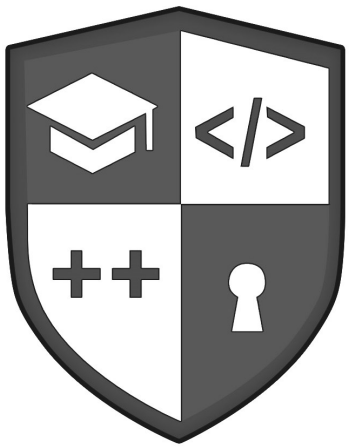
Міністерство освіти і науки України
Державна наукова установа “Інститут модернізації змісту освіти”
Центральноукраїнський національний технічний університет

Комп’ютерна інженерія і кібербезпека: досягнення та інновації

Матеріали ІІ Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених

м. Кропивницький, 25–27 листопада 2020 р.



Кропивницький ЦНТУ 2020

УДК 004
ББК 32.97
К63

К63 **Комп'ютерна інженерія і кібербезпека : досягнення та інновації** : матеріали II Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених, м. Кропивницький, 25–27 листоп. 2020 р. / М–во освіти і науки України, Держ. наук. установа "Інститут модернізації змісту освіти", Центральноукр. нац. техн. ун–т ; [відп. за вип. О. П. Доренський]. — Кропивницький: ЦНТУ, 2020. — 147 с.

Збірник містить тези доповідей учасників II Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених "Комп'ютерна інженерія і кібербезпека: досягнення та інновації", яка відбулася 25–27 листопада 2020 року в онлайновому форматі на базі Центральноукраїнського національного технічного університету, місто Кропивницький. Праці учасників конференції присв'ячені актуальним питанням інформаційних систем і технологій, інженерії програмного забезпечення, комп'ютерних систем штучного інтелекту, мережних IT, інформаційної безпеки національного сегмента кіберпростору, боротьби з кіберзлочинністю, захисту програм та даних в комп'ютерних системах і мережах.

Видання призначене для здобувачів вищої освіти за IT-спеціальностями у ЗВО України, науковців, викладачів, фахівців галузі інформаційних технологій, а також буде корисним всім, хто цікавиться сучасними досягненнями та інноваціями у сферах комп'ютерної інженерії й кібернетичної безпеки.

УДК 004
ББК 32.97
К63

Рекомендовано до друку Науково-технічною радою Центральноукраїнського національного технічного університету (протокол № 10 від 24 листопада 2020 р.)

Відповідальний за випуск: канд. техн. наук Доренський О. П.

Тексти матеріалів, тез доповідей друкуються у авторській редакції, мовою оригіналу. За достовірність наведених у публікаціях даних, назв, імен, цитат та іншої інформації відповідальність несуть автори.

Адреса організаційного комітету конференції
Центральноукраїнський національний технічний університет
Кафедра кібербезпеки та програмного забезпечення
просп. Університетський, 8, м. Кропивницький, 25006
(0522) 55-10-49, 39-04-49; cntu-conference@ukr.net; www.kntu.kr.ua

ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

КОМП'ЮТЕРНІ СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ

МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ІНФОРМАЦІЙНА БЕЗПЕКА НАЦІОНАЛЬНОГО СЕГМЕНТА КІБЕРПРОСТОРУ ТА БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ

ЗАХИСТ ПРОГРАМ ТА ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

UDC 004.432

A. Hafiiak[1], A. Chepurko[2]
[1]*National University «Yuri Kondratyuk Poltava Polytechnic»*
[2]*Scientific lyceum №3 of Poltava city council*

Information asset protection technologies

The direction that is experiencing rapid development is artificial intelligence (AI). So artificial intelligence in security, artificial intelligence security and protection against artificial intelligence will come to the fore. Security "y" is the beginning of a new era of cybersecurity tools, the need for which is already urgent, as hackers are already using artificial intelligence today. The security of AI itself is the need to formalize the cybersecurity approach in the development and use of artificial intelligence modules and tools. And protection from "is" the need for regulatory work to create rules of conduct and attitudes to artificial intelligence. This is already necessary in order to protect humanity from ethical or technical problems in the future[1].

Artificial intelligence is one of the newest sciences that appeared in the second half of the 20th century on the basis of computer science, mathematical logic, programming, psychologists, linguistics, neurophysiology and other fields of knowledge. The task of scientists was to build a computer that works in such a way that the results of his work would be impossible to distinguish its activities from the activities of the human mind. Artificial Intelligence is now considered as an applied field of research related to the simulation of certain functions of human intelligence. Pattern recognition, machine translation, intelligent agents, robotics - these are just some of the areas in which artificial intelligence systems are developing. It turned out that to create machines that mimic the work of the human brain, you need to understand how billions of its interconnected neurons work. The concept of "artificial intelligence" has a different meaning - from the recognition of intelligence in computer technology, solving logical or even any computational problems, to the classification of intelligent only those systems that solve the whole set of tasks performed by man, or even more a wide range of them[2].

Humanoid robots, helicopters, which act independently, analyzing information about the environment with the help of sensors (motion, sound, light, pressure, etc.) and make decisions based on the obtained data. One of the capabilities of robots is computer vision - an artificial intelligence technology for collecting, processing and analyzing video information in real time. All this requires the development of algorithms for automatic visual perception, correct movement in space, learning from mistakes, performing actions aimed at achieving the goal. An example is an unmanned vehicle that is programmed to reach its destination, can park, move in the flow of cars, correctly determine the shortest route. Writing bots, chatbots, strategy games, where the computer can calculate a large number of possible options for the game and choose the best. Heuristic algorithms of game artificial intelligence are used in a wide variety in many areas within the game.

The most obvious use of game AI is in controlling non-game characters, although scripting is also a very common method of control. Finding a way is another common application of game AI - it is especially evident in real-time strategies. Finding a way is a method for determining how a non-game character can move from one point on the map to another: you need to take into account the landscape, obstacles and, perhaps, the "fog of war". Game AI is also associated with dynamic game balancing.

Web analysis of data of social network users to determine the needs and interests, which can then be used to promote advertising intended for a narrow specialized group of users in targeted products. Generation on the basis of the collected data of selections of films, products, etc. according to interests of the user. Development of algorithms for analyzing texts, posts on social networks and determining whether the information provided in the profile is true; development of software for photo analysis, video of the user and determination of his emotions. Such data can be used in the fight against terrorism, the search for criminals and more.

Note an important point concerning the fact that, the use of artificial intelligence for pattern recognition will allow to create practical systems for identifying graphic objects on the basis of similar features. Any characteristics of the objects to be recognized can be considered as features. Signs should be invariant to the orientation, size and shape of objects. One of the tasks of SSI is to segment objects in images and identify people from the stream. An example of artificial intelligence is also sound typing and handwriting in mobile phones, as well as determining the location of the house captured on a mobile phone camera (online guide) and drawing its internal structure in 3D [3, 4].

Two directions of AI development are viewed: the first is to solve the problems associated with the approximation of specialized AI systems to human capabilities and their integration, which is realized by human nature; the second is the creation of an Artificial Mind, which represents the integration of already established AI systems into a single system capable of solving the problems of mankind [1, 2, 4].

It should be emphasized that, artificial intelligence on the lookout for data security: innovative technologies and cloud services help ensure cybersecurity. Despite all the obvious fears about cyberattacks and the ever-growing ingenuity of hackers to undermine the integrity of companies' databases, many of them simply cannot afford the integrated implementation of AI technologies to combat such cases. At the same time, according to Capgemini, almost two-thirds of those organizations that have already implemented such technologies are convinced that AI has not only solved their problems in this regard, but even reduced the total cost and resource cost of detecting and responding to violations security. At the same time, three quarters of respondents stressed that AI has reduced the response time to any risk situation, and therefore is an extremely profitable and necessary tool. The developers of intelligent security systems themselves claim that intelligent algorithms will not only increase the accuracy of detecting violations and speed up this process, but also directly detect the violators themselves. According to experts, because cybersecurity analysts are overwhelmed and do not always have a quick response to information about the incoming problem, it will soon be even more difficult to successfully counter the threat due to the scale of technology, and therefore the introduction and use of artificial intelligence have to think today.

References

1. *Cybersecurity in 2019: what are we waiting for and what awaits us? https://10guards.com/ua/articles/cybersecurity-trends-2019/.*
2. *"Computer systems of artificial intelligence" syllabus.pdf* https://www.wunu.edu.ua/opp/fkit/komputerna_inzheneriya/komputerna_inzheneriya_bakalavr/kompjuterni_systemy_shtuchnogo_intelektu/syllabus.pdf.
3. *What is an artificial intelligence system* http://ai.lviv.ua/ais/.
4. *Artificial intelligence* https://uk.wikipedia.org/wiki/%D0%A8%D1%82%D1%83%D 1%87%D0%BD%D0%B8%D0%B9_%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0% B5%D0%BA%D1%82.
5. *Artificial intelligence on guard of data security: innovative technologies and cloud services help to ensure cybersecurity* https://cacds.org.ua/?p=7448.

UDC 004.93:006.9

M.V. Mihajluk[1], T.V. Ponomarenko[2]
[1]*M.A. Student, National university of shipbuilding named by admiral Makarov*
[2]Associate professor, *National university of shipbuilding named by admiral Makarov*

Improvement of a verification model for the information-measuring system with limited resources

Relevance. The problem of verification of systems with limited resources is considered. The key point in the development of minicomputer systems is their limited system resources, which leads to stricter requirements for the final products based on them. Accordingly, this limits their scope of application in critical real-time systems such as the defense industry or medical applications. Therefore, the development of verification tools for minicomputer systems to confirm their stable functioning is an urgent task.

The object of the research is the process of modeling the functioning of reconfigurable systems with limited resources. The aim of the work is to improve the reliability of the functioning of systems with limited resources with reconfigurable components by ensuring data integrity and automating the verification process.

Method. A verification model for systems with limited resources is obtained, based on the verification model of web-oriented systems, which allows describing the components of verified objects and a method of data exchange based on a dynamic data transfer model. The concept of "functional unit" has been modified by adding not only software, but also hardware blocks, which makes it possible to automate testing of these elements. The peculiarity of this model is that it takes into account the results of verification of devices connected to minicomputer systems and describes the optimal log period for reading archive files, which allows ensuring the relevance and integrity of test results for systems with limited resources. The architecture of a minicomputer system based on the Raspberry Pi was considered as an experimental model.

To verify systems with a web interface, we took the verification model for web-oriented systems [9], which was built on the basis of the next concept:

$$MV = (interprototype, E_d, E_h DB, rmv),$$

$$rmv: iterprototype \rightarrow E_d \times DB \vee \forall e_a, e_a \in rp(a), rm(a), e_a \rightarrow e, e = \{e_d\}.$$ MV = (interprototype, E, DB, rmv), rmv: interprototype → Ed × DB|∀ea, ea ∈ {rp (a), rm (a)}, ea → e,e = {ed}.

To define the object of testing in the verification model of web-oriented systems, the ed element is highlighted - a resource or document available over the network and identified by a unique URI:

$$rd: C_A \rightarrow E_d | \forall c \in C_a: e_d = rd(c), e_d \cup E_d$$

For verification, the concept of a "functional unit of a system" f - an elementary structural component of the information system, realizing a complete functional block for checks which can be developed by one or more automated or automated validation tests:

$$F = (E_d, P, r) | \forall e_d, e_d \in E_d, \exists p, p \in P$$

The peculiarity of modern embedded systems is that the system architecture also becomes adaptive, for which we define that the set explicit UP (u) and implicit UM (u) user requirements includes not only many prototype elements interface, but also many requirements for the hardware elements. We will accept a lot of resources for E, the set of adaptive hardware elements is denoted by Eh then for adaptive inline of the system we will assume E = Ed ∪ Eh, e ∈ E. Considering advantages, the model for verifying systems with limited resources *MV* will take the form:

$$MV = (interprototype, E_d, E_h DB, rmv, Y, n), rmv: \rightarrow E_d \times E_h \times DB \vee \forall e_a, e_a \in rp(a), rm(a), e_a \rightarrow e, e = \{e_d\}.$$

Conclusions. The paper proposes a modified verification model for systems with limited resources, which, in contrast to the verification model of web-based systems, describes the adaptive architecture of embedded systems and contains a period for transferring verification results to external storage, which allows this model to be applied to various hardware configurations.

UDC 347.1

K. E. Radoutskiy[1], O. V. Turuta[2], A. K. Radoutska[3]
[1]*Senior lecturer, V. N. Karazin Kharkiv National University*
[2]*Ph.D, Associate Professor, Kharkiv National University of Radio Electronics*
[3]*Student, Kharkiv National University of Radio Electronics*

Using of free licenses in information technology

Modern society is constantly evolving, and the established canons are replaced by new progressive ideas that correspond to the realities of the modern world. In the digital age, we have access to data and ability to dispose of it from anywhere on the planet. But the Internet and information technology have not only made it easier for us to find and distribute content, but have also brought about changes in the field of copyright. One of the most interesting and advanced ideas was the emergence of the institution of free licenses. Their importance is difficult to overestimate because they give society many benefits. They contribute to the rapid development of information technology, save developers time, as there is no need to invent an existing object, but user can improve and refine it legally, and facilitate the management of copyrighted material.

Free licensing is carried out on the initiative of the author of the creative activity, and he is the one who determines the amount of rights he wishes to grant. The right holder himself chooses a greater or smaller amount of rights to provide for an indefinite number of potential users. Also, licenses are based on copyright and, therefore, guarantee the creator compliance with copyright. Each license operates worldwide and is valid for as long as the copyright, and also guarantees the attribution of the works.

Today, there are two most common types of free licenses, which are used in information technology - Creative Commons and GNU.

Creative Commons, abbreviated CC - a non-profit organization that has created to use standard contracts. Depending on the scope of rights granted under their license, they can be divided as free and unfree. Free licenses include: Attribution (by) - license with indication of authorship and Attribution-ShareAlike (by-sa) - license with indication of authorship - with preservation of conditions. All other licenses are non-free, they impose more restrictions on users. These types of licenses are based on 4 main conditions. Depending on the list of these conditions in the license, the user is granted a certain set of rights.

All Creative Commons licenses have common features. First, all licenses are non-exclusive, for example, the author may enter into agreements with Creative Commons licenses and may also enter into an exclusive agreement with another person. Second, the licensor enters into an agreement with each individual. Third, Creative Commons is not a party to the agreement and will not reimburse the parties for any damages incurred in connection with the conclusion of a free license. And, in addition, the indication of the author of the work is mandatory for all licenses.

The next most common type of license in the world is the GNU Free Software License. According to the GNU Manifesto, the organization's main goal is developing so much software as possible to do without programs that are not free. For programs, which are distributed under such licenses, a certain list of mandatory conditions is presented. From them it becomes clear that further distribution of the program is possible only under the conditions under which the software was originally provided to the user. He can neither expand nor narrow the scope of these rights. Even if you use a piece of product under a GNU license when creating new software, you must provide the entire new program under that license.

Thus, free licenses - a type of license agreement under which the right holder gives an indefinite number of persons the right to use, distribute, modify works on the terms specified in the agreement with a mandatory indication of its authorship. The essential conditions of the license are the conditions on the subject and type of permitted use. The indication of the territory and the term are not significant. Licenses are valid worldwide and are valid for the duration of copyright protection. These licenses can be both paid and free. The creation of the concept of a free license has greatly facilitated the use of copyrighted materials and copyright in general to information technology. In general, the emergence of the concept of free licenses was due to the fact that copying digital content is virtually inexpensive, and the "old" copyright was not able to protect creators in the digital age.

UDC 004.93:005

A. O. Tarasova
M.S. student, National university of shipbuilding named by admiral Makarov

Model of the load balancing of the information-measuring systems by means of use of genetic algorithm

Balancing communication channels has become an essential component of for constructing and optimizing the load on the components of information-measuring systems assembled both on the basis of several Raspberry Pi 3 and similar microprocessor-based measuring systems. In modern networks, there is a need for a solution optimization of data transmission (traffic) by many criteria. Classic algorithms are not applicable to problems of this type, belonging to the class of NP-hard. The need arises to form new approaches and algorithms for balancing the load on communication channels in the network.

In the load balancing problem, the system components are represented as a weighted directed graph $G = (V, E, C)$, where V is the set of vertices, $E \in V \times V$ is the set of graph edges, $C_{i,j} : E \rightarrow R$ - bandwidth of each connections (graph edges). Information about the flow between each pair of vertices is given by function Fi, j, where i is the original vertex, j is top destination. The proposed algorithm can be applied to a separate part of the networks. In this case, a specific subgraph of graph G is used.

Genetic load balancing algorithm uses a network routing table containing $m_{i,j}$ alternative paths between each pair of vertices (i, j). This table stores all intermediate vertices of the path $(i\ j)$, as well as the weight of each route based on the routing algorithm. This approach allows applying the genetic algorithm in information measuring systems using routes(connection) between two vertices (system parts) with different metrics and distance.

During network operation, each route between vertices i and j is used with a certain probability $\alpha_k\ (i,\ j)$ and $\sum_k (\alpha_k(i,j) = 1, k = 1 \dots m_{i,j}$. The bandwidth utilization of a particular connection can be calculated as follows:

$$P(l,m)^n = \sum_k \sum_{i,j \in V} X_{l,m}{}^k(i,j)\alpha_k(i,j)F_{i,j}/C_{l,m},$$

where $X_{l,m}{}^k(i,j) = \begin{cases} 1, & if\ (l,m) \in (i \rightarrow j) \\ 0, & if\ (l,m) \notin (i \rightarrow j) \end{cases}$.

Let $P_{max} = \max_{(l,m) \in E} (P(l,m))$, then the task of load balancing is reduced to minimizing the maximum consumption of the data transmission channel on the network, so to search for such a configuration of data transmission routes for which P_{max} will be minimal: $\Phi = \min_{(l,m) \in E} (P_{max})$.

*Genetic algorithm.*The chromosome of a certain generation of the genetic algorithm Y consists of a sequence of alleles $A_{i,\ j}$, which contain sets of coefficients $\alpha_k(i,j)$ for each pair of vertices $(i,j) \in V'$, so

$A_{i,j} = \{\alpha_k(i,j)\}$.

*Initial population.*The formation of the initial population of chromosomes depends on the selected routing algorithm. When multiple routing algorithms are used, this value depends on the route metric and the administrative distance of the routing protocol. The coefficients of the initial population of the genetic algorithm are chosen as follows:

$$\alpha_k(i,j) = \frac{q_{i,j}{}^k}{\sum_k q_{i,j}{}^k} \ and\ V' \subset V.$$

Mutation and crossover. The mutation operation for the proposed algorithm consists in randomly changing a certain allele of the chromosome $A_{i,j}$ (single-point mutation) or changing several alleles of the chromosome at the same time (multipoint mutation). Let within the current generation the largest channel consumption is observed for the channel $(l,m) \in E^t$. Only alleys $A_{i,j}$ for which •k∈ $(1 \ldots m_{i,j}) and\ \alpha_k(i,j) \neq 0, X_{l,m}{}^k(i,j) = 1.$

Selection. Since equality (3) corresponds to the problem of the minimum search, fitness function of the chromosome Y can be calculated as:

$$F(Y) = (\max_{(l,m)\in E}(P(l,m)))^{-1}$$

The algorithm uses a proportional selection method in combination with the method of preserving the best individuals in the population (elitism). This means that the probability of selecting a certain chromosome is proportional to the value of the fitness function of this chromosome. Let the population size N, and the value of the fitness function of the chromosome Y_i, be equal to $F(Y_i,)$, then the probability of selection Y_i, is calculated as follows $p_i{}^k = F(Y_i)(\sum_k F(Y_i))^{-1}$, where

$$p_c = \begin{cases} p_1(P_{max} - F(Y_i)/(P_{max} - F(Y_i), F(Y_i) \geq Fav \\ p_2, \quad F(Y_i) < Fav, \end{cases}$$

$$p_m = \begin{cases} p_3(P_{max} - F(Y_i)/(P_{max} - F(Y_i), F(Y_i) \geq Fav \\ p_4, \quad F(Y_i) < Fav, \end{cases},$$

where P_{max} is the value of the fitness function of the best chromosome in the population, F is the average value of the fitness function of chromosomes in the population 0 <p1, p2, p3, p4 < 1.

Routing. After the genetic load balancing algorithm is completed, its results should be used in the network routing process. Since the balancing algorithm is based on information about all intermediate nodes of the routes, the classical format of the routing table and algorithm should be extended.

the rhythm of routing in general. Consider the routing table at the intermediate node k. In the proposed approach, each table entry corresponding to a route (*i* - *j*) that passes through vertex k additionally contains information about the initial vertex i. If there are several alternative paths between vertices i and j, then the record also contains the probability of choosing a certain route.

Let there be *m* paths (i - j) passing through the vertex k, then the probability of choosing a certain route is defined as follows

$$\beta_s(i,j) = \frac{\alpha_s(i,j)}{\sum_k \alpha_s(i,j)}, s = 1 \ldots m.$$

Conclusion. The described approach is applicable for constructing and optimizing the load on the components of information-measuring systems assembled both on the basis of several Raspberry Pi 3 and similar microprocessor-based measuring systems. Its implementation will make it possible to use resources more efficiently and significantly improve the dynamic characteristics of load balancing systems in information and measurement systems.

Supervisor — Candidate of Technical Sciences, Associate Professor, Ponomarenko Tetyana Viktorivna, Associate Professor of the Department of Automated Systems Software of the Admiral Makarov National University of Shipbuilding.

УДК 004.73:005.8

О. В. Борисов[1], О. І. Маршак[2], О. С. Бобровський[3]
[1]*здобувач вищої освіти другого (магістерського) рівня*
[2]*завідувач відділення інформаційних технологій*
[3]*фахівець центру інформаційних технологій*
[1,3]*Національний університет кораблебудування імені адмірала Макарова*
[2]*Відокремлений структурний підрозділ «Фаховий коледж корабелів Національного університету кораблебудування імені адмірала Макарова»*

Розробка організаційно-функціональної структури підсистеми «Абітурієнт» сайту закладу освіти

Вступна частина. Здобування фахової освіти є важливим кроком у житті кожної людини. Прагнення до цього повинно враховуватися при побудові рекламної кампанії навчальних закладів, де головним інструментарієм є використання сайтів.

Відокремлений структурний підрозділ «Фаховий коледж корабелів Національного університету кораблебудування імені адмірала Макарова» (далі «Коледжу») створено Наказом № 157 від 05.02.2013 р. МОН України як окремий підрозділ Національного університету кораблебудування імені адмірала Макарова, який включатиме у себе відділення морської техніки, енергетики і електричних систем, інформаційних технологій, економіки і менеджменту, екологічної безпеки. Відділення інформаційних технологій здійснює підготовку молодших спеціалістів за спеціальністю 122 – Комп'ютерні науки, які працюють на посадах техніка-програміста, техніка інформаційно-обчислювального центра, операторів комп'ютерного набору та верстання та продовжують навчання за кваліфікаційним рівнем бакалавр на кафедрі інформаційних управляючих систем і технологій. Тому створення сайту Коледжу є важливою науково-практичною задачею, вирішення якої вимагатиме створення спеціалізованої підсистеми «Абітурієнт», використання якої спрямовано на спрощення пошуку інформації про Коледж та підвищення кількості бажаючих до вступу.

Метою роботи є розробка організаційно-функціональної структури підсистеми «Абітурієнт» для створення сайту Відокремленого структурного підрозділу «Фаховий коледж корабелів Національного університету кораблебудування імені адмірала Макарова».

Основна частина. Призначенням підсистеми «Абітурієнт» є групування різних сутностей сайту в єдиному місці для зручного та швидкого доступу до неї. У подальшому ця підсистема має бути інтегрована з вже існуючою інформаційною системою сайту Коледжа. Головні вимоги до проектування підсистеми наведено у таблиці 1. Організаційно-функціональну структуру підсистеми «Абітурієнт» наведено на рисунку 1.2. Основними компонентами підсистеми «Абітурієнт» є: СУБД, серверна платформа і серверне програмне забезпечення; клієнтська платформа і клієнтське програмне забезпечення; мережеве середовище; засоби розробки. Робота менеджерів або адміністратора з підсистемою «Абітурієнт» інформаційної системи сайту Коледжа полягає під собою спільну роботу менеджерів, комп'ютери яких знаходяться в єдиній мережі. Для передачі даних по мережі використовується протокол TCP/IP. Програмне забезпечення підсистеми «Абітурієнт» інформаційної системи сайту Відокремленого структурного підрозділу «Фаховий коледж корабелів Національного університету кораблебудування імені адмірала Макарова» передбачає використання одного серверу та декількох клієнтських машин.

Таблиця 1 – Головні вимоги до проєктування підсистеми «Абітурієнт»

Вимоги	Формулювання вимог
до підсистеми	- відповідність режиму роботи сайту; - можливість розвитку і модернізації компонентів системи; - зберігання цільового призначення системи
до функцій	- аутентифікація та ідентифікація користувача; - конфіденційність передачі даних; - додавання та редагування інформації; - пошук інформації; - подальша інтеграція з інформаційною системою сайту коледжу
до інформаційного забезпечення	- відкритість, мобільність, інтероперабельність; - підтримка розподіленої багаторівневої архітектури; - забезпечення захисту даних; - робоче середовище – система 1С-Bitrix: Управление сайтом
до документації	1. загальний опис системи; 2. керівництво користувача; 3. інструкція з формування і ведення бази даних; 4. керівництво адміністратора з установки програмного забезпечення на серверах; 5. програма і методика тестування

Рисунок 1 – Організаційно-функціональна структура підсистеми «Абітурієнт»

Висновок. За результатами аналізу вимог до проєктування та реалізації розроблено організаційно-функціональну структуру підсистеми «Абітурієнт» для створення сайту Відокремленого структурного підрозділу «Фаховий коледж корабелів Національного університету кораблебудування імені адмірала Макарова». Перспективи подальших досліджень пов’язані з моделюванням процесу онлайн-спілкування абітурієнт–адміністратор, що сприятиме підвищенню якості вступної кампанії.

Науковий керівник — доктор технічних наук, професор Казимиренко Ю. О., професор кафедри інформаційних управляючих систем та технологій Національного університету кораблебудування імені адмірала Макарова.

УДК 004:056

Д. О. Вакуленко
студентка, Центральноукраїнський національний технічний університет

IoT-платформи як засіб полегшення обробки інофрмації для контролю за якістю врожаю в господарствах

Сьогодні в усіх сферах нашого життя присутні інформаційні технології, сільське господарство не є винятком. За останні 5 років покоління технологічних рішень в аграрній сфері змінюється дуже швидко:нещодавно для того, щоб зробити хімічний аналіз грунту потрібно було відбирати по декілька проб і везти їх в лабораторію, пізніше можна просто купити портативний пристрій і відбирати проби прямо в полі. Зараз це ще простіше та швидше, на штанзі сільськогосподарської техніки встановлюють спеціальні датчики, котрі аналізують стан та потребу грунту в тих чи інших елементах.

Кожен аграрій хоче отримувати максимальні прибутки від врожаїв з мінімальними втратами. Для того, щоб досягти такої мети необхідно обробляти та аналізувати великий об’єм даних [3].

Для спрощення процесу обробки інформації в АПК почали впроваджувати діджитал- проєкти із застосуванням Інтернету речей чи IoT.

Тож, що таке IoT і навіщо чого використовують в сільському господарстві? IoT з англійської дослівно означає Internet of Things чи Інтернет речей (датчики, контролери та інше), які обмінюються даними між собою без втручання людини. На основі цих даних програмне забезпечення формує зрозумілі звіти для аграріїв.

Дані від IoT-платформи легко інтегруються з 1С, ERP, CRM системами, із Microsoft Power BI, завдяки чому менеджмент і власник бачать повну та чітку картину діяльності агропідприємства: від розрахунків собівартості сушіння зерна на елеваторі, виходячи з фактичної вологості, зафіксованої датчиком, до нарахування заробітної платні за фактично оброблені гектари.

Складові елементи IoT-платформи [1]:

1. Електронні мапи полів;
2. Датчики на техніці: GPS-трекери, лічильники насіння і добрив, датчики заповнення бункера комбайна;
3. Датчики рівня пального та проточні витратоміри;
4. Ультразвукові сканери (глибина оранки поля, наповнення кузова зерновоза, аналіз мікроелементів у ґрунті, ін.);
5. Електронні вагові контроллери на елеваторі, вологоміри на елеваторі;
6. Електронні АЗС;
7. RFID картки та зчитувачі: автоматична ідентифікація водія і МС;
8. BLE-мітки причіпного обладнання;
9. Система “свій-чужий” для комбайна та зерновоза;
10. Погодні станції;
11. Дрони, супутники.

Така платформа буде корисною для тих фермерів, які користуються послугами айманих комбайнерів та трактористів, зерновозів. Першим етап ото контролю є встановлення датчиків наповнення на бункер комбайна.

На другому етапі, щоб із власного комбайна збіжжя не було відвантажено в чужий зерновоз, необхідно встановити електричні мітки на техніку.

Далі аграрію для контролю маршруту від поля до елеватора, програмне забезпечення автоматично інформує про порушення або негаразди під час транспортування.

На останньому, четвертому етапі, виконується зважування зібраного врожаю. Це вирішується шляхом встановлення на елеваторах і вагових, послугами яких користується агропідприємство, незалежного вагового контролера на комп'ютер ваговика, а також встановлення власного вологоміра, що приєднаний до програмного забезпечення.

Завдання, які вирішує IoT в аграрній сфері:

– автоматичний розрахунок оброблюваної площі поля в розрізі технологічних операцій і для нарахування зарплати;

– автоматична ідентифікація водія;

– автоматизований контроль видачі пального з ідентифікацією водія і транспортного засобу, зливи ПММ;

– маршрути, автоматичні повідомлення про порушення, фото- та відеофіксація;

– облік насіння, добрив і ЗЗР. Загальні витрати підприємства на полі та на гектар;

– загальні витрати пального на господарство в розрізі типів польових робіт;

– контроль і облік видачі пального з АЗС, контроль наявності МС під час заправки;

– заправки/зливи пального, витрата пального на 1 гектар обробленої площі, контроль рівня пального у баці;

– ідентифікація ТЗ під час вивантаження з комбайна (BLE і RFID-мітки), контроль наявності ТЗ під час вивантаження, контроль роботи шнека, намолот у розрізі комбайнів;

– урожайність, валовий збір, карта врожайності поля;

– супутникові знімки полів, прогнозування врожайності, моніторинг полів дронами;

– аналітика розвитку культур – індекси стану рослин: EVI2, GRVI, VARI, NDVI, NDRE, ENDVI;

– дані від локальної метеостанції, температура та вологість ґрунту, кількість опадів за період, контроль погодних умов під час роботи обприскувачів;

– незалежний облік ваги на елеваторі, ідентифікація ТЗ на ваговій, вологість і вага зерна, що перевозять з поля, автоматичне визначення поля і культури.

Всі отриманні данні від IoT-платформи, обробляє програмне забезпечення та інтегрує в такі системи обліку як 1С, Microsoft Power BI [1,2].

На мій погляд, фермерів лякають такі причини, як не компетентність у користуванні ІТ та небажання навчатися цьому та невпевненість у доцільності запровадження ІТ в своєму господарстві. Але ж почекайте, зараз весь світ намагається долати проблеми за допомогою цифрових рішень, а витрати на програмне забезпечення в декілька разів менші, ніж втрати від розкрадання ЗЗР, насіння, добрив..

Список використаних джерел

1. *Що таке IoT-платформа чи Інтернет речей для аграрія? https://agroelita.info/2020/03/shho-take-iot-platforma-chy-internet-rechej-dlya-agrariya/*
2. *Тверезовська Н.Т., Нєлєпова А.В. Інформаційні технології в агрономії. Навчальний посібник. — К. : Центр учбової літ-ри, 2013. — 282 с.*
3. *Крачок Л.І. Новітні технології у сільському господарстві: проблеми і перспективи впровадження / Л.І. Крачок // Сталий розвиток економіки. – 2013. – Вип. 20. – С. 224-231.*

Науковий керівник — Доренська А. О., асистент кафедри економіки, менеджменту та комерційної діяльності Центральноукраїнського національного технічного університету.

УДК 004.4

А. А. Вітряченко
студентка, Центральноукраїнський національний технічний університет

Огляд методів прискорення пошукових запитів при роботі з базами даних

У сучасних веб-додатках, що взаємодіють з базами даних (БД), важливим моментом є швидкість обробки даних і виконання пошукових запитів. Часто час відгуку системи з великими обсягами даних на запити користувачів стає неприйнятним, якщо не приділяти увагу швидкості виконання запитів. Огляд існуючих методів підвищення ефективності виконання запитів буде необхідний і актуальний для розробників веб-додатків, що працюють з БД.

