеспечена за счет целостности данных, защищенных каналов передачи данных и криптографии. В данной работе описываются криптоалгоритмы для повышения безопасности облачных вычислений.

Криптографические принципы и алгоритмы

Криптография существенно повышает уровень безопасности облачных вычислений. Это наука безопасного хранения сообщений путем преобразования исходных данных в формы, которые не могут быть прочитаны. В настоящее время все существующие криптосистемы принято разделять на два класса: симметричные и асимметричные. Соответственно, говорят о симметричной криптографии и асимметричной криптографии.

Симметричные схемы шифрования

Симметричное шифрование использует один и тот же ключ как для шифрования, так и для дешифрования. Ключ необходим как для аутентификации, так для авторизации. Симметричные алгоритмы имеют то преимущество, что не занимают слишком большой вычислительной мощности и работают с очень высокой скоростью шифрования.

Наиболее популярные алгоритмы с симметричным ключом, используемые в облаке, это Data Encryption Standard (DES), TripleDES(3DES), Advanced Encryption Standard (AES) и Blowfish. Отдельно хочется отменить алгоритм Blowfish – 64 разрядный блочный шифр с переменной (от 32 до 448 бит) длиной ключа. Он превосходит DES по скорости и стойкости. Это непатентованный, бесплатный и беспошлинный алгоритм, который используется во многих коммерческих приложениях. Безопасность симметричных криптосистем определяется двумя факторами: стойкостью самого алгоритма и длиной ключей.

Криптография с открытым ключом

В отличие от симметричной криптосистемы это совершенно другая концепция. Для шифрования и дешифрования используются разные ключи. В асимметричных криптосистемах (системах с открытым ключом) используется два ключа: открытый ключ – для шифрования и соответствующий ему секретный – для расшифрования. Наиболее известными криптографическими алгоритмами с открытым ключом являются: RSA (Rivest Shamir Adleman), алгоритм Эль-Гамаля, алгоритм Диффи-Хелмана, а также DSA (Digital Signature Algorithm).

Однако, в отличие от RSA и схемы Эль-Гамаля, DSA — алгоритм с использованием открытого ключа для создания электронной подписи, но не для шифрования. Наиболее широко распространенным на практике асимметричным алгоритмом является алгоритм RSA, который базируется на сложности (предполагаемой) задачи факторизации. Основным недостатком всех алгоритмов с открытым ключом является медленное исполнение как в аппаратной, так и программной реализациях. Симметричные алгоритмы, по крайней мере, в 1000 раз быстрее алгоритмов с открытым ключом. Поэтому на практике асимметричные криптографические алгоритмы используются для шифрования не самих сообщений, а для засекречивания и распространения сеансовых ключей.

Выводы

Облачные технологии являются тем новым трендомы о выборе которого задумываются многие организации. Однако проблемы безопасности остаются критичными для многих компаний, при принятии решения о переносе данных в облако из-за опасений, что конфиденциальные данные могут попасть третьим лицам. Однако существует множество алгоритмов шифрования данных, повышающих безопасность данных в облачных технологиях. Мы можем использовать криптографию для авторизации и идентификации в облаке, а также безопасного хранения данных.

Список литературы

1. Stinson D.R. Cryptography: Theory and Practice. New York: Chapman and Hall/CRC, 2005.

2. Vijayapriya M. Security algorithm in cloud computing: overview, International Journal of Computer Science & Engineering Technology (IJCSET), Vol.4, no. 9, pp. 1209-1211, Sep. 2013.

3. Nigoti R., Jhuria M., and Singh S., A survey of cryptographic algorithms for cloud computing, International Journal of Emerging Technologies in Computational and Applied Sciences, 4(2), pp. 141-146, March-May 2013.

4. Задирака В.К., Кудин А.М. Облачные вычисления в криптографии и стеганографии / В.К. Задирака, А.М. Кудин // Кибернетика и системный анализ. — 2013. — Т. 49, № 4. — С. 113-119

УДК 004.057.4

Використання SSL-сертифіката для захисту даних при передачі за допомогою протоколу HTTPS

Ярошенко О.С., студент 3 курсу
Науковий керівник – Кулаков Ю.О., д.т.н., професор
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

Протокол HTTPS (з англ. Hypertext Transport Protocol Secure) – це назва мережевого протоколу, що надає можливість конфіденційного обміну пакетами між користувачем і сайтом в мережі Інтернет. Безпечність з'єднання досягається за допомогою криптографічного протоколу SSL або TLS, що застосовують 3-рівневий захист:

1. Використання алгоритмів шифрування даних. Це забезпечує захист від перехоплення інформації.
2. Збереження даних. Усі зміни в переданих даних фіксуються.
3. Аутентифікація. Дозволяє захистити клієнта від перенаправлення.

SSL (з англійської Secure Socket Layer) – це протокол шифрування, що гарантує захищене підключення між сервером і клієнтом. Він складається з пари ключів, перший з яких призначений для кодування даних, а інший – для дешифрування. При цьому, обидва ключі можуть виступати як в ролі шифрувальника, так і декодера.

Для застосування протоколу SSL використовується середовище, що складається з декількох рівнів, які забезпечують безпечний обмін даними. Безпечність обміну організовується з використанням конфіденційного підключення, що є відкритим лише для цільового користувача.

Безпечний SSL розташований поміж двох протоколів: протоколу, який використовується клієнтською програмою (HTTP, IMAP, FTP, Telnet,і т.д.) і протоколом транспортного рівня TCP/IP. Під час використання створюються своєрідні бар'єри з обох сторін, що захищають та перенаправляють інформацію на транспортний рівень. Застосування багаторівневого принципу взаємодії надає змогу SSL протоколу підтримувати різні протоколи клієнтських програм.

Структура SSL протоколу розділена на два рівні. Перший – це рівень підтвердження підключення (Handshake Protocol Layer). Цей рівень містить три підпротоколи: протокол підтвердження підключення (Handshake Protocol), протокол змін налаштування шифру (Change Cipher Spec Protocol) та протокол попереджень (Alert protocol). Другий рівень – це рівень протоколу запису. На рис.1 зображена схема рівнів шарів протоколу SSL.

Рис. 1 Рівні протоколу SSL

Після встановлення безпечного підключення клієнтська програма може запитувати дані ідентифікації з сервера при кожному запиті, наприклад, коли браузер відкриває посилання на сторінку, що містить SSL. В якості відповіді сервер повідомляє клієнту копію сертифіката SSL, що міститься на хостингу Після отримання цієї інформації клієнтський браузер зобов'язаний надати підтвердження справжності та повідомити про це іншу сторону, яка відправила згоду на шифрування даних з підписом при передачі.

Після виконання цих пунктів SSL-сертифікат розпочне шифрування всієї інформації, що передається від браузера до сервера. Інформація про це може бути надана в URL адресі сайту. В такому разі до абревіатури «http» дописується буква «s» – «secure», тобто безпечно. Для того аби додатково виокремити дану інформацію, на початку рядка адреси сторінки також вміщують зображення замка, а абревіатура «https» виділяється зеленим кольором.

Є різні типи SSL-сертифікатів. Є сертифікати, що активні лише для одного домену. Таким є SSL-сертифікат з підтримкою субдоменів, і якщо мова йде про сертифікат саме такого типу, то він поширюється не тільки на основне доменне ім'я, а також і на усі його субдомени.

Висновки. Показано організацію безпечної передачі даних за допомогою протокола HTTPS з використанням сертифіката SSL. Описано рівні роботи протоколу SSL та його застосування для захисту інформації при передачі в комп'ютерних мережах.

Список літератури

1. HTTP - Hypertext Transfer Protocol [Електронний ресурс]. – Режим доступу: http://www.w3.org/Protocols

2. Олифер В.Г., Олифер Н.А., Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов – СПб: Питер, 2007.

3. Рзаєв Д.О., Шарапов О.Д., Ігнатенко В.М., та Дибкова Л.М. Інформатика та комп'ютерна техніка. Навчально-методичний посібник для самостійного вивчення дисципліни – К: КНЕУ, 2003.

UDC 004.75

The efficiency of the promotion of commercial websites

Basyuk T.M., Ph.D., Associate professor
National University "Lviv Polytechnic", Lviv

Introduction. Today, the global network of Internet is boundless source of news, a means of communication and learning, but the openness and prevalence of services makes it indispensable for the work of a plurality of trading platforms. According to Netcraft's analytical report, at the beginning of 2018, the number of employees in the global network of Internet resources exceeded 1.2 billion, in addition, all of them differ not only in terms of subject matter and objective, but also in a variety of other characteristics. As for the subject matter, the largest share belongs to commercial resources, which are created both for popularizing the company and for attracting new customers.

Overview of literature. An overview of well-known studies [1-2] shows that there are many methods and approaches that determine the effectiveness of both promoting the resource and returning invested investment. However, there is practically no research on the description of approaches towards calculating the minimum conversion rate of the required web site. Therefore, the actual task is to determine the main stages of the process of finding the minimum level of conversion of a commercial Internet resource in order to form conclusions about the effectiveness of its functioning.

Major research results. Determination of the minimum possible conversion rate is an extremely important task, since it directly shows the ability to cover the cost of rent, advertising and indicates the profitability of the project. Taking into account the above features during the research, a general algorithm for determining the level of conversion of an online resource by key queries was developed, depending on its ranking. Basic steps of the algorithm are the following:

1) The calculation of the match ratio, as the ratio of the number of users who got to the online resource from the search engine to the number of users who should enter it based on its rating.

2) Determination of the search engines ranking of the region and target audience for which commercial resource is oriented. In particular, if commercial activity is limited to the territory of Ukraine, then it is necessary to find a rating of search engines in Ukraine. According to the analytical company PROSEO, Google's share in the fourth quarter of 2017 is 75.7%.

3) Assessment of the number of requests and corresponding users who were interested in this subject area (category) for the analyzed time interval. When researching statistics in this search engine, it is expedient to use the Google

Analytics service, which allows you to assess archival data, determine the "degree of decline or growth of subject matters" and thus predict possible commercial potential. In particular, when analyzing the internet resource that is engaged in the construction of apartments, according to the key query "Purchase of an apartment" in the last month (February 2018), according to the Google Analytics service, the number of requests was 234,146.

4) Determination of the number of potential users for a given region. This metric is calculated as the product of the number of queries in the search engine on its ranking. Namely, 234146*(100/75,7)=309307 users per month. Similarly, the share of the search engine META (the second-highest in Ukraine) is found and the number of queries per month is determined. We get a share equal to 14.3%, and the number of queries is 46322, respectively.

5) Determination of the number of users who make the transition to an online resource, depending on its ranking. For this purpose, you can use a plurality of statistical resources [3]. As for the analyzed resource, it is in 8 positions in Ukraine. According to the received distribution, about 0,7% of users should pass on it. Given that, the number of users will be the following: 309,307*0,757*0,7 = 163901. Respectively, for the META search engine, this value will be equal to: 4636.

6) Comparison of the obtained values with actual transitions. This option is also worth assessing with Google Analytics, which also provides recommendations for title quality and a brief description of the online resource (annotations) that users see with search results.

Depending on the results, the analyzed resource is recognized as having a high conversion rate, and recommendations are made to increase its ranking for other key queries, or as a list of technical works on raising the conversion rate for the query is formed.

Conclusion. The research of the conversion rate showed that most commercial Internet resources are characterized by medium and above average rate. However, despite a sufficient conversion rate, there is a need to increase it, which will primarily affect the products and services that are being promoted.

References

1. Kennedy G. Seo: Marketing Strategies to Dominate the First Page (SEO, Social Media Marketing). CreateSpace Independent Publishing Platform, 122p., 2016.

2. Enge E., Spencer S., Stricchiola J., Fishkin R. Mastering Search Engine Optimization – O'Reilly Media, 994p., 2015.

3. Basyuk T. The Popularization Problem of Websites and Analysis of Competitors. Advances in Intelligent Systems and Computing II. CSIT 2017. Advances in Intelligent Systems and Computing, vol 689. Springer, Cham pp. 54-65, IEEE (DOI:10.1007/978-3-319-70581-1_4), 2018.

UDC 621.39 (043.2)

Quality of service assessment rules development for mobile operators

Odarchenko R., PhD, Associate Professor,
Gnatyuk V., PhD, Associate Professor,
Sydorenko V., PhD, Associate Professor,
Kotelianets V.
National aviation university, Kyiv, Ukraine

Building an information society in Ukraine is one of the most pressing challenges of our times. The use of the global informational network Internet is one of the priority directions of state policy in the field of information.

Therefore, based on the foregoing, it can be said that the development of the broadband Internet access infrastructure throughout the territory of Ukraine based on 4th generation high-speed networks, is a very relevant and promising task. For the average user of 4G, the main advantages of it are quite obvious: firstly, high speed of data transmission, secondly, a short response time, and thirdly, the phone will work even in the area of the cell phone suppressor.

In these circumstances, it is important always to obtain high-speed and high-quality access to network resources, regardless of location. Moreover, the operator needs to monitor continuously quality of service key parameters, which will allow to control the quality of services provided to users and data transmitted security.

One of the most important tasks when organizing mobile cellular networks remains the task of planning, optimizing and the most possibly effective use of this network resources, in which protection of data transmission should be the key point in planning of such networks and their further use.

Therefore, in order to optimize already existing and to build new 3G/4G networks, it is necessary to develop certain procedures for choosing the best criteria for quality of service indicators (in terms of security) with the introduction of new services that will allow operators to control the key parameters in more flexible and accurate ways.

It should be noted that in Ukraine there is no documentation that regulates the quality indicators of mobile 3G/4G cellular networks. Service quality control is carried out within the framework of the communications company internal audit, which is only partially controlled by public institutions. There are no specific algorithms and methods of quality control services. Thus, it is expedient to develop and create a unified database of controlled quality indicators that are important both for the users and for enterprises. It is important to introduce the certain rules on these indicators and allowable values, measurement methods, which will be common for all mobile operators, and could be used by regulatory bodies to improve the quality of communication services. In the conditions of competition in the telecommunications market, it is necessary to develop

appropriate regulatory documents.

This task is not trivial, so it will be divided into several sub-tasks. Therefore, the purpose of this work will be to develop a method for selecting and evaluating key security indicators in modern cellular networks.

To develop this method, we will use the provisions that are based on the use of key quality and performance indicators. So, first of all it is necessary to determine the difference between the KQI and the KPI. As it is shown on Figure 1, the KPI (Key Performance Indicator) is an indicator that is directly related to the quality of the network operation itself. The creation and use of these indicators is aimed directly to the network. The KQI (Key Quality Indicator) functions at the service level. CEI (Customer Experience Indicators) is responsible for the management of these indicators.

Fig.1. Quality function assessment levels of the cellular communication network

That is, as it can be seen from Fig. 1 and Table 1, the KQI are formed on the basis of KPI. KQI indicators are not always objective because they are based on the personal experience of the network users. It is advisable to determine the interdependence of these subjective indicators with the objective, for which the following method has been developed.

Conclusions. Thus, this article contains a developed evaluating method for quality of service key indicators and productivity of cellular networks, based on their security criteria. It consists in the sequential definition of the range of evaluated services, in the choice of statistics quality data for the maintenance of optimal criteria for evaluating the network operation based on correlation-regression analysis, in the direct evaluation of this data and comparison with the permissible level.

The developed method allows evaluating the most important indicators of the quality of service and cellular operator network performance with a view to optimization during implementation of new services customer service.

References

1. Order of the Cabinet of Ministers of Ukraine № 386-r since May 15, 2013. «About approving the strategy for the information society development in Ukraine» [Electronic resource]. Available at: http://zakon3.rada.gov.ua/laws/show/386-2013-%D1%80

УДК 004.413.2

Життєвий цикл розробки комп'ютерних ігор

Абашина А.А, студентка 1 курсу
Наукові керівники – Мелешко Є.В., к.т.н., доцент, Хох В.Д., аспірант
Центральноукраїнський національний технічний університет
м. Кропивницький

Ігри – це унікальна галузь індустрії програмування. Унікальність, зокрема, визначається тим, що процес розробки підданий несподіваним потрясінням, котрі багато з розробників ігор, на відміну від розробників звичайного програмного забезпечення, рахують чимось природним і нормальним. Однак, це не означає, що планування розробки ігор є безглуздим заняттям, оскільки, маючи добре продуманий технічний проект, можливо точно знати мету розробки, навіть якщо виникає гостра потреба в змінах. У таких ситуаціях знадобиться лише відкоректувати план-графік, після чого виробництво можливо відновити, звівши втрати часу до мінімуму. Розробка комп'ютерних ігор потребує великої кількості спеціалізованих програмних інструментів. В розробці сучасних комп'ютерних ігор задіяні десятки, а іноді і сотні фахівців з самих різних галузей.

Основна частина. Кожна компанія має власний метод розробки комп'ютерних ігор, однак в основному існує три стадії таких розробок. Першою стадією є пре-продакшен, другою – продакшен, третьою – пост-продакшен [1].

На стадії пре-продакшена всі ігрові ідеї обробляються, перероджуються, поки не залишається одна ігрова думка, сутність усієї гри. У більшості випадків автор ідеї пише документ, в якому описує основні концепти і ідеї. Потім даний документ подається на розгляд дизайнерам і керуючим компанією. Далі пишуть дизайн-документ, де дизайнер чи гейм-дизайнер описує ігровий світ і основні ігрові елементи. Після цього до процесу підключається відділ маркетингу, який розраховує, наскільки популярним буде даний продукт, чи буде він «конкурентоздатним» [1].

Команда програмістів і гейм-дизайнерів створює свій технологічний документ, де вона аналізує здатність і вимоги до ігрового рушія. Гейм-дизайнери створюють технічні документи, де висвітлюються задачі для різних команд: дизайнерів, звуковиків. Якщо компанія достатньо велика, то відділи самі готують подібні документи.

Після схвалення проекту на першій стадії дається дозвіл на виконання наступної стадії – стадії продакшена. На цій стадії розпочинається робота над ігровими моделями. Програмісти займаються кодом гри, левел-дизайнери – розробкою ігрових рівнів. Дизайнери все ще можуть вносити

значущі зміни в гру. На даному рівні дуже важливо, щоб здійснювалося своєчасне тестування всіх ігрових елементів.

Після завершення всіх основних робіт випускається бета-версія гри. На даному етапі критичні зміни вже не можливі, команда повинна лише удосконалювати гру, ліквідувати баги і коректувати ігровий баланс.

Після повної оптимізації гра підходить до третьої, останньої стадії пост-продакшена. На цьому етапі основну роль відіграє відділ маркетингу, який розробляє компанію щодо продажу гри. При цьому створюються об'яви, додаткові матеріали до гри – картки, колекційні видання. Часто на цьому етапі виходить демоверсія гри, призначена для відслідковування відзивів і настрою гравців.

Деякі розробники комп'ютерних ігор притримуються концепції, що включає сім етапів. Однак аналіз показує, що в даній концепції також реалізуються ті ж три стадії, лише стадія «продакшен» подається у вигляді п'яти підстадій. Розглянемо їх більш детально [2].

Концептування (Concept). Це фактично стадія пре-продакшен. На цьому етапі команда придумує концепцію гри і здійснює початкову проробку ігрового дизайну. Головна мета даного етапу – це гейм-дизайнерська документація, що включає в себе розвернутий документ, який описує гру як кінцевий бізнес-продукт, і початкову проробку всіх аспектів гри.

У своїй документації гейм-дизайнер формулює і зберігає свої ідеї. Виконавцю документація дозволяє вірно розуміти свої задачі щодо реалізації продукту. Тестувальник чітко вбачає, що і як тестувати. Для продюсера ця документація є матеріалом для формування планів і контролю виконання задач. Особливо на ранніх стадіях інвестору стає зрозумілим, на що саме він виділяє кошти.

Вкрай важливо, щоб вся проектна і продуктова документація підтримувалась в актуальному стані на усіх етапах розвитку проекту. Серед ключових принципів формування продуктової документації важливо відмітити наступні: структурованість, захищеність від різночитання, повне описання продукту, регулярна актуалізація [2].

Стадія продакшен у даній концепції подається у вигляді п'яти підстадій, які подані на рис. 1. Розглянемо їх більш докладніше.

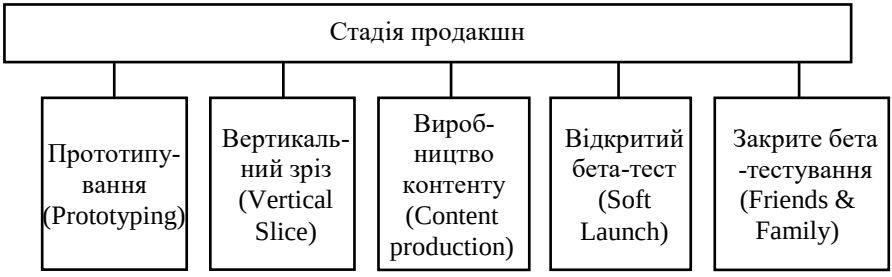


Рисунок 1 – Структура стадії продакшн

Прототипування є важливим етапом проектування будь-якої гри – це створення прототипу. Прототип реалізується для оцінки основного ігрового процесу, перевірки різних гіпотез, проведення тестів ігрової механіки, для перевірки ключових технічних моментів. На етапі створення прототипу дуже важливо реалізувати лише те, що потрібно перевірити у стиснуті терміни. Прототип повинен бути простим у реалізації, оскільки після досягнення поставлених перед ним цілей він більше не використовується [2].

Метою вертикального зрізу є отримання мінімально можливої повноцінної версії гри, яка містить у собі повністю реалізований основний ігровий процес. При цьому високу якість проробки обов'язково необхідно втілити лише для тих ігрових елементів, які суттєво впливають на сприйняття продукту. Тут всі базові особливості гри мають місце як мінімум в чорновій якості. При цьому реалізується мінімальний, але достатній для втілення повноцінного ігрового процесу набір змісту, що представляє один рівень або одну локацію.

На етапі виробництва контенту виробляється достатня його кількість для першого запуску на зовнішню аудиторію. Реалізується більшість задумок, запланованих до закритого бета-тестування. Це найбільш тривалий етап, який може займати для крупних проектів рік і більше. На цьому етапі задіяна найбільша кількість фахівців, які займаються виробництвом усього основного наповнення гри. Художники створюють всі графічні ресурси, гейм-дизайнери налагоджують баланс і заповнюють конфігі, програмісти реалізують і полірують всі опції.

На етапі бета-тестування продукт вперше демонструється достатньо широкій аудиторії. Серед найбільш важливих задач на цьому етапі виступають наступні: пошук і впровадження гейм-дизайнерських помилок, проблем ігрової логіки. На цьому етапі в грі приймають участь всі ключові опції, створено достатньо контенту для повноцінної гри тривалий час, налагоджені збір і аналіз статистики. Тестування йде за тест-планом, здійснюються стрес-тести вже з залученням реальних гравців [2].

На етапі відкритого бета-тестування продовжується тестування гри, але вже на широкій аудиторії. Відбувається оптимізація під великі навантаження. Гра повинна бути готовою для великого трафіку. У грі реалізовано білінг і приймаються платежі. На цьому етапі повністю завершується розробка нових опцій. Програмісти припиняють реалізовувати щось нове, а повністю переключаються на відлагодження опцій, які вже є в наявності. Гейм-дизайнери, продюсер і аналітики роблять висновки з зібраної на закритому бета-тестуванні статистики. При цьому до початку етапу повинна повністю функціонувати інфраструктура проекту: сайт, групи в соціальних мережах, канали залучення, підтримка користувачів. На цьому етапі стадія продакшен закінчується.

Сьомий етап Release у цій концепції за намірами практично співпадає з розглянутою третьою стадією – продакшен. Однак розглянемо її більш

детальніше, враховуючи певні відмінності. Її ключова мета – отримання прибутку. Тут базовим критерієм виступає: кількість грошей, які приносить у середньому один гравець за весь час повинна перевищувати витрати на залучення цього гравця. На цьому етапі необхідно повністю налагодити оперування продукту, витримувати маркетингові і фінансові плани, проводити роботи щодо покращення фінансових показників, активно відпрацьовувати канали щодо залучення трафіку. Команда розробників на цьому етапі займається виправленням технічних багів, які виявляються в процесі експлуатації та оптимізації продукту. Гейм-дизайнери займаються тонким налагодженням гейм-плея під реальну ситуацію у гральному світі. Також відбувається розробка та інтеграція в продукт нового контенту, який підтримує інтерес гравців [3].

Нині в розробці комп'ютерних ігор здебільшого приймає участь наступний персонал: продюсер, видавець, команда розробки, до складу якої входять гейм-дизайнер, художник, програміст, гейм-дизайнер рівнів, звукорежисер, тестувальник. Кожний представник приведеного персоналу має свої конкретні обов'язки при розробці комп'ютерної гри.

Для великих і середніх проектів виникла необхідність документувати процес розробки. Зміст і перелік документів значно варіюється в залежності від рівня розробника, але можливо виокремити три основних документа: концепт-документ, дизайн-документ, документ-пропозиція.

Зазвичай підтримка полягає у випуску засобів для виправлення помилок, які знайдені вже після виходу гри. Однак у випадку масових онлайн-ігор з широким використанням MMORPG, підтримка може зрівнятись або навіть перевищити виробництво як за трудомісткістю, так і за часом, оскільки успішна MMORPG повинна безперервно розвиватись і розширюватись, щоб запобігти відтоку гравців.

Висновки. Таким чином, комп'ютерні ігри, розробка яких розпочалась зовсім недавно, стрімко розвиваються. Нині ігрова індустрія набирає широких розмахів. Повсюдно спостерігається, що виробництво комп'ютерних ігор стає все більш організованим і відлагодженим. Важливість формалізації усвідомлюють не лише розробники, але і видавці. Більш формалізованє і організоване виробництво дозволяє використовувати робочий час розробників раціональніше. При цьому розробники отримують більше можливостей для прояву творчих здібностей в удосконаленні вмісту гри. Завдяки цьому сьогодні вже можливо побачити ігри, що мають розвинутий сюжет, потужну естетичну складову та емоційне забарвлення.

Список літератури

1. Moore M. Basics of Game Design / M. Moore. – Florida: CRC Press, 2011. – 400 p.

2. Schell J. The Art of Game Design: A Book of Lenses / Jesse Schell. – USA: Morgan Kaufmann Publishers, 2014. – 600 p.

3. Роллингз Э. Проектирование и архитектура игр / Э. Роллингз, Д. Моррис. – М: Издательский дом "Вильямс", 2006. – 1040 с.

УДК 004.358

Проблемы использования устройств дополненной реальности пилотами военной авиации

Алешко Н.С., студент 3 курса, Анкуда Д.И., студент 3 курса,
Савенко А.Г., ассистент, магистр технических наук
Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники, г. Минск

На сегодняшний день инструменты дополненной реальности применяются для решения широкого спектра задач, от медицины до компьютерных игр. Однако стоит отметить, что история применения AR начинается в военной авиации.

Первым устройством, использовавшим технологии AR, стал ИЛС (индикатор на лобовом стекле, head-up display (HUD)) британского самолета de Havilland Mosquito. Разработанный в 1942 году, он был призван совместить информацию, поступающую с РЛС с установленным на самолете прицелом, для обеспечения пилота информацией во время выполнения задач ночного истребителя. Совмещение происходило с помощью небольшого дисплея, установленного на одной линии с прицелом пилота [1].

Рисунок 1 – Современный ИЛС, установленный на истребителе F/A-18

Современные ИЛС позволяют демонстрировать пилоту значительно большее количество информации, например, такие показатели, как угол атаки, навигационные отметки при взлете\посадке, силу тяги двигателя и вектор траектории, а в вариантах системы, используемых военными- расстояние до цели, статус вооружения, положение сенсоров наведения, скорость сближения с целью[2]. Пример такого индикатора приведен на рисунке 1. Также у современных ИЛС существует возможность выводить на экран изображение с внешних источников, таких как подвесные контейнеры целеуказания и навигации, а также внешние видеокамеры [2].

Следующим шагом в использовании дополненной реальности в военной авиации стало создание систем нашлемного целеуказания и индикации (НСЦИ, Helmet-mounted display, HMD). Концепция устройства

заключалась в выведении дополнительной информации прямо на индикатор, находящийся в шлеме пилота. Первым устройством данного типа стал Super Cockpit, разработанный по заказу ВВС США в 1969 году [3]. Конструктивно оно представляло из себя шлем, в котором совмещались дополненная и виртуальная реальность (более подробная схема изображена на рисунке 2). Основной целью разработки являлось упрощение выполнения задач на малых высотах [3].

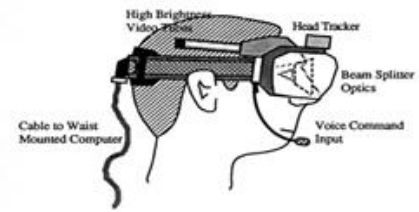


Рисунок 2 – Схема устройства Super Cockpit

В общем случае, нашлемная система целеуказания и индикации состоит из пяти основных частей: собственно, шлема, оптической системы, источника изображения, комплекса электронных систем, а также устройства отслеживания взгляда летчика. Сюда же могут входить и устройства, позволяющие ориентироваться ночью, например, модули ночного видения, которые крепятся к шлему пилота.

В дальнейшем системы HMD совершенствовались добавлением нового функционала, а именно выведения изображения с внешних камер и отображения информации о текущем состоянии летательного аппарата и маршруте полета (Integrated Helmet And Display Sight System (IHADSS), 1985 г. [4]). Очень важным событием стало создание НСЦИ «Щель-3УМ». Система позволяла осуществлять наведение ракеты «воздух-воздух» с помощью движений головы, что давало пилоту преимущество в воздушном бою [5]. «Щель-3УМ» являлась первой НСЦИ с таким функционалом, второй (и пока единственной, принятой в эксплуатацию) такой системой является Joint Helmet-Mounted Cueing System (JHMCS) (изображенная на рисунке 3), поставленной на вооружение ВВС США в 2003 году [6].

Рисунок 3 – Пилот в шлеме Joint Helmet-Mounted Cueing System

На сегодняшний день самой совершенной НСЦИ является Helmet-Mounted Display System (HMDS), разработанная специально для

истребителя 5-го поколения F-35. В данном устройстве реализована интеграция с 6 внешними инфракрасными камерами, установленными на самолете, что позволяет пилоту осуществлять наблюдение буквально «вокруг» всего самолета. В шлеме присутствует возможность наведения всего спектра оружия, применяемого самолетом, а также возможность регулирования выводимой на дисплей НСЦИ информации. К примеру, пилот может выбрать отображаемые в визоре шлема параметры полета или цели [7]. Такой широкий спектр возможностей позволил конструкторам F-35 отказаться от ИЛС вовсе в пользу НСЦИ.

Проводя соответствующую оценку, можно выделить преимущества устройств дополненной реальности применительно к пилотам военной авиации.

Уменьшение времени реакции с помощью выведения и настройки объема необходимой информации с приборов на дисплей ИЛС\визор НСЦИ, что актуально при активном маневрировании, например, в ближнем воздушном бою. Особенно это касается НСЦИ с системой целеуказания – они позволяют использовать вооружение значительно быстрее, упрощая наведение до простого движения головы.

Стоит отметить и упрощение маневрирования летательного аппарата в целом. С помощью ИЛС\НСЦИ пилот может быть визуально проинформирован о том, какое маневрирование является безопасным, а какое – нет. Также стоит отметить возможность ИЛС\НСЦИ выводить пилоту информацию о рекомендуемых параметрах для взлета\посадки (которые считаются самыми опасными моментами в полете), включая скорость и высоту, а также систему «контрольных точек», что значительно упрощает действия пилота.

Однако у устройств дополненной реальности есть также очевидные недостатки.

Характерной особенностью некоторых НСЦИ является то, что конструктивно визор может использоваться лишь одним глазом, второй глаз при этом визором остается незадействованным. Из-за разницы в получаемом зрительной системой человека изображении пилоты могут ощущать дискомфорт, вплоть до сильной головной боли [8]. Также стоит отметить большую массу НСЦИ, что приводит к большой нагрузке на шею носителя и вызывает боли в спине [9].

Значимой проблемой является информационная перегрузка. Несмотря на то, что в современных НСЦИ и ИЛС существует возможность фильтрации выводимой информации, в некоторых ситуациях потоки данных, демонстрируемые пользователю, не могут быть своевременно им обработаны, что увеличивает вероятность совершения пилотом ошибки. Особенно это опасно при выполнении сложных маневров на малой высоте или во время нахождения в зоне боевых действий.

Еще одной общей проблемой устройств дополненной реальности в военной авиации является их сложность и, следовательно, надежность.

Большая часть современных НСЦИ испытывает проблемы как на стадии разработки, так и на стадии непосредственной эксплуатации [10]. Эти проблемы являются решаемыми и своевременно исправляются, однако на время внесения исправлений в аппаратную или программную части НСЦИ перестает быть рабочим инструментом.

Сложность AR-устройств также потенциально уменьшает темпы подготовки пилотов. Учитывая все возможности НСЦИ, пилота требуется дополнительно обучать использовать функционал устройства, что занимает достаточно большой промежуток времени ввиду наличия широкого спектра инструментов.

Несмотря на все недостатки, устройства дополненной реальности находят все более широкое применение в военной авиации, что говорит о том, что риск их использования в сравнении с преимуществами все же не является настолько большим. С учетом постоянного совершенствования технологий и развития возможностей AR, вышеперечисленные проблемы могут быть решены в самом скором времени.

Список литературы

1. White I. The History of Air Intercept (AI) Radar and the British Nightfighter / I.White. – Casemate Publishers, 2007. – 326 p.

2. Spitzer, Cary R., ed. Digital Avionics Handbook. Head-Up Displays. – Boca Raton, FL: CRC Press, 2001. – 206 p.

3. Military Applications of Augmented Reality / Mark A. Livingston [and other]. – Washington: Naval Research Laboratory, 2011. – 36 p.

4. USAARL Report No. 88-13 [Электронный ресурс]. – Режим доступа: http://www.usaarl.army.mil/TechReports/88-13.PDF.Дата доступа:18.03.2018

5. Авиашлемы. Вирутальная реальность в настоящем бою [Электронный ресурс]. – Режим доступа: https://naked-science.ru /article/tech/aviashlemy-virtualnaya-realnost-v/. Дата доступа: 18.03.2018.

6. Joint Helmet Mounted Cueing System [Электронный ресурс]. – Режим доступа:https://www.rockwellcollins.com/Products_and_Services/Defense/Avionics/Displays_and_Controls/Helmet_Mounted_Displays/Joint_Helmet_Mounted_Cueing_System.aspx. Дата доступа: 18.03.2018

7. F-35 Gen III Helmet Mounted Display System [Электронный ресурс]. – Режим доступа: https://www.rockwellcollins.com/Products_and_Services/ Defense/Avionics/Displays_and_Controls/Helmet_Mounted_Displays/F-35 _Gen_III_Helmet_Mounted_Display_System.aspx. Дата доступа: 18.03.2018

8. Rash C.E. Helmet Mounted Displays: Design Issues for Rotary-wing Aircraft / C. E. Rash. – SPIE, 2001. – 258 p.

9. Newman D.G. Flying Fast Jets: Human Factors and Performance Limitations / D.G. Newman. – CRC Press, 2014. – 184 p.

10. Pentagon: Here are all the problems with the F-35 [Электронный ресурс]. – Режим доступа: http://www.businessinsider.com/here-are-all-the-problems-with-the-f-35-that-the-pentagon-found-in-a-2014-report-2015-3. Дата доступа: 18.03.2018.

УДК 004.021

Сравнительный анализ алгоритмов поиска ассоциативных правил

Антипорович С.В., магистрант
Научный руководитель – Марковская Н.В., к.ф.-м.н., доцент
Гродненский государственный университет им. Я. Купалы

В настоящее время объемы данных, подлежащих сохранению с целью последующего использования, растут высокими темпами. Сохраненные данные в дальнейшем подвергают анализу для выявления определенного рода зависимостей. Для выявления данных зависимостей применяются ассоциативные правила.

Ассоциативным правилом называют способ обнаружения взаимосвязи (ассоциации) между событиями (явлениями, процессами, предметами). Для автоматизации процесса нахождения таких правил применяются алгоритмы, которые, принимая входные данные, строят набор правил, позволяющих искать взаимосвязи между событиями (ассоциации). Входными данными для данного рода алгоритмов является определенный набор множеств. Данный набор условно называется базовым набором. Каждое множество внутри базового набора называется транзакцией. Первоначально алгоритмы поиска ассоциативных правил находили свое применение в решении задач, связанных с нахождением ассоциаций в потребительской корзине. Именно с этим фактом связано появление значительной части терминологии, относящейся к области ассоциативных правил.

Основными критериями оценки ассоциативных правил являются поддержка, а также достоверность. Поддержка – это отношение количества транзакций, содержащих условие и следствие, к общему числу транзакций (задается на входе вместе с базовым набором). Достоверность – это отношение числа транзакций, содержащих условие и следствие, к транзакциям, содержащим условие.

Алгоритмы поиска ассоциативных правил работают в два этапа:

- нахождение множеств признаков с поддержкой не ниже заданной на входе;
- построение ассоциативных правил на основе найденных множеств признаков.

Ниже приведены наиболее распространенные алгоритмы поиска ассоциативных правил.

Алгоритм Apriori. Работа алгоритма состоит из нескольких этапов. Каждый из этапов состоит из следующих шагов:

• формирование кандидатов (алгоритм, сканируя базу данных, создает множество i-элементных кандидатов (i — номер этапа). На этом

шаге поддержка кандидатов не рассчитывается);

• подсчет кандидатов (шаг, на котором вычисляется поддержка каждого i-элементного кандидата; осуществляется отсечение кандидатов, поддержка которых меньше минимума, установленного пользователем).

На первом этапе происходит формирование одноэлементных кандидатов. Далее алгоритм подсчитывает поддержку одноэлементных наборов. Наборы с уровнем поддержки меньше установленного отсекаются. Оставшиеся наборы считаются часто встречающимися одноэлементными наборами.

Далее происходит формирование двухэлементных кандидатов, подсчет их поддержки и отсечение наборов с уровнем поддержки меньше установленного. Оставшиеся двухэлементные наборы считаются часто встречающимися и принимают участие в дальнейшей работе алгоритма.

На последнем этапе n алгоритм формирует n-элементные наборы, подсчитывает их поддержку и отсекает наборы с уровнем поддержки меньше установленного. Набор размерностью n может быть назван часто встречающимся.

Отсечение кандидатов происходит на основе предположения о том, что у часто встречающегося набора товаров все подмножества должны быть часто встречающимися. Если в наборе находится подмножество, которое на предыдущем этапе было определено как нечасто встречающееся, этот кандидат уже не включается в формирование и подсчет кандидатов.

Среди достоинств алгоритма можно выделить:

- простоту;
- быстрое уменьшение числа кандидатов (в случае установки высокого уровня поддержки).

Среди недостатков алгоритма можно выделить:

- большое число сканирования базового набора;
- большое число сгенерированных кандидатов в случае установления низкого уровня поддержки или большом наборе данных.

Если применить данный алгоритм к базовому набору размерностью 100, то алгоритм сгенерирует порядка 2^{100} кандидатов. После данного рода генерации буду выполнены все необходимые проверки.

Исходя из выше приведенных фактов можно сделать вывод, что алгоритм может быть эффективным только для наборов данных небольшой размерности, либо при высоком установленном уровне поддержки.

Для повышения эффективности работы алгоритма были разработаны его модификации, направленные на сокращение количества обходов базового набора, сокращение количества сгенерированных кандидатов (AprioriTid и AprioriHybrid). При этом сглаживания недостатков алгоритма удается достичь не всегда.

Алгоритм FP-growth. Данный алгоритм – один из наиболее

эффективных алгоритмов поиска ассоциативных правил. Алгоритм позволяет избежать не только затратной по ресурсам процедуры генерации кандидатов, но и уменьшить число обходов базового набора. В основе алгоритма лежит предварительная обработка базового набора, в процессе которой базовый набор преобразуется в специальную компактную древовидную структуру, называемую Frequent-Pattern Tree (дерево популярных предметных наборов). В общем виде алгоритм представлен из следующих шагов:

- производится полный обход базового набора, при этом все элементы каждой транзакции сортируются в порядке убывания поддержки этих элементов в базовом наборе.
- Производится удаление элементов, для которых уровень поддержки меньше установленного.
- Построение префиксного Frequent-Pattern Tree из оставшихся элементов.
- Извлечение частных предметных наборов.

Узлом Frequent-Pattern Tree является структура, содержащая в себе значение узла, ссылки на дочерние элементы и значение поддержки дочернего элемента для текущего узла.

Построение префиксного Frequent-Pattern Tree происходит в несколько этапов:

- построение корневого узла.
- Для каждого элемента отсортированной транзакции из базового набора строятся узлы по следующему правилу:
  - если для элемента в текущем узле есть потомок, содержащий этот элемент, то новый узел не создается, а значение поддержки для данного потомка увеличивается на единицу, в противном случае создается новый узел-потомок с поддержкой 1. Текущим узлом при этом становится найденный или построенный узел.

При этом размер дерева зависит от того, как элементы были отсортированы. Обычно, описанный в шаге 1 способ приводит к значительному уменьшению дерева.

Алгоритм извлечения популярных наборов имеет вид:

- Для каждого элемента в дереве начиная с элемента с наименьшим уровнем поддержки выполнить:
  - добавить этот элемент во множество A.
  - Построить условное дерево по этому элементу. В случае если такое дерево оказывается пустым, то записать в результат элементы множества A (они и будут очередным популярным набором), иначе выполнить этот алгоритм для построенного условного дерева.
  - Исключить элемент из множества A.
  - Исключить элемент из дерева. Таким образом, дерево

проходится рекурсивно снизу вверх полностью, и при этом генерируются все возможные популярные наборы.

Достоинства алгоритма:

- Позволяет избежать затратной процедуры генерации кандидатов, характерной для Apriori.
- Сжатие базового набора в компактную структуру, обеспечивающие быстрое и полное извлечение предметных наборов.
- Число сканирования входного набора сокращено.
- Размер дерева обычно меньше размера базового набора данных.

Недостатки алгоритма:

- Построение дерева – затратная по времени операция.
- В некоторых случаях, вследствие большого числа узлов и связей, размер Frequent-Pattern Tree может намного превышать размер входного набора данных.

Существует множество модификаций алгоритма, направленных на улучшение его свойств.

Список литературы

1. Agrawal R. Fast algoritms for missing association rules in large databases / R. Agrawal, R. Srikant // Proceedings of the 20th International Conference on Very Large Data Bases – 1994. – P. 487–499.

2. Apriori – масштабируемый алгоритм поиска ассоциативных правил [Электронный ресурс]. – Режим доступа: https://basegroup.ru/community/articles/apriori.

3. FPG – альтернативный алгоритм поиска ассоциативных правил [Электронный ресурс]. – Режим доступа: https://basegroup.ru/community/articles/fpg.

4. Введение в анализ ассоциативных правил [Электронный ресурс]. – Режим доступа: https://basegroup.ru/community/articles/intro.

5. Методы поиска ассоциативных правил [Электронный ресурс]. – Режим доступа: https://www.intuit.ru/studies/courses/6/6/lecture/186?page=3.

УДК 004.415.25

Система масового оповіщення з використанням мобільних девайсів

Арутюнян В.Е., аспірант кафедри інформаційних технологій
Запорізький інститут економіки та інформаційних технологій

Актуальність дослідження полягає у необхідності створення перспективного і орієнтованого на практичні дії комплексу заходів по зменшенню небезпеки надзвичайних ситуацій на місцевому, національному, регіональному і міжнародному рівнях. Для оцінки стану процесу досягнення передбачуваних результатів, на 3-тій Всесвітній конференції ООН зі зменшення небезпеки надзвичайних ситуацій у 2015 році в Японії визначено сім глобальних цільових задач, однією з яких є розвиток систем раннього оповіщення про небезпеку надзвичайних ситуацій, яка є актуальною на найближчі 15 років.

Метою дослідження є теоретичне обґрунтування та розробка моделей і методів створення інтелектуальної системи для оповіщення населення в надзвичайних ситуаціях.

Проведений критичний аналіз показав, що всі діючі системи масового оповіщення при надзвичайних ситуаціях не відповідають повною мірою сучасним вимогам, які до даних систем значно зросли через масове використання смартфонів. Всі впроваджені системи масового оповіщення є статичними і не мають можливості динамічно змінювати свої алгоритми вже в процесі роботи з огляду на безліч параметрів, які безпосередньо впливають на ефективність роботи системи. Автором була запропонована і розроблена клієнт-серверна модель для сучасної системи масового оповіщення при надзвичайних ситуаціях, а також використання сервісів інтерактивних карт місцевості для налагодження зв'язку між сервером та мобільними девайсами потерпілих, обміну та обробки необхідної інформації. Розроблений програмний комплекс складається з двох частин: клієнтська частина, яка представлена у вигляді мобільних додатків для Android і iOS, які можуть бути встановлені на будь-якому мобільному девайсі; серверна частина, на якій запрограмовані спеціальні алгоритми обробки інформації, API та яка взаємодіє з сервісами Google Maps.

В процесі роботи програмного комплексу додаток-клієнт збирає необхідні параметри, такі як координати, швидкість пересування, висота над рівнем моря, і передає ці дані на сервер. Сервер обробляє отриману інформацію за допомогою своїх спеціальних алгоритмів та сервісів Google Maps і передає потерпілому кращий план евакуації в даний момент. Одночасно різні учасники процесу евакуації можуть отримати різні плани евакуацій, які сервер вважає найефективнішими для кожного потерпілого.

Отже, така система дозволить рятувати більшу кількість людей.

УДК 004.051

Технології оптимізації коду в сучасних компіляторах

Бісюк В.А., викладач
Центральноукраїнський національний технічний університет, м. Кропивницький

Стрімкий розвиток апаратних комп'ютерних і мобільних платформ, вдосконалення і поява нових програмних засобів, значне розширення сфери використання IT-технологій обумовлює необхідність розробки і впровадження нових компіляторів, які відповідають більш високим вимогам до швидкодії та оптимальному використанню апаратних і системних програмних ресурсів.

Швидкодія сучасних процесорів забезпечується не тільки вдосконаленням апаратної архітектури, але й з використанням нових процесорних команд та технологій обчислень. Зрозуміло що це неможливо без впровадження нових компіляторів, які дозволять використати всю потужність нових технологій.

Майже щорічно ведучі компанії оновлюють свої лінійки компіляторів щоб забезпечити підтримку нових процесорів.

Наприклад компілятор Intel враховує всі особливості архітектури процесорів, які випускаються компанією і забезпечує високу продуктивність програм, дозволяє отримати поліпшення продуктивності на 10-15% для платформи x86.

Виділяють декілька характеристик коду, що визначають продуктивність програми, і відповідно є методи, які застосовуються всередині компілятора для досягнення того чи іншого критерію ефективності додатка.

Найбільш впливова характеристика – ефективність обчислень: ефективне перевикористання отриманих раніше результатів обчислень, виконання максимальної кількості обчислень під час компіляції, ефективне видалення «мертвого» коду, винос інваріантів з циклів та інші оптимізації такого типу. Їх використання призводять до того, що обчислення можуть виконуватися при компіляції програми, а не під час її виконання.

Другий за впливом фактор – ефективність роботи з підсистемою пам'яті. Оскільки сучасні обчислювальні системи забезпечуються декількома рівнями кеш-пам'яті, то швидкість обчислень значно збільшується, якщо пам'ять, яку використовує програма, грамотно розподілена: об'єкти, які спільно використовуються компактно розташовуються в пам'яті, і робота з об'єктами в пам'яті добре прогнозована і дозволяє процесору ефективно асистувати обчисленням, заздалегідь дозавантажуючи в кеш-пам'ять необхідні дані. Інакше зростає

навантаження на шину, а отже і загальний час виконання. Для підвищення ефективності роботи пам'яті програми використовуються різні оптимізації циклів та автоматична програмна передвибірка з пам'яті, коли компілятор розставляє в коді програми спеціальні інструкції для передвибірки необхідних додатку адрес пам'яті.

Ще один спосіб підвищення ефективності додатка за рахунок більш ефективного використання векторних інструкцій і роботи автоматичного векторизатора, що заміняє скалярний код на векторний. В цьому випадку підвищення продуктивності досягається завдяки зменшенню кількості виконуваних інструкцій.

Впровадження багатопроцесорних та багатоядерних процесорів зробило актуальним ще один фактор оптимізації – розпаралелення обчислень для рівномірного завантаження всіх доступних ресурсів системи. Деякі сучасні компілятори пропонують розробникам використовувати автопараллелізацію – механізм автоматичного розпаралелювання циклів. Автоматична паралелізація активно взаємодіє з іншими цикловими оптимізаціями, змінюючи порядок і евристичні механізми прийняття рішень по оптимізації.

Слід пам’ятати, що наслідки оптимізацій при компіляції іноді досить складно передбачити, можуть виникати ситуації, коли оптимізація тільки погіршує продуктивність. Тому рекомендується використовувати інструменти для аналізу продуктивності програми, такі наприклад, як VTune Amplifier або The Grinder, що дозволяють, аналізувати і модифікувати код з використанням різних ключів та директив компіляції. Крім того наслідки оптимізації можуть впливати на такий актуальний для мобільних пристроїв фактор, як енергоефективність. Збільшення кількості паралельних потоків значно підвищує енерговитрати під час роботи програми.