Існують декілька підходів до зменшення середнього часу виконання запитів на читання інформації БД:

- підхід, заснований на статистичному аналізі групи запитів на читання інформації й отримання оптимального набору індексів таблиць для мінімізації часу виконання запиту [1] [2];

- денормалізація БД - приведення структури БДбази даних в стан, що не відповідає критеріям нормалізації, з метою прискорення операцій читання з бази шляхом додавання надлишкових даних;

- секціонування даних - основний сенс полягає в фізичному розміщенні частин однієї таблиці по різних файлах, взаємодія з якими на рівні файлової системи та дискового масиву здійснюється паралельно [3];

- рефакторинг табличних структур, який ґрунтується на їх вертикальному розділенні [1].

Питання рефакторингу табличних структур і його доцільності піднімається досить часто, особливо для систем оперативної обробки транзакцій (OLTP). Але всі методики зводяться до рекомендацій для проектувальників БД та є умоглядними, чіткої методики розділення таблиці, що досліджується, на дочірні немає [1].

На швидкість пошуку інформації в БД впливають: обсяг блоку в байтах, обсяг файлу, кількість записів в блоці файлу, кількість записів в блоці індексу, кількість блоків у файлі, частка резервної частини блоку, число полів в запису, розмір запису в байтах.

Серед найпоширеніших методів, що підвищують ефективність виконання запитів - вивчення плану виконання запиту, індексування полів реляційних таблиць (РТ) і аналіз ступеня вибірковості індексів [2]. План запиту створюється в фазі оптимізації обробки даних компонентом ядра БД, що називають оптимізатором запитів. Він бере до уваги безліч різних чинників, намагається підібрати найбільш ефективний алгоритм обробки даних.

Правильно побудовані індекси можуть значно скоротити час обробки даних. Кластеризовані та некластеризовані індекси допомагають серверу БД знаходити результат значно швидше, використовуючи для цього різні варіанти збалансованих B-дерев і хеш-таблиць.

Рекомендується використовувати правило формування оптимальних систем, яке регламентує виставлення індексів на зовнішніх ключах табличних зв'язків. Саме по цих полях система здійснює пошук того або іншого запису в різних таблицях.

Слід враховувати, що індекси уповільнюють виконання команд DML (Data Manipulation Language). Багато СКБД блокують використання індексів, якщо: індексне поле використовується в виразах, що обчислюються, як операнд порівняння зі

значеннями неіндексованого поля, в операціях, які використовують порівняння з невизначеним значенням NULL, або є параметром вбудованих або призначених для користувача функцій.

Щодо питань організації індексів, у розробників різних СКБД є свої підходи [2]. Різні СКБД працюють з різними видами індексів.

Оптимізатори більшості СКБД відшукують коефіцієнт для обчислення селективності при першому зверненні до таблиці та зберігають його в пам'яті для використання при обчисленні планів у наступних запитах до цієї таблиці. Найбільш корисними для оптімізатора є критерії запиту за індексованими полями з високою вибірковістю. У загальному випадку, чим більше дублікатів в індексованому стовпці, тим гірше працює індекс.

Тип таблиці також відіграє велику роль у визначенні підсумкової швидкості роботи БД.

Технологія партіціювання (Partitioning) - це поділ збережених об'єктів баз даних на окремі логічні частини з роздільними параметрами фізичного зберігання. В [3] автори розглядають горизонтальне партіціювання (поділ таблиць по записах). Була розроблена система, що містить модуль заповнення БД за випадковим принципом з можливістю завдання виду секціонування, що використовується, а також модуль зчитування інформації з БД, який здійснює облік часу виконання запиту. Експерименти проводилися для декількох обсягів таблиць. Перший експеримент стосувався підрахунку часу виконання команди «Select». Другий експеримент - дослідження залежності швидкості виконання команди «Select» від частоти розбивки та підсумкової кількості отриманих підтаблиць - партіцій. Проаналізувавши результати експериментів автори [3] зробили висновок, що для партіціювання існує межа ефективності. Після досягнення певної кількості партіцій підвищення швидкості відгуку зупиняється, а потім ефективність розбиття стає негативною.

Завдання підвищення продуктивності великих інформаційних систем є особливо актуальним у зв'язку із загальною тенденцією до глобалізації та централізації у сфері інформаційних систем і технологій. Дослідження, що розглядались підтвердили доцільність використання технології секціонування для якісного зменшення часу виконання запитів до реляційних СКБД. Основні види індексів досить ефективні стосовно полів реляційних таблиць з унікальними значеннями, або з низькою щільністю значень. Планується продовжити експерименти з різними БД та різними СКБД з метою вивчення технології секціювання і застосування нових технологій в комбінації для підвищення швидкості відгуку.

Список використаних джерел

1. *Бельченко И.В., Методика повышения производительности крупних информационных систем за счет реструктуризации даннях на основе кластерного анализа статистики запросов // 2018 [Електронний ресурс] – Режим доступу: https://cyberleninka.ru/article/n/metodika-povysheniya-proizvoditelnosti-krupnyh-informatsionnyh-sistem-za-schet-restrukturizatsii-dannyh-na-osnove-klasternogo-analiza.*
2. *Носова Т.Н., Калугина О.Б., Использование алгоритма битовых шкал для увеличения эффективности поисковых запросов, обрабатывающих данные с низкой избирательностью // 2018 [Електронний ресурс] – Режим доступу: https://cyberleninka.ru/article/n/ispolzovanie-algoritma-bitovyh-shkal-dlya-uvelicheniya-effektivnosti-poiskovyh-zaprosov-obrabatyvayuschih-dannye-s-nizkoy.*
3. *Голиков О.И., Панкратов И.А., Исследование способов повышения эффективности обработки данных в реляционных БД на примере СУБД MySQL // 2016 [Електронний ресурс] – Режим доступу: https://cyberleninka.ru/article/n/issledovanie-sposobov-povysheniya-effektivnosti-obrabotki-dannyh-v-relyatsionnyh-bd-na-primere-subd-mysql.*

Науковий керівник — Константинова Л.В., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.42

Д. С. Горбенко
студент, Центральноукраїнський національний технічний університет

Особливості оцінювання надійності складних програмних засобів

Інтерес до оцінювання надійності програмного забезпечення виник одночасно з появою програм. Він був викликаний природнім прагненням одержати традиційну імовірнісну оцінку надійності технічного пристрою (ЕОМ), робота якого, в основному, і призначалась для функціонування программного забезпечення. Останнє було визначено, як одна зі складових частин машини, тому підхід до оцінювання надійності програмної частини спочатку мало відрізнявся від оцінювання надійності техніки і полягав у переносі відомих статистичних методів класичної теорії надійності на новий ґрунт, утворивши її окрему галузі – теорію надійності програмного забезпечення. У цілому цей підхід зберігся до теперішнього часу. Однак в міру розвитку обчислювальної техніки прийшло чітке розуміння того, що програмне забезпечення – не просто складова частина ЕОМ. У сучасних умовах розвитку цифрової техніки спеціальне програмне забезпечення перестало бути приналежністю однієї обчислювальної системи (як це було раніше), а стало використовуватися на сотнях і тисячах аналогічних ЕОМ (в основному – персональних). Навіть якщо не чіпати питань інформаційної безпеки, проблема забезпечення стійкого функціонування розрахункових програм, виявлення їх помилок сьогодні вкрай гостро стоїть перед розробниками.

При застосуванні понять надійності до програмних засобів (ПЗ) слід враховувати особливості і відмінності цих об'єктів від традиційних технічних систем, для яких спочатку розроблялася теорія надійності:

- не для всіх видів програм застосовні поняття і методи теорії надійності – їх можна використовувати тільки до ПЗ, що функціонують у реальному часі і безпосередньо взаємодіючим із зовнішнім середовищем;
- при розробці і оцінці якості програмних компонентів до них не застосовні поняття надійності функціонування, якщо при обробці інформації вони не використовують значення реального часу і не взаємодіють безпосередньо із зовнішнім середовищем;
- домінуючими факторами, що визначають надійність програм, є дефекти і помилки проектування та розробки, і другорядне значення має фізичне руйнування програмних компонентів при зовнішніх впливах;
- відносно рідке руйнування програмних компонентів і необхідність їх фізичної заміни, приводить до принципової зміни понять збою і відмови програм і до поділу їх по тривалості відновлення щодо деякого припустимого часу простою для функціонування інформаційної системи;
- для підвищення надійності комплексу програм особливе значення мають методи автоматичного скорочення тривалості відновлення і перетворення відмов у короткочасні збої, шляхом введення в програмні засоби тимчасової, програмної та інформаційної надмірності;
- непередбачуваність місця, часу й імовірності прояву дефектів і помилок, а також їх рідке виявлення при реальній експлуатації досить надійних програмних

засобів, не дозволяє ефективно використовувати традиційні методи апріорних розрахунків показників надійності складних систем, орієнтовані на стабільні, вимірювані значення надійності складових компонентів;

- традиційні методи форсованих випробувань надійності систем шляхом фізичного впливу на їхні компоненти не застосовні для програмних засобів і їх слід заміняти на методи форсованого впливу інформаційних потоків зовнішнього середовища.

З урахуванням перерахованих особливостей застосування основних понять теорії надійності складних систем до життєвого циклу й оцінці якості комплексів програм дозволяє адаптувати й розбудовувати цю теорію в напрямку надійності програмних засобів.

Тобто до завдань оцінювання надійності складних ПЗ можна віднести наступні:

- формулювання основних понять, використовуваних при дослідженні й застосуванні показників надійності ПЗ;

- виявлення й дослідження основних факторів, що визначають характеристики складних програмних комплексів;

- вибір і обґрунтування критеріїв надійності для комплексів програм різного типу й призначення;

- дослідження дефектів і помилок, динаміки їх зміни при налагодженні й супроводі, а також впливу на показники надійності ПЗ;

- дослідження методів і засобів контролю й захисту від викривлень програм, обчислювального процесу й даних шляхом використання різних видів надмірності й завадостійкості;

- розробка методів і засобів визначення й прогнозування характеристик надійності в життєвому циклі комплексів програм з обліком їх функціонального призначення, складності, структурної побудови й технології розробки.

Результати розв'язку цих завдань є основою для створення сучасних складних ПЗ із заданими показниками надійності.

Список використаних джерел

1. *Иыуду К.А. Надежность, контроль и диагностика вычислительных машин и систем / К.А. Иыуду. - М.: Высшая школа, 1989.*
2. *Карповский Е.А. Надежность программной продукции / Е.А. Карповский, С.А. Чижов. - К.:Техника,1990.*
3. *Самойленко А.П. Расчет надежности программно-аппаратных средств информационно-вычислительных комплексов / А.П. Самойленко. – Таганрог: ТРТИ, 1992.*
4. *Ятрик В.М. Структурное проектирование надежностных программ встроенных ЭВМ / В.М. Штрик, Л.Г. Осовецкий. – Л.: Машиностроение, 1994.*
5. *http://www.sgmu.ru/info/str/metod/files ... selfws.rtf*
6. *guap.ru/guap/kaf84old63/meth/sam_rab_ilinskaya.pdf*
7. *Методические рекомендации по выполнению самостоятельной работы студентов / профессор, д.э.н. Е.М. Ильинская. - Санкт-Петербург, 2011.*

Науковий керівник – кандидат технічних наук, доцент Минайленко Р. М., доцент кафедри кібербезпеки та программного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.021

М. Р. Джевлах
студент, Центральноукраїнський національний технічний університет

Порівняльний аналіз методу Ньютона та методу Лагранжа інтерполяції таблично заданих функцій

Дуже часто при проведенні наукових експериментів, дослідженні складних систем та процесів, будь то технологічні, інформаційні чи біологічні системи, науковці стикаються з задачею інтерполяції таблично заданих функцій. Це пов'язано з тим, що які б прилади та методи не були використані при дослідженні процесів чи систем, результати спостережень та вимірювань отримуються в дискретному вигляді. Для того, щоб мати змогу проводити подальший аналіз результатів досліджень, будувати прогнози поведінки досліджуваних об'єктів та розробляти стратегії управління, неможливо оминути процес математичної постановки задачі. Працювати з дискретним набором даних досить складно, він не дає змогу уявити поведінку реального об'єкту в проміжках між вимірюваннями та спостереженнями, або за межами інтервалу вимірювань.

Для того, щоб мати змогу уникнути цих недоліків і побудувати коректну математичну модель, яка буде закладена в основу подальшого аналізу, в тому числі і за допомогою програмних засобів, результати досліджень повинні бути представлені у вигляді аналітичних функцій, рівнянь або їх систем. Одним з найпоширеніших інструментів початкової обробки даних наукових експериментів є інтерполяція. Вона дозволяє представити дискретний набір даних у вигляді аналітичної функції. В залежності від особливостей досліджуваного процесу для інтерполяції можуть використовуватись різні функції. Так, наприклад, для наближення швидкозмінних процесів краще підійдуть гіперболічні функції, а для наближення періодичних, коливних процесів – тригонометричні. Але досить часто для інтерполяції дискретних даних використовують поліноміальні функції. Вони є досить універсальними, і для роботи з ними існує потужний математичний апарат.

Є досить велика кількість методів, які дозволяють інтерполювати точкові функції у неперервні поліноміальні. Двома досить поширеними методами є метод Ньютона та метод Лагранжа.

Для множини n+1 точок з координатами (x_i,y_i), кожна з яких є, наприклад, результатом вимірювання значення досліджуваного параметру в певний момент часу, інтерполяційний поліном Лагранжа будується наступним чином:

$$L_n(x) = \sum_{i=0}^{n} y_i \cdot l_i(x), \text{ де } l_i(x) = \frac{(x-x_0)(x-x_1)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_{n-1})(x-x_n)}{(x_i-x_0)(x_i-x_1)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_{n-1})(x_i-x_n)}.$$

При таких же початкових умовах інтерполяційний поліном Ньютона матиме вигляд:

$$P_n(x) = f(x_0) + \sum_{k=1}^{n}\left(f(x_0,\cdots,x_k)\cdot\prod_{i=0}^{k-1}(x-x_i)\right),$$ де $f(x_0,\cdots,x_k)$ – розподілена різниця k – го порядку, яка визначається через розподілені різниці k-1 – го порядку.

Обидва ці методи дозволяють інтерполювати таблично задану функцію з n+1 елемента поліномом n-го степеня, але при обранні методу інтерполяції треба враховувати таку особливість методу Лагранжа, що при зміні кількості точок хоча б на одну, доведеться заново виконувати весь процес інтерполяції. Тоді як при використанні методу Ньютона, незважаючи на його більшу обчислювальну складність, доведеться виконати обрахунки лише для додаткового члену полінома, а всі попередні розрахунки залишаться незмінними.

Науковий керівник — Гермак В. С., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.02

О. С. Дробко
здобувачка вищої освіти (бакалаврський рівень),
Центральноукраїнський національний технічний університет

Структура і методологічні засади реалізації мобільного застосунку муніципальної інформаційної системи медичних послуг

Розвиток сучасних технологій, популяризація проекту "Країна в смартфоні", намагання органів місцевого самоврядування покращити співпрацю з населенням стали передумовою ініціативи зі створення інформаційних систем, які підвищують ефективність надання громадянам муніципальних послуг. Наприклад, проект "Зелений Кропивницький" є інструментом, який допомагає інформувати громадськість про рішення, прийняті у сфері озеленення та контролювати ці рішення [1].

Як відомо, органи місцевого самоврядування м. Кропивницького ініціювали створення інформаційної системи (ІС) медичних послуг. Вони зацікавлені в сервісі, який буде забезпечувати громаді доступ до актуальних даних про медичне обладнання всіх лікарень міста за допомогою мобільного застосунку. Отже, є актуальною задача реалізації означеного програмного продукту, розроблення його структури та формулювання методологічних засад реалізації відповідного мобільного застосунку.

Муніципальні ІС включають в себе сукупність трьох складових елементів: бази даних (систему самостійних інформаційних матеріалів); обчислювальні засоби, технічні канали зв'язку і пов'язана з ними інфраструктура; інформаційні технології [2]. Для створення дієвої системи розповсюдження інформації шляхом використання мобільного застосунку слід використати концепцію розділення функціоналу, обов'язків з обробки даних та відповідальності між клієнтами та серверами, які взаємодіють один з одним. Для вирішення сформульованої задачі обрано клієнт-серверну архітектуру [3]. Таким чином, мобільний застосунок буде виступати клієнтом та у належній формі презентувати користувачеві інформацію, яка динамічно оновлювлюється сервером.

Враховуючи, що левова частина роботи буде виконуватися сервером, структура мобільного ПЗ буде наступна: інтерфейс користувача; обробник запитів до серверу (Network layer); власне локальне сховище (для збереження даних та надання доступу до них); додаткові елементи, необхідні користувачу (карти, чати, робота з камерою); аналітика (збір даних про активність користувачів).

Виходячи з означеного, під час реалізації програмної системи слід врахувати таке: інтерфейс повинен бути створений з урахуванням вимог UX і UI; для реалізації ІТ-проєкту ефективними будуть лише ті мобільні архітектури, що підтримуватимуть функціонал відправлення і отримання запитів на сервер; повинні бути створені сервіси, що забезпечуватимуть роботу усіх елементів застосунку (збір аналітики тощо).

Варто зазначити, що ПЗ може створюватися як в спеціалізованих середовищах розробки, так і в мультиплатформових IDE, а за побажанням замовника – органів місцевого самоврядування – можуть довільно додаватися різні програмні елементи. Разом з тим, під час реалізації застосунку необхідним є врахування, що його мета для користувача – бути зручним у використанні та надавати доступ до всієї інформації в системі, а для органів місцевого самоврядування – надавати можливість відслідковувати активність та потреби громадян в відповідній сфері суспільного життя.

Список використаних джерел

1. *Електронний сервіс "Зелений Кропивницький": веб-сайт. URL :https://texty.org.ua/d/2018/trees/ (дата звернення: 20.11.2020).*
2. *Інформаційна система: веб-сайт. URL:https://stud.com.ua/34527/informatika/informatsiyna_sistema (дата звернення: 20.11.2020).*
3. *Федорчук Л. Б. Мобільний застосунок взаємодії викладач-студент: дип. на здобуття наук. ступеня бакалавра: Київ, 2019. 31 с.*

Науковий керівник — канд. техн. наук Доренський О. П., доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.773.5

Т. М. Кіріченко
студентка, Центральноукраїнський національний технічний університет

Використання системи Discord для подання навчального матеріалу при дистанційному навчанні

Дистанційне навчання - це форма отримання освіти, при якій викладач і студент взаємодіють на відстані за допомогою інформаційних технологій. Основними принципами дистанційного навчання є інтерактивна взаємодія у процесі роботи, надання студентам можливості самостійного освоєння досліджуваного матеріалу, а також консультаційний супровід у процесі дослідницької діяльності.

Сьогодні дистанційне навчання є однією з провідних світових тенденцій в освіті – ця технологія реалізує принцип безперервної освіти і здатна задовольнити постійно зростаючий попит на знання в інформаційному суспільстві.

Розглянемо одну з платформ дистанційного навчання, а саме Discord. Це інтуїтивно зрозуміла і зручна VoIP програма, яка призначена для створення спільнот, починаючи від геймерських, закінчуючи освітніх та бізнес-спільнот. Discord має все, що потрібно для спільної роботи: підтримка ОС Windows, Mac, Android, iOS, а також є версія для Web-браузера, розробляється версія для ОС Linux. Завантажити Discord можна абсолютно безкоштовно з офіційного сайту. Програма підтримує безліч мов, у тому числі і українську.

Discord складається з множини серверів, доступ до яких можна отримати тільки по запрошенню. На серверах є окремі канали: в них можливо спілкуватися зі студентами або спікерами. У Discord можна використовувати голосовий чат, текстовий чат, відео-зв'язок і, з недавнього часу, демонстрацію екрану для учасників сервера. Він має функцію оверлею, яка показує студентам або викладачам хто зараз розмовляє, що зручно під час он-лайн трансляції лекції. Іншими словами, викладач може спілкуватися наступним чином: викладач розповідає - студенти слухають, запитує когось конкретно - відповідає, можна показати алгоритм вирішення або виконання завдання за допомогою режиму відео або використовуючи демонстрацію екрану для трансляцій мультимедіа матеріалу. Також можна відправляти файли (картинки, документи) прямо в текстовому чаті.

Основними перевагами Discord є: хороша якість звуку і відео; відмінна оптимізація програми - дуже економне використання ресурсів комп'ютера; зрозумілий інтерфейс; сучасний дизайн; можливість створення серверів (аналог груп в скайпі) з функцією поділу на підгрупи-чати і присвоєння учасникам різних ролей; безпека-в режимі стримера Discord блокує дані від інших користувачів; можливість додавання у сервери ботів для розваги та інформування відвідувачів.

Але є ряд недоліків: для відправки файлів вагою більше 8мб, потрібна платна підписка Discord Nitro; інколи бувають баги, та краш серверів.

Провівши аналіз роботи платформи Discord для подання навчального матеріалу при дистанційному навчанні можна відмітити, що, у той час як існує досить багато платформ для проведення он-лайн уроків, він є одним з кращих виборів, незважаючи на те, що початкова задумка була для ігрової індустрії. Адже він є безкоштовною платформою, де не потрібно платити за додатковий час (як в Zoom), або як за групи з нормальним Інтернет з'єднанням (Google Meet).

Науковий керівник — канд. техн. наук Коваленко А. С., старший викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.773.5

Д. С. Колесник[1], А. С. Коваленко[2]
[1]*студентка, Центральноукраїнський національний технічний університет*
[2]*ст. викладач, Центральноукраїнський національний технічний університет*

Аналіз можливостей платформи дистанційного навчання MOODLE як основної системи управління навчанням у ВНЗ

Moodle - це безкоштовна, відкрита система управління навчанням. Вона реалізує філософію «педагогіки соціального конструктивізму» та орієнтована насамперед на організацію взаємодії між викладачем та студентом. Moodle перекладена на десятки мов, в тому числі й українською що значно спрощує використання системи у вищих навчальних закладах (ВНЗ) України. В даний час понад 90 тисяч офіційно зареєстрованих сайтів що працюють на Moodle. Цей проект є відкритим, відтак в ньому бере участь велика кількість інших розробників що розширює вже існуючій функціонал. Moodle написана на PHP з використанням бази даних SQL. Moodle відповідає стандартам та специфікаціям стандарту Sharable Content Object Reference Model (SCORM). Існує декілька способів встановлення Moodle: сервер або ПК користувача; віддалений хостінг; сайт moodlecloud.com.

Можливості Moodle для студентів ВНЗ: вибір курсу навчання, індивідуальна освітня програма, різноманітні засоби комунікації з викладачем і студентами, використання «нестандартних» засобів і методів навчання (соціальний конструктивізм).

Можливості Moodle для викладачів ВНЗ: формування курсу, запис студентів на курс, розподіл по групам, перегляд профайлу студентів, гнучка система оцінювання, використання різноманітних засобів комунікації (повідомлення, форуми, коментарі), дозволяє викладачам легко додати форуми, блоги і чати в курсах, завантажити відео, аудіо файли, зображення, PDF-файли і презентації в своїх навчальних дисциплінах. Основною перевагою системи дистанційного навчання Moodle є можливість її безкоштовного використання. Ще однією важливою перевагою є те, що вона поширюється у відкритому вихідному коді, що дозволяє адаптувати її під специфіку завдань ВНЗ, які повинні бути вирішені з її допомогою. Низькі системні вимоги до сервера, підійде навіть звичайний офісний ПК якщо кількість користувачів буде незначною. Кількість студентів у системі обмежено тільки апаратною складовою сервера. Є можливість розробити надбудову будь-якої складності (модуль), яка дозволить керувати великими контингентами студентів, які навчаються за кількома спеціальностями. Разом з усіма перевагами, Moodle має значний недолік – по замовчанню в системі не передбачені групи рівня сайту, що робить дуже складним облік студентів різних спеціальностей. Групи платформі Moodle існують не для управління правами доступу до курсів, а для поділу груп слухачів в одному курсі. Щоб одні слухачі не бачили активність інших.

Як висновок можна заключити що Moodle є оптимальною платформою дистанційного навчання у ВНЗ якщо у бюджеті ВНЗ не закладено значних коштів на підтримку і розвиток дистанційного навчання закладу. Проте спеціалізоване налаштування платформи та довготривала підтримка все одно вимагає від ВНЗ залучення кваліфікованих ІТ кадрів. Як значний недолік можна вказати що групи створюються всередині курсу і не можуть бути перенесені в інші. Крім цього, оцінками слухача можна оперувати тільки всередині курсу. Немає можливості скласти підсумкову відомість, наприклад, з усіх дисциплін семестру, та й саме поняття семестру в базовій версії системи відсутня. Проте незважаючи на все платформа Moodle зараз є однією з найпопулярніших нині платформ дистанційного навчання серед ВНЗ України.

УДК 621.397

В. Р. Коноваленко
магістрант, Одеська національна академія зв'язку ім. О.С. Попова

Порівняння кодеків сіткового кодування зображень

Ми досліджуємо загальне поліпшення якості сіткових зображень в порівнянні з кодеком EMD + 16. Як і в (El Sayeh Khalil et al., 2016), ми також порівнюємо максимальну та середню кількість бітів, що кодують одну вершину сіткової моделі у кодеках Wavemesh (Valette і Prost, 2004b) і IPR (Valette et al., 2009).

EMD + 16 був реалізований з використанням точок швидкості для кожної роздільній здатності; це більш грубий, ніж кодек IPR, який дає зміну швидкості після кожної бітової площини. Для Wavemesh ми використовували загальнодоступне програмне забезпечення з включеним геометричним критерієм вейвлету. Ми також зробили порівняння для моделей з інтелектуальною власністю (IPR), для яких ми отримали їх розшифровані результати. В якості моделей були обрані фандіск (fandisk), що складається з 6 475 вершин, кінь (horse), що побудовано на 19 851 вершинах і кролик (rabbit) з роздільною здатністю 67 039 вершин. Результати порівняння швидкості цифрових потоків при кодуванні зразків двох кодеків EMD + 16 та IPR свідчить на користь другого (Таблиця 1).

Таблиця 1 - Конкурентні результати кодека IPR порівняно з кодеком EMD + 16.

Модель	*Зростання швидкості*
fandisk (6475)	−0.015bpv (-0.057%)
horse (19851)	+0.022bpv (+0.087%)
rabbit (67039)	+0.073bpv (+0.32%)

Результати над невеликим набором моделей наведені в таблиці 2. У цій таблиці використано показник, подібний до частоти дельти Бйотенганрда (Bjøntegaard, 2001). Він інтерполює точки швидкості в межах обмеженого діапазону швидкості, та відбирає значення спотворення і вимірює відмінності в швидкості на цих зразках. Таким чином, ми можемо знайти максимальне, мінімальне і середнє значення цих відмінностей, з позитивною різницею, що вказує, що сучасний кодек вимагає більше бітів для тієї ж якості, а негативна різниця вказує на те, що новий кодек перевершує запропонований кодек (IPR).

Таблиця 2 - Порівняння довжин кодових слів по відношенню до зразків

Модель	*Кодер*	*Δсер*	*Δмакс*	*Δмін*
fandisk (6 475)	EMD+16 Wavemesh IPR	+0.08 +0.25 +0.43	+0.73 +0.93 +2.90	0.0 +0.04 −0.03
horse (19 851)	EMD+16 Wavemesh IPR	+0.10 +0.15 +2.40	+0.39 +0.84 +7.60	0.0 −0.17 +0.55
rabbit (67 039)	EMD+16 Wavemesh IPR	+0.011 +0.06 −0.15	+0.29 +1.3 +0.40	0.0 0.0 −0.80

Щоб отримати однакову якість при швидкостях до 3bpv, цифри вказані у bpv (gavg) середню швидкість виграшу, (Δmax) найбільшу швидкість виграшу, а (Δmin) найменшу швидкість виграшу. Позитивне значення означає, що потрібно більше швидкості, ніж в пропонованому кодеку, негативне значення означає, що запропонований кодек виконує кодування гірше.

На Рис.1 наведено порівняння швидкості цифрових потоків чотирьох кодеків при кодування сіткових моделей з різною роздільною здатністю.

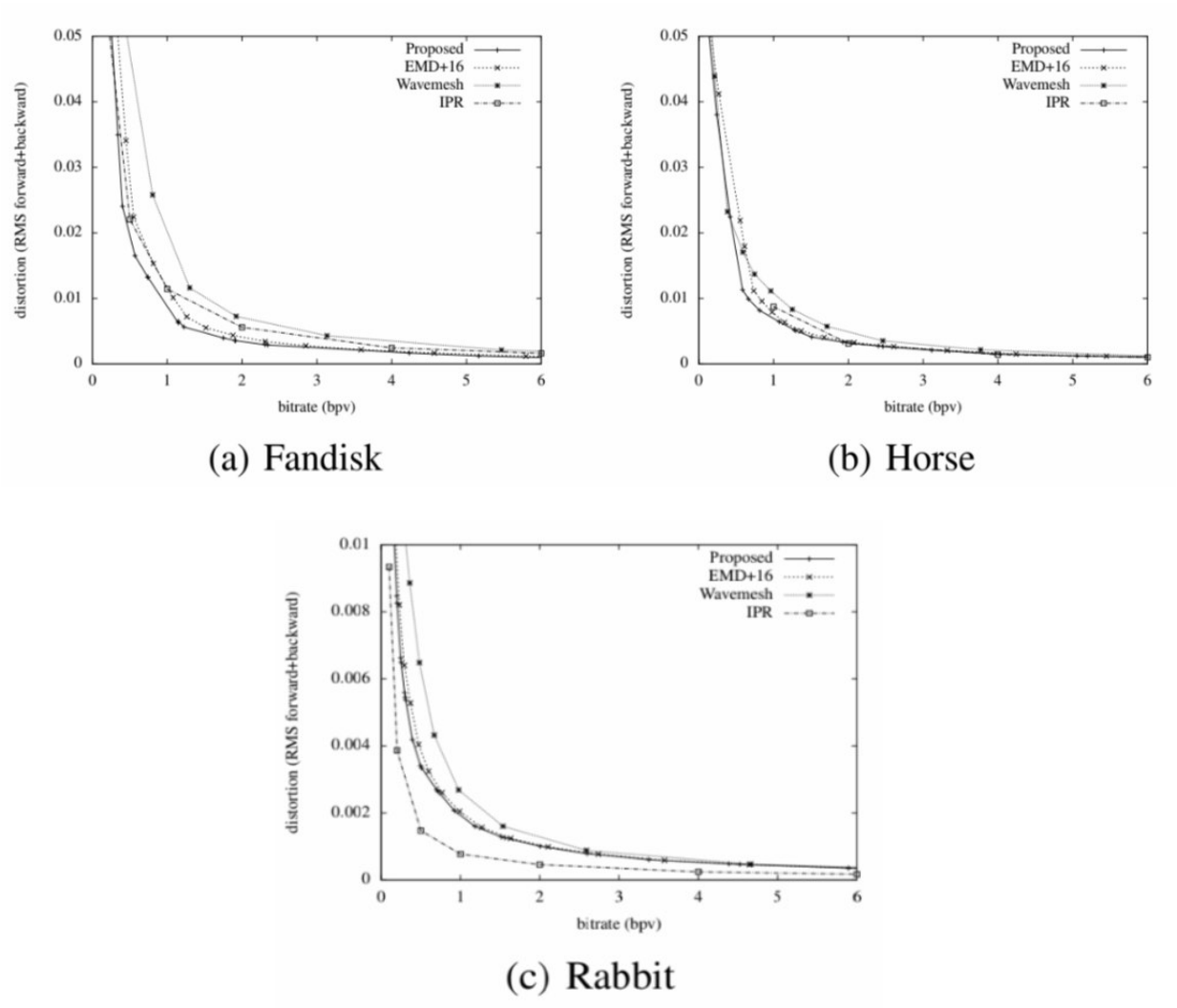


Рисунок 1 – Порівняння швидкості цифрових потоків чотирьох кодеків

У випадку багатофункціональної моделі fandisk, наші результати після оптимізації спотворення швидкості покращуються як за Wavemesh, так і за IPR. У випадку з horse, результати цілком нарівні або краще, ніж у попередній роботі, навіть при найнижчих показниках. Нарешті, для моделі rabbit, з низькою характеристикою результати залишаються майже незмінними порівняно з EMD + 16; Інтелектуальна власність IPR залишається кращим рішенням.

Науковий керівник — кандидат технічних наук, доцент Ошаровська О. В., заступник завідувача кафедри телебачення та радіомовлення.

УДК 004.773.5

О. Р. Кот
студентка, Центральноукраїнський національний технічний університет

Порівняльний аналіз використання сервісів Twitch та Skype як освітньої платформи

Отриманні знання в наш час — найцінніший досвід. В умовах динамічної зміни ринку праці необхідність підвищити рівень кваліфікації або навіть кардинально змінити спеціальність є дуже актуальною. Головна мета більшості — щоб навчання було гнучким та мобільним, не займало багато часу, але давало максимум результату. І тут у пригоді, як завжди, стає інтернет.

Онлайн-освіта набирає все більших обертів. До того ж під час карантину всі установи були змушені перейти в онлайн-формат. Навчання на відстані — часто вже навіть не вибір людини, а вимушений захід.

Тож необхідно визначитись, яким саме сервісом користуватися враховуючи їх переваги та недоліки. Пропоную порівняти такі сервіси як Twitch та Skype у ролі освітньої платформи.

Twitch - відеострімінговий сервіс, який спеціалізується на тематиці комп'ютерних ігор, в тому числі трансляціях геймплея і кіберспортивних турнірів. Відео на платформі Twitch можна переглядати як в реальному часі, так і за запитом.

Сервіс був створений в 2011 році відділенням від схожого сервісу justin.tv, що має більш широку тематику. Крім комп'ютерних ігор, Twitch проводить трансляції та відео іншої тематики, наприклад, музичних виступів або турнірів з покеру.

На Twitch також можливо проводити освітні стріми. Чат в реальному часі прекрасно підходить для питань учнів, але таке практикують дуже мало.

Переваги Twitch як освітньої платформи це:

1) Трансляції проводять дійсно майстри свого діла. Тобто людина, яка буде проводити лекцію або урок, дійсно знає та розуміється на темі.

2) Мобільний додаток Twitch дозволяє дивитися стрім на окремому мобільному віконці. Це дає змогу паралельно працювати в інших додатках. Глядач може робити нотатки і записувати моменти, які його зацікавили, без використання звичайного методу (ручка та зошит).

Недоліки Twitch:

1) Відеозаписи зберігаються максимум 14 днів.
2) Якість трансляції може бути дуже низькою.
3) Слабка підтримка інтернет-зв’язку.

Skype - платформа також відома для більшості і вважається однією з найзручніших платформ для навчання. Вона є безкоштовним програмним забезпеченням, що забезпечує текстовий, голосовий та відео зв’язок через Інтернет. Усе, що потрібно для використання цієї платформи, – це встановити Skype на пристрій, де є робочі динаміки, мікрофон (гарнітура/навушники), веб-камера і якісний Інтернет.

Програма дозволяє здійснювати конференц-дзвінки, відеодзвінки (до 50 абонентів, включаючи ініціатора), а також забезпечує передавання текстових повідомлень (чат) та файлів. Програма надає можливість разом із зображенням з веб-камери передавати зображення з екрану монітора, створювати й відправляти відеоповідомлення користувачем з настільних версій програми.

Комунікаційна система Skype потроху знижує свої позиції, але й досі залишається популярною платформою для online-викладання.

Пропоную розглянути переваги та недоліки Skype.

Почнемо з переваг:

1) Популярність - про нього знають усі, за замовчуванням встановлений на більшості пристроїв, а значить в учнів не буде проблем з установкою та функціоналом.

2) Безліміт у часі - необмежений час групових конференцій.

3) Доступність трансляції екрану з мобільних пристроїв.

4) Технічні можливості. Можливостей Skype достатньо для потреб онлайн-навчання. Можна давати пояснення та ставити запитання віч-на-віч, надсилати файли, переписуватися у чаті, показувати презентації, відтворювати аудіо і відео у режимі демонстрації екрану. Викладачу і учню не треба здійснювати складних технічних дій та витрачати час на навчання саме роботі у Skype.

5) Окремі підрозділи на сайтах підбору репетитора. Часто викладач і учень (або батьки учня) зустрічаються на спеціальних платформах для підбору репетитора, наприклад preply.com, repetitor.org.ua, або buki.com.ua

На абсолютній більшості таких платформ немає окремого підрозділу для онлайн-викладачів, проте є окремий підрозділ для викладання у Skype. Отже часто у батьків (та й у викладачів) складається враження, що Skype – це єдина можливість зустрітися он-лайн репетитору і учню.

6) Комфорт. Дистанційні заняття передбачають можливість займатися і зовсім не виходячи з дому, на улюбленому дивані або кріслі, під ковдрою з чашкою кави в руках. Вдома, як відомо, і стіни допомагають, а точніше, вас ніщо не буде відволікати: дискомфорт через незручні стільці чи неможливість побачити щось на дошці через поганий зір.

7) Гнучкий графік. Кожен день додаткові заняття до 10 вечора? Або у вас змінний графік і ви пропускаєте 50% занять англійською у звичайній школі? Не проблема! Займаючись по Skype, ви можете скласти абсолютно будь-який зручний вам розклад, тобто вибрати і час занять, і їх тривалість.

8) Не потрібно купувати додаткові матеріали. Немає необхідності у додаткових витратах на книги або диски. Вся потрібна інформація вже вбудована в платформу і завжди знаходиться у вас перед очима.

Основними недоліками зазначеної програми є:

1) Поширеність інших месенджерів. Самі школяри і студенти в побутовому житті найчастіше користуються іншими більш сучасними “модними” месенджерами, такими як Телеграм або Вайбер. Їхні можливості принаймні не менші, а часто значно більші ніж у Skype. Чого варті наприклад навчальні боти та наліпки у Телеграмі! Тому, коли викладач пропонує завантажити і встановити Skype, у учня виникає питання, а навіщо? Підлітки, як справжні представники покоління Z, майже не випускають смартфон із своїх рук. Для них набагато зручніш й зрозуміліше використовувати програми, створені саме для смартфонів і планшетів, і Skype для них дещо “не в тренді”.

2) Не підходить для занять у великих групах.

3) Можна вивести тільки демонстрацію свого екрану, але не окремих додатків.

4) Програма дуже «важка» для старих моделей ноутбуів: потребує значних ресурсів, «підвисає» сама та уповільнює роботу інших програм.

Проаналізувавши дві платформи можна визначити, що Skype чудово підходить для дистанційного індивідуального або в невеликих групах навчання. Twitch більш розрахований на лекції для великої аудиторії. Кожна з цих платформ чудово підходить для дистанційного навчання, але для різних цілей.

Науковий керівник — канд. техн. наук Коваленко А. С., старший викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.021

М. В. Кузьменко
студент, Центральноукраїнський національний технічний університет

Класифікація алгоритмів сортування

При розв'язанні майже будь-яких задач, як при створенні програмних систем та засобів, так і в побуті, ми стикаємось з таким поняттям, як сортування даних. Це може бути впорядкування домашньої бібліотеки, або створення та робота з багатотисячною базою даних, кожен елемент якої містить десятки параметрів, або обробка результатів наукових досліджень. В будь-якій сфері людської діяльності не можна обійтись без впорядкування даних за певними параметрами.

Зважаючи на дуже широку сферу застосування процесу сортування та різноманітність параметрів та умов, які повинні виконуватись в залежності від конкретної задачі, було розроблено дуже багато алгоритмів сортування. Кожен з них має свої сильні та слабкі сторони, будь-який з них в одній ситуації може дати прекрасний результат, а в іншій, м'яко кажучи, не дуже. Для того, щоб в кожному конкретному випадку обрати оптимальний алгоритм, треба чітко уявляти, якими особливостями той чи інший алгоритм володіє.

Основними класифікаційними ознаками, за якими можна розрізняти алгоритми сортування, є:

– часова складність алгоритму (характеризує швидкодійність алгоритму);

– природність поведінки (чи зменшується час роботи алгоритму за умови, якщо дані майже впорядковані);

– стійкість (чи змінюється взаємне розташування рівних елементів під час сортування, це особливо актуально для елементів, які складаються з декількох полів, кожне з яких може виступати в ролі параметра сортування);

– ємнісна складність алгоритму (потреба у виділенні додаткової пам'яті під час роботи алгоритму);

– сфера застосування алгоритму (чи буде він працювати з даними в оперативній пам'яті, чи з даними розташованими на зовнішньому носії);

– логічна складність алгоритму (складність для розробника в його реалізації).

В залежності від умов конкретної задачі, яка ставиться перед розробником програмного забезпечення, пріоритетною може виявитись та чи інша характеристика. У випадку, коли ми маємо справу з системами реального часу, критичною буде швидкодійність алгоритму. Якщо програмний засіб найчастіше матиме справу з впорядкованими масивами, слід обирати алгоритм, який має природню поведінку. У випадку роботи з базами даних, елементи яких складаються з різних полів, і сортування в залежності від потреби буде проводитись за різними полями, слід звернути увагу на стійкі алгоритми. При роботі з великими масивами даних, які будуть зберігатись на зовнішньому носії і не можуть бути одночасно розміщені в оперативній пам'яті треба звертатись до алгоритмів зовнішнього сортування, так як алгоритми внутрішнього сортування в даній ситуації виявляться непридатними.

Таким чином, для розробки якісного програмного забезпечення, яке буде задовольняти всім потребам замовника, треба проаналізувати, в яких умовах воно буде працювати, з якими вхідними даними переважно треба буде мати справу. Потрібно мати чітке уявлення про сферу застосування та про вимоги до швидкодійності програмного засобу і вже на основі цих уявлень обирати алгоритми сортування, які будуть закладені в основу програмного забезпечення.

Науковий керівник — Гермак В. С., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.715

О. О. Сандаков
студент, Центральноукраїнський національний технічний університет

Деякі аспекти програмної реалізації візуальної орієнтації на основі системи RTOS

Розвиток роботизованих систем базується на сучасних досягненнях математичної теорії. Розробка робототехнічних систем вимагає знань теорії управління, теоретичної та аналітичної механіки. Це дає можливість проектувати і створювати складні інтелектуальні системи, системи керування роботами і безпілотними літальними апаратами.

Завдання реального часу складають одну з найскладніших і вкрай важливих областей застосування обчислювальної техніки. Як правило, вони пов'язані з контролем і управлінням процесами, які є невід'ємною частиною сучасного життя. Управління прокатними станами, роботами, рух на автомагістралях, контроль за станом навколишнього середовища, управління атомними і космічними станціями і багато іншого - область завдань реального часу. Ці завдання пред'являють такі вимоги до апаратного та програмного забезпечення, як надійність, висока пропускна здатність передавального середовища в розподілених системах, своєчасна реакція на зовнішні події і т.д. Для виконання цих вимог і створюються системи реального часу, апаратне і програмне забезпечення.

Операційна система реального часу (ОСРЧ, англ. Real-time operating system, RTOS) — тип операційної системи, основне призначення якої — надання необхідного та достатнього набору функцій для роботи систем реального часу на конкретному апаратному обладнанні, як правило, без затримок в буфері та позиціонується як інструмент для створення конкретного апаратно-програмного комплексу реального часу.

Ключовою характеристикою RTOS є рівень її узгодженості щодо кількості часу, який потрібен для прийняття і завершення завдання додатка.

Головною задачею RTOS є встигнути зреагувати на події, що відбуваються на обладнанні. RTOS орієнтована на обробку зовнішніх подій.

Структура ОСРЧ еволюціонувала від монолітної до багатошарової структури ОС і далі до архітектури клієнт-сервер:

а) Монолітна структура - ОС складається з набору модулів, і зміни одного модуля впливають на інші модулі. Чим більше модулів, тим більше хаосу при експлуатації такої системи. Крім того, неможливо розподілити ОС багатопроцесорної системи.

б) Багатошарова структура - зміни одного шару впливають на сусідні шари; крім того, звернення через шар неможливо. Для систем реального часу має бути забезпечено пряме звернення до кожного шару ОС, а іноді безпосередньо до апаратури.

в) Клієнт-серверна структура - зведення базису ОС до мінімуму (планувальник і примітиви синхронізації). Вся інша функціональність виноситься на інший рівень і реалізується через потоки або завдання. Сукупність таких серверних завдань відповідає за системні виклики. Додатки є клієнтами, які запитують сервіси через системні виклики. Клієнт-серверна технологія дозволяє створювати масштабовані ОС і спрощує розподіл багатопроцесорної системи. При експлуатації системи заміна одного модуля не викликає ефекту "сніжного кома"; крім того, збій модуля не завжди тягне за собою відмову системи в цілому. З'явилася можливість динамічного завантаження і відвантаження модулів.

Головною проблемою в цій моделі є захист пам'яті, оскільки серверні процеси повинні бути захищені. При кожному запиті сервісу система повинна перемикатися з

контексту програми на контекст сервера. За підтримки захисту пам'яті час перемикання з одного процесу на інший збільшується.

Розглянемо RTOS для мікроконтролерів. Мікроконтролер, або однокристальний мікрокомп'ютер - виконаний у виді мікросхеми спеціалізований комп'ютер, що включає мікропроцесор, оперативну та постійну пам'ять для збереження виконуваного коду програм і даних, порти вводу-виводу і блоки зі спеціальними функціями (лічильники, компаратори, АЦП та інші).

Перш за все, мікроконтролер працює в режимі реального часу, тобто час реакції мікроконтролерного пристрою на зовнішню подію має бути строго менше заданої величини і має бути порівнянним зі швидкістю протікання зовнішніх процесів.

Мікроконтролери часто працюють під управлінням операційних систем, у яких може не бути вбудованих функцій для підключення до локальних мереж або хмари, через що використання таких пристроїв для Інтернету речей стає непростим завданням. FreeRTOS дозволяє вирішити цю проблему і надає як ядро, яке може працювати на пристроях з малим енергоспоживанням, так і бібліотеки програмного забезпечення, які спрощують безпечне підключення до хмари (або інших периферійних пристроїв). Таким чином, можна збирати дані з цих пристроїв Інтернету речей і виконувати необхідні дії.

FreeRTOS написана на мові С, асемблерні вставки мінімального обсягу застосовуються лише там, де неможливо застосувати С через специфіку конкретної апаратної платформи. Робота планувальника FreeRTOS в режимі витісної багатозадачності має багато спільного з алгоритмом перемикання потоків в сучасних ОС загального призначення. Витісна багатозадачність передбачає, що будь-яка виконавча задача з низьким пріоритетом переривається готовою до виконання задачею з більш високим пріоритетом, що дозволяє значно скоротити час реакції системи на переривання, пов'язане з зовнішньою подією.

Розглянемо вимоги, що пред'являються до пам'яті мікроконтролера. Для ядра потрібно додатковий простір пам'яті (ПЗУ).

Розмір ядра залежить від багатьох факторів. Залежно від функціональності, код ядра може займати від 1 до 100 Кб. Ядро для 8-бітногомікроконтролера, яке забезпечує тільки планування завдань, перемикання контексту, управління семафора, затримки і тайм-аути, вимагає приблизно 1-3 Кб. Залежно від застосовуваного мікроконтролера і ядра, може використовуватися окремий стек для обробки всього коду рівня переривання. Це забезпечить бажану особливість, так як вимоги до стека для кожного завдання можуть бути істотно зменшені.

Таким чином, саме FreeRTOS надає можливість забезпечити надійність, високу пропускну здатність передавального середовища в розподілених системах, своєчасну реакцію на зовнішні події, необхідні для програмної реалізації візуальної орієнтації.

Список використаних джерел

1. *Зиль С. Операційна система реального часу QNX: від теорії до практики. - 2-е вид. - СПб .: БХВ-Петербург, 2004. - 192 с..*
2. *Комп'ютерні системи реального часу, навчальний посібник [Електронний ресурс]: навч. посіб. для здобувачів ступеня магістра спеціальності 123 «Комп'ютерна інженерія»/ В. Г. Зайцев, Є. І. Цибаєв; КПІ ім. Ігоря Сікорського. - Електронні текстові дані (1 файл: 4 Мбайт). - Київ: КПІ ім. Ігоря Сікорського, 2019. - 162 с.*
3. *Борисов-Смирнов А. [Электронный ресурс] / Электронный журнал №5 (129), 2008 Операционные системы реального времени для микроконтроллеров Режим доступа: https://docplayer.ru/52758646-Operacionnye-sistemyrealnogo-vremeni-dlya-mikrokontrollerov.html*

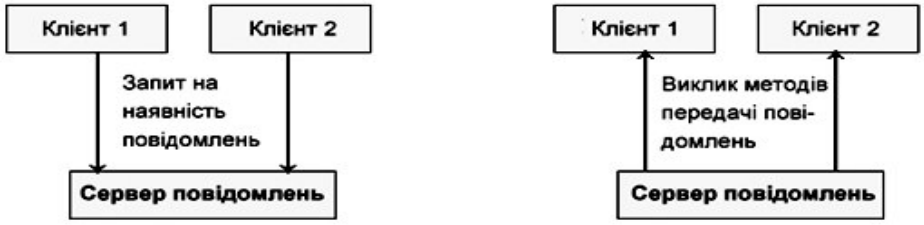
Науковий керівник — к.ф.-м.н., доцент Якименко Н. М., доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.42

Б. О. Сільман
студент, Центральноукраїнський національний технічний університет

Переваги та недоліки механізмів передачі даних технології CORBA

В CORBA існують два різних типи передачі повідомлень - механізм PUSH та механізм PULL. Механізм PULL, рис.1, являє собою наступне: коли клієнт готовий обробляти повідомлення, він опитує сервер на наявність у нього нових повідомлень. Якщо нових повідомлень немає, то клієнт через певний проміжок часу повторює операцію. В залежності від контексту розв'язуваної задачі та пропускних здатностей мережних каналів, тип взаємодії клієнта та сервера може бути асинхронним або синхронним. Механізм PUSH, в певному розумінні, протилежний механізму PULL. В цьому випадку сервер повідомлень сам, у міру надходження нових повідомлень, буде інформувати про це клієнтів. Тобто клієнти самі є серверами, а сервер повідомлень лише викликає в них відповідні методи, надсилаючи їм повідомлення. Як і в моделі PULL, взаємодія клієнта та сервера повідомлень може бути асинхронною та синхронною.



а) механізм PULL б) механізм PUSH

Рисунок 1 – Типи механізмів передачі повідомлень: а) PULL, б) PUSH

В разі використання механізму PULL, на обробку кожного запиту клієнта, сервер витрачає свої системні ресурси за наявності великої кількості клієнтів, які його регулярно опитують, і помітно знижує його продуктивність. Багато залежить від того, як часто клієнти опитують сервер. За великої кількості клієнтів, які очікують, та нетривалого часу між двома запитами до сервера, продуктивність сервера знижується ще більше. У випадку, коли зв'язок між клієнтами та сервером незначний, то ефективність роботи механізму буде ще знижуватися у міру погіршення якості зв'язку. Тривалість виконання запитів буде збільшуватися, а канали зв'язку будуть зайнятими.

В моделі PUSH сервер повідомлень завантажений помітно менше. Сервер звільнений від необхідності регулярно реагувати на виклики клієнтів, які очікують. Тепер він взаємодіє з клієнтами-слухачами. Надсилання повідомлень клієнту застосовується особливо в тих випадках, коли повідомлення, які з'явилися на сервері повідомлень, повинні бути негайно оброблені клієнтом (клієнтами).

За наявності неякісного зв'язку між вузлами, механізм PUSH набагато рентабельніший, порівняно з PULL – він використовує канал лише один раз для кожного клієнта. За умови реальних розробок інформаційних систем, мають місце обидва представлених способи взаємодії компонентів. Розумна комбінація компонент інформаційних систем, які підтримують PUSH/ PULL моделі обміну повідомленнями, дає змогу досягнути високого рівня гнучкості та продуктивності створюваної інформаційної системи.

Науковий керівник – кандидат технічних наук, доцент Минайленко Р. М., доцент кафедри кібербезпеки та программного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.4

М. В. Стецюк[1], О. С. Савенко[2], В. М. Стецюк[3]
[1]*аспірант, Хмельницький національний університет*
[2]*декан факультету, Хмельницький національний університет*
[3]*старший викладач, Хмельницький національний університет*

Модель архітектури автоматизованих інформаційних систем супроводу фінансово-господарських процесів та підтримки управлінських рішень в закладах вищої освіти

Складність задач супроводу фінансово-господарських процесів та підтримки управлінських рішень для підприємств, організацій та установ, рішення яких забезпечується використанням інформаційних технологій, збільшується через потребу посилення стійкості самих інформаційних систем (ІС), підтримки живучості в різних критичних умовах експлуатації та організації захисту інформації в них. Як правило, такі інформаційні системи реалізуються розподілено, передбачають роботу багатьох користувачів одночасно, що потребує реалізації їх з врахуванням забезпечення відмовостійкості і живучості, зокрема і при наявності загроз несанкціонованого вторгнення [1]. Крім того, актуальність захисту інформації в них стрімко зростає порівняно з інформаційними системами з інших прикладних галузей, бо вони відносяться до забезпечення фінансово-господарських процесів, які цікавлять зловмисників і відповідно стають об'єктами атак зловмисного ПЗ [2].

Аналіз роботи відомих ІС ("1С: Підприємство", "БЕСТ", "Парус: Підприємство") [3,4], які призначені для автоматизації фінансово-господарських процесів з точки зору захисту інформації були виявлені деякі проблеми, які впливають на продуктивність їх роботи в умовах впливу зловмисного ПЗ: складність початкового налаштування системи, їх громіздкість, викликаною бажанням бути максимально універсальними. В умовах, коли предметна область, яку вони забезпечують, базується на нормативній базі, яка в свою чергу, постійно динамічно змінюється, в процесі життєдіяльності суспільства, це призводить до значних фінансових витрат на їх утримання для забезпечення їх відмовостійкості та живучості в умовах постійно діючих загроз, стосовно інформації, яка в них обробляється.

Метою цієї роботи є технологія побудови ІС, позбавленої вказаних недоліків, яка відрізняється від існуючих:

1. Інший підхід до модульного принципу побудови систем, а саме - за масштабом модульності. В існуючих системах в якості модуля вибрано реалізацію підрозділу, або кількох суміжних підрозділів (навіть якийсь аспект роботи цілої організації). В розробленій системі за модуль вибрана посада, яка реалізується як окреме АРМ. А підрозділ формується як набір АРМ.

2. Асинхроний режим роботи програмних модулів. Аналіз роботи систем із жорсткою синхронізацією роботи всіх програмних модулів показав, що в них можливі значні втрати часу на очікуваня завершення проведення по системі супроводжуваних нею фінансово-господарських процесів, оскільки досить важко забезпечити рівномірне завантаження всіх користувачів, за всіма напрямками роботи системи в один і той же момент часу. Синхронізація роботи всіх АРМ забезпечується по лівій межі звітного періоду головного АРМ.

3. Дворівнева система адміністрування. Перший рівень адміністрування реалізується традиційним способом. В системі створюються ролі (програмні еквіваленти посади), між якими розподіляються права доступу до об'єктів БД системи та її функціональності. Другий рівень адміністрування реалізований з використанням модульного принципу побудови системи, його задачею є оперативне управління роботою окремих АРМ та їх груп.

4. Робота окремих АРМ в двох часових шкалах. Це дозволяє відображати інформацію як в загально прийнятих звітних періодах (місяць, квартал, фінансовий

рік), так і періодах прийнятих в ЗВО (семестр, навчальний рік).

5. Забезпечується здійснення маневру обчислювальними потужностями апаратної платформи ІС. Налаштування програмного забезпечення АРМ дозволяє маневрувати місцем виконання «важких», з точки зору витрат обчислювальних ресурсів, розрахункових задач, забезпечуючи завантаження одних апаратних засобів ІС, відповідно до їх обчислювальної потужності і, розвантажуючи інші.

Побудована по такій технології ІС отримує можливість динамічно змінювати свою архітектуру з дворівневої клієнт-серверної на 2,5-рівневу клієнт-серверну. Такий підхід дозволяє більш ефективно використовувати ресурси ПЗ та апаратної платформи ІС для підвищення відмовостійкості та живучості в умовах впливів зловмисного ПЗ.

Рисунок 1 – Абстрактна модель архітектури ІС

Такий метод вибору технології клієнт-серверної взаємодії в ІС дозвроляє підвищити живучість ІС, при зростані навантаження на неї. Абстрактна модель архітектури ІС, що реалізує вказану технологію, показано на рисунку 1.

На основі представленої моделі була реалізована клієнт-серверна архітектура з вертикальним розподілом ІС. Як видно з моделі, інформаційні потоки установи знаходяться на перетині вертикального та горизонтального інформаційних каналів (рисунок 2).

З розробленою ІС проводився експеримент, який включав в себе визначення часу необхідного на формулювання завдання на проектування нового АРМ, саму розробку, тестування та введення в експлуатацію. Встановлено таку закономірність – впровадження в ІС кожного нового АРМ займає менше часу, ніж попереднього, навіть при зміні розробників, що пояснюється напрацюванням типових програмних елементів системи.

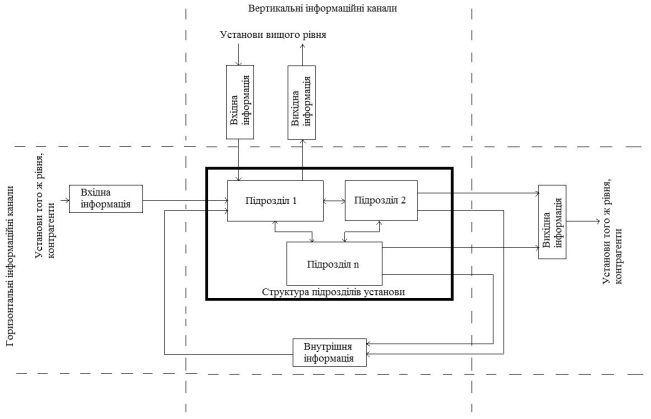


Рисунок 2 – Узагальнена модель інформаційних потоків ІС

Розроблена архітектура ІС є динамічною, дозволяє здійснювати підтримку реалізації принципів живучості, стійкості та захисту інформації в умовах впливу зловмисного ПЗ. Напрямком подальших досліджень є розробка складових АІС, які відповідатимуть за стійкість, живучість та захист інформації, а також відповідних методів їх забезпечення.

Список використаних джерел

1. *Державний стандарт україни. Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97.*
2. *Указ Президента України №133/2017 Про рішення Ради національної безпеки і оборони України від 28.04.2017 "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)".*
3. *Порівняльний аналіз автоматизованих систем бухгалтерського бліку на підприємствах України [Електронний ресурс]. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=5661.*
4. *Інформаційна система "Бест" [Електронний ресурс]. //Ефективна економіка № 6, 2017 – Режим доступу: : https://www.megos.org.ua/referaty/oblik.1.5.1.html.*

УДК 004.021

Ю. П. Толмачов
студент, Центральноукраїнський національний технічний університет

Порівняльний аналіз методів розробки ефективних алгоритмів

В наш час при розробці програмних засобів розробники досить часто вдаються до використання готових програмних модулів для виконання деяких складових своєї задачі. Але інколи задача, яка поставлена перед розробником може бути неординарною, або досить складною, або може бути призначена для роботи в незвичних умовах або з нестандартними наборами даних. В такому випадку може виникнути потреба або в розробці алгоритму з нуля, або в модифікації та оптимізації одного з відомих алгоритмів, або принаймні у осмисленому виборі з множини відомих алгоритмів такого, який найоптимальніше працюватиме в даних умовах.

Для того, щоб якнайкраще виконати поставлену задачу, треба розуміти, що алгоритм, який ідеально працював при одних умовах, може бути абсолютно непридатним в інших. Все залежить від того, що виходить в конкретній задачі на перший план – швидкодія, точність отриманих результатів, об'єм пам'яті, потрібний для роботи алгоритму, тощо.

Методів розробки алгоритмів існує дуже багато. Розглянемо основні з них.

1) Методи грубої сили (brute force). Це методи, які полягають у розв'язані задачі, як то кажучи, в лоб. До методів грубої сили відноситься і метод повного перебору, який полягає в перебиранні всіх можливих варіантів розв'язання задачі та вибору серед них оптимального. Сюди ж можна віднести і алгоритми пошуку з поверненням, як варіант перебірних алгоритмів. Дана група методів дає оптимальні результати для простих задач або для задач з невеликим обсягом вхідних даних. Точність у таких алгоритмів дуже висока, але про часову і ємнісну оптимальність не може бути і мови.

2) Жадібні алгоритми. Це алгоритми, які на кожному етапі розв'язання задачі обирають найоптимальніший для цього кроку варіант. Недолік таких алгоритмів в тому, що на останніх кроках ми можемо бути змушені обирати найгірші варіанти. Такі алгоритми підходять для задач, у яких сума локальних оптимумів в результаті дає глобальний оптимум. Точність у таких алгоритмів не стовідсоткова, але вони прості в реалізації і досить швидкодійні.

3) Алгоритми декомпозиції. Це алгоритми, засновані на принципі розбиття задачі на ряд менших (або за кількісними характеристиками, або за складністю), розв'язанні цих задач, і потім отриманні розв'язку вихідної задачі шляхом комбінування їх розв'язків. Сюди ж можна віднести і методи гілок та меж та методи динамічного програмування. Алгоритми швидкодійні, але в деяких випадках неприйнятні.

4) Евристичні алгоритми. Це алгоритми, які не мають математичного обґрунтування, але дають непогані практичні результати. Сюди ж можна віднести метод спроб та помилок. Засновані на специфіці процесу людського мислення.

5) Алгоритми, які ґрунтуються на здобутках інших галузей наукових знань – генетичні, мурашині, тощо.

Таким чином, на даний час для розробки алгоритмів розв'язання складних задач може бути використана велика кількість методів, які дозволяють по-різному вирішити одну і ту ж саму задачу. Кожен з методів має свої особливості реалізації і відмінності в результативності роботи. Знаючи ці особливості та уважно проаналізувавши специфіку проблеми можна розробити дійсно ефективний алгоритм розв'язання поставленої задачі.

Науковий керівник — Гермак В. С., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.51

А. О. Функендорф
студентка, Харківський національний університет радіоелектроніки

Дослідження методів оцінки ефективності UX-проектування інтерфейсів

UX-проектування інтерфейсів є невід'ємною частиною життєвого циклу інформаційних систем, використання яких передбачає взаємодію з користувачем. В основі методів UX-проектування інтерфейсів полягає концепція «Human-Centered Design», якій відповідають етапи проектування, орієнтованого на кінцевого користувача: розуміння контексту використання, визначення вимог користувача, розробка проектних рішень та їх оцінка [1].

Проведення UX-досліджень, як основи UX-проектування інтерфейсів, дозволяє мінімізувати час розробки програмного продукту, зменшити виробничі витрати, а також підвищити його кінцеву ефективність за показниками коефіцієнту конверсії та рентабельності [2].

На цей час виділяють 96 методів UX-проектування інтерфейсів [3, 4]. Вони використовуються як на етапах первинних досліджень (інтерв'ю, опитування, сортування карток, концепти «Persona» чи «Jobs To Be Done» та ін.) так і під час тестування прототипів (юзабіліті-тестування, A/B тестування та ін.) та кінцевого тестування продукту (теплові карти, аналіз форм та ін.). Але більшість з них не э доцільним для використання у випадках розробки типових WEB-інтерфейсів, що призводить до виникнення задачі прийняття рішень щодо вибору доцільних та ефективних для проектування окремого типового інтерфейсу методів UX-досліджень.

Для вирішення цього завдання в межах реалізації його першого етапу – формування множини методів, використання яких є доцільним для проектування типових WEB-інтерфейсів, було обрано 30 найбільш застосовуваних методів UX-досліджень [4]. Їх кластеризація виконувалась із застосуванням виділених критеріїв ефективності та доцільності: відповідність етапу життєвого циклу розробки програмного продукту, час на реалізацію, кінцева мета створення інформаційної системи (продаж фізичних продуктів, продаж інформаційних продуктів, продаж послуг, надання інформаційних послуг), тип дослідження (лабораторні дослідження з групами, лабораторні дослідження з особами, польові дослідження, експертні оцінки), придатність для проектування типових WEB-інтерфейсів у відповідності до їх цільових завдань (експертне опитування серед репрезентативної виборки з 20 фахівців з досвідом роботи у UX-проектуванні інтерфейсів не менше ніж 5 років). Це дозволяє виділити множини методів, кожна з яких в узагальненому вигляді може бути описана математичною моделлю цілеспрямованої системи зі структурою та властивостями, що забезпечують досягнення кінцевої мети кластеризації:

$$S = < (M \times R_M) \times (P \times R_P) >, \quad (1)$$

де M – множина методів UX-досліджень, що відповідає кластеру S;

R_M – множина відносин між елементами множини M, що упорядковує елементи в окремий кластер S шляхом відповідностей підмножинам властивостей P;

P – підмножина властивостей (значень виділених критеріїв k), що відповідає діапазонам, заданим для кластеру S:

$$P = \{k_1, k_2 \ldots k_n\}; \quad (2)$$

R_P – множина відносин між елементами множини P, що упорядковує елементи в окрему множину M шляхом відповідностей підмножинам властивостей P.