Висновки. Розглянуто основні технології оптимізації програмного коду та підвищення продуктивності програмних додатків, які використовуються в сучасних компіляторах.

Список літератури

1. Автоматическая оптимизация при компиляции [Електронний ресурс]. – Режим доступу: https://www.osp.ru/os/2011/02/13007711

2. Ахо А.В., Лам М.С., Сеті Р., Ульман Д.Д. Компиляторы. Принципы, технологии и инструментарий. Киев, 2008. – С. 911-1061

УДК 004.891.2

Классификация вакансий с целью последующей оптимизации публикации объявлений

Быстрова М.В., студентка 4 курса
Белорусский Государственный Университет, г. Минск

В эпоху современной глобализации ситуация на рынке труда такова, что компании желают видеть на рабочих местах сотрудников с опытом работы и определенным набором знаний. Но такого рода специалисты, как правило, уже трудоустроены в других компаниях и ищут работодателя, способного предложить более выгодные условия труда.

По статистике, заполнение большинства рабочих мест происходит с помощью публикаций объявлений о вакансиях. Успех такого набора зависит от того, как компания преуспела в составлении соответствующего объявления. Важно знать критерии, которые способны заинтересовать потенциального сотрудника, или же, другими словами, ценность предложения для работника. Данные критерии можно выделить, проанализировав все вакансии, на которые идет отклик.

При реализации алгоритма определения порядка близости между публикациями вакансий была использована технология Doc2Vec, предназначенная для обработки текстовых данных и представления их в виде векторного пространства.

Технология Doc2Vec

Данная технология собирает статистику совместного появления слов в фразах, а после этого при помощи нейронных сетей решает задачу снижения размерности, формируя на выходе компактные векторные представления слов максимально учитывая степень отношения этих слов в обрабатываемом тексте.

В Doc2Vec используется нейронная сеть прямого распространения, на вход которой должны подаваться векторы фиксированной длины. Для того, чтобы было возможно применять данную технологию для работы с текстами разной длины, выполняется приведение векторов к одной размерности. При таком усреднении учитывается порядок слов благодаря добавлению вектора-абзаца и вектора-документа.

Технология Doc2Vec базируется на двух методах (см. Рисунок 1):

- *Distributed Memory*/распределенная память (DM) – прогнозирует слово по известным предшествующим словам и вектору абзаца.
- *Distributed Bag of Words*/распределенный мешок слов (DBOW) – прогнозирует случайные группы слов в абзаце на основании вектора

абзаца.

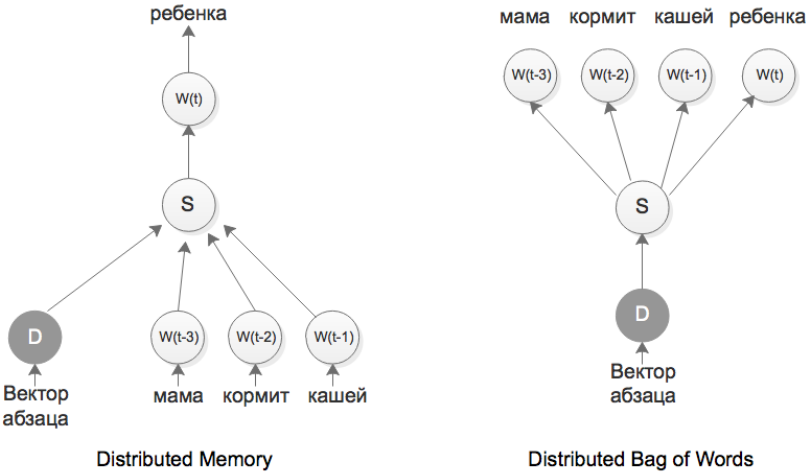


Рисунок 1. Архитектура методов Distributed Memory и Distributed Bag of Words

Данная технология хорошо подходит для анализа небольших документов (таких как рецензии или же публикации вакансий), в которых необходимо анализировать слова не по отдельности, а в рамках всего документа.

Основные этапы построения классифицирующей модели

Этап 1. Предварительная обработка и индексация.

Под предварительной обработкой понимают процесс преобразования последовательности слов, встречающихся в документе, в n-мерное пространство [1]. При этом происходит извлечение наиболее значимых слов (термов), удаление стоп-слов и html-тегов, а также и более сложные формы обработки текстовой информации такие, как морфологический и синтаксический анализ документов. Следует отметить, что многие классифицирующие алгоритмы требуют подачи на вход предварительно размеченной выборки.

Этап 2. Построение и обучение классификатора.

После формирования и предварительной обработки тренировочного набора документов следует выбор и построение классифицирующей модели. На вход данной модели подается тренировочная выборка для формирования словаря и дальнейшего обучения. Качество

классифицирующей модели зависит от условий поставленной задачи и сформированной тренировочной выборки.

Этап 3. Оценка качества работы классификатора.

Для оценки качества работы классификатора используется тестовая выборка документов, для которых заранее определены классы. Ее подают на вход классификатора, после чего используется одна из следующих характеристик: *доля правильных ответов (accuracy), полнота (recall), точность (precision)* и *F-мера*.

Следует отметить, что эффективность работы классификатора напрямую зависит от размера и качества предварительной обработки данных, выступающих в качестве тренировочной выборки, а также метода построения самого классификатора.

Алгоритм определения порядка близости между публикациями вакансий на базе технологии Doc2Vec

Разработанный в рамках данной работы алгоритм представляет собой веб-сервис, работающий по протоколу HTTP. Сама модель построена с использованием набора инструментов Gensim, предназначенного для моделирования векторного пространства, языка программирования Python.

Имеется некоторая выборка, состоящая из 10 тысяч документов, разбитых более, чем на 20 классов (Accounting, Audit, Design, HR, Nursing и т.д.). Каждый документ проходит через этапы предварительной обработки: удаляются html теги и знаки пунктуации. Далее каждый документ преобразуется в массив слов, который размечается согласно требованиям алгоритма Doc2Vec. При этом, помечается принадлежность документа определенному классу. Например, для класса «Audit» - tags=['AUDIT_#документа'].

После создания модели, формирования словаря и обучения, в модели хранятся векторы документов с наиболее существенными словами, которые называются термами. В рамках реализованной модели, каждому документу соответствует ровно сто термов с весовыми коэффициентами, определяющими значимость в рамках отдельного документа. Также можно выделить термы, соответствующие определенному классу документов.

Например, для класса «Audit» получили набор термов с весовыми коэффициентами:

[(u'financial', 0.6264161467552185), (u'english', 0.5597227215766907), (u'management', 0.5499826669692993), (u'communication', 0.5458555221557617),

(u'presentation', 0.5436646938323975), (u'excel', 0.5335297584533691), (u'analyse', 0.5295985341072083), (u'engineer', 0.5220131874084473), (u'experience', 0.5190562009811401), (u'sql', 0.5189145803451538)]

Представленные выше термы, в той или иной степени отражены в большинстве документов класса. Их также можно получить и проанализировать.

Можно также определить, какие документы являются похожими в рамках данной модели, а также найти похожие термы по всем документам.

Например, для документа, помеченного *AUDIT_1* результаты поиска близких по смыслу ранее опубликованных вакансий:

[('AUDIT_7', 0.4295151162147515), ('AUDIT_19', 0.3395153326147522), ('AUDIT _3', 0.314151162736152), ('AUDIT _28', 0.304158459836152), ('AUDIT_33', 0.297155656064251), ('AUDIT _10', 0.296252651984625), ('AUDIT _60', 0.2844726321794921), ('AUDIT_98', 0.2815384230262146), ('AUDIT_5', 0.2799204210281372), ('AUDIT_87', 0.2797151162147542)]

Видно, что поиск схожих публикаций вакансий осуществляется в рамках класса, которому принадлежит документ, т. к. в рамках модели они считаются наиболее схожими.

Заключение

Как было ранее отмечено, анализ публикации вакансий имеет большую практическую значимость для анализа рынка вакансий, так и для компаний, заинтересованных в приеме на работу квалифицированных специалистов. С задачей анализа публикаций хорошо справился алгоритм на базе технологии Doc2Vec, который позволил выявить набор наиболее значимых термов, как в рамках отдельно взятой публикации, так и в рамках определенного класса вакансий. Отличительной особенностью использованной технологии является то, что она работает с заранее размеченным набором документов, что позволяет обрабатывать документ в рамках определенного класса, а не всей тренировочной выборки.

Планируется также классифицирование резюме и в дальнейшем разработать алгоритма с целью определения соответствия резюме предоставляемой вакансии и наоборот.

Литература

1.Агеев, М. С. Методы автоматической рубрикации текстов, основанные на машинном обучении знаниях экспертов / М. С. Агеев. - М.: Либроком (Editorial URSS), 2004. – 106 с.

УДК 681.03

Технологии Big Data и их применение для анализа пользователей сети

Вдовиченко И.Н., доцент, к.т.н.
Криворожский национальный университет, г. Кривой Рог

Термин Big Data имеет отношение к наборам данных, размер которых превосходит возможности стандартных баз данных по обработке, хранению, управлению и анализу информации. Это инструмент и метод анализа данных.

Аналитическая компания IDC представила в декабре 2012 г. отчет, в котором предсказывалось, что объемы информации будут удваиваться каждые 2 года в течение следующих 8 лет. За ближайшие 7 лет количество данных в мире достигнет 40 ЗБ (1 ЗБ = 10^21байт), а это значит, что на каждого жителя Земли будет приходиться по 5200 ГБ данных [2].

Традиционные методы анализа информации не могут угнаться за огромными объемами постоянно растущих и обновляемых данных, что в итоге и открывает дорогу технологиям Big Data.

Корпорация EMC провела исследование, в ходе которого было выявлено, что использование Big Data ведет к существенному улучшению процессов принятия решений, повышает конкурентоспособность компаний и упрощает управление рисками [1].

Большие данные – это системный, качественный переход к составлению цепочек ценностей, основанных на знаниях. По эффекту его можно сравнить с появлением доступной компьютерной техники в конце прошлого века.

Кроме стандартного применения, Big Data дают возможность для проведения серьезных психологических анализов. На основе синтеза данных из социальных сетей можно получить интереснейшие выводы за счет выявления скрытых закономерностей.

В последние годы начинает проявляться принципиально новый эффект от массового применения этого подхода в обработке данных. Ученые ищут скрытые корреляции между исследуемым явлением (объектом, процессом) и тысячей других факторов, где в качестве исходных данных использовалась огромная статистика, накопленная за долгие годы. Использование этих, эмпирически открытых закономерностей, обещает прогресс в развитии многих научных направлений.

Сложные современные модели Big Data все чаще выявляют некие на первый взгляд иррационально-фантастические зависимости, позволяя заглядывать далеко за пределы известной научной картины мира [3].

Безусловно, предсказательные способности Big Data обладают

впечатляющими возможностями.

Как уже говорилось, что объемы информации быстро растут (на 40% ежегодно). Большая часть сохраняемой в мире информации не структурирована, то есть не пригодна для исследования и применения. Big Data – инструмент, который позволяет адаптироваться к этой массе информации.

Классические СУБД, такие как Postgres, MySQL, Oracle не имеют такой гибкости в масштабировании при обработке больших массивов данных и при увеличении объемов дальнейшая обработка становится невозможной.

В силу сказанного, актуальным становится задание использовать технологии Big Data для анализа пользователей сайтов сети Интернет. Проведенное нами исследование, представляет собой выполнение анализа больших данных, полученных с украинских сайтов, которые используют информационные агентства. Предполагается использовать и продемонстрировать возможности языка программирования R, как одного из ведущих инструментальных средств технологии Big Data.

Намечено проанализировать зависимость частоты посещения различных сайтов молодыми людьми, в возрасте от 17 до 35 лет, от их пола, обеспечения работой, доходов и возраста.

Собранные данные сформированы в виде таблицы текстовой информации. Таблица состоит из четырех столбцов (признаков):

- пол молодого человека (POL: женский = 0 и мужской = 1);
- занятость (ZAN: студент =1, рабочий =2, безработный = 3);
- доходы в грн. (DOH);
- возраст (VOZR).

Как один из вариантов анализа, можно представить следующий пример. Создадим отдельный объект с данными для мужчин старше 25 лет: data.m.big <- data[data$POL == 1 & data$VOZR > 25,]

```
> data.m.big <- data[data$POL == 1 & data$VOZR > 25,]
> str(data.m.big)
'data.frame':   16 obs. of  4 variables:
 $ POL : int  1 1 1 1 1 1 1 1 1 1 ...
 $ ZAN : int  2 3 2 3 2 2 2 3 3 2 ...
 $ DOH : int  2500 500 3000 500 5000 6000 7000 500 500 5000 ...
 $ VOZR: int  26 28 27 30 30 31 33 35 30 35 ...
```

Рисунок 1 – Результат выборки: данные только для мужчин старше 25 лет

Проанализируем критерий доходов (DOH). summary(data$VES.R)

```
> summary(data$DOH)
   Min. 1st Qu.  Median    Mean 3rd Qu.    Max.
    500     500    1100    2327    4000    8000
>
```

Рисунок 2 – Статистические характеристики критерия DOH

Вычислим средние значения доходов отдельно для всех комбинаций возраста и пола.

> tapply(data$DOH, list(data$POL, data$VOZR), mean)

```
> tapply(data$DOH, list(data$POL, data$VOZR), mean)
    17   18   19   20   21   22   23   24   26   27   28       29   30   31
0 1100 1100 1100 1100 1100 1100 1100 1100 5000   NA 5000  500.000  500  500
1 1100   NA 1100   NA 1100 1100   NA   NA 2500 3000  500 4833.333 2000 3250
    32   33   34   35
0 4250 2250 3800 4000
1  500 7000   NA 2000
>
```

Рисунок 3 - Средние значения доходов отдельно для всех комбинаций возраста и пола

В ходе исследования были применины 13 методов анализа. В результате использования технологии Big Data получены любопытные результаты, которые служат достаточным основанием для следующих выводов.

Наши ожидания, что доходы существенно зависят от возраста не подтвердились, зависимость есть, но слабая. Нет связи между доходами и полом молодых людей. По результатам расчетов видно, что мужчины реже посещают сайты. И многие другие выводы были получены при использовании технологии Big Data, которые можно использовать для:

– при планирования рекламной продукции, рассчитанной на конкретную аудиторию пользователей;

– при изучении социальных проблем;

– при планировании тематических сайтов;

– при организации досуга молодежи и др.

Литература

1. Сьюзен Т. Большие данные: все, что вам необходимо знать, PC Week/RE, №25 (810), 2012.

2. Иванов П.Д., Вампилов В.Ж. Технологии Big Data и их применение на современном промышленном предприятии, Инженерный журнал: наука и инновации, вып. 8, 2014.

3. Савчук И. Big Data – технология, рождающая новый тип бизнеса. журнал «Бит», Выпуск №3 (36), 2014

УДК 004.04

Аналітичний огляд парадигм подійно-орієнтованого та автоматного програмування

Гайдук К. С., магістрант другого року навчання,
Шевченко О. Г., старший викладач
Донецький національний технічний університет, м. Покровськ

Вступ. Існує два основних стиля розробки програмного забезпечення (ПЗ): потоковий та подієво-орієнтований [1]. У першому випадку, ПЗ організовується у вигляді множини потоків (задач), які по черзі отримують час центрального процесора. У другому випадку, ПЗ організовується у вигляді множини обробників подій, що викликаються диспетчером при настанні відповідної події. Якщо логіка роботи програмного забезпечення досить складна і залежить від передісторії, то воно, в разі подієво-орієнтованого програмування, може бути організовано у вигляді системи взаємодіючих кінцевих автоматів, які на своїх переходах викликають необхідні обробники.

Використання подієво-орієнтованого стилю програмування дозволяє позбутися багатьох проблем, характерних для паралельних систем (гонитви, взаємні блокування, інверсія пріоритетів та ін.), а також має ряд інших переваг перед потоковим стилем, в числі яких економія оперативної пам'яті, скорочення часу перемикання контексту, скорочення обсягу вихідного коду програм до 40% [2] та ін.

В даній роботі досліджуються основні принципи автоматного програмування, яке можна розглядати як розширення парадигми подієво-орієнтованого програмування, а також наводяться приклади його практичного застосування.

Подієво-орієнтоване програмування. З появою проблеми 10-ти тисяч підключень (C10k), почалися пошуки альтернативних способів досягнення паралелізму [3]. У тому випадку, якщо на кожне клієнтське підключення на сервері виділяється окремий потік, а кількість підключень обчислюється десятками тисяч, а то й мільйонами, стають істотними накладні витрати, пов'язані з виділенням кожному потоку персонального стеку, а також з часом перемикання контексту.

Вирішення зазначеної проблеми було знайдено у використанні подієво-орієнтованої архітектури додатків (Event-Driven Architecture, EDA) [3]. В найпростішому випадку, додаток із зазначеною архітектурою складається з черги подій, що підлягають обробці, диспетчера, та множини обробників – функцій зворотного виклику.

Диспетчер послідовно витягує з черги повідомлення, і викликає відповідні обробники, передаючи в них повідомлення в якості вхідного параметра. Подіями можуть бути зміни станів елементів управління

користувацького інтерфейсу, спрацьовування таймера, отримання повідомлення від іншого обробника (обробники можуть обмінюватися повідомленнями) або вузла мережі та ін. У тому випадку, якщо робота обробника атомарна (тобто, один обробник не може переривати виконання іншого), немає потреби у виділенні кожному обробнику персонального стека - в системі може бути один загальний стек. Крім того, радикально скорочується розмір контексту (що скорочує час його перемикання), так як зникає потреба в збереженні та відновленні значень всіх регістрів.

Спорідненою по відношенню до EDA архітектурою є сервіс-орієнтована архітектура (Service-Oriented Architecture, SOA), в рамках якої програмне забезпечення організовується у вигляді множини взаємодіючих сервісів. Однією з основних відмінностей SOA від EDA є спосіб взаємодії компонентів ПЗ (сервісів і обробників відповідно): у першому випадку, як і в клієнт-серверній архітектурі, взаємодія заснована на відправці запиту і очікуванні відповіді; в разі ж EDA, відправник не очікує відповіді.

Вигідним рішенням є об'єднання названих архітектур. В такому випадку, система складається з множини сервісів, кожен з яких характеризується множиною анонсованих ним подій – подій, які він може генерувати, та множиною подій інших сервісів, тобто таких, які даний сервіс може обробляти. Взаємодія між сервісами організовується виключно за рахунок обміну повідомленнями: один сервіс не може безпосередньо викликати функцію або метод іншого сервісу - він може лише надіслати йому повідомлення. Обмін повідомленнями реалізується з використанням так званого проміжного ПЗ, яке забезпечує доставку повідомлень адресатам, а також перетворення форматів повідомлень, в разі потреби. Також характерною рисою зазначених систем є використання неблокуючого асинхронного вводу-виводу.

Прикладом серверного програмного забезпечення з архітектурою, основаною на парадигмі подієво-орієнтованого програмування, може служити хмарна операційна система (ОС) Corezoid, що використовується такими сервісами як Telegram, Amazon та ін. Дана ОС дозволяє створювати інтернет-роботів, графічно описуючи алгоритми їх поведінки за допомогою кінцевих автоматів та мереж Петрі.

Автоматне програмування (АП) – це парадигма програмування, відповідно до якої програмне забезпечення описується системою взаємодіючих кінцевих автоматів. Парадигма АП є близькою по відношенню до парадигми подієво-орієнтованого програмування, проте це не одне й те ж саме, оскільки в разі EDA система не зобов'язана описуватися моделлю автомата з пам'яттю, і може відповідати моделі автомата без пам'яті (комбінаційній схемі). Основною ж моделлю АП є автомат з пам'яттю.

В [4] автоматне програмування розглядається як розширення парадигм процедурного та об'єктно-орієнтованого програмування, відповідно до

чого виділяються процедурне програмування з явним виділенням станів та об'єктно-орієнтоване програмування з явним виділенням станів. В якості основних автоматних моделей, використовуються автомати Мілі, Мура та змішаний автомат (С-автомат).

Серед переваг АП, в [4, 5] відзначаються наступні:

1. Відділення логіки від семантики. Автомат описує логіку роботи системи, а семантика зосереджена в обробниках, що викликаються на переходах. В результаті, програмне забезпечення ділиться на системонезалежну (незалежну від апаратної платформи, операційної системи, мови програмування та ін.) та системозалежну частини. Дана обставина є важливою в контексті портування програмного забезпечення під інші ОС або апаратні платформи. Крім того, такий поділ підвищує читабельність вихідного коду, оскільки позбавляє його від складних перевірок умов з великою кількістю змінних-прапорів.

2. Ізоморфна відповідність вихідного коду графам переходів автоматів (виняток становить системозалежна частина). Дана обставина робить можливою автоматичну генерацію коду за графами переходів, які можуть бути описані в редакторі MS Office Visio, за допомогою UML або іншим способом.

3. Декларативний опис логіки роботи ПЗ. Граф переходів автомата може розглядатися не просто як еквівалент граф-схеми алгоритму, але як специфікація програми.

4. Формалізація програмного забезпечення. Програміст, у разі використання АП, працює не з аморфним кодом, а з математичним об'єктом.

Автоматно-спроектовані операційні системи. Парадигми подієво-орієнтованого та автоматного програмування застосовуються і при розробці операційних систем. Найбільш яскравим прикладом є операційна система для бездротових сенсорних вузлів SenOS. В даній ОС кожна задача описується окремим кінцевим автоматом, який представляється в оперативній пам'яті за допомогою прямої структурної таблиці (ПСТ), яка визначає переходи автомата і його виходи - обробники, що викликаються на переходах. Множина всіх обробників, використовуваних задачами-автоматами в системі, зберігається в Flash-пам'яті мікроконтролера у вигляді бібліотеки функцій зворотного виклику. Ядро ОС написано на мові С, і складається всього з 700 рядків коду. Також до складу системи входить так званий монітор (гіпервізор), який дозволяє віддалено завантажувати задачі та змінювати існуючі, шляхом перезапису відповідних ПСТ. Система має єдину чергу подій і диспетчер, який вибирає події з черги, та викликає відповідні задачі-автомати. Переходи автоматів в SenOS є атомарними, і оберігаються за допомогою мьютекса.

В неявному вигляді кінцеві автомати використовуються в таких широко відомих подієво-керованих ОС для бездротових сенсорних вузлів як TinyOS, Contiki та ін. Вбудована ОС FX-RTOS підтримує одночасно два стилі програмування: подієво-орієнтований і потоковий, надаючи

розробнику вибір. У разі подієво-орієнтованого стилю, програмне забезпечення організовується у вигляді множини обробників, що підлягають плануванню. Якщо в черзі повідомлень є повідомлення, відповідні обробнику, то такий обробник вважається готовим до виконання, і ставиться до черги. Планування виконання обробників здійснюється на підставі пріоритетів. У деяких системах мова ведеться не про пріоритет обробників, а про пріоритет повідомлень, і плануванню підлягають не обробники, а обробка повідомлень [6]. По суті, обидва варіанти відображають два різних погляди на один предмет.

Іншими прикладами подієво-орієнтованих і автоматно-спроектованих ОС можуть служити LIMOS (суміщені потоковий і подієво-орієнтований стилі), JaMOS (до складу ОС входить кінцевий автомат, що інтерпретує одержуваний по мережі байт-код), Chimera II (розробка NASA для багатопроцесорних систем з загальною пам'яттю; задачі описувалися за допомогою моделі кінцевого автомата) та ін.

Окремо варто відзначити систему TIMES, яка дозволяє описувати прикладне ПЗ систем реального часу за допомогою часових автоматів, з подальшою автоматичною генерацією коду, а також можливістю симуляції роботи і верифікації системою UPPAAL. Існує також ряд інших прикладів застосування моделі кінцевих автоматів при розробці ПЗ (опис інтерфейсів, виявлення кібератак, формальний опис ПЗ та ін.).

Висновки. Створення програмного забезпечення в потоковому стилі для більшості розробників є зрозумілим та звичним: більшість ОС орієнтована на виконання програм, написаних саме в потоковому стилі. Однак, потокове програмування характеризується неефективним використанням оперативної пам'яті, низькою реактивністю, складнощами синхронізації та рядом інших недоліків. Автоматне програмування вільне від недоліків потокового стилю, і має суттєві переваги.

Список літератури

1. Event-driven Programming for Robust Software / [F. Dabek, N. Zeldovich, F. Kaashoek та ін.] // Proceeding EW 10 Proceedings of the 10th workshop on ACM SIGOPS European workshop. – 2002. – P. 186–189.
2. FX-RTOS [Електронний ресурс] – Режим доступу до ресурсу: fxrtos.ru/module_kernel/обзор.
3. Welsh M. The Staged Event-Driven Architecture for Highly-Concurrent Server Applications / Matt Welsh // Computer Science Division. – 2000.
4. Поликарпова Н.И. Автоматное программирование / Н.И. Поликарпова, А. А. Шалыто. – Санкт-Петербург, 2008. – 167 с.
5. Шалыто А.А. SWITCH-технология — автоматный подход к созданию программного обеспечения «реактивных» систем / А. А. Шалыто, Н.И. Туккель // 2001. – №5. – С. 45–62.
6. Kaiser J. COSMIC A middleware for event-based interaction on CAN / J. Kaiser, C. Mitidieri, C. Brudna // Emerging Technologies and Factory Automation. – 2003.

УДК 004.94: 004.622

Обробка потоку даних сенсора вологості сипучих матеріалів

Дрєєв О.М., к.т.н., Минайленко Р.М., к.т.н., доц., Собінов О.Г., викладач
Центральноукраїнський національний технічний університет, м.Кропивницький

В автоматизованих системах сушіння зернових ключову роль мають визначені фізичні властивості матеріалів та устаткування. Однак, при використанні технологій сушіння рухомих мас, коли в процесі сушіння зерновий матеріал є рухомим, спостерігається явище значного відхилення локальних параметрів від середньостатистичного за рахунок неоднорідності розподілу вологості та щільності. Тому для врахування значних пікових відхилень постає **задача** при меншій кількості вимірів краще приблизитися до реального середньостатистичного показника з мінімальним запізненням.

Проведено порівняльний аналіз результатів вимірювання рухомих та нерухомих мас зерна. В результаті виявлено значно менший розкид показників вимірювання при нерухомих масах. Тому при реалізації приладу потрібно конструктивно передбачити порційний автоматизований відбір порцій зерна з потоку. Але автоматизація відбору не дає можливості контролювати якість проб, тому в пробах є присутніми мілкі інородні предмети, що залишилися в процесі очищення зернових, а також присутні локальні різкі зміни вологості та випадкові похибки самого сенсора. На основі проведених експериментів побудовано імітаційну модель результатів вимірювання:

$$W_k = W + R_k + I_k.$$

Тут використано позначення: W_k – результат вимірювання; W – реальне значення вологості зернової маси; R_k – випадкове відхилення вимірювання сенсору; I_k – випадкове імпульсне відхилення, характеризується ймовірністю виникнення та амплітудою (при наявності). Результат моделювання відповідає реальним даним і показаний на рис. 1.

Розглянуто фільтрування вхідної послідовності для отримання результату найближчого до дійсного за критерієм середньоквадратичного відхилення, латентності фільтру (запізнення, або швидкість реакції на зміну вхідних величин) та максимального відхилення. Було випробувано наступні фільтри: лінійний фільтр усереднення, медіанний фільтр та фільтр Калмана.

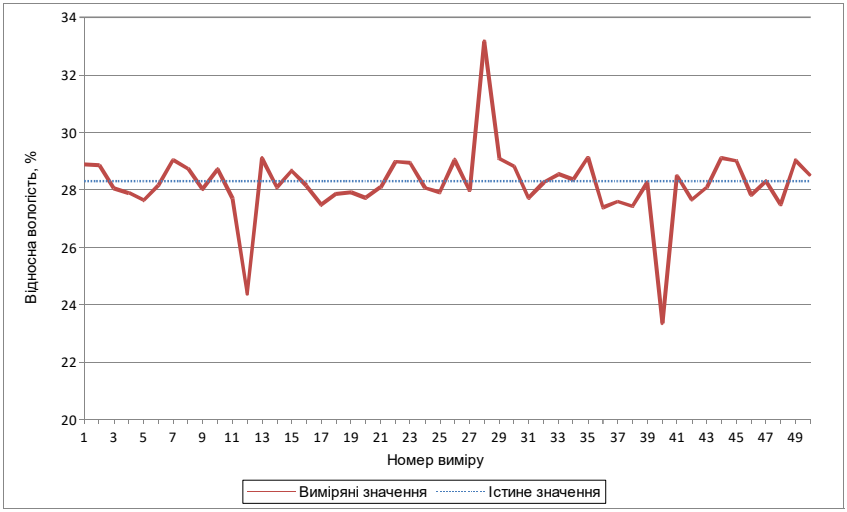


Рис. 1 – Результат моделювання вимірювання вологості

Оцінювання роботи фільтрів проводилося над багаторазовими реалізаціями «реального» сигналу, результат фільтрації порівнювався з поточними істинними значеннями. Також експеримент був повторений з різними лінійними змінами істинних значень під час вимірювання. Результати випробування надано в наступній таблиці:

Таблиця

Результати випробування фільтрів

	Усереднення	Медіанна фільтрація	Фільтр Калмана
Дисперсія	0,5702	0,3244	0,3163
Максимальне відхилення	1,484	0,6351	0,9671

Також роботу фільтрів наочно можна оцінити на типовому графіку результатів фільтрування вхідних даних, який представлено на рис. 2. Значним обмеженням у використанні вказаних фільтрів є малі значення апертури, інакше запізнення в отримані результатів вимірювання стають непридатними для систем автоматичного керування процесом сушіння зернових.

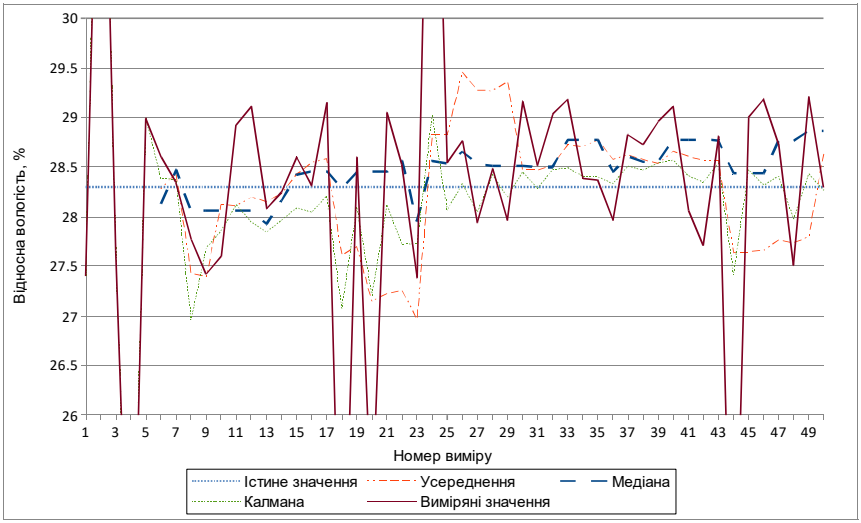


Рис. 2 – Демонстрація роботи фільтрів

Експерименти показали, що за критерієм мінімальності дисперсії різниці отриманих та істинних значень найкращим вибором є лінійний фільтр Калмана, хоча ця різниця і не велика. Однак за критерієм мінімізації максимального відхилення від істинних значень, значно кращі результати надає медіанний фільтр.

Висновки. В результаті показано, що для мікроконтролерних систем керування процесом сушіння зернових, більш доцільним є використання медіанного фільтру за критеріями мінімізації максимального та середньоквадратичного відхилення та простотою реалізації для мікроконтролерних систем, в яких часто не реалізують апаратну підтримку операцій з дійсними числами.

Список літератури

1. Kalman R.E. A New Approach to Linear Filtering and Prediction Problems // Transactions of the ASME–Journal of Basic Engineering. – Vol. 82 (Series D). – P. 35-45.

2. Прэтт У. Цифровая обработка изображений: Пер. с англ. — М.: Мир, 1982. — Кн. 2 — 480 с.

3. Hussain A., Khan M.A., Ul-Qayyum Z. Modified Directional Weighted Median Filter [Electronic resource]. – Access mode: https://pdfs.semanticscholar.org/41fb/652dfe2981fc5527677c53ae9aa468dd94eb.pdf

УДК 681.518

Створення мультимедійної гри засобами мови програмування Objective-C

Єлькін В.І., студент
Науковий керівник – Паращук С.Д., к.т.н., доцент
Центральноукраїнський державний педагогічний університет, м. Кропивницький

Програмувати додатки для операційних систем виробництва Apple можливо виключно за допомогою вбудованого середовища розробки XCode. Xcode – програма для розробки додатків під OS X і iOS з частково відкритими програмними компонентами, розроблена корпорацією Apple. Тобто, певною мірою Xcode є вільним програмним забезпеченням [3].

Основним додатком пакету є вбудоване середовище розробки, яке називається Xcode [9]. Крім цього, пакет Xcode включає в себе більшу частину документації розробника від Apple і Interface Builder – додаток, що використовується для створення графічних інтерфейсів (про нього мова йтиме далі) [8]. Пакет Xcode включає в себе змінену версію вільного набору компіляторів GNU Compiler Collection (GCC, apple - darwin9 - gcc - 4.0.1, який з липня 2012 р. більше не буде існувати в складі інструментарію розробників для OS X (в Xcode 4.4), і підтримує мови C, C + +, Objective - C, Objective - C + +, Java, AppleScript, Python і Ruby з різними моделями програмування, включаючи (але не обмежуючись) Cocoa, Carbon і Java [7]. Сторонніми розробниками реалізована підтримка GNU Pascal, Free Pascal, Ada, C #, Perl, Haskell і D [1].

Interface Builder - додаток від Apple для операційної системи Mac OS X. Він є частиною Xcode (колишній Project Builder), спеціальної системи інструментів для розробників Apple Developer Connection [6]. Interface Builder дозволяє Cocoa і Carbon розробникам створювати графічні інтерфейси для додатків. Результат розробки зберігається у файлі з розширенням. Nib, скорочення від NeXT Interface Builder, хоча останнім часом частіше використовується Xib [4].

Одним з центральних компонентів розробки мобільного програмного забезпечення є Cocoa, об'єктно-орієнтований прикладний програмний інтерфейс (API) для операційної системи Mac OS X виробництва компанії Apple [5]. Важливими є фреймворки (надбудови) Foundation.framework для забезпечення низькорівневої програмної взаємодії, CoreMedia.framework для керування медіавмістом гри, AVFoundation.framework для управління аудіоінфомацією та відеофайлами, MediaToolbox.framework (додатковий інструментарій для роботи з медіа), UIKit.framework, що надає доступ до елементів управління графічного користувацького інтерфейсу [2].

Проілюструємо можливості XCode, створивши мультимедійну розвиваючу гру для мобільної платформи жанрового типу «головоломки». Ігрову механіку програми проілюстровано на рис. 1.

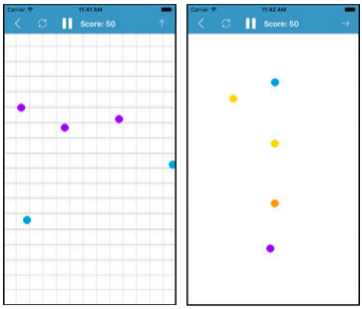


Рисунок 1 – зображення графічного інтерфейсу

Висновки. Можна переконатися, що за допомогою інстументів вбудованого середовища розробки XCode можливо створювати широкий клас програмних засобів для мобільних операційних систем, в тому числі й ігрового напряму. Передбачається можливість розширення програмного функціоналу створеного додатку шляхом введення нових пунктів головного меню програми, створення контролерів вікна, додавання елементів та бонусів тощо.

Список літератури

1. Кнастер С. Objective-C. Программирование для Mac OSX и iOS. – М.: Вильямс, 2012. – 304 с.

2. Конвэй Д. Программирование под iOS. – СПб.: Питер, 2011. – 608 с.

3. Кочан С. Программирование на Objective-C 2.0. – М.: ЭКОМ, 2012. – 608 с.

4. Лафоре Р. Объектно-ориентированное программирование в С. – СПб.: Питер, 2011. – 928 с.

5. Lim B.G., Mac Donell M.C. iOS 7 in action. – Manning, 2014. – 370 p.

6. Марк Д. Разработка приложений для iPhone, iPad и iPod touch с использованием iOS SDK. – М.: Вильямс, 2010. – 624 с.

7. Марк Д. iOS 5 SDK. Разработка приложений для iPhone, iPad. – М.: Вильямс, 2012. – 672 с.

8. Нахавандипур В. iOS. Разработка приложений для iPhone, iPad и iPod. – СПб.: Питер, 2010. – 864 с.

9. Нойбург М. Программирование для iOS 7. Основы Objective-C, Xcode и Cocoa. – М.: Вильямс, 2014. – 384 с.

УДК 681.518

Автоматизована система безпеки потоків дронів в умовах їх масового використання в міських умовах

Єршов В. В., аспірант
Науковий керівник – Ізвалов О. В., к.т.н., доцент
Льотна академія НАУ, м. Кропивницький

Дрон, у технологічному контексті, – це безпілотний літальний апарат. Формально дрони відомі як безпілотні літальні апарати (БПЛА) або безпілотні повітряні системи (БППС).

БПЛА можуть бути дистанційно керованими і можуть самостійно літати з вбудованим програмним забезпеченням (план польоту), працюючи в тісному зв'язку з бортовими датчиками та системами GPS.

У минулому безпілотні літальні апарати мали виняткове військове застосування, де їх спочатку використовували для знищення повітряних цілей та збирання розвідувальної інформації.

Станом на сьогодні безпілотники широко використовуються під час пошуково-рятувальних операцій, спостереження, моніторингу погоди, руху, пожежогасіння, для особистих цілей, бізнесу з акцентом на фото- та відеозйомці, у сільському господарстві та навіть у доставці вантажів.

Загальна концепція безпілотних літальних апаратів. У багатьох країнах світу розробляються і впроваджуються правила використання безпілотних літальних апаратів для регулювання польотів і ліквідації потенційних небезпек. Розглянемо законодавчі норми ряду держав.

Росія. З початку квітня 2016 року в Росії введена обов'язкова реєстрація БПЛА вагою понад 250 грам, включаючи іграшкові дрони. Їх реєстрацією займається Федеральна служба безпеки. Відповідний указ був прийнятий і підписаний 30.12.15. Власники безпілотних апаратів, як придбаних в Росії, так і ввезених на територію РФ з-за кордону, зобов'язані зареєструвати їх в контролюючому органі. У керівне відомство необхідно повідомити інформацію про країну-виробника дрона, його серійний номер, рік виготовлення, призначення апарату, максимальну злітну масу, а також тип, кількість і потужність двигунів. Крім цього, власникам БПЛА потрібно повідомити до ФСБ ім'я власника (або назву організації, якій належить безпілотник), дату і місце народження, а також його паспортні та контактні дані.

Білорусь. З 28 серпня 2016 набули чинності "Правила використання авіамоделей", які відрізняються значним рядом обмежень [1]. Зараз відбувається робота щодо пом'якшення деяких правил, однак вона поки не завершена, і операторам слід орієнтуватися на існуючі норми. З вересня 2017 року легально управляти дронами можуть виключно члени "Білоруської федерації безпілотної авіації". Незаконне управління дроном

передбачає штраф і конфіскацію апарату. Правила встановлюють поняття зон, де заборонене пілотування будь-яких літальних апаратів без дозволу державних структур, які мають безпосередній стосунок до таких зон. Про конкретний перелік таких зон можна дізнатися з документів Міністерства оборони і Міністерства транспорту і комунікацій. Перед здійсненням повітряної зйомки потрібно за три дні подати заявку в Міністерство оборони, а також отримати дозвіл від "Белаеронавігації" (воно включає також медичний дозвіл на пілотування). Крім обмежень по зонам польотів вводиться обмеження по висоті, що характерно для багатьох інших національних законів.

Ірландія. Починаючи з 21.12.15 всі дрони масою більше 1 кг повинні бути зареєстровані в Ірландській Авіаційній Агенції (IAA). Схожі положення діють також у ряді інших країн Європи.

Італія. В Італії діє заборона на використання квадрокоптера (для некомерційної зйомки, легше 25 кг) у місцях скупчення людей, в містах, поряд із залізничними вокзалами, аеропортами, військовими об'єктами, електростанціями та урядовими установами. Дозволяється запуск дронів на відкритому, добре видимому просторі в віддаленні не менше ніж 150 метрів від міської інфраструктури при постійному збереженні візуального контакту з апаратом. Заборонено наближатися більш ніж на 50 метрів до людей і об'єктів приватної власності. Зйомка заборонена в радіусі 8 км від аеропорту. Для комерційної зйомки необхідне прилбання ліцензії.

Австрія. В Австрії зони, дозволені для польотів, діляться на 4 категорії. Без ліцензії дозволено літати тільки на відкритих просторах (на природі) та поблизу сільськогосподарських угідь (ферм).

Чехія. У Чехії польоти дронів заборонені в містах та в місцях скупчення людей. БПЛА масою менше 7 кг дозволено запускати на безпечній відстані від людей і будівель, апарати масою від 7 до 20 кг повинні літати на відстані не менше 150 метрів від людей і будівель.

Законодавче регулювання польотів БПЛА в Україні. Державною авіаційною службою України (ДАС) розроблено "Концепцію регулювання напряму безпілотних повітряних суден" [2]. Подібні правила - FAR-107 - вже діють в США з серпня 2016 року. У травні 2017 року європейський регулятор European Aviation Safety Agency (EASA) опублікував проект свого документа з регулювання ринку.

У документі ДАС передбачено два види класифікації безпілотних літальних апаратів: за максимальною злітною масою і за типами управління. Згідно з першим критерієм є чотири категорії повітряних суден (ПС):

1) до 0,250 кг;
2) 0,25-20 кг;
3) 20-150 кг;
4) більше 150 кг.

За другим критерієм є ручний візуальний, ручний інструментальний і

автономний апарати. Крім того, передбачається, що будуть розрізняти комерційну і некомерційну експлуатацію.

При цьому можуть бути введені певні вимоги до операторів безпілотників. Власники літальних апаратів 1 класу (від 0,25 до 20 кг) можуть експлуатувати їх тільки в умовах прямого візуального контакту без додаткових пристроїв. Максимальна швидкість не повинна перевищувати 150 км/год при максимальній висоті польоту до 120 м і радіусі 500 м. Введено заборону на виконання польотів в 8-кілометровій зоні від периметра аеропорту, а також заборонених зонах. Використання БПЛА даного класу можливе тільки в світлий час доби.

Введено визначення дистанційного пілота і візуального спостерігача. Перший з них – це особа, яка маніпулює органами управління безпілотного повітряного судна під час польоту і має право остаточного рішення, а також несе відповідальність за безпеку БПЛА під час польотів. Другий – візуально спостерігає за ВС і надає інформацію про параметри його польоту дистанційного пілотові.

Для апаратів другого класу (20-150 кг) передбачається обов'язкова сертифікація в Державіаслужбі, сертифікація типу/вимоги льотної придатності і отримання сертифіката експлуатанта.

Автоматизований розрахунок безпеки руху БПЛА в повітряних умовах. За результатами аналізу наведених вище правил виникає необхідність автоматизувати оцінку безпеки польотів безпілотних літальних апаратів. Така автоматизація може бути досягнута шляхом адаптації моделі потоків повітряного руху, використаної в [3] для розробки тренувань у симуляторах керування повітряним рухом. Важливим є врахування різниці в продуктивності літаків і БПЛА, а також різниці між рівнями обслуговування повітряного руху в масштабах великих територій та в межах єдиного міста. В даний час ведеться розробка програмного забезпечення, яке включає ці моделі, дозволячи враховувати законодавчі норми на фактичній території, та розрахувати безпечні маршрути для безпілотних літальних апаратів відповідно до цих правил.

Програмне забезпечення містить карту поточного міського простору із загальними траєкторіями маршрутів, показаними чорними пунктирними лініями. Місця потенційних небезпечних зон показані червоними колами. Програмне забезпечення виявляє ці зони та оптимізує маршрути, щоб уникнути зіткнень між безпілотниками. Схема користувацького інтерфейсу системи подана на Рисунку 1.

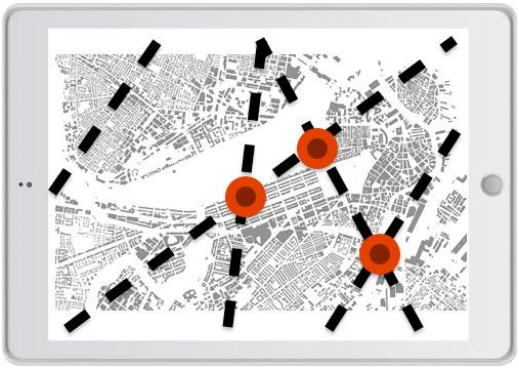


Рисунок 1 – Зображення графічного інтерфейсу

Програмне забезпечення призначене для роботи на мобільних пристроях. Можливі області застосування програмного забезпечення можуть включати розрахунок безпеки для відкриття нових повітряних трас, оцінку впровадження нових БПЛА, планування окремих маршрутів.

Висновки. Великий попит на комерційні та приватні безпілотники також спричинив і ряд проблем, пов'язаних з безпекою, наслідками зіткнень та втрати контролю. У зв'язку з цим багато країн на законодавчому рівні внесли ряд поправок до правил повітряного руху. З'явилися зони "No-fly".

Внаслідок різноманіття правових норм існує необхідність створення автоматичної системи для обчислення безпеки потоків безпілотників у міських умовах та для прогнозування безпечних маршрутів їх руху.

Список літератури

1. Использование авиамоделей в Республике Беларусь. Совет Министров Республики Беларусь; Постановление, Правила от 16.08.2016 No 636. – [Електронний ресурс]. – Режим доступу: http://government.by/upload/docs/fileaeab4fba05047ee0.PDF

2. Про затвердження Правил польотів повітряних суден та обслуговування повітряного руху в класифікованому [...]. Мінтранс України; Наказ, Правила від 16.04.2003 No 293. – [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/z0346-03.

3. Set of Software for Automatic Control System of the Air Traffic Modeling Complex / Aleksey Izvalov, Sergey Nedelko, Vitaliy Nedelko // Збірник наукових праць Кіровоградського націо- нального технічного університету. Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. - 2014. - Вип. 27. - С. 266-274. — [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/znpkntu_2014_27_41.

УДК 621.391

Обобщенные преобразования Хаара

Иванов В.Г., д.т.н., профессор
Национальный юридический университет имени Ярослава Мудрого, г. Харьков

Одним из наиболее фундаментальных и эффективных средств цифровой обработки сигналов являются методы обобщенных преобразований Фурье, которые обладают мощными декоррелирующими свойствами и алгоритмами быстрых вычислений [1]. Арсенал ортогональных преобразований постоянно пополняется новыми преобразованиями. Это связано с многообразием задач и необходимостью иметь широкий спектр преобразований с заданными свойствами. Главный недостаток классического преобразования Фурье – это интегральная оценка всех частотных составляющих спектра вне зависимости от времени их существования. Преобразование Фурье прекрасно подходит для стационарных сигналов, но не годится для нестационарных, у которых определённые частотные компоненты существуют только в определённые промежутки времени. В ряде случаев оказывается более удобным в качестве базисов разложения использовать такие системы функций, для которых коэффициенты разложения учитывают поведение исходной функции лишь в нескольких близкорасположенных точках [2]. Использование такого базиса по своей сути означает переход от частотного анализа к масштабному, т.е. исходная функция анализируется с помощью некоторой "стандартной" математической функции, изменяемой по масштабу и сдвигу на некоторую величину. Первое упоминание об этих функциях появилось в работах Хаара в 1910 году [2]. В 1980 году Гроссман и Марлет определили такие функции как Wavelet-функции (всплески). К wavelet-подобным функциям относятся и кусочно-постоянные функции Хаара, которые имеет наименьшую вычислительную сложность среди других быстрых ортогональных преобразований. Однако, на сегодняшний день отсутствуют простые аналитические формулы анализа и синтеза данных в обобщенной системе Хаара, когда число этих данных может быть как составным, так и простым числом. Решение этой задачи позволит внести определенный вклад в теорию ортогональных преобразований, а так же получать и исследовать новые свойства спектров для данных такого типа.

Известно [2], что любая функция $S(x)$, непрерывная на отрезке [0, T], разлагается в равномерно сходящийся ряд:

$$S(x) = \sum_{m=1}^{\infty} \sum_{j=1}^{2^{m-1}} C_{mj} \chi_{mj}(x), \qquad (1)$$

где C_{mj} – коэффициенты разложения функции $S(x)$ в ряд Фурье-Хаара.

Представим формирование сумм преобразования Хаара в виде следующего рекуррентного выражения [3]:

$$x_i^n = \sum_{k=2i-1}^{2i} x_k^{(n-1)}, \quad (2)$$

где $n = 1,2,..., (\log_2 N - 1)$, $i = 1,2,..., \frac{N}{2^n}$.

В этом выражении значения $x_k^{(0)}$ представляют собой исходные отсчеты сигнала. С учетом свойства локальности существования функций Хаара и формулы (2) коэффициенты Хаара можно вычислить следующим образом:

$$C_{mj} = \frac{1}{N} 2^{\frac{m-1}{2}} \left[X_k^{(\log_2 N - 1) - r} - X_{k+1}^{(\log_2 N - 1) - r} \right], \quad (3)$$

где $m = 1,2,..., \log_2 N$; $j = 2^{m-1}$, а для выражения, стоящего в квадратных скобках $r = m - 1$, а $k = 2j - 1$.

Тогда коэффициент C_{01} (свободный член) примет вид:

$$C_{01} = \frac{1}{N} \left[X_k^{\log_2 N - 1} + X_{k+1}^{\log_2 N - 1} \right]. \quad (4)$$

Приведенные выражения характеризуются однотипностью процедур, легко программируются, и являются частным случаем общей аналитической формы преобразований Хаара для произвольного числа точек , вывод которого приводится в работе.

Если число дискретных отсчетов сигнала равно четырем, то для нахождения коэффициентов Хаара можно записать систему уравнений [3]:

$$\begin{cases} C_1 + C_2 + C_3\sqrt{2} = d_1 & C_1 + C_2 - C_3\sqrt{2} = d_2 \\ C_1 - C_2 + C_4\sqrt{2} = d_3 & C_1 - C_2 - C_4\sqrt{2} = d_4 \end{cases}, \quad (5)$$

где $d_1 \ldots d_4$ – значения сигнала в дискретных точках; $C_1 \ldots C_4$ – коэффициенты Хаара.

При добавлении пятого отсчета сигнала d_5 первое уравнение системы (5) разбивается на два:

$$C_1 + C_2 + C_3\sqrt{2} + 2C_5 = d_1, C_1 + C_2 + C_3\sqrt{2} - 2C_5 = d_5. \quad (6)$$

Вычитая одно уравнение из другого, определим C_5 и подставим его значение, равное $(d_1 - d_5)/4$, в (6). После несложных преобразований система (6) сводится к двум уравнениям с одинаковыми правыми частями:

$$C_1 + C_2 + C_3\sqrt{2} = (d_1 + d_5)/2 \ , \ C_1 + C_2 + C_3\sqrt{2} = (\mathrm{d}_1 + \mathrm{d}_5)/2 \, , \tag{7}$$

которые могут быть заменены одним уравнением, аналогичным первому уравнению в (5) с правой частью $d^{(1)}$, равной $(d_1+d_5)/2$, то есть снова получим систему из четырех уравнений:

$$\begin{cases} C_1 + C_2 + C_3\sqrt{2} = d^{(1)} & C_1 + C_2 - C_3\sqrt{2} = d_2 \\ C_1 - C_2 + C_4\sqrt{2} = d_3 & C_1 - C_2 - C_4\sqrt{2} = d_4 \end{cases}. \tag{8}$$

Решив (8), найдем коэффициенты Хаара в виде:

$$\begin{aligned} &C_5 = (d_1 - d_5)/4; \ \ C_4 = (d_3 - d_4)/2\sqrt{2}; \ \ C_3 = (d_1 + d_5 - 2d_2)/4\sqrt{2}; \\ &C_2 = (d_1 + d_5 + 2(d_2 - d_3 - d_4))/8; \ C_1 = (d_1 + d_5 + 2(d_2 + d_3 + d_4))/8. \end{aligned} \tag{9}$$

В случае шести отсчетов сигнала будем также иметь систему из четырех уравнений:

$$\begin{cases} C_1 + C_2 + C_3\sqrt{2} = d^{(1)} & C_1 + C_2 - C_3\sqrt{2} = d^{(2)} \\ C_1 - C_2 + C_4\sqrt{2} = d_3 & C_1 - C_2 - C_4\sqrt{2} = d_4 \end{cases}, \tag{10}$$

где $d^{(1)}= (d_1+d_5)/2$; $d^{(2)}= (d_1+d_6)/2$ и т.д., до поступления $(2N-1)$-го дискретного значения сигнала.

Введем понятие базового вектора данных N^*, который определим по отношению к числу исходных входных отсчетов сигнала N как:

$$N^* = 2^n, \tag{11}$$

где n=1,2,…,($2^n \le N$), причем n должно давать min Ц($N/2^n$); Ц(•) – целая часть.

Тогда, в свою очередь, базовые исходные отсчеты сигнала x* будут формироваться из начальных входных отсчетов по правилу

$$\begin{aligned} &x^*_p = (x_p + x_{N^*+p})/2 \text{ , если p=1,2,…,(N-N*);} \\ &x^*_p = x_p \text{ , если p=(N-N*+1),(N-N*+2),…,N*.} \end{aligned} \tag{12}$$

С учетом свойств системы Хаара запишем получение соответствующих сумм преобразования Хаара в виде:

$$x_i^n = \sum_{k=2i-1}^{2i} x_k^{n-1}, \tag{13}$$

где n=1,2,…,(log N*-1); i=1,2,…,$N^*/2^n$; а x_k^0 – базовые отсчеты сигнала x_p^*.

Вычислив (13), определим коэффициенты Хаара:

$$C_{mj} = 2^{(m-1)/2} \Big/ N * \left[x_k^{(\log N-1)-m^*} - x_{k+1}^{(\log N-1)-m^*} \right] , \quad (14)$$

где m=1,2,…,logN; $j=2^{m-1}$, а для выражения, стоящего в квадратных скобках, m*=m-1, k=2j-1. С учетом принятой индексации коэффициент C_{01} (свободный член) запишется в виде:

$$C_{01} = 1 \Big/ N * \left[x_k^{\log N-1} + x_{k+1}^{\log N-1} \right]. \quad (15)$$

Остальные коэффициенты определятся по формулам:

$$C_{N^*+i} = (x_i - x_{N^*+1}) / N^* , \quad (16)$$

где i=1,2,…,(N-N*), x(·) – исходные отсчеты сигнала.

Полученные в работе соотношения образуют единую алгоритмическую методику обобщенного спектрального анализа и синтеза сигналов в базисе Хаара любой размерности и позволяют повысить эффективность систем обработки или защиты данных по тем или иным критериям.

Список литературы

1. Агаян С.С. Успехи и проблемы быстрых ортогональных преобразований (для обработки сигналов изображений) // Распознавание, классификация, прогноз. Математические методы и их применение. – М.: Наука, 1992. – Вып. 3. – С. 146-215.

2. Соболь И.М. Многомерные квадратурные формулы и функции Хаара/ И.М. Соболь. – М.: Наука, 1970. – 288 с.

3. Іванов В.Г. Формальное описание дискретных преобразований Хаара / В.Г. Іванов // Проблемы управления и информатики. – Київ, 2003. – № 5, – С. 68-75.

УДК 004.9

Создание нового лабораторного учебного стенда изучения SCADA систем

Имнаишвили Л.Ш. д.т.н., проф., руководитель департамента компьютерной инженерии,
Бединеишвили М.М., д.т.н., проф.,
Годердзишвили Г.И., д.т.н.,проф., руководитель учебно-научно-экспертной лабораторий факультета информатики и систем управления,
Иашвили Н.Г., руководитель центра автоматизации
Грузинский технический университет, г. Тбилиси, Грузия

В Грузинском техническом университете разработан и изготовлен стенд для проведения лабораторных работ по изучению **SCADA** систем.

С точки зрения ведения учебных занятий предлагаемый лабораторный стенд дает возможность изучить следующие вопросы:

- управление COM-портом PC;
- функционирование интерфейса RS-485;
- функционирование MODBUS;
- функционирование программируемых логических контроллеров;
- программирование логических контроллеров в стандарте IEC 61131-3;
- функционирование стандартного пакета программного обеспечения Trace Mode;
- мониторинг и управление объектом в режиме реального времени;
- функционирование баз данных в режиме реального времени;
- конфигурирование программируемых логических контроллеров как в ручную так и от PC;
- функционирование арифметики с фиксированной и плавающей запятой;
- измерительные микропроцессорные устройства;
- функционирование промышленных компьютерных систем;
- интерфейс человек/PC.

В настоящее время в вузах обучение SCADA систем ведется с помощью виртуальных и реальных учебных стендов. Как показывает опыт, виртуальные учебные материалы не дают возможность полностью изучить вопросы проектирования подобных систем, в последствии, все таки приходиться провести практические занятия на реальных системах. Физические учебные стенды одновременно дают возможность изучить как вопросы проектирования SCADA систем, так и их эксплуатации. В первом случае стенды можно применять для обучения студентов с компьютерной инженерной ориентацией, во втором случае – для

технологов, с целью изучения вопросов эксплуатации. В первом случае студенты должны глубоко знать аппаратные и программные вопросы проектирования SCADA систем, имея при этом представление о технологическом процессе. Технологи должны глубоко знать технологические процессы, имея при этом некоторое представление об аппаратных и программных средствах SCADA систем.

Для проведения лабораторных работ предусмотрено применение следующих программных пакетов:

- SCADA Conect, который был разработан специально для лабораторного стенда, который используется для изучения COM-порта ПК, интерфейса RS-485 и протокола MODBUS.
- LPConfig software (компания Lumel), который используется для изучения конфигурирования мультифункциональных блоков.
- eCon software (компания Lumel), который также используется для изучения конфигурирования мультифункциональных блоков.
- Trace Mode (производитель фирма AdAstra), который используется для создания SCADA-проектов.

Согласно протоколу MODBUS требуется наличие в системе одного ведущего и одного или нескольких ведомых устройств. В случае лабораторного стенда PC – ведущие устройство, а ведомыми устройствами являются: преобразователь стандартных и температурных сигналов P30U, преобразователь параметров питания однофазной сети P30P, блоки ввода бинарных сигналов SM5 и их вывода SM4.

Лабораторное рабочее место SCADA представляет собой систему микропроцессорных устройств и персонального компьютера, связанных между собой последовательным интерфейсом RS-485. Открытая архитектура предлагаемого лабораторного SCADA стенда позволяет расширить её функциональные возможности. Указанный стенд дает возможность реализовать SCADA систему по традиционной схеме, реализуемой по следующей последовательности: рабочее место оператора - канал связи - устройства ввода-вывода - исполнительные объекты и сенсоры. Архитектура системы основана на продукции компании Lumel.

С точки зрения функциональных возможностей, разработанный стенд дает возможность изучать чрезвычайно широкий спектр вопросов.

Ясно, что функциональные возможности лабораторного стенда SCADA систем не исчерпываются перечисленными выше вопросами. Его возможности полностью будут раскрыты и расширены на практике. Кроме того, открытая архитектура стенда дает возможность добавить в структуре другие модули или специальные физические модели технологических процессов.

УДК 004.75:004.455

Технологія предиктивного аналізу на основі IoT та BIGDATA

Івченко Р.А., аспірант
Науковий керівник – Купін А.І., д.т.н., професор
ДВНЗ «Криворізький національний університет» м. Кривий Ріг

Методи BIGDATA надають можливість обробки структурованих і неструктурованих даних дуже великих обсягів для отримання результатів, ефективних в умовах безперервного приросту, розподілених за вузлами обчислювальної мережі. Необхідність використання таких методів викликана все більшим розвитком технологічності процесів та самого обладнання на підприємствах. Використовуватися вони можуть для збору інформації з датчиків задля предиктивних аналізів, упорядкування даних. Також використовуються в цілях підвищення безпеки та модульності (наприклад, у цілях попередження поломок обладнання).

Відомі технології включають в себе [3]:

1. Розпізнавання графічних елементів як нову частину імплементації розпізнавання голосу.
2. Адаптивні роботи та пов'язані автоматизовані транспортні засоби.
3. Напівавтоматичні, гнучкі машини для додаткових послуг.
4. Повністю автоматизоване забезпечення якості для пристосування до швидких змін у попиті.
5. Розумне, автоматичне управління об'єктами для більшої ефективності.
6. Підвищення безпеки та модульність.

Підвищення безпеки на виробництвах є апріорним за важливістю. Тому головним чином підвищення безпеки можливе завдяки предиктивному аналізу для запобігання нештатних ситуацій.

SAP Predictive Analytics [2] в останні роки сфокусувалася на розвитку машинного навчання, обробці великих даних і розвитку IoT. Це три найважливіших технологічних напрямки, які компанія розвиває в своїх рішеннях. SAP працює не тільки над розвитком інструмента, але і на застосуванні цих технологій на практиці. Наявність великої кількості клієнтів, автоматизації свого бізнес-процесу на продуктах SAP, дозволяє аналізувати клієнтські потреби комплексно, пропонувати нові підходи у використанні клієнтських даних для збільшення ефективності бізнес-процесів.

Можна завантажити тимчасовий ряд в інструмент аналізу даних, але без попередньої обробки даних отримана модель буде невисокої якості. При підготовці даних необхідно виконання двох етапів обробки. Перший етап – це Data Engineering, тобто збір, розуміння, очищення та первинна обробка даних. Другий етап – Feature Engineering: формування описових

ознак до даних, які містять інформацію про різні аспекти поведінки об'єкта, модель якого будується. З точки зору методології CRISP-DM [2] ї ці етапи аналогічні до Data Understanding і Data Preparation.

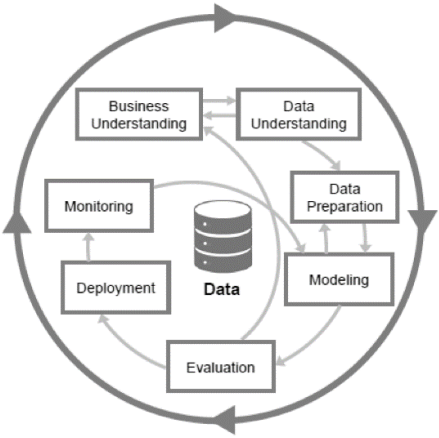


Рисунок 1 – Кроки методології CRISP-DM з можливими напрямками переходу між етапами [2]

Невід'ємною частиною початкових етапів процесу машинного навчання є відбір ознак (feature selection), тобто змінних, на основі яких навчається модель. Відбір може здійснюватися за допомогою різних інструментів, а також залежати від безлічі факторів, наприклад, таких як кореляція ознак з цільової змінної або якість даних. Наступним (і більш важливим) кроком може стати створення нових ознак на основі вже наявних, т.зв. feature engineering – інжиніринг, створення ознак. Ця операція може дозволити інженерам поліпшити якість моделі, одночасно отримавши більш повне пояснення даних, у разі, якщо модель інтерпритована. У нашому випадку першим етапом побудови моделі в SAP Predictive Analytics стало створення нових ознак за допомогою вбудованого рішення Data Manager.

У підготовленому наборі даних є показники індикаторів, які впливають на цільову змінну в поточний момент часу. Однак, можна отримати додаткову інформацію, якщо встановити вплив цих індикаторів за певний період до поточного моменту. У нашому випадку були обрані тимчасові інтервали: за 1 годину і за 1 день до поточного моменту в часі. Ще більш інформативною може виявитися ступінь зміни індикаторів від моменту в минулому до поточного моменту. У якості методу був обраний натуральний логарифм приватного поточних індикаторів та індикаторів з інтервалом 1 годину і 2 дні. Отже, вдалося отримати ступінь зміни індикатора від моменту в минулому (збільшився він або зменшився, і

якщо так, то наскільки).

Резюмуючи, зазначимо, що вдалося встановити не тільки залежність між поточними значеннями індикаторів і цільової змінної, але і взяти до уваги ці індикатори в минулому, а також ступінь їх зміни.

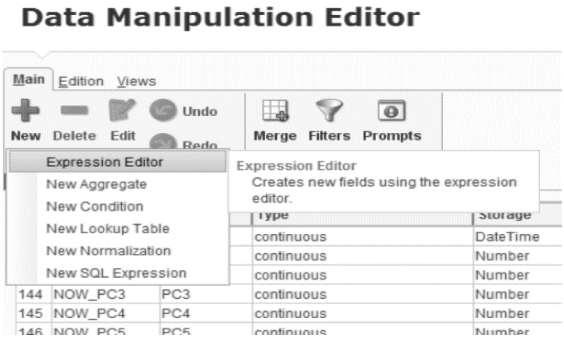


Рисунок 2 – Створення нового виразу в Data Manipulation Editor [4]

У Expression Editor додається функція зсуву дати по годинах (для другої змінної – по днях), для кожної з яких виставляється залежне поле "date" (від якого йде обчислення), а також параметр "-1", тому що нас цікавить минуле.

Висновки. Було сформулювано технології роботи з BIGDATA. Моделювання SAP Predictive Analytics буде важливе в процесі збору інформації з датчиків обладнання та можливості в подальшому його аналізу, наприклад, на його справність.

Проведено огляд технологій та моделей керування бізнес процесів, у ході аналізу яких наведені рекомендації, які будуть використовуватися для предиктивного аналізу в умовах BIGDATA.

Список літератури

1. SAP predictive analysis: what it can and cannot do [Електронний ресурс]. – Режим доступу: https://www.asug.com/news/sap-predictive-analysis-what-it-can-and-cannot-do

2. Как предсказать курс рубля к доллару при помощи SAP Predictive Analytics [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/company/sap/blog/345108/

3. Comparison of metadata editors [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Comparison_of_metadata_editors

4. What is the CRISP-DM methodology? [Електронний ресурс]. – Режим доступу: https://www.sv-europe.com/crisp-dm-methodology/

УДК 004.41:004.056

Розробка методу передтестової компіляції й розподілу доступу

Коваленко О.В., доцент кафедри, к.т.н., доцент,
Коваленко А.С., старший викладач, к.т.н.,
Смірнов О.А., завідувач кафедри, д.т.н., професор,
Смірнов С.А., старший викладач, к.т.н.
Центральноукраїнський національний технічний університет, м. Кропивницький

Проведені дослідження показали, що в процесі керування розробкою програмного забезпечення, проектування, реалізації, верифікації, а також тестування безпеки програмного забезпечення існує ряд загальних і спеціальних рекомендацій розроблених і випробуваних на практиці експертами.

Серед них можна виділити наступні: керування якістю, інжиніринг вимог безпеки, моделювання загроз, аналіз атак, аналіз уразливостей у наявному коді, перевірка вхідних даних, забезпечення безпеки компілятором, статичний аналіз, що проникає тестування, аудит коду, розробка керівництва й контрольних списків розроблювачів, незалежний огляд безпеки й ін.

Аналіз представлених рекомендацій показав, що здебільшого вони зачіпають відомі розроблювачам ситуації безпеки. У той же час вони не враховують можливостей безпосередньої тестової роботи кодерів-розроблювачів програмного забезпечення в рамках методів «смокі»-тестування й передтестової роботи в рамках компіляції програмного коду.

У той же час, як показують дослідження, саме в рамках передтестової роботи існують додаткові можливості підвищення безпеки програмного забезпечення за рахунок обліку профілю програм і користувачів, а також оптимізації системи розподілу доступу до досліджуваних даних.

У рамках розроблювального методу розподілу доступу при оптимізації з обліком передкомпіляційного профілю програми відбувається необхідний збір даних, формованих у безлічі профілів користувачів.

Для підвищення точності обліку профілів користувача, специфіки його діяльності й характеристик комп'ютерної системи пропонується розбивка процесу компіляції на дві фази:

– фаза синтезу програмного забезпечення з урахуванням можливостей сучасних компіляторів;

– фаза адаптації й розподілу доступу до програмного забезпечення з урахуванням профілів програми й користувача.

Такий поділ передтестової компіляції на дві фази дозволить вирішити наступні завдання:

1. Розподіл доступу користувачів з урахуванням можливостей

персоналізації відповідних профілів.

2. Облік внутрішніх характеристик комп'ютерної системи користувачів (архітектури, планувальника команд, і ін.).

3. Облік можливостей розподілу доступу при складанні й підтримці програмного забезпечення.

Для рішення завдань динамічної машинно-незалежної оптимізації доцільно скористатися відомою технологією компіляції LLVM.

З літератури відомо, що в рамках цієї технології представлені:

– статичний компілятор;

– компонувальник;

– віртуальна машина;

– ЛТ-компілятор.

Функціонування системи забезпечується єдиною внутрішньою структурою, що може бути проілюстрована в текстовому форматі, у формі структур даних в оперативній пам'яті, а також у двійковому виді як біт-код.

Цей біт-код може бути збережений у проміжних об'єктних файлах для подальшої оптимізації, у тому числі динамічної.

При цьому можливо використовувати всі надавані LLVM можливості по обробці внутрішнього подання (включаючи різні аналізи, трансформації й т.п.).

Тому інфраструктура LLVM надає зручну базу для досліджень по динамічній оптимізації програм.

У запропонованому методі передтестової компіляції й розподілу доступу в першій фазі виконується процедура машинної-незалежної компіляції з використанням LLVM. Результат першої фази зберігається у файл LLVM і додатково генеруються дані про архітектуру програмного засобу й алгоритми можливої інсталяції.

Виконання другої фази можливо з використанням програмних засобів віртуального моделювання (віртуальних машин), а так само безпосередньо на комп'ютерних системах користувачів з урахуванням особливості їхніх профілів і характеристик обчислювальних засобів.

Таким чином, розроблений метод передтестової компіляції й розподілу доступу користувача, що відрізняється від відомих обліком профілів, при синтезі додатка, а також використанням ресурсів «хмарних сховищ» у процесі одержання інсталяційних версій. Це дозволить підвищити рівень безпеки розроблювальних додатків.

УДК 004.9

Дослідження різновиду пошукової оптимізації сайту Social media optimization

Конопліцька-Слободенюк О.К., викладач
Центральноукраїнський національний технічний університет, м. Кропивницький

Соціальні мережі є нині одними з основних медіа середовищ. І, звичайно, маркетологи хочуть більше знати про користувацьку аудиторію соціальних мереж та належно це використовувати.

Користувачі ж соціальних мереж все більше починають довіряти тій соцмережі в якій зареєстровані. Деяким зручно переглядати новини, деяким якісь соціальні та доброчинні проекти. Існує навіть теорія, що Дональд Трамп виграв на виборах в президенти через те, що його піар-менеджери грамотно побудували піар-кампанії в Facebook і Twitter. Також, наприклад, сотні тисяч людей збиралися на київському Майдані Незалежності в 2013-му після закликів в патріотично налагоджених групах. Іноді, навіть, завдяки зворушливим історіям, розміщеним на сторінках соцмереж рятуються людські життя. Отже, маркетологи починають звертати увагу на цю інформацію, проводячи дослідження аудиторії користувачів. І тут можна виділити три напрямки: опитування, вивчення статистики в групах, аналіз отриманих результатів. Ці дані допомагають вимірювати кількість відгуків і коментарів під записами; виділяти самі обговорювані тематики за заданий відрізок часу; складати рейтинг авторів по індексу соціальної залученості, знаходити продукти конкурентів зі схожої тематики.

З розвитком соціальних мереж і інтеграцією сайту компаній зі співтовариствами, виникла необхідність в оптимізації сайту для залучення відвідувачів з соцмереж. Один з методів оптимізації – Social media optimization (SMO) – спрямований саме для того, щоб створити додаткові можливості для сайту та популяризувати його в мережі.

Концепція полягає в тому, що сайт оптимізують не для пошукових машин, а для блогів і співтовариств, щоб на нього посилалися в соціальних мережах та робили цитування у блогах, отже контент з сайту повинен просто поширюватись в соціальну мережу. Це, вирішують кнопками "Мені подобається" або "Поділитися".

Завдання, які потрібно вирішити, щоб SMO був ефективним:

- Технічна перевірка сайту. Це дозволить виявити сильні та слабкі сторони та зупинитись на правильній стратегії.

- Наповнення сайту. Контент сайту повинен бути корисним і зручним для сприйняття з оптимально-правильним підбором ключових слів, та інтригуючими заголовками.

- Зв'язане посилання. Внутрішнє зв'язування сторінок покращує пошук по сайту. Це вигідно, як відвідувачам так і, навіть, пошуковим системам.

- Інструменти SMO. Це соціальні кнопки, плагіни, форми коментарів і підписки на розсилку. Цей пункт є одним з найважливіших.

- Карта сайту. Сайт має кращу презентабельність, якщо додати посилання на найпопулярніші матеріали, що найбільше коментуються, і на нові публікації. Відвідувачам подобається така презентація і багато хто дійсно проходять по запропонованих посиланнях.

Переваги використання SMO:

- орієнтованість на користувачів (сайт розробляється так, щоб пошукові системи змогли легко знаходити потрібну інформацію, що може привести до погіршення отримання інформації для користувачів);

- "вірусний" ефект (у соціальних мережах інформація про сайт розноситься блискавично за рахунок кнопок "Мені подобається", реп остів, а від SMO подібного чекати не доводиться);

- якість трафіку (люди, що прийшли на ваш сайт з соціальних мереж, частенько більше "цільові", ніж ті, хто відвідав веб-портал через пошукову видачу);

- кращий результат при мінімальних витратах (по-перше, SMO - просування дає свої плоди куди швидше. чим пошукова оптимізація; по-друге, не варто забувати і про фінансову сторону питання: соціальне просування обходиться дешевше, ніж пошукове);

- просте розкручування. SMO.

Недоліки використання SMO:

-обов'язкове розкручування (співтовариство, створене для розкручування веб-порталу, саме потребує популяризації. Це займає час і віднімає досить багато сил);

- постійна підтримка співтовариств(у соціальних мережах треба контролювати те, що відбувається в співтоваристві та постійно підтримувати "життя");

- стримування негативу (вміння стримувати негативні відгуки і коментарі - обов'язкова навичка власників груп, чого не скажеш про звичайне просування);

- недостатня вивченість (сьогодні SMO тільки починає свій розвиток, тому іноді ще відчувається дефіцит фахівців).

Насправді ж, якщо оптимально і грамотно поєднати всі напрями, це дозволить в найкоротші терміни розкрутити сайт, охопивши усі аспекти та задіявши всі способи залучення аудиторії на веб-порталі.

УДК 004.056.53

Дослідження методів візуалізації графів

Константинова Л.В., викладач,
Мелешко Є.В., канд. техн. наук, доцент
Центральноукраїнський національний технічний університет, м. Кропивницький

Візуалізація інформації є на сьогоднішній день ключовим моментом у багатьох додатках в науці і техніці. Одним із способів, що дозволяють візуалізувати складні дані, є використання графів [1]. Графи допомагають представляти інформацію в наочному і зручному для розуміння вигляді, і зараз, задача розробки алгоритмів та систем їх візуалізації є актуальною. Зробити огляд вже існуючих способів візуалізації графів є необхідним кроком для вирішення цієї задачі.

Різноманітність видів графів породжує відмінності способів відображення графів.

Прямолінійне представлення буде кращим для графів, наприклад, з невеликим числом вершин і відповідною кількістю ребер (міська система доріг може служити прикладом). У випадку графа соціальної мережі, буде недостатньо прямолінійного способу відображення, через велику кількість дуг.

Відомі способи відображення графів [2]: довільне відображення; прямолінійне (ребра представляються відрізками); сіткове; полігональне (ламані використовують для відображення ребер; ортогональне (ребра видаються ламаними, відрізки яких – вертикальні або горизонтальні лінії); планарне; висхідне та низхідне (для орієнтованих графів).

Естетичні критерії визначають параметри відображення. Найбільш поширені серед них [2]:

• Перетинання: мінімізація загальної кількості перетинів ребер. В ідеалі, якщо це можливо, повинно бути отримано планарне відображення.

• Області: мінімізація розмірів областей.

• Загальна довжина ребер: мінімізація сумарної довжини всіх ребер.

• Максимальна довжина ребер.

• Універсальна довжина ребер: мінімізація відмінностей в довжинах ребер.

• Загальна кількість вигинів: зменшення загальної кількості вигинів.

• Максимальна кількість вигинів.

• Кутова роздільна здатність.

• Характеристичне відношення.

• Симетрія.

Відомо багато програмних засобів для відображення графів такі як: Graphviz[3], yEd [4], WilmaScope 3D [5], Walrus [6], GVF - The Graph

Visualization Framework[7], uDraw(Graph) [8], Comp.compilers: tools for graph visualization [9], Cytoscape [10], i2 Analyst's Notebook [11], Sentinel Visualizer [11], CrimeLink [11], Xanalys Link Explorer [11] и Tom Sawyer Software [11]. Хоча присутні деякі відмінності в деталях, за функціональністю і призначенням ці системи візуалізації багато в чому схожі.

Можна виділити дві загальні первинні області - робочий простір (пул, що містить взаємопов'язані елементи даних) і панель інструментів (масив властивостей, елементів меню).

Існують загальні вторинні ознаки, які можуть бути використані для опису функціональності GVS (Graph Visualization Software), такі як:

Підтримка викладення графів у тривимірному просторі, як додаток до планових малюнків за замовчуванням.

Можливість автоматичного розміщення елементів графа відповідно до відомих макетів (силове, ортогональне, деревоподібне та інше) та чи включені ці макети (як для Wilmascope 3D) або вимкнено (як для Graphviz) за замовчуванням.

Підтримка створення кластерів та підграфів для розпаду та розширення структурних частин великих графіків для спрощення розуміння та маніпулювання (як для Wilmascope 3D та yFiles).

Можливість активувати пост-обробку вже візуалізованих структур графа, щоб виділити окремі ділянки тіла графа – збільшувальну лінзу, гіперболічний вид зору і т. д.

Підтримка імпорту та експорту вироблених макетів з/до відомих мов опису графіків (GML, GDL).

Можливість відтворювати вміст робочої області у растровому форматі (наприклад, BMP, JPG або PDF), векторний формат (наприклад, SVG) або відправити його безпосередньо на пристрій друку.

Підтримка анімації динамічних процесів в графіках, наприклад - Petri Nets (як для yFiles, так і для aiSee).

Можливість імпортувати сторонні плагіни для розширеної функціональності GVS (як для Tulip).

Підтримка налаштування вторинних параметрів GVS (таких як чутливість вхідних пристроїв або індивідуальні параметри макета) [12].

i2 Analyst's Notebook, CrimeLink, Sentinel Visualizer і Xanalys Link Explorer є програмними продуктами, призначеними для аналізу систем взаємопов'язаних об'єктів і вивчення динаміки послідовних подій. Tom Sawyer Software представляє собою набір бібліотек для створення інструментів візуалізації і аналізу мереж з різних предметних областей. У перерахованих вище системах спостерігається ряд недоліків: відсутність переносних рішень, відсутність власних спеціалізованих сховищ, а також те, що системи не орієнтовані на роботу з графами великих розмірів [11].

Висновки. Графи застосовуються для моделювання різноманітних об'єктів і зв'язків між ними в самих різних областях науки і техніки.

Зробивши аналіз деяких сучасних пакетів GVS можливо викласти рішення щодо інтегрованої бази даних загальних компонентів, які могли б допомогти у складанні нового GVS для представлення інформації в більш наочному і зручному для розуміння вигляді.

Список літератури

1. Костина М.А., Мельникова Е.А. Алгоритмы искусственного интеллекта в задаче визуализации графа // Вектор науки ТГУ, 3(41), 2017 [Електронний ресурс]. – Режим доступу: КиберЛенинка: https://cyberleninka.ru/article/n/algoritmy-iskusstvennogo-intellekta-v-zadache-vizualizatsii-grafa.

2. Di Battista G., Eades P., Tamassia R., Tollis I.G. Graph Drawing: Algorithms for the Visualization of Graphs. – Prentice-Hall, 1999. – 397 p. ISBN 0-13-301615-3.

3. Graphviz - Graph Visualization Software [Електронний ресурс]. – Режим доступу: http://www.graphviz.org/documentation/.

4. yWorks the diagramming company. yEd Graph Editor [Електронний ресурс]. – Режим доступу: http://www.yworks.com/products/yed.

5. WilmaScope [Електронний ресурс]. – Режим доступу: http://wilma.sourceforge.net/.

6. Walrus - Graph Visualization Tool [Електронний ресурс]. – Режим доступу: http://www.caida.org/tools/visualization/walrus/.

7. GVF - The Graph Visualization Framework [Електронний ресурс]. – Режим доступу: http://gvf.sourceforge.net/.

8. uDraw (Graph) - The powerful solution for graph visualization [Електронний ресурс]. – Режим доступу: http://www.informatik.uni-bremen.de/uDrawGraph/en/uDrawGraph/uDrawGraph.html.

9. Tools for graph visualization - summary [Електронний ресурс]. – Режим доступу: https://compilers.iecc.com/comparch/article/96-09-043.

10. Cytoscape [Електронний ресурс]. – Режим доступу: http://download.cnet.com/Cytoscape-64-bit/3000-2054_4-75749785.html.

11. Коломейченко М.И., Чеповский А.М. Визуализация и анализ графов больших размеров // Бизнес-информатика. 2014. – №4(30). – [Електронний ресурс]. – Режим доступу: https://cyberleninka.ru/article/n/vizualizatsiya-i-analiz-grafov-bolshih-razmerov

12. Zabiniako V., Rusakov P. Definition of General Requirements for Graph Visualization Softwar. – 2012. – [Електронний ресурс]. – Режим доступу: http://lib.znate.ru/docs/index-40230.html.

УДК 644.12

Автоматизована система енергоопалення житлових приміщень

Коренко О.О., студент 5-го курсу,
Іщенко М.О., к. т.н., доцент
ДВНЗ «Криворізький національний університет», м. Кривий Ріг

Зараз у нашій країні гостро постає питання ціни за використовуване опалення в житлових приміщеннях оскільки виросла ціна за газ. Один із варіантів зменшення витрат на опалення – застосування електробатарей, при їх використанні ціна за електрику може бути знижена, це вигідно для споживачів і для українських постачальників газу, оскільки їм буде потрібно закупати менший об'єм газу.

За допомогою «Wi-Fi Wireless Smart Switch for MQTT COAP Smart Home» (SONOFF) можна настроїти автоматичне ввімкнення та вимкнення електробатареї для досягнення цільової температури, яка задається на сервері зі встановленим OpenHAB. Зв'язок між SONOFF та OpenHAB виконується через технологію Wi-Fi за допомогою протоколу MQTT, який використовується в місцях, де необхідно передавати невеликі повідомлення, обмеженої пропускної здатності мережі. При сумісному використанні цих технологій, наприклад, можна задавати потрібну температуру кімнати перед приходом додому з телефону через Інтернет.

SONOFF оснований на контролері ESP-8266. Основні характеристики наведено в таблиці 1. Даний контролер прошивається через USB-UART користувачем.

Таблиця 1 – Основні характеристики SONOFF

Напруга:	~90-250В (50/60Гц)
Максимальний струм:	10А
Максимальна потужність:	2200 Вт
Розміри:	88* 38* 23 мм
Вологість:	5%-95%
Протоколи WiFi:	802.11. b/g/n
Робоча температура:	-20℃ +75℃

Для забезпечення можливості автоматичного досягнення необхідної

температури використано датчик температури DS1820, його діапазон вимірюваних температур від -55 С до +125 С та абсолютна похибка перетворення менше 0,5 С.

Спроектовано апаратну частину автоматизованої системи енергоопалення житлового приміщення для проекту будівлі, що складає 24.9 м^2, загальна ціна проекту склала 5020 гривень, в таблиці 2 наведено ціни за елементи системи.

Таблиця 2 – Економічні затрати на реалізацію проекту

Назва	**Кількість**	**Загальна ціна**
ТСМ-450	2	2390 грн
ТСМ-400	1	1195 грн
SOnOff	2	358 грн
DS1820	4	368 грн
Силовий кабель ВВГ –нг-3х2 5 мм^2	39,22 м	709 грн
Загальна ціна		5020 грн

Висновки

Розглянуто автоматизовану систему енергоопалення на основі сумісного використання пристрою SONOFF та серверу на OpenHAB. Було розглянуто основні характеристики сучасного автоматичного приладу. Дана технологія буде використана для проектування автоматизованої системи енергоопалення в житлових приміщеннях.

УДК 004.432+004.942+519.254

Автоматизована інформаційна система обчислення моделей різної складності

Куницька С.Ю., к.т.н., доцент,
доцент кафедри інформаційної безпеки та комп'ютерної інженерії
Черкаський державний технологічний університет, м. Черкаси

Головним питанням, що розглядається в доповіді є розробка так званого програмного інструменту, тобто фільтру прогнозування, у вигляді автоматизованої інформаційної системи, що дозволяє обробляти вхідні дані у вихідну інформацію, які описані на математичному рівні за допомогою обчислення полінома Колмогорова-Габора [1]:

$$\varphi = a_0 + \sum_{i=1}^{m} a_i x_i + \sum_{i=1}^{m}\sum_{j=1}^{m} a_{ij} x_i x_j + \sum_{i=1}^{m}\sum_{j=1}^{m}\sum_{k=1}^{m} a_{ijk} x_i x_j x_k + \ldots \quad (1)$$

Головна задача, яка поставлена в роботі – це автоматизація обчислювального процесу щодо обрахунку нелінійних систем відомим методом найменших квадратів та приведення систем рівнянь до нормалізації з метою подальшої роботи фільтру прогнозування.

Інформаційну систему розроблено об'єктно-орієнтованою мовою програмування C# з підтримкою інтегрованого середовища Visual Studio Professional 2017 на платформі .NET, вона має досить зручний інтерфейс користувача, що дозволяє автоматизувати процес обробки інформації та містить необхідні для роботи кнопки управління [2].

Найпростіший програмний інтерфейс дає змогу вносити та аналізувати історичні данні необхідні для подальшого дослідження, а також не тільки автоматизувати процес обчислення моделей, але й зберігати всю необхідну інформацію по отриманню навчених моделей різної складності, що й зображено на рисунку 1. Діапазон необхідних даних обирається з файлу Excel, куди попередньо було занесено масив вхідних даних.

Особливість роботи даної інтерфейсної частини полягає в тому, що кожна кнопка управління є обов'язково активною. Розглянемо, наприклад, роботу блоку «Вхідні дані», де описуються вхідні дані, в якому користувач має змогу:

- завантажити ряд – тобто заявити про конкретний масив даних, який може бути необмеженого об'єму вхідних значень. В нашому випадку наведено приклад для масиву, що складається зі 100 значень;

- обирати діапазон ряду, тобто це ті важливі експериментальні точки, що внесено до Excel, як вхідні дані. При цьому ми обираємо будь-який діапазон ряду, але точок обраних повинно бути не менш ніж 10. Це так

званий мінімальний набір для необхідного обчислення [2];

- вибирати опорний вигляд моделі, тобто управлінська кнопка «Кількість невідомих» спочатку дозволяє обрати необхідну кількість невідомих аргументів із загального виду полінома, що описано формулою (1), а вже потім програма автоматично виводить на інтерфейс конкретну модель, на основі якої і відбувається подальше обчислення [3].

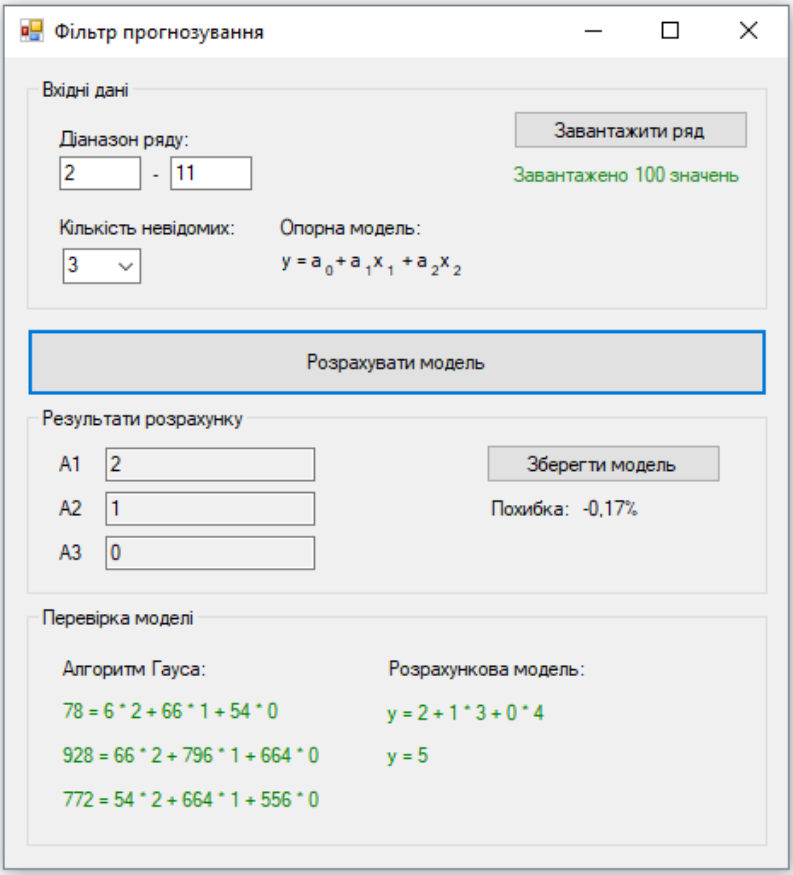


Рисунок 1 – Інтерфейс користувача

Блок 2 – «Розрахувати модель», дозволяє отримати результати розрахунку у вигляді перелічених невідомих аргументів при обраній моделі певної складності. На рисунку 1 представлені результати обчислення опорної моделі з трьома невідомими, яка має наступний вигляд (2):

$$y_k = a_0 + a_1 x_i + a_2 x_j \quad (2)$$

Також в програмному алгоритмі автоматизована функція перевірки, тобто підстановка отриманих значень аргументів як до нормалізованої системи, так і до опорного виду полінома обраної складності. Управлінська кнопка «Зберегти модель» необхідна подальшого розгляду історичних даних, необхідних для аналізу обчислювального процесу.

Також інтерфейс має кнопку обчислення похибки, що представляє собою середнє квадратичну похибку прогнозу для перевірки прогнозованої послідовності [3].

Зрозуміло, що програмний алгоритм значно полегшує обчислення складних систем, а його графічне представлення у вигляді інтерфейсу надає візуальне розуміння процесу, це спрощує аналізування історичних даних та обрання в подальшому необхідних методів дослідження.

Висновок: завдяки розробленій автоматизованій інформаційній системі було показано роботу програмного алгоритму, як інструменту прогнозування, що дозволив не тільки отримати досить простий і зручний програмний інтерфейс користувача, але й повністю автоматизувати процес за наступними складовими: обрання діапазону експериментальних точок, вибір опорного виду поліному в залежності від кількості невідомих аргументів полінома, та отримання моделі на основі сформованої нормалізованої системи рівнянь, що необхідна для подальшої роботи програми.

Список літератури

1. Куницька С.Ю. Приведення системи умовних рівнянь до нормалізації // Проблеми інформатизації: тези доп. п'ятої міжнародн. наук.-техн. конф., Черкаси, 13-15 листопада 2017 року. – Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2017. – С. 60.
2. Ивахненко А.Г., Юрачковский Ю.П. Моделирование сложных систем по экспериментальным данным. – М.: Радио и связь, 1987. – 120 с.
3. Куницька С.Ю. Технологія обробки інформації нормалізованих систем / С.Ю. Куницька // Вісник Черкаського державного технологічного університету. Серія: Технічні науки. – 2017. – №4. – С. 94-98.

УДК 004.1032

Підготовка даних виділення алгоритму з бінарного коду для аналізу безпеки програмного забезпечення

Лисиця Д.О., аспірант
Науковий керівник – Семенов С.Г., д.т.н., с.н.с.
Національний технічний університет "Харківський політехнічний інститут", м. Харків

Аналіз останніх світових подій, що пов'язані з інформаційною безпекою показав, що практично кожна сучасна IT-структура має певні уразливості до кібератак. При цьому існує певна тенденція збільшення кібератак, що досягли своєї зловмисної цілі. На погляд авторів, це багато в чому пов'язане з недостатністю уваги, що приділяється питанням тестування безпеки програмного забезпечення (ПЗ), а також різночитанням фахівців-розробників програмного забезпечення самої сутності терміну та функцій тестування безпеки ПЗ.

Не знижуючи важливості цих принципів та не обмежуючи вказаної в цих джерелах [1–2], основної стратегічної мети тестування безпеки ПЗ, слід зауважити, що деякі організації-розробники ПЗ при тестуванні безпеки зосереджуються лише на звісних зовнішніх факторах і моделюючи різні ситуації використовують, наприклад, такі способи етичного хакінгу:

– спроби дізнатися пароль за допомогою зовнішніх засобів;

– атака системи за допомогою спеціальних утиліт, які аналізують захист;

– придушення, приголомшення системи (з розрахунком, що вона відмовиться обслуговувати інших клієнтів);

– цілеспрямоване введення помилок в надії проникнути в систему в ході відновлення;

– перегляд і аналіз несекретних даних в надії знайти ключ для входу в систему.

Це визначає актуальність розробки методу виділення алгоритму з бінарного коду з використанням додаткових трас для аналізу безпеки програмного забезпечення.

Загальна структура виділення алгоритму з бінарного коду схематично представлена на рис 1.

Проведені дослідження [1, 2] показали, що при аналізі простих програм часто досить застосувати процедуру один раз. У складних випадках вона повинна застосовуватися ітеративно.

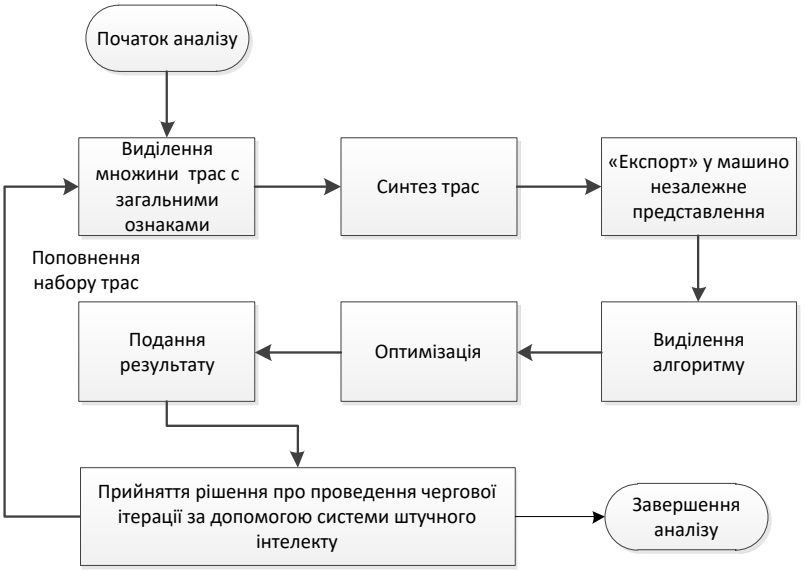


Рисунок 1 – Схема відновлення алгоритму

Як видно з рисунку, відновлення алгоритму починається з підготовки вихідних даних та виділення множини трас з загальними ознаками. Далі проводиться синтез інформації про досліджувану систему з вихідних трас за допомогою графового підходу представлення у системі. Після цього відбувається «експорт» коду в машино-незалежне представлення, на базі якого проводиться виділення тієї частини коду, яка відноситься до досліджуваного алгоритму. При цьому застосовуються оптимізаційні рішення, що спрощують отримане представлення та, нарешті, результат представляється у вигляді, придатному для перегляду аналітиком та використання у системі підтримки прийняття рішення з використанням штучного інтелекту. У цей момент аналітиком приймається рішення про проведення чергової ітерації аналізу або його завершення.

Висновки. Таким чином, етап підготовки даних виділення алгоритму з бінарного коду є дуже важливим у процесі аналізу безпеки ПЗ.

Список літератури

1. Лисица, Д. А. Модель оценки риска разработки программного обеспечения / Д. А. Лисица, С. Г. Семенов // Матеріали XV Міжн. НТК «Проблеми інформатики і моделювання». – 2015. – С. 82.

2. Лисица, Д. А. GERT–модель начальной генерации кода кибератаки несанкционированного доступа к ресурсам компьютерной системы одноранговой сети / Д.А. Лисица, С.Г. Семенов, А.В. Мовчан // Вісник Національного технічного університету «ХПІ». – 2016.–№44(1216).– С.147–161.

УДК 004.38

Створення вбудованої системи на базі мікрокомп'ютера Raspberry PI

Манжара В.В., старший лаборант
Черкаський національний університет ім. Б. Хмельницького, м. Черкаси

Вбудована система – це спеціалізована комп'ютерна система або обчислювальний пристрій, призначений для виконання обмеженої кількості функцій. Такі пристрої широко використовуються в побуті та на виробництві. Вбудовані системи можуть бути як малими (наприклад, портативні музичні програвачі або цифрові годинники), так і великими (світлофори, пристрої керування виробництвом). Часто вбудовані системи призначені для виконання обмеженої кількості функцій. Апаратна частина для цих систем розробляється спеціально під функції, які треба виконувати. Це дозволяє досягти високої продуктивності та надійності. Однак розробка апаратного забезпечення не є одним з найдешевших варіантів створення вбудованих систем. До того ж, така система проектується каскадно, тобто всі можливі функції повинні бути закладені під час проектування, та не можуть бути змінені, додані чи прибрані після створення системи. В більшості випадків значно дешевше та зручніше буде взяти за основу універсальний контролер, та на його базі створити вбудовану систему. Це дозволить зекономити не лише кошти, але і час, що піде на розробку самої системи, а не лише апаратної частини. До того ж, готові комп'ютери дають змогу застосувати ітераційний метод розробки, коли можливо додати функції, яких не було на етапі проектування, або необхідність цих функцій виявлено вже на етапі експлуатації системи. Одним з таких універсальних контролерів є мінікомп'ютер Raspberry PI.