Формування кластерів методів реалізовувалось за принципом виділення головного критерію в межах рішення завдання багатокритеріальної оптимізації [5]. Головному критерію відповідає опис вимоги до рентабельності застосування всіх методів M в межах одного кластеру S, а саме, не перевищення сумарного значення витраченого на застосування всіх методів від часу, що не перевищує 18% (визначено за експертним опитуванням) від загального часу на реалізацію інформаційної системи. В даному випадку ці критерії характеризуються відношенням між елементами підмножини властивостей P та можуть бути описані наступною моделлю:

$$T \le R_{P_i} = \sum_{i=m}^{n} k_{ti} \in P, \tag{3}$$

де T – значення часу, що не перевищує 18% від загального часу на реалізацію інформаційної системи;

$R_{k_t \in P}$ – головний критерій рентабельності застосування всіх методів M в межах одного кластеру S;

k_{ti} – час, на реалізацію i-го методу у кластері S.

Цей підхід дозволяє враховувати інші критерії у відповідності до їх граничних значень, що додатково звужують області допустимих рішень. Тим самим приводячи вихідне багатокритеріальне завдання до класичного однокритеріального.

В ході проведеного дослідження розроблені математичні моделі та отримані за ними кластери методів UX-проектування інтерфейсів, що дозволяють визначати найбільш ефективні групи методів для проектування окремих типових WEB-інтерфейсів. На основі результатів планується подальша розробка програмної системи, що дозволить реалізувати вибір найбільш ефективних методів UX-проектування інтерфейсів відповідно до кінцевої мети розробки типових інформаційних WEB-систем у автоматизованому режимі.

Список використаних джерел

1. *ISO 9241-210. Ergonomics of human–system interaction — Part 210: Human-centered design for interactive systems. International Standard. Switzerland, 2019. 33 p.*
2. *Miklos Philips: The Complete Guide to UX Research Methods. https://www.toptal.com/designers/user-research/guide-to-ux-research-methods.*
3. *Arnold P.O.S. Vermeeren, Effie Lai-Chong Law, Virpi Roto, Marianna Obrist, Jettie Hoonhout, Kaisa Väänänen-Vainio-Mattila. Proceedings of the 6th Nordic Conference on Human-Computer Interaction 2010, Reykjavik, Iceland, October 16-20, 2010. P. 521-530. https://www.researchgate.net/publication/221248254_User_experience_evaluation_methods_Current_state_and_development_needs.*
4. *Virpi Roto, Marianna Obrist, Kaisa Väänänen-Vainio-Mattila. User Experience Evaluation Methodsin Academic and Industrial Contexts – Interact 2009 conference, User Experience Evaluation Methodsin Product Development (UXEM'09), Workshop in Interact'09 conference, Uppsala, Sweden. August 25th, 2009. P. 1-5. https://static.googleusercontent.com/media/research.google.com/ru//pubs/archive/37660.pdf.*
5. *Петров Э.Г., Новожилова М.В., Гребенник И.В., Соколова Н.А. Методы и средства принятия решений в социально-экономических и технических системах: учебное пособие / Под общей редакцией Э.Г. Петрова. Херсон: ОЛДІ-плюс, 2003. 380 с.*

Науковий керівник — кандидат технічних наук, професор Дудар З. В., завідувачка кафедри програмної інженерії Харківського національного університету радіоелектроніки.

УДК 004.773.5

Є. Д. Ховренко[1], А. С. Коваленко[2]
[1]*студентка, Центральноукраїнський національний технічний університет*
[2]*ст. викладач, Центральноукраїнський національний технічний університет*

Аналіз можливостей сервісу Google Classroom для подання навчального матеріалу

Google клас – є розробкою корпорації Google, призначеною для шкільних закладів. Він покликаний спростити створення, поширення і оцінку завдань безпаперовим способом. Безкоштовна інтерактивна платформа Google Classroom дозволяє командам некомерційних проектів ділитися досвідом, підвищувати кваліфікацію і спілкуватися з колегами в «віртуальних аудиторіях».

Проведемо аналіз можливостей Google Classroom. У Classroom можна створити власний віртуальний клас і окремі курси, доступ до яких учні отримують завдяки унікальним кодам. Також самостійно запрошувати учнів до класу, якщо у них є профіль Google. На сторінці кожного курсу можна, наприклад, публікувати навчальні матеріали, проводити опитування, тести й створювати тематичні завдання.

У Classroom є 3-4 основні вкладки (в залежності від того зайшов користувач як вчитель чи учень): «Потік», де видно всі навчальні матеріали, завдання і т.п.. В залежності від налаштувань, робити дописи у потоці можуть як учні, так і вчителі. Кожен допис доступний для коментарів. «Завдання», де учні можуть переглядати всі завдання курсу, а вчитель створювати нові та бачити виконані. «Люди», який надає можливість подивитись всіх учнів на курсі. Викладачі ж можуть побачити список своїх колег. «Оцінки», де лише вчителі можуть бачити інформацію щодо успіхів учнів.

Загалом Classroom надає такі можливості: надсилати матеріали всім учням одразу, дистанційно; збирати роботи он-лайн, а не нести додому стоси зошитів; бачити статистику виконання завдань; створювати анкетні опитування; планувати час розсилки завдань та встановлювати дедлайни; налаштовувати невидиме для інших учнів індивідуальне спілкування з більш сором’язливими школярами у формі приватних повідомлень.

Основними перевагами Google Classroom є:

- користування є безкоштовним та відсутність реклами;
- користуватися можна як з комп'ютера, так і з мобільного завдяки додатку;
- зрозумілий та простий інтерфейс, що зрозуміє дитина;
- налаштована інтеграція з багатьма сервісами Google, наприклад Gmail, Google Документами та Google Календарем;
- підтримує 38 різних мов й серед них є українська;
- підтримує різні формати файлів;
- захищений від втрати інформації, адже всі дані копіюються на Google-диск.

Також Google Classroom має свої недоліки:

- для користування потрібний профіль Google;
- при великій кількості учнів швидко закінчується місце на Google-диску;
- повідомлення у додатку приходять невчасно.

Аналіз показав, що Google Classroom має свої переваги та недоліки, але все ж може значно спростити процес обміну навчальними матеріалами між вчителями та учнями. Він допомагає викладачам розподіляти завдання і ефективно взаємодіяти з учнями не тільки під час дистанційного навчання, а є й зручним доповненням для самостійного опрацювання вдома.

УДК: 004.93’1; 004.932

Д. Г. Чурсінов[1], Т. О. Гріненко[2], О. П. Нарєжній[3]
[1]*студент, Харківський національний університет радіоелектроніки*
[2]*доцент, Харківський національний університет радіоелектроніки*
[3]*доцент, Харківський національний університет імені В. Н. Каразіна*

Многомодальна біометрична верифікація за структурою райдужної оболонки ока та відбитку пальця

Фундаментальна проблема використання відкритих біометричних образів в системах автентифікації полягає в тому, що вони є доступними зловмиснику. Відомі безліч способів фальсифікації відкритих біометричних образів. Тому реальна практика і сучасні стандарти в області інформаційної безпеки (ISO/IEC 24745: 2011, ISO/IEC 24761: 2009, ISO/IEC 19792: 2009 та інші) регламентують захист біометричного образу (шаблону) від компрометації. Внаслідок цього розробка багатофакторних методів біометричної автентифікації є актуальною темою сучасних досліджень. Перспективним напрямком досліджень є розробка методів багатофакторної автентифікації з використанням динамічних біометричних шаблонів.

Для виключення або мінімізування можливих ризиків безпеки потрібно своєчасно виявляти спроби імітації чужої біометрії – виявляти підробку в реальному часі і підтверджувати або спростовувати, що данні представлені істинним володарем. Перевірка на живий/неживий з використанням багатофакторної ідентифікації значно підвищує безпеку і робить компрометацію будь-якого елементу персональних біометричних даних несуттєвою.

Забезпечити якісну і надійну верифікацію користувачів можна реалізувавши багатофакторне рішення, коли реєструються кілька біометричних характеристик.

Надійна біометрична система автентифікації повинна відповідати певним критеріям: універсальність, унікальність, сталість та вимірність. Порівняльна характеристика біометричних систем верифікації та ідентифікації наведена у таблиці 1.

Таблиця 1 – Експертна оцінка біометричних характеристик людини (P_e – оцінка експерта, 1 – низька оцінка, 2 – середня оцінка, 3 – висока оцінка)

Характеристика	Універсальність				Унікальність	Сталість	Вимірність
	FRR, %	FAR, %	EER, %	Pe	Pe	Pe	Pe
Відбиток пальця	0,0001	0,0001	0,01	2	3	3	2
Сітківка ока	-	-	-	3	3	2	1
Голос	-	-	2-5	2	1	1	2
Підпис	-	-	2,46	1	1	1	3
Геометрія обличчя	0,103	0,0047	0,75	3	1	2	3
Райдужна обол. ока	0,009	$1*10^{-6}$	0,0021	3	3	3	2
Особливості вуха	-	-	-	2	2	2	2

Отже, виходячи з даних таблиці 1, можна побачити, що відбиток пальця та райдужна оболонка ока мають найвищі показники по заданим критеріям.

У ході проведеного аналізу літератури [1, 2] було встановлено, що для забезпечення довіри користувачів до біометричної верифікації необхідно забезпечити надійність та безпеку за двома основними напрямами.

Перший напрям – біометрична верифікація в режимі реального часу з перевіркою на підробку. Відомо, що для райдужної оболонки ока основні методи боротьби – додаткові апаратні засоби, що представляють собою зміну райдужної оболонки, наприклад, коливання діаметру зіниці у відповідь на раптову зміну освітлення (при включенні додаткового діода) та додаткова взаємодія з користувачем, наприклад, виведення підказок з проханням закрити/відкрити повіки.

Для відбитка пальця відомі основні методи боротьби з підробками [2]. Захист на рівні пристрою, що зчитує (полягає в тому, що в самому сканері реалізований алгоритм отримання зображення, який дозволяє отримати відбиток пальця тільки з живого пальця, а не з муляжу. Наприклад, так працюють оптоволоконні сканери. Захист по додатковій характеристиці (суть даного методу полягає в отриманні за допомогою скануючого пристрою деякої додаткової характеристики, за якою можна прийняти рішення чи є наданий ідентифікатор підробкою). Наприклад, за допомогою ультразвукових сканерів можна отримувати інформацію про наявність пульсу в пальці, в деяких оптичних сканерах з високим дозволом можна визначити наявність на зображенні частинок поту і т.д. Захист за попередніми даними (на деяких сканерах відбиток пальця останньої людини, яка торкалася до нього, залишається на його поверхні, цим можна скористатися при виготовленні муляжу). В цьому випадку для захисту необхідно зберігати кілька останніх зображень зі сканера (для кожного виробника це число різне), з якими в першу чергу порівнюється будь-яке нове зображення. В залежності від встановленого рівня значущості збігу шаблонів приймається рішення про застосування муляжу.

Другий напрям – це шифрування біометричних даних або застосування алгоритмів, які знецінюють вкрадені біометричні дані. Тобто, ми не можемо змінити свої біометричні дані, але можемо поміняти методи зберігання і алгоритми роботи з ними. Напрям заснований на навмисному повторному спотворенні біометричних даних. Біометричний шаблон спотворюється при реєстрації та при кожній верифікації. Такий підхід дозволяє використовувати для кожного запису свій метод, що перешкоджає перехресному порівнянню. Крім того, якщо екземпляр перетвореної біометрії був скомпрометований, досить змінити алгоритм конвертації, щоб згенерувати новий варіант для повторної реєстрації. Для забезпечення безпеки використовуються незворотні функції. Таким чином, навіть якщо алгоритм спотворення відомий і є перетворені біометричні дані, то відновити по ним вхідні дані не вийде.

У ході роботи було з’ясовано, що поліпшити надійність біометричних систем верифікації можливо за рахунок: застосування багатофакторної біометрії; шифрування біометричних даних; біометричної верифікації у режимі реального часу з перевіркою на муляж; застосування алгоритмів, які знецінюють біометричні дані; швидкої адаптації алгоритмів до появи нових вразливостей.

Список використаних джерел

1. *Abate A. [et al.]. Two-Tier Image Features Clustering for Iris Recpgnition on Mobile. – 2017. – Vol. 10147. – P. 260-269.*
2. *Задорожный Виталий. Идентификация по отпечаткам пальцев, PC Magazine/Russian Edition №1,2.,100 стр., 2004. Інтенсивна технологія вирощування озимого ріпаку в Україні: навч. посіб. / [Г. І. Лазар, О. М. Лапа, А. В. Чехов та ін.]; за заг. ред. О. М. Лапи. – К., 2006. – 100 с.*

УДК 004.3`1/`2

Ю. О. Шеліхов[1], М. Є. Якімаха[1]
[1]*студент, Харківський національний університет радіоелектроніки*

Система контролю мікроклімату для забезпечення наближених природних умов

Вступ. Сьогодні набуває популярність відкриття невеликих City-Farm, ця назва складається з двох слів: Город-ферма, це автоматизовані ферми у приміщеннях, будинках, квартирах та житлових масивах і так як знаходиться безпосередньо у межах міста це дуже спрощує логістику та реалізацію продукції, а також практично будь-який покупець може прийти за вказаною адресою та побачити процес створення товару [1]. Така сфера діяльності передбачає створення та використання персональної автоматизованої системи контролю мікроклімату для забезпечення природних умов у приміщенні.

Як було зазначено, на сіті-фермах використовують сучасне обладнання для контролю мікроклімату, до апаратної частини цих систем відносять датчики, комутатори для з'єднання та лічильники. Так як господарська діяльність знаходиться у приміщенні, їй потрібен свій клімат, а це: певна вологість, температура, яка коригується для різних культур та зміни дня і ночі, штучне освітлення, штучний вітер та вентиляція.

Результати. Сьогодні господарські поля та фермерська діяльність знаходиться на далекій відстані від населених пунктів, більшість ресторанів та закладів харчування шукають інгредієнти для своїх страв на базарах та у постачальників, витрачають кошти на доставку товару, його пошук та якість буде різна. Тому більш сучасні підприємці починають відкриття своїх мікро-ферм прямо в самому городі. Використовують приміщення такі як: квартири, будинки, складські приміщення, офіси, для облаштування. Найчастіше, підприємці створюють фермі відкритого типу за для залучення своїх зацікавлених споживачів на демонстрації, що підвищує рівень довіри. При створенні мікроклімату найважливіше це підійти максимально близько до природних умов навколишнього світу, але так, як діяльність відбувається у приміщенні дуже просто редагувати клімат, вирощувати різні види продукції у різні сезони, забезпечити захист від погодних умов, зміни навколишнього середовища та ніколи не боротись з шкідниками. Наприклад, ви відвідуєте магазин 28 грудня за 3 дні до нового року та на полиці бачите красиву, смачну полуницю, її ніяк не виростити у теплиці або у полі взимку, але на сіті-фермі легко, та значно швидше за допомогою створення притаманного мікро-клімату. Тому дуже важливо створити пристрої для спрощення дій персоналу за доглядом. Система має налаштування світла, яка вмикається та вимикається за встановленими інтервалами, також коригує роботу вентиляції, яка зменшує вологість у приміщенні (за для захисту продукції від плісняви), обігрівачі у холодну пору року, роботу стаціонарних вентиляторів для забезпечення рівномірного обдуву продукції, що заміняє вітер та багато інших факторів.

Висновки. При створенні такої системи слід урахувати деякі фактори, які будуть заважити системі функціювати. Наприклад, усунення проблеми знеживлення, яка може вимкнути систему на довгих проміжок часу, що недопустимо. А також масштабування системи та використання драйверів для економії електроенергії, але станом на сьогодні, більшість сіті-ферм обладнані сучасними джерелами енергії такі як сонячні панелі та вітро-генератори.

Список використаних джерел

1. *Камінь у твій город: як до нас прийшло садівництво [Електронний ресурс] – Режим доступу до ресурсу: https://bzh.life/ua/gorod/city_garden.*

Науковий керівник — канд. техн. наук Сердюк Н. М., доцент кафедри комп'ютерних інтелектуальних технологій та систем Харківського національного університету радіоелектроніки.

УДК 004.42

В. С. Шелудяков
студент, Центральноукраїнський національний технічний університет

Аналіз методів передачі даних між процесорами

Тривалість передачі даних між процесорами визначає комунікаційну складову тривалості виконання паралельного алгоритму в багатопроцесорній обчислювальній системі. Основний набір параметрів, що описують тривалість передачі даних, складається з наступного ряду величин: тривалість початкової підготовки ($t_п$) характеризує тривалість підготовки повідомлення для передачі, пошуку маршруту в мережі і т.п.; тривалість передачі службових даних ($t_с$) між двома сусідніми процесорами (тобто для процесорів, між якими є фізичний канал передачі даних). До службових даних може відноситися заголовок повідомлення, блок даних для виявлення похибок передачі і т.п.; час передачі одного слова даних по одному каналу передачі даних ($t_к$). Тривалість подібної передачі визначається полосою пропускання комунікаційних каналів в мережі.

До числа найпоширеніших методів передачі даних відносяться два основних способи комунікації. Перший з них орієнтований на передачу повідомлень (метод передачі повідомлень, чи МПС) як неподільних (атомарних) блоків інформації (store and-forward routing або SFR). При такому підході процесор, який містить повідомлення для передачі, готує весь об'єм даних для передачі, визначає процесор, якому слід направити дані, і запускає операцію пересилки даних. Процесор, якому направлено повідомлення, в першу чергу здійснює прийом повністю всіх даних і тільки потім приступає до пересилки прийнятого повідомлення далі за маршрутом. Тривалість пересилання даних $t_{пд}$ для методу передачі повідомлення розміром m байтів за маршрутом довжиною l визначається виразом: $t_{пд} = t_п + (mt_k + t_с)l$.

За умови достатньо довгих повідомлень тривалістю передачі службових даних можна знехтувати і вираз для тривалості передачі даних можна записати в простішому вигляді:

$$t_{пд} = t_н + mt_k l .$$

Другий спосіб комунікації базується на представленні повідомлень, що пересилаються, у вигляді блоків інформації меншого розміру - пакетів, в результаті чого передача даних може бути зведена до передачі пакетів (метод передачі пакетів або МПП). За умови такого методу комунікації (cut-through routing або CTR) процесор, що приймає, може здійснювати пересилку даних за подальшим маршрутом безпосередньо відразу після прийому чергового пакету, не очікуючи завершення прийому даних всього повідомлення. Тривалість пересилання даних при використанні методу передачі пакетів визначається виразом:

$$t_{пд} = t_у + mt_k + t_с l .$$

Порівнюючи отримані вирази, можна помітити, що в більшості випадків метод передачі пакетів приводить до більш швидкого пересилання даних; крім того, даний підхід знижує потребу в пам'яті для зберігання даних, що пересилаються, при організації прийому-передачі повідомлень, а для передачі пакетів можуть використовуватися одночасно різні комунікаційні канали. З іншого боку, реалізація пакетного методу потребує розробки більш складного апаратного та програмного забезпечення мережі, може збільшити накладні витрати (тривалість підготовки та тривалість передачі службових даних).

Науковий керівник – кандидат технічних наук, доцент Минайленко Р. М., доцент кафедри кібербезпеки та программного забезпечення Центральноукраїнського національного технічного університету.

УДК 621.397

С. В. Шурова
магістрант, Одеська національна академія зв'язку ім. О.С. Попова

Стиснення зображень фрактальним модифікованим генетичним алгоритмом

Фрактал – це структура, виділена при аналізі зображення, і ця структура володіє схожою формою незалежно від її розмірів.

Генетичний алгоритм (ГА) представляє собою алгоритмічний підхід до вирішення екстремальних задач однокритеріального вибору, який заснований на тому, щоб моделювати основні фактори еволюційного розвитку популяції.

Коли використовують ГА для пошуку оптимальних рішень, кожен елемент простору оптимізації повинен бути представлений як вектор з символів двійкового алфавіту. Також необхідно, щоб простір оптимізації складався із скінченного числа елементів.

Популяцією чисельності вважається такий вектор простору, координати якого називаються генотипами особин даної популяції.

Кроком ГА є перехід від поточного покоління до наступного, тобто отримання нової популяції. У процесі побудови чергової особини нової популяції беруть участь оператори кросинговеру (схрещування), мутації і випадковий оператор відбору, дія якого полягає у виборі номера особини батька при породженні чергового нащадку.

Щоб визначити ГА необхідно задати оператор кросинговеру і оператор мутації.

Дія кросинговеру полягає у виборі випадковим чином деякої позиції, після чого формується результат.

Вплив кросинговеру регулюють за допомогою ймовірності спрацьовування цього оператора (в іншому випадку все залишається без змін).

Оператор мутації в кожній позиції аргументу із заданою вірогідністю замінює її вміст на випадковий елемент двійкового алфавіту, обраний відповідно з рівномірним розподілом (в іншому випадку все залишається без змін).

Цільова функція вихідної задачі, замінюється в генетичному алгоритмі на функцію придатності генотипу.

Процес роботи алгоритму є послідовна зміна поколінь, на кожному кроці якої популяція наповнюється парами нащадків від особин популяції.

Тобто індивіди витягуються попарно після кросинговеру і мутації

Зміна ймовірностей мутації і кросинговеру дозволяє регулювати роботу ГА і налаштовувати його на конкретні завдання.

Модифікований генетичний алгоритм. Опишемо схему ГА у застосуванні до задачі фрактального стиснення. Вектор зручно взяти в якості генотипу ГА, компонентами якого будуть піксельні координати області вихідного зображення, визначеного на тороідальній поверхні, і число кодує афінне перетворення. Є вісім способів афінного перетворення квадрата в квадрат: поворот на чотири сторони або дзеркальне відображення і поворот на чотири сторони. Отже, на кодування цього перетворення достатньо трьох біт.

У цій роботі ми розглянемо параметричний алгоритм фрактального стиснення зображень, в якому попередньо розраховуються статистичні параметри для рангових блоків.

В алгоритмі фрактального стиснення, як і в інших алгоритмах стиснення з втратами, дуже важливі механізми, за допомогою яких можна регулювати ступінь стиснення і ступінь втрат, таким механізмом у фрактальному модифікованому генетичному алгоритмі є поріг розміру рангового блоку.

Було визначено параметри для тестового зображення “кішка” у залежності від порогу (табл.1).

Таблиця 1 - Параметри для нерухомого зображення “кішка”

Поріг	*0,1*	*0,01*	*0,001*
Рангові блоки	60712	336445	666133
Доменні блоки	134	134	134
Розмір блоків	60713	336446	666134
Коефіцієнт стиснення	6,544116	1,239801	1,01
Час стиснення, с	10,292513	21,297584	36,234251
Час декодування, с	22,625596	132,827828	219,818460
Відношення сигнал/шум, дБ	22,834498	22,889807	22,616287

На Рис.1 наведено залежність коефіцієнта стиснення від розміру блоків.

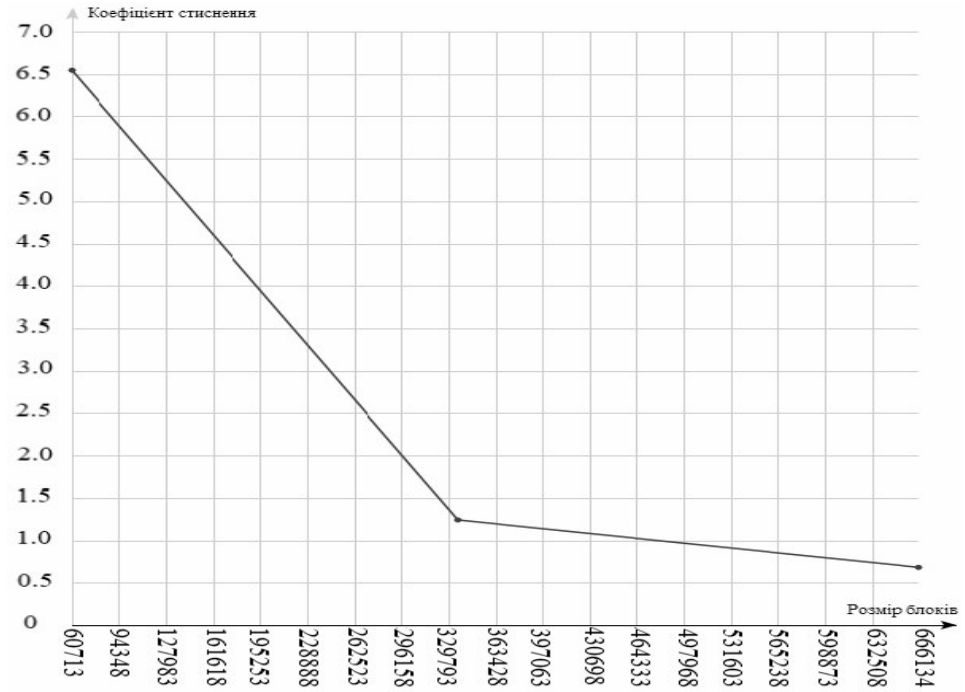


Рисунок 1 - Залежність коефіцієнта стиснення від розміру блоків

Можемо підсумувати, у роботі використано алгоритм, який для деяких класів зображень може значно зменшити обсяг обчислень. Параметрами алгоритму служать рівень втрат при кодуванні і мінімальний розмір областей . Цей алгоритм забезпечує рівномірну якість кодування всього зображення. Коефіцієнт стиснення можна регулювати, змінюючи розміри рангових блоків, тим самим варіювати якість декодованого зображення. Побудована залежність відношення сигналу до шуму в залежності від кількості блоків і розмірів рангових блоків. Розраховано кількість рангових та доменних блоків при різних порогах.

Науковий керівник — кандидат технічних наук, доцент Ошаровська О. В., заступник завідувача кафедри телебачення та радіомовлення.

UDC 004.415.538

O. Bershadskyi[1], M. Rysovanyi[1], V. Ruzhyn[1], I. Kolodiazhnyi[2]
[1]*Student (Bachelor level), Central Ukrainian National Technical University*
[2]*Student (Master level), Central Ukrainian National Technical University*

Conceptual Requirements for the Main Attributes of Test Cases for Software System Testing

Software is nowadays developed and implemented in almost all spheres of society. An important and integral step in the development of any software is testing, including system-level testing (system testing). Conformity verifying of actual software characteristics, properties and behaviour with the expected ones during the testing. It is for this reason that test cases [1, 2] are often chosen, which are the means of documenting the software testing process. Test suites are a set of formally recorded test cases, each of which is a set of input data, prerequisites and conditions of execution, expected results and afterwords designed for a particular test scenario to verify an implementation of specific requirement, i.e. properties or behaviour of software [1-3].

Students face difficulties in correctly describing the test case identifier, test steps and the expected result when creating test cases for system testing of their own software during practical classes on the course “Programming basic methodologies and technologies” (speaker – PhD in IT, Assoc. Prof. O. Dorenskyi, Central Ukrainian National Technical University). Therefore, there is an urgent task of formulating conceptual requirements for the identifier, test steps and the expected result of the test case in order to increase the efficiency of the process of qualified software testing at the system level.

The quality of the test case is determined by the test steps and the expected result. If they are formulated incorrectly, it becomes impossible to perform system testing. These attributes must provide a reasonable ratio of execution time to test coverage [1]. The test steps and expected result must essentially contain a sequence of instructions that have most of the algorithm features (except generality): precision, finiteness, feasibility, uniqueness, efficiency. These features have studied in [1, 3].

The test case identifier does not have to be just a serial number. It should contain prefixes, suffixes and other meaningful components that allow you to quickly determine the purpose of the test case, part of the program, belonging to the test suite, etc.

The "Action" field is required to create a standard test case. In this field, actions should be formulated clearly and consistently one after the other, but details that are obvious to the tester can be neglected. It is also forbidden to refer to other test cases. It is necessary to clearly describe the initial data (different understanding is critically unacceptable for different testers) during formalising the expected results of the test case. Using the constructions "application window: … (then write the expected results)" or "the application window has ... (and a clear list of what should be available)” is most suitable. Such detailing allows the tester to correctly evaluate the obtained results and compare them with the expected.

The report presents requirements for the test case identifier, test steps and expected result as the main attributes of test cases for the software system testing. The obtained results provide an opportunity to improve the quality of test suites for software system testing, as well as to increase the efficiency of the process of qualified software testing at the system level.

References

1. *Доренський О. Критерії деталізації тестових випадків для кваліфікованого тестування програмних засобів. Інтернет-Освіта-Наука - 2016 : 10-а міжнар. наук.-практ. конф. ІОН-2016, 11–14 жовт. 2016 р : зб. праць. Вінниця: ВНТУ, 2016. С. 86–88. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/4285.*
2. *Куликов С. С. Тестирование программного обеспечения. Базовый курс. Минск: Четыре четверти, 2017. 312 с. URL: https://careers.epam.by/content/dam/epam/by/book_epam_by/Software_Testing_Basics_2_izdanie.pdf.*
3. *Dorenskyi O. P. The Methodology of Evaluating the Test Cases Quality for Simple IT Monoprojects Software Testing. Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій : тези доп. VIII Міжнар. наук.-практ. конф. (21–23 вересня 2016 р., м. Запоріжжя). Запоріжжя : ЗНТУ, 2016. С. 111-112. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/3770.*

Scientific Supervisor PhD in Information Technology Oleksandr Dorenskyi, Associate Professor, Cybersecurity and Software Academic Department, Central Ukrainian National Technical University.

UDC 004.415.2:005:83
D. O. Zapotockij[1], D. S. Cherviakov[1], T. V. Ponomarenko[2]
[1]*M.A. Student, National university of shipbuilding named by admiral Makarov*
[2]*Associate professor, National university of shipbuilding named by admiral Makarov*

Probabilistic model for the freelancing platforms contracts risk assessment in Yii2 based software development

The analysis of domestic and foreign publications revealing the problems and prospects of the functioning of the outsourcing services sphere, management and organization processes in this sector of the economy, led to the conclusion that a number of important aspects of the research problem are insufficiently worked out, including: management procedures for the transfer of business processes for outsourcing; assessing possible risks of the outsourcing business model and finding tools to reduce them; systems of interaction between the outsourcing company and the customer company; instrumental and methodological apparatus for increasing the organizational efficiency of outsourcing software projects and assessing the quality of management of this process. Insufficient development of the problem, as well as its theoretical and practical significance, determined the choice of the topic of the current research, determined the setting of goals and objectives.

Project risk from the mathematical point of view is function, which depends on the environmental project factors E and uncertainty U. $R_i = f(E,U)$. The total probability of the emergence of an project risk is understood as the sum of the products of the probabilities of each risk by the probability of a particular scenario of the development of an innovative project with this risk. The total likelihood of an innovative risk is calculated based on: data on possible innovative risks and scenarios for the development of an innovative project under their influence; data on the probabilities of occurrence of the risks under consideration and, corresponding to them, the probabilities of scenarios for the development of an innovative project: $P_A = \sum P(R_i) \times P(A \mid Ri)$ where, P_A is the total probability of software project risk, $P(R_i)$ is the probability of the i-th software project risk, $P(A_i \mid R_i)$ - the probability of one or another scenario of the development of an innovative project, corresponding to the i-th software project risk. Using this formula, we arrive at a mathematical, probabilistic model for assessing innovative risks, which makes it possible to assess not only all the innovative risks of an enterprise carrying out innovative activities, separately, but also the total probability of all innovative risks and scenarios for the development of innovative activities of an enterprise corresponding to the considered innovative risks.

Let's consider an example of the application of this method. Let the enterprise develop a basic software project with the highest risks, which, for example, can be: obtaining a negative customers feedback on Upwork, losing the top rated status, and problems with customers market success. Those risks will be denoted by R_1, R_2 and R_3, respectively. The probabilities of these risks occurring, respectively: $P(R_1) = 5\% = 0.05$; $P(R_2) = 35\% = 0.35$; $P(R_3) = 60\% = 0.6$. Moreover, it should be noted that the sum of the probabilities of the occurrence of all considered risks should be equal to 100%. As a result of these risks, the company may lose the investor. The probability of this event under the action of the risks discussed above is, respectively: 30%, 10% and 15%. In our notation: $P(A \mid R_1) = 0.3$; : $P(A \mid R_2) = 0.1$; : $P(A \mid R_3) = 0.15$. We will find the full probability of software project risk and determine the further fate of the basic software project. Let's use the above formula: $R_A = 0.05 \cdot 0.3 + 0.35 \cdot 0.1 + 0.6 \cdot 0.15 = 0.975$. Thus, the total probability of software project risk is 9.75%, which is an acceptable value for the project, so we can start with its further implementation.

The proposed model makes it possible to form risk protection in the initiation stage of the projects of an freelance agencies from the action of integral net risk through a combination of self-insurance and insurance in the total amount of compensation for losses, which increases the efficiency of risk management in conditions the formation of a new entrepreneurial economy. Moreover, their the combination is due to the need to retain the advantages of self-insurance and insurance while compensating for their shortcomings.

УДК 004.42:004.91

А. С. Ганжа[1], О. О. Байлим[1]
[1]*здобувач вищої освіти,*
Дніпровський національний університет імені Олеся Гончара

Розробка вебдодатку для автоматизації документообігу факультету

Ефективність роботи кожної організації залежить від рівня швидкої і оперативної обробки документації та інформації. Тому автоматизація документообігу є однією з першочергових задач будь-якої фірми, компанії або закладу.

Система електронного документообігу (СЕД) — авторизована багатокористувацька система, що супроводжує процес керування роботою ієрархічної організації з метою забезпечення виконання цією організацією своїх функцій[1]. Найчастіше керування документами зосереджується на даних, що, перш за все, стосуються діяльності організації і зазвичай застосовується відповідно до юридичної цінності документів.

Практика управлінням документами може включати:

– планування потреби в інформаційному забезпеченні системи;

– визначення необхідної для збору інформації;

– створення, затвердження і дотримання політик і практик стосовно даних, включаючи їхнє збереження і знищення;

– розробку плану зберігання даних;

– ідентифікацію, класифікацію і збереження даних;

– розподіл доступу до записів в організації та поза нею, вимог конфіденційності, конфіденційності даних і загального доступу;

– здійснення відбору записів, що не потрібні для використання, для їхнього знищення[2].

Основною метою розробки є скорочення часу, який працівники деканату витрачають на розв’язання щоденних завдань, та спрощення процесу роботи з даними.

Основними задачами розроблюваної програми є:

– розробка бази даних, що містить дані про викладачів та навантаження, дані про студентів та їхню успішність, робочі навчальні плани кожного студента;

– розробка інтерфейсу для ведення бази данних (додавання, редагування чи видалення інформації);

– формування різноманітних довідок для студентів, рейтингових списків та відомостей на стипендію.

Загалом, розробка буде являти собою клієнт-серверний додаток. Програму доцільно розробляти на платформі ASP.net MVC. Вона являє собою фреймворк для створення сайтів і вебдодатків за допомогою реалізації паттерна MVC. Вебдодаток буде локально розгорнуто на комп’ютері за допомогою технології IIS (Internet Information Services[3]).

Список використаних джерел

1. *Система автоматизации документооборота — Википедия URL:*https://ru.wikipedia.org/wiki/Система_автоматизации_документооборота *(дата звернення:10.11.2020./*
2. *Управление записями — Википедия URL:* https://ru.wikipedia.org/wiki/Управления_запи сями.
3. *Публикация на веб-сервере IIS — metanit.com URL:*https://metanit.com/sharp/mvc/13. 2.php *(дата звернення: 18.11.2020).*

Науковий керівник — к.т.н., доцент Антоненко С. В., доцент кафедри математичного забезпечення ЕОМ ДНУ.

УДК 004.912

І. В. Груздо[1], А. О. Функендорф[2]
[1]*доцент, Харківський національний університет радіоелектроніки*
[2]*студентка, Харківський національний університет радіоелектроніки*

Проблеми розпізнавання та визначення мови в текстах

Проблема розпізнавання мови друкованих текстів – одна з проблем, що вирішується більше 50 років і на сьогоднішній день залишається актуальною. Розпізнавання мови – завдання автоматизованого визначення тексту на природній мови є одним із головних завдань як в дослідженнях, так і в комерційних програмах обробки природної мови. Найчастіше розпізнавання мови є одним з підготовчих етапів більш складного завдання.

Завдання розпізнавання мов ускладнюється здебільшого, через те що у багатьох алгоритмах на попередніх етапах отриманий текс «змінюється», за рахунок маніпуляцій, наприклад усунення союзів, стоп-слів, та т.п.. У більшості популярних досліджень, що проводяться ІТ-фахівцями робляться різні припущення, та виконуються зміни самих структурних елементів природної мови, щоб простіше було описати природню мову на мові програмування. Також в процес дослідження здебільшого не залучають фахівців знавців природніх мов, а саме лінгвістів, за рахунок чого в дослідженні забувають про основні елементи мови та правила, що формують її. Природні мови ж мають свою структуру, алфавіт, часті послідовності символів і інше. Наприклад, частота аналізується текс по «частоті вживання літер» [1] та розробляються на їх основі різні алгоритми для ідентифікації мови тексту.

Ще одним великим напрямок дослідження є представлення фактів у вигляді фреймів [2]. Фрейм розглядається як структура, з пойменованими елементами - слотами. Фрейми і слоти наділяються певною семантикою, в залежності від предметної області, в якій вони використовуються та для якої саме мови вони будуються.

Також є окремі напрямки, котрі займаються машинним навчанням для розпізнавання образів та тексту та автоматизацією вилучення знань з таких неструктурованих наборів даних як текст займається відгалуження даталогії (text mining). На основі отриманих даних вони будують алгоритми розпізнавання мови друкованих текстів.

Але хоча проблема розпізнавання мови друкованих текстів і віршується більше ніж пів століття, ніхто не спробував в своїх роботах описати взаємозв’язки, що існують у різних мовах, при цьому при виконані маніпуляцій над текстом існує стандартне припущення те, що в тексті використовується лише одна мова, хоча і існують тексті де є включення слів з різних природних мов. Для вирішення задачі розпізнавання мови друкованих текстів було спочатку зроблено припущення, що текст неоднорідний і в ньому є елементи різних мов.

В ході дослідження були обрані такі мови: українська, російська, англійська, італійська, французька, німецька мови, а також івріт і латинь (т.я. вони дещо відрізняються по своїй структурі). В ході роботи було виділено основні елементи мови (були залучені лінгвісти знавці відповідної мови), зроблене припущення, що кожна мова має три складові: алфавіт, синтаксис і семантику. Алфавіт – це фіксований набір символів. Синтаксис визначає, за якими правилами із символів утворюються тексти. Семантика – набір правил тлумачення, що дозволяють по тексту зрозуміти його сенс. Потім на основі дослідження [3] були описані елементи природні мови за допомогою металінгвістічної формули Бекуса-Наура, завдяки чому різні мови та їх елементи можна було представити у вигляді правил запису. Завдяки цьому було виконано порівняння серед складових мов та складена порівняльна характеристика, та таблиця

відповідностей мовних елементів. На основі отриманих результатів було розроблено схему БД лінгвістичних мов, яка є основою, для подальших досліджень.

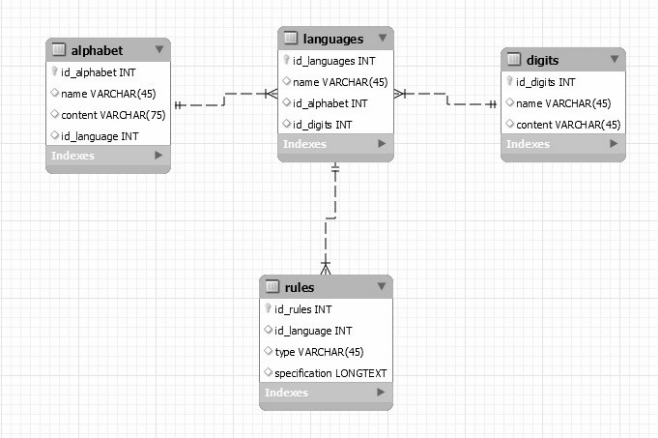


Рисунок 1

Схема бази даних включає в себе чотири таблиці: мови (languages), алфавіт (alphabet), цифри (digits) і правила (rules). Таблиця languages містить назву мови і id його складових; поля: Id_languages – тип int – первинний ключ, інкремент; Name – тип varchar (45) – назва мови; Id_alphabet – тип int; Id_digits – тип int. Таблица alphabet поля: Id_alphabet – тип int –- первинний ключ; Name – тип varchar (45); Content – тип varchar (75); Id_language – тип int. Таблиця digits поля: Id_digits – тип int – первинний ключ; Name – тип varchar (45) – назва набору цифр; Content – тип varchar (45) – цифри. Таблиця rules містить правила мов, поля: Id_rules – тип int – первинний ключ; Id_language – тип int; type – тип Varchar (45) – розділ до якого відноситься правило. Наприклад, орфографія, пунктуація; specification – тип Longtext – містить опис правила.

Між таблицею alphabet і language зв'язок 1 до багатьох, так як один алфавіт може міститися в декількох мовах, але в 1 мові тільки 1 алфавіт. FOREIGN KEY (id_alphabet) REFERENCES mydb.alphabet (id_alphabet). Аналогічно між таблицею digits і language зв'язок 1 до багатьох FOREIGN KEY (id_digits) REFERENCES mydb.digits (id_digit). Між таблицями language і rules зв'язок 1 до багатьох, так як у однієї мови може бути багато правил, а одне конкретне правило відноситься тільки до однієї мови. FOREIGN KEY (id_language) REFERENCES mydb.languages (id_languages)

Дана схема БД підійде для зберігання і впорядкованість лінгвістичних мов їх алфавітів і використовуваних правил. Для побудови БД мов програмування дана схема не підходить, так як їх структура і зміст значно відрізняються від лінгвістичних мов.

Наприкінці слід зазначити, що інноваційний досвід отриманих результатів має значення для розвитку методологічної та методичної бази розпізнавання мови друкованих текстів, а також дозволяє знаходити альтернативні рішення з точки зору виділення їх структур, а також є основою для подальших досліджень спрямованих на визначення змісту текстових документів (семантичний аналіз документів).

Список використаних джерел

1. *Amine A., Amine A., Elberrichi Z., Simonet M. Automatic Language Identification: An Alternative Unsupervised Approach Using a New Hybrid Algorithm – An Overview. International Journal of Computer Science and Applications. – 2010. Vol. 7, No. 1, P. 94 – 107.*
2. *Jun-Tae Kim, Dan I. Moldovan, PALKA: a system for lexical knowledge acquisition. CIKM '93: Proceedings of the second international conference on Information and knowledge management. – 1993. December, P.124–131. https://doi.org/10.1145/170088.170116*
3. *Вылиток А.А. В92 Металингвистические формулы и синтаксические диаграммы: Учебно-методическое пособие. – Москва: МАКС Пресс, 2012. 24 с. ISBN 978-5-89407-484-9*

Науковий керівник — кандидат технічних наук, професор Дудар З. В., завідувач кафедри програмної інженерії, член вченої ради, член НТР, Харківський національний університет радіоелектроніки.

УДК 004

В. А. Губенко
студент, Центральноукраїнський національний технічний університет

Особливості програмування контролера переривань

Контролери переривань у перших комп'ютерах виконувались на мікросхемах i8259, кожна з якихмала 8 входів запиту переривань. У IBM PC AT застосовувалося дві таких мікросхеми, у результаті кількість входів запитів переривань збільшилася до 15. Режими роботи контролерів переривань визначаються процесором шляхом запису відповідних керуючих слів та команд.

Для програмування Pic використовується 2 порти переривання 20h та 21h. Через ці порти передаються 4 команди ініціалізації: ICW1…ICW4 які визначають режим робоботи PIC і 3 керуючих команди: OCW1…OCW3. У порт 21h (з парною адресою) вводиться ICW1, ICW2, ICW3(біт D4 показуэ ICW чи OCW). У порт 21h (з непарною адресою) вводиться ICW1, ICW2, ICW3, OCW1. Слід пам'ятати: слова ініціалізації повинні слідкувати порядок вводу команд, яких указано для портів 20 та 21 h. Для першого PIC ICW3 непотрібно. Наявність ICW4 визначає каскадування. Після ініціалізації подальше управління роботою контролера переривань здійснюється за допомогою слів УСО керуюче слово обміну (OCW). Таких слів передбачено три. На відміну від СНУ вони видаються МП в будь-якому порядку, коли це потрібно програмі.

Слово УСО1 - маска запитів, одиничне значення відповідного біта в цьому слові маскує запит. Друге керуюче слово УСО2 використовується для управління пріоритетами переривань. Біт D7 визначає можливість отримання пріоритетів. Отримуючи запити від пристроїв введення - виведення, контролер переривань визначає (як зазначалося вище), який із запитів володіє найвищим рівнем пріоритету.

Рівні пріоритетів IRQ7-IRQ0 знаходяться завжди в певному співвідношенні, яке прийнято називати статусом рівнів пріоритету. Форма завдання статусу рівнів пріоритету є пріоритетне кільце. Структура пріоритетів, яка встановлюється за умовчанням, визначає фіксований порядок від вищого для входу IRQ0 до нижчого IRQ7.

Ставлячи положення дна кільця, можна визначати пріоритет кожного входу контролера переривань. Контролером передбачено кілька програмних способів завдання дна пріоритетного кільця. встановивши розряд D7 = 1, можна задати режим циклічної обслуговування переривань, при якому обслуговуваному пристрію присвоюється низький пріоритет (дна кільця); режим обслуговування переривань, при якому за допомогою трьох молодших розрядів цього слова (поле L) задається входом IRQ (дно пріоритетного кільця) з найнижчими пріоритетом. Якщо розряд D5 = 1, то при наявності в розряді D6 одиниці поле L визначатиме номер скидається розряду в регістрі маски після закінчення обслуговування переривань. Слово УСО3 використовується для оперативного управління контролером переривань. В цьому слові можна встановити дисципліну обслуговування переривань, що використовує режим опитування: опитуються всі УВВ і вибирається той з них, який в ланцюжку стоїть найближче до МП і виробив переривання; D6 ,D5 – режим спеціального маскування (11 - встановити спеціальне маскування, 10 - скинути спеціальне маскування, 0X - спеціальне маскування не використовувати (тобто, застосовується, коли немає спеціального маскування)); D2 – зберегти або скинути режим опитування (1 - зберегти, 0 - скинути). За допомогою бітів D1 і D0 можна прочитати в МП вміст регістра запиту переривання і регістра обслуговування переривання: 0X - не використовується 11 - регістр обслуговування переривання, 10 - регістр запиту переривання.

Висновки. Всі операції початкового налаштування контролерів переривань виконує BIOS і користувачу потрібно використовувати програмування цих конролерів тільки при необхідності зміни режимів обслуговування чи при написанні власної програми обробки апаратних переривань.

Науковий керівник – доктор технічних наук, професор Сидоренко В. В., професор кафедри кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет.

УДК 004.414.3

Ю. В. Гурова
студентка, Харківський національний університет радіоелектроніки

Вимоги до програмної системи збору та підготовки даних для маркетингових відділів

Кожен із підприємців світу зацікавлений в тому, щоб збільшити свій прибуток. У сфері продажів, грамотне використання та розуміння важливих аспектів маркетингу може допомогти збільшити кількість споживачів, а отже і прибуток, тому ефективна маркетингова діяльність може стати основним критерієм у досягненні успіху в сфері продажів. Головним завданням маркетингу для будь-якого магазину є дослідження, аналіз, оцінка потреб реальних і потенційних споживачів задля створення великого потоку якісних покупців, які купують багато і часто, і тим самим заробляє йому непогані гроші.

Маркетингова діяльність базується на наступних принципах:

– розуміння потреб покупців і реальних можливостей організації;

– задоволення потреб користувачів;

– ефективна реалізація продукції чи послуг у зазначені терміни та у запланованих обсягах;

– забезпечення стратегії до постійних зміни потреб споживачів.

Маркетинг – комплексна система організації виробництва і збуту продукції, орієнтована на задоволення потреб конкретних споживачів і отримання прибутку на основі дослідження й прогнозування ринку, вивчення внутрішнього і зовнішнього середовища підприємства-експортера, розробки стратегії і тактики поведінки на ринку за допомогою маркетингових програм. Також, маркетингова програма передбачає проведення цінової політики фірми, формування попиту, стимулювання збуту та ін. У той час, коли клієнти вимагають швидкого і максимально персоналізованого обслуговування, на допомогу маркетологам приходять найновіші технології, які покращують методи збирання та аналізу інформації у формі, придатній для прийняття рішень.

Проте існують проблеми, пов’язані з відсутністю систем, які розраховані не тільки на збір інформації, а й на її аналіз та висновки. Новизна системи полягає у тому, що вона допомагає не тільки зібрати матеріали та надати у зручній для аналізу формі, а й надає рекомендації відповідно до результатів аналізу.

Для рішення цієї та інших проблем предметної області, розроблювана програмна система повинна мати наступний набір функцій:

– регулярна агрегація та структуризація інформації для маркетингової програми певного бізнесу;

– створення статистики за певний період часу;

– самостійний зручний аналіз інформації від споживачів;

– функціонал, що дозволяє спеціалістам робити більш ефективний аналіз стану бізнеса клієнта та сегментацію ринку;

– можливість визначення цільової групи споживачів певного бізнесу;

– формування ряду рекомендацій щодо проведення маркетингових заходів задля збільшення прибутку певного клієнта;

– реалізація алгоритму факторного аналізу для визначення взаємозв'язку між товарами;

– реалізація алгоритму кластерного аналізу для визначення поведінки покупців та можливостей нового товару;

– реалізація алгоритму регресійного аналізу для прогнозування рівня продажів та долі ринку;

– можливість створення критеріїв за якими буде відсіюватись інформація для кожного клієнта. Ці критерії будуть визначатись самим замовником.

Тобто розроблювана система передбачає наявність спеціаліста в сфері маркетингу, який буде перевіряти коректність створених рекомендацій для покращення стану супроводжуваного бізнесу.

В якості архітектури розроблюваної програмної системи необхідно обрати SOA (Service oriented architecture) архітектуру.

Кожен із сервісів програмної системи повинен мати MVC (Model-View-Control) архітектуру, яка є найпоширенішою на даний момент часу. Серверну частину буде реалізовано за допомогою мови програмування Java, а саме Spring Framework, що забезпечує гнучкість та швидкість розробки, зокрема Spring Boot. Окрім цього буде використано реляційну базу даних PostgreSQL, що забезпечує швидкість роботи та безпеку зберігання інформації. Для написання frontend частини – JavaScript, з використанням бібліотеки ReactJs. Для мобільного додатку, який буде реалізовано для об’єктів спостереження, буде використано Flutter, як фреймворк-обгортка над нативними застосунками Андроїд та iOS пристроїв, що дозволяє з легкістю переходити від однієї ОС до іншої. Також, в якості IoT пристрою, за допомогою якого повинен здійснюватися збір даних, буде використовуватися Single Board Computer, а саме Raspberry Pi, так як будь-яка з ОС, яку вона підтримує, побудована на Unix ядрі, а тому має можливості використання високорівневих мов програмування для збільшення можливостей до створення складних обчислень (у порівнянні з Arduino). Роль датчиків для взаємодії з IoT пристроєм, будуть виконувати Beacons (BLE Devices). Beacons може бути встановленим у корзинки, торговельні візки, візки для перевезення дітей та продуктів. Також у якості Beacon може виступати мобільний телефон, на який встановлено певний додаток. Beacon кодує невеликий об'єм даних у двійковий вигляд та розповсюджує його на радіус дії апаратного забезпечення блютуз модуля. Пристрої, які будуть виступати в ролі отримувачів даних, розкодовують сигнал від Beacon та проводять з ним певні операції. В нашому випадку пристроєм зчитування буде Raspberry PI, що сканувати зовнішнє середовище на предмет наявності сигналу від Beacon, розкодовуватиме інформацію та силу сигналу, вираховуватиме відстань до Beacon та відправлятиме дані на сервер.

Для аналізу інформації споживачів маємо використати фреймворк для роботи з BigData – Spark Framework.

Програмна система має бути розгорнута використовуючи сервіси Heroku, що дозволяють зручно адмініструвати інфраструктуру проекту та вчасно реагувати на ті чи інші повідомлення від сервісів.

Отже, було висунуто вимоги до програмної системи, яка дозволить збільшити попит на ряд послуг чи товарів шляхом збору та підготовки даних для маркетингових відділів. Ця система надасть змогу проводити аналіз показників, які відображають фінансовий стан підприємства, рівень витрат, обсяги матеріальних запасів та інші показники внутрішньої звітності підприємства. Зчитування показників відбуватиметься за допомогою спеціального пристрою – мікрокомп'ютеру. Як результат люди будуть використовувати систему задля забезпечення максимального задоволення потреб споживачів та активного формування їх попиту.

Науковий керівник – Широкопетлєва М. С., старший викладач кафедри програмної інженерії Харківського національного університету радіоелектроніки.

УДК 004.414; 004.9

О. Ю. Клочко
студент, Харківський національний університет радіоелектроніки

Функції програмної системи для відстеження вмісту алергенів у повітрі

Сьогодні все частіше ми чуємо про проблеми екології та забруднення навколишнього середовища. У містах внаслідок забруднення повітря, що постійно збільшується, неухильно росте число хворих. Медики встановили прямий зв'язок між ростом числа людей, що хворіють на алергію та бронхіальну астму, і погіршенням екологічного стану в даному регіоні. Тож постає питання щодо відстеження вмісту токсичних сполук, алергенів, а також знаходження в яких з них може значно погіршуватися стан здоров'я та призводити до виникнення захворювань.

Програмна система, розглянута в даній роботі, насамперед призначена для людей, що хворіють на алергію та мають бронхіальну астму, і допомагає прогнозувати можливе підвищення вмісту алергенів в повітрі. Визначити допустимі норми концентрації пилку в повітрі для всіх користувачів неможливо тому, що реакція на алергени у всіх різна. Алергія виникає тоді, коли кількість пилку перевищує індивідуальний поріг чутливості людини. Тому головну небезпеку становить пилок широко поширених рослин, з якими люди стикаються щодня.

Отже, для користувача є актуальною система, що допомагає відстежувати ці дані для їх подальшої обробки, прогнозувати рівень їх концентрації, контролювати стан здоров'я людини, що допомагає забезпечити профілактику загострень хвороб та спростити життя алергікам. Абсолютних аналогів даної системи немає. Одним з часткових аналогів є система «Pollen Patrol» - це мобільний додаток, що показує інформацію про поточний вміст пилку у повітрі, має функцію щоденника, де можна залишати короткі записи про своє самопочуття та дивитися відмітки про стан інших. Але також вона має свої недоліки, зокрема доступність лише на платформі iOS, мала кількість регіонів, які охоплюються та нестабільна робота.

Запропонована для розгляду програмна система реалізує наступні можливості:

– ведення особистого профілю з можливістю перегляду та редагування, а також оцінки стану свого здоров'я у даний момент часу за допомогою іконок «гарно», «задовільно», «погано», отримання статистичних даних про зміни у самопочутті та отримання рекомендації щодо відвідання лікаря при значному погіршенні стану здоров'я в порівнянні з нормою;

– перегляд карти, де помічені показники вмісту алергенів у повітрі, а також карт з прогнозом розповсюдження алергенів у повітрі на визначеній території з використанням прогнозів погоди з відкритими API та поточних даних;

– перегляд інформації про класифікацію алергенів та їх вплив на здоров'я.

– підготовка даних для аналізу впливу зовнішніх факторів на здоров'я людини.

Для прогнозування розроблено алгоритм, в якому в залежності від поточних показників погоди, а саме температури повітря, швидкості вітру, наявності опадів та фази розвитку рослин змінюються показники концентрації алергенів у повітрі, що дозволить заздалегідь попереджати осіб з алергічним статусом.

Тож розроблена система може бути використана як компонент в єдиній програмній системі контролю здоров'я людини.

Науковий керівник – Широкопетлєва М. С., старший викладач кафедри програмної інженерії Харківського національного університету радіоелектроніки.

УДК 004.421

Н. В. Ламекін
студент, Центральноукраїнський національний технічний університет

Аналіз практичного застосування алгоритмів сортування

У нашому реальному житті так багато речей, що нам потрібно шукати, наприклад, певний запис у базі даних, номери записів у списку послуг, конкретний номер телефону в телефонному довіднику, певну сторінку книги тощо. Ми б мали безлад, якщо дані зберігалися невпорядкованими та несортованими, але, на щастя, з'явилася концепція сортування, що полегшує кожному упорядкувати дані, отже, полегшує пошук.

Алгоритми сортування використовується не тільки в інформаційно-пошукових системах, а й у банківській та військовій справі, та ще багато де. З початку епохи програмування вчені-інформатики працюють над вирішенням проблеми сортування, придумуючи різні алгоритми сортування даних.

Існує кілька критеріїв, які слід використовувати для оцінки алгоритму сортування: час роботи, вимоги до пам'яті і стабільність. Як правило, елементарний алгоритм сортування вимагає O (n^2) кроків для сортування n випадково розташованих елементів. Більш складні алгоритми сортування вимагають в середньому O (n log n) кроків. Крім того, деякі алгоритми сортування більш чутливі до природи введення, ніж інші. Алгоритми сортування є найбільш ефективними з точки зору використання пам'яті, оскільки вони практично не потребують додаткової пам'яті. Стабільність - це здатність алгоритму сортування зберігати відносний порядок рівних ключів.

У даному дослідженні розглядаються бульбашкове сортування, сортування вибором, вставками та швидке сортування. Кожен з цих алгоритмів є стабільним і використовує O(1) додаткової пам'яті.

Для практичного порівняння швидкодії роботи алгоритмів сортування, була написана програма на C#. В результаті були практично перевірені всі вищеназвані алгоритми. Для сортування використовувалися масиви з 10 елементів, з 100 елементів, з 1000 елементів, з 10000 елементів, з 30000 елементів, чисельні значення яких були згенеровані випадковим чином. Отримані результати зведені до таблиці 1.

Таблиця 1 – Результати виконання алгоритмів сортування

N	Кількість проходів				Кількість порівнянь				Кількість перестановок				Час (мс)			
	бульбашкове	вставками	вибором	швидке	бульбашкове	вставками	вибором	швидке	бульбашкове	вставками	вибором	швидке	бульбашкове	вставками	вибором	швидке
10	5	1	9	19	45	22	45	81	13	13	7	10	< 1	< 1	< 1	< 1
100	90	1	99	167	8910	2459	4950	1404	2360	2360	92	175	< 1	< 1	< 1	< 1
1000	976	1	999	1775	975024	249142	499500	21860	248145	248143	994	2587	18	10	4	< 1
10000	9976	1	9999	17645	99750024	24962876	49995000	265172	24952888	24952873	9992	33913	1505	554	348	2
30000	29890	1	29999	51873	896670110	225450666	449985000	902896	225420710	225420667	29983	114015	12928	5040	3129	7

З таблиці видно, що прямі алгоритми сортування значно поступаються швидкому, і чим більше елементів у масиві, що сортується, тим більше різниця у швидкості їх виконання. Навіть при різних вхідних даних, час покращується за рахунок частково відсортованих масивів.

Результат цього дослідження доводить, що алгоритм швидкого сортування є більш ефективним ніж прямі алгоритми і робить його вартим більш детального вивчення для знаходження ефективних шляхів його реалізації.

Список використаних джерел

1. Мелешко Є.В., Якименко М.С., Поліщук Л.І. Алгоритми та структури даних: Навчальний посібник. – Кропивницький: Видавець – Лисенко В.Ф., 2019. 156 с.

Науковий керівник — Поліщук Л. І., старший викладач кафедри кібербезпеки та програмного забезпечення.

УДК 004.6

Д. С. Марков
магістрант, Центральноукраїнський національний технічний університет

Аналіз можливостей застосування MySQL 8.0 для роботи з великими даними

Важливість Big Data, основні напрямки використання (наука і досліди, соціальні медіа, політика, охорона здоров'я, маркетинг). Задачі, що ставляться до роботи з великими даними – зберігання, управління, обробка, аналітика та візуалізація великих даних. Апаратні комплекси від деяких корпорацій, на кшталт Teradata, EMC, Hana компанії SAP і комплекс Exalytics компанії Oracle.

Основні недоліки реляційних баз даних (необхідність знати структуру даних до їх отримання, труднощі з горизонтальним масштабуванням, велика складність зміни структури вже існуючих даних). MySQL вирішує питання зберігання даних та частково вирішує питання їх обробки та управління (завдяки синтаксису запитів SQL). В цілому, при роботі з малими об'ємами даних що мають чітку структуру реляційні бази даних проявляють себе дуже добре. А от при роботі з Big Data постає кілька питань і перше з них – розділення великих об'ємів даних. Відомо, що реляційні бази даних чудово пристосовані до вертикального масштабування, але MySQL 8.0 також має можливості і горизонтального масштабування. Для побудови високонавантажених систем велике значення має можливість реплікації. MySQL 8 підтримує одразу два методи реплікації – з використанням бінарних журналів та з використанням глобальних ідентифікаторів транзакцій.

Також важливим питанням є сумісність MySQL з інфраструктурою інструментів для роботи з Big Data. На прикладі зв'язки MySQL – Apache Hadoop ми можемо побачити що MySQL використовується для роботи зі структурованими даними і за допомогою модуля Apache Sqoop відбувається імпорт даних з MySQL до Hadoop та імпорт структурованих даних назад до MySQL. Враховуючи те, що Apache Hadoop використовує власну систему зберігання даних HDFS, MySQL у даній зв'язці використовується лише для збереження структурованих даних. Більш повною мірою можливості MySQL для роботи з великими даними розкриваються у зв'язці з MySQL Applier. Ця технологія дозволяє проводити реплікацію даних з MySQL до Hadoop і навпаки у режимі реального часу. Завдяки цій зв'язці ми можемо зберігати структуровані дані у MySQL і легко візуалізувати їх, в той час як в Hadoop будуть зберігатися неструктуровані дані, котрі в зв'язці з даними з MySQL будуть опрацьовуватися з метою пошуку закономірностей, прогнозування поведінки та іншими цілями.

MySQL 8.0 добре підходить для зберігання та роботи зі структурованими даними, в тому числі такими, що мають великий об'єм. За допомогою вертикального та горизонтального масштабувань забезпечується висока продуктивність та ефективність роботи з різними об'ємами даних. Коли необхідно зберегти чітку структуру даних і можливість простої візуалізації певної вибірки даних, MySQL є оптимальним рішенням. Що стосується функцій аналізу, прогнозування та обробки даних – для них ефективніше використовувати додаткові інструменти для роботи з Big Data. Зокрема, у зв'язці з Apache Hadoop та модулями Sqoop, MySQL Applier та іншими можна досягти високої ефективності в аналізі даних в режимі реального часу, зберігши при цьому структурованість та легкий доступ до даних.

Список використаних джерел

1. *Чаллавала Ш., Лакхатария Дж., Мехта Ч., Патель К. MySQL 8 для больших данных / пер. с анг. А. В. Логунова. - Москва : ДМК Пресс, 2018. 226 с.*

Науковий керівник — к.т.н., доц. Босько В. В., доцент кафедри КБіПЗ, Центральноукраїнський національний технічний університет.

УДК 004.415.2

В. В. Нарманія
студент, Харківський національний університет радіоелектроніки

Проектування алгоритму нарахування бонусів для програмної системи оренди велосипедів

На сьогоднішній день відбувається розвиток оренди транспортних засобів пересування, а особливо велосипедів. Світ захоплюють велосипеди. Якщо переходити до цифр, то зараз світовий ринок велошерінгу зростає приблизно на $1 млрд на рік, згідно з прогнозом консалтингового агентства Navigant Research, до 2025 року буде оцінюватися в $24,4 млрд [1]. Причиною тому є те, що велосипед позитивно впливає, як на зовнішнє середовище, так і на саме тіло людини. Через зростання попиту на велосипеди їх ціна зросла, тому оренда велосипедів це один з кращих варіантів для пересування.

У наш час існує дуже багато систем для велошерінгу по всьому світу, наприклад, “City Bike”, “Next Bike”, “Коло Bike” та інші [2, 3]. Всі ці системи надають можливість брати велосипед на тимчасове використання за допомогою смартфону, що робить цей процес швидким та зрозумілим, так як зараз телефон є невід’ємною частиною нашого життя. Також їх перевагою є те, що станції з велосипедами знаходяться майже по всьому місту, що робить людину більш мобільною, так як час пошуку станції є мінімальним. Хоча у даних систем існує певна проблема. Вона полягає в тому, що на станції може не бути велосипедів зовсім, тобто потрібно чекати поки з’явиться доступний велосипед або шукати іншу станцію. Також за недолік можна вважати те, що вони не заохочують клієнтів користуватися саме їх застосунком, наприклад, за допомогою системи накопичення бонусів у вигляді знижок або взаємодії між користувачами, яка б покращила комунікацію спільноти велосипедистів.

Пропонується для розгляду програмна система “One Bike”, що зможе надати можливість користувачам отримувати велосипед у тимчасове використання. Користувач зможе отримувати бонуси, які можна обмінювати на винагороди у вигляді знижок та подарунків за оптимізацію розташування велосипедів на станціях, створення та проходження квестів.

Метою роботи є проектування алгоритму для нарахування бонусів у програмній системі “One Bike”, що може бути використаний задля вирішення проблеми випадку, коли на станції будуть відсутні велосипеди або їх буде мала кількість запропоновано алгоритм нарахування збільшених бонусів за транспортування велосипеду зі станції з великою кількістю доступних транспортних засобів до пункту з малою кількістю. Алгоритм полягає в тому, щоб знайти значення кількості бонусів, яка буде нарахована після закінчення поїздки користувачем. Спочатку необхідно знайти відсоток доступних велосипедів на початковій станції, після того, як користувач закінчить свою подорож потрібно знайти відсоток велосипедів на кінцевій станції. Далі в алгоритмі обчислюється різниця відсотків. Якщо це значення менше за нуль, то бонуси користувачу не нараховуються, бо оптимізація розташування не була здійснена. Якщо значення різниці відсотків більше за нуль, необхідно отримати час, який знадобився користувачу, щоб доставити велосипед з початкової до кінцевої станції. Далі обчислюється значення бонусів для зарахування користувачеві за формулою:

$$B=D+D\cdot T100,$$

де B – кількість бонусів, D – різниця відсотків, а T – час подорожі.