Raspberry PI це одноплатний комп'ютер, розроблений британським фондом Raspberry Pi Foundation. Його головне призначення – стимулювати навчання базових комп'ютерних наук у школах. Дуже швидко цей комп'ютер, через ціну та можливості, став популярним не лише в освітній сфері, а і в ентузіастів та малих підприємствах. Raspberry PI має USB порти, що дозволяють підключати пристрої введення інформації, такі як цифрова клавіатура чи маніпулятор "миша", HDMI для підключення пристроїв виведення зображення, Ethernet-порт, що дозволяє під'єднатись до мережі Інтернет. Також, деякі моделі мають шини для дисплеїв та камер, Wi-Fi, Bluetooth. Окремо варто зазначити про GPIO піни, за допомогою яких можна підключити різні датчики та сигнальні пристрої, по типу світлодіодів. Всі ці інтерфейси дозволяють створити гнучку систему, яку можна розвивати та, без заміни апаратного забезпечення, удосконалювати систему.

Raspberry PI працює на видозміненій операційній системі Linux, що розроблена спеціально для цього комп'ютера. Це дозволяє використовувати як термінал для забезпечення швидкодії у випадках, коли нам не потрібно відображати інформацію (наприклад, під час розробки системи розумного дому), так і розробити користувацький інтерфейс для відображення змін в реальному часі (наприклад, при розробці системи контролю на виробництві).

Розробка програмного забезпечення системи ведеться на мові Python. Python інтерпретована об'єктно-орієнтована мова програмування високого рівня зі строгою динамічною типізацією. Структури даних високого рівня разом із динамічною семантикою та динамічним зв'язуванням роблять її привабливою для швидкої розробки програм, а також як засіб поєднання існуючих компонентів. Python підтримує модулі та пакети модулів, що сприяє модульності та повторному використанню коду. Інтерпретатор Python та стандартні бібліотеки доступні як у скомпільованій, так і у вихідній формі на всіх основних платформах. Основними перевагами мови Python є:

- чистий синтаксис;
- стандартний дистрибутив, який має велику кількість корисних модулів;
- можливість використання мови в діалоговому режимі;
- відкритий код.

Для Raspberry PI розроблено спеціальну операційну систему – Raspbian. У операційній системі Raspdian вже є середовище розробки Python. Готовий програмний продукт не обов'язково запускати щоразу через це середовище. Достатньо додати збережений скрипт в автозавантаження. При завантаженні операційної системи, яка стартує достатньо швидко, запуститься скрипт, який буде керувати системою.

Отже, з появою на ринку одноплатних комп'ютерів розробка вбудованих систем стала набагато простішою, адже не потрібно розробляти апаратне забезпечення. Достатньо взяти готовий виріб та розробити вбудовану систему. Також роботу полегшує той факт, що навколо raspberry PI створилось потужне співтовариство, а це означає, що в мережі можна легко знайти потрібну інформацію. Raspberry PI ідеально підходить для малосерійного виробництва або вбудованих систем під замовлення.

УДК 681.5.015

Алгоритми визначення середньозваженого розміру руди в процесах подрібнення-класифікації

Мацуй А.М., канд.техн.наук, доцент
Центральноукраїнський національний технічний університет
м. Кропивницький

Вступ. Україна входить в десятку країн за кількістю продукції чорної металургії, більше половини якої випускається з магнетитового концентрату рудозбагачувальних фабрик, значна частина якого імпортується в інші країни. Залізорудні збагачувальні фабрики України є найбільшими в світі, в той же час в даній галузі накопичились і певні проблеми. Зокрема, вітчизняний залізорудний концентрат поступається за собівартістю порівняно з продукцією інших економічно розвинутих країн. Однією з важливих причин такого стану є недостатній рівень автоматизації технологічних процесів, особливо подрібнення руди. Найбільшими втратами відрізняється перша стадія подрібнення руди, яка в основному здійснюється у кульових млинах, що працюють у замкненому циклі з механічними односпіральними класифікаторами. Гальмом у розвитку автоматизації виступає відсутність деяких інформаційних засобів, зокрема ведучих, датчиків крупності подрібненої руди. Оскільки нині такі засоби відсутні, а галузь несе значні збитки, тема даної роботи є актуальною. Робота присвячена отриманню даної інформації.

Викладення основного матеріалу. При автоматизації процесів подрібнення руди в першій стадії важливо на необхідному рівні, який змінюється, підтримувати розрідження пульпи у кульовому млині, оскільки це впливає як на роботу куль, так і на швидкість проходження матеріалу, що подрібнюється, вздовж барабана технологічного агрегату. При визначенні рівня розрідження пульпи ведучим параметром є середньозважена крупність матеріалу, що поступає на подрібнення. Визначення середньої крупності матеріалу на вході технологічного агрегату в певній мірі здійснюється лише у випадку стержневих млинів, які працюють у розімкненому циклі. У замкненому циклі даний параметр ніколи не визначався, оскільки на вході кульового млина зустрічається два потоки – суха крупна до 25 мм вихідна руда і піски класифікатора, крупність яких незначна і вони вологі, містять близько 12% води. Крупність циркулюючих пісків також автоматично ніколи не вимірювалася. В таких технологічних циклах робилися спроби вимірювання крупності лише вихідної руди. Вимірювання не відрізнялися високою точністю. Вивчення даної проблеми показало, що задача є достатньо складною і її розв’язання можливе лише на рівні використання сучасних мікропроцесорних засобів.

Спочатку здійснювалися спроби розв'язання задачі визначення середньозваженої крупності дробленого матеріалу на вході кульового млина. Доведено, що середньозважену крупність подрібненого матеріалу на вході кульового млина можливо визначити за середньозваженими крупностями вихідного живлення та пісків механічного спірального класифікатора, а також масовими витратами вихідної руди та пісків. Ці дані перевірені і доведені в ході технологічного експерименту у виробничих умовах. Алгоритмічна схема визначення середньозваженого розміру твердого на вході кульового млина приведена на рис. 1. В алгоритмі використані наступні параметри: d_A, d_B – відповідно середньозважений розмір руди вихідного живлення та пісків механічного односпірального класифікатора; Q_A, Q_B – відповідно масові витрати вихідного живлення та пісків класифікатора. Масову витрату вихідного живлення можливо виміряти достатньо точно однороликовими конвеєрними вагами з фільтром Калмана-Б'юсі [1]. Забезпечити високу точність вимірювання масової витрати пісків класифікатора проблематично, однак знайдені підходи для суттєвого підвищення точності вимірювання цього технологічного параметра, що буде достатньо для даних умов [2]. Більш складно виміряти середньозважені крупності вихідного живлення та пісків класифікатора.

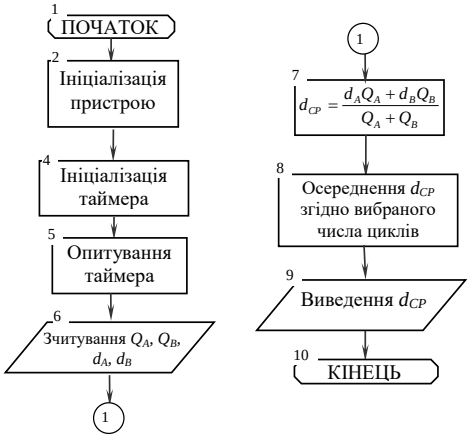


Рисунок 1 – Алгоритмічна схема визначення середньозваженого розміру твердого на вході кульового млина

Раніше здійснювалися спроби вимірювання середньозваженої крупності вихідного живлення кульового млина, однак їх точність для даного випадку недостатня. У зв'язку з цим розроблявся новий підхід визначення крупності руди на конвеєрній стрічці. Він виявився більш вдалим, дозволяє визначити середньозважену крупність вихідного живлення за рядом технологічних, конструктивних і двома виміряними

параметрами. Алгоритмічна схема визначення середньозваженого розміру дробленого матеріалу показана на рис.2.

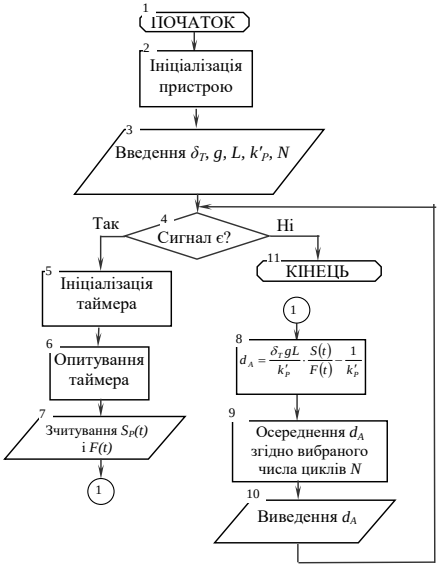


Рисунок 2 – Алгоритмічна схема визначення середньозваженого розміру дробленого матеріалу

В алгоритмі (рис.2) для визначення середньозваженого розміру вихідної руди використовуються наступні параметри: δ_T – густина руди; g – прискорення земного тяжіння; L – відстань між опорними роликами конвеєрних вагів (звичайно L=1 м); k'_P – постійний коефіцієнт, що визначаться особливостями розпушення руди; $S(t)$ – площа поперечного перерізу матеріалу на конвеєрній стрічці; $F(t)$ – погонне навантаження руди на конвеєрній стрічці; N – число циклів, обране з технологічних умов.

Крупність пісків механічного односпірального класифікатора ніколи не вимірювалася і це складає достатньо непросту задачу. В процесі досліджень запропоновано пристрій вимірювання середньозваженої крупності пісків класифікатора та алгоритм обробки його сигналів. Основу пристрою складає магнітна система з постійним магнітом і двома полюсними наконечниками, які створюють в пісках магнітне поле невеликого об'єму. При переміщенні такого датчика вздовж пісків з постійною швидкістю в обмотках, розташованих на полюсних наконечниках, індукується е.р.с., пропорціональна середньозваженому розміру пісків. Перетворювачем Холла; встановленим в магнітній системі, компенсується вплив зміни вмісту магнетиту в твердому на величину е.р.с. Алгоритмічна схема визначення крупності пісків односпірального класифікатора приведена на рис.3. В

алгоритмі (рис.3) для визначення середньозваженого розміру пісків використані сигнали перетворювача Холла $U_Ф$, задавача нормативного сигналу $U_З$ та е.р.с. індукційної обмотки магнітної системи $U_і$.

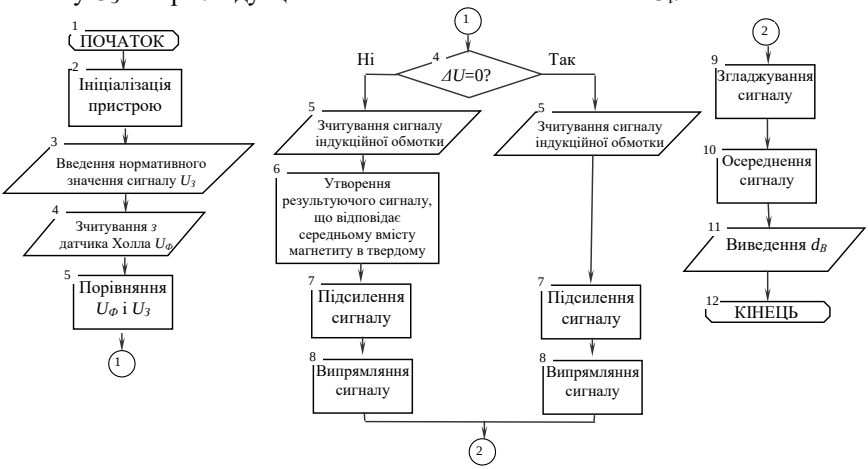


Рисунок 3 – Алгоритмічна схема визначення середньозваженої крупності пісків механічного односпірального класифікатора

Розроблені алгоритмічні схеми і підходи вимірювання параметрів дозволяють з використанням мікропроцесорних засобів здійснити визначення середньозваженої крупності матеріалу, який направляється на подрібнення в кульовий млин.

Висновки. Таким чином, вперше розроблено підходи і алгоритми визначення середньозваженого розміру руди в процесах її подрібнення і класифікації, що дозволяє автоматичне керування цими процесами підняти на якісно новий рівень і цим внести ще одну лепту у майбутнє зниження собівартості вітчизняних залізорудних концентратів.

Список літератури

1. Кондратець В.О. Вимірювання рудного завантаження млинів конвеєрними вагами з подвійною фільтрацією сигналу погонного навантаження / Кондратець В.О. // Електротехнічні та комп'ютерні системи. – К.: Техніка, 2014. – №13. – С. 62-69.

2. Кондратець В.О. Віртуальне визначення характеристик потоку в пісковому жолобі односпіральних класифікаторів / В.О. Кондратець, А.М. Мацуй // Радіоелектроніка, інформатика, управління. – Запоріжжя: ЗНТУ, 2017. – №1. – С. 24-32.

УДК 004.6

Дослідження методів побудови рекомендаційних систем заснованих на фільтрації контенту

Мелешко Є.В., канд. техн. наук, доцент
Центральноукраїнський національний технічний університет, м. Кропивницький

На сьогоднішній день у мережі Інтернет для таргетованої реклами товарів та послуг все частіше використовуються рекомендаційні системи.

Рекомендаційна система – програмне забезпечення, що використовується для прогнозування того, які об'єкти (товари, веб-сайти, фільми, новини тощо) будуть цікаві користувачу, на основі зібраної про нього інформації.

Існують 3 основні типи рекомендаційних систем в мережі Інтернет [1]:

1. Засновані на контентній фільтрації (content-based filtering).
2. Засновані на колаборативній фільтрації (collaborative filtering).
3. Гібридні методи.

Контентна фільтрація формує рекомендації на основі поведінки користувача, наприклад, на основі того, які веб-сторінки він відвідував раніше, які оцінки поставив товарам тощо. Такі рекомендаційні системи беруть до уваги схожість об'єктів з інформацією відомою про користувача.

Інформація про кристувача може бути отримана з його профілю та/або зібрана з його дій на веб-сайті – написаних відгуків та коментарів, придбаних товарів, переглянутих веб-сторінок тощо.

Для створення рекомендацій такі системи аналізують інформацію про користувача, формують ключові слова про його інтереси та вподобання. Рекомендуватися будуть об'єкти з бази даних, вибрані на основі визначених ключових слів.

Основні методи класифікації, на основі яких може бути здійснена контентна фільтрація [1, 2]:

1. Класифікатори на основі Байєсівських мереж.
2. Класифікатори на основі нейронних мереж.
3. Класифікатори на основі дерев рішень.
4. Класифікатори на основі алгоритмів кластеризації.

Класифікатори на основі Байєсівських мереж. Одним з найвідоміших класифікаторів є наївний байєсівський класифікатор. В його основі лежить ймовірнісна модель теореми Байєса. Для роботи алгоритмів з використанням даного класифікатора необхідно створити модель Байєса для кожного користувача, який оцінював будь-які об'єкти, на основі ознак цих об'єктів (для фільмів це можуть бути актори або жанри, для новин – ключові слова тощо). Для знаходження найбільш

ймовірної категорії необхідно обчислити умовні ймовірності приналежності будь-якого об'єкту до кожної категорії і вибрати ту, яка має найбільшу ймовірність:

$$Pr(\mathrm{C}|O) = \frac{Pr(O|\mathrm{C})\cdot Pr(\mathrm{C})}{\Pr(\mathrm{O})}, \quad (1)$$

$$Pr(O|\mathrm{C}) = \prod_{i=1}^{n} Pr(W_i|\mathrm{C}), \quad (2)$$

де O – об'єкт (товар, послуга тощо); C – категорія; W – слово (ознака); n – кількість слів (ознак); Pr(C) – повна ймовірність того, що випадково обраний об'єкт потрапляє у катергорію C; Pr(O) – повна ймовірність появи об'єкту O; $Pr(W_i|C)$ – умовна ймовірність того, що при наявності слова W_i в описі об'єкту O, об'єкт O відноситься до категорії C.

Для кожної категорії можна задати порогові значення. Тоді щоб новий об'єкт був віднесений до деякої категорії, ймовірність його віднесення до цієї категорії повинна бути більша ймовірності його потрапляння в будь-яку іншу категорію на величину порогового значення.

Перевагою байєсівських класифікаторів є можливість навчання, простота алгоритму навчання, можливість перегляду даних про важливість ознак, одержану в процесі навчання. Основний недолік – неможливість враховувати залежність результату від поєднань ознак.

Класифікатори на основі нейронних мереж.

Для контентної фільтрації можна використати, наприклад, багатошаровий перцептрон, якщо є дані для попереднього навчання і мережу Кохонена, якщо доведеться вчити мережу в процесі використання. Розглянемо загальну структуру перцептрону для використання у контентній фільтрації (рис. 1). Входами нейромережі будуть коди ознак об'єктів A = {a_1, a_2, … a_n}, а виходами – коди категорій об'єктів C = {c_1, c_2, … c_m}.

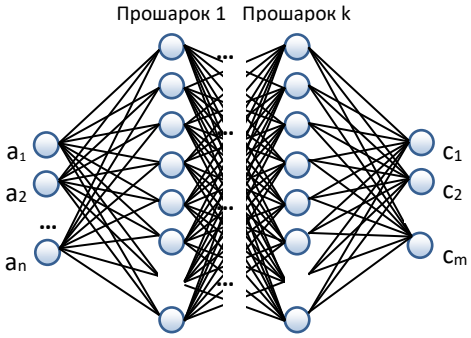


Рис. 1. Загальна схема нейронної мережі для класифікації об'єктів у рекомендаційній мережі

Нейромережа буде містити декілька прихованих прошарків, кількість

прошарків та нейронів у них зазвичай визначаються експериментальним шляхом. Загальною є рекомендація, що кількість нейронів у прихованих прошарках має бути більшою за кількість нейронів у вхідному прошарку.

Зазвичай при побудові нейронної мережі всі вузли створюються заздалегідь. У контентній фільтрації для рекомендаційних систем в [2] пропонується новий прихований вузол створювати тоді, коли зустрічається нова комбінація ознак та створювати для нього зв'язки з вагами за замовчуванням.

Нейронні мережі здатні справлятися зі складними нелінійними функціями та знаходити залежності між різними вхідними даними. Нейронні мережі допускають адаптивне навчання в процесі використання. Основні недоліки – вони працюють як чорний ящик, відсутні тверді правила по вибору структури та розміру мережі, швидкості навчання.

Класифікатори на основі дерев рішень. Дерево рішень – це модель, яка являє собою сукупність правил для прийняття рішення, в даному разі – рішення, до якої категорії віднести об'єкт [1]. Графічно її можна уявити у вигляді дерева, де вузли – умови переходу, а листки – назви категорій. Якщо для даного об'єкту умова у вузлі істина то здійснюється перехід по лівому ребру, якщо ж ні, то по правому. Залежно від рішення, прийнятого у вузлах, об'єкт відноситься до певної категорії.

Метод дерев рішень реалізує *принцип рекурсивного поділу*. Ця стратегія також називається «розділяй і володарюй». У вузлах, починаючи з кореневого, вибирається ознака, значення якої використовується для розбиття всіх даних на 2 класи. Процес триває до тих пір, поки не виконається критерій зупинки. Це можливо в таких ситуаціях:

– Всі (або майже всі) дані даного вузла належать одному і тому ж класу;

– Не залишилося ознак, за якими можна побудувати нове розбиття;

– Дерево перевищило заздалегідь заданий «ліміт зростання» (якщо ліміт було встановлено).

Існують різні чисельні алгоритми побудови дерев рішень. Одним з найбільш відомих є алгоритм під назвою C5.0 [3], розроблений програмістом Джоном Квінланом. Фактично алгоритм C5.0 є стандартом процедури побудови дерев рішень. Ця програма реалізується на комерційній основі, але версія, вбудована в пакет R доступна безкоштовно.

Дерева рішень корисні не тільки для класифікації, а також і для інтерпретації результатів. На відміну від баєсівського класифікатору легко спраправляються з взаємозалежними ознаками. Але дерева рішень не підтримують адаптивне навчання в процесі використання.

Класифікатори на основі алгоритмів кластеризації. Кластеризація (кластерний аналіз) – це задача розбиття множини об'єктів на групи, які називаються кластерами. Методи кластерного аналізу діляться на: ієрархічні та ітеративні [1, 4]. Ієрархічні в свою чергу поділяються на агломеративні і дивізимні.

Ієрархічні агломеративні методи послідовно об'єднують окремі об'єкти в кластери.

Ієрархічні дивізимні методи кластеризації полягають, навпаки, у виділенні в окремий кластер об'єктів, що мають найменші показники схожості, при тому, що спочатку вся мережа розглядається як окремий кластер.

Перевагами ієрархічних методів кластеризації є їх наочність і можливість отримати детальне уявлення про структуру даних. Недоліки ієрархічних методів кластеризації – обмеження об'єму набору даних; вибір міри близькості; негнучкість отриманих класифікацій. Ієрархічні методи використовуються при невеликих об'ємах наборів даних. При великій кількості даних вони не придатні. У таких випадках використовують ітеративні методи.

Ітеративні методи – методи кластеризації, в яких кластери формуються виходячи з умов розбиття, які можуть бути змінені користувачем для досягнення бажаної цілі. Ці методи можуть призвести до утворення перетину кластерів, коли один об'єкт може одночасно належати декільком кластерам.

Найбільш поширений метод ітеративної кластеризації – *метод k-середніх*.

Ітеративні методи можна використовувати для великих об'ємів даних, також вони виявляють вищу стійкість по відношенню до шумів і викидів, некоректного вибору метрики, включення незначущих змінних в набір, що беруть участь в кластеризації. Недоліком ітеративних методів є те, що треба заздалегідь визначити кількість кластерів. Якщо невідоме число кластерів, треба використовувати ієрархічні алгоритми, або декілька разів використати ітеративні методи з різною кількістю кластерів.

Перевагою контентної фільтрації є те, що для початку роботи рекомендаційної системи не потрібно великої кількості зареєстрованих користувачів. Головним недоліком даного підходу є неможливість системи рекомендувати нові об'єкти, які не прив'язані до інтересів користувачів.

Список літератури

1. Jones M. Recommender systems, Part 1. Introduction to approaches and algorithms. Learn about the concepts that underlie web recommendation engines [Electronic resource] / M. Jones. – 2013. – Access mode: https://www.ibm.com/developerworks/opensource/library/os-recommender1/ index.html? s_tact=105agx99&scmp=cp

2. Сегаран Т. Программируем коллективный разум. Пер. с англ. – СПб: Символ-Плюс, 2013. – 368 с.

3. C5.0: An Informal Tutorial [Electronic resoursce]. – Access mode: https://www.rulequest.com/ see5-unix.html

4. Глибовець М.М., Олецький О.В. Штучний інтелект: Підручник. – К.: Вид. дім "КМ Академія", 2002. – 366 с.

УДК 004.3

Сучасні пристрої вимірювання вологості зерна. Проблеми та пошук рішень

Минайленко Р.М., к.т.н., доцент, Дрєєв О.М., к.т.н., доцент,
Собінов О.Г., викладач
Центральноукраїнський національний технічний університет, м. Кропивницький

На теперішній час на вітчизняних зернопереробних підприємствах використовуються прилади для одноразового вимірювання вологості, (стаціонарне лабораторне обладнання), або мобільні (ручні) прилади.

Серед зарубіжних виробників поточних вологомірів сипучих матеріалів можна виділити німецьку компанію SWR Engineering. В моделях вологомірів німецької компанії запроваджена система безконтактного вимірювання висоти насипу матеріалу, що транспортується по конвеєрній стрічці. Завдяки цьому вимірювач вологості стає повністю незалежним від режимів роботи конвеєра, продовжуючи здійснювати точні вимірювання вологості потоку

Мікрохвильові вологоміри застосовуються для вимірювання вологості матеріалів в бункерах та інших технологічних ємностях, спускових жолобах, трубах, при гвинтовій подачі матеріалу і навіть безпосередньо в технологічному процесі. Для цього створені спеціальні модифікації вимірювачів.

Мікрохвильовий вимірювач вологості M-Sens 2 відрізняється простою налаштування та калібровки. Завдяки стійкості до ударного впливу і до підвищеної вологості, гарантується висока експлуатаційна надійність і великий строк служби датчика. Керамічний диск, що захищає вікно сенсору, забезпечує стійкість до абразивної дії, а також до надлишкового тиску.

Принцип дії поточного вимірювача вологості M-Sens 2 (рис.1) полягає

Рисунок 1 – Принцип дії вологоміра M-Sens 2

у вимірюванні напруги високочастотного поля та прямої цифрової обробки сигналу, що забезпечує високий ступінь розширення.

Оскільки поверхнева і капілярна вологість матеріалу сильно впливає на його провідність, вологість може бути точно виміряна через усереднену об'ємну щільність.

Калібровка виконується оператором шляхом натискання кнопки і введення відомого опорного значення вологості. Флуктації значення, що вимірюється, викликані зміною об'ємної щільності матеріалу. Вони усуваються шляхом фільтрації сигналу. Також в сенсорі передбачена автоматична компенсація впливу температури.

Система вимірювання вологості складається з наступних компонентів (рис.2):

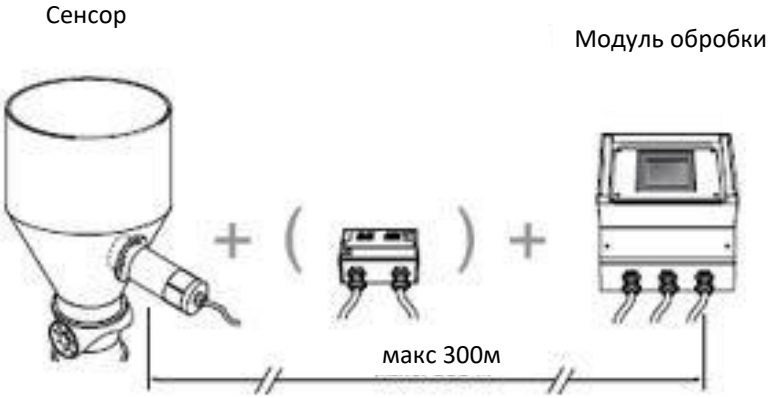


Рисунок 2 – Склад системи вимірювання вологості

Модуль обробки з'єднується із сенсором за допомогою 4-жильного екранованого кабелю. Максимальна відстань між сенсором і модулем обробки 300 м.

Можливі неточності вимірювань, що викликані неоднорідністю матеріалу, можуть бути суттєво зменшені за рахунок підключення до модуля обробки ММЕ 300 до 3-х сенсорів. Одночасно зменшується і вплив на результати вимірювання коливань об'ємної щільності, яка, як правило, однакова у всій вимірювальній зоні.

Крім того даний вимірювач вологості можна встановлювати в шнековому живильнику, на стрічковому конвеєрі, міксері, а також у випускній секції бункера.

Серед країн бувшого СНД можна виділити російську компанію «Промрадар». У вимірювачах вологості, що виробляються даною компанією, теж застосовується мікрохвильовий принцип дії.

Серед вітчизняних виробників обладнання для вимірювання вологості зернових в потоці слід відмітити ГНПП «Ельдорадо» м. Дніпро, що

виробляє поточні вологоміри зерна. Дані вологоміри відповідають вимогам Технічного завдання виробника зерносушарок ДСП-32 і ДСП-50 «Карлівського машинобудівного заводу». Обладнання випускається з 2003 року. На сьогоднішній день впроваджено більш ніж 300 комплектів (поточний вологомір зерна і блок управління).

Блок **БИВП** (поточний вологомір зерна) спільно з **ПКТП СЗ** (блок управління) (рис.3).

Рисунок 3 – Блок **БИВП** (поточний вологомір зерна) спільно з **ПКТП СЗ** (блок управління)

Пристрій забезпечує технологічний вимір і індикацію вологості зерна в потоці, середню по двом шахтам (абсолютна систематична похибка не більше ±1% в області значень номінальної вологості зберігання після попереднього калібрування вимірювальних каналів вологоміра зерна на порожній зерносушарці для наступних культур: кукурудза, пшениця, жито, ячмінь, соняшник, гречка. Під час сушіння таких культур, як рапс, соя та деяких інших використовується калібрувальна характеристика однієї з вищезгаданих культур. При цьому похибка поточного вологоміру зерна може дещо зрости, але задовольняє технологічні вимоги.

Зазначена похибка поточного вологоміра зерна (±1%) забезпечується при наступних умовах:

- через вологомір зерна проходить сировина в діапазоні від номінальної вологості зберігання до 20% вологості;
- через вологомір зерна проходить сировина в інтервалі температур від +5 до +45 °С;
- при сушінні кондиційного зерна, яке задовольняє відповідним ДСТУ;
- при відповідності конструкції і режимів сушіння конструкторській та експлуатаційній документації на зерносушарку.

Вищевказана похибка поточного вологоміру зерна (ПКТП СЗ і БИВП) може бути знижена в процесі сушіння до ± 0,3% шляхом додаткового калібрування приладу користувачем за показаннями, отриманими на СЕШ-3М.

Загальний вигляд приладу контролю технологічних параметрів сушіння зерна ПКТП С3 представлено на рис. 4:

Рисунок 4 – Загальний вигляд приладу контролю технологічних параметрів сушіння зерна ПКТП С3

Характеристики приладу:

- 5 каналів вимірювання температури в діапазоні от –99,9 до 400,0 °С з основною похибкою ±0,3°С;
- 1 канал для підключення блоку вимірювання вологості зерна в потоці (поточного вологоміра аба вологоміра зерна);
- 4 цифрових 4-х розрядних індикатора;
- контроль температури агента сушки в 1-й та 2-й зонах и нагріву зерна в 1-й та 2-й шахтах;
- попереджувальна сигналізація та аварійне відключення топки по уставкам;
- 2 канали управління випускними механізмами (функції апарата КЕП) з завданням періоду спрацьовування від 10 до 255 сек. з дискретністю 1 сек.;
- можливість моніторингу та реєстрації всіх вимірюваних параметрів на віддаленому персональному комп'ютері.

При вивченні ринку європейських і вітчизняних постачальників вологомірів для сипучих продуктів виявилось, що проблема вимірювання вологості в потоці актуальна не лише для України, а й для Європи.

На даний час деякі вітчизняні підприємства намагаються вирішити проблему за допомогою безперервних вологомірів зарубіжного або вітчизняного виробництва. Але ці прилади є ще технічно недопрацьованими (нестабільні показники), мають високу вартість і низьку якість вимірювання.

Враховуючи вищезгадані обставини, на деяких підприємствах застосовують експрес-аналізатори вологості зерна, як правило, зарубіжного виробництва. Навіть, якщо експрес-аналізатор вологості зерна атестований Держстандартом України і перевірений, використання його має наступні недоліки: наявність людського фактору, який може проявитись в несвоєчасному вимірюванні вологості зерна; відібрана проба, може характеризувати не все зерно, а лише ту частину, яка знаходиться в експрес-аналізаторі вологості зерна. Таким чином, вітчизняний агропромисловий комплекс не має вологоміра зерна в потоці доступного по ціні і відповідаючого необхідним вимогам і показникам.

Тому, розміри втрат, навіть на рівні окремих комбінатів хлібопродуктів (КХП) досягають десятків тисяч гривень в сезон. Актуальність цієї проблеми в цілому для агропромислового комплексу є очевидною.

Список літератури

1. Птушкин А.Т., Новицкий О.А. Автоматизация производственных процессов в отрасли хранения и переработки зерна: [2-е изд., допол. и перераб.] / А.Т. Птушкин, О.А. Новицкий. – М.: Агроатомиздат, 1985. – 318 с.

2. Шандров Б.В. Компьютерное управление технологическим процессом, експерементом, оборудованием / Б.В. Шандров – М.: Горячая линия – Телеком, 2009. – 608 с.

3. Конюх В.Л. Компьютерная автоматизация производства / В.Л. Конюх - НГТУ, 2006. – 108с.

4. Пашенко В.Ф. Основи проектування електронних пристроїв систем автоматики: [навчальний посібник] / В.Ф. Пашенко. – Кіровоград: КІСМ, 1998. – 328 с.

5. Головко Д.Б. Автоматика і автоматизація технологічних процесів / Д.Б. Головко. – К.: Либідь, 1997. – 232 с.

6. Промрадар / Промышленные датчики и приборы управления. – [Электронный ресурс]. – Режим доступа: www.promradar.ru.

7. Техноком : технологии эффективных решений [Электронный ресурс]. – Режим доступа: www.iktk.ru.

8. Хранение зерна и зерновых продуктов: Пер. с англ. канд. техн. наук В.Н. Дашевского, канд. биолг. наук Г.А. Закладного. – М.: Колос, 1978.– 472 с.

9. ОВЕН / Оборудование для автоматизации [Электронный ресурс]. – Режим доступа: www.owen.ru.

УДК 004.9

Всеобщий менеджмент качества на основе CALS-информационных технологий как фактор улучшения качества высшего образования

Отакулов М.К.[1], к.т.н., доцент,
Каримов Ж. М.[2], студент 3 курса
[1]Отраслевой центр переподготовки и подготовки педагогических кадров при Ташкентском Аграрном университете
[2]Ташкентский Международный Вестминстерский университет

С момента обретения независимости в 1991 году Республика Узбекистан избрала поэтапный подход к структурным преобразованиям во всех отраслях экономики и, в том числе, в образовательной сфере. С учетом фактора глобализации образования и вызова времени и информационных технологий переход на новый качественный уровень образования в вузах республики рассматривается через призму информатизации всего образовательного процесса в рамках страны.

На сегоднящный день одним из основных возможных вариантов перехода образования на более интегрированный качественный уровень является внедрение всеобщего менеджмент качества [1] – TQM (Total Quality Management) на основе более прогрессивных информационных технологий, таких как CALS-технология [2].

Современное состояние дел в области внедрения TQM на основе CALS-технологий в масштабе образования, как правило, сводится к разработке инструкций по оформлению и хранению служебной документации, схем деятельности подразделений, порядка согласования и утверждения тех или иных видов деятельности в отдельных разработках. В лучшем случае начинается внедрение системы электронного документооборота, что, требует системного подхода к этой задаче.

В целом CALS-технология – это современный подход к проектированию образовательной деятельности [3], заключающейся в использовании компьютерной техники и современных информационных технологий на всех стадиях процесса образования. В данном цикле обеспечивается единообразный способ управления процессами и взаимодействия всех участников начиная от начальной стадии подготовки до их реализации в соответствии с требованиями системы международных стандартов [4] и TQM, регламентирующих правила указанного взаимодействия преимущественно посредством электронного обмена данными на основе CALS-технологий.

Однако нельзя повысить качество управления деятельностью вузов с внедрением IT менеджмента в систему управления на основе CALS-технологии за счет разработки самых идеальных стандартов, инструкций и документов, описания тех или иных процессов даже с использованием

специально разработанных систем, например, BP WIN, Rational Rose, ARIS и т.п. Этот комплект документов не предполагает применение серьезных информационных систем и технологий управления, таких как TQM на основе CALS-технологий, т.е. непрерывной информационной поддержки жизненного цикла образовательного процесса вуза на основе индикаторов качества, позволяющих управлять разнородными процессами в различных подразделениях и учебным процессом в целом в единой информационной среде.

Применение TQM на основе CALS-технологий в цикличной форме в цепочке начиная от заказчика специалистов вуза и студента до преподователя и администрации вуза, а также карьерный рост выпускника в совокупности будут мониториться и позволят повысить их конкурентоспособность. Соответственно повышение качества образования будет достигнуто путем существенного сокращения объемов проектных и бюрократических работ, а также ряда транзакционных издержек.

Описания многих узлов комплексной работы образовательного процесса вуза путем применения TQM на основе CALS-технологий, хранятся в унифицированных форматах данных на сетевых серверах, доступных любому пользователю участника настоящей цепочки технологий в образовательной деятельности вуза. При этом существенно облегчается решение проблем образовательных услуг в зависимости от требования международного стандарта и отдельного стандарта определенных стран. Улучшается интеграции на глобальный рынок образовательных услуг с учетом их конъюнктур, а также макро- и микросреды образовательного рынка, адаптации к меняющимся условиям глобального вызова международного рынка.

Предполагается, что достижение показателей стандарта TQM на международном рынке образовательных услуг будет немыслимо вне CALS-технологий, так как непрерывная информационная поддержка жизненного цикла образовательных услуг от потребности в специалистах-выпускниках вуза до их продвижения по карьерной лестнице в целом в единой информационной пространстве нуждается в постоянном мониторинге образовательной деятельности.

Основными факторами в направлении совершенствования и повышения качества образовательных услуг на основе CALS-технологии с учетом TQM являются:

• внедрение в систему управления качества эффективных информационных методов, таких как CALS-технологии в сочетание с TQM в образовательных услугах;

• ориентация на конечного клиента образовательных услуг на основе CALS-технологии с учетом TQM в образовательных услугах;

• усиление механизма воздействия систем управления качеством на основе CALS-технологии на все этапы жизненного цикла образовательных услуг.

Современные проблемы ограниченности их внедрения носят уже не методологический, а чисто практический характер, причинами которых являются отсутствие квалифицированных кадров, ограниченность организационно-технической и материальной базы предприятия, недостаточный опыт массового использования статистических методов, отставание в автоматизации технологических и управленческих процессов.

Практика показывает, что внедрение международных стандартов TQM ограничивается не только высокими требованиями к организации материально-технического снабжения, финансирования, программного обеспечения, но и препятствиями социально-психологического характера, вызванными стереотипами старого мышления. ВУЗы, внедряющие стандарты качества TQM на основе CALS-технологий, сталкиваются с непониманием необходимости осуществления этой работы в существующих условиях образования. Условия, принципы и требования, закрепленные в уже переработанных стандартах, на практике выполняются не в полном объеме, что противоречит системному подходу в решении задач качества.

Активное использование CALS-технологий [5] в управлении образовательных услуг обеспечивает повышение качества и достижение требование TQM выпуска конечного продукта за счет контроля выполнения определенного технологического цикла. К тому же применение CALS-технологий может сыграть не последнюю роль в снижении неоправданных затрат на управленческий аппарат и материальное обеспечение технологического процесса.

Сегодня созданием единого информационного пространства на основе CALS-технологий занимаются в основном крупные компании и корпорации. Тем не менее, система образовательных услуг может также работать в едином ключе, т.е. в виде цепочки образовательной деятельности, поэтапно внедряя элементы CALS-технологий, в том числе и в систему менеджмента качества. Для этого необходимо разработать методику перехода производства на работу в условиях единого информационного пространства образовательной деятельности начиная от вузов, что является весьма нетривиальной задачей. Это потребует обследования всего технологического цикла и формализации процессов, выполненных специалистами в этой области, разработки рабочих потоков и их реализации в PDM-системе (Product Date Management – системе управления данными), разработки баз данных о кадрах, финансах, программных продуктах по цепочкам учебного процесса.

Применительно к высшему образованию, CALS-технологии – это создание единого информационного пространства, в котором каждый участник учебного процесса (ректор, декан, преподаватель, студент) в нужное время и в нужной форме может получить нужную информацию, воспользоваться ей и, при необходимости, иметь возможность управлять

элементами учебного процесса, чтобы привести его в соответствие с изменяющимися требованиям рынка.

Развитие CALS-технологий должно привести к появлению так называемых виртуальных библиотек, в которых процесс создания спецификаций с информацией для программного управления технологическим процессом, достаточной для полного цикла, может быть распределен во времени и пространстве между многими организационно автономными обучающими системами образовательного рынка.

Построение открытых распределенных автоматизированных систем для проектирования и управления в образовательной деятельности составляет основу современных CALS-технологий. Главная проблема их построения — обеспечение единообразного описания и интерпретации данных, независимо от места и времени их получения в общей системе образовательной деятельности, имеющей масштабы вплоть до глобальных рынков. Структура документации образовательной деятельности и языки её представления должны быть стандартизированными. Для обеспечения информационной интеграции и CALS использует стандарты IGES и STEP в качестве форматов данных. В CALS входят также стандарты электронного обмена данными, электронной технической документации и руководства для усовершенствования процессов.

Таким образом, внедрения в учебный процесс вузов TQM на основе CALS-технологий с одной стороны, как универсальная программа-оболочка в виде электронного учебника и материалов: электронный учебник, контрольно-обучающая программа и тестирующей программы и, с другой стороны, как автоматизированная рабочая места и интегрированная программная продукция с различными фондами занятости будет способствовать повышению качества образовательного процесса и интеграцию их в глобальную образовательную сеть.

В заключении необходимо отметить, что внедрение в систему управления в образовательный процесс эффективных информационных методов как CALS-технологии в сочетание с TQM позволит, увеличит качество образовательных услуг и снизит транзакционные затраты образовательного процесса.

Список литературы

1. ИСО 9000, 9001, 9004 – 2001 Системы менеджмента качества.

2. CALS-технологии [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/CALS-технологии

3. Пятаев А.В. Универсальные программы-оболочки для образовательных систем вузов РУз // Сборник трудов ТГАИ, часть II. – Ташкент, 2005.

4. ИСО 9000-2001 Системы менеджмента качества.

5. Бондаренко И.Б., Иванова Н.Ю., Сухостат В.В. Управление качеством электронных средств. – СПб: СПбГУ ИТМО, 2010. – 211с.

УДК 004.9

Визначення центральностей у соціальному графі засобами графової бази даних Neo4j

Охотний С.М., студент 4 курсу,
Мелешко Є.В., канд. техн. наук, доцент
Центральноукраїнський національний технічний університет, м. Кропивницький

Одним з важливих напрямків аналізу соціальних мереж є дослідження властивостей структурної позиції її користувачів. Найважливішою характеристикою структурної позиції користувача є значення його центральності. Центральним є користувач, який залучений до великої кількості зв'язків і як їх ініціатор, і як реципієнт. Прикладами загальних методів вимірювання центральності є визначення центральності за посередництвом, за близькістю, за степенем, за власним вектором тощо [1].

Neo4j – графова система керування базами даних з відкритим вихідним кодом, реалізована на Java [2]. Станом на 2017 рік вважається найпоширенішою графовою СКБД. Розробник – американська компанія Neo Technology, розробка ведеться з 2003 року. З 2007 року стала публічно доступною. У Neo4j присутні всі характеристики баз даних, включаючи дотримання ACID, підтримка розбиття на кластери і відновлення після збою в системі.

Графова база даних – це така база даних (БД), яка використовує графові структури для побудови семантичних запитів з використанням вузлів, ребер і властивостей в процесі подання та зберігання даних. Графові БД використовуються для зберігання, управління та виконання запитів до складних і тісно взаємопов'язаних груп даних. Крім цього, архітектура графової БД особливо добре пристосована до аналізу даних на предмет виявлення збігів і аномалій в великих масивах даних, а також до вигідного використання укладених в БД взаємозв'язків.

Мова запитів Cypher – найпоширеніша мова запитів до графових баз даних, що обумовлено його використанням в СКБД Neo4j. Cypher є декларативною мовою і дозволяє створювати, оновлювати і видаляти вершини, ребра, мітки і властивості, а також керувати індексами і обмеженнями.

Графові БД найкраще застосовувати в тих випадках, коли в системі є численні з'єднані один з одним пристрої або ресурси з множинними зв'язками між ними і всередині них. Одним із таких випадків є соціальні мережі, де між різними об'єктами, такими як користувачі, групи, пости існує велика кількість зв'язків. Однією з найбільших переваг Neo4j є набір вбудованих алгоритмів аналізу графової інформації зокрема є алгоритми які застосовуються при аналізі соціальних мереж, а саме визначення

центральностей (центральність за степенем, центральність за посередництвом, центральність за близькістю). Також реалізовані алгоритми визначення групи, а саме алгоритми визначення сильно та слабко пов'язаних вузлів, алгоритм визначення коефіцієнту кластеризації, а також розповсюдженості певної інформації (бренду). Крім того є алгоритми з пошуку найкоротшого шляху в графі та алгоритми доступності та якості шляху.

Приклад запиту на мові Cypher, для визначення рангової центральості в графі:

```
CALL algo.pageRank(
  'MATCH (p:Page) RETURN id(p) as id',
  'MATCH  (p1:Page)-[:Link]->(p2:Page)  RETURN  id(p1)  as
source,                      id(p2)                      as
   target',
  {graph:'cypher', iterations:5, write: true}
)
```

Приклад запиту Cypher для обчислення центральності за посередництвом:

```
CALL
algo.betweenness.stream('User','MANAGE',{direction:'out'})
YIELD nodeId, centrality
RETURN nodeId,centrality order by centrality desc limit 20;
```

Всі алгоритми представляються у вигляді процедур. Їх можна викликати безпосередньо в Cypher з браузера Neo4j, з cypher-shell, або з клієнтського коду. Для більшості алгоритмів пропонуються по дві процедури: одна з назвою algo.<ім'я>, яка записує результати в граф у вигляді властивостей вузлів та звітної статистики; та інша з назвою algo.<ім'я>.stream, яка повертає результат у вигляді потоку даних, наприклад ідентифікатори вузлів та обчисленні значення. Для великих графів процедура потокового відтворення може повернути мільйони або мільярди результатів, тому зазвичай зручніше зберігати результати алгоритму, а потім використовувати їх з пізнішими запитами.

Список літератури

1. Мелешко Є.В. Дослідження методів визначення центральності акторів у соціальних мережах для задач інформаційної безпеки / Є.В. Мелешко, В.С. Гермак, С.М. Охотний // Системи управління, навігації та зв'язку. - 2016. - Вип. 4. – С. 67-70

2. Neo4j Documentation [Електронний ресурс] – Режим доступу до ресурсу: https://neo4j.com/docs/

УДК 004.734

Метод маршрутизации трафика в гетерогенной информационной системе

Поддубный Б.А., аспирант
Науковий керівник – Купин А.И., д.т.н., професор
Государственное высшее учебное заведение «Криворожский национальный университет», г. Кривой Рог

На текущий момент существуют множество методов маршрутизации трафика с учетом разных параметров, однако практически отсутствуют разработки в области гетерогенных сетей с нестабильной структурой [1, 2]. Основное отличие нестабильной гетерогенной сети от стабильных – отсутствие постоянных каналов связи. Это ограничение не дает возможности выстраивать прямые маршруты между источником и приемником.

Авторами разработан и апробирован метод поиска маршрута на основе статистической информации о состоянии линий связи.

Актуальность вопроса и постановка задачи. Для построения маршрута необходима информация о состоянии маршрутов и отдельных линий связи между соседними узлами: w – пропускная способность, измеряемая в единицах, принятых для сети (бит/с, байт/с, пакеты/с и т.д.); prob – вероятность наличия соединения (отношение времени наличия соединения ко всему времени измерения метрики); cost – стоимость передачи данных по маршруту или линии связи. При построении маршрута необходимо произвести декомпозицию сети на составляющие части: прямые линии без ответвлений и треугольники, состоящие из трех соседних узлов и имеющие соединения между всеми вершинами.

Реализация метода. Маршрутизация любой сети (как гетерогенных, так и локальных, глобальных и т.д.) и сводится к поиску маршрутов внутри этого треугольника (рис 1). Алгоритм построения маршрута:

1. Узел (D) после добавления уведомляет всех соседей (C, E) о своем наличии в сети.
2. Соседние узлы (C, E) оценивают параметры доступа [w, prob, cost].
3. При отсутствии ответвлений в сети узел (E) передает информацию о состоянии линии связи следующему узлу (B), при этом линия объединяется в единый фрагмент (DB) с едиными параметрами оценки.
4. При наличии ответвлений в сети (C), такие линии разделяются на независимые фрагменты для которых рассчитывается отдельные маршруты (DCA и DCB).

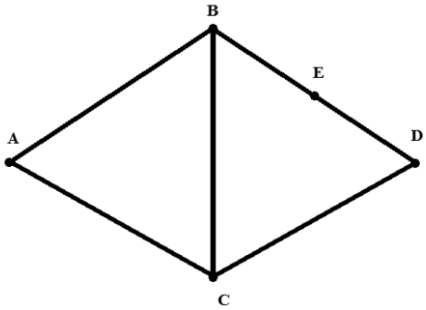


Рисунок 1 – Модель гетерогенной сети

5. Если между узлами есть существующая линия связи (BC), такой фрагмент считается треугольником (DCB), для которого необходимо исключить наиболее дорогой фрагмент сети. Для этого рассчитывается стоимость передачи по линиям DCB, DBC и их значения попарно сравниваются со значениями стоимости линий DC и DB. Прямые линии, которые имеют большую стоимость, чем соответствующие им составные, исключаются из расчета маршрута.

6. Далее узлы передают информацию об узле D и найденном маршруте (с его характеристиками) далее своим соседям до тех пор.

7. При схождении нескольких маршрутов в одну точку (A) выбирается маршрут с наименьшей стоимостью.

Выводы. Такой метод позволяет оперативно находить маршруты в сетях любого типа, в том числе гетерогенных и нестабильных [3], без сбора информации о топологии сети, основываясь только на информации о маршрутах соседей к узлу назначения и состояния линий связи.

Список литературы

1. Зеленцов В.А., Цивирко Е.Г., Чукарин А.В. Метод маршрутизации трафика в информационно-коммуникационной гетерогенной сети // Известия высш. учебных заведений. – 2010. – Том 53, № 11. – С. 56-61.

2. Березко М.П., Вишневский В.М., Левнер Е.В., Федотов Е.В. Математические модели исследования алгоритмов маршрутизации в сетях передачи данных // Информационные процессы. – 2001. – Т. 1, № 2. – С. 103-125.

3. Купин А.И. Математическая модель маршрутизации трафика в гетерогенной информационной среде / А.И.Купин, И.О.Музыка, Б.А.Поддубный // Системні технології. Регіональний міжвузівський збірник наукових праць. – Дніпро, 2017. – Вип. 2(109). – С. 14-19.

УДК 004.9

Дослідження програмних додатків для створення 2d- та 3d-анімації

Пономаренко А.С., студент 2 курсу
Науковий керівник – Мелешко Є.В., к.т.н., доцент
Центральноукраїнський національний технічний університет, м. Кропивницький

Комп'ютерна анімація – мистецтво створення рухомих зображень, за допомогою комп'ютера, є підрозділом комп'ютерної графіки. На відміну від більш загального поняття «графіка CGI», що відноситься як до нерухомих, так і до рухомих зображень, комп'ютерна анімація має на увазі тільки рухомі зображення.

Створення мультиплікаційного ролику включає у себе почерговий процес роботи з різними видами мультимедійних файлів у спеціалізованих анімаційних та мультимедійних програмах та роботою з середовищами програмування, які мають можливість обробки графіки.

Анімаційні програми – це програми, призначені для розробки анімаційних роликів, мультфільмів та анімаційних вставок.

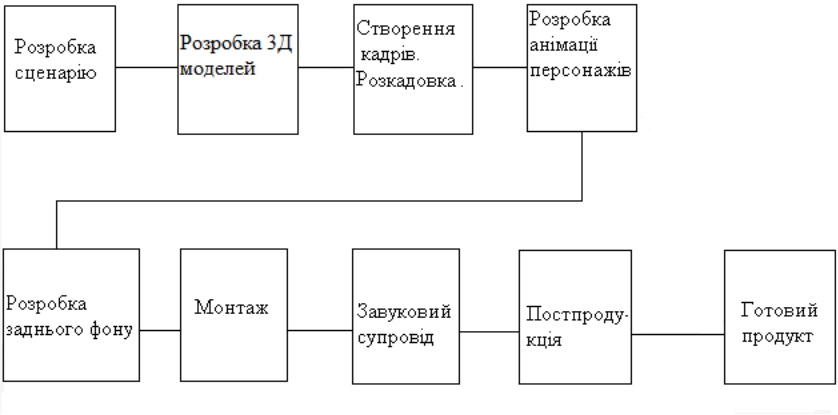


Рис. 1 – Етапи створення анімаційного проекту

Для одержання тривимірного зображення на площині потрібні такі кроки:

- Моделювання – створення тривимірної математичної моделі сцени і об'єктів в ній.
- Рендеринг (візуалізація) – побудова проекції відповідно до обраної фізичної моделі.

- Виведення отриманого зображення на пристрій – дисплей або принтер.

Широке застосування в мережі отримали дві мови, за допомогою яких програмуються рухи анімованих об'єктів:

– JavaScript – браузерна мова;

– ActionScript – мова роботи з додатками Flash.

Перевага програмованої анімації – у зменшенні розміру вихідного файлу, недолік – навантаження на процесор клієнта.

3D-анімація створюється за допомогою спеціальних програм (3D Studio MAX, Maya, PovRay, LightWave та ін.). Підсумкове зображення в них отримують шляхом візуалізації сцени, яка включає набори об'єктів, джерел світла, текстур та камер.

Було досліджено 2 програми – **Autodesk Maya** та **Blender,** описано їх мінуси та плюси.

Autodesk Maya – графічний редактор, для моделювання тривимірних об'єктів, анімації, композитингу та візуалізації (за допомогою систем рендерингу) [1-2]. В даний час є стандартом для розробки 3D-графіки для кіно і телебачення. Спочатку розроблена для ОС IRIX (платформа SGI), потім була портована під ОС Linux, Microsoft Windows і Mac OS. З 2013 року, версії програми випускаються тільки для 64-бітових систем.

Візуалізація в Maya реалізована трьома вбудованими механізмами: Maya Software, Maya Hardware, Maya Vector Render, а також рендером, mental ray Standalone, що встановлюється окремо. Існує й ряд візуалізаторів від сторонніх розробників, в яких включена підтримка Maya. Основні з них: V-Ray, RenderMan, finalRender, 3Delight, Gelato, Turtle, Maxwell Render, Fryrender, Indigo Renderer, Brazil R/S.

PlayblastVR – апаратний рендер (на основі OpenGL та DirectX) для створення швидких тестових візуалізацій сцен. Підтримує стандартні джерела світла і шейдери, об'ємні ефекти Maya Fluids і FumeFX, штрихи Maya Paint Effects, частки nParticles, систему волосся nHair і систему моделювання одягу і тканин (nCloth). На виході дозволяє отримати зображення в 15-х основних форматах панорам, включаючи LatLong, використовуваний The Foundry в розробці їх нових інструментів VR.

Blender – пакет для створення тривимірної комп'ютерної графіки, що включає засоби моделювання, анімації, вимальовування, післяобробки відео, а також створення відеоігор [3-5]. Особливостями пакету є малий розмір, висока швидкість вимальовування, наявність версій для багатьох операційних систем – FreeBSD, GNU/Linux, Mac OS X, SGI Irix 6.5, Sun Solaris 2.8 (sparc), Microsoft Windows, SkyOS, MorphOS та Pocket PC.

Пакет має такі функції, як динаміка твердих тіл, рідин та м'яких тіл, систему гарячих клавіш, велику кількість легко доступних розширень, написаних мовою Python. Починаючи з версії 2.61 з'явились функції "відстеження камери" (англ. camera tracking), та "захоплення руху" (англ. motion capture або mocap).

Програма є вільним програмним забезпеченням та розповсюджується під ліцензією GNU GPL.

Cinema 4D – програмний пакет для створення тривимірної графіки та анімації, розроблюваний MAXON [5]. Cinema 4D є універсальною комплексною програмою для створення і редагування тривимірних ефектів і об'єктів. Дозволяє рендерити об'єкти за методом Гуро.

Основна програма містить інструменти для моделювання, текстурування, рендеру та анімації. Основою для створення об'єктів слугують примітиви на кшталт сфери чи площини, поділені на полігони. Об'єкти, як цілком, так за виділеними полігонами, можуть змінюватися базовими перетвореннями, такими як обертання, зміна розміру, та просунутими – скручування, тиснення, перетворення за формулою тощо. Програма надає ряд деформаторів і генераторів складних об'єктів, наприклад, ландшафтів. Особливістю Cinema 4D є інструмент «ніж» для ручного розділення більшого полігона на менші. Програма також дає змогу малювати полігональні стрічки, прив'язувати одні полігони до інших, перетворювати грані на дуги. Інструмент MoGraph дозволяє автоматично створити з базового об'єкта чи їх групи складний об'єкт перетвореннями на кшталт клонування чи симетричного копіювання.

Висновок

Кожен редактор має свої плюси та мінуси. Blender – зручний інтерфейс, безкоштовний присутній морфінг, скульптінг для розробки моделей, а також "рік" для створення анімації руху моделей. Autodesk Maya має безкоштовну версію на 3 роки, потім треба придбати повну версію для подальшої роботи. Користувачу треба вирішувати для якої операції потрібен редактор та на який термін.

Список Літератури

1. Maya computer animation software [Електронний ресурс]. – Режим доступу: https://www.autodesk.com/products/maya/overview

2. 3dmaya [Електронний ресурс]. – Режим доступу: https://3dmaya.com.ua/

3. Blender [Електронний ресурс]. – Режим доступу: https://www.blender.org/

4. Blender3D. Уроки по Blender [Електронний ресурс]. – Режим доступу: https://blender3d.com.ua/

5. Простой Blender. Часть 1 [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/post/272519/

6. Cinema4D [Електронний ресурс]. – Режим доступу: https://www.maxon.net/ru/produkty/cinema-4d/obzor/

7. CSS анимации. Контроль над ними из JavaScript. Анимации на чистом JavaScript [Електронний ресурс]. – Режим доступу: https://learn.javascript.ru/animation

8. Кривые Безье [Електронний ресурс]. – Режим доступу: http://vdfilms.com/ua/info/statti/animatsiya-pryklady-vydy-zastosuvannya/

УДК 004.896

Інформаційна система організації індивідуальних міських поїздок

Проніна О. І., асистент
ДВНЗ «Приазовський державний технічний університет», м. Маріуполь

У сучасному світі інформаційні технології активно використовуються в усіх сферах людської діяльності. В даний час велика увага приділяється питанням інновацій в сфері пасажирських перевезень.

Дослідження моделей взаємодії користувача і клієнта показали, що найбільш ефективний варіант взаємодії – це модель виклику таксі «без диспетчера», коли взаємодія водія і клієнта йде безпосередньо, без посередника. У цій моделі клієнт вибирає собі автомобіль згідно зі своїми бажаннями і перевагами, але навіть тут виникають складнощі, оскільки в будь-якій моделі присутній людський фактор.

Таким чином, актуально розгляд інформаційної системи, що радить, яка дозволить оптимізувати процес вибору оптимального варіанту поїздки на основі всіх існуючих параметрів. Оскільки область оцінки параметрів суб'єктивна, вирішено використовувати апарат нечіткої логіки.

Інформаційна система організації індивідуальної міської поїздки складається з окремих частин: підсистема Клієнта, підсистема Водія, Серверна частина, підсистема Вибору оптимальної поїздки.

Функціональні можливості підсистем наступні:

- підсистема «Клієнт» реалізує завдання координат для початку і кінця поїздки, а також можливість вибору із запропонованого списку водіїв і автомобілів поїздку і здійснення на пряму дзвінка водію або ж замовлення функції «передзвонити мені»;
- підсистема «Сервер» представляє список вільних водіїв клієнту, передає дані про замовлення водієві, зберігає всі поточний координати водіїв;
- підсистема «Водій» реалізує можливість установки режиму роботи «я вільний», «я зайнятий», можливість передачі своїх координат сервера, а також отримання всіх даних про замовлення;
- підсистема «Вибір оптимальної поїздки» реалізує оцінку кожної запропонованої поїздки, згідно з заданим обмеженням, а також здійснює визначення ступеня впевненості кожної поїздки, для подальшої побудови рангового списку поїздок. Основу цієї підсистеми становить нечіткий висновок, представлений видом (1).

Для визначення ступеня впевненості поїздки використовується нечітка модель вибору. В основі нечіткої моделі вибору оптимальності поїздки лежить формальна система виду (1).

$$HM_2 = < \{V\}_{i=1}^{5}, \{W\}_{j=1}^{1}, \{R\}_{k=1}^{107} > \quad (1)$$

Множина {V}, {W}, {R} є множини базових елементів, відповідно, множина

вхідних змінних: V = {β_1, β_2, β_3, β_4, β_5}; множина вихідних лінгвістичних змінних: W = {ϖ_j}; множина правил нечітких продукцій: R = {R_1, R_2, …, R_{107}}.

У підсистемі «Вибір оптимальної поїздки» присутні два агента: клієнт і водій, представлених на рис. 1. На діаграмі варіантів використання відображені операції, які потрібно виконати користувачеві для формування поїздки: вибрати координати початку поїздки, вибрати із запропонованого списку водіїв, того що цікавить або вибрати оптимальну поїздку.

Користувачеві (клієнту) надається основна можливість – це підбір поїздки. Підбір поїздки обов'язково включає в себе надання списку водіїв (остаточне рішення по поїздки приймає користувач), можливість з цього списку вибрати для себе водія або дозволити підсистемі визначити оптимальну поїздку. Також водієві від клієнта передається всі подробиці поїздки і для клієнта є можливість зв'язатися з водієм безпосередньо (за допомогою дзвінка) або замовити «передзвонити мені».

Для водія можливість роботи з підсистемою - це участь у формуванні поїздки, що включає в себе формування протоколу поїздки і зміну режиму зайнятості.

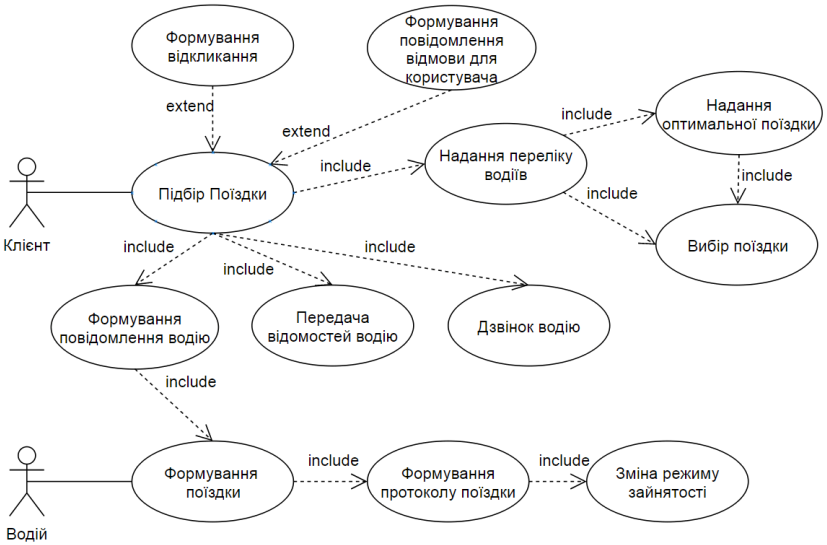


Рис. 1. Діаграма варіантів використання підсистеми

Вхідними даними для системи є дані з підсистеми «Клієнт» і дані з підсистеми «Водій».

1) **Призначення і склад системи.** Розроблена система призначена для:

- відображення на карті всіх працюючих в даний момент водіїв, з колірним позначенням статусу роботи (зелений колір означає, що водій вільний, червоний, що в даний момент він здійснює замовлення), що

дозволяє миттєво оцінювати кількість працюючих водіїв їх максимальне скупчення. Ці показники допомагають водію, який приступає до роботи вибрати більш вільний район, а клієнту оцінити можливість отримання послуги якомога швидше.

- обробка геолокаційних даних, які надходять з підсистеми водія і клієнта, для формування замовлення і підбору водіїв, для здійснення майбутньої поїздки;

- рекомендації щодо оптимальності кожної запропонованої поїздки.

Рекомендації пропонуються у вигляді рангового списку, де головним оцінним показником є ступінь впевненості в оптимальності поїздки, дане значення розраховане на основі моделі нечіткого виведення.

2) **Основними підсистемами в складі системи є:**

- База даних системи.

- Підсистема «Клієнт». Підсистема «Клієнт» призначена для установки координат для поїздки, а також вибору із запропонованого списку водія, який буде здійснювати поїздку. У підсистемі є можливість прямого дзвінка водію, а також можливість замовлення функції «передзвоніть мені».

- Підсистема «Водій». Підсистема «Водій» призначена для передачі статусу роботи, передачі в режимі реального часу координат водія, можливость налаштувати свої тарифи, а також можливість встановити маяк, де найближчим часом опиниться водій для більш ранньої участі у виборі за запитом клієнта на підбору поїздки.

- Підсистема «Вибір оптимальної індивідуальної міської поїздки». Завдання підсистеми є розрахунок ступеня впевненості в оптимальності поїздки за даними про кожну запропонованої поїздки користувачеві, щоб за запитом користувача видавати ранжируваних список поїздок.

- В роботі системи важливу роль відіграє сервер, за рахунок якого відбувається передача всіх даних необхідних для роботи системи. На сервері здійснюється виконання підбору автомобілів по кожному запиту клієнта, з урахуванням закладених правил.

3) **Вхідні дані.** Вхідними даними для системи є дані з підсистеми «Клієнт» і дані з підсистеми «Водій».

З підсистеми «Клієнт» надходять геолокаційні дані про початкові координатах поїздки, а також геолокаційні дані про кінцеву точку поїздки або адреса трансформована в координати. Крім того з підсистеми «Клієнт» передається інформація про вибір поїздки.

З підсистеми «Водій» надходять статус включення програми та готовність до роботи, статус водія - «я вільний» або «я зайнятий», які передбачають можливість брати участь у відборі водіїв для поїздки, а також геолокаційні дані місцезнаходження водія в реальному режимі часу.

4) **Опис БД.** Реляційна база даних (СКБД ORACLE) є ядром системи. Вона призначена для зберігання даних в режимі реального часу про

місцезнаходження всіх активних водіїв, їх статус роботи, повний перелік інформації про зареєстрованих водіїв, інформація про поточні координати клієнтів для створення замовлення, базу знань в форматі, необхідному для роботи підсистеми вибору оптимальної поїздки.

Додаток БД системи керують інформаційними обмінами як всередині системи, так і поза нею. В БД створені такі моделі даних:

- модель підсистеми «Клієнт»;
- модель підсистеми «Водій»;
- модель даних підсистеми «Вибір оптимальної індивідуальної міської поїздки» (розраховані ступеня впевненості по кожній запропонованій для вибору клієнта поїздки, правила за якими здійснюється розрахунок);
- всі дані про зареєстрованих водіїв (реєстраційні дані, а саме ім'я користувач, пароль, прізвище, номер телефону до якого прив'язаний акаунт, модель машини, номер машини, всі тарифи, опис автомобіля та ін.);
- модель даних призначена для зберігання всіх замовлень: відкритих, скоєних і попередніх;
- інформація про запропоновані поїздках відправлених на запит користувача з урахуванням правил підбору автомобіля для здійснення поїздки.

Перелік кількох основних сутностей існуючих в базі даних:

- водій, описує набір даних який характеризує кожного водія;
- клієнт, супереч даних про клієнта, сутностей які характеризують клієнта дві, клієнт зареєстрований і клієнт без реєстрації, кожна з яких має свій перелік даних;
- клас автомобіля, описує характеристики автомобіля водія;
- тарифи, описує зв'язок класу автомобіля з тарифною сіткою налаштовується користувачем;
- позиція водія, поточне місце розташування водія яке відображається на карті і доступно клієнтам і іншим водіям;
- замовлення, вся інформація про поточні замовленні які передаються водіям, що буде їх виконувати;

Сутностей «замовлення» в моделі кілька, вони розділені за принципом «поточне замовлення», «попереднє замовлення», у кожного замовлення є свій статус, що також є сутністю БД. Статусами є інформація про виконання замовлення – виконаний, відкритий, закритий. Крім цього існує ще безліч сутностей, які описують всі процеси моделі.

Для вибору оптимальної індивідуальної міської поїздки була застосована модель нечіткого виведення на підставі продукційних правил моделі вибору оптимальної поїздки.

Розроблена інформаційна система організації індивідуальних міських поїздок спрощує надання послуги перевезення та дозволяє виключити людський фактор при виборі оптимальної поїздки. Отже збільшує показник ефективності обраної поїздки в цілому як для клієнта так і для водія. Крім цього завдяки впровадженню розробленої моделі в підсистему вибору оптимальної поїздки скорочено час обслуговування клієнта.

УДК 681.518

Розробка програмного додатку ігрового спрямування під управлінням операційної системи iOS

Ругало Д.А., студент
Науковий керівник – Царенко О.М., к.т.н., доцент
Центральноукраїнський державний педагогічний університет, м. Кропивницький

У наш час логічні ігри є популярним ігровим жанром. Грати в логічні міні-ігри люблять усі, незалежно від статі, віку, займаної посади та соціального статусу. Логічні ігри діляться на велику кількість різновидів, одним з яких є логічні міні-ігри – головоломки, в яких необхідно вибудовувати фішки за заданими правилами, паззли, в яких збираються гравцем картинки з різних дрібних фрагментів, наприклад, всесвітньо відома логічна гра Маджонг. Список таких ігор можна продовжувати довго, але можна безпомилково зробити висновки: розробка комп'ютерних ігор ще довго залишатиметься перспективною.

Так само актуальною є iOS – операційна система, яка запускається виключно на пристроях iPhone, iPod touch і iPad. Операційну систему розробляє корпорація Apple, що за ринковою долею капіталу сьогодні є однією з найбільших у світі. iOS має широке розповсюдження, а отже, має популярність значної кількості користувачів. Ця операційна система керує обладнанням цих пристроїв і надає технології необхідні для написання переносних орієнтованих додатків. Операційна система поставляється з різними системними додатками.

Набір засобів розробки додатків для iOS (iOS SDK) включає інструменти та інтерфейси, необхідні для розробки, установки, запуску і тестування платформо-орієнтованих додатків. Платформо-орієнтовані додатки збираються за допомогою системних бібліотек iOS і мови програмування Objective-C і запускаються безпосередньо в операційній системі iOS. На відміну від веб-додатків, такі додатки встановлюються на пристрій фізично і тому завжди доступні користувачеві, навіть якщо пристрій знаходиться в режимі «Польоту». Вони розташовуються разом з іншими системними додатками, і, одночасно, самі додатки і призначені для користувача дані синхронізовані з комп'ютером користувача через програму iTunes.

В якості інструменту практичної реалізації поставленої задачі було обрано мову програмування Objective-C, зважаючи на її поширеність, універсальність і функціональність (багатий набір інструментарію для розробника). Objective-C – рефлективна, високорівнева об'єктно-орієнтована мова програмування загального призначення, розроблена у вигляді набору розширень стандартної C, використовується для

написання додатків для операційних систем Apple. Розроблена компанією Apple, використовується в основному у Mac OS X та GNUStep — середовищах, розроблених на основі стандарту OpenStep, та Cocoa — бібліотеки компонентів для розробки програм. Програму на Objective-C, що не використовує цих бібліотек можна скомпілювати для будь-якої платформи, яку підтримує gcc компілятор з підтримкою Obj-C.

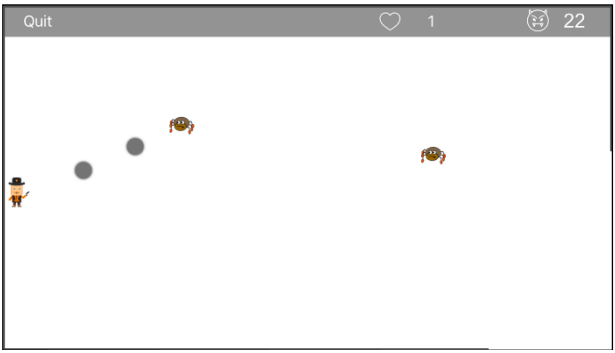


Рисунок 1 – зображення графічного інтерфейсу

Мовою програмування Objective-C написано ігровий додаток, у якому метою є влучання гравцем кулями у якомога більшу кількість ворогів під час ігрового сеансу. Зовнішній вигляд гри показано на рис. 1.

Висновки. З метою ілюстрації можливостей мови програмування Objective-C створено образ типового ігрового додатку логічного жанру. Створена програма призначена для тренування уваги, реакції та моторики потенційного користувача.

Список літератури

1. Гэлловей М. Сила Objective-C 2.0. Эффективное программирование для iOS и OS X. – СПб.: Питер, 2014. – 304 с.
2. Далримпл М. Objective-C 2.0 и программирование для Mac. – Вильямс, 2010. – 315 с.
3. Донован Д. Системное программирование. – М.: Мир, 1975. – 540 с.
4. Елисеев Д. Разработка и продажа программ для iPhone и iPad. – СПб.: БХВ-Петербург, 2010. – 336 с.
5. Здзиарски Д. iPhone. Разработка приложений с открытым кодом. – СПб.: БХВ-Петербург, 2011. – 368 с.
6. Здзиарски Д. iPhone SDK. Разработка приложений. – СПб.: БХВ-Петербург, 2012. – 506 с.

УДК 004.457

Ідентифікація компонентів персонального комп'ютера засобами мови програмування C#

Савеленко Д.І., магістрант 2 курсу
Наукові керівники – Петренюк В. І., к. ф.-м. н., доцент, Хох В.Д., аспірант
Центральноукраїнський національний технічний університет, м. Кропивницький

Ідентифікація та моніторинг компонентів персонального комп'ютера (ПК) – це основні заходи, необхідні при розробці операційних систем, систем управління, а також програм ідентифікації, що використовуються при налагоджені та вдосконалені ПК. Для ідентифікації компонентів ПК використовують різні способи. Способи ідентифікації компонентів можна поділити на апаратні та програмні. В більшості випадків достатньо даних, які можна отримати за допомогою програм. Тому вони більш відомі та застосовані. Подібні програми досить легко можна розробити, використовуючи мову програмування C#.

Серед відомих об'єктно-орієнтованих мов високого рівня широкого розповсюдження набула мова програмування C#. Синтаксис C# близький до C++ і Java [3]. Вона надає багато можливостей для створення графічного інтерфейсу тому широко застосовується в різних сферах програмування.

Для розробки програмного забезпечення ідентифікації компонентів ПК можна використати бібліотеки System.Management та OpenHardwareMonitor [1,2]. Бібліотека System.Management надає доступ до великого набору відомостей про систему, пристрої і додатки, які підтримують інфраструктуру інструментарію управління Windows (WMI). Доступні дані можна отримати з керованих і некерованих компонентів з репозиторію, що містить інформацію про класи. В основі структури даних WMI покладена Common Information Model (CIM), яка реалізує об'єктно-орієнтований підхід до представлення компонентів ПК. Особливістю WMI є динамічна властивість об'єктів, тому на запит користувача надаються поточні параметри. WMI класи зберігаються у просторі імен Root, яке поділяється на 4 підпростори: Default, Security, CIMv2 та WMI. Для ідентифікації компонентів ПК використовують CIMv2, а для роботи з подіями – WMI. Інформацію про компоненти можна отримати після виконання запиту до класів. Запит здійснюється за допомогою мови запитів WMI Query Language (WQL). Дана мова є різновидом Structured Query Language (SQL) та має обмеження на роботу с даними – користувачеві доступно лише зчитування інформації. Стандартний запит WMI представляє собою звичайний рядок, який містить інформацію про параметр класу та назву класу, з якого його потрібно отримати.

Бібліотека OpenHardwareMonitor на відміну від System.Management надає наступну інформацію про апаратну частину ПК: відеокарта, процесор, материнська плата, жорсткий диск, оперативна пам'ять, шина, BIOS. OpenHardwareMonitor зберігає класи до свого простору імен root/OpenHardwareMonitor. Дана бібліотека зрозуміліша та легша у використанні за рахунок власного API та розподілу інформації на дані про компонент та його датчики (рис 1). Кожен клас Hardware має власні сенсори які показують інформацію про вольтаж, частоту, температуру тощо. Бібліотека дозволяє отримати інформацію і через звичайний WMI запит, який звертається то простору імен root/OpenHardwareMonitor.

Рисунок 1 – Різниця структури класів в просторі імен

Висновки. Отже, проблему ідентифікації компонентів ПК засобами мови програмування C# можна вирішити, використовуючи описані вище бібліотеки. Вибір бібліотеки потрібно виконувати в залежності від компонентів, які потребують ідентифікації.

Для отримання значного обсягу інформації про системні компоненти, сервіси та події краще застосувати System.Management. В іншому випадку, коли необхідна інформація про апаратну частину ПК, її ідентифікатори та характеристики доцільно буде використати OpenHardwareMonitor.

Список літератури

1. Open Hardware Monitor [Електронний ресурс]. – Режим доступу: https://github.com/openhardwaremonitor/openhardwaremonitor

2. Windows Management Instrumentation [Електронний ресурс]. – Режим доступу: https://msdn.microsoft.com/en-us/library/aa394582(v= vs.85).aspx

3. Мова програмування C# [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/C_Sharp

УДК 004.514

Реклама, как угроза информационно-психологической безопасности личности

Савенко А.Г., ассистент, магистр технических наук,
Заяц И.Л., студент 3 курса, Лазаренко Р.А., студент 3 курса
Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники, г. Минск

Информационно-психологическая безопасность личности в информационном пространстве рассматривается как одна из центральных ценностей современного общества. Одним из каналов воздействия на личность является реклама, влияние которой носит двойственный характер. Рекламная безопасность связана с проблемами свободы выбора и идентичности человека в современном информационном обществе.

Общий источник внешних угроз информационно-психологической безопасности личности – та информация, которая не только вводит людей в заблуждение, в мир иллюзий, не позволяет адекватно воспринимать окружающее и самого себя, но и травмирует сознание индивида своим возрастающим количеством [1].

Интернет становится формой организации совместной информационно-познавательной и коммуникативной деятельности людей, выступая носителем нравственных ценностей [2]. Цель рекламы в интернете – умело скрыть недостатки и подчеркнуть достоинства товара или услуги. Поэтому большая часть рекламы – обман. Несмотря на внешнюю простоту, реклама использует достаточно сложные механизмы воздействия на человека. Риски для потребителя могут быть связаны не только с тем, что недобросовестная реклама намеренно вводит его в заблуждение, но и с тем, что она освобождает человека от необходимости мыслить самостоятельно, взвешивать соответствующие обстоятельства.

У большинства населения сознание постепенно начинает исполнять роль хранилища штампов и стереотипов, которые воспроизводятся в том же виде, в котором были получены. Процесс критического восприятия информации часто отсутствует.

Специалисты называют эти психологические изменения «руинизацией психики», при которой человеку становится все труднее использовать свои потенциальные интеллектуальные и волевые возможности. В постсоветских странах феномен руинизации особенно выражен у молодых поколений, у которых формирование сознания пришлось на последнее десятилетие.

Первопроходцами в блокировке рекламы стала компания Apple. В сентябре 2015 года компания представила iOS 9 — новую версию операционной системы для мобильных устройств. Тогда в браузере Safari

появилась поддержка расширений, способных «блокировать контент». Adblock Plus и другие поставщики подобных расширений для десктопных браузеров смогли опубликовать в App Store свои продукты для Safari.

По данным счётчика «Рейтинг Mail.ru», 9,66% пользователей рунета используют блокировщики. При этом на пользователей такого ПО приходится 10,44% сессий и 11,92% просмотров, что подтверждает гипотезу: блокировщиками пользуется продвинутая и активная, наиболее интенсивно взаимодействующая с сайтами аудитория. Отсюда вытекает очевидное следствие, что аудитория, которая использует блокировщики, наиболее активна, потому что пользоваться интернетом без рекламы гораздо удобнее и приятнее.

С момента появления первых блокировщиков началась гонка вооружений между рекламщиками и блокировшиками. Рекламщики становились все изощренными в методах обхода блокировок. Большинство популярных «эдблокеров» сегодня умеют не только блокировать рекламу, но и запрещать рекламным системам собирать информацию о пользователе.

Самые первые блокировщики имели в основе следующий принцип: они скрывали от глаз пользователя рекламные элементы, которые уже были загружены на страницу. Сейчас этот способ используется в некоторых программах как вспомогательный. Также можно вспомнить браузерные расширения, которые скрывают с сайтов и соцсетей тексты на определенные тематики, ориентируясь по ключевому слову.

Современные «эдблокеры» препятствует коммуникации между отображающей веб-страницу программой, например, браузером, и серверами, с которых загружаются рекламные элементы (баннеры, объявления, видео, попапы и так далее). Или другие элементы, которые он призван блокировать (например, счетчики статистики или кнопки соцсетей).

Основной проблемой на данный момент является то, что в основе блокировки рекламы в интернете лежит не искусственный интеллект на самообучающихся нейросетях, а ручной труд, причем не только разработчиков, но и сообщества.

Продукт этого ручного труда – фильтры, то есть списки правил для определения рекламы и отделения её от полезного контента. Критерии отделения рекламы от всего остального обычно определяются волевым решением основателя того или иного фильтра с учётом мнения сообщества, которое помогает его формировать. Самый популярный набор фильтров называется EasyList. Он не принадлежит какому-то конкретному блокировщику, но используется в большинстве популярных продуктов (в том числе в Adblock Plus, uBlock Origin, AdGuard).

Именно от того, насколько оперативно обновляются фильтры, зависит качество блокировщика. Заинтересованные в показе рекламы компании постоянно работают над обходом блокировки. Они меняют все уже

попавшие в фильтры идентификаторы рекламных элементов или шифруют запросы страниц к серверам рекламы, чтобы блокировщик их не остановил. Эта деятельность требует столь же постоянных контрмер.

Однако ещё до того, как началась эта борьба, началась саморегуляция. В 2011 году Adblock Plus объявил о запуске программы Acceptable Ads. Рекламодатели и площадки, согласившиеся адаптировать свою рекламу под критерии допустимости и качества, помещались в «белый список», а пользователи Adblock Plus видели их рекламу (если не отключали это в настройках).

Учитывая, как быстро происходит смена подходов к отображению рекламных объявлений и нахождению способов борьбы с ней, современные способы блокирования рекламы являются неудовлетворительными. Сервисы не могут реагировать достаточно быстро на обратную связь пользователей, в следствие чего новая реклама появляется быстрее, чем блокируют старую.

Для обеспечения безопасности ментального здоровья следует разработать нейронную сеть, с возможностью настройки отображаемой рекламы. Система будет сама подстраиваться под предпочтения пользоваться, и отталкиваясь от них, будет блокировать ту или иную рекламу. Этот подход обеспечит своевременную реакцию на новые угрозы.

Автоматизировать распознавание рекламы сложно, помимо прочего, еще и потому, что даже у людей нет единого мнения насчет того, что является рекламой, а что нет. Поэтому приложение будет отслеживать поведение конкретного пользователя на странице.

После установки приложения пользователю предлагается выбрать определенный паттерн блокировки рекламы. В него будут включаться сайты из «белого списка», а также наиболее приемлемые паттерны рекламы по отзывам других пользователей.

Основываясь на общей статистике приложение будет скрывать ту рекламу, которая оказалась наиболее неприемлемой, по мнению других пользователей. Рейтинг неодобрения пользователей будет основываться на использовании пользователями одного из способов защиты от негативного информационного влияния – «ухода». Приложение будет отслеживать положение курсора, клики и окна, которые будут активно использоваться. Будет отслеживаться время насколько долго реклама находилась на странице, пока пользователь ее не закрыл. Чем это время больше – тем выше лояльность пользователей к данному типу рекламы.

Также активно будет использоваться технология аиртрекинга [3]. Она будет отслеживать на сколько долго пользователь фокусировал внимание на блохах рекламы. Также, как и в случаях с пользовательским вводом, чем выше это время – тем выше лояльность пользователей.

Основываясь на этих данных, приложение будет скрывать «неугодную» для пользователя рекламу. Однако полностью скрыть всю

рекламу не представляется возможным. Это происходит потому, что реклама является, в большинстве своем, основным источников доходов для владельцев сайта и крупных поисковых систем.

Постепенно накапливая и анализируя информацию, будут приниматься соответствующие меры по блокированию рекламы.

Список литературы

1. Дроздова А. В. Воздействие рекламы на безопасность личности в современном информационном обществе: социально-психологический аспект. // Вестник Московского университета. Серия 14. Психология - 2011. – №4 – С. 58-65.
2. Филиппова Т.В. Интернет как инструмент социологического исследования // Социологические исследования. – 2001. – №4 – с. 115-122.
3. Окулография [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Окулография. Дата доступа: 20.03.2018.

УДК 004.67

Алгоритм ранжування вузлів у квазіієрархічних мережах соціального характеру

Соболєв А.М., аспірант
Науковий керівник – Ланде Д.В., д.т.н., старший науковий співробітник
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", м. Київ

Під визначенням **"мережа соціального характеру"** потрібно розуміти мережу, вузлами якої є соціальні суб'єкти, а зв'язками – контакти, які супроводжуються обміном інформації між ними. Квазіієрархічною мережею слід вважати таку мережу, яка близька до ієрархічної, але її ієрархія порушується невеликою кількістю додаткових зв'язків, типовим прикладом є соціальні мережі, які розвертаються на просторах глобальної мережі Інтернет. Під ранжуванням мережі соціального характеру потрібно розуміти процес упорядкування вузлів за конкретною ознакою, який дозволяє визначити впливовість заданих вузлів між собою.

Для візуального представлення, дані мережі зображають у вигляді направленого графа, в якому вузлами виступають маркери суб'єктів а ребрами направлені зв'язки, які відбуваються між ними. У математичному представленні такий граф зображають у вигляді матриці суміжності вузлів, а значення у клітинці даної матриці відображає кількість направлених зв'язків.

Запропоновано алгоритм ранжування вузлів в соціальних мережах, що дозволяє визначити найбільш впливові вузли мережі та здійснювати аналіз в мережі.

Аналіз квазіієрархічної мережі. Розглянемо схему квазіієраріїчної мережі соціального характеру на рис. 1, де зв'язками між вузлами виступають процеси, які відбувались між ними для передачі інформації. Також, цифра біля кожного зв'язку відображає кількість фактів взаємодії з конкретним вузлом у мережі. На таких схемах вузлами, зазвичай, можуть представляти почтові скриньки, профілі в соціальних мережах, телефонні номери, нікнейми в чатах, ідентифікатори співробітників в компанії та інше.

Для ранжування вузлів в даній мережі потрібно використовувати модифікований алгоритм HITS.

$$hub\ A_i = \sum_{j \leftarrow i} auth\ A_j \cdot \ln(E_{ij}),$$

де $auth\ A_i$ – показник авторства вузла A_j мережі;
$hub\ A_i$ – показник посередництва вузла A_j ;

E_{ij} – вага зв'язків між вузлами A_i та A_j.

$$auth\ A_i = \sum_{j \to i} hub\ A_j \cdot \ln(E_{ij}),$$

де $hub\ A_i$ – показник посередництва вузла A_j мережі;

$auth\ A_i$ – показник авторства вузла A_j;

E_{ij} – вага зв'язків між вузлами A_i та A_j.

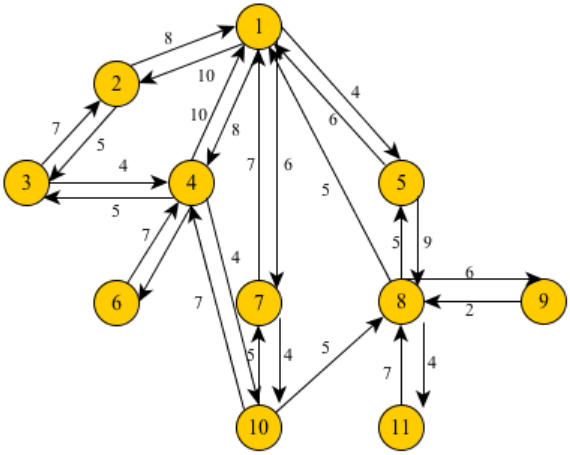


Рисунок 1 –Квазіієрархічна мережа соціального характеру

1. Після ранжування вузлів мережі буде отримано два параметри, перший $auth\ A_i$ буде відповідати за авторство інший $hub\ A_i$ за показник посередництва в мережі.
2. Для отримання середнього значення двох параметрів використати метрику, яка об'єднує у собі інформацію про показники авторства та посередництва модифікованого алгоритму HITS (F-міру) та відсортувати отримані дані в порядку спадання параметру F-міри.
3. Здійснити аналіз вузлів з найбільш високим значенням отриманого параметру F-міри.

Алгоритм розрахунку F-міри для значення $auth$ та hub:

$$F(A_j) = \frac{2}{\frac{1}{auth\ A_j} + \frac{1}{hubA_j}},$$

де $F(A_j)$ – F-міра вузла A_j мережі;

$hub\ A_i$ - показник посередництва;

$auth\ A_i$ – показник авторства.

Висновки. Запропоновано алгоритм для аналізу мереж соціального

характеру, який є ефективним для ранжування вузлів в даних мережах. Розглянутий алгоритм дозволяє визначити найбільш впливові вузли та на основі чого, здійснювати аналіз мереж соціального характеру.

Список літератури

1. Langville A.N., Meyer C.D. Google's PageRank and Beyond: The Science of Search Engine Rankings. – 2013. – P.115-121

2. Bargh J.A., Chen M., Burrows L. Automaticity of Social Behavior: Direct Effects of Trait Construct and Stereotype Activation on Action // Journal of Personality and Social Psychology. – 1996. – 71. – № 2. – P. 230-244.

3. Liu Y.Y., Jean-Jacques Slotine J.J., Barabasi A.L. Control centrality and hierarchical structure in complex networks // PLOS ONE, 2012. – 7. – № 9. – P. e44459 (1-7)

УДК 004.92

Перехід від Canvas до Open GL ES у графічних додатках для Android

Старкіна О.Д., студентка 3 курсу
Науковий керівник – Мелешко Є.В. к.т.н., доцент
Центральноукраїнський національний технічний університет,
м. Кропивницький

Чимало додатків для платформи Android містять складні графічні елементи, відображення яких вимагає значних ресурсів. Під час розробки таких елементів слід обирати найоптимальніший інструмент для їх реалізації. Нерідко вже існуючі елементи інтерфейсу переписують з використанням більш оптимальних інструментів.

Canvas – спеціальний клас для роботи з графікою, що дозволяє створювати анімацію та малювати складні зображення.

Open GL ES (OpenGL for **E**mbedded **S**ystems – OpenGL для вбудованих систем) **–** Open Graphics Library бібліотека з відкритим вихідним кодом для роботи з 2D та 3D графікою.

Робота з Canvas та Open GL ES

За допомогою Canvas малювання відбувається на растровому зображенні (Bitmap), яке потім розміщується на екрані. Canvas може використовуватись разом з SurfaceView. SurfaceView – спеціальний підклас View, який надає поверхню для малювання в ієрархії View. Для роботи слід створити екземпляр класу SurfaceView та імплементувати SurfaceHolder. Callback, описати клас Thread, де буде відбуватися процес малювання.

При використанні Open GL ES слід розуміти як працювати з двома основними класами: GLSurfaceView та GLSurfaceView.Renderer. GLSurfaceView – це View де можна малювати об'єкти та управляти ними, схожий на SurfaceView. GLSurfaceView.Renderer – інтерфейс, що визначає методи для малювання у GLSurfaceView. Для роботи треба реалізувати даний інтерфейс та приєднати його до екземпляру GLSurfaceView, використовуючи GLSurfaceView.setRenderer().

Перехід від Canvas до Open GL ES

В рамках Global Game Jam 2017 автором була розроблена гра для пристроїв з ОС Android на базі рушія створеного власноруч.

Рушій містить графічний модуль (рис.1), що використовує Canvas, однак ігрова графіка потребує значної швидкості і складності відображення, тож під час доробки рушія було вирішено замінити Canvas на Open GL ES.

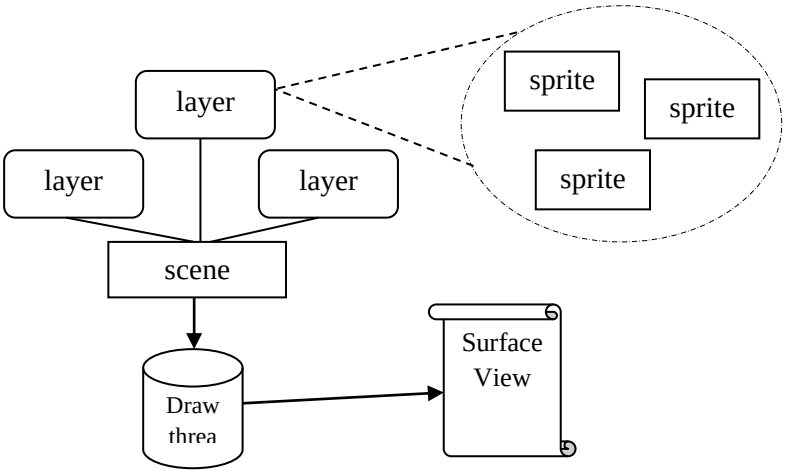


Рис. 1 – Структура графічного модуля (з використання Canvas)

При переході від Canvas до Open GL ES найбільшу складність являє реалізація класів, що описують потрібні у роботі фігури, а також реалізація власне процесу малювання. На рівні взаємодії з іншими частинами рушія навпаки відбудеться спрощення (рис.2), адже замість власного потоку і власного SurfaceView треба буде лише імплементувати інтерфейс GLSurfaceView.Renderer та приєднати його до екземпляру GLSurfaceView; всередині перевизначеного методу onDrawFrame описати логіку малювання поточного фрейму.

Тож замість власного потоку використовується GLSurfaceView, який інкапсулює потік рендеренгу, а власне малювання відбувається набагато швидше.

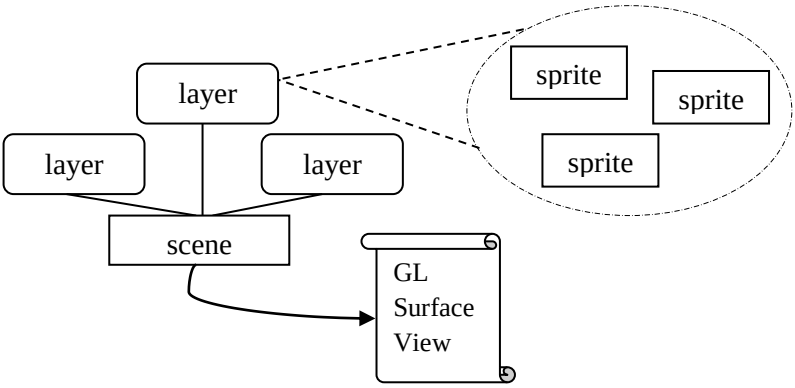


Рис. 2 – Структура графічного модуля (з використання Open GL ES).

УДК 004.9

Можливість застосування еталонних моделей ІТ для побудови та аналізу інформаційних моделей технічних та соціальних структур

Сьомочкина С.В., к.т.н., доцент
ДВНЗ «Криворізький національний університет», м. Кривий Ріг

Надмірність, надлишковість та різноманітність сучасних джерел інформації перевантажують засоби її сприйняття. Проблема полягає в тому, що обробка та усвідомлення, використання інформації людиною не встигає за засобами і методами збору і генерації контенту, які занадто швидко розвиваються, що знецінює і робить неефективними останні досягнення у галузі інформаційних технологій.

Методи вирішення, які пропонуються:

1) Виділення пріоритетних напрямків розвитку ІТ з подальшою класифікацією та упорядкуванням існуючих знань. Найважливішою складовою є гуманізація – пріоритети для застосування в галузях здоров'я, екології, медицини, освіти та розвитку особистості. Комерціалізація, звичайно, необхідна складова ринкових відносин, але потрібно виховувати свідомість користувача ІТ, для зниження попиту на екстенсивні методи, перевиробництво, нераціональне використання ресурсів тощо.

2) Усунення інформаційної надмірності – за рахунок систематизації існуючих ресурсів та створення чіткої структури для подальшого розвитку. Якість та застосовність інформації повинні мати пріоритетне значення порівняно з її кількістю та обсягом. Особливо важливим це є на освітньому рівні, щоб допомогти зорієнтуватися користувачеві, починаючи від школяра, до майбутнього фахівця, надаючи зручний інструментарій для творчої та наукової діяльності, замість низькоякісних або навіть шкідливих розважальних ресурсів. Цьому також сприяє відповідне залучення заходів інформаційної безпеки.

3) Зниження складності сприйняття - інтуїтивного, адаптивного, сенсорного. Ускладнення технологій призводить до погіршення адаптаційного рівня людини стосовно природних умов, зниження фізичних та аналітичних здібностей. Застосування інформаційних технологій повинне бути тільки допоміжним засобом, а не самоціллю.

Для більш ефективного виконання задач класифікації та систематизації інформаційних ресурсів можливо та корисно застосовувати існуючі архітектурні специфікації (еталонні моделі) інформаційних технологій або систем. Ці моделі визначають структуризацію конкретних розділів ІТ, задаючи тим самим контекст розробки відповідних цим розділам стандартів. Аналіз архітектурних специфікацій ІТ показує, що сучасна методологічна база відкритих систем є складною системою концептуальних, структурних, функціональних, поведінкових і лінгвістичних моделей, взаємопов'язаних між собою, а також допоміжних процедур і засобів [1].

Але еталонні моделі можуть розглядатися не тільки в якості фундаментальних моделей (законів) в просторі IT (інформаційно-технологічної «матерії»), але також і в багатьох суміжних технічних та соціальних галузях.

На першому етапі побудови інформаційної моделі потрібно зробити опис функціональної області, а на другому – визначитись, застосування яких уніфікованих, єдиних програмних та інформаційних рішень є необхідним. Окрім систематизації та структуризації розробка таких моделей дозволяє вивчати поведінку об'єктів моделювання під впливом різних факторів, причому незалежно від природи їх формування – енергетичної, економічної, соціальної, біологічної тощо.

Серед загальних підходів до розробки необхідно відзначити:

- активне використання міжнародного досвіду, глобалізацію рішень, пріоритет міжнародних стандартів над національними;
- публічний характер документів в області розробки;
- орієнтацію на взаємодію і використання internet-технологій і Web-сервісів при міжсистемній взаємодії.

Наприклад, модель RM ODP (Reference Model of Open Distributed Processing) використовує підхід об'єктного моделювання до специфікації систем та визначає п'ять точок зору: організаційну, інформаційну, обчислювальну, інженерну та технологічну [1].

Також з цією метою можливе використання базових фреймворків, наприклад DoDAF (Department of Defense Architecture Framework), який надає досить зручну методологію для складання моделей.

Відмінною особливістю DoDAF є орієнтація на дані, що визначає клас систем, на проектування яких орієнтований цей фреймворк – це перш за все системи збору, зберігання і обробки даних з метою їх використання в процесі прийняття рішень. В рамках DoDAF використовується мета-модель даних Data Meta-Model. Вона являє собою онтологію і має кілька рівнів, кожен з яких відображає найбільш важливий для конкретної групи користувачів рівень представлення інформації. Крім того, DoDAF дає користувачеві значно велику свободу вибору інструментальних засобів і моделей для вирішення конкретного завдання і активно пропонує йому вибирати тільки потрібні моделі [2].