На рисунку 1 наведено блок-схему даного алгоритму.

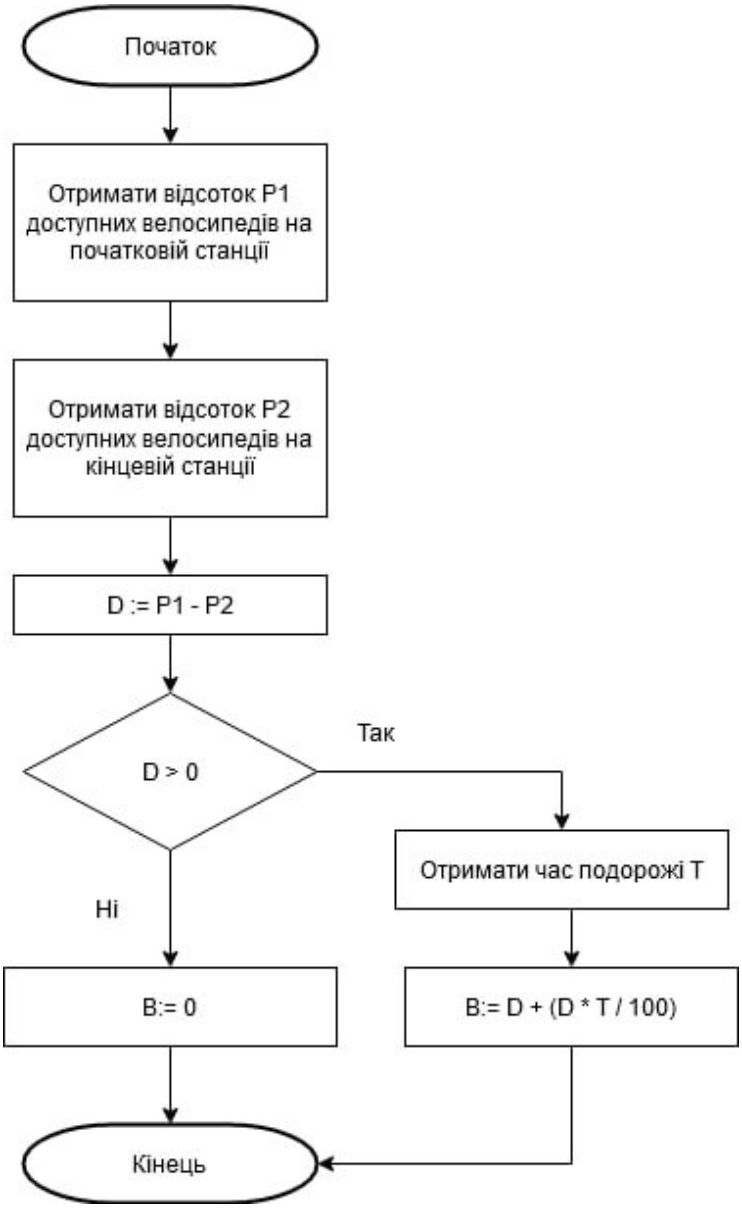


Рисунок 1 – Блок-схема алгоритму нарахування бонусів

Було запропоновано алгоритм для програмної системи оренди велосипедів, яка вирішує проблему з відсутністю транспортних засобів на станціях за допомогою алгоритму нарахування бонусів за перевезення з урахуванням доступних велосипедів на станціях.

Список використаних джерел

1. *Стартапи, які змінять наше життя. URL: https://www.gq.ru/success/19-startapov-kotorye-izmenyat-nashu-zhizn-v-2019-godu/ (дата звернення 10.11.2020).*
2. *Громадський прокат велосипедів в Україні від Next Bike. URL: https://www.nextbike.ua/uk002/ (дата звернення 15.11.2020).*
3. *Citybike Wien. URL: https://www.citybikewien.at/en/ (дата звернення 19.11.2020).*

Науковий керівник — Широкопетлєва М. С., старший викладач кафедри програмної інженерії, Харківський національний університет радіоелектроніки.

УДК 004

М. Ю. Окунєв
студент, Центральноукраїнський національний технічний університет

Алгоритми визначення контролером переривань адреси таблиці обробки переривань

Підвищення продуктивності обчислюваль них систем (ОС) реального часу є важливою задачею в області застосування автоматичних систем управління. Особливістю таких систем є функціонування в режимі реального часу, що вимагає забезпечення гарантій виконання жорстких часових вимог. Складність виконуваних задач підвищують вимоги до сучасних ОС реального часу і обумовлюють розробку нових апаратних та програмних засобів для підвищення ефективності обробки та обміну даними. Проблема підвищення продуктивності систем реального часу вирішується за рахунок модифікації архітектури системи переривань, що забезпечить гарантоване обслуговування переривань від великої кількості зовнішніх пристроїв на протязі фіксованого часу циклу управління.

З кожним переривання зв'язана та чи інша подія. Система повинна розпізнати, яке переривання за яким номером відбулося і яку відповідну підпрограму треба виконати.

Відомо два види переривань: апаратне і програмне. Програмне переривання зручно використовувати для організації доступу для окремих спільних для всіх програм модуля. Прикладні програми можуть самі встановлювати свої обробники переривань для їх послідуючого використовування іншими програмами.

Програмні переривання зручно використовувати для організації доступу до окремих і спільних для всіх програмних модулів. Прикладні програми можуть встановлювати власні обробники переривань. Для цього переривання повинні бути резедентними у пам'яті. Використовуючи переривання з повільними пристроями дозволяю поєднати/О інформації з обробкою даних у ЦП.

Деякі переривання (перші 5) зарезервовані для використання самим процесором для виконання деяких подій. Складання особистих програм обробки переривання і заміна стандартних обробників є відповідальною і складною роботою. Необхідно врахувати усі тонкості роботи апаратури і взаємодії програмного і апаратного забезпечення. Для виконання необхідної послідовності команд при наявності декількох переривань необхідно переривання з вищим пріоритетом замаскувати. Це можна зробити за допомогою команди CLI. Ця команда забороняє тільки масковані переривання, а немасковані завжди оброблюються процесором. Якщо використовується заборона переривань за допомогою CLI, то в кінці обов'язково треба поставити команду STI.

Якщо програмі потрібно змінити обробку деяких переривань, то програма повинна пере назначити вектор переривання на свій обробник. Одним із шляхів вирішення є зміна в таблиці відповідного з векторів переривань. Послідовність дій для нерезедентних програм обробки переривань: прочитати зміст елемента таблиці векторів переривань для вектора з потрібним вам номером; запам'ятати цей зміст (адреса старого обробника) у область даних програми; встановити нову адресу у таблиці векторів переривань так, щоб вона відповідала початку вашої; перед завершенням роботи програми прочитати із області даних адресу старого обробника переривання і записати у таблицю обробника переривання.

Висновки. Застосування розподіленого КПП відповідає модульному принципу організації ОС і ефективно вирішує задачу масштабування обчислювальних систем з відкритою архітектурою, що до кількості зовнішніх пристроїв.

Науковий керівник — доктор технічних наук, професор Сидоренко В. В., професор кафедри кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет.

УДК 004.4

Д. М. Подкопаєв
студент, Центральноукраїнський національний технічний університет

Огляд і аналіз автоматизованих платформ для вивчення web-програмування

В епоху пандемії вдосконалення освітнього процесу, підвищення якості навчання неможливо без активного використання електронних освітніх ресурсів, без застосування інноваційних технологій, до числа яких можна віднести і технології дистанційного навчання. Для розробки сучасних освітніх платформ для вивчення web-програмування буде актуальним виконати огляд і аналіз програмних продуктів, що вже існують.

Серед основних переваг використання автоматизованих засобів навчання, в порівнянні з традиційними, виділяють наступні можливості: обслуговування великого потоку користувачів в порівняно короткі терміни; оптимального поєднання масового і індивідуальних підходів до процесу навчання; ефективної організації дистанційного навчання та підвищення мотивації студентів до навчального процесу [1].

Було розглянуто такі програми: Codeacademy, HTML Academy, Codingame,Code Basics, FreeCodeCamp, Scrimba [2] і Prometheus.

HTML Academy навчає програмуванню сайтів. Основний контент у форматі підписки, але має й декілька безкоштовних курсів з HTML, CSS і JavaScript. Розглядаються більшою мірою основи веб-розробки. Code Basics - це безкоштовний сервіс. Навчання складається з невеликих порцій теорії, що чергуються з закріплення практики в тренажері. Зараз пропонуються уроки з PHP, JavaScript, Python, Java, HTML, CSS і Racket.

FreeCodeCamp – це велика некомерційна автоматизована платформа. Вчить з нуля основам веб-розробки: HTML, CSS і JavaScript. В кінці є ознайомчі блоки по React / Redux, візуалізації даних і навіть трохи по бекенду. Scrimba, англомовна платформа – органічне поєднання відео уроків та завдань у браузері. Вміщує велику кількість тем з веб-розробки: від «флексбоксів» і Bootstrap до React, Vue і Angular. Codeacademy – це одна платформа для вивчення основ кодингу за різними технологіями: Python, SQL, Java, верстка, JavaScript та інші. Все орієнтовано на рішення простих завдань. Codingame – це платформа з якісною графікою для навчання програмуванню в ігровій формі. Вивчення Python, Java, JavaScript, C++/# виглядає як проходження рівнів гри [3]. Prometheus – перший та найбільший проект безкоштовної освіти в Україні. Має 9 безкоштовних курсів з програмування. Серед них «Основи Web UI розробки» - Front-end, Back-end, HTML/CSS/Javascript.

З огляду на переваги та недоліки існуючих платформ можна створити комплекс програм, який буде використовуватися студентами й викладачами як допомога у вивченні web-програмування та інших дисциплін. Його застосування дозволить істотно скоротити час, що витрачається викладачем на формування навчального контенту.

Список використаних джерел

1. *Еникеев А.Е., Бухараев Н.Р., Гайнуллина Э.А., Романова И.В. Системма автоматизированного обучения и тестового контроля знаний по дисциплинам в области компьютерных и информационных технологий // 2013 [Електронний ресурс] – Режим доступу: https://cyberleninka.ru/article/n/sistema-avtomatizirovannogo-obucheniya-i-testovogo-kontrolya-znaniy-po-distsiplinam-v-oblasti-kompyuternyh-i-informatsionnyh/viewer*
2. *Шесть бесплатных автоматизированных платформ для изучения программирования // 2018 [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/hexlet/blog/432802.*

Науковий керівник — Константинова Л.В., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.388

Є. В. Середа
студент, Центральноукраїнський національний технічний університет

Про детермінованість імовірнісних автоматів

У наш час в багатьох сферах інформаційних технологій, таких як кібербезпека, програмування та криптографія, використовуються імовірнісні автомати. Часто маємо справу з автоматами або алгоритмами, які видають «зовсім випадкові» числа.

Будь-який ймовірнісний автомат є недетермінованим. Недетермінований автомат – це абстрактний автомат, який при даному вхідному сигналі і певному внутрішньому стані може переходити в декілька різних внутрішніх станів з різною ймовірністю.. Здається, що він не зможе перейти у абсолютно довільний інший стан, адже за однаковим набором або вхідними даними, алгоритм повинен перевести його у конкретний інший стан.

Кожен автомат працює за деяким алгоритмом, який складається з деталізованих інструкцій, що реалізують процес обчислення, який, починаючи з початкового стану, відбувається через послідовність логічних станів і завершується кінцевим станом. Алгоритму властива детермінованість. Перед виконанням першої операції відомі початкові дані, у будь-який момент часу точно відомі наступні операції (прогнозованість) та результат попередньої операції.

Більшість ймовірнісних автоматів використовують генератори випадкових чисел, які за певними формулами та вхідними даними видають чіткий результат. В чому тоді випадковість? Саме у вхідних даних! Існують два види цих генераторів – випадкові та псевдовипадкові. Випадкові генератори використовують такі величини, які майже неможливо детермінувати. Такі генератори працюють, наприклад, на атмосферному шумі, який формується завдяки ударам блискавки і береться результат створеного шуму. Його неможливо точно визначити, адже за одну секунду по всій земній кулі б'ють сорок блискавок. Псевдовипадкові генератори використовують величини, які можна передбачити. Наприклад, час або сила натиску на кнопку. Можна створити генератор випадкових чисел, який буде в якості вхідних даних приймати швидкість інтернету та визначати результат за математичною формулою. Якщо цей самий генератор буде вимірювати певні величини, то тоді він буде видавати результат лише в деякому діапазоні, з чого випливає, що деякі результати будуть зустрічатися декілька разів, а деякі – ніколи, через те, що значення знаходиться в іншому діапазоні. Це так, але обчислювальний вираз алгоритму можна зв'язати і з іншими величинами. Наприклад, опір у електричному полі та час. Якщо ми будемо проводити множення деякого не зовсім випадкового числа, ще й на опір, який також може змінюватись, тоді значення буде майже неможливо передбачити і воно буде у досить великому діапазоні.

Отже, зв'язуючи автомат з деяким генератором, який вимірює певні величини, та з іншими фізичними чинниками, які впливають на нього, та дію яких досить важко передбачити, можна отримати достатньо випадковий результат. І автомат буде ймовірнісним.

Список використаних джерел

1. Прийма С.М. Теорія алгоритмів: Навчальний посібник. – Мелітополь: ФОП Однорог Т.В., 2018. – 116 с.
2. Панкратов С.. «Законы непредсказуемы» журнал «Наука и жизнь». — М. : Правда, 1988. — С. 75-77.

Науковий керівник — к.ф.-м.н., доцент Якименко Н. М., доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.42; 004.14

Ю. В. Чаговець
студент, Харківський національний університет радіоелектроніки

Про підхід до вирішення проблеми обліку та утилізації пакування з використанням програмного забезпечення для служб доставки

Сучасний стан екології у світі та безпосередньо в Україні є досить невтішним. Серед проблем є глобальні, пов'язані із різноманітними викидами заводів, підприємств та більш локальні, які стосуються кожної людини окремо, а саме мова йде про викинуте кожним із нас сміття. Велика його кількість не доходить до відповідних пунктів утилізації та залишається на звалищах або взагалі просто на вулиці.

Проаналізувавши різні сфери життя людини, особливу увагу привернули служби доставки. Наразі у період всесвітньої пандемії та карантину попит на подібні послуги тільки збільшився. Було виявлено, що сервіси служб доставки мають по собі дуже велику кількість відходів. Кожне відправлення має бути упаковане відповідним чином. Досить велику складність становить розуміння, як подібні речі правильно утилізувати. Зазвичай на пунктах видачі відправлень присутні бокси для відповідного сміття, але мало хто з клієнтів їх помічає, або взагалі розпаковує товар на місці.

Впровадження програмного забезпечення підтримки обліку та доставки утилізації пакування для служб доставки має привернути увагу клієнтів до описаної вище проблеми та заохотити приділити більше уваги на утилізацію пакування від відправлень. Пропонується впровадити програмне забезпечення обліку та утилізації пакування для служб доставки, яке дозволяє: реєструвати у системі та зберігати у базі даних інформацію про клієнта та його відправлення; введення можливості часткової оплати пакування відправлення балами у запропонованому програмному забезпеченні: при оплаті замовлення клієнтом з його рахунку у створеному обліковому записі знімати відповідні бали; при передачі пакування на утилізацію після отримання відправлення - нараховувати відповідні бали у створеному обліковому записі клієнта; при наявності балів на рахунку клієнта в особистому обліковому записі - оплатити пакування наступного відправлення цими балами.

З програмним забезпеченням підтримки обліку та утилізації пакування для служб доставки працюватиме дві сторони - працівник поштового відділення та клієнт. Працівник відповідатиме за оформлення відправлень та відповідно запускатиме процес списання балів з рахунку клієнта, який оплачує відправлення. При необхідній кількості балів, працівник пошти зможе провести оплату пакування списуючи наявні бали клієнта. Клієнт, зі свого боку, має можливість підтвердити утилізацію пакування, що дозволяє нарахувати бали на його рахунок.

Отже, запропоноване програмне забезпечення підтримки обліку та утилізації пакування для служб доставки є корисним та зручним не тільки для самих служб, а ще дає додаткові можливості користувачам та при цьому сприяє більш свідомому використанню та утилізації відповідних відпрацьованих матеріалів, що має позитивно сказатися на стані екології та свідомості людей. Така система є надійною, зрозумілою для звичайного користувача та правильно зберігає й оброблює всю необхідну інформацію.

Науковий керівник — Широкопетлєва М. С., старший викладач кафедри програмної інженерії Харківського національного університета радіоелектроніки.

УДК 004.4

С. О. Шаліков
магістрант, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут»

Model-checking верифікація діаграм станів

Нині багато мережевих застосунків є досить складною розподіленою системою, яка включає роботу багатьох компонентів. У зв'язку з цим, досить складно скласти повну модель системи, яку можна було перевірити методами формального аналізу. Також, постає проблема виконання формальної верифікації такої системи. Для вирішення подібних задач використовується model-checking метод.

"Перевірка моделей – метод автоматичної формальної верифікації паралельних систем з кінцевим числом станів, дозволяє перевірити, чи задовольняє задана модель системи формальним специфікаціям" [1].

Таким чином, даний метод має певні переваги, тому що дозволяє виконати формальну верифікацію моделі без участі людини. У такому випадку, ефективність методу залежить від повноти моделі, яка подається програмі верифікатору.

Дана проблема частково вирішена в існуючих програмних засобах, які автоматично будують модель на основі вихідного коду програми. У даного підходу є певні обмеження: не можна протестувати систему без вихідного коду, чи систему, яка складається з компонентів, реалізованих на різних мовах програмування.

В інших випадків розробнику системи необхідно самостійно описати модель на синтетичній мові програмування. Даний процес передбачає описання моделі у вигляді автомату Мілі. Вимоги до програмного забезпечення записуються у вигляді правил темпоральної логіки. Даний підхід є досить складним, бо потребує від розробника певного досвіду та знань щодо model-checking верифікації [2].

Проблему побудови моделей великих систем можна вирішити, використовуючи моделі інших нотацій. Так UML діаграма станів може бути побудована у вигляді скінченного автомату. Додавши до моделі вимоги, можна виконати подальшу model-checking верифікацію системи.

UML діаграма станів показує поведінку об'єкта у вигляді системи переходів від одного стану до іншого. Загалом, дана діаграма є скінченним автоматом, має всі його характеристики та включає всі його елементи [3]. Перевага UML діаграми станів у тому, що дана нотація підтримує композитні структури, які представляють більш складну поведінку ніж переходи скінченного автомату:

– складений стан – стан з внутрішньою структурою, з вкладеними станами та переходами (стан є автоматом, на діаграмі ізолюється у вигляді окремого стану);

– історичний стан – дозволяє складеному стану пам'ятати останній стан на момент виходу назовні (при наступному переході з зовні на історичний стан процес продовжується з моменту зупинки);

– ортогональний стан – сполучення складених станів, які виконуються незалежно один від одного (паралельно).

Суть методу верифікації полягає в генерації системи переходів LTS (Labeled Transition System), яка відповідає зазначеним елементам на діаграмі станів.

Для реалізації методу було розроблене програмне забезпечення за допомогою рушія vis-network, який надає API для редагування та візуалізації скінченних автоматів. В програмному забезпеченні реалізовані чотири екрани, для кожного з етапів model-checking верифікації:

1) проектування діаграми станів;

2) написання специфікацій;

3) генерація/коригування формальної моделі;

4) верифікація моделі.

На рисунку 1 наведено скріншот роботи програми із зображенням діаграми станів та відповідну їй формальну модель. На діаграмі показано історичний стан gate, вкладені стани node1, node2 та зовнішній стан node3.

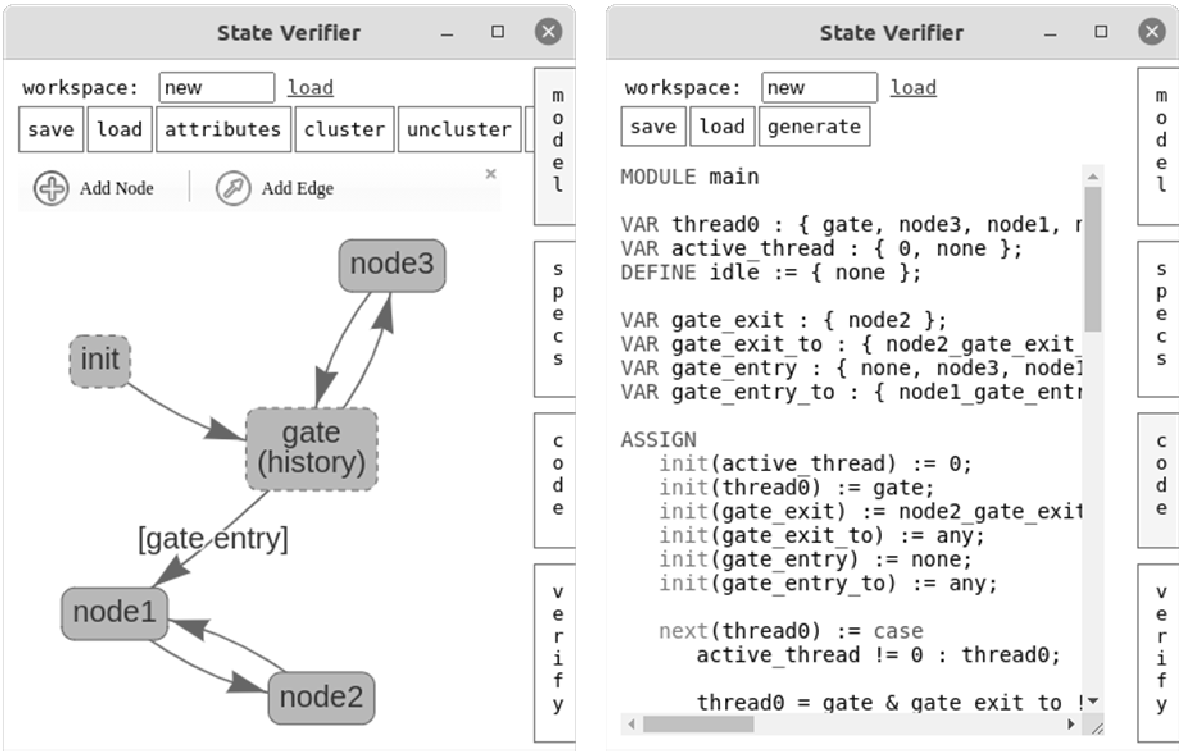


Рисунок 1 – Скріншот роботи програми

Верифікація в програмі виконується за допомогою верифікатору NuSMV [4], у зв'язку з чим формальна модель діаграми станів генерується на синтетичній мові даного верифікатору. Таким чином, верифікацію можна виконувати безпосередньо за допомогою даної програми, описавши формальну модель на синтетичній мові програмування. При достатньому рівні підготовки, розробник може виконувати верифікацію складних моделей.

Розроблене програмне забезпечення перевірки діаграми станів спрощує задачу розробника у порівнянні з верифікаторами простих LTS моделей, оскільки автоматично генерує модель скінченного автомату та складні конструкції типу ортогональних областей та вкладених автоматів.

Список використаних джерел

1. *Верификация и валидация [Електронний ресурс]. – Режим доступу: https://qalight.com.ua/baza-znaniy/verifikatsiya-i-validatsiya/. (дата звернення: 23.11.2020).*
2. *Вельдер С. Введение в верификацию автоматных программ на основе метода Model checking / С. Вельдер, А. Шалыто. – Санкт-Петербург, 2006. – 52 с.*
3. *Граді Б. Мова UML. Керівництво користувача / Б. Граді, Я. Джеймс, Я. Івар. – М.: ДМК Пресс, 2006. – 496 с.*
4. *Cavada R. NuSMV 2.6 Tutorial [Електронний ресурс] / R. Cavada. – Режим доступу: http://nusmv.fbk.eu/NuSMV/tutorial/v26/tutorial.pdf. (дата звернення: 23.11.2020)*

Науковий керівник — канд. техн. наук, доцент Шевченко І. В., доцент кафедри інженерії програмного забезпечення Національного аерокосмічного університету ім. М.Є. Жуковського «ХАІ».

УДК 004.414

Д. М. Шаповалова
студентка, Харківський національний університет радіоелектроніки

Про підхід до виявлення MBTI типу особистості людини за допомогою програмної системи аналізу текстових повідомлень

Психологія на сьогоднішній день є однією з найважливіших наук, що привертає до себе багато уваги оточуючих. Люди прагнуть до самопізнання та самосвідомості. Окрему увагу та популярність серед людей, які починають інтересуватися психологією, має типологія – спроби вчених класифікувати групи людей або психічних властивостей за допомогою виділення ключових характеристик, що відрізняють їх один від одного [1].

Існує багато різних видів психологічної типології, які були винайдені у різні періоди часу: типологія Гіппократа, Дільтея, Ясперса, тест Роршаха тощо. Однією з найбільш популярних видів сьогодні стає індикатор психотипів Маєрс-Бріґґз – MBTI (Myers-Briggs Type Indicator). Це система діагностики індивідуальних відмінностей, яка виникла на основі ідей Юнга [2]. Видатний психіатр і родоначальник аналітичної психології припустив, що сприйняттю людини допомагають чотири основні психологічні функції: мислення, почуття, інтуїція и відчуття. Цю типологію було створено у 1940-х роках та пізніше було підтримано багатьма вченими. Вона складається з чотирьох шкал: тип енергії (EI, екстраверт або інтроверт), тип мислення (SN, сенсор або інтуіт), стиль поведінки (TF, логік або етик) та стиль життя (JP, раціонал або ірраціонал). У залежності від отриманого типу та різних підходів до оточуючого середовища кожним з цих типів можливо підібрати ряд професій, який найкраще підходить людині з даним типом.

Визначення типу за MBTI виконується у форматі самотестування. Людина проходить опитування на певну кількість питань (94, 144 або 167) та відповідає, не втрачаючи багато часу на розмірковування. На сьогодні існує декілька варіацій тесту, які легко знайти та самостійно пройти. Метою даної роботи є не створення нового виду тестування, а можливість передбачити тип людини без необхідності проходити тест. Для цього використовуються соціальні мережі та почтове листування. Соціальні Інтернет-мережі відіграють свою роль у вільному поширенні інформації та завдяки майже цілковитій відсутності певних обмежень для користувачів створюють комфортне плюралістичне середовище для обміну своїми думками та висловлення своїх громадянських позицій [3]. Соціальні мережі стали невід'ємною частиною нашого життя і відображають нашу особистість. Манера спілкування, інтереси, використані слова чи фрази – усе це характеризує людину та її характер. Так само індивідуальні риси характеру можна простежити, проаналізувавши листування з певною людиною.

У ході роботи пропонується створити програмну систему, здатну аналізувати текстові повідомлення користувача та передбачити тип особистості за системою MBTI. Для цього необхідно використати відкриті набори даних з співвідношенням психологічного типу та повідомлень, на основі нейромережевого підходу розробити та навчити на цих даних модель, здатну отримати на вхід текстові повідомлення з мережі Facebook або фрагменти листування через будь-який поштовий клієнт, проаналізувати їх (частоту використання певних слів, побудову речення тощо) та повернути тип особистості, який найбільш чітко характеризує автора цього тексту. На основі цього

функціоналу буде розроблено веб-орієнтовану систему для роботодавців та рекрутерів, які матимуть змогу проаналізувати надані кандидатом соціальні мережі та листи для створення портрету потенціального робітника. Разом з результатом система зможе надавати характеристики кожного з типів, їх слабкі та сильні сторони та підхід до виконання задач для того, щоб допомогти роботодавцю краще зрозуміти свого майбутнього робітника та передбачити можливі проблеми.

Окрему увагу слід приділити виявленню шумів у вхідному наборі даних та валідації цього набору, що може бути реалізовано з використанням фільтрації повідомлень та формування декількох наборів вхідних даних для одного користувача. При цьому в якості функції фільтрації може використовуватися кластер користувача мережі, до якого надходить повідомлення.

Програмна система, що розробляється, буде веб-орієнтованою та буде складатися з клієнтської частини, серверу та створеної моделі обробки даних. Система буде реалізовувати трирівневу архітектуру з шарами відображення даних, їх обробки та доступу до даних.

Для реалізації аналізу текстових даних буде розроблено можливість доступу до публічного API соціальної мережі Facebook, а також обробку текстових повідомлень у форматі csv, які попередньо буде імпортовано з поштового клієнту користувачем системи.

Клієнтська частина буде розроблятися за допомогою мови програмування JavaScript та бібліотек react.js, redux. Серверну частину буде написано мовою Python з використанням фреймворку Django. Для зберігання даних буде використано реляційну базу даних PostgreSQL. Для реалізації моделі аналізу даних необхідно використати спеціальні бібліотеки Pandas, Skipy, Numpy, TensorFlow, PyTorch, а модуль аналізу розробляється мовою Python.

Для реалізації прототипу системи введемо обмеження на використання мов для аналізу повідомлень: для MVP проекту передбачити можливість аналізу вхідних даних лише англійською мовою, що обумовлено наявними наборами даних для навчання моделі, але в подальшому слід розглянути можливості створення нового набору даних різними мовами та їх аналізу, що допоможе локалізувати систему.

Під час написання цієї роботи було запропоновано створення програмної системи аналізу тексту для виявлення типу особистості за індикатором психотипів MBTI. Розроблену систему у подальшому можливо буде використовувати роботодавцями під час пошуку нових співробітників – визначення типу особистості потенціального робітника допоможе краще зрозуміти його характер, переваги та недоліки у роботі. За необхідністю отриманий результат можливо підтвердити або спростувати за допомогою проходження кандидатом тесту на визначення типу за MBTI.

Список використаних джерел

1. *Психологічні типології. [Електронний ресурс] : стаття. URL: https://dic.academic.ru/dic.nsf/ruwiki/1328747 (дата звернення: 18.11.2020).*
2. *Типологія Майєрс-Бріггс: що вона оцінює і як її використовувати HR-фахівцю? [Електронний ресурс] : стаття. URL: https://hurma.work/blog/tipologiya-maj%d1%94rs-briggs-shho-vona-oczinyu%d1%94-i-yak-%d1%97%d1%97-vikoristovuvati-hr-fahivczyu/ (дата звернення: 19.11.2020).*
3. *Вахула Б. Я. Соціальні інтернет-мережі, їхні функції та роль у формуванні громадянського суспільства. Вісник Львівського університету. Серія соціологічна. 2012. № 6. С. 311–319.*

Науковий керівник — Широкопетлєва М. С., старший викладач кафедри програмної інженерії, Харківський національний університет радіоелектроніки.

УДК 004.051

В. С. Шелудяков
студент, Центральноукраїнський національний технічний університет

Практичні способи обробки помилок часу виконання програмного коду засобами мови програмування Erlang

Erlang розроблений компанією Ericsson для використання в телекомунікаційних розподілених системах «м'якого» реального часу. Erlang є універсальною, і одночасно, функціональною мовою програмування з суворою динамічною типізацією. Система часу виконання Erlang досить унікальна і призначена для створення ефективних і відмовостійких систем розподілених обчислень реального часу виконання. Erlang-програми компілюються в байт-код, що виконується віртуальною машиною, причому ВМ може бути кілька на різних вузлах розподіленої обчислювальної мережі. Erlang-системи підтримують гарячу заміну коду, що виключає зупинку систем при установці програмних оновлень. Тому він з успіхом використовується як в телекомунікаційних системах, так і в розробці високонавантажених розподілених веб-додатків. Наприклад: чат Facebook і WhatsApp написані саме на Erlang, який довгий час застосовується в NoSQL-базах даних високої доступності з лінійною масштабованістю – відмовостійких, нереляційних кластерів.

Erlang пропонує засоби (примітиви мови і архітектурні патерни), використання яких значно підвищує стійкість до виникаючих помилок. Проте, це не означає, що створюваний код відразу мегастійкий, але те,– що розробникам доступні хороші засоби для вдосконалення своїх здібностей щодо практичного застосування знань та поглиблення досвіду. Безумовно, що «гаряче оновлення коду» – є незамінно-корисним інструментом, що доречно дозволяє «оновити» сервер без його зупинки.

Віртуальна машина Erlang має свою реалізацію багатопотоковості, свої планувальники, що працюють поверх процесів операційної системи, і вміють створювати і керувати десятками і сотнями тисяч потоків по ~ 2,5 Кб кожен. У кожного потоку своя область пам'яті і свій збирач сміття. Продумано також і відсутність розділеної між потоками пам'яті (керованої за допомогою блокувань) і помилок типу dead lock і race condition. Простіше кажучи: Потоки обмінюються повідомленнями один з одним. При цьому дані копіюються з пам'яті одного потоку в пам'ять іншого потоку. Таким чином, потік ніяк не може зіпсувати чужу пам'ять. І це значно спрощує розробку багатопотокових додатків в цілому.

Коли вся програма виконується в одному потоці, то аварійне завершення цього потоку означає аварійне завершення програми. І, якщо це сталося в місці, де явно непередбачена обробка помилок,– тоді залишається мінімум інформації для діагностики й усунення проблеми. Тому, створюючи продукт, розробники, як правило, намагаються передбачити обробку всіх можливих помилок у всіх місцях їх виникнення. Такий стиль програмування називається Defensive Programming. Дотримання його часто призводить до того, що сама програма містить більше коду для обробки помилок, ніж коду, що виконує основне завдання. Звичайно ж,– це значно ускладнює написання самого коду та його подальшу підтримку.

Тому Erlang пропонує інший підхід: треба чітко реалізувати основне завдання (happy path) минаючи написання частин коду для обробки помилок. Завдяки багатопоточності і поділу потоків на робочі і супервізори,– будь-яка помилка завжди буде помічена і записана у лог. А система в цілому продовжить свою роботу далі. Цей підхід називається Let It Crash. Тим часом, в Erlang є всі інструменти для Defensive Programming. Адже повністю від цього підходу відмовлятися – недоречно. Обидва ці підходи цілком успішно застосовуються в Erlang.

Розробники Erlang розміркували, що буде набагато більш розумним розглядати збій на рівні будь-якої іншої звичайної run-time події. Отже, коли Erlang-процес видає збій, ця ситуація реєструється просто як повідомлення іншого типу, що надходить в поштову скриньку процесу. Усвідомлення переваг такого рішення критичних програмних подій спонукало дизайнерів створити мову з покращеними основними функціями:

В Erlang немає концепції глобальної пам'яті – і всі процеси відносно один одного є ізольованими середовищами виконання;

Процеси Erlang можуть: а)бути породженими дуже дешево; б) спілкуватися між собою тільки за допомогою передачі повідомлень; в) стежити один за одним (це дозволяє організовувати процеси в ієрархії, відомі як «дерева супервізорів»).

Процес повинен виконати своє завдання або зазнати невдачі;

Про збій процесу повідомляється просто – у вигляді повідомлення.

Як в і більшості мов програмування, в Erlang є виключення і спосіб їх перехопити і обробити. Реалізовано три типи винятків і три різні способи їх генерувати.

Основна сила Erlang – якісна реалізація паралелізму виконання завдань. Він має невеликий, але потужний набір примітивів для створення процесів і взаємодії між ними. Процеси є основним засобом структурування додатків Erlang. Вони не є ні процесами операційної системи, ні потоками, а легкими процесами, які плануються виконуючими їх віртуальними машинами. Подібно процесам операційної системи (але відрізняючись від них), Erlang-потоки не мають загального стану один з одним, тому можливо створити безліч автономних процесів без різкого зниження продуктивності.

Хоча Erlang був розроблений, щоб заповнити нішу, і залишався маловідомою мовою протягом більшої частини свого існування, його популярність зростає через попит на паралельні сервіси. Erlang знайшов застосування в розгортанні серверів масових багатокористувацьких рольових онлайн-ігор (MMORPG). Erlang був використаний для написання систем WhatsApp і Facebook-чату. У 2014 році офіційні представники Ericsson повідомили, що Erlang використовується в належних корпорації вузлах підтримки, в мобільних мережах GPRS, 3G і LTE по всьому світу, а також Nortel і T-Mobile. З часу випуску в якості відкритого вихідного коду Erlang поширився за межі телекомунікацій, утвердившись в інших вертикалях, таких як FinTech, Gaming, Healthcare, Automotive, IoT і Blockchain. Крім WhatsApp, серед історій успіху Erlang вказані і інші компанії: Vocalink (компанія MasterCard), Goldman Sachs, Nintendo, AdRoll, Grindr, BT Mobile, Samsung, OpenX, SITA.

На Erlang створено близько 99% відмовостійкого коду використовуваного у всесвітній інформаційній мережі з найменшими витратами щодо його оновлення. А розширення цього надійного засобу (відповідно до основних критеріїв рівня надійності),– дозволяють зручним чином створювати складні системи для якісної обробки критичної інформації, зводячи до мінімуму рівень шкоди їх продуктивності від помилок часу виконання в цілому.

Список використаних джерел

1. *Erlang – язык программирования. https://ru.qaz.wiki/wiki/Erlang_(programming_language).*
2. *Язык программирования Erlang. https://web-creator.ru/technologies/webdev/erlang.*
3. *https://ru.qaz.wiki/wiki/Erlang_(programming_language).*
4. *Эрланг на практике. Способы обработки ошибок. Let It Crash. https://ru.hexlet.io/courses/erlang_101/lessons/practical_erlang_let_it_crash/theory_unit.*

Науковий керівник — к.ф.-м.н., доцент Якименко Н. М., доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.414

С. В. Шемет
студент, Харківський національний університет радіоелектроніки

Функції рекомендаційної програмної системи в галузі зерновирощування

Впровадження ІТ в сферу зерновирощування дозволяє зменшити використання трудових ресурсів, знизити витрати протягом процеса зерновирощування та підвищити врожайність з посівів. Основними факторами, які впливають на вирощування зернових культур в сільському господарстві, є: грунт, зернова культура, погодні умови, своєчасне внесення мінеральних речовин та добрив, своєчасне проведення грунтообробних операцій.

Програмна система «Моніторинг процесів зерновирощування» дозволяє врахувати взаємодії перелічених вище факторів та забезпечити підвищення врожайності з посівів.

Підвищення ефективності використання посівних земель можна досягнути за рахунок впровадження якісної сівозміни (з точки зору прибутковості та покращення якості ґрунту), створення рекомендацій щодо якої є основною функцією системи.

Сівозміна – інтенсивна система землеробства, науково обґрунтоване чергування сільськогосподарських культур і парів у часі і на території або тільки в часі (ротація) за заздалегідь визначеним планом, що супроводжується відповідною системою обробки ґрунту та угноєння [1]. Графік сівозмін в системі представлений в вигляді орієнтованого графу [2], де за допомогою дуг відображається порядок змін культур.

Маючи інформацію про попередні посіви, система за допомогою графу з урахуванням погодних умов, пропонує доступні варіанти засіву ділянок. Кожен з варіантів містить прогнозовану інформацію щодо ймовірного прибутку та впливу на грунт.

Також система дозволяє візуалізувати земельні ділянки у вигляді відміток на карті, що реалізовано з використанням Google Maps API. Кожна відмітка при натиснені відображає інформацію про земельну ділянку, зернову культуру, що вирощується та прогноз погоди з використання інформації з відкритих API.

Окрему увагу слід приділити можливості формування плану грунтообробних операцій та операцій підживлення грунту в залежності від виду культури для певної земельної ділянки, а також планування та облік людських трудовитрат.

В системі здійснюється моніторинг витрат під час грунтообробних операцій на певній ділянці таким чином, що користувач може отримати інформацію про сумарні витрати на кожну ділянку та прогнозований прибуток в кінці зерновирощувального циклу.

Програмна система побудована за шаблоном клієнт-сервер. Для зберігання даних використовується реляційна СУБД MS SQL Server. Серверна частина побудована з використанням .Net Core 3.1. Клієнт побудований за допомогою фреймворку Angular 9.

Таким чином розглянута система дозволить зменшити витрати трудових ресурсів та коштів протягом процесе зерновирощування, а також підвищити врожайність.

Список використаних джерел

1. Гудзь В. П. Землеробство. Підручник. — К.: ЦУЛ, 2010.
2. Оре, Ойстин. Теорія графов. — М.: Наука, 2008.

Науковий керівник — Широкопетлєва М. С., старший викладач кафедри програмної інженерії Харківського національного університету радіоелектроніки.

УДК 004.6

К. В. Шкуренко
магістрант, Центральноукраїнський національний технічний університет

Аналіз систем для зберігання, обробки і управління великими даними

Big Data – досить молоде поняття, яке виникло лише на початку 2000-х років. Розвиток мережі Інтернет та технологій в цілому привели до виникнення величезної кількості даних. Цілком логічно, що постало питання про їх систематизацію, опрацювання та аналізу. Досить швидко великі корпорації збагнули, що дані – одна з найбільших цінностей, що вони мають. Але, хоча цінність даних досить висока, працювати з ними також не легко. Отже, виникла потреба в нових інструментах для роботи з величезними об'ємами даних. Одним з таких інструментів став Apache Hadoop.

Передумови створення Hadoop:

- постійне зростання кількості даних;
- маркетингові цілі обробки даних;
- MapReduce.

Обґрунтування актуальності Hadoop:

- різноманіття постачальників ПЗ (Apache, Cloudera, Hortonworks, MapR);
- використання великими корпораціями (Yahoo, Facebook, Amazon та інші).

Також важливо відзначити актуальність дослідження, що пов`язана з різноманітністю дистрибутивів та систем, побудованих на базі Hadoop. Окрім того, дистрибутиви мають величезну кількість відмінностей, починаючи від швидкості та ефективності виконання тих чи інших дій з певними наборами даних і завершуючи відмінностями у внутрішніх мовах для конструювання запитів. Тож, для вибору конкретного ПЗ для роботи з певним набором даних треба ознайомитись принаймні з найбільш популярними рішеннями, що є на ринку.

Задачі інструментів роботи з великими даними:

- зберігання великих даних (ВД);
- обробка ВД;
- управління ВД;
- візуалізація ВД;
- аналітика ВД.

Що таке Apache Hadoop?

Apache Hadoop забезпечує розподілене зберігання та обробку наборів даних на кластерах з промислового комп'ютерного обладнання. Він дозволяє пришвидшити виконання обробки даних за рахунок використання кластеру для паралельної обробки даних замість одного окремого комп`ютера.

Apache Hadoop виконує такі функції:

- зберігання;
- обробка;
- доступ;
- управління;
- операції над даними.

Apache Hadoop не є єдиним ПЗ, а являє собою набір модулів. Основними модулями є:

- ядро (Hadoop Distributed File System (HDFS) та MapReduce);

- YARN (планувальник завдань та управління кластерами);
- Hadoop Common.

Apache Tez — фреймворк наступного покоління, як альтернатива Hadoop MapReduce.

Інші інструменти: Hive, Pig, Hue, Ganglia, Oozie та Hbase. Гнучка природа Hadoop — модульність, альтернативність модулів, відкрите програмне забезпечення.

Аналіз наборів ПЗ від різних постачальників: Apache, Cloudera, Hortonworks, MapR.

Cloudera: CDH (Cloudera Distribution including Apache Hadoop) — зв'язка найбільш популярних інструментів з інфраструктури Hadoop під управлінням Cloudera Manager. Менеджер бере на себе відповідальність за розгортання кластера, встановлення всіх компонентів та їх подальший моніторинг. Основна перевага — намагання першими надати доступ до нових функцій. Основний недолік — невисока стабільність.

Apache: Hadoop — основний дистрибутив та центральний репозиторій для всіх напрацювань. Основна перевага — велике ком'юніті опен-соурс розробників, швидкість виходу нових функцій, велика кількість курсів та матеріалів для навчання. Недоліки — не завжди актуальна та повна документація, нестабільність.

Hortonworks: HDP (Hortonworks Data Platform). Використовують допрацьовані модулі від Apache. Основна перевага — стабільність.

MapR. На відміну від попередніх ПЗ має безкоштовну урізану версію та повну платну. Переваги — багато оптимізацій, партнерська програма з Amazon.

Кількість підприємств, що використовують великі дані, безперервно зростає. Практика останніх років продемонструвала, що застосування результатів аналізу великих масивів даних може принести реальний ефект.

Компанії обирають Hadoop, щоб збирати складні та різноманітні дані: історія відвідувань веб-сайтів, логи, дані про використання мобільних пристроїв й інформації з соцмереж та багато іншого. Цими даними складно оперувати у СКБД. Можна витягувати структуровані дані з Hadoop для SQL-аналізу, але більш перспективними є такі підходи як машинне самонавчання та інші, що дозволяють співвіднести нові дані зі вже накопиченою, проаналізованою та структурованою інформацією. BI та SQL системи досить добре себе проявили, але постійно виникають нові потреби та нові питання, що виходять за межі поточних можливостей. Окрім того, Hadoop не є одним цілісним ПЗ, а являє собою набір модулів від різних постачальників з різними властивостями. Тож, вибір конкретної реалізації залежить від набору даних та задач які ставляться для їх обробки.

Отже, в результаті проведеного дослідження, було проаналізовано системи для зберігання, управління та обробки великих даних. Були визначені найбільш розповсюджені інструменти що використовуються для цього та встановлені основні їх переваги та недоліки.

Список використаних джерел

1. *Чаллавала Ш., Лакхатария Дж., Мехта Ч., Патель К. MySQL 8 для больших данных / пер. с анг. А. В. Логунова. - Москва : ДМК Пресс, 2018. 226 с.*

Науковий керівник — к.т.н., доц. Босько В. В., доцент кафедри КБіПЗ, Центральноукраїнський національний технічний університет.

УДК 004.8

М. О. Бубела
студент, Центральноукраїнський національний технічний університет

Аналітичний огляд наслідків впливу розробок з застосуванням штучного інтелекту на розвиток суспільства

Штучний інтелект - це одночасно і область науки, і набір обчислювальних технологій. У поняття «штучний інтелект» немає одного чіткого визначення, і це зовсім не заважає його розвитку. Якщо намагатися пояснити, що це, найправильніше буде сказати, що штучний інтелект - це напрямок технологічних розробок, яке робить механізми розумними. А розумні механізми - це ті, які можуть діяти правильно в залежності від обставин [1]. Сьогодні штучний інтелект є одним із перспективних і нерозкритих з достатнім ступенем напрямків розвитку інтелектуальних управляючих систем, тому дослідження питань, пов'язаних із штучним інтелектом є актуальним.

Сьогодні не знайдеться ні однієї галузі, де не намагалися застосувати штучний інтелект. Наприклад, у США на сьогоднішній день жителі вже можуть отримати юридичну консультацію за багатьма питаннями законодавства в робота за лічені секунди. Причому з 85-90% точністю в порівнянні з 70-80% точністю, зробленою людиною юристом [2].

Свої переваги штучний інтелект демонструє також у фабричному виробництві. У результаті заміни роботами 90% працівників фабрики, яка виробляє мобільні телефони, технологічний процес було переведено на цілодобовий режим, продуктивність праці зросла на майже 250%, а кількість браку зменшилася на 80%.

Щодо використання можливостей штучного інтелекту в медицині, то кращого помічника в постановці діагнозу та призначенні саме персоналізованої терапії, заснованої на аналізі великої кількості даних пацієнта, важко знайти. Практики та досвіду лікаря може бути недостатньо для того, щоб своєчасно виявити ту чи іншу проблему в організмі людини, тоді як нейронна мережа, що володіє доступом до величезного обсягу даних, передової наукової літератури і мільйонам історій хвороб, зможе швидко класифікувати будь-який випадок, співвіднести його зі схожими проблемами у інших пацієнтів і запропонувати план лікування. Наприклад, штучний інтелект показує вражаючі результати в рішенні завдання раннього розпізнавання раку шкіри. Машина правильно розпізнала злоякісні утворення в 95% випадків, тоді як люди показали результат тільки в 86%.

Поки штучний інтелект має лише ситуаційне використання в організаційному розвитку. Але якщо спрогнозувати подальше розповсюдження масштабу реалізації штучного інтелекту - автоматизований та керований ним завод виробляє продукцію, інтелектуальний транспорт її доставляє, а електронний магазин реалізує - тоді виникає закономірне питання – яким чином споживачі зароблятимуть кошти для придбання таких товарів та послуг? Крім цього є інші загрози для людини:

- конфлікт між природною і штучною формами мислячого життя;
- знищення інституту суспільності;
- здатність штучного інтелекту до самовідтворення та втрата контрольованості з боку людини.

Зараз штучний інтелект не може передбачити наслідки своїх помилок, оскільки він позбавлений здатності розпізнавати чинники, які знаходяться поза межами автоматизованих алгоритмів, що регулюють життя цивілізації. Багато механізмів з інтелектуальними системами на основі нейронних мереж, що обробляють дані з

використанням глибокого навчання, згодом приймають рішення, часом не зрозумілі й неочікувані самим розробникам. Ніколи не можна бути повністю впевненим у тому, що саме така система знає та вміє. Принцип побудови нейронних мереж і систем глибокого навчання робить їх схильними до особливої поведінки і відповідно зростає база помилок, що допускає штучний інтелект. Це знижує безпеку кінцевого результату роботи будь-якої розумної машини, яка спочатку може бути запрограмована на конкретні дії, а за фактом вчинити на власний розсуд.

З огляду на вищенаведене випливає формування дуже важливої і серйозної науково-практичної задачі на сьогодні, яка полягає в оцінюванні потенційних ризиків від розробок з застосуванням штучного інтелекту і оптимізації їх наслідок.

Необхідність приділяти підвищену увагу питанням безпеки ще примушує розвиток інтелектуальних технологій у військових справах, як [3]:

- функціонування інтегрованих систем розвідки та управління, дистанційно-керованих, розвідувально-ударних бойових комплексів;
- моделювання, ведення бойових дій та обґрунтування складу сил та засобів;
- управління мобільними розподіленими системами бойової охорони заданих кордонів та об'єктів, ударно-розвідувальними безпілотними літальними апаратами.

При розробці інтелектуальних систем на етапі забезпечення можливості раціональної поведінки у складній динамічній обстановці може бути задіяна функція цілевизначення, тобто як стратегія перспективи - формування загальної концепції, яка є реалізацією дії колективного розуму з розумінням проблем і єдністю стереотипів поведінки. Стратегія управління спрощує прийняття рішення і покращує його якість тим, що об'єднує різні знання в єдине ціле та полегшує застосування аналітичних інструментів.

Проте, якщо від ушкодження «мозку» штучного інтелекту в результаті впливу вражаючих факторів можливо вберегтись параметричними та координатними методами, то захист від негативного цілевизначення встановити майже неможливо.

Хоча, на сьогодні спостерігається тільки поступовий розвиток, вдосконалення існуючих досягнень, але складності впровадження систем штучного інтелекту є, і наслідки їх серйозні. Проте перспективи використання штучного інтелекту спонукають шукати рішення для подолання будь-яких перешкод. Тому у планах подальших досліджень у цьому напрямку є формування підходу до питань безпеки щодо наслідок від розробок штучного інтелекту, ідентифікації і формулювання системи принципів, на основі яких мають розроблятись ефективні стратегії управління в інтелектуальних системах відповідального призначення.

Список використаних джерел

1. *Попок Т.В. Штучний інтелект: перспективи та загрози / Т.В. Попок // Студентський вісник національного університету водного господарства та природокористування: – Рівне: НУВГП, 2015. – №.2(4) – С. 252-253.*
2. *Форд М. Пришестя роботів. Техніка і загроза майбутнього безробіття / Мартін Форд; пер. з англ. В. Горбатько. – Київ: Наш Формат, 2016. – 394 с.*
3. *Демідов Б.О. Розвиток та застосування Повітряних Сил, інших видів Збройних Сил України, удосконалення їх системи управління / Б.О. Демідов, Ю.Ф. Кучеренко, О.Г. Матющенко // Наука і техніка Повітряних Сил Збройних Сил України: – Харків: ХУПС ім. Івана Кожедуба, 2018. – № 4(33). – С. 7-15.*

Науковий керівник — Ладигіна О. А., викладач кафедри кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет.

УДК 004.93

Д. Ю. Варченко
студентка, Харківський національний університет радіоелектроніки

Розширення сучасних підходів обробки природної мови

Вступ. На сьогодні обробка природних мов у письмовій формі має дуже вузький напрямок в сторону стилістики текстів. Провідні комерційні компанії світу, основні методи навчання та дослідницькі проекти загалом орієнтовані на такі можливості обробки як: розбиття тексту на речення, розбиття речення на лексеми, тегування лексем (виділення основних морфологічних ознак слів), пошук та ідентифікація омонімії, зазвичай без подальшого коригування, а також глобальна перевірка орфографії та граматики. Відсутність повного аналізу за розділами мовознавства призводить до великої кількості до хиб та помилок.

Обробка текстів, що написані природною мовою (Natural Language Processing, NLP) – загальний напрямок штучного інтелекту і математичної лінгвістики. Основна мета цього напрямку – це вивчення проблеми комп'ютерного аналізу і синтезу текстів природними мовами.

Аналіз та синтез – це дві найважливіші складові, які поєднують мову у письмовій(текстовій) формі та можливості штучного інтелекту її обробити. Широкий спектр можливостей обробки мови за її розділами (графіка, фонетика, словотворення та морфеміка) буде означати створення більш зручної форми взаємодії комп'ютера і людини.

Згідно із концепцією ідеальної обробки природної мови, існує шість рівнів її аналізу і синтезу [1]:

1. Фонологічний – аналіз організації та відтворення звуків у текстовому форматі. Аналіз відбувається за фонетичними, фонемними та просодичними правилами, що вважаються базовими.
2. Морфологічний – аналіз форми та структури слів.
3. Лексичний – аналіз коректного поділу тексту на слова, речення, абзаци та розділи, у порядку «від найоб'ємнішого до найменшого».
4. Синтаксичний – аналіз граматичної структури речення.
5. Семантичний – аналіз контексту речення у тексті.
6. Прагматичний – аналіз речення як частини абзацу.

Результати. Наразі не існує ідеальної концепції або моделі обробки (аналізу та синтезу) природної мови. Сучасні підходи (статистичний, символічний, коннективістський), що збудовані на основі запропонованої концепції потребують або вдосконалення за першими двома рівнями, або їх повного впровадження у нейронну мережу. В будь-якому випадку структура нейронної мережі має бути змінена шляхом відокремлення цих двох рівнів, що робить її універсальною [2].

Алгоритм впровадження фонологічного та морфологічного рівнів наступний:

– створити рівень нейронної мережі виключно для обробки слів;
– при виділенні лексем у реченні заносити їх до даного рівню;
– аналіз слова за його структурою та формою;
– детальний аналіз фонетики та фонетичної транскрипції;
– подальше автоматичне відтворення слова у подальшому аналізі та синтезі текстів.

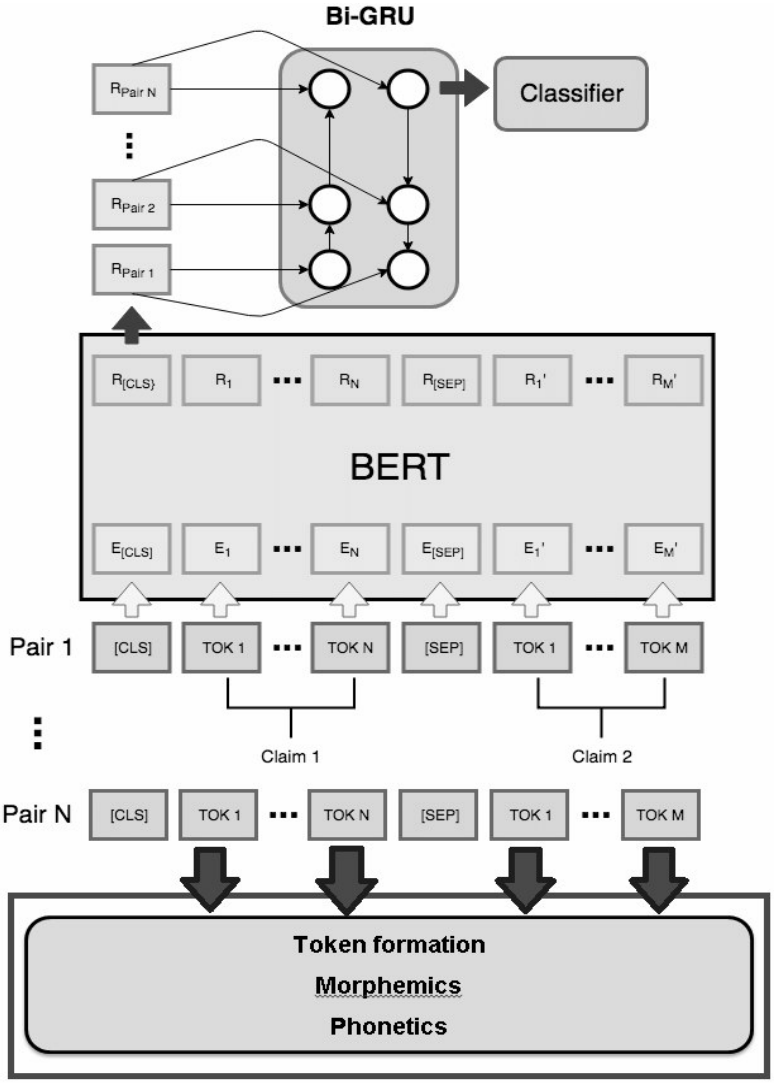


Рисунок 1 – Розширення нейронної мережі першим та другим рівнем обробки на основі моделі BERT

Висновки. Вивчаючи слова як окрему одиницю, нейронні мережі не тільки зменшують кількість хиб та помилок при синтезі речень або цілого тексту, а й відкривають шлях до більш глибинних досліджень етимології слів, схожість між ними не тільки в одній природній мові, а й між іншими. Таким чином, розширення спектру можливостей штучного інтелекту в лінгвістиці і особливо напрямку NLP дозволяє вивчати основи побудови природних мов не тільки в області розділів лінгвістики, а й глобально (діалектизми, архаїзми, неологізми).

Список використаних джерел

1. *Olaronke G. Iroju, Janet O. Olaleke, A Systematic Review in Natural Language Processing in Healthcare // I.J. Information Technology and Computer Science. – 2015. – #8. – P. 45*
2. *Lebret, R., Grangier, D., & Auli, M. (2016). Generating Text from Structured Data with Application to the Biography Domain. Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing. Retrieved from http://arxiv.org/abs/1603.07771*

Науковий керівник – канд. техн. наук Сердюк Н. М., доцент кафедри комп'ютерних інтелектуальних технологій та систем Харківського національного університету радіоелектроніки.

УДК 330.341.1:004

А. М. Гафіяк[1], М. В. Шевченко[2]
[1]*Національний університет «Полтавська політехніка імені Юрія Кондратюка»*
[2]*Науковий ліцей №3 Полтавської міської ради*

Можливості та переваги систем штучного інтелекту

Сьогодні, в епоху всебічного розвитку інформаційно-комунікаційних технологій, штучний інтелект є одним з найперспективніших напрямків серед комп'ютерних наук, який досліджує низку задач та їх розв'язання, деякі з яких не мають способів їх вирішення. Системи штучного інтелекту можуть характеризуються унікальною можливістю самонавчання, самовдосконалення та оперування великим обсягом даних. Сфери застосування таких систем є необмеженими – від роботів, а саме їх створення, обслуговування, супроводження певних дій, які самостійно приймають рішення, вміють виконувати низу операцій, як в реальному часі, так і в режимі офф-лайн тощо [1, 2].

Штучний інтелект характеризується здатністю цифрового комп'ютера або керованого комп'ютером робота виконувати завдання, які опосередковані співпрацею з низкою суб'єктів процесу, пов'язаного з обробкою великого обсягу даних. Згадане поняття зазвичай застосовують до проекту розвитку систем, наділених інтелектуальними процесами, характерними для людини, такими як здатність міркувати, узагальнювати або вчитися на минулому досвіді. Слід зауважити, що визначення поняття «штучний інтелект» найчастіше зводиться до опису комплексу споріднених технологій і процесів, таких як, наприклад, машинне навчання, віртуальні агенти і експертні системи. Системи штучного інтелекту - одна з галузей науки, яка займається дослідженнями, зокрема теоретичними, розроблює і застосовує програмно-апаратні та аналітичні системи і комплекси з елементами штучного інтелекту та моделюванням інтелектуальної діяльності людини [1].

Серед головних напрямів досліджень слід вказати, по-перше розроблення теоретичних засад застосування та створення систем штучного інтелекту різного призначення. Окремої уваги слід приділити питанням аналізу прикладних проблем та теоретичних засад створення інтелектуалізованих робото-технічних систем. Саме моделювання інтелектуальної діяльності людини та застосування в системах штучного інтелекту, на нашу думку, заслуговує більш детального аналізу з точки зору розвитку сучасних інформаційно-комунікаційних технологій. Також важливе місце посідає розробка програмно-апаратних засобів та алгоритмів, методик для систем комп'ютерного розпізнавання та відтворення мовного і зорового образу. Низка вчених займається проблемою моделювання принципів їхнього відтворення та дослідження принципів формування образів на підставі формальної логіки. Через призму розробки інтелектуальних систем керування роботехнічними комплексами та автономними роботами досліджуються окремі напрямки систем штучного інтелекту.

Особливого значення набуває розв'язок низки проблеми розроблення сенсорної інтелектуальної системи розпізнавання. Слід також акцентувати увагу дослідників на створенні й застосуванні сучасних високоінтелектуальних мультимедійних та гіпермедійних технологій і засобів для систем штучного інтелекту, що є передумовою виникнення, створення віртуального середовища з елементами штучного інтелекту, а також проектування та розробки математичних моделей,

заснованих на принципах нечіткої логіки для застосування в системах штучного інтелекту.

Неможливо залишити поза увагою розроблення методів, принципів і архітектурного розв'язання побудови базових знань і технологій їх експортування, що безумовно є важливою складовою експертних та багатоагентних системи. Розвитку набули такі напрями штучного інтелекту, як комп'ютерна лінгвістика і лексикографічні системи, синтез, аналіз і моделювання нейронних мереж, розробка сучасних методів їх проектування, навчання та оптимізації, а також розробка сучасних технологій застосування нейрокомп'ютерів, прикладні системи на основі нейронних мереж[5].

Науковці вважають особливо важливим, сьогодні, досягти того, щоб штучний інтелект міг вирішувати ще більше різноманітних завдань. Але про досягнення рівня людського інтелекту говорити передчасно, оскільки мислення не зводиться тільки до одних алгоритмів. На даному етапі накопичення та аналізу інформації, який зараз досягнутий людством, штучний інтелект відрізняється від мислення людини. Однак в майбутньому можуть виникнути новітні ідеї, які вплинуть на різкий стрибок у розвитку штучного інтелекту.

Зрозуміло, що теорія обчислювальної складності фокусується на класифікації обчислювальних задач відповідно до властивої їм складністю і зв'язуванні цих класів один з одним. Обчислювальна завдання - це завдання, яке вирішується комп'ютером. Завдання обчислення можна вирішити механічним застосуванням математичних кроків, таких як алгоритм. Щоб зрозуміти роль і нинішню хвилю штучного інтелекту в сьогоднішньому і завтрашньому контексті бізнесу і суспільства, важливо поглянути на реалії і технології, які стоять за великим перекриває загальним терміном. Також важливо бачити нинішню хвилю розвитку штучного інтелекту в контексті великих даних, неструктурованих даних, інтеграції та цифрового перетворення. Одна з причин, чому розвиток завдань, що вирішуються засобами систем штучного інтелекту стає настільки актуальною зараз, полягає в тому, що їх інструментарій є зручним і незамінним помічником - для інших технологій і можливостей, які вони пропонують, а саме методи штучного інтелекту. Штучний інтелект вже зробив величезний вплив на розвиток нашого світу, що було неможливо передбачити нещодавно. Механізми його систем ще вивчені недостатньо, але експерти прогнозують, що розвиток систем штучного інтелекту ще більш наблизиться до розвитку людського мозку вже в найближчі роки, що матиме безперечний вплив на розвиток всього суспільства.

Список використаних джерел

1. *Засоби штучного інтелекту: навч. посіб. / Р. О. Ткаченко, Н. О. Кустра, О. М. Павлюк, У. В. Поліщук ; М-во освіти і науки України, Нац. ун-т «Львів. політехніка». — Львів: Вид-во Львів. політехніки, 2014. — 204 с. : іл. — Бібліогр.: с. 200 (11 назв).* — ISBN 978-617-607-692-6
2. *Системи штучного інтелекту: навч. посіб. / Ю. В. Нікольський, В. В. Пасічник, Ю. М. Щербина ; за наук. ред. В. В. Пасічника ; М-во освіти і науки, молоді та спорту України. — 2-ге вид., виправл. та доповн. — Львів: Магнолія-2006, 2013. — 279 с. : іл. — (Серія «Ком'пютинг»). — Бібліогр.: с. 275—278 (58 назв).* — ISBN 978-617-57-40-11-4
3. *Системи штучного інтелекту : навч. посіб. / Г. Ф. Іванченко ; Держ. вищ. навч. закл. "Київ. нац. екон. ун-т ім. Вадима Гетьмана". — К. : КНЕУ, 2011. — 382 с. : іл., табл. ; 21 см. — Бібліогр.: с. 336—337 (26 назв) та в кінці розд. — 255 пр.* — ISBN 978-966-483-544-9
4. *Системи штучного інтелекту : навч. посіб. / С. В. Кавун, В. М. Коротченко; Харк. нац. екон. ун-т. - Х., 2007. - 320 с. - Бібліогр.: С. 316-318.*
5. *Системи штучного інтелекту: нечітка логіка, нейронні мережі, нечіткі нейронні мережі, генетичний алгоритм : монографія / В. П. Лисенко, В. М. Решетюк, В. М. Штепа, Н. А. Заєць, В. О. Мірошник, А. О. Дудник. - Київ : НУБіП України, 2014. - 332 с. - Бібліогр.: С. 331-332.*

УДК 519.1

В. А. Губенко
студент, Центральноукраїнський національний технічний університет

D_{17} -9-ти вершинна граф-обструкція для тора

Розглянемо задачу подання графів-обструкцій роду 2 на 9-ти вершинних, у яких кожне ребро є суттєвим відносно роду при операції видалення ребра, як результату ототожнення по підмножинам множин вершин одного із графів K_5, $K_{3,3}$ та квазізірки з центральним графом G. Наведений в [1] повний список 63-х 2-неприведених графів із 9-ма вершинами; 51 із них (48 міноров) можливо побачити в он лайн PHD-дисертації Hur Suhjin «The Kuratowski covering conjecture for graphs of order less than 10».