Таким чином, створення відкритих бібліотек для базових відомостей з найважливіших галузей знань та об'єднання інструментів онтології і таксономії дозволить упорядковувати та інтегрувати існуючі, а також створювати нові, досконаліші моделі технічних та соціальних структур.

Список літератури

1. Информационные технологии: учебник / под ред. В.В. Трофимова. – М.: Издательство Юрайт; ИД Юрайт, 2011. – 624 с.

2. Архитектура информационных систем: учебник / Б. Я. Советов, А.И. Водяхо, В.А. Дубенецкий, В. В. Цехановский. — М. : Издательский центр «Академия», 2012. — 288 с.

УДК 004.031.4

О некоторых вопросах применения технологии Интернета вещей в нефтегазовой промышленности

Фаталиев Т.Х., зав. отделом,
Мехтиев Ш.А., зав. отделом
Институт информационных технологий НАНА, г. Баку, Азербайджан

Быстрое развитие информационно-коммуникационных технологий способствовало внедрению современных датчиков, а также Интернета вещей (Internet of Things- IoT) различного назначения, оборудования для сбора данных, беспроводных сетей, коммуникационных устройств и решений для удаленных вычислений. Эта эволюция – основа структуры современных Киберфизических систем (КФС) (Cyber Physical System-CPS). КФС – это физическая и инженерная система, состоящая из многочисленных компонентов, в том числе внедренных IoT различного назначения, управляемых компьютерными алгоритмами, тесно интегрированная с Интернетом и пользователями [1]. К ним относятся такие системы, как Smart Cities, Smart Grids, Smart Factory, Smart Buildings, Smart Houses и Smart Cars, где каждый объект подключен ко всем другим объектам. Они призваны обеспечить адаптивное, гибкое и экономически эффективное функционирование. Можно предположить, что нефтегазовая промышленность в какой-то степени является фабрикой по обработке информации, что вписывается в информационно-технологическую концепцию КФС. Это большое количество устройств со встроенными сенсорами, процессорами и средствами хранения данных; интеграция, позволяющая достигнуть наибольшего эффекта путем объединения отдельных компонентов в большую систему; исключение человеческого фактора при принятии решений (human out of loop) либо дополнение способностей человека (human in the loop).

IoT по определению МСЭ-Т – это "глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий" [2] и, как концепция, определяет развитие промышленности на ближайшие годы. Обязательным условием функционирования любого производства, в том числе нефтегазового комплекса в рамках этой концепции является прямое информационное взаимодействие оборудованных всевозможными сенсорами различных типов объектов, наличие интеллектуальных устройств, которые смогут передавать данные, принимать решения и взаимодействовать друг с другом.

Архитектура IoT может быть представлена четырьмя системами [3]:

1. Вещи: они определяются как уникально идентифицируемые узлы, прежде всего сенсоры (датчики), которые общаются без взаимодействия человека с использованием стандартных протоколов.
2. Шлюзы: это подключение к Интернету, безопасность и управляемость.
3. Сетевая инфраструктура, состоящая из маршрутизаторов, концентраторов, шлюзов, повторителей и других устройств, которые управляют потоком данных.
4. Облачная инфраструктура: содержит кластеры виртуализированных серверов и хранилища, которые объединены в сеть.

С момента появления и развития микропроцессоров и сетевых устройств активно изучалась возможность применения микроконтроллеров, дополненных сенсорами и механизмами, для обеспечения большей надежности, эффективности и безопасности производственных процессов в нефтегазовой промышленности (геологические изыскания, бурение, добыча, переработка, транспортировка и т.п.), так как здесь высокий уровень финансовых, экологических и гуманитарных рисков.

Так в [4] указано, что процессы обработки информационных потоков и управления в нефтегазодобывающих предприятиях происходят на трех уровнях. На нижнем уровне при помощи локально-групповых устройств осуществляется мониторинг, сбор данных с сенсоров и первичная обработка информации с целью выработки управляющих воздействий на объекты нефтегазодобычи в режиме реального времени. Замена консервативных и в большей степени ручных средств управления и мониторинга и обеспечение процессов добычи, транспортировки и переработки в нефтегазовой отрасли новыми, удобными для установки сенсорами позволяет вести непрерывный автоматический контроль за технологическими процессами, регистрировать и накапливать данные о параметрах, производить удаленную настройку. Тем самым можно повысить надежность, безопасность, энергоэффективность, влиять на экологические показатели, такие как выбросы газа, утечки и разливы первичного сырья. На следующем уровне вырабатываются решения об оптимизации процессов, определении периодичности ремонтных мероприятий для сокращения простоев и оптимизации интервалов техобслуживания узлов и агрегатов, обеспечения эффективной работы и т.д. Незапланированные простои из-за поломок оборудования, которые приводят к потере времени и финансов, можно сократить благодаря внедрению интеллектуальных систем технического обслуживания, в том числе и э-техобслуживания. Третий уровень – это уровень компании (корпорации), на котором реализуется аналитика (обработка больших данных), по результатам которой осуществляется координация действий входящих в состав компании (корпорации) предприятий и структур для

достижения общей эффективности, принимаются меры по повышению безопасности и уменьшению рисков.

Данное представление информационных потоков согласуется с архитектурно-технологической моделью IoT, в которой:

1. Сенсоры измеряют какие-либо физические параметры;
2. Микроконтроллеры обеспечивают интеллектуальность;
3. Имеется возможность коммуникации по Интернету;
4. Возможно использование облачных сервисов.

Необходимо отметить, что в облачных сервисах IoT происходит перераспределение нагрузки на туманные (fog) и мобильные (mobile) вычисления. Например, в концепции «умное месторождение» (smart field) от компании Schneider Electric [5] на основе данных от проводных и беспроводных сенсоров в режиме реального времени моделируются процессы внутри пласта и осуществляется управление добывающими нефть насосами различных модификаций. Данные сохраняются в памяти интеллектуальных контроллеров и периодически передаются в диспетчерский пункт, где обрабатываются специальными программами. За счет внедрения интеллектуальной системы сокращаются время простоев оборудования, затраты на электричество, пар, воду, а также оптимизируется весь процесс добычи.

В международной практике объекты нефтегазовой промышленности относятся к критическим инфраструктурам и, безусловно, широкое распространение IoT здесь будет зависеть от гарантий безопасности в целом как на уровне системы, так и на уровне IoT (сенсоры, съем данных, обработка, хранение и передача информации). Известные случаи аварий на объектах нефтегазовой промышленности показывают насколько уязвима структура IoT к кибератакам [6].

В рекомендации МСЭ-Т безопасность IoT предлагается решать, исходя из его трехуровневой архитектурно-технологической модели, так как потенциальные угрозы могут проявиться на каждом уровне [2].

Анализ теоретических и реальных угроз и атак на критические инфраструктуры показывает, что на каждом уровне необходимы решения по авторизации, аутентификации, защиты конфиденциальности и целостности данных [7].

Виды угроз в IoT, рассмотренные в многочисленных источниках, также могут быть реализованы злоумышленниками при реализации IoT в нефтегазовой промышленности. Например, на уровне устройств могут быть считаны значения с сенсоров, которые важны для функционирования всей системы. Открытые или не полностью устраненные проблемы безопасности в IoT можно в целом классифицировать следующим образом:

- Стандартизация для гетерогенных устройств;
- Масштабируемость;
- Конфиденциальность;

- Уязвимость программного и аппаратного обеспечения;
- Физическая безопасность устройств;
- Энергопотребление и эффективность.

Выводы. Существует множество возможных направлений дальнейших исследований в области применения и обеспечения безопасности IoT, в первую очередь из-за его постоянно растущего и всеобъемлющего характера. Согласно прогнозу «Gartner» к 2020 году к Интернету подключится 20 миллиардов объектов. Любая атака на одном подключенном узле может разрушить инфраструктуру и привести к росту связанных рисков. Чтобы гарантировать успешную реализацию и практическую полезность IoT, необходимы решения по внедрению стандартов, обеспечению качества обслуживания, конфиденциальности и надежности, управлению большими объемами данных и обеспечению эффективности.

Данная работа выполнена при финансовой поддержке Фонда Науки Государственной нефтяной компании Азербайджанской Республики – **Грант № 01 LR – HANA, SOCAR ФН 2017**

Список литературы

1. Фаталиев Т.Х., Мехтиев Ш.А., Некоторые вопросы безопасности КФС, Актуальные проблемы информационной безопасности, III Республиканский научно-практический семинар, Баку, 8 декабря 2017 г.

2. Recommendation ITU-T, Y.2060: Overview of the Internet of things, 06/2012.[Online]. Available: https://www.itu.int/rec/T-REC-Y.2060-201206-I

3. Banafa A, Securing the Internet of Things (IoT). [Online]. Available: https://www.researchgate.net/publication/281525537_Securing_the_Internet_of_Things_IoT

4. Алиев А.И., Мехтиев Ш.А., Алгулиев Р.М., Об иерархически-распределенной системе управления и обработки информации в НГДУ / Проектирование автоматизированных систем контроля и управления сложными объектами, Харьков, 1986, с. 54-55.

5. Schneider Electric. Smart field. [Online]. Available: https://www.schneider-electric.com/en/search/smart+field

6. Critical Infrastructure. [Online]. Available: https://www.pandasecurity.com/rfiles/resources/forms/whitepapers/1611-WP-CriticalInfrastructure-EN.pdf

7. Oracevic A., Dilek S., Ozdemir S. Security in Internet of Things: A Survey, Conference ISNCC, 2017

УДК 004.3

Апаратно-програмний комплекс для контролю параметрів з пунктів обліку теплової енергії

Шаліновська Н.В., студентка, Минайленко Р.М., к.т.н., доцент
Центральноукраїнський національний технічний університет, м. Кропивницький

Розвиток сучасної обчислювальної техніки, електроніки й радіотехніки дозволяє створювати складні системи, призначені для виконання різних наукових, виробничих, технологічних завдань [1-5]. Використання таких систем покликано поліпшити якість, ефективність тих або інших виробничих цілей.

Існує кілька наукових напрямків, в основі яких лежить об'єднання обчислювальної техніки й електроніки з технологічними процесами та радіоапаратурою [3-6]. Якщо раніше об'єднання різних високонаукових технологій і засобів обчислювальної техніки використовувалося в основному в рішенні різних наукових проблем, таких як освоєння космосу, вивчення надр землі й багатьох інших, то зараз такі технології використовуються й у повсякденному житті. Одним з напрямків використання мікропроцесорної техніки, є її застосування для реалізації контролю параметрів різних комунальних мереж та управління ними.

Особливістю проекту, що розробляється, є його практична реалізація у складі діючої системи теплопостачання міста Кропивницький. При цьому передбачено технічне оснащення більше 100 пунктів обліку теплової енергії, розташованих у Кропивницькому. Апаратно-програмний комплекс призначений для передачі й контролю вимірюваних параметрів з пунктів обліку теплової енергії, зосереджених на території міста Кропивницький, на центральний диспетчерський пункт.

Застосування апаратно-програмного комплексу дозволить підвищити продуктивність роботи системи теплопостачання міста, поліпшить оперативність виконання тих або інших відбудовних робіт, так як комплекс буде стежити за роботою системи теплопостачання цілодобово.

Список літератури:

1. Щелкунов Н.Н., Дианов А.П. Микропроцессорные средства и системы. – М., Радио и связь, 1989.-288с.

2. Сташин В.В., Урусов А.В., Мологонцева О.Ф. Проектирование цифровых устройств на однокристальных микроконтроллерах. – М., Энергоатомиздат, 1990.-224с.

3. Майоров В.Г., Гаврилов А.И. Практический курс программирования микропроцессорных систем. – М., Машиностроение, 1989.-272с.

4. Каган Б.М., Сташин В.В. Основы проектирования микропроцессорных устройств автоматики. М., Энергоатомиздат, 1987.-304с.

5. Рафикузаман М. Микропроцессоры и машинное проектирование микропроцессорных систем. В 2 кн. Кн.1. – М.,Мир.,1988.-312с.

6. Уильямс Г.Б. Отладка микропроцессорных систем. – М., Энергоатомиздат. 1988.-253с.

УДК 004.9

Властивості потокової бібліотеки Tweetinvi для аналізу твітів

Шингалов Д.В., аспірант
Науковий керівник – Мелешко Є.В., к.т.н., доцент
Центральноукраїнський національний технічний університет, м. Кропивницький

Twitter забезпечує значний рівень доступу до даних про активність користувачів за допомогою своїх API-функцій, які можуть використовуватися для відстеження поточної активності користувачів або використання окремих ключових слів і хеш-тегів у твітах. Twitter API дозволяє користувачам автоматично отримувати дані про будь-які твіти, що містять задані ключові слова (включаючи хеш-теги), з порівняно незначними обмеженнями по часу та кількості запитів з однієї IP-адреси [1]. Однак існують суттєві обмеження щодо даних, які можуть бути отримані безпосередньо через API.

Для роботи з API-функціями Twitter зручно використовувати відкриті бібліотеки, наприклад, бібліотеку Tweetinvi для мови програмування C#, що дозволяє працювати з REST та потоками Twitter API [2].

Потоки – це дуже потужні інструменти, які можна використовувати для аналізу Twitter, що дають доступ до інформації у реальному часі. Потоки лежать в основі бібліотеки Tweetinvi.

Твіттер має 3 типи потоків для публічних API.

- Зразковий потік: повертає випадкові публічні твіти;
- Користувацькі потоки: відео, будь-яка мультимедійна та текстова інформація про будь-яку подію, що відбувається на сторінці конкретного користувача;
- Відфільтрований потік: повертає всі публічні твіти, що відповідають певному набору критеріїв.

В першу чергу, слід зазначити, що кожен з різних типів потоків створюються зі статичного класу Stream всередині простору імен Tweetinvi. Це робиться за допомогою функції Stream.Create Stream() де вказано тип потоку. Також роботу кожного типу потоку може бути тимчасово припинено, відновлено, і зупинено. При виклику будь-якого з цих методів, Stream.StreamState потоку буде змінено. Цю властивість можна використовувати для визначення поточного стану потоку [3].

Потоки Tweetinvi можуть бути використані, щоб повідомити про те, що надійшло повідомлення з потоку в Twitter:

- JsonObjectReceived: повідомляє, що повідомлення json були отримані;
- UnmanagedEventReceived: повідомляє, що було отримано повідомлення, яке не обробляється Tweetinvi;

- LimitReached: повідомляє, що потік намагається отримати доступ до більш ніж 1% від загальної кількості твітів, що було опубліковано;
- DisconnectMessageReceived: повідомляє, що Twitter вирішив закрити цей потік з'єднання;
- TweetDeleted: повідомляє, що твіт був видалений;
- TweetLocationInfoRemoved: повідомляє про те, що геоінформаційний твіт був видалений;
- TweetWitheld: повідомляє, що твіт був утриманий у вашій країні;
- UserWitheld: попереджає, що користувач був не у вашій країні;

Зразковий потік є найпростішим типом потоків. Він просто повертає 1% всіх публічних твітів, що публікуються в Twitter в будь-який час. Twitter випадковим чином вибирає один твіт на кожні 100 твітів і публікує такий твіт в потоці. Цей потік є досить цікавим для дослідників і дозволяє проаналізувати деякі статистичні дані.

Користувацькі потоки дозволяють отримати широкий спектр даних, пов'язаних з конкретним користувачем. Наприклад, ви можете отримувати сповіщення, коли користувач публікує повідомлення, додає друга або просто робить будь-який ретвіт [4]. Також цей потік дозволяє отримувати сповіщення про вхідні повідомлення, нових підписників, нові рекомендовані списки та багато інших подій користувача.

У випадку відфільтрованих потоків можна вибирати тип твітів, які повертаються за трьома критеріями:

1. Фільтр за ключовими словами за допомогою методу AddTrack;
2. Фільтр по місцю розташування, використовуючи метод AddLocation;
3. Фільтр по конкретному користувачу за допомогою методу AddFollow.

Коли принаймні один фільтр був створений, можна запустити трансляцію потоку. Також можна налаштувати кожен з фільтрів, таким чином, щоб кожен з них містив декілька значень.

Список літератури

1. Harris, C. (2007). Tweets at Your Library. School Library Journal. 53(11), Retrieved August 8 2009 from Library Literature and Information Science Fulltext database. 24-25.
2. Tweetinvi [Electronic resource] - Access mode: https://github.com/linvi/tweetinvi
3. Brown P.F., Desouza P.V., Mercer R.L., Pietra V.J.D., and Lai J.C. (1992). Classbased n-gram models of natural language. Computational Linguistics, 18(4), 467–479.
4. Spence Green, Marie-Catherine de Marneffe, and Christopher D Manning. (2012). Parsing models for identifying multiword expressions. Computational Linguistics, 39(1), 195–227.

UDC 621.398.724

Simulation of neuron-equivalentors as hardware accelerators of self-learning equivalent-convolutional neural structures (slecns)

Krasilenko V.G., Ph. D., S. Sc., As. Prof., Lazarev A.A., Ph. D., As. Prof., Nikitovich D.V.
Vinnytsia National Technical University, s. Vinnytsia

Introduction, analysis of recent research, publications. For many applications used in the creation of biometric systems, machine vision systems are necessary to solve the problem of object recognition in images. The basis of most known methods and algorithms consists in comparing of two different images of the same object or its fragment. Discriminant measure of the mutual alignment reference fragment with the current image, the coordinate offset is often a mutual two-dimensional correlation function. In paper [1, 2, 3] it was shown, that to improve accuracy and probability indicators with strong correlation obstacle-damaged image, it is desirable to use recognition methods based on mutual equivalently 2D spatial functions, nonlinear transformations and adaptive-correlation weighting. For the recognition and clustering of images, various models of neural networks are also used. Models of equivalence (EM) of auto-associative memory (AAM) and hetero-associative memory (HAM) were proposed [2-6]. These EM studies have shown, that these models allow the recognition of vectors with 1024 ÷ 4096 components and a significant percentage (up to 25-30%) of damage, at a network power that is 3 to 4 times higher than the number of neurons [3, 5, 6]. For of analysis and recognition the problem of clustering of objects should be solved. This previous clustering allows organizing proper automated grouping data, to cluster analysis, to evaluate on the basis of many signs each cluster, put a class label and improved subsequent learning procedures and classification. At the same time, knowing the significant advantages of EM when creating on their basis improved neural networks (NNs), multiport AAM and HAM, there was a suggestion about the possibility of modifying EM and MHAM for parallel cluster image analysis [6, 7, 8]. At the same time, an urgent task is to study a more general, spatially invariant (SI) equivalence models (SI EMs) that is more invariant to spatial displacements and the possibilities of its application for image clustering [7-9]. And the latter are basic operations in the most promising paradigms of convolutional neural networks (CNN) with deep learning [8, 9]. In our previous paper [8] questions of new possible ways of self-learning in such advanced models, explaining some important fundamental concepts of diverse associative recognition and understand the principles of the functioning of biological NN structures, perform modeling of processing processes, training and extraction of regularities in such models, and propose

their implementation were considered. These questions were considered for bitmaps of multi-level images. In paper [9] we showed that the self-learning concept works with directly multi-level images without processing the bitmaps. In SI EM, we compute the spatially dependent normalized equivalence functions (SD_NEF) whose elements will correspond to the value of the normalized equivalence of the fragment of the input image X and one of the selected fragments from the training matrix. For implementation SLECNS [9], we need certain new or modified known devices capable of calculating normalized spatial equivalence functions (NSEqFs) with the necessary speed and performance. Such specialized devices by authors of papers were previously called "image equivalentor". There are known connections of equivalent functions with correlation functions that make it possible to calculate NSEqFs. Thus, the image equivalentor is itself a doubled correlator or a doubled convolver. In paper [8, 9] we showed models for the recognition and clustering of images that combine the process of recognition with the learning process. For all known convolutional neural networks, as for our equivalence models, it is necessary to calculate the convolution of the current fragment of the image in each layer with a large number of templates which are used, selected or formed during the learning process. But, as studies show, large images require a large number of filters to process images, and the size of the filters can also be large. Therefore, the problem of increasing the computing performance of hardware implementations of such CNNs is acute. It should be noted that the accuracy of calculations, especially for large filter sizes and a large dynamic range (8 bits) of halftone images, is required to make the correct decisions when determining neuron-winners. The last decade was marked by the activation of works aimed at the creation of specialized neural accelerators, which compute the function of comparing two 2D arrays and using the operations of multiplication and addition-accumulation. But as our experiments show, our models also allow the construction of SLECNS.

Formulation of the problem and goal of the work. Therefore, in this paper, using our approaches to designing one-dimensional neuron-equivalents, we consider the structure of the neuron-equivalent, generalized for processing 2D arrays.

Presentation of the main material, research results. The Fig. 1 shows the block diagram of the main unit of SLECNS. The matrix **X** forms a certain number of convolutions in the form of matrices **e** using a set of defined filters-templates **W** which, in our case, are multilevel values, in contrast to the binary ones we used earlier. Thus, we compare each filter with a current fragment in the matrix **X**. As a measure of the similarity of the fragment of the matrix **X** and the filter the equivalent measures of proximity or other measures such as a histogram can be used. Thus, we compare for each filter similar fragments in the matrix. Figure 2 shows the new structure of our proposed system, allowing parallel processing, with a high rate, equal to the speed of selection from the processed image of its shifted current fragment, to compute a set of stream

components (elements) immediately one-cycle all the equivalents convolutions of the current fragment with the corresponding filters. It consists of a micro-display dynamically displaying current fragments, an optical node in the form of a micro-lens array (MLA) with optical lenses (not shown!) and a 2D array of neuron-equivalentors **(NEqs**) with optical inputs. Each **NEq** is implemented in a modular hierarchical manner and can consist of similar smaller sub-pixel, also 2D type, base nodes. The **NEq** has a matrix (ruler) of photo-detectors, on which a halftone image of the fragment is projected through the microlens array (MLA), and the number of electrical analog inputs equal to the number (number) of photo-detectors, to which by means of any known method: from the sample and hold device (SHD), from the analog memory, with subsequent conversion using a set of DACs, etc. the filter components are fed. These components are represented in the form of microcurrents. Each **NEq** has its own filter mask from a set of filters selected or formed by training. Thus, at the inputs of each **NEq** we have two arrays (vectors) of analog currents representing the compared current fragment and the corresponding filter-standard, and the output of the **NEq** is an analog current signal, nonlinearly transformed in accordance with the activation function and representing some measure of their similarity, proximity). In our case, this measure is a normalized equivalence (eq) and nonequivalence (neq), we can calculate them by averaging the component maxima and minima currents. Therefore, the base node, see Fig. 3, contains N two input counters of maximum and minimum currents and one normalizer on current mirrors, which forms two output signals corresponding to normalized eq and neq from two N-component vectors.

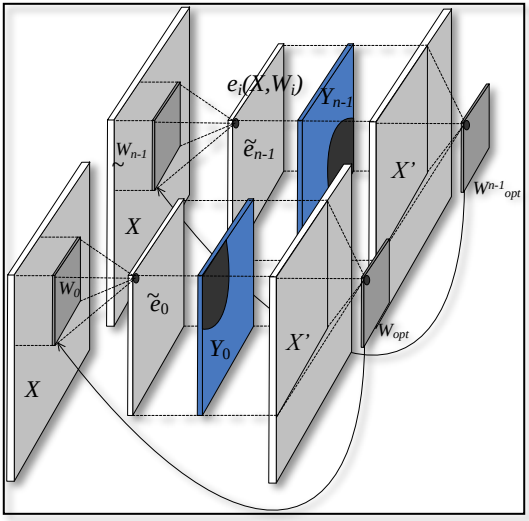


Figure 1. The structure of the basic unit of the SLECNS, which explains the principle of its functioning; Figure explains the principles of learning neural network model based on the multi-port memory to find centroid cluster elements

The basic unit for calculating the normalized Eq (NEq) by averaging the component peak and minima of currents on the basis of current mirrors and the schemes of the limited difference is shown in Fig. 3. Sources of analog currents are shown as current generators for modeling in OrCAD. The dimension of the vector inputs is 9, which corresponds to the filter size 3x3. The results of modeling this basic unit with a nonlinear transformation are shown in Fig. 4. At the instants of 11 - 12μs and 13 -14 μs, the output signals of equivalence and nonequivalence testify to the coincidence of the input vectors. The results of modeling the base unit for the filter size 3x3 (with 9 inputs) showed, that processing time is from 1μs to 0.1μs for currents Imax=5μA, consumption power is from 200μW to 50μW.

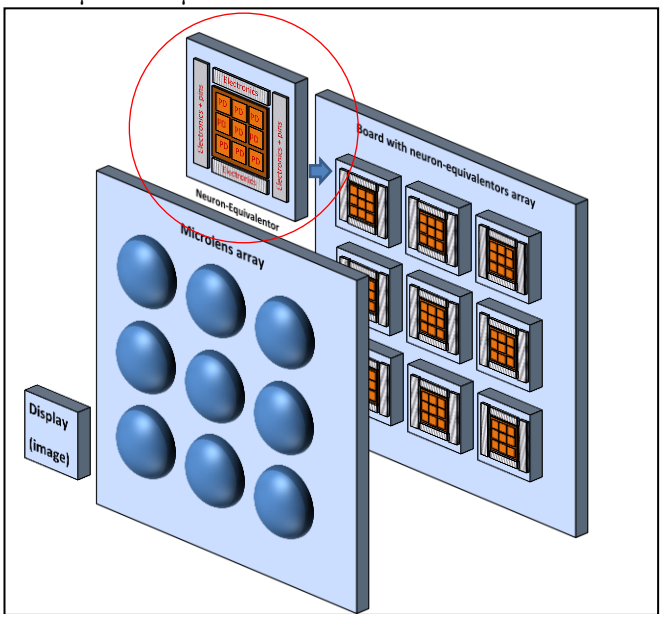


Figure 2. The system structure that uses an array of neuron-equivalentors

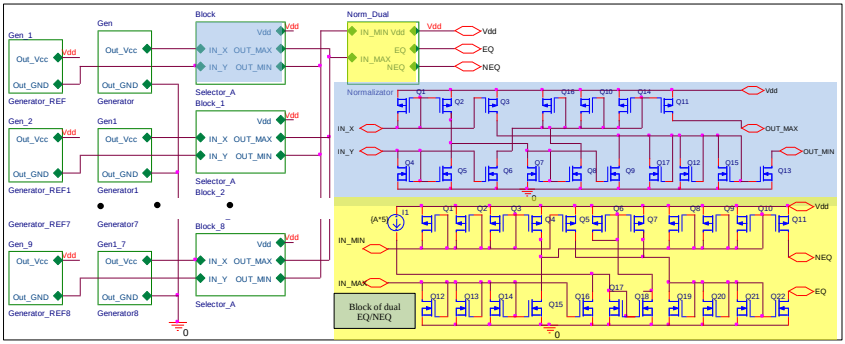


Figure 3. The basic unit for calculating the normalized Eq (NEq) by averaging the component peak and minima of currents on the basis of current mirrors and the schemes of the limited difference

In addition to simulate the base node on 9 inputs, we additionally synthesized a neuron-equivalent circuit having 8 such nodes, each of which compares 8 input vectors, resulting in a neural element circuit having 2 vector inputs of 64 dimensions. For a non-linear transformation, we used a node of a circuit, which realizes a piecewise linear approximation of the power-law activation function (auto-equivalence). The simulation results of 64 input NE with nonlinear output conversion showed that such a NE comparing the two 64 component vectors from the current signals provides good time characteristics and has a total power consumption of approximately 2mW, a low supply voltage, contains less than 1000 CMOS transistors with which summation circuits are implemented, limited subtraction and multiplication of analog currents on current mirrors. The simple build-up of nodes and the additional introduction of the coordinators of the levels of normalizers allow us to increase the number of entrances and increase the dimension of the filters. On the basis of combining nine 9-input NEs, NEs were designed and modeled for two 81-component inputs, i.e. for convolution by a 9 × 9 filter. It has 2 bus analog inputs.

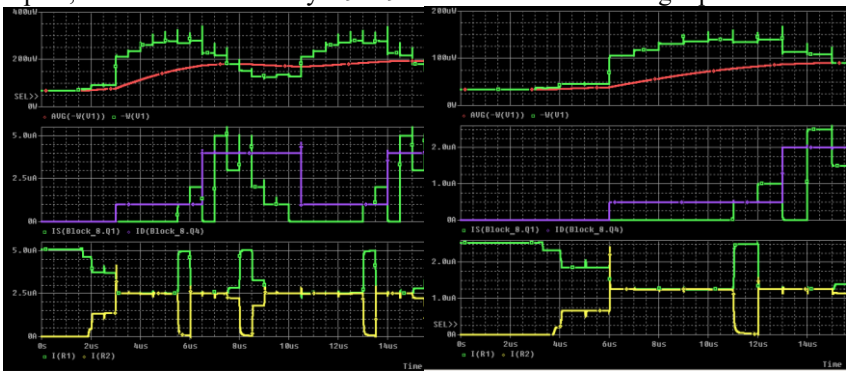


Figure 4. The results of modeling the base unit for the filter size 3x3 (with 9 inputs): on the left for current Imax=5μA, T=0.5μs, V=1.8V, P=200μW. On the right for current Imax=2.5μA, T=1μs, P=100μW. Red line shows power consumption, input (green) and reference (lilac) signals are showed on the midle graphs, on the bottom graph normalized eq (green) and neq (yellow) are showed.

To verify the functioning of the developed NEs within the network, we created a mini-network of eight 9-input NEs, the simulation results of which will be discussed in the report.

Conclusions. NEs have a processing-conversion time of 0.1-1μs, low supply voltages of 1.8-3.3V, minor relative computational errors (1-5%), small consumptions of no more than 1-2mW, can operate in low-power modes less than 100μW) and high-speed (10-20MHz) modes. The efficiency of NEs relative to the energy intensity is estimated at a value of not less than 10 ^ 12

an. op. / sec on W and can be increased by an order of magnitude. The obtained results confirm the correctness of the chosen concept and the possibility of creating NE and MIMO structures on their basis. They can become the basis for the implementation of CNN and self-learning biologically inspired devices with the number of such NEs equal to 1000, to realize the parallel calculation of equivalent convolutions with filter sizes up to 32 * 32.

REFERENCES

1. Krasilenko, V. G., Saletsky, F. M., Yatskovsky, V. I., Konate, K., "Continuous logic equivalence models of Hamming neural network architectures with adaptive-correlated weighting," Proceedings of SPIE Vol. 3402, pp. 398-408 (1998).

2. Krasilenko, V. G., Magas, A. T., "Multiport optical associative memory based on matrix-matrix equivalentors," Proc. of SPIE Vol. 3055, pp. 137 – 146.

3. Красиленко В. Г. Експериментальні дослідження просторово-інваріантних еквівалентністних моделей асоціативної та гетероасоціативної пам'яті 2D образів / В. Г. Красиленко, Д. В. Нікітович // Системи обробки інформації. - 2014. - Вип. 4. - С. 113-120. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2014_4_25.

4. Krasilenko, V. G, "Research and design of equivalence model of heteroasociative memory," The Scientific session of MIFI-2010 Vol.2, pp.83-90.

5. Krasilenko, V. G., Lazarev, A., Grabovlyak, S., "Design and simulation of a multiport neural network heteroassociative memory for optical pattern recognitions," Proc. of SPIE Vol. 8398, 83980N-1 (2012).

6. Krasilenko V. G. , Alexander A. Lazarev, Sveta K. Grabovlyak, Diana V. Nikitovich, "Using a multi-port architecture of neural-net associative memory based on the equivalency paradigm for parallel cluster image analysis and self-learning," Proceedings of SPIE Vol. 8662, 86620S (2013).

7. Krasilenko V.G., Nikitovich D.V., "Simulation of self-learning clustering methods for selecting and grouping similar patches, using two-dimensional nonlinear space-invariant models and functions of normalized "equivalence," Electronics and information technologies: collected scientific papers, Lviv: Ivan Franko National University of Lviv, Issue 6, pp. 98-110 (2015). http://elit.lnu.edu.ua/pdf/6_11.pdf.

8. Krasilenko V.G., Lazarev A.A., Nikitovich D.V., "Modeling and possible implementation of self-learning equivalence-convolutional neural structures for auto-encoding-decoding and clusterization of images", Proc. SPIE Vol. 10453, 104532N (2017) ; https://doi.org/10.1117/12.2276313

9. Krasilenko V.G., Lazarev A.A., Nikitovich D.V., "Modeling of biologically motivated self-learning equivalent-convolutional recurrent-multilayer neural structures (BLM_SL_EC_RMNS) for image fragments clustering and recognition", Proc. SPIE 10609, MIPPR 2017: Pattern Recognition and Computer Vision, 106091D (8 March 2018); doi: 10.1117/12.2285797; https://doi.org/10.1117/12.2285797

UDC 004.93

Usage of keypoint descriptors based algorithms for real-time objects localization

Marchenko I., post-graduate student,
Petrov S., assoc. prof, PhD in tech. sciences,
Pidkuiko A., post-graduate student
Sumy State University, Sumy, Ukraine

In order to achieve high level of security in our everyday life we produce huge amount of data. Significant part of information is presented by videos, sounds or images. A computer is used to extract useful information from raw data [1]. Pattern recognition is branch of computer vision, which allows us to get information from images [2] and videos. Information extraction is crucial problem of pattern recognition. This problem is divided into next branches: object presence; object localization; object classification.

There are a lot of algorithms for object localization. The youngest and the most perspective group of algorithms – algorithms based on keypoints detection and descriptors building [3]. Keypoint is circular region with orientation. Keypoints describe contrast differences, edges, corners in image. Descriptor - histogram of keypoint gradients. Each keypoint characterizes by its descriptor. As an example, you can see Fig 1 where bunch of keypoints describe the places where corners and brightness changes dramatically.

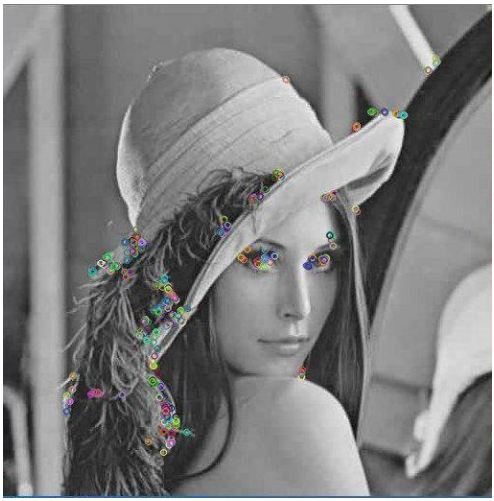


Fig. 1 – Keypoints locations in image

Object localization algorithm describes by next steps: build object keypoints and descriptors; build scene keypoints and descriptors; matching between object and scene descriptors.

Descriptors can be matched using kNN classifier [4], which finds two nearest neighbors for every object descriptor. If both neighbors are similar, algorithm will discard both of them. These descriptors can be discarded due to the fact that they cannot belong to the object. Resultant descriptors set builds from remaining descriptor pairs by selection only the first occurrence in each pair. On the next stage, the algorithm builds vector of distances between object and scene descriptors [5]. After that this set will be divided into two classes with Otsu's method [6]. Class which has less distances describes the object.

Proposed algorithms were tested on real-time video. We used implementation of SIFT, SURF, ORB, BRIEF, FAST, AKAZE, BRISK algorithms from OpenCV library.

We have tested three of proposed algorithms no dataset, which consist of 4 different companies logo. For each logo the following number of keypoints was found:

	Nike	Adidas	Coca-Cola	Twitter
ORB	84	562	713	184
FAST	17	207	1835	259
BRISK	31	301	454	120

As the result we found that all algorithms had built similar descriptors. Only FAST, ORB and BRISK algorithms have perfect performance, so they can work in real-time mode. We divided set of descriptors into two classes, but they intersected. So we cannot locate descriptors, which belong to the object. That's why there is no possibility to divide set of descriptors into two independent classes with high reliability. From this point of view, "out of the box" implementations of these algorithms cannot be used to solve applied problems.

References

1. Cabena P. et al. Discovering data mining : from concept to implementation. Prentice Hall, 1998. 195 p.

2. Chan T.F., Shen J. (Jackie). Image Processing and Analysis. Society for Industrial and Applied Mathematics, 2005.

3. Lew M.S., Jain R. Content-Based Multimedia Information Retrieval: State of the Art and Challenges.

4. Altman N.S. An Introduction to Kernel and Nearest-Neighbor Nonparametric Regression // Am. Stat. 1992. Vol. 46, № 3. P. 175–185.

5. Lowe D.G. Object Recognition from Local Scale-Invariant Features // Corfu. 1999.

6. Otsu N. A Threshold Selection Method from Gray-Level Histograms // IEEE Trans. Syst. Man. Cybern. 1979. Vol. 9, № 1. P. 62–66.

УДК 004.891

Экспертная система диагностики сердечно-сосудистых заболеваний

Барсук А.С., магистрант
Научный руководитель – Скудняков Ю.А., к.т.н., доцент
Белорусский государственный университет информатики и радиоэлектроники, г. Минск

Введение. Сердечно-сосудистые заболевания являются частой причиной смертности или инвалидности [1, 2].

Важной задачей для медиков является своевременное выявление болезни в процессе диагностики и назначение правильного курса лечения. Диагностика заболевания представляет собой сложный процесс анализа многочисленных симптомов и принятия решений. Благодаря достижениям в области искусственного интеллекта появилась возможность разрабатывать интеллектуальные информационные системы, способные не только хранить и предоставлять информацию по запросу, но и предоставляющие пользователям инструменты анализа данных и поддерживающие принятие решений. Разновидностью подобных систем являются экспертные системы [3]. Основные функции экспертных систем – осуществлять рассуждения на основании имеющихся фактов, заданных правил логического вывода и непрерывно накапливать новые знания о предметной области. Экспертная система способна не только делать тот или иной вывод, но и обосновывать его путём описания хода рассуждений, что представляет ценность при диагностике заболеваний.

В данной работе предлагается способ автоматизации диагностики сердечно-сосудистых заболеваний при помощи экспертной системы.

Структура экспертной системы. Структура экспертной системы включает: машину логического вывода, хранящей рабочий список правил; базу знаний; рабочую память; средства объяснений и приобретения знаний; пользовательский интерфейс. Данная структура характерна для продукционных экспертных систем, то есть основанных на правилах.

Правила в продукционной модели знаний описывают ход рассуждения эксперта и задаются в следующем виде:

$$(i) \quad Q; P; A>B; N, \tag{1}$$

где i – это имя продукционной модели знаний или ее порядковый номер;

Q – сфера применения правила;

A > B – ядро продукции, представляющая условную конструкцию”ЕСЛИ-ТО”;

P – условие применимости ядра продукции;

N – постусловие продукции.

Разработка правил базы знаний становится важнейшей задачей при разработке экспертной системы.

Для решения этой задачи зачастую привлекаются эксперты в выбранной предметной области. Машина логического вывода взаимодействует с базой знаний, извлекая оттуда правила и помещая их в свой рабочий список.

Рабочая память содержит факты, которые пользователь помещает туда в процессе взаимодействия с экспертной системой.

При появлении того или иного факта, машина логического вывода применяет те или иные правила в порядке их приоритета, в зависимости от того, соответствуют ли факты из рабочей памяти условию применимости ядра продукции и сфере применения правила.

Пользователь может наблюдать за ходом рассуждений через средство объяснения и создавать новые правила через средство приобретения знаний.

Взаимодействие пользователя с экспертной системой может осуществляться через текстовый и графический интерфейс. Система задаёт вопросы, а пользователь будет на них отвечать. Так его ответы помещаются в рабочую память, создавая факты.

В экспертной системе диагностики сердечно-сосудистых заболеваний в качестве фактов будут показатели основных клинических характеристик: длительность болей в районе грудной клетки, эффект от приёма нитроглицерина, наличие сердечной недостаточности, падение артериального давления, повышение температуры тела, нарушение ритма, лейкоцитоз, шум трения перикарда.

В работе приведен ряд примеров правил анализа клинических характеристик (таблица 1).

В результате проведенного анализа определяется постусловие продукции N, в частности формулируются определения: «Подозрение на очаговые дистрофии миокарда» (в случае, если артериальное давление не понижено), «Подозрение на микроинфаркт или инфаркт миокарда» (в случае, если артериальное давление понижено).

В качестве машины логического вывода использована одна из известных систем разработки продукционных экспертных систем, таких как CLIPS. Основными компонентами CLIPS являются: список фактов, база знаний и машина логического вывода. Для описания фактов используются шаблоны, представляющие собой объекты с полями для хранения значений. В этом случае приведённые выше правила переписываются в соответствии с правилами языка CLIPS.

Таблица 1 – Примеры правил анализа клинических характеристик

(i)	Q	P	A > B	N
1	Диагно-стика	-	ЕСЛИ есть боль, длит_болей <= 10 ТО приём валидола или нитроглицерина	-
2	Диагно-стика	Принят валидол или нитроглицерин	ЕСЛИ приём дал эффект ТО подозрение на стенокардию	-
3	Диагно-стика	Принят валидол или нитроглицерин	ЕСЛИ приём не дал эффекта ТО измеритьртериальное адавление	-
4	Диагно-стика	-	ЕСЛИ длит_болей >10,длит_ болей <= 40 ТО измерить артериальное давление	-
5	Диагно-стика	Измерено артериальное давление	ЕСЛИ давление не понижено ТО проверить сердечный ритм	Подозре-ние на очаговые дистро-фии мио-карда
6	Диагно-стика	Измерено артериальное давление	ЕСЛИ давление понижено ТО измерить температуру	Подозре-ние на микроин-фаркт или инфаркт миокарда
7	Диагно-стика	Измерена температура	ЕСЛИ температура повышена ТО проверить наличие шума трения миокарда	-

Заключение. В данной работе предложена структура и рассмотрены основные параметры экспертной системы для автоматизации диагностики сердечно-сосудистых заболеваний, описаны основные компоненты экспертной системы, структура правил (продукции) и приведены их примеры.

Список литературы

1. Всемирная организация здравоохранения [Электронный ресурс]: Сердечно-сосудистые заболевания. – Режим доступа: http://www.who.int/mediacentre/factsheets/fs317/ru/. – Дата доступа: 22.03.2018.

2. Гардиенко А. Н. Справочник врача-кардиолога / А. Н. Гардиенко Мн.: Современный литератор, 2002. – 128с.

3. Джарратано Д., Райли Г., Экспертные системы. Принципы разработки и программирование [4-е издание]. – Вильямс, 2007. – 1152с.

УДК 629.735.33-519(045)

Керування безпілотним літальним апаратом на основі біометричних характеристик оператора

Білан С.М., доцент, кандидат технічних наук,
Дротов В.В., магістрант
Інститут спеціального зв'язку та захисту інформації, Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Сьогодні безпілотні літальні апарати (БПЛА) є невід'ємною частиною суспільства. Вони використовуються у різних галузях. Особливо вони ефективні у військовій галузі для реалізації багатьох розвідувальних операцій. Їх використання є високоефективним засобом для здобуття важливої інформації про об'єкт спостереження. Проте для того щоб ефективно використовувати БПЛА в спеціальних операціях потрібно щоб оператор БПЛА міг забезпечити повністю контрольований політ з можливістю маневрів у реальному часі. Особливо це стосується місцевості зі складним географічним рельєфом (міська та складна гірська місцевість). Задля цього операторів БПЛА навчають на спеціалізованих курсах по декілька місяців і за умови повноцінного навчання вони через декілька місяців можуть керувати (не професійно) безпілотним літальним апаратом.

Проблема полягає в тому, що пульт для керування не є повністю пристосований до людини, не є логічним продовженням руки та рухів оператора. Тож на виході присутня не зручна система керування польотом, а також витрачається велика кількість часу на його освоєння та великі затрати для того щоб забезпечити якісне навчання оператора.

На даний час існує декілька рішень даної проблеми починаючи від перенесення оператора за монітор комп'ютера до створення систем керування, що намагаються відтворити звичні для людини рухи в польоті БПЛА. Останній варіант є найбільш перспективним проте не доопрацьований. Не доопрацьований в тому плані що існують такі ж самі звичайні пульти як і були раніше. При цьому їх потрібно тримати однією рукою і вони керуються значеннями, що отримані наприклад з акселерометра що знаходиться в пристрої керування.

Рішення вище описаних проблем полягає у створенні спочатку зручного пульту керування, який був би ергономічним, закріплювався на передпліччі оператора та міг звільнити саму руку для ситуації коли, наприклад, потрібно взяти інший предмет або виконати якусь дію, наприклад, по запису необхідної інформації. Далі створення стабільної системи для передачі значень що зчитуються з пульта керування. На передпліччі використовуються показники з акселерометра та гіроскопа,

які накладаються, порівнюються та фільтруються за допомогою алгоритму Калмана. Останнім є створення невеликого нейрон-інтерфейсу, що відповідатиме за зняття показників Альфа-, Бета- та Тета- ритмів для того, щоб виконувати базові операції пульта, такі як увімкнення та вимкнення БПЛА, робота з індикацією в небі, а також можливість зміни каналу для радіосигналів. Дана система стає можливою, якщо використати біометричні сигнали, які є сигналами електроенцефалограми.

Роботу системи керування можливо описати чотирма частинами.

1. Частина (Механіка). Пульт управління виконаний з алюмінію та обладнаний зручною системою фіксації на руці оператора для того, щоб під час переходів або простої ходьби пульт не злітав з руки та залишався в постійній готовності. Всі частини де є електронні компоненти включно з дисплеєм покрито захисними шарами алюмінію для попередження ушкоджень електронних компонентів. Окрім вище описаного пульт обладнано освітленням для кращої орієнтації в нічний час.

2. Частина (Електроніка). Все апаратне забезпечення системи керування складається з чотирьох частин. Перша отримує фільтрує та надає значення положення руки в просторі, друга відслідковує показники погодних умов та надає рекомендації з приводу польоту. Третя приймає та обробляє значення ритмів головного мозку, а четверта надсилає всі значення на БПЛА та виводить на невеликий дисплей на пульті всі отримані значення.

3. Частина (Зчитування даних ритмів головного мозку). Для того щоб реалізувати дану частину були розроблені додаткові складові, такі як електроди, що накладаються на шкіру та зчитують ритми у визначених діапазонах, а також підсилювач частот до можливих для зчитування апаратурою. Таким чином оператор може зосередившись увімкнути БПЛА, розсіяти увагу та спричинити підвищення частоти іншого ритму і відповідно виконати іншу операцію управління.

4. Частина (Передача даних). Вся передача інформації в даній системі базується на використанні PPM сигналу оскільки він є значно зручнішим для використання та надає змогу відмовитись від великої кількості проводів що покращує налаштування БПЛА.

Загалом система представляє собою монолітну та повністю ергономічну систему, що не заважає рухам людини, дає можливість повноцінно виконувати поставлені задачі, зменшує період навчання операторів з декількох місяців до декількох годин, а також відмова від різноманітних тумблерів та перемикачів за допомогою використання нейрон-інтерфейсів. Також однією з важливих доповнень є система віртуальної реальності та спеціальна FPV камера що встановлена на борту БПЛА. Тобто в разі, якщо оператор знаходиться в приміщенні або місці, де йому не загрожує небезпека, він може скористатися окулярами доповненої реальності та виконувати політ від першого обличчя.

УДК 004.855.5

Класифікатор біомедичних зображень на основі нейронної мережі

Знакомський І.В., студент
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", м. Київ

Використання нейронних мереж у світі розвивається дуже швидко. І обробка зображень з використанням нейронних мереж є важливим напрямком застосування сучасної обчислювальної техніки. Відомі такі завдання обробки зображень, як фільтрація і відновлення зображень, сегментація зображень, як засобу стиснення інформації. Проблеми розпізнавання зображень, крім класичної задачі розпізнавання фігур заданої форми на зображенні ставлять нові завдання розпізнавання ліній і кутів на зображенні, розпізнавання краю зображення. Проте застосуванню нейронних мереж для класифікації біомедичних зображень приділено недостатньо уваги.

Запропоновано метод класифікації біомедичних зображень на основі нейронної мережі з використанням радиально-базисних функцій.

Задача класифікації біомедичних зображень. Об'єкти інтересу дослідження на біомедичних зображеннях, використовуваних в діагностиці, зазвичай бувають невеликими і поганої контрастності порівняно з фоном. При візуальному виявленню цих об'єктів – виконання першого кроку під час діагностики по зображенню можуть виникнути проблеми.

Метод класифікації біомедичних зображень на основі РБФ

Оскільки необхідно налаштовувати параметри активаційної функції кожного нейрона, нейронна мережа реалізовується з використанням ітераційних чисельних методів оптимізації, градієнтних методів. Було обрано один з методів навчання РБФ мережі, в якому використовується поєднання генетичних алгоритмів для підбору активаційних функцій і методів лінійної алгебри для розрахунку вагових коефіцієнтів вихідного шару за формулою: $\overline{W} = A^{-1}H^T\bar{y}$ (1), де $\overline{W}$ – вектор ваги, а A^{-1} – інверсія добутку матриці H на транспоновану матрицю H, H – інтерполяційна матриця базисних функцій $h(\bar{x})$.

На кожній ітерації пошуку генетичний алгоритм самостійно обирає, в яких точках простору вхідних сигналів мережі розмістити центри активаційних функцій нейронів прихованого шару і назначає для кожної з них ширину вікна. Для отриманої таким чином сукупності параметрів прихованого шару по формулі (1), обчислюються вага вихідного шару і отримана при цьому помилка апроксимації, яка служить для генетичного алгоритму індикатором того, на скільки поганий або хороший даний варіант. На наступній ітерації генетичний алгоритм відкине погані

варіанти і буде працювати з наборами, які показали найкращі результати на попередній ітерації. Алгоритм наведено на рисунку 1.

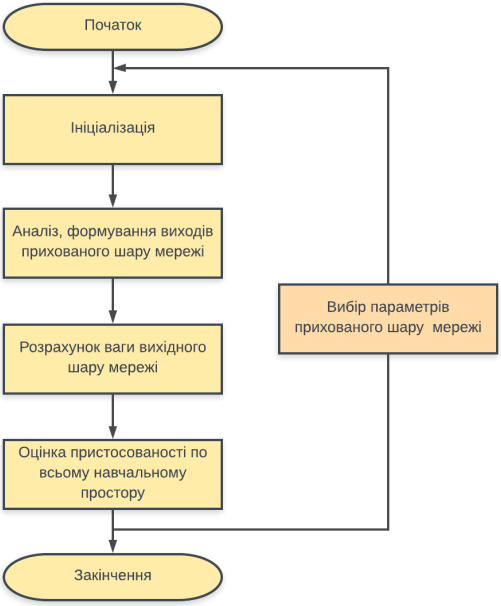


Рис. 1. Алгоритм навчання РБФ мережі, за допомогою генетичного алгоритму

Далі групуються шаблони навчальної множини за ступенем їх близькості у просторі вхідних значень в меншу кількість кластерів. Кількість таких кластерів задає кількість нейронів у прихованому шарі мережі, а їх середні характеристики використовують для початкової ініціалізації параметрів активаційних функцій.

Висновки. Показано задачу, яка виникає при організації класифікації біомедичних зображень з використанням нейронних мереж. Запропоновано спосіб класифікації таких зображень за допомогою РБФ мереж.

Список літератури

1. Балухто А.Н., Булаев В.И. и др. «Нейрокомпьютеры в системах обработки изображений». Книга 7. – М.: «Радиотехника», 2008. – 192 с.

2. The neural network posted on september 14, 2016 by Fjodor Van Veen [Електронний ресурс] – Режим доступу: http://www.asimovinstitute.org/neural-network-zoo/

3. Дороничева А.В., Савин С.З. Методы распознавания медицинских изображений для задач компьютерной автоматизированной диагностики // Современные проблемы науки и образования. – 2014. – № 4. [Електронний ресурс]. – Режим доступу: https://www.science-education.ru/ru/article/view?id=14414

УДК 629.7.07

Модель самообучающейся системы поддержки принятия решений

Землянский А.В., старший преподаватель,
Сало Н.А., старший преподаватель
Летная академия Национального авиационного университета, г. Кропивницкий

Модель системы поддержки принятия решения (СППР), которую мы разрабатываем, включает в себя следующие компоненты: выявления и классификации нарушений, выбора решения и хранения принятых решений.

Наша модель СППР должна работать в трех режимах:

- режиме классической СППР (выдача рекомендаций по решению ПКС),
- режиме самообучения (накопления данных),
- гибридном режиме, включающем в себя оба предыдущих режима.

Для обучения системы поддержки принятия решений (СППР) нам необходимо организовать процесс накопления данных о выбранных методах решения потенциально-конфликтных ситуаций (ПКС). Организовать такой процесс мы можем по трем направлениям:

- автоматическое выполнение тренажерных упражнений с применением системы поддержки принятия решений в режиме самообучения. В таком режиме система самостоятельно проходит упражнение (или целый набор упражнений) без участия операторов и накапливает данные для последующего анализа;
- накопление необходимых данных в режиме поддержки принятия решений при выполнении тренажерных упражнений авиадиспетчерами или курсантами. Система работает в режиме поддержки принятия решений и одновременно фиксирует результаты парирования ПКС. Причем следует учитывать, что обучаемый может использовать предложенные СППР рекомендации, а может игнорировать их и принимать решения самостоятельно;
- анализ результатов и процесса решения, ранее выполненных тренажерных упражнений авиадиспетчерами или курсантами с применением СППР и без применения СППР. Анализ ранее выполненных упражнений может быть полезным при определении влияния факторов, которые ранее не учитывались или были не определены.

Очевидно, что самообучающаяся (не статичная) система поддержки принятия решений должна иметь минимум два режима работы:

- режим самообучения – это режим, в котором система накапливает и анализирует информацию о парировании ПКС в различных ситуациях.

Накопление данных производится при помощи компонента хранения принятых решений и позволяет автоматизировать сбор информации в объеме, достаточном для ее дальнейшего анализа. Анализ информации может производиться как в автоматическом режиме, когда система по заранее заданным алгоритмам производит выбор наиболее предпочтительного решения (например, верным может считаться решение, которое в заданных условиях дает максимальный процент парирования ПКС), так и в режимах с привлечением экспертов, когда по полученным данным эксперт определяет дальнейшее поведение СППР.

На рис. 1 показан алгоритм работы СППР в режиме самообучения.

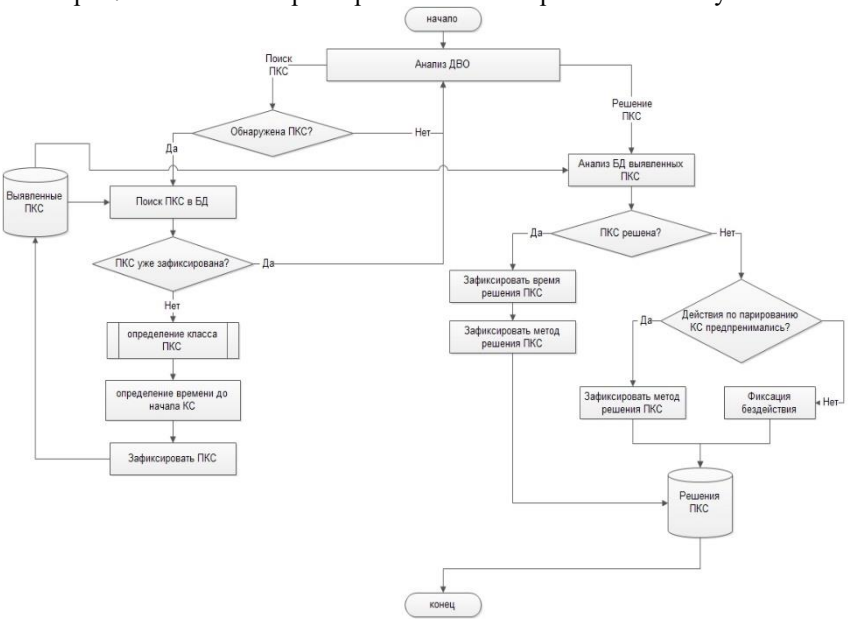


Рис. 1. Схема алгоритма работы СППР в режиме самообучения

- режим поддержки принятия решений – это нормальный режим для работы любой СППР авиадиспетчера, в котором она позволяет выдавать рекомендации по парированию ПКС.

Так же следует учитывать, что СППР может работать в гибридном режиме, когда одновременно производится сбор и анализ информации и выдаются рекомендации по парированию ПКС. На рисунке 2 показан алгоритм работы СППР в гибридном режиме.

Интерес так же представляют собой системы, в которых возможен сбор и анализ информации о работе СППР на большом количестве рабочих мест. Это могут быть системы, построенные как на предприятиях, так и в учебных заведениях. Анализ работы СППР в различных условиях (учебные и контрольные упражнения в учебных заведениях; тренировка действующих авиадиспетчеров в тренажерных

центрах и т.д.) позволит значительно расширить возможности для анализа собранных данных, а так же повысить качество работы самих СППР. Организация работы таких систем возможна с применением следующих моделей построения:

1. Сетевая модель реального времени – позволит оперативно (в режиме реального времени) анализировать информацию по методам решения ПКС и предлагать обновленные рекомендации по решению ПКС. Может применяться при относительно небольшом количестве источников информации, например, в пределах одного тренажерного центра.

2. Модель накопления и анализа информации в одном центре – подразумевает существование центра сбора и анализа информации с большого количества источников. Целесообразно использовать при наличии большого количества источников информации (нескольких тренажерных центров) или для организации единой системы сбора и анализа данных.

3. Модель накопления и анализа информации в нескольких центрах – используется при наличии крайне большого количества источников информации, когда возможности обработки одним центром могут быть не достаточны. Так же такая модель может применяться при невозможности организации постоянной связи требуемого уровня между несколькими объединениями источников информации.

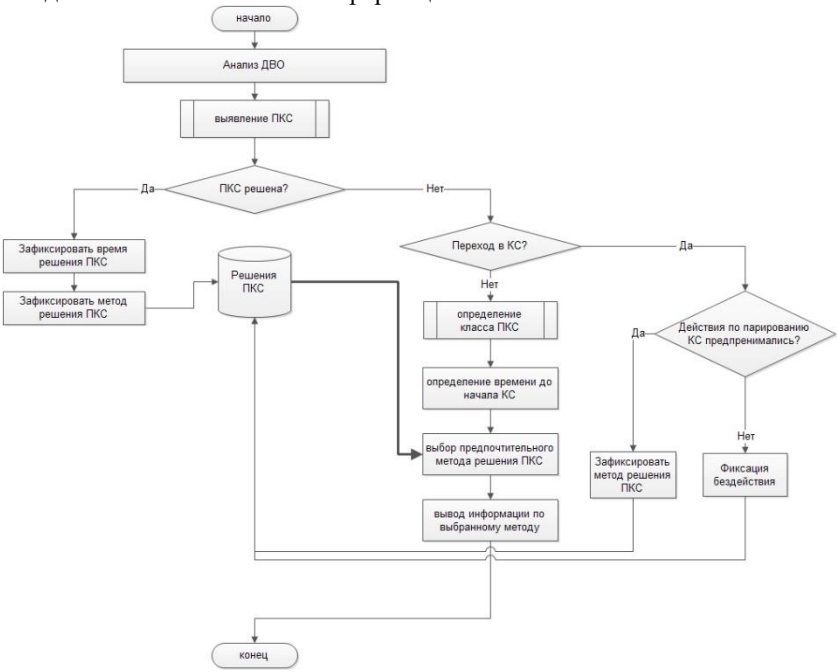


Рис. 2. Схема алгоритма работы СППР в гибридном режиме

УДК 004.827

Особливості інфологічного моделювання недосконалих даних в інформаційній системі контролю витрат ресурсів

Золотухіна О.А., аспірант
Науковий керівник – Шушура О.М., к.т.н., доцент
Державний університет телекомунікацій, м. Київ

Інформаційна складова системи контролю витрат ресурсів включає різноманітні, в тому числі і нечіткі, дані про характеристики ресурсів, режими експлуатації, порядок технічного обслуговування та ремонту обладнання тощо.

Запропоновано при побудові інфологічної моделі системи контролю витрат ресурсів використовувати для нечітких значень на рівні атрибутів сутностей та відношень розширення звичайної моделі сутність-зв'язок (ER-модель) з можливістю представлення нечітких значень атрибутів.

Рівні нечіткості інформації в системі контролю витрат ресурсів. В процесі моделювання нечітких даних визначають три рівні нечіткості [1]:

1) наявність сутностей, відношень або множин атрибутів, для яких задані ступені належності до моделі (дані про конкретний матеріальний ресурс та/або витратний матеріал можуть враховуватися у загальній моделі розрахунку витрат із деякими ступенями важливості);

2) нечіткість відношень між сутностями (важливість кожного із витратних матеріалів, пов'язаних із певним механізмом/обладнанням та/або режимом роботи може виражатися через нечіткість відношень між відповідними сутностями, крім того, ймовірності вибору ресурсів для режиму можуть представлятися засобами нечіткої моделі даних);

3) присутність нечітких значень в атрибутах сутностей та відношень (характеристика або параметр деякого ресурсу чи режиму його використання може бути задана інтервальним значенням, бути відсутня або не визначена, бути отримана з похибкою або представлена в різних джерелах різними значеннями).

Вибір моделі для представлення недосконалих даних в інформаційній системі контролю витрат ресурсів. Для представлення недосконалих (нечітких) даних застосовуються різні види моделей, серед яких можна виділити:

–розширення звичайної моделі сутність-відношення (ER) за рахунок введення можливості представлення нечітких значень атрибутів [2];

–нечіткі розширені моделі сутність-відношення (FEER), в яких значення істинності може бути пов'язане із кожним типом зв'язку в схемі і використовується для визначає ступеня нечіткості кожного з понять узагальнення, спеціалізації, категорії та агрегації [3];

–графо-орієнтовані схеми, які дозволяють визначити та обробити

нечіткість за допомогою пояснювальної бази із семантичними інтерпретаціями атрибутів та зв'язків [4];

–модель ExIFO, яка розширює концептуальну модель IFO шляхом введення високорівневих примітивів для моделювання нечітких сутностей, а також визначення нечіткої інтерпретації логічних операторів OR, XOR та AND [5].

Для моделювання даних системи контролю витрат ресурсів підприємства можна застосовувати будь-яку з представлених моделей, але з урахуванням того, що найбільша кількість недосконалої інформації представлена у вигляді нечітких атрибутів пропонується використання розширення звичайної моделі сутність-відношення із нечіткими значеннями атрибутів.

Висновки. Показано проблему представлення недосконалої інформації в системі контролю витрат ресурсів підприємства. Проведено аналіз рівнів недосконалості та моделей нечіткої інформації. Запропоновано використати розширення ER-моделі нечіткими типами даних для представлення атрибутів ресурсів та режимів роботи обладнання/механізмів, що дозволяє одночасне представлення чітких та нечітких атрибутів сутностей та відношень та забезпечує можливість побудови на основі даної моделі реляційних або об'єктно-орієнтованих баз даних з подальшою їх реалізацією за допомогою існуючих систем управління базами даних.

Список літератури

1. Galindo J. Relaxing Constraints in Enhanced Entity-Relationship Models Using Fuzzy Quantifiers/ J. Galindo, A. Urrutia, R. Carrasco, M. Piattini// IEEE Transactions on Fuzzy Systems. – 2004. – №.12. – P.780–796.

2. Ruspini E. Imprecision and uncertainty in the entity-relationship model// Fuzzy Logic in Knowledge Engineering, H. Prade and C. V. Negoita, Eds. Berlin, Germany: Verlag TUV Rheinland. – 1986. – P.18–22.

3. Ma Z. M., Zhang W. J., Ma W. Y., Chen G. Q. Conceptual design of fuzzy object-oriented databases using extended entity-relationship model/ // Int. J. Intell. Syst., vol. 16, – 2001. – №6. – P.697–711.

4. Fujishiro et al. The design of a graph-oriented schema for the management of individualized fuzzy data // Jpn. J. Fuzzy Theory Syst., vol.3. – 1991. – № 1. – P.1–14.

5. Yazici A., Buckles B. P., Petry F. E. Handling complex and uncertain information in the exifo and NF data models // IEEE Trans. Fuzzy Syst., vol. 7. – Dec.1999. – P.659–676.

УДК 004.83

Прикладні аспекти використання систем нечіткого логічного висновку в задачах багатокритеріальної оптимізації

Ковалишин О.С., аспірант
Науковий керівник – Ткаченко Р.О., д.т.н., професор
Національний університет «Львівська політехніка», м. Львів

В епоху активного впровадження сучасних інформаційних технологій та інтелектуальних систем актуальності набувають задачі багатокритеріальної оптимізації.

Для такої категорії задач характерною є невизначеність цілей: існування рішень які б максимізували відразу декілька цільових функцій є рідкісним випадком, тому з математичної точки зору завдання багатокритеріальної оптимізації представляє собою пошук деякого компромісного рішення.

Відповідно більшість методів розв'язування таких задач засновано на зведенні початкової задачі з векторним критерієм до оптимізаційної задачі із скалярним критерієм. Між собою методи відрізняються тільки механізмом реалізації такого зведення. Найбільш поширеними з них є: згортання часткових критеріїв, головного часткового критерію, цільового програмування послідовних поступок.

Недоліками цих способів є[1]:

- жорстке співвідношення між значеннями відхилень критеріїв оптимальності, що значно звужує множину допустимих планів;
- слабо формалізована методика об'єктивного визначення коефіцієнтів;
- значенню деякого критерію може відповідати множина значень інших, за яких оптимальний план ефективніший.

Вирішенням вище зазначених проблем може стати використання механізмів нечіткого логічного висновку – математичних систем, що з'явилися як інструмент для вирішення невизначених, неточних або якісних проблем прийняття рішень.

Нечіткий логічний висновок являє собою апроксимацію залежності між входами і виходами системи за допомогою нечіткої бази знань та операцій над нечіткими множинами. Відображенням j множини станів у множину рішень виступає база знань, яка складається з набору правил. Оптимальність прийнятого в такий спосіб рішення залежить від точності функцій належності величин та бази знань.

Використання такого підходу надає наступні переваги [2]:

- можливість обробляти вхідні дані, представлені в нечіткій формі: наприклад, інформацію, що змінюються в часі, значення, що неможливо задати однозначно (результати статистичних опитувань, рекламні компанії та т. ін.);

- можливість нечіткої формалізації критеріїв оцінки і порівняння: оперування критеріями "більшість", "переважно", "часто" і т. ін.;
- можливість проведення якісних оцінок як вхідних даних, так і вихідних результатів: можна оперувати не тільки власне значеннями даних, але їхнім ступенем вірогідності та її розподілом;
- можливість проведення швидкого моделювання складних динамічних систем і їхній порівняльний аналіз із заданим ступенем точності: оперуючи принципами поведінки системи, описаними fuzzy-методами.

Розроблено кілька алгоритмів нечіткого логічного висновку, які переважно відрізняються правилами висновку та здійсненням логічних операцій. На сьогоднішній день найбільш поширеними є моделі нечіткого логічного висновку Сугено і Мамдані. Особливої уваги заслуговує система T-Controller, яка передбачає однозначність процедури виводу та нульову методичну похибку її виконання, що досягається за рахунок використання лінійної нейронної мережі на основі моделі геометричних перетворень [3].

Висновки. Розглянуто проблематику вирішення задач багатокритеріальної оптимізації, зокрема досліджено методи згортання векторного критерію. Запропоновано використання методів заснованих на використанні нечіткої логіки, а саме системи T-Controller для вирішення проблеми скаляризації вектору обмежень.

Список літератури

1. Michael C. Ferris, Michael P. Mesnier, Jorge J. More NEOS and Condor: Solving optimization problems over the Internet: User's guide for Solver. – 1998. – 40 p.
2. Круглов В.В., Дли М.И., Голунов Р.Ю. Нечеткая логика и искусственные нейронные сети: Учеб. пособие. – М.: Издательство физико- математической литературы, 2001. – 224 с.
3. Дорошенко А. В., Ткаченко Р. О. Нейроподібні структури машини геометричних перетворень у завданнях інтелектуального аналізу даних // Міжнародна наукова конференція «Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту» ISDMCI'2009 : зб. наук. пр. у 2 т., 18-22 трав. 2009 р., Євпаторія, Україна. — Х. ; Херсон, 2009. — Т. 2. — С. 309-314.

УДК 004.056.53

Дослідження алгоритмів та методів машинного навчання

Колодяжний І.О., студент другого курсу
Науковий керівник - Мелешко Є.В., к.т.н., доцент
Центральноукраїнський національний технічний університет, м. Кропивницький

Машинне навчання – це технологія аналізу даних, яка дозволяє комп'ютеру вчитися на досвіді, як це робить людина або тварина. Алгоритми машинного навчання використовують обчислювальні методи для "вивчення" інформації безпосередньо з даних, не покладаючись на заздалегідь визначене рівняння як модель. Алгоритми адаптивно підвищують їх продуктивність, оскільки збільшується кількість зразків, доступних для навчання. Завдяки машинному навчанню програміст не зобов'язаний писати інструкції, що враховують всі можливі проблеми і містять всі рішення. Замість цього в комп'ютер (або окрему програму) закладають алгоритм самостійного знаходження рішень шляхом комплексного використання статистичних даних, з яких виводяться закономірності і на основі яких робляться прогнози.

Вибір того, які алгоритми машинного навчання використовувати, залежить від ряду обставин, зокрема, від розміру, якості і природи даних. Також від того, що потрібно зробити з відповіддю і скільки часу є на обробку даних, яку точність відповіді необхідно отримати [1]. Навіть найдосвідченіші фахівці з даних не зможуть з абсолютною впевненістю визначити найкращий алгоритм для певної задачі, не перевіривши на практиці, який з існуючих алгоритмів дасть кращі результати.

Машинне навчання використовує два типи технік: контрольоване навчання – яке тренує модель на відомих вхідних і вихідних даних так, щоб вона змогла передбачати майбутні виходи та безконтрольне навчання, яке знаходить приховані шаблони або внутрішні структури у вхідних даних [1, 2].

Основні методи машинного навчання: навчання з вчителем (задача класифікації, задача регресії, задача ранжування, задача прогнозування), навчання без вчителя (задача кластеризації, задача пошуку асоціативних правил, задача фільтрації викидів, задача побудови довірчої області, задача зменшення розмірності, задача заповнення пропущених значень), часткове навчання, трансдуктивне навчання, навчання з підкріпленням, динамічне навчання, активне навчання, метанавчання (багатозадачне навчання, індуктивний перенос) [3, 4].

Методи контрольованого навчання [1-3]

Дерево прийняття рішень - засіб підтримки прийняття рішень, яке використовує деревовидний граф або модель прийняття рішень, а також можливі наслідки їх роботи, включаючи ймовірність настання події, витрати ресурсів і корисність.

З точки зору бізнес-рішення, дерево класифікації є мінімальною кількістю питань «так/ні», відповівши на які, можна зробити вірний вибір. Якщо розглядати дерево як метод, то воно дозволяє підійти до вирішення проблеми зі структурованого і систематичного боку, щоб в результаті прийти до логічного висновку.

Наївні байєсовські класифікатори представляють собою сімейство простих ймовірнісних класифікаторів, які засновані на застосуванні Теореми Баєса зі строгими (наївними) припущеннями про незалежність функцій. Формула наступна: P(A\B) = P(B\A)P(A)\P(B); тут P(A\B) є ймовірністю гіпотези А при настанні події В (апостериорна ймовірність), P(B\A) - ймовірністю настання події В при істинності гіпотези А, P(A) - апріорної ймовірності гіпотези А і P(B) – повної ймовірності настання події В.

Абстрагуючись від теорії і переходячи до практики, можна виділити наступні сфери застосування теорема Баєса:

- визначення спаму в електронній пошті;
- сегментація новинних статей за їх тематиці;
- визначення емоційного забарвлення блоку тексту;
- програмне забезпечення для розпізнавання осіб.

Метод найменших квадратів. Найменші квадрати виступають в ролі методу для реалізації лінійної регресії. Найчастіше лінійна регресія представляється у вигляді завдання підгонки прямої лінії, що проходить через множину точок. Є декілька варіантів її здійснення, і метод найменших квадратів – один з них. Можна намалювати лінію, а потім виміряти відстань по вертикалі від кожної точки до лінії і «перенести» цю суму вгору. Необхідною лінією буде та конструкція, де сума відстаней буде мінімальною. Іншими словами, крива проводиться через точки, що мають нормально розподілене відхилення від істинного значення.

Якщо лінійна функція може бути застосована для підбору даних, то метод найменших квадратів відноситься до типів метрики помилок, яка мінімізує похибки.

Логістична регресія – потужний статистичний метод прогнозування ймовірності виникнення деякої події з однією або декількома незалежними змінними. Логістична регресія визначає ступінь залежності між категоріальною залежною й однією або декількома незалежними змінними шляхом використання логістичної функції, що є акумулятивним логістичним розподілом.

Даний алгоритм активно використовується в реальному житті, а саме при:

- оцінці кредитоспроможності особи (кредитного скорингу);
- вимірі показників успішності маркетингових кампаній;
- прогнозі доходів з певного продукту;
- обчисленні можливості виникнення землетрусу в конкретний день.

Метод опорних векторів (SVM) – це набір алгоритмів, що використовуються для задач класифікації та регресійного аналізу. Враховуючи, що в N-вимірному просторі кожен об'єкт належить одному з двох класів, SVM генерує (N-1)-мірну гіперплощину з метою поділу цих точок на 2 групи. Крім того, що метод виконує сепарацію об'єктів, SVM підбирає гіперплоскість так, щоб та характеризувалася максимальним віддаленням від найближчого елемента кожної з груп.

Серед найбільш масштабних проблем, які були вирішені за допомогою методу опорних об'єктів (і його модифікованих реалізацій) виділяють відображення рекламних банерів на сайтах, розпізнавання статі на підставі фотографії та сплайсинг людської ДНК.

Методи неконтрольованого навчання [1-3]

Алгоритми кластеризації. Завдання кластеризації полягає в групуванні безлічі об'єктів таким чином, щоб помістити максимально схожі між собою елементи в одну групу (кластер).

Алгоритмів кластеризації існує досить багато, і всі вони відрізняються один від одного. Найпопулярніші з них:

- алгоритми на базі центру ваги трикутника;
- алгоритми на основі підключення;
- алгоритми щільності на основі просторової кластеризації;
- ймовірнісний алгоритм;
- алгоритм зменшення розмірності;
- нейронні мережі і машинне навчання.

Алгоритми кластеризації використовуються в біології, соціології та інформаційних технологіях. Наприклад, в біоінформатиці за допомогою кластеризації аналізуються складні мережі взаємодіючих генів, що складаються часом з сотень або навіть тисяч елементів. А при аналізі результатів соціологічних досліджень рекомендується здійснювати аналіз методом Уорда, при якому всередині кластерів оптимізується мінімальна дисперсія, в результаті створюються групи приблизно рівних розмірів.

Метод головних компонент (PCA) - це статистична процедура, яка використовує ортогональное перетворення з метою конвертації набору спостережень за можливо корельованими змінними в набір значень лінійно некорелірованних змінних, які називаються головними компонентами.

Окремі області застосування PCA включають в себе стиснення і спрощення даних для полегшення навчання, а також візуалізацію. Рішення про використання методу головних компонент залежить від рівня пізнання предметної області. PCA не підходить для застосування у

випадках з погано впорядкованими даними (всі компоненти методу мають досить високу дисперсію).

Сингулярне розкладання. В лінійній алгебрі під сингулярним розкладанням (SVD) розуміють розкладання прямокутної речовинної або комплексної матриці. Для матриці M розмірністю [m * n] існує таке розкладання, що M = UΣV, де U і V - унітарні матриці, а Σ - діагональна матриця.

Метод головних компонент є простим застосуванням сингулярного розкладання. Перші алгоритми комп'ютерного бачення використовували PCA і SVD, щоб представити обличя у вигляді суми базисних компонент, виконати зменшення розмірності, а потім зіставити їх із зображеннями з навчальної вибірки. І хоча сучасні методи характеризуються більш складною реалізацією, багато хто з них як і раніше працюють на базі подібних алгоритмів.

Аналіз незалежних компонент (ICA) являє собою статистичний метод виявлення прихованих чинників, які лежать в основі множини випадкових величин, сигналів і інших вимірів. ICA визначає модель для досліджуваних багатофакторних даних, які зазвичай подаються у вигляді великої бази даних зразків. У моделі змінні подаються як лінійна суміш деяких прихованих змінних, а будь-яка інформація про закони змішування відсутня. Передбачається, що приховані змінні незалежні один від одного і представляються як негауссовські сигнали, тому вони називаються незалежними компонентами досліджуваних даних.

Аналіз незалежних компонент безпосередньо пов'язаний з методом головних компонент, але це набагато більш потужна техніка, здатна знайти приховані чинники джерел, коли класичні методи в особі PCA дають збій. Алгоритм ICA застосовується в телекомунікаціях, астрономії, медицині, розпізнаванні мови і зображень, діагностуванні та тестуванні складних електронних систем і, нарешті, пошуку прихованих чинників і джерел руху фінансових показників.

Список літератури:

1. Выбор алгоритмов машинного обучения Microsoft Azure [[Электронный ресурс] – Режим доступа: https://docs.microsoft.com/ru-ru/azure/machine-learning/studio/algorithm-choice

2. 10 главных алгоритмов машинного обучения [Электронный ресурс] – Режим доступа: http://ru.datasides.com/code/algorithms-machine-learning/

3. Машинное обучение [Электронный ресурс] – Режим доступа: http://www.machinelearning.ru/wiki/index.php?title=Машинное_обучение

4. Machine Learning in MATLAB [Electronic resource] - Access mode: https://www.mathworks.com/help/stats/machine-learning-in-matlab.html?requestedDomain=true

УДК 004.8

Дослідження базових архітектур нейронних мереж

Коломієць Д.О., студент 4 курсу
Науковий керівник – Смірнов О. А., д.т.н., професор
Центральноукраїнський національний технічний університет
м. Кропивницький

Незадовільне керування технологічними процесами у багатьох галузях промисловості України приводить до значних економічних збитків, підвищення собівартості продукції, зниження конкурентоспроможності товарів на світовому ринку. Значно покращитии ситуацію у сфері управління виробництвом можливо розширенням застосування засобів штучного інтелекту. Нині серед таких засобів найбільше поширення знаходять: експертні системи; нейромережеві підходи та нейрокерування; нечітка логіка. Оскільки нейромережеве керування при його великих можливостях знаходить порівняно нешироке практичне використання, приділимо саме йому увагу, розглянувши його основу – базові архітектури нейромереж.

Викладення основного матеріалу. На сьогодні найбільш поширеними є різновиди архітектур нейронних мереж, показані на рис.1.

Рисунок 1 – Найбільш поширені різновиди архітектур нейронних мереж

Одношарові мережі. Шаровою є мережа, яка складається із груп нейронів розподілених за шарами. Якщо шарів більше ніж один, мережа стає багатошаровою. Якщо сигнали спрямовуються постійно в одному напрямку: з початку до кінця мережі, то вона є прямоспрямованою.

Мережа складається з двох шарів – вхідного та вихідного. Нейрони, які знаходяться у вхідному шарі, виконують функцію ретранслювання сигналу на вихідний шар, не змінюючи їх. Формування реакції межі здійснюється завдяки перетворенню сигналів, яке відбувається у вихідному шарі.

Через те, що обчислення у такій мережі відбувається лише на одному шарі, не дивлячись на прийняту класифікацію, такі мережі називають не двошаровими, а одношаровими [1,3].

Багатошарові прямоспрямовані мережі.

Одна з головних характеристик багатошарових прямоспрямованих мереж це наявність прихованих шарів, один або більше, які здійснюють перетворення інформації. Нейрони, які знаходяться у прихованому шарі, заведено називати схованими вузлами або прихованими нейронами. Завдяки використанню схованих шарів вдалося реалізувати нелінійні перетворення типу "вхід-вихід" не залежно від їх складності, а також аналізувати вхідні дані для того щоб витягти статистичні показники високих порядків. Ці властивості, які унікальні для багатошарових мереж, особливо помітні при високій розмірності вхідних сигналів.

Схема тришарової прямоспрямованої нейронної мережі із прихованим шаром зображена на рис. 2. Для того щоб описати цю нейрону мережу потрібно використати запис виду *KK5-3-2*. Розмір вхідного шару позначений - 3, вихідного - 2, а схованого - 5. Прямоспрямована нейрона мережа із *q* вхідними та вихідними нейронами та *u* прихованими шарами із розміром *h*, буде мати вигляд $KKq\text{-}h_1h_2\text{-}...h_u\text{-}q$.

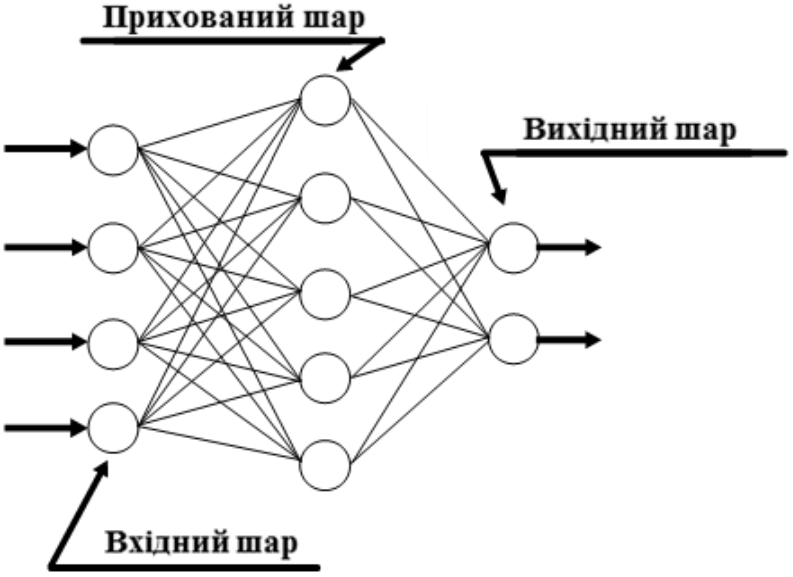


Рисунок 2 – Повнозв'язна трьохшарова прямоспрямована мережа

В мережах такого типу вхідний шар нейронів не здійснює перетворень вхідного сигналу, а лише ретранслює його на перший схований шар. У свою чергу приховані шари здійснюють нелінійне перетворення сигналів.

Нейрони вихідного шару пов'язані із нейронами останнього прихованого шару, який подає перетворені сигнали, формуючи таким чином реакцію мережі.

Активаційні функції у нейронів вихідного шару можуть бути такими ж, як і у нейронів прихованого шару, проте найпоширеніша є модель прямоспрямованої мережі з лінійними вихідними нейронами. Багатошаровими персептронами називають нейронні мережі, які мають активаційні функції у прихованому шарі. Такий тип мереж використовується для вирішення завдань різного типу, і досить часто стає об'єктом досліджень.

Повністю зв'язана нейрона мережа зображена на рис. 2. Вона здобула таку назве через те, що всі нейрони у такій мережі пов'язані. Тобто нейрони першого шару повністю пов'язані із нейронами другого шару. Досить часто застосовують прямоспрямовані нейроні мережі які частково пов'язані. У такому типі мереж нейрони першого шару частково пов'язані із нейронами другого шару. Завдяки такій архітектурі вдалося реалізувати в нейронах первинні знання про закон обробки сигналів мережі.

Для реалізації завдань апроксимації, керування, класифікацій та розпізнавання образів досить поширене використання прямоспрямованих тришарових нейронних мереж [1].

Рекурентні мережі. Мережі, у яких є елементи тимчасової затримки, або, у яких є зворотні зв'язки, називають рекурентними. Найпростіший вид рекурентної мережі є мережа, яка складається з одного шару нейронів, які охоплені зворотними зв'язками. Таким чином кожен нейрон зв'язаний з іншими нейронами, але отримує сигнал від них із затримкою.

У випадку коли рекурентна нейрона мережа має у своїй структурі прихований шар, то він отримує окрім вхідних сигналів, вихідні сигнали мережі. Нейрона мережа, у якої присутні зворотні зв'язки, може мати необмежену кількість прихованих шарів.

Завдяки тому, що нейронна мережа має елементи часової затримки та рекурентні зв'язки, вона здобуває нелінійні властивості. У свою чергу це впливає на здатність нейронної мережі до навчання. Для того, щоб тренувати рекурентні мережі, потрібно робити облік їх динамічних властивостей.

Основне застосування даного типу нейронних мереж полягає у нейроемуляції динамічних об'єктів, їх ще називають нейромережевими моделями. Рекурентні мережі широко використовуються при вирішені таких завдань як розпізнавання образів, апроксимація часових послідовностей, керування та класифікація [2,3].

Мережі із повним зв'язком. Такий тип мереж ще називають повнозв'язними. Їх головна особливість полягає у тому, що між всіма нейронами існують зв'язки. Нейрона мережа Хопфілда є однією із найбільш відомих нейронних мереж такого типу. У повнозв'язних мережах нейрони мають двосторонні зв'язки. Якщо розглядати загальну

структуру мережі Хопфілда, то вона має кільцеву структуру, у неї відсутній прихований шар і неможливо визначити єдиний напрямок сигналів. Головний нейрон контролює обмін даними та роботу повнозв'язної нейронної мережі.

Як приклад можна навести мережу Хопфілда як повнозв'язну динамічну мережу яка побудована на принципах самоорганізації, але у якій явно не використовуються елементи часової затримки.

До іншого прикладу можна навести ґратчасті нейронні мережі. Вони створюються як масив нейронів і вхідні нейрони пов'язані із кожним елементом даного масиву. Через розмірність масиву можна визначити розмірність мережі. Через те, що у такій нейронній мережі відсутні зворотні зв'язки вона є прямостпрямованою, проте виділити у ній приховані шари або елементи не можливо.

Для вирішення завдань класифікації й розпізнавання образів особливо часто використовують повністю зв'язані мережі [3].

Радіально-базисний тип мереж. Радіально-базисна мережа це тришарова прямо спрямована мережа. Перший шар служить для ретрансляції вхідних сигналів. Нейрони прихованого шару здійснюють нелінійне перетворення вхідних сигналів. Лінійні нейрони підсумовують сигнали зі схованого шару й формують вихід мережі, при цьому зсув покладається рівним нулю. На відміну від багатошарового персептрона, для схованих нейронів РБФ-мережі відсутнє поняття вагсинаптичних зав'язків. У результаті параметризації мережі здійснюється настроювання аргументів радіально-базисних активаційних функцій прихованих вихідних нейронів [1].

Висновки. Розглянуто базові архітектури нейромереж. Показано їх сучасні особливості. Для того, щоб вирішити завдання апроксимації, класифікації, керування та розпізнання образів доцільніше всього використовувати тришарові прямоспрямовані нейронні мережі. Найчастіше всього рекурентні мережі застосовують у нейроемуляторах динамічних об'єктів. Також є можливість застосовувати їх для вирішення наступних завдань: апроксимація часових послідовностей, розпізнання образів, керування класифікація. Для вирішення завдань класифікації й розпізнавання образів більше всього підходять повністю зв'язані мережі.

Список літератури

1. Хайкин С. Нейронные сети: полный курс: пер. с англ. - 2-е изд. / С. Хайкин// – М.: Издательский дом "Вильямс". - 2006. – 1104 с.

2. Каллан, Роберт. Основные концепции нейронных сетей. /Р.Каллан//. - М.: Издательский дом "Вильямс". - 2001. - 288 с.

3. Кононюк А.Ю. Нейронні мережі і генетичні алгоритми. /А.Ю. Кононюк// К.: «Корнійчук». – 2008. – 446 с.

УДК 004.8

Дослідження сучасних методів штучного інтелекту

Константинова А.А., студент
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Центральноукраїнський національний технічний університет, м. Кропивницький

Головною метою досліджень штучного інтелекту (ШІ) є отримання методів, моделей та програмних засобів, які дозволяють штучним пристроям реалізувати цілеспрямовану поведінку та розумні міркування. Тому дослідження та огляд вже існуючих методів є необхідним для автоматизованого вирішення складних задач за допомогою ШІ.

ШІ - це наука і технологія створення інтелектуальних машин, програм, властивість інтелектуальних систем виконувати творчі функції, які традиційно вважаються прерогативою людини [1].

Представлення знань – один з найбільш сформованих напрямків ШІ [2]. Традиційно до нього відносилась розробка формальних мов та програмних засобів для відображення та опису так званих когнітивних структур. До представлення знань відносять також дослідження за дескриптивною логікою, логікою простору та часу, онтологіями [3].

Автоматизоване вирішення складних завдань потребує створення в комп'ютері штучних гетерогенних систем з самоорганізацією «віртуальних колективів», здатних інтегрувати різнорідну інформацію (нечітку, лінгвістичну, статистичну тощо), що надходить з багатьох джерел, і на її основі надавати рекомендації особі що приймає рішення. При цьому слід не просто об'єднати в рамках однієї системи кілька різних технологій ШІ, вони повинні доповнювати і компенсувати недоліки одна одної. Результат такої інтеграції – прояв синергетичного ефекту, коли інтегроване рішення якісно краще рішень, пропонованих застосуванням окремих методів [4].

Дуже важливо зрозуміти, яким чином слід інтегрувати методи ШІ, щоб отримати систему релевантну складній задачі. В реальних системах прояв синергетичного ефекту багато в чому обумовлено самоорганізацією, яка пов'язана з колективними процесами (координацією, узгодженістю і суперечкою) [4].

Технології синергетичного ШІ: 1) еволюційні обчислення, зокрема, генетичні алгоритми; 2) нейронні мережі; 3) клітинні автомати; 4) гібридні інтелектуальні системи; 5) багатоагентні системи.

Еволюційні обчислення беруть за основу еволюційні механізми природи і включає: генетичні алгоритми, еволюційне моделювання та еволюційне програмування, які сильно різнилися на початкових етапах розвитку, але сьогодні важко віднести конкретний алгоритм до того чи іншого напрямку [4].

Генетичні алгоритми (ГА) можна віднести до групи адаптивних методів. Вони поєднують елементи детерміністичного і стохастичного підходів, застосовуються в комбінаціях з аналітичними методами або іншими алгоритмами. В основі ГА лежить принцип природного відбору. В процесі пошуку аналізуються кілька гілок еволюції. Застосовуючи «функцію пристосованості», що визначає якість виконання завдання і виконує роль навколишнього середовища при моделюванні еволюційного процесу, генетичні алгоритми «вирощують» популяції об'єктів, «генна» структура яких більш пристосована до поточної ситуації [5].

Нейронна мережа (neural network) представляє собою машину, що моделює спосіб обробки мозком конкретного завдання. Ця мережа зазвичай реалізується за допомогою електронних компонентів або моделюється програмою, яка виконується на цифровому комп'ютері [6].

Найбільш розповсюдженими задачами, якими займаються нейронні мережі є класифікація, розпізнавання, передбачення. Нейрон – це обчислювальна одиниця, яка отримує інформацію, виконує з нею прості обчислення та передає її далі. Вони діляться на три основні типи: вхідний, прихований і вихідний. Функція активації – це спосіб нормалізації вхідних даних. Тобто, якщо на вході буде велике число, пропустивши його через функцію активації, ви отримаєте вихід в потрібному вам діапазоні.

Клітинні автомати (КА) є дискретними динамічними системами, поведінка яких повністю визначається в термінах локальних залежностей. В значній мірі також це підходить для великого класу безперервних динамічних систем, визначених рівняннями в приватних похідних [7]. КА складається з періодичної решітки комірок, кожна з яких може перебувати в одному з кінцевої множини станів, таких як 1 і 0. Решітка може бути будь-якої розмірності. Для кожної комірки визначено безліч комірок, які називаються околом. Необхідно задати початковий стан всіх комірок та правил переходів комірок з одного стану в інший. На кожній ітерації, застосовуючи правила переходу з стану сусідніх комірок, визначається новий стан кожної з них. Зазвичай правила переходу однакові для всіх комірок та застосовуються відразу до всієї решітки. Тема КА дуже актуальна, тому що може привести до розгадок багатьох питань в навколишньому світі.

Гібридна інтелектуальна система (ГіІС) - система, в якій використовується більше одного методу імітації інтелектуальної діяльності людини.

Термин ГіІС з'явився в 1992 р. Автори вкладали в нього значення гібридів таких методів, як експертні системи, нейромережі та генетичні алгоритми. Експертні системи – символьні, а штучні нейронні мережі і генетичні алгоритми – адаптивні методи ШІ [5].

Міждисциплінарний напрямок «гібридні інтелектуальні системи» об'єднує вчених, які досліджують придатність декількох методів з різних

класів методів формалізованого представлення систем (МФПС): аналітичних, статистичних, логіко-лінгвістичних, нечітких та інших - до вирішення задач прийняття рішень. Жоден з класів МФПС не може претендувати на універсальність. Переваги одних, компенсуючи слабкі сторони інших за рахунок взаємозв'язків частин цілого, дадуть нову інтеграційну властивість нову, корисну сутність, більш повний задачно-орієнтований опис предметної області, що досліджується [5].

Наукові роботи в області багатоагентних систем (БАС) ведуться вже давно [2]. Однак лише в останні часи вони оформились в багатопланові розділи ШІ [5].

Ключова ідея багатоагентного підходу – соціальний характер інтелекту. В БАС передбачається, що окремий агент не може охопити всю задачу цілком, здатний вирішити лише деяку її частину. Тому для вирішення складної проблеми потрібні організація (самоорганізація) та координація агентів [5].

У штучному інтелекті, під терміном інтелектуальний агент мають на увазі розумну сутність, здатну до автономних дій у середовищі, що необхідні для досягнення мети, яка ставилась при його розробці. Це може бути як вбудована програмна система, так і робот.

У штучному інтелекті існує кілька типів агентів (фізичний агент, часовий агент).

Усіх агентів можна розділити на п'ять груп, за типом обробки інформації, що сприймається: агенти з простою поведінкою, агенти з поведінкою, заснованою на моделі, цілеспрямовані агенти, практичні агенти, агенти, що навчаються (Autonomous intelligent agents). Агентів класифікують за ступенем антропогенності (природні, штучні), за ступенем матеріальності (матеріальні, ідеальні), рухомості (статичні, мобільні), розвитку внутрішньої моделі зовнішнього світу (реактивні, інтелектуальні), за способом поведінки (імпульсивні, трофічні, інтенціональні, рефлекторні).

Функції, що визначають інтелектуального агента повноцінним: когнітивна, регулятивна, ресурсна, комунікативна.

Під інтелектуальним агентом розуміється активний елемент, що моделює поведінку людини в процесах збору і обробки інформації і автономно просувається в інформаційному просторі в напрямку мети.

Здатність функціонувати в умовах нечіткої суперечливої інформації – є найважливішою особливістю інтелектуального агента. Але агент не здатен визначати вичерпно параметри середовища та не може точно прогнозувати результати намічених дій, тому що у нього обмежені можливості рецепторів і ефекторів.

В БАС зв’язки між агентами виникають в процесі її роботи.

В останні роки дуже інтенсивно розвивається машинне навчання. Його ціллю є автоматизація вирішення складних професійних задач в різних сферах діяльності. Методи машинного навчання можна розділити на 3

основні категорії: контрольоване, неконтрольоване і навчання з підкріпленням. Часто застосовується індивідуальний підхід при вирішенні задачі машинного навчання. Для контролю складності, більш популярним з методів є кросс-валідація, коли відбувається декілька процесів навчання при різних параметрах алгоритма та вибирається найбільш вдалий варіант.

В наш час зацікавленість прикладними інтелектуальними технологіями поступово зростає. Велика увага приділяється створенню технологій, що доповнюють інтелектуальність у нашому оточенні життя. На сучасному етапі розвитку різні методи штучного інтелекту можуть вирішити окремо взяті проблеми, причому доволі успішно [8]. Але теорії загального інтелекту ще не існує.

Список літератури

1. Аверкин А.Н., Гаазе-Рапопорт М. Г., Поспелов Д.А. Толковый словарь по искусственному интеллекту.- М.: Радио и связь, 1992. - 256 с. [Електронний ресурс] – Режим доступу: http://www.raai.org/library/tolk/aivoc.html#L208

2. Осипов Г.С. Искусственный интеллект: состояние исследований и взгляд в будущее [Електронний ресурс] – Режим доступу: http://www.raai.org/about/persons/osipov/pages/ai/ai.html

3. Осипов Г.С. Методы искусственного интеллекта. – М.: ФИЗМАТЛИТ, 2011. – 296 с.

4. Колесников А.В., Кириков И.А., Листопад С.В. Гибридные интеллектуальные системы с самоорганизацией: координация, согласованность, спор. – М.: ИПИ РАН, 2014. – 189 с.

5. Решение сложных задач коммивояжера методами функциональных гибридных интеллектуальных систем / А. В. Колесников, И. А. Кириков, С. В. Листопад, С. Б. Румовская, А. А. Доманицкий. – М.: ИПИ РАН, 2011. - 295 с.

6. Саймон Хайкин Нейронные сети: полный курс, 2-е издание. : Пер. с англ. М. Издательский дом "Вильямс", 2006. 1104 с. : 7. Астафьев Г. Б., Короновский А.А., Храмов А.Е. Клеточные автоматы: Учебно-Методическое пособие. – Саратов: Изд–во ГосУНЦ «Колледж», 2003. 24с.

8. Гершман А. Заблуждения искусственного интеллекта // [Електронний ресурс] – Режим доступу: https://postnauka.ru/faq/80051

УДК 004.832.34:004.827

Дефазифікація результуючої функції приналежності виводу з бази правил при нечіткому управлінні

Мацуй А.В., студент,
Єніна І.І., к.т.н., доцент
Центральноукраїнський національний технічний університет
м. Кропивницький

Вступ. Нечітка логіка («fuzzy logic») або управління на основі методів теорії нечітких множин використовується при недостатньому знанні про об'єкт управління або наявності досвіду управління ним [1]. Тому в нелінійних системах, опис яких дуже трудомісткий, використання досвіду експертів-технологів є бажаним, а в деяких випадках і необхідним. Нечітка логіка імітує людське мислення і забезпечує ефективні засоби відображення невизначеностей і неточностей реального світу. Наприклад, людина може відповісти на питання невизначено: так, швидше за все так, можливо так, не знаю, можливо ні, швидше за все ні, ні. В нечіткій логіці такі вирази можна висловлювати математично і обробляти на комп'ютері.

Оскільки інформація, отримана від оператора, виражена, як правило, словесно або у формі даних журналів контролю, які потребують додаткової обробки і аналізу, то для її використання в описі моделі процесу застосовують лінгвістичні змінні і апарат теорії нечітких множин, який був розроблений Л. Заде в 1965 году [1].

В даний час, регулятори з нечіткою логікою використовуються в багатьох системах управління, застосовуваних для наведення телекамер при трансляції спортивних подій; в системах кондиціонування повітря, при управлінні подачею технологічної сировини і продуктів; для автоматичного керування електродвигунами, а також в багатьох інших системах.

Викладення основного матеріалу. Головним недоліком регуляторів, заснованих на правилах нечіткої логіки, є складність визначення даної функції приналежності. В цьому розумінні сама теорія нечітких множин теж є нечіткою. Наприклад, в літературі наводиться більше 10 способів різних визначень функції приналежності для перетину множин, але не сказано, яку з них потрібно вибрати для вирішення конкретного завдання. Тому при вирішенні використовують більш зрозумілу операцію знаходження функцій приналежності множин, аналогічно правилами теорії ймовірності [2]. Система нечіткого виводу, будь-якого нечіткого керування, складається з п’яти функціональних блоків (рис.1).

Для застосування методів нечіткої логіки, перш за все, необхідно перетворити звичайні чіткі змінні в нечіткі. Дана процедура називається фазифікацією.

Важливу роль в отриманні якісного управління відіграє процес дефазифікації нечіткої множини. Тобто, це операція знаходження чіткого значення величини, яке б найбільш «раціональним» чином представляло нечітку множину. Найбільш відомими методами дефазифікації є [3]:

- метод середнього максимуму (Middle of Maxima);
- метод першого максимуму (First of Maxima);
- метод останнього максимуму (Last of Maxima);
- метод центру ваги (Center of gravity);
- метод центру сум (Center of Sums);
- метод висот (Height).

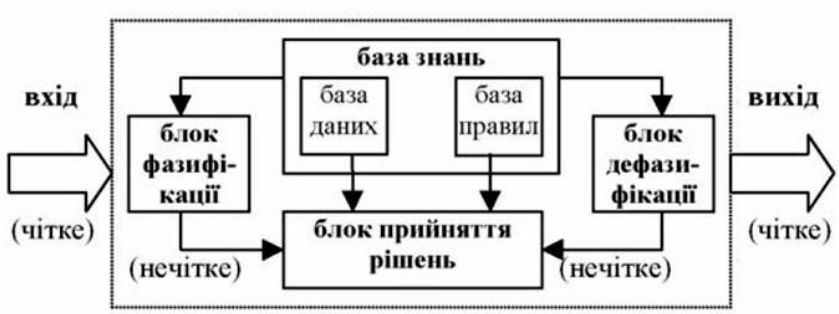


Рисунок 1 – Структурна схема системи нечіткого виводу

Розглянемо основні переваги та недоліки кожного з методів.

Метод середнього максимуму (ММ). Функцію приналежності можна розглядати як функцію, яка представляє інформацію про подібність між окремими елементами множини і про найбільш типовому її елементі.

Перевагою даного методу є простота обчислень, що допускає використання в системах управління дешевших мікропроцесорів. Разом з тим, простота обчислень досягається ціною певних недоліків.

Недолік методу полягає в тому, що на результат дефазифікації впливає тільки нечітка множина, що має найбільший ступінь активізації - множини, активізовані в меншій мірі, ніякого впливу на результат не надають.

Метод першого максимуму (FM). В методі першого максимуму в якості чіткого значення, що представляє результуючу нечітку множину-висновок, вибирається найменше значення, що максимізує її функцію приналежності.

Переваги методу:

- низька вартість обчислень;
- велика (в порівнянні з методом ММ) чутливість до змін ступеня активізації висновків бази правил.

Недоліки методу:

- неоднорідність;

- врахування в процесі дефазифікації тільки множини з найбільшим ступенем активізації.

Метод останнього максимуму (LM). Метод останнього максимуму в якості чіткого значення для представлення результуючої нечеткої множини-висновку вибирає найбільше значення, відповідного максимуму функції приналежності.

Метод LM має ті ж переваги і недоліки, що і метод FM.

Метод центру ваги (CG). Метод центру ваги передбачає, що в якості чіткого значення для представлення результуючої нечіткої множини, що задається функцією приналежності, повинна вибиратися координата центра ваги фігури, обмеженої графіком цієї функції.

Переваги методу CG:

- в дефазифікації беруть участь всі активізовані функції приналежності висновків (всі активні правила), тобто метод центру ваги є «демократичним» і забезпечує більш високу чутливість нечіткої моделі до зміни вхідних сигналів, ніж методи FM, LM і MM.

Недоліки методу CG:

- висока вартість обчислень, пов'язана з інтеграцією поверхонь нерегулярної форми, особливо у випадку використання функцій приналежності, які не складаються з прямолінійних ділянок (наприклад, гауссових функцій). Для інтегрування необхідно визначити точки перетину окремих складових функцій приналежності, розбити поверхню на сектори і виконувати інтегрування у межах кожного з секторів. Обчислення спрощуються, якщо використовувати прямокутні функції приналежності, хоча функції іншої форми можуть забезпечити більш високу точність моделювання.

- звуження інтервалу дефазифікації. Даний недолік можна усунути, розширюючи крайні нечіткі множини так, щоб їх центри ваги збігалися з межами діапазону можливих значень операції. Даний метод називається розширеним методом центру ваги (Extended Center of Gravity, ECG).

- нечутливість методу у тому випадку, коли активізується тільки одна вихідна функція приналежності. Даний недолік можна зменшити, якщо не використовувати у правилах однакові нечіткі множини.

- зниження чутливості методу CG у випадку, коли носії вихідних множин нечіткої моделі значно розрізняються по ширині.

Метод центру сум (CS). В базі правил нечіткої моделі можуть часто зустрічатися правила, у висновку яких міститься одна і та ж нечітка множина. Існують бази правил, у яких одна і та ж нечітка множина на виході моделі активізується одночасно декількома правилами. Враховувати даний вплив дозволяє метод центру сум (CS), який виробляє акумуляцію множин відповідних висновків окремих правил.

Переваги методу:

- зниження вартості обчислень в порівнянні з методом CG;

- участь всіх правил у процесі розмірковувань, що здійснює позитивний вплив на ряд нечітких моделей і регуляторів.

Інші переваги і недоліки такі ж, як у методу CG.

Метод висот (H). Є спрощеним дискретним варіантом методу центру сум. Кожна нечітка множина на виході моделі тут замінюється синглетон (одноелементною множиною), що збігається з модальним значенням цієї множини. Тому даний метод називають також методом одноелементних множин.

Переваги методу висот:

- значне зменшення вартості обчислень в порівнянні з методами CG і CS;
- ширина носіїв вихідних множин не впливає на результат дефазифікації;
- вид функцій приналежності не впливає на дефазифікацію. (Для деяких завдань це може бути недоліком.);
- неперервність;
- чутливість.

В нечіткому моделюванні та управлінні метод висот використовується досить часто, що обумовлено, перш за все, простотою обчислень, а також іншими її перевагами. Якщо множини значень вхідних величин є нечіткими (а не одноелементними, як вихідні), то модель (регулятор) зберігає свій нечіткий характер.

Проведений аналіз літературних джерел показав, що, незважаючи на ряд недоліків, найпоширенішим і універсальним є метод центру ваги.

Висновки. Таким чином, правильно обраний метод дефазифікації дозволяє розробляти інтелектуальні регулятори, на основі принципів нечіткої логіки, для різних галузей промисловості. Це пов'язано з тим, що даний тип засобів і систем регулювання, дозволить створити абсолютно новий клас пристроїв, що дозволяють не тільки обчислювати настройки, які відповідають певним обмеженням і вимогам технологічного процесу, а й прогнозувати поточні зміни величин, підбираючи оптимальні значення параметрів.

Список літератури

1. Егупов, Н. Д. Методы робастного, нейро-нечеткого и адаптивного управления: Учебник/ Н. Д. Егупов. – 2-е изд. – М.: МГТУ им. Баумана, 2002. – 744 с.

2. Круглов, В. В. Нечеткая логика и искусственные нейронные сети / В. В. Круглов, М. И. Дли, Р. Ю. Годунов. – М. : Физматлит, 2001. – 224 с.

3. Пегат А. Нечеткое моделирование и управление / А. Пегат; пер. с англ. – 2-е изд. – М.: БИНОМ. Лаборатория знаний, 2013. – 798 с.

УДК 004.852

Дослідження методів машинного навчання

Нестеряк Е.В., студент
Науковий керівник – Константинова Л.В., викладач
Центральноукраїнський національний технічний університет, м. Кропивницький

В останні роки дуже інтенсивно розвивається машинне навчання. Його ціллю є автоматизація вирішення складних професійних задач в різних сферах діяльності. І тому дослідження методів машинного навчання є актуальним завданням на сьогоднішній день.

Одними з найпопулярніших сфер застосування машинного навчання на сьогоднішній день є: розпізнавання зображень, тексту, голосу, тощо; покращення алгоритмів інформаційного пошуку, створення чатботів, підбір таргетованої реклами, задачі прогнозування та управління і т.д.

Підхід до задач навчання – це концепція, парадигма, точка зору на процесс навчання, яка приводить до набору базовых пропозицій, гіпотез, евристик, на основі яких будується модель, функціонал якості та методи його оптимізації.

Розділ методів за підходами доволі умовний. За допомогою різних підходів можливо отримати однакову модель, але різні методи її навчання. В деяких випадках ці методи набагато відрізняються, в інших – майже не відрізняються та «плавно трансформуються» один в одного шляхом незначних модифікацій.

На даний момент існує велика кількість різних навчальних методів. Вони мають різні параметри, які можливо налаштовувати, покращуючи якість їх роботи для конкретних задач.

Методи машинного навчання можна розділити на 3 основні категорії: контрольоване, неконтрольоване і навчання з підкріпленням [1].

Як правило методи машинного навчання використовуються для класифікації або кластеризації деяких об’єктів. Розглянемо групи методів машинного навчання, що використовуються у задачах класифікації та кластеризації.

Статистична класифікація. Серед даних методів можна виділити три групи методів: параметричне оцінювання щільності (квадратичний дискримінант; лінійний дискримінант Фішера) [2], непараметричне оцінювання щільності (метод парзеновського вікна), оцінювання щільності як суміші параметричних щільностей (поділ суміші розподілів, ЕМ-алгоритм; метод радіальних базисних функцій). Наївний байєсовський класифікатор [4] – метод, який може бути як параметричний, так і непараметричений. Він заснований на нереалістичному припущенні про статистичну незалежність ознак. Завдяки цьому метод надзвичайно простий.

Класифікація на основі подібності. Метричні алгоритми класифікації застосовуються в тих завданнях, де вдається природним чином задавати об'єкти не їх ознаковими описами, а матрицею попарних відстаней між об'єктами. Класифікація об'єктів за їх схожістю заснована на гіпотезі компактності.

Метричні алгоритми відносяться до методів міркування на основі прецедентів (Case Based Reasoning, CBR). Найбільш відомі метричні алгоритми класифікації: метод найближчих сусідів; метод парзеновського вікна; метод потенційних функцій; метод радіальних базисних функцій; відбір еталонних об'єктів.

Класифікація на основі роздільності. Велика група методів класифікації заснована на явній побудові поверхні, що розділяє в просторі об'єктів (лінійний дискримінант Фішера, SVM (Support Vector Machine) [2] та ін.).

Регресія застосовується для вирішення задач регресійного характеру (лінійна, нелінійна, логістична) [2,3].

Алгоритми кластеризації відносяться до неконтрольованого навчання [4,5]. Найпопулярніші з них: алгоритми на базі центру ваги трикутника; алгоритми на основі підключення; алгоритми щільності на основі просторової кластеризації; імовірнісний алгоритм; алгоритм зменшення розмірності; нейронні мережі.

Алгоритми кластеризації використовуються в біології, соціології та інформаційних технологіях. Наприклад, в біоінформатиці за допомогою кластеризації аналізуються складні мережі взаємодіючих генів, що складаються часом з сотень або навіть тисяч елементів.

Метод головних компонент (PCA) [4] – це статистична процедура, яка використовує ортогональне перетворення з метою конвертації набору спостережень за можливо корельованими змінними в набір значень лінійно некорельованих змінних, які називаються головними компонентами.

Аналіз незалежних компонент (ICA) [4] являє собою статистичний метод виявлення прихованих чинників, які лежать в основі безлічі випадкових величин, сигналів і інших вимірів.

Виявлення аномалій є прикладом неконтрольованого підходу до машинного навчання [4].

У навчанні з підкріпленням алгоритм вибирає дію у відповідь на кожну точку даних. Алгоритм навчання отримує сигнал, що сповіщає про успіх, який дає зрозуміти, наскільки вдало було прийнято рішення. На основі цього алгоритм змінює свою стратегію для досягнення кращого результату [4].

Вирішуючи задачу машинного навчання в більшості випадків застосовується індивідуальний підхід. Людина, що вирішує цю задачу на основі власного досвіду вибирає певний алгоритм, налаштовує його параметри. Для контролю складності, більш популярним з методів є

кросс-валідація, коли відбувається декілька процесів навчання при різних параметрах алгоритма та вибирається найбільш вдалий варіант [6].

Важливою проблемою в машинному навчанні є вибір методу перетворення вхідних даних в вектори, які допускають класифікацію. Часто доводиться робити спроби та аналізувати велику кількість таких методів для вибору найбільш оптимального з точки зору розділення класів [6].

Машинне навчання має величезний потенціал, а сфера його застосування весь час розширюється. Одним з головних завдань для розробки якісного програмного забезпечення з використанням машинного навчання є підготовка високоякісних даних для навчаючої вибірки. У багатьох організаціях такі дані розпорошені по різним файловим сховищам та базам даних, або зберігаються у форматах, які доволі важко обробити. Підготовка даних для машинного машинного навчання є актуальним питанням та підлягає більш детальному вивченню.

Список літератури

1. Выбор алгоритмов машинного обучения Microsoft Azure// 2017 [Електронний ресурс] – Режим доступу: https://docs.microsoft.com/ru-ru/azure/machine-learning/studio/algorithm-choice

2. Machine Learning with MATLAB// MathWorks [Електронний ресурс]. – Режим доступу: https://www.mathworks.com/solutions/machine-learning.html

3. Стрижов В. В. Методы индуктивного порождения регрессионных моделей. М.: ВЦ РАН. 2008. 55 с.

4. 10 главных алгоритмов машинного обучения// 2016 [Електронний ресурс] – Режим доступу: http://ru.datasides.com/code/algorithms-machine-learning/

5. Machine Learning, Streaming IoT, and Connected Medical Devices// 2017 [Електронний ресурс]. – Режим доступу: https://mapr.com/blog/ml-iot-connected-medical-devices/

6. Невоструев К. Н. Обзор литературы по методам машинного обучения// Компьютерные инструменты в образовании. - 2014 [Електронний ресурс] – Режим доступу: https://cyberleninka.ru/article/v/obzor-literatury-po-metodam-mashinnogo-obucheniya-machine-learning

УДК 004.853

Адаптивная вероятностная кластеризация в задачах анализа текстов

Пирус А.Е., студетка 5-го курса, Прийма А.К., студетка 6-го курса
Научный руководитель – Бодянский Е.В., д.т.н., проф.
Харьковский национальный университет радиоэлектроники, г. Харьков

The introduced methods allow to work directly with the matrix data, avoiding the bulky operations of vectoring and an opposite operation of vectoring, and improving the time of clustering (the quality of the developed and modifiable algorithms is the same).

На данный момент кластерный анализ является важной задачей, поскольку оценка результатов кластеризации не может быть объективной, и различные методы дают различные результаты для одних и тех же данных. Также, кроме большого количества существующих проблем появляются новые, требующие новых методов решений или усовершенствования старых. Например, к таким проблемам могут относиться представление данных в матричной, а не векторной форме или большая размерность вектора данных.

Формально под задачей кластерного анализа заданного множества объектов понимается задача нахождения некоторого разбиения этого множества объектов на непересекающиеся подмножества таким образом, чтобы элементы, относимые к одному подмножеству, отличались между собой в значительно меньшей степени, чем элементы из разных подмножеств.

Данная работа посвящена разработке алгоритма кластеризации для анализа текстов и его модификация для обработки матричных наблюдений (сигналов).

Пусть W = $\{w_1, \ldots, w_{|W|}\}$ − заданное множество слов, словарь. Документом d назовем множество слов из W, порядок которых не важен: d=$\{w_j\}$, где $w_j \in$W− j-ое слово в документе d, j = 1,…, |d|.

Пусть D = $\{d_1, \ldots, d_{|D|}\}$ − множество всех текстовых документов, k− заданное число кластеров, на которое требуется разбить множество D. Требуется задать функцию расстояния на множестве документов: $\rho(di, dj): D \times D \rightarrow R_+$, и провести кластеризацию текстовой коллекции. Предлагается удалить из текстов стоп-слова и слова, встречающиеся не более одного раза в тексте, как шумовую составляющую. Стоп-слово формально определим как слово из некоторого заранее заданного списка S. Представим каждый преобразованный документ в виде вектора:

$$\mathbf{d_i} = \begin{pmatrix} n(d_i, w_1) \\ \dots \\ n(d_i, w_j) \\ \dots \\ n(d_i, w_{|w|}) \end{pmatrix}, \quad (1)$$

где $n(d_i, w_j)$ − число вхождений слова $w_j \in W$ в текст d_i.

Далее используя это представление документа, ввести расстояние между документами как расстояние между векторами: $\rho(d_i, d_j) = \rho(\mathbf{d_i}, \mathbf{d_j})$

В качестве функции расстояния ρ(x, y) между векторами x, $y \in R^n$ можно взять Евклидову метрику:

$$E = \sum_{i=1}^{N} \sum_{j=1}^{C} u_{ij}^m \left\| x_i - c_j \right\|^2, \quad (2)$$

где m − любое вещественное число, большее 1, u_{ij} − степень принадлежности x_i к кластеру j $0 \le u_{ij} \le 1$, x_i − значения *i*-го признака у *i*-го (*j*-го) объекта, c_j – центр масс j-го кластера.

Предлагается, используя функцию расстояния $\rho(\mathbf{d_i}, \mathbf{d_j})$, провести кластеризацию текстовой коллекции алгоритмом C-means. Метод кластеризации можно рассматривать как точный или приближённый алгоритм поиска оптимума некоторого функционала. Если y_j — номер кластера, к которому отнесет j-ый документ алгоритм кластеризации, то можно ввести следующие функционалы качества:

$$F_0 = \frac{\sum_{i<j}[y_i = y_j] p(d_i, d_j)}{\sum_{i<j}[y_i = y_j]} \to min, \quad (3)$$

т.е. нужно минимизировать среднее внутрикластерное расстояние,

$$F_1 = \frac{\sum_{i<j}[y_i \neq y_j] p(d_i, d_j)}{\sum_{i<j}[y_i \neq y_j]} \to max, \quad (4)$$

т.е. нужно максимизировать среднее межкластерное расстояние. Чтобы учесть и внутрикластерное и межкластерное расстояние можно ввести функционал F :

$$F = \frac{F_0}{F_1} \to min. \quad (5)$$

В данном докладе был исследован алгоритм кластеризации текстов, описаны основные проблемы, которые могут возникнуть при решении данной задачи, а также предложено решение данной задачи.

УДК 681.5

Обґрунтування розробки інтелектуальної системи підтримки прийняття рішень для вибору комбінації джерел

Рубцов В.С., студент 3 курсу,
Погорілий М.С., студент 2 курсу
Науковий керівник – Голик О.П., к.т.н., доцент
Центральноукраїнський національний технічний університет, м. Кропивницький

Наразі суттєвою є проблема енергозабезпечення споживачів як побутового сектора, так і підприємств. Це пояснюється в першу чергу зростанням тарифів на енергоносії. Одним із шляхів розв'язання даної проблеми є використання відновлюваних джерел енергії (ВДЕ).

Головний вплив на впровадження та розвиток ВДЕ в Україні мають наступні фактори:

- рівень політичної та громадської підтримки розвитку ВДЕ;
- конкурентоспроможність ВДЕ по відношенню до традиційних джерел та обсяги необхідної фінансової підтримки на загальнодержавному та місцевих рівнях для їх впровадження та розвитку;
- жорсткість екологічних обмежень та вимог;
- обсяги впровадження ВДЕ на базі використання механізмів реалізації проектів спільного впровадження та торгівлі квотами на викиди газів, які викликають парниковий ефект.

Як показала практика найдоступнішими ВДЕ є сонячна енергія та енергія вітрових потоків. Привабливість сонячної та вітрової енергій обумовлена рядом причин: безкоштовність енергії; екологічна чистота; територіальна розповсюдженість і доступність; тривалість існування на перспективу. Головними недоліками цих енергій є: періодичність надходження; стохастичний характер надходження; в окремих випадках можливість завдання шкоди фауні.

Існуючі автоматизовані системи керування (АСК) енергозабезпеченням споживачів на основі вітрової та сонячної енергій не завжди можуть адекватно реагувати на порушення та збої в процесі керування системою. Пояснюється це тим, що в певних умовах в системі існують невизначеності, а це в свою чергу, суттєво може змінити режим роботи системи та погіршити показники якості. Тому виникає потреба у пошуку нових методів керування АСК.

Новим напрямом у розвитку теорії і практики керування АСК в умовах невизначеності є використання інтелектуальних систем підтримки прийняття рішень (ІСППР).

Дослідженню питання щодо використання ІСППР в умовах невизначеності для АСК енергозабезпеченням на основі енергій сонця та

вітру присвячено небагато робіт. Серед них можна виділити [1-3].

Сучасний ринок пропонує багато різних сонячних та вітрових установок. Таким чином розробка ІСППР для АСК енергозабезпеченням споживачів полягає перш за все у чіткому виборі енергоустановок.

І тут у споживача (замовника системи) виникає необхідність у виборі енергоустановок, які б могли задовольнити енергетичні потреби споживача та мати невисоку вартість. Як правило, споживачу самостійно прийняти рішення щодо вибору комбінації енергоустановок досить складно. Оскільки на прийняття рішення впливають багато факторів:

- питома вартість установки;
- номінальна потужність установки;
- можливість задовольнити енергетичні потреби та ін.

Таким чином приходимо до висновку, що доцільним є розробити ІСППР для вибору комбінації енергоустановок, які б могли задовольнити вимоги споживача.

Пропонується розробити таку ІСППР, яка б мала базу даних та базу знань. До складу бази даних повинна входити інформація про існуючі на сучасному ринку сонячні та вітрові установки, їх технічні характеристики, вартість та ін. До складу бази знань необхідно внести результати прийняття рішення щодо вибору тієї чи іншої енергоустановки (або їх комбінації), які б могли задовольнити вимоги споживача. В результаті споживач зможе прийняти рішення щодо вибору енергоустановок, спираючись на свої потреби.

Для розробки бази знань такої системи доцільно використовувати дерева рішень. Метод дерева рішень може використовуватись як в ситуаціях, в яких використовується матриця рішень, так і в більш складних ситуаціях, в яких результати одного рішення впливають на наступні рішення (послідовні рішення).

Дерева рішень зазвичай використовують при ПР в умовах ризику. Його будують за типом алгоритму роботи системи. Визначаються етапи прийняття рішень, імовірності при прийнятті даного рішення та імовірнісні наслідки реалізації певного рішення.

На рис. 1 наведено дерево рішень для прийняття рішення щодо керування АСК енергозабезпеченням в умовах ризику.

Згідно даної структури маємо такі рішення:

1 – прийняття рішення щодо типу джерела енергії.

2 – прийняття рішення щодо стану ВЕУ.

3, 4, 15, 16, 26, 27, 38, 39, 43, 44 – прийняття рішення щодо потреб споживача в електроенергії.

5, 17, 28 – прийняття рішення щодо кількості виробленої енергії.

6, 18, 29 – прийняття рішення щодо передачі енергії до АКБ.

7, 10 – прийняття рішення щодо використання іншого джерела енергії – сонячна енергія.

8, 9, 19, 20, 30, 31, 41, 45 – прийняття рішення щодо перерозподілу отриманої енергії.

11, 13, 22, 24, 33, 35, 37 – прийняття рішення щодо стану АКБ.

12, 14, 23, 25, 34, 36 – прийняття рішення щодо заряду АКБ.

21, 32 – прийняття рішення щодо використання іншого джерела енергії – АКБ.

40 – прийняття рішення щодо різниці між потрібною енергією та кількістю енергії в АКБ.

42 – прийняття рішення щодо використання іншого джерела енергії – ДВЗ.

46 – прийняття рішення щодо сигналізації про стан ДВЗ.

На дереві рішень маємо наступні альтернативні варіанти:

a_1 – використання вітрової енергії.

a_2 – енергія від ВЕУ надходить.

a_3 – енергія від ВЕУ не надходить.

a_4 , a_6 , a_{23} , a_{25} , a_{42} , a_{44} , a_{59} , a_{60} , a_{63} , a_{65} , a_{72} , a_{74} – потреби в енергії на даний момент існують.

a_5 , a_7 , a_{24} , a_{26} , a_{43} , a_{45} , a_{64} , a_{66} , a_{73} , a_{75} - потреби в енергії на даний момент немає.

a_8 – кількість виробленої ВЕУ енергії більша ніж потрібна споживачу.

a_9 - кількість виробленої ВЕУ енергії дорівнює потребам споживача.

a_{10} – кількість виробленої ВЕУ енергії менша ніж потреби споживача.

a_{11} , a_{13} , a_{30} , a_{32} , a_{49} , a_{54} , a_{69} , a_{76} – передача енергії до споживача.

a_{12} , a_{17} , a_{31} , a_{36} , a_{50} , a_{55} – передача енергії до АКБ.

a_{14} , a_{18} , a_{33} , a_{37} , a_{51} , a_{56} , a_{61} – АКБ заряджена.

a_{15} , a_{19} , a_{34} , a_{38} , a_{52} , a_{57} , a_{62} – АКБ розряджена.

a_{16} , a_{20} , a_{35} , a_{39} , a_{53} , a_{58} – заряджання АКБ.

a_{21} , a_{40} – енергія від СБ надходить.

a_{22} , a_{41} – енергія від СБ не надходить.

a_{27} , a_{46} – кількість виробленої СБ енергії більше ніж потрібно споживачу.

a_{28} , a_{47} – кількість виробленої СБ енергії дорівнює потребам споживача.

a_{29} , a_{48} – кількість виробленої СБ енергії менша ніж потреби споживача.

a_{67} - кількість енергії в АКБ більше ніж потрібно споживачу.

a_{68} – енергії в АКБ не вистачає для задоволення потреб споживачів.

a_{70} – у баках ДВЗ паливо є.

a_{71} – палива у баках ДВЗ немає.

a_{77} – подача сигналу споживачеві про відсутність палива.

q_{ij} – імовірнісні наслідки реалізації певного рішення.

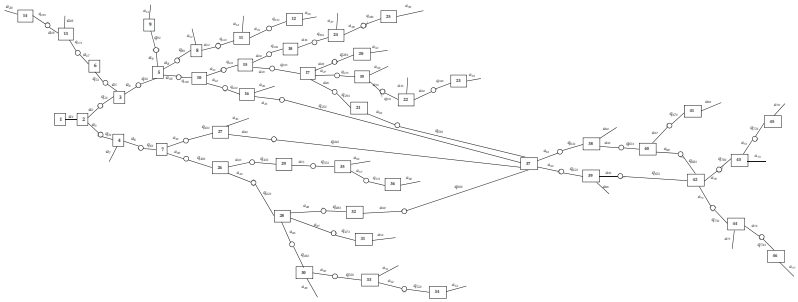


Рисунок 1 – Структурне зображення процесу енергозабезпечення в задачі вибору оптимального керування АСК

Висновки. Використання ІСППР на початковому етапі вибору енергоустановок, які можуть задовольнити потреби споживача, дає можливість приймати рішення в умовах невизначеності та ризику, постійно поповнювати базу даних та спростити процес вибору комбінації джерел енергії.

Список літератури

1. Ланге О. Оптимальные решения. Основы программирования. – М.: «Прогресс», 1967. – 289 с.

2. Голик О. П. Пошук оптимальних рішень щодо комбінацій енергетичних потоків у автоматизованій системі керування автономним енергопостачанням на основі відновлюваних джерел енергії в умовах невизначеності / О. П. Голик, Р. В. Жесан, Т. Ф. Шмельова // Управление, автоматизация и окружающая среда [Текст]: Материалы международной науч.-техн. конф., Севастополь, 24-28 мая 2010 г. / М-во образования и науки Украины, Севастоп. нац. техн. ун-т [и др.; редкол.: Пашков Е. В. (предс.) и др., науч. ред. Барабанов А. Т.] – Севастополь: Изд-во СевНТУ, 2010. – С. 214-218.

3. Голик О. П. Моделювання процесу прийняття рішень в умовах невизначеності для автоматизованої системи керування автономним енергопостачанням на основі вітрової та сонячної енергій / О. П. Голик, Р. В. Жесан // Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту: зб. наук. праць за матеріалами міжнар. наук. конф., 17 – 21 травня 2010 р., Євпаторія. Т. 1 – Херсон: ХНТУ, 2010. – С. 170-174.

УДК 629.7.07

Реализация системы поддержки принятия решений инструктора в моделирующем комплексе управления воздушным движением

Землянский А.В., старший преподаватель,
Сало Н.А., старший преподаватель
Летная академия Национального авиационного университета, г. Кропивницкий

Развитие современного общества делает процесс подготовки и постоянного повышения квалификации специалистов все дороже и дороже. На первое место выходят как проблемы доучебного тестирования и отсева кандидатов (профориентация), так и всемерное удешевление процесса подготовки при сохранении приемлемой эффективности.

С целью создания тренажерного комплекса управления воздушным движением (УВД) нового поколения, позволяющего реализовать индивидуальный подход к обучению в процессе тренажерной подготовки в Научно-производственном институте аэронавигации Летной академии Национального авиационного университета был разработан прототип многоцелевого моделирующего программного комплекса, который решает множество задач как процедурного, так и модульного тренажера.

Моделирующий комплекс позволяет производить пошаговый анализ выполненного упражнения по его завершению, используя систему поддержки принятия решений (СППР) инструктора. Это стало возможным благодаря созданию механизма хранения и анализа динамической воздушной обстановки (ДВО), а также действий обучаемого при выполнении упражнения.

Сбор данных для последующего анализа, как и пересчёт ДВО, происходит в «реальном времени». Анализ ДВО на текущий момент происходит «на лету», что позволяет оперативно выявлять и фиксировать возникновение потенциально конфликтных ситуаций (ПКС). Вслед за анализом ДВО следует оценка действий обучаемого, согласно введенных в СППР критериев в соответствии с требованиями зоны управления. Технология анализа ДВО, как и фиксация выявленных ошибок заложена в СППР.

Описанная система не имеет аналогов среди тренажерных комплексов на Украине, в связи с чем оценка, получаемая обучаемым при работе на таких комплексах, основана только на субъективном мнении инструктора и не всегда соответствует истинному уровню обучаемого.

При работе же с моделирующим комплексом погрешность при выставлении оценок за выполненные упражнения сводится к минимуму, поскольку СППР включает в себя систему объективного контроля (СОК), позволяющую проанализировать поведение обучаемого в тех или иных полетных ситуациях и выявить наиболее критичные ошибки,

допускаемые им при разрешении потенциально конфликтных ситуаций в процессе ОВД. СППР в состоянии самостоятельно поставить оценку, основываясь на заложенных критериях оценивания. Критерии и параметры оценивания могут варьироваться в зависимости от сложности упражнений и учебных задач, которые ставит перед обучаемыми инструктор. Кроме того, инструктору нет необходимости наблюдать за процессом выполнения задания, что положительно влияет как на количество одновременно обучаемых курсантов, так и на качество их обучения. По окончанию выполнения упражнения инструктор имеет возможность его просмотра в ускоренном режиме с детальным анализом допущенных ошибок. Отображение информации в режиме просмотра в точности соответствует отображению при выполнении упражнения. Это позволяет дополнительно обратить внимание инструктора на то, какие ошибки обучаемый допустил по невнимательности, а какие просто не видел и уделить время на их рассмотрение. Дополнительным преимуществом просмотра упражнения «глазами обучаемого» является то, что инструктор может оценить своевременность обнаружения ПКС обучаемым и правильность действий для его разрешения.

При выполнении упражнения производится сбор максимально возможного количества данных, что в свою очередь даёт возможность переоценки выполнения записанного упражнения путём введения дополнительных критериев оценки либо же изменения существующих. Это позволит инструктору своевременно выявить «узкие места» в обучении и привить необходимые для эффективной работы навыки. На рисунке 1 показан интерфейс СППР инструктора для разбора допущенных ошибок при просмотре выполненного упражнения.

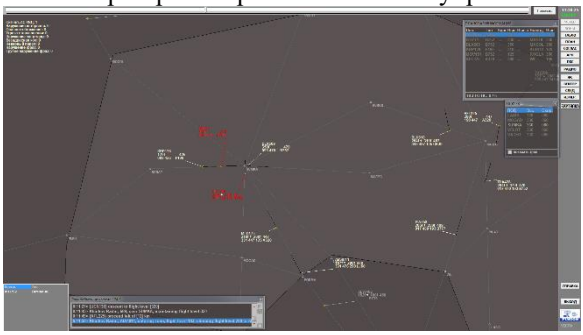


Рис. 1. Интерфейс СППР инструктора

Помимо сказанного, одним из весомых преимуществ моделирующего программного комплекса перед тренажерными средствами УВД является его мобильность. Он не требователен к программно-аппаратным ресурсам персонального компьютера и не подразумевает какой-либо специальной подготовки для установки и настройки. Поэтому, комплекс может быть легко установлен в любом компьютерном классе.

УДК 004.023, 539.18

Квантовий генетичний алгоритм вищих порядків для 0-1 задачі пакування рюкзака

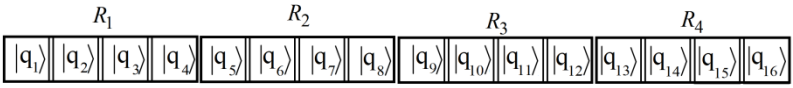
Ткачук В.М., к.ф.-м.н., доцент
Прикарпатський національний університет імені Василя Стефаника, м. Івано-Франківськ

Квантовий генетичний алгоритм (QGA) є новим еволюційним алгоритмом, що поєднує в собі ідеї квантових обчислень на технології класичних генетичних алгоритмів [1]. При реалізації QGA мінімальною одиницею інформації є кубіт – квантова система, що може перебувати в двох базових станах: $|0\rangle$ та $|1\rangle$ [2]. Квантова природа кубіта полягає в принципі суперпозиції:

$$|q\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle, \quad {\alpha_0}^2 + {\alpha_1}^2 = 1 \qquad (1)$$

Потужність квантових обчислень зумовлена квантовим паралелізмом, що ґрунтується на принципі суперпозиції та заплутаності станів. Можливість та ефективність використання заплутаних станів в QGA до задач комбінаторної оптимізації була проілюстрована в [3].

Структура квантової хромосоми. Якщо квантова хромосома складається із $N = 16$ кубітів, причому кожні чотири з них перебувають у заплутаному стані ($r = 4$) , то її можна представити наступним чином:



В даному випадку хромосома складається із чотирьох квантових регістрів (R_1, R_2, R_3, R_4). Кількість основних станів регістру рівна $2^r = 2^4 = 16$:

$$|0000\rangle, |0001\rangle, |0010\rangle, \dots, |1111\rangle$$

Згідно принципу суперпозиції його стан є лінійною комбінацією базових станів:

$$|q\rangle = \alpha_0|0000\rangle + \alpha_1|0001\rangle + \alpha_2|0010\rangle + \alpha_3|0011\rangle + \ \dots + \alpha_{16}|1111\rangle$$

При переході до квантових регістрів вищих порядків ($r > 2$) для представлення квантової хромосоми необхідно додатково збільшити розмір матриці M, необхідний для представлення особини популяції. Так, при $r = 4$:

$$M = \frac{N}{r} \cdot 2^r = \frac{16}{4} \cdot 2^4 = 64 > 2 \cdot N = 32$$

Оператор квантового гейту. Вся інформація про задачу та алгоритм її розв'язку закладається в квантовий гейт, тому його робота є визначаль-

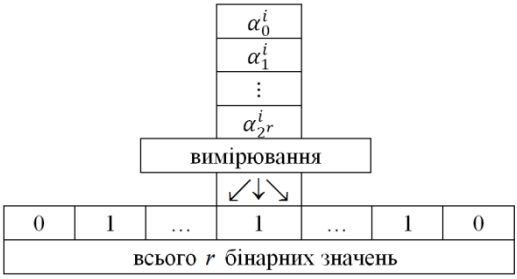
ною при побудові будь-якого QGA. Роботу оператора можна поділити на два етапи. На першому для кожного регістру R_i збільшується амплітуда ймовірності вибраного квантового стану b:

$$\left(\alpha_i^b\right)' = \sqrt{\left[\alpha_i^b\right]^2 + \mu\left(1 - \alpha_i^b\right)} \qquad (3)$$

Стан b визначається десятковим представленням фрагменту класичної хромосоми найкращої особини популяції, що відповідає квантовому регістру R_i. Значення μ лежить в межах $[0,1]$ та підбирається за результатами попередніх досліджень. Як показали моделювання, зважаючи на адаптивний характер роботи оператора, для задач комбінаторної оптимізації можна прийняти $\mu \approx 1$.

На другому етапі необхідно пропорційно зменшити амплітуди ймовірності інших станів регістру R_i для забезпечення виконання умови нормування. Таким чином у кожному новому поколінні забезпечується збільшення ймовірності того, що в результаті спостереження генеруються класичні особини, більш схожі на найкращу. При такому алгоритмі роботи квантового гейту також можна обійтися без таблиці пошуку, що є одним із принципових недоліків традиційного QGA.

Алгоритм вимірювання стану квантової хромосоми реалізований згідно запропонованого в [3] підходу. Схематично процес вимірювання стану регістру R_i та перехід до класичного представлення хромосоми можна зобразити наступним чином:



Процедура відновлення квантової хромосоми. В процесі ініціалізації популяції, чи в ході її еволюції завжди є ймовірність отримати ряд «поганих» особин, які не задовільняють умові обмеження загальної ваги рюкзака. Процедура відновлення в QGA принципово інша, ніж в класичному генетичному алгоритмі, бо вимагає корекції і квантової хромосоми. Процес її відновлення реалізовано згідно представленого нижче алгоритму:

Відновлення квантової хромосоми

1 **for** $i \in \{1, \dots, k\}$ **do**
2 $sum \leftarrow 0$

3 **for** $j \in \{0, \dots, 2^r - 1\}$ **do**
4 $sum \leftarrow sum + x_i \cdot 2^j$
5 **for** $j \in \{0, \dots, 2^r - 1\}$ **do**
6 $\alpha_i^j \leftarrow \sqrt{(1-\beta^2)/(2^r-1)}$
7 **end for**
8 $\alpha_i^{sum} \leftarrow \beta$
9 **end for**
10 **end for**

Тут x_i – класична хромосома, отримана із квантової в результаті квантового вимірювання та наступного відновлення. $\beta \in [0,1]$ - параметр роботи алгоритму. Дослідження показали, що він не залежить від розміру системи N, рівня кореляції вхідних даних і оптимальним в подальших моделюваннях взято $\beta = 0.985$ (див. рис.1).

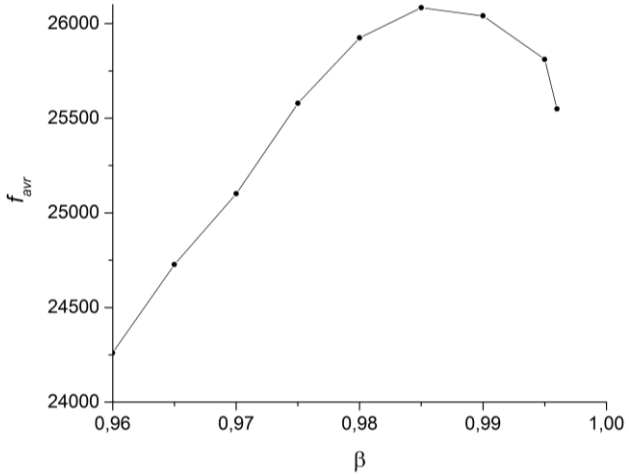


Рисунок 1. Вплив $\boldsymbol{\beta}$ на середню пристосованість найкращої особини популяції при $\boldsymbol{N = 500}$ некорельованих вхідних даних

Результати моделювання. При реалізації QGA розмір популяції складав $s = 50$ особин, час еволюції $t = 500$, $N = 500$ некорельованих вхідних даних. Ефективність роботи оцінена за середньою пристосованістю найкращої особини популяції f_{avr} та середнім часом роботи алгоритму t_{sd}. Їх типову поведінку приведено на рис.2 (точне значення рівне 28857).

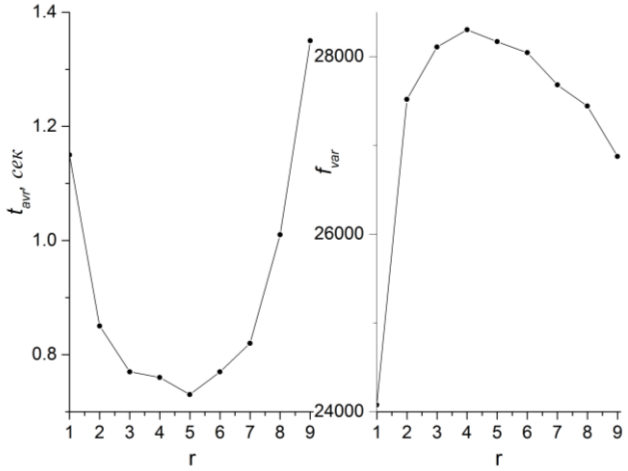


Рисунок 2. Середній час роботи $\mathbf{t_{avr}}$ та середня пристосованість найкращої особини популяції $\mathbf{f_{avr}}$ в залежності від розміру квантового регістру **r**.

Висновки. Перехід в QGA до квантових регістрів вищих порядків ілюструє хорошу можливість глобального пошуку завдяки використанню процедури відновлення квантової хромосоми та оператора квантового вимірювання. Швидка локальна збіжність забезпечується адаптованим алгоритмом роботи оператора квантового гейту, який для своєї реалізації не вимагає використання таблиці пошуку. Проведені моделювання дозволяють за співвідношенням ефективність/продуктивність вважати за оптимальний розмір квантового регістру порядку 3-6 кубітів.

Список літератури

1. Han K.–H., Kim J.–H. Genetic quantum algorithm and its application to combinatorial optimization problem // Proc.Congress on Evolutionary Computation. – Vol. 2, La Jolla, CA, July 2000. – P. 1354-1360.

2. Narayanan A., Moore M. Quantum-inspired genetic algorithms // Proceedings of the IEEE International Conference on EvolutionaryComputation (ICEC'96), Nagoya, Japan. – 1996. – P. 61–66.

3. Nowotniak R., Kucharski J. Higher-Order Quantum-Inspired Genetic Algorithms // Federated Conference on Annals of Computer Science and Information Systems. – 2014. – P.465-470.

УДК 004.023

Рекомендація існуючих методів вирішення задач у програмному продукті

Шнепов О.С., аспірант
Науковий керівник – Семенов С.Г., д.т.н., професор
Харківський національний університет радіоелектроніки, м. Харків

Задача: рекомендувати існуючі механізми вирішення проблеми у програмному продукті, розробленому на мові програмування Java, на основі короткого опису, виконаного на англійській мові.

Рекомендаційна система – підклас системи фільтрації інформації, яка будує рейтинговий перелік об'єктів, яким користувач може надати перевагу [1]. До стандартних видів рекомендаційних систем відносять:

- фільтрація на основі контенту;
- колаборативна фільтрація.

Перший вид підходить краще для даної задачі, так як не потребує знань про пошук на основі інших описів задач.

Представимо опис нашої задачі як "мішок слів" [2], однак додаймо сюди не тільки слова з опису, а й усі синоніми до слів з опису. Синоніми будемо добирати програмно, використовуючи, на приклад, Thesaurus [3]. Далі кожний метод, кожного класу [4], нашого програмного продукту, теж представимо у вигляді "мішка слів", використовуючи при цьому слова з назви класу та методу, знову також візьмемо всі синоніми. Після чого, порівняємо опис нашої задачі з усіма описами існуючих методів. Будемо вважати, що метод буде тим більш підходящім, чім у його "мішку слів" є більше слів з "мішка" опису нової задачі.

Таким чином, ми знайдемо кількісну характеристику схожості кожного методу до опису нової задачі. На основі чого, ми зможемо рекомендувати, наприклад, 10 найбільш схожих методів вирішення поставленої задачі нашому користувачу.

Як правило, програмні продукти, розроблені на мові програмування Java, складаються з великої кількості Java методів, тому представлений вище пошук може бути доволі повільним. Однак, цю ситуацію можна значно покращити, якщо при реалізації, по-перше: робити перед підготовку, яка буде включати у себе створення "мішків слів" для кожного Java методу та збереження їх на диск у зручному форматі і по друге: виконувати пошук у декілька потоків, кількість потоків слід обирати виходячи з розміру програмного продукту.

Діаграма описаної системи представлена на рисунку 1.

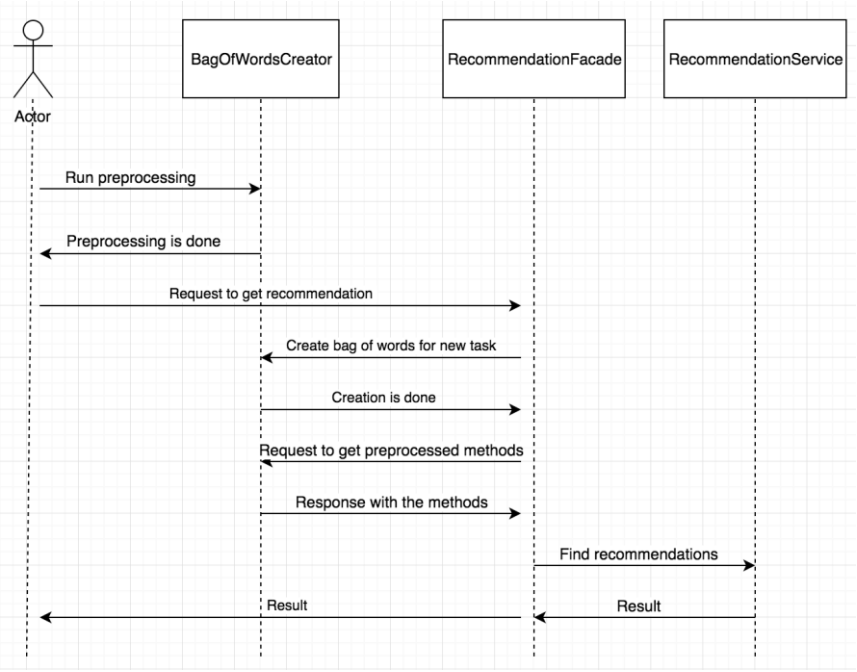


Рисунок 1 – Діаграмма системи рекомендацій

Після реалізації, вище описану систему можна буде додати до існуючих інтегрованих систем розробки, таких як IntelliJ IDEA [5] чи Eclipse [6], у вигляді плагинів.

Список літератури

1. Рекомендаційна система [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Рекомендательная_система
2. Bag-of-words model [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Bag-of-words_model
3. Thesaurus [Електронний ресурс]. – Режим доступу: http://www.thesaurus.com/browse/java
4. Java methods [Електронний ресурс]. – Режим доступу: https://www.tutorialspoint.com/java/java_methods.htm
5. IntelliJ IDEA [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/IntelliJ_IDEA
6. Eclipse [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Eclipse_(среда_разработки)

Активну участь в організації III Міжнародної науково-практичної конференції "Інформаційна безпека та комп'ютерні технології" приймає студентський науковий гурток «New Horizons» кафедри кібребезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

Фото учасників гуртка. Фотографувала Анастасія Абашина

Науковий керівник гуртка – Мелешко Єлизавета Владиславівна, канд. техн. наук, доцент, доцент кафедри кібербезпеки та програмного забезпечення;

Голова гуртка – Хох Віталій Дмитрович, аспірант кафедри кібербезпеки та програмного забезпечення;

Староста гуртка – Константинова Аліна Андріївна, студентка кафедри кібербезпеки та програмного забезпечення.

Члени гуртка бажають учасникам конференції натхнення та успіхів у їхніх наукових дослідженнях!

New Horizons Club

НАУКОВЕ ВИДАННЯ

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

III МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

“ІНФОРМАЦІЙНА БЕЗПЕКА ТА
КОМП’ЮТЕРНІ ТЕХНОЛОГІЇ”

INFOSEC & COMPTECH

19-20 квітня 2018 року

Тези доповідей надруковано в авторській редакції.
Відповідальність за зміст несуть автори.

Відповідальна за випуск: Мелешко Є.В.

Підписано до друку 16.04.2018
Тираж 50 прим.

©Кафедра кібербезпеки та програмного забезпечення ЦНТУ,
м.Кропивницький, пр.Університетський, 8.
Тел. (0522) 39-04-49