Визначення 1. Граф G називається таким, що неприводиться над S, або $\gamma(G)$-неприведеним (irreducible) для S, якщо для будь-якого власного підграфа H графа G має місце нерівність: $\gamma(H)\le\gamma(S)<\gamma(G)$. Множину всіх $\gamma(G)-$ неприведених над S графів позначимо через ζ(S).

Лема 1. Для графу D_{17} як 9-вершинної граф-обструкції для тору має місце наступне φ-перетворення:

1) $\varphi(K_5+St_{1,1.1(2)}(K_4),\sum_{i=1}^{3}(i'+i''))\to(D_{17},\{i\}_{i=1}^{3})$, де $K_5^0=\{i'\}_{i=1}^{5}$, $St^0_{1,1,1(2)}(K_4)=\{i''\}_{i=1}^{3}\cup K_4^0$.

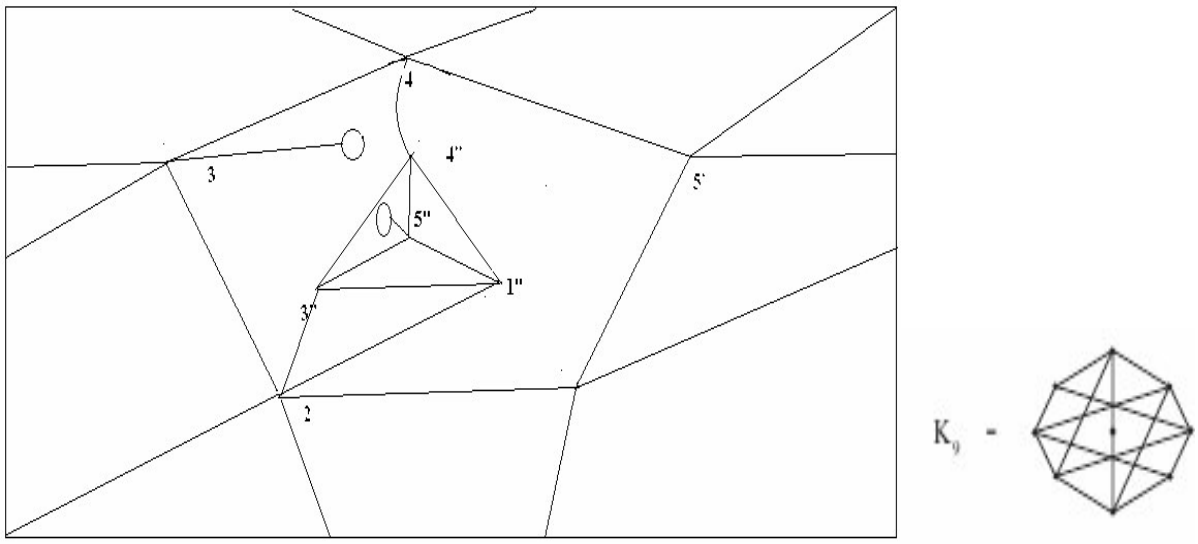


Рисунок 1 – Граф D_{17} 2-неприведений для тору та його доповнення

Таким чином наведено структуру 9-ти вершинного графа-обструкцію для тору з метою використання при побудові багатовершинних графів-обструкцій для тору.

Список використаних джерел

1. *Хоменко М. П. φ-перетворення графів. Препринт ІМ НАНУ, Київ, 1971, 378 с.*
2. *Hur Suhjin «The Kuratowski covering conjecture for graphs of order less than 10». Інтернет-ресурс PhD dissertation,Ohio State University, 2008.*

Науковий керівник — кандидат фізико-математичних наук, доцент Петренюк В. І., доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.65.014.1

В. Ю. Кривохижа
студент, Централноукраїнський національний технічний університет

Переваги та недоліки штучного інтелекту

Вступ. Штучний інтелект (ШІ) застосовується все ширше і впливає на все більшу кількість сфер людського життя, причому вплив це може бути як позитивним, так і негативним.

Основна частина. Переваги штучного інтелекту безсумнівні. Він уже використовується для вирішення актуальних прикладних задач[1]:

- експертні системи допомагають виробляти ефективні рішення там, де не вистачає висококваліфікованих фахівців;

- автономні пристрої досліджують середовища, де людина не може перебувати без шкоди для здоров'я або небезпеки для життя (космос, океанські глибини, зони пожеж або радіоактивних забруднень і т.п.);

- ШІ сприяє мінімізації людського фактора в критично важливих сферах діяльності на монотонних роботах (авіадиспетчер), там, де потрібно багатогодинна зосереджена діяльність (асистент хірурга); на транспорті ШІ використовується для безпілотного управління поїздами, автомобілями, судами, дозволяючи переміщатися тривалий час без перерв на відпочинок водія; користувачам комп'ютерів ШІ надає зручні інтерфейси, що дозволяють віддавати команди і сприймати інформацію в природній формі (розпізнавання і синтез мови).

Разом з тим, ШІ таїть в собі ряд небезпек: в соціально-політичній сфері його застосування може проявитися у вигляді прагнення до тотального контролю; накопичення величезної кількості персональних даних про користувачів комп'ютерних систем веде до обмеження особистих свобод, причому якщо в авторитарних і деспотичних суспільствах у громадян залишається хоча б теоретична можливість чинити опір владі і домовлятися з ними, то в ситуації, коли рішення буде приймати автоматика, люди опиняться перед обличчям сил, які чинять спротив звичайному людському впливу; з точки зору екології ШІ несе небезпеку; людство руйнує навколишнє середовище, але поблизу свого житла люди намагаються підтримувати сприятливі умови; пристрої, що працюють під управлінням ШІ, можуть врахувати не всі екологічні фактори, оскільки менш вимогливі до чистоти навколишнього середовища; застосування ШІ може негативно вплинути і на економіку: скорочення робочих місць внаслідок автоматизації може призвести до різкого зростання безробіття; вже зараз багато професій виявилися під загрозою; наприклад, в зв'язку з впровадженням безпілотних транспортних засобів потрібно менше водіїв.

Висновок. У той же час ряд дослідників вважає, що побоювання, пов'язані з розвитком штучного інтелекту, перебільшені. Боротися треба з людьми-зловмисниками, що використовують потужні комп'ютерні технології в корисливих цілях.ШІ ж як такої поки ніяк не продемонстрував своїх "злих намірів". Це пов'язано з тим, що можливості ШІ з розпізнавання образів і прийняття рішень поки поступаються не тільки людським, але і властивим менш організованим тваринам, наприклад, мурахам.

Список використаних джерел

1. *https://spravochnick.ru/informatika/ponyatie_iskusstvennogo_intellekta/plyusy_i_minusy_iskusstvennogo_intellekta/.*

Науковий керівник — Савеленко О. К., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 519.1

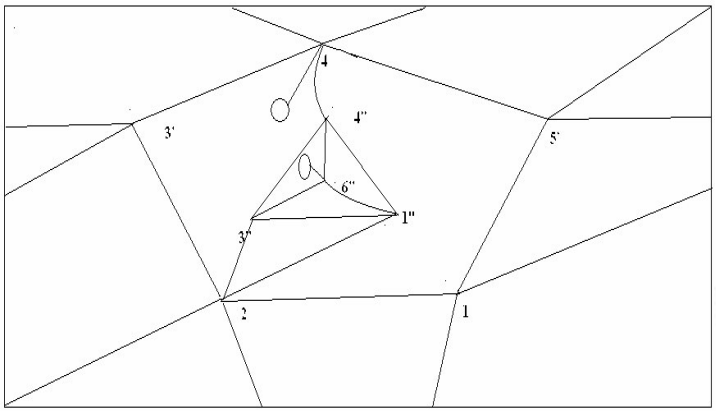
М. Ю. Окунєв
студент, Центральноукраїнський національний технічний університет

Граф D_{18} як обструкція для тора

Задача полягатиме у поданні графів-обструкцій роду 2 на 9-ти вершиннах, у яких кожне ребро є суттєвим відносно роду при операції видалення ребра, як результату ототожнення по підмножинам множин вершин одного із графів K_5, $K_{3,3}$ та квазізірки з центральним графом G. Визначення 1. Граф G називається таким, що неприводиться над S, або $\gamma(G)$-неприведеним (irreducible) для S, якщо для будь-якого власного підграфа H графа G має місце нерівність: $\gamma(H)\le\gamma(S)<\gamma(G)$. Наведений повний список 63-х 2-неприведених графів із 9-ма вершинами; 51 із них (48 мінорів) можливо побачити в [2]. Множину всіх $\gamma(G)-$ неприведених над S графів позначимо через ζ(S).

Визначення 2. Граф G є мінімальний (мінор) над S, якщо для будь-якого графа G', отриманого з графа G видаленням або стисканням довільного ребра, має місце нерівність $\gamma(G)\le\gamma(S)<\gamma(G)$. Множину всіх графів мінімальних над S позначимо через Γ_S. Множина всіх графів, що неприводяться над S містить Γ_S характеризує множину всіх графів рід яких не менше $\gamma(S)+1$.

Лема 1. Для графу D_{18} як 9-вершинного графу-обструкції для тору має місце наступні φ-перетворення: 1) $\varphi(K_5+St_{2(2)}(K_4),\sum_{i=2,4}(i'+i''))\to(D_{18},\{i\}_{i=2,4})$, де $K_5^0=\{i'\}_{i=1}^5$, $St_{2(2)}^0(K_4)=\{i''\}_{i=2,4}\cup K_4^0$-множина вершин графа K_5 із однією розщепленою вершиною.



K_9 -

Рисунок 1 – Вкладення графа D_{18} в 2-тор та його доповнення

Наведено структуру 9-ти вершинного графа-обструкції для тору з метою використання при побудові багатовершинних графів-обструкцій для тору

Список використаних джерел

1. Хоменко М. П. φ-перетворення графів. Препринт ІМ НАНУ, Київ, 1971,378с.
2. Hur Suhjin «The Kuratowski covering conjecture for graphs of order less than 10». Інтернет-ресурс PhD dissertation,Ohio State University, 2008.

Науковий керівник — кандидат фізико-математичних наук, доцент Петренюк В. І., доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.81

Д. О. Пархоменко
студент, Центральноукраїнський національний технічний університет

Доцільність використання інструментів штучного інтелекту в кібербезпеці

Штучний інтелект за останні роки продемонстрував значний прогрес і розвиток, це дозволило створити широкий спектр корисних додатків. Він покращує можливість передбачити і запобігти кіберзлочинам, захищає пристрої з нульовим рівнем довіри, може контролювати навіть старіння паролів.

Сучасні методи штучного інтелекту направлені на виконання кількох завдань, що дозволяють поліпшити системи безпеки і запобігти атакам:

– Виявлення аномалій - завдання, яке визначає нормальну поведінку, потрапляння в певний діапазон, і ідентифікує будь-яку іншу поведінку як потенційну загрозу.

– Виявлення неправомірного використання - протилежна задача, яка ідентифікує шкідливу поведінку, визначається на основі навчання з позначеними даними і пропускає весь трафік, не класифікований як шкідливий.

– Дослідження даних - це метод визначення характеристик даних, часто використовує візуальне дослідження, яке безпосередньо допомагає аналітикам безпеки підвищити «читання» вхідних запитів.

– Оцінка ризику - це ще одне завдання, яке оцінює ймовірність поведінки певного користувача як зловмисника, що може бути зроблено шляхом приписування абсолютного балу ризику або класифікації користувачів на основі ймовірності того, що вони є поганими дійовими особами.

Програмне забезпечення, на якому працюють наші комп'ютери і інтелектуальні пристрої, схильне до помилок в коді, а також вразливе до загроз, які можуть бути використані хакерами. Сучасні системи на основі штучного інтелекту можуть виявляти і усувати ці помилки і вразливості, а також захищатися від вхідних атак. Наприклад, системи штучного інтелекту можуть знайти і визначити, чи можна використовувати підозрілу поведінку коду. У разі виявлення бот самостійно створює «робочий рядок експлойта для захоплення потоку управління», тобто забезпечує захист вразливих місць. Що стосується прогнозування, то в таких проектах платформа штучного інтелекту під назвою AI2 дозволяє прогнозувати кібератаки, постійно використовуючи дані експертів-людей.

Захист від експлойтів нульового дня має вирішальне значення, оскільки цю загрозу рідко помічають одразу. Машинне навчання захищає системи від таких атак, виявляючи шкідливу поведінку, виявляючи ненормальний рух даних та допомагають виявляти шахраїв.

На основі штучного інтелекту створили новий спосіб забезпечення конфіденційності. Цей спосіб пропонує зберігати приватні дані в мережі, одночасно надаючи цілеспрямовані "доказові гарантії" захищеній підгрупі населення та використовуючи алгоритми для дослідження цільових груп населення. Цей тип рішення може бути використаний для спроб знайти схеми або ознаки терористів серед цивільного населення, знайти заражених громадян серед більш здорового населення.

Отже, використання інструментів штучного інтелекту в кібербезпеці різноманітне та перспективне. За допомогою штучного інтелекту простіше визначати, розставляти пріоритети і усувати слабкі місця в системі до того як відбудеться атака. Швидкість реагування штучного інтелекту дозволить ефективніше реагувати на кібератаки.

Науковий керівник — Конопліцька-Слободенюк О. К., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.056+004.8

Д. О. Пархоменко
студент, Центральноукраїнський національний технічний університет

Вивчення загроз використання штучного інтелекту у кібератаках

На сьогоднішній день у світі є дуже актуальним розвиток та використання штучного інтелекту, його застосовують в різних сферах людської діяльності. Штучний інтелект за останні роки продемонстрував значний прогрес і розвиток, це дозволило створити широкий спектр корисних додатків, які допомагають людству.

У міру того як вони почали проникати в більш чутливі області, такі як охорона здоров'я, конфіденційна інформація, секретна інформація, виникли побоювання щодо стійкості системи кібербезпеки.

Штучний інтелект може використовуватися професіоналами в області IT-безпеки для забезпечення належного захисту у сфері кібербезпеки та швидкого знаходження ймовірних кіберзагроз. У той же час зловмисники, злочинні кібербанди і ідеологічні хакери можуть використовувати ті ж методи штучного інтелекту, щоб подолати захист і уникнути виявлення. В цьому і полягає проблема розвитку таких технологій у сфері кібербезпеки.

Адже хакери можуть перешкодити алгоритмам безпеки, націлюючись на дані, на яких вони навчаються, можуть використовувати штучний інтелект для підриву захисту і розробки шкідливого ПО, яке змінює свою структуру, щоб уникнути виявлення. Якщо маніпуляції з даними залишаться непоміченими, організаціям буде складно відновити правильні дані, які використовуються в їх системах штучного інтелекту, з потенційно катастрофічними наслідками.

Головна небезпека штучного інтелекту пов'язана з загрозами міжнародній інформаційно-психологічній безпеці. Зловмисне використання штучного інтелекту може загрожувати безпеці кількома способами:

– злом цифрової безпеки або використання соціально-інженерних підходів на людському або надлюдському рівні продуктивності;

– вплив на нашу особисту безпеку за допомогою використання фізичних впливів;

– вплив на суспільство шляхом усунення конфіденційності, нагляду, профілювання, репресій та використання автоматизованих та цілеспрямованих кампанії дезінформації.

Отже, штучний інтелект це, безсумнівно, великий крок у майбутнє, але разом з цим постає проблема кібератак за допомогою цієї технології.

В результаті вкрай важливо, щоб директивні органи усвідомлювали цю проблему, виявляли вразливі системи і вживали заходів щодо зниження ризику до того, як станеться напад.

Потрібно почати вирішувати цю проблему сьогодні, щоб захистити себе від цих небезпек, створивши програми забезпечення відповідності вимогам безпеки штучного інтелекту. Ці програми створять набір передових практик, які забезпечать прийняття користувачами штучного інтелекту належних запобіжних заходів для захисту від атак. В областях застосування штучного інтелекту з високим рівнем ризику, таких як використання штучного інтелекту в державних установах і в найважливіших галузях промисловості, дотримання вимог може бути обов'язковим і забезпечуватися відповідними регулюючими органами.

Науковий керівник — кандидат технічних наук, доцент Марченко К. М., доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.5

О. О. Пупченко
магістрант, ДВНЗ «Донецький національний технічний університет»

Побудова траєкторії руху колісного транспорту в ігрових додатках

У наш час дуже популярною є тема безпілотних автомобілів, та не менш популярні навчання і вивчення їх поведінки в різних середовищах моделювання. Причина цього є простою – набагато менші фінансові витрати та можливість створення специфічних ситуацій на дорозі, які складно (та дорого) відтворити в реальному житті. Одним з актуальних методів рішення проблеми автоматичного пересування є навчання за допомогою нейронної мережі, які й будуть розглянуто в роботі. Отже, метою роботи є реалізація алгоритму автоматичного проходження автомобілем траси із використанням апарату нейронних мереж.

Як середовище моделювання використовувався ігровий движок (фреймворк) Unreal Engine 4 (UE4) [1]. Він має величезну функціональність, підтримує мову C++, на якій і реалізована нейронна мережа. За замовчуванням в UE4 вже є клас автомобіля з можливістю регулювати його характеристики, але він підтримує лише ручне керуванням. В роботі виконана спроба автоматизувати цей клас, тобто замінити ручне керування на автоматичне із використанням розробленої нейронної мережі.

Для навчання нейронної мережі роботи була потрібна модель траси, для чого з вільного доступу було взято 3D-модель італійської траси для перегонів. В оригіналі вона мала понад 1 500 00 полігонів, що перенавантажувало обчислювальну машину. Тому модель трасу було оптимізовано та зменшено в програмному додатку Blender до 16 000 полігонів. Крім того, модель була доопрацьована з метою розміщення стінок-бортиків уздовж всієї траси, завдяки яким автомобіль може відчувати її межі.

В роботі використано два методи до побудови маршруту автомобіля (рис. 1).

Рисунок 1 – Методи, що використані в роботі: а) метод прямого слідування; б) метод трасування променів

Метод прямого слідування (рис. 1а) полягає в тому, що спочатку будується маршрут з кривих Без`є. Далі на точному постійному віддалені від автомобіля, точно по маршруту, запускаються дві сфери (рис. 2). Розраховуючи кут між напрямом руху автомобіля та положенням сфер можна задавати кут повороту коліс та силу руху вперед-назад. Метод має декілька коефіцієнтів налаштування, для визначення яких й була використана нейронна мережа.

Метод трасування променів передбачає запуск від автомобіля 2 і більше променів в різних напрямках. Промені контактують з перешкодою и виявляють дистанцію до неї.

Далі усі отримані відповіді аналізуються, та приймається рішення про зміщення (поворот) коліс автомобіля. Наприклад, якщо дистанція зліва замала, а справа відносно велика, то автомобілю потрібно повернути вправо. При проведенні експериментів було використано близько 5 променів, а для розрахування коефіцієнтів було покладено на нейронну мережу.

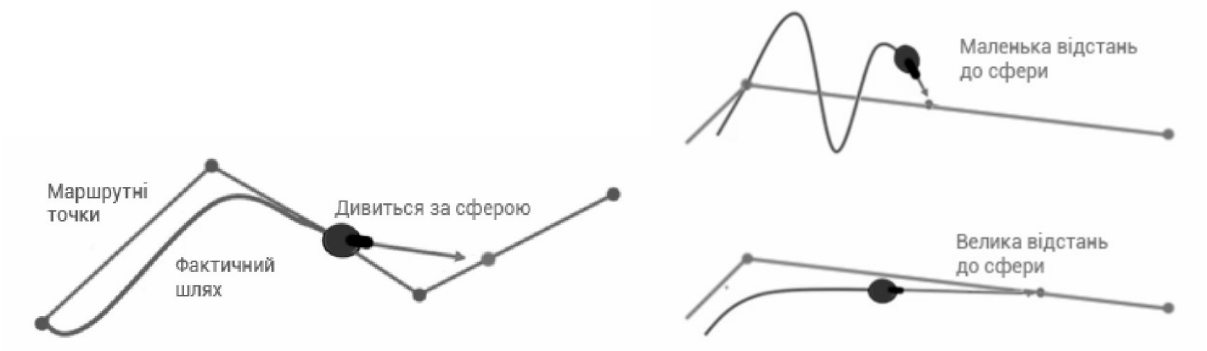


Рисунок 2 – Загальний принцип та окремі випадки
методу прямого слідування

Для використання апарату нейронних мереж в UE4-клас автомобіля був доданий ряд функцій, в яких й було описано роботу нейронних мереж. Спочатку був застосований метод із трасуванням променів. На вхідному шарі мережі було 2 параметри – відстань зліва та справа, на вихідному шари отримувались значення повороту коліс. Швидкість автомобіля була постійною. Після цього на вхідний шар були додані додаткові вхідні параметри та суматор. Відповідно були додані функції активації, збільшено кількість нейронів та розширені скриті шари. Використання нейронної мережі в методі прямого слідування має декілька відмінностей – інша кількість вхідних параметрів, іншій стандартизації даних та кількість вхідних параметрів в нейронній мережі.

Загальним результатом роботи став додаток, де можна порівняти поведінку автомобіля при використанні цих двох методів. Значною перевагою роботи є власна реалізація роботи із нейронними мережами, тоді як серед готових реалізацій можна знайти переважно приклади на мові Python, з використанням бібліотек типу TensorFlow [2]. Завдяки цьому кваліфікаційна робота добре демонструє розвиток від одного нейрона, виконуючого лінійну фільтрацію, до нейронної мережі с багатою кількістю вхідних параметрів та скритими шарами. Крім того, використання, двох підходів дає змогу порівнювати результати між собою.

Перспективним вектором розвитку є тестування інших методів побудови мережі, наприклад з використанням генетичного алгоритму, що може збільшити швидкість навчання мережі. Цікавим буде і гібридний підхід, коли сумісно використовуються метод прямого слідування та трасування променів.

Список використаних джерел

1. *Unreal Engine 4 [електронний ресурс]. – Режим доступу: https://www.unrealengine.com/.*
2. *TensorFlow [електронний ресурс]. – Режим доступу: https://www.tensorflow.org/.*

Науковий керівник — канд. техн. наук, доцент Цололо С. О., доцент кафедри комп'ютерної інженерії ДВНЗ «Донецький національний технічний університет».

УДК 004.56.5

О. О. Середа
студент, Центральноукраїнський національний технічний університет

Проблеми впровадження штучного інтелекту

Штучний інтелект - це одночасно і область науки, і набір обчислювальних технологій. Частково вони створені за зразком людського організму, де нервова система дозволяє нам відчувати, отримувати інформацію, думати і приймати рішення.

За останні 15 років розробки в галузі штучного інтелекту стали частиною повсякденного життя: вони використовуються, наприклад, при створенні комп'ютерних ігор, при обробці та монтажу відеозаписів, в програмному забезпеченні побутової техніки або особистих помічників для мобільних телефонів, які розпізнають голос. При цьому з розвитком штучного інтелекту з'являється і багато нових питань: хто повинен брати на себе відповідальність, якщо безпілотний автомобіль потрапляє в аварію, а інтелектуальний медичний пристрій помиляється? Чим зароблятимуть на життя люди, чиї навички стали не потрібні з появою роботів?

Автономний транспорт уже в найближчі 15 років може стати звичайним явищем. Його розробники пропонують суспільству довірити свою безпеку штучному інтелекту, тому безпілотне обладнання почнуть масово використовувати, коли воно стане для цього досить надійним.

Чим більше технології проникають в життя, тим більше трагічними будуть їх помилки. І хоча у безпілотників буде менше шансів потрапити в аварію, ніж у живих водіїв, на кожен нещасний випадок за участю робота звертатимуть куди більше уваги.

Медицина з самого початку вважалася перспективним напрямком для тих, хто працює зі штучним інтелектом - новітні технології могли б уже в найближчі роки допомогти мільйонам людей. Штучний інтелект - особливо алгоритми глибокого навчання - останнім часом досягло величезного прогресу в автоматичній діагностиці захворювань, зробивши діагностику більш дешевою і доступною. Але для широкого впровадження потрібно, щоб і лікарі, і самі пацієнти почали довіряти штучному інтелекту.

Крім того, людство може почати втрачати навички: відомо, що, коли в школах дозволили використовувати калькулятори, учні стали гірше лічити про себе. Ще «розумні» додатки можуть посилити розрив між різними групами населення. Наприклад, пристрої, які переводять розмови з однієї мови на іншу, гірше розпізнають жіночі голоси, ніж чоловічі, і погано розшифровують фрази, якщо люди вимовляють їх з акцентом. І це лише частина проблем, які можуть виникнути через впровадження штучного інтелекту в життя суспільства.

Питання впровадження штучного потребує всесторонньої уваги та ще багато досліджень, але переваги використання систем штучного інтелекту безумовно цього варті.

Список використаних джерел

1. *Що таке СШІ //[Електронний ресурс]. - Режим доступу: http://ai.lviv.ua/ais/*
2. *4 способа применения искусственного интеллекта в медицине //[Електронний ресурс]. - Режим доступу: https://futurenow.com.ua/ru/prymenenye-yskusstvennogo-yntellekta-v-medytsyne-4-osnovnye-sposoby/*

Науковий керівник — Бісюк В. А., викладач кафедри кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет.

УДК 004.056

В. О. Смутко
студент, Центральноукраїнський національний технічний університет

Застосування інтелектуальних технологій для підвищення ефективності управління інформаційною безпекою

Інциденти інформаційної безпеки є частиною кризових і виняткових ситуацій, які можуть виникати в інформаційній та соціально-технічній інфраструктурі, а також в інформаційно-комунікаційних мережах. Основним завданням для системи управління інцидентами, є найбільш швидке відновлення функціонування сервісів і мінімізація можливих наслідків інциденту на роботу підприємства.

Використовуючи інтелектуальні технології в управлінні інцидентами інформаційної безпеки можна значно підвищити ефективність управління даним процесом. Відомо про чотири інтелектуальних технології: 1) технологія асоціативної пам'яті; 2) технологія структури нейронної мережі; 3) технологія нечіткої логіки; 4) технологія базових експертних систем. Технологія для підтримки прийняття рішень з використанням експертних систем є найактуальнішою в області інформаційної безпеки через її здатність допомогти адміністратору прийняти правильне рішення.

У ролі інтелектуальної системи запропонована інформаційна система, яка підтримує прийняття рішень і працює за наступною інструкцією:

Дані від датчиків безпеки слід аналізувати і оцінювати на наявність відомих шаблонів інцидентів з використанням бази даних інформаційної системи підтримки прийняття рішень.

Інформаційна система яка підтримує прийняття, заснована на аналізі, повинна надавати вказівку для ліквідації причин та наслідків інциденту, якщо його шаблон є в базі.

У разі інциденту, для якого шаблон відсутній у базі, інформаційна система, яка підтримує прийняття рішень надає кілька припущень про подальші дії.

Вживання заходів для уникнення повторення інциденту інформаційної безпеки. Визначено основні чинники, критерії та показники автоматизованих процедур підтримки прийняття рішень в галузі управління інцидентами інформаційної безпеки. При успішному забезпеченні інформаційної системи підтримки прийняття рішень особа, уповноважена приймати рішення по інцидентах інформаційної безпеки, матиме кілька припущень, які будуть включати певні дії на етапі реагування для найшвидшої ліквідації і мінімізації можливих наслідків.

Список використаних джерел

1. *Толюпа С.В. Проектирование систем поддержки принятия решений в процессе восстановления и обеспечения комплексной защиты в информационных системах. // Науково-технічний журнал "Сучасний захист інформації".– 2012. - №4. – С. 69-74.*
2. *Куканова Н. Управление инцидентами информационной безопасности // Открытые системы. — 2006. — № 10. — Електронний ресурс.*
3. *Стандарт ISO/IEC TR 18044:2004 "Менеджмент інцидентів інформаційної безпеки".*
4. *С.В. Гладиш. Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах. Експертні системи та підтримка прийняття рішень. – с. 116-124.*

Науковий керівник — кандидат технічних наук, доцент Марченко К. М., доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.056+004.8

О. С. Ткаченко
студент, Центральноукраїнський національний технічний університет

Застосування штучного інтелекту у галузі кібербезпеки

З кожним роком все більше людей користується інтернетом. За даними International Telecommunication Union [1] порівняно з 2010 роком, коли кількість користувачів інтернету перевищила 2 мільярди, кількість людей, які користуються інтернетом зросла більше ніж у 2 рази, і зараз сягає вже 4,7 мільярди користувачів. І так як все більше людей отримує доступ до мережі, виникає і необхідність захищати користувачів від негативного впливу інтернету. Але звичайно зрозуміло, що так як кількість інтернеткористувачів вже перевищила половину всього населення Землі, і так як кожному вже фізично неможливо виділити свого «персонального» захисника у сфері користування інтернетом і навіть всі існуючі захисники у сфері кібербезпеки навряд чи зможуть забезпечити нормальне функціонування системи захисту даних для всіх. На допомогу кіберфахівцям починає приходити штучний інтелект. Але наскільки це виходить виправдано?

Поява штучного інтелекту як такого, та впровадження його у різних сферах життя створює двобічну ситуацію саме у сфері захисту інформації.

З одного боку технології штучного інтелекту (ШІ) і машинного навчання вже зараз широко застосовуються в інформаційних системах для збільшення продуктивності праці, підвищення продажів, навчання. Їх використання в захисті від кібератак стає одним з ключових напрямків в інформаційній безпеці. Штучний інтелект дає змогу швидше оцінити і обробити данні про небезпеки, проаналізувати поточний стан та прогнозує можливі або навіть вірогідні атаки. Причому він повинен це робити точно, без помилкових спрацювань, щоб не підірвати довіру в себе, і потім коли потрібно буде реальну загрозу відбити, до його прогнозів прислухалися.

Штучний інтелект також відкриває широкі можливості, такі як: інструменти для аналізу розвідувальних даних у величезному обсязі та з нескінченним потенціалом до самовдосконалення через залучення машинного навчання; поліпшення захисту існуючих систем методом пошуку в них прогалин за допомогою штучного інтелекту; оптимізація роботи систем за допомогою вираховування оптимальних та найшвидших варіантів дій; моделювання потенційних ситуацій за допомогою штучного інтелекту та машинного навчання при підготовці кадрів; створення автономних систем для виконання спецоперацій без залучення людського ресурсу, і т. д. [2].

Але є і інша сторона. На поточний момент кількість атак росте, а специфіка загроз змінюється з блискавичною швидкістю. Наприклад, продукти Kaspersky відображають більш 700 млн онлайн-атак в квартал (дані за другу чверть 2019 року) по всьому світу, а Cisco заявляє про блокування 20 млрд мережевих атак в день (більше 7 трильйонів атак за 2018 рік). Очевидно, що при таких обсягах шкідливої діяльності зловмисники активно застосовують засоби автоматизації кібератак, в тому числі використовують технології штучного інтелекту і машинного навчання для їх вдосконалення та трансформації, а також для обходу відомих засобів захисту. Так, наприклад, ефективним прототипом є відомий троян Emotet. Основним каналом для розповсюдження даного вірусу є спам-фішинг, і угруповання, що стоїть за створенням Emotet, могла без особливих труднощів використовувати штучний інтелект для посилення атаки, вбудовуючись в ланцюжки розмов і використовуючи аналіз тексту на природній мові.

У 2019 світовий ринок технологій штучного інтелекту в інформаційній безпеці оцінюється експертами (MarketsandMarkets, Zion Market Research) в $ 8 млрд, з досягненням $ 30 млрд в 2025 році і щорічним зростанням на 23%.

Прогноз обсягу світового ринку технологій штучного інтелекту в інформаційній безпеці на 2019-2025 роки, за даними MarketsandMarkets. Організації, які впроваджують технології штучного інтелекту для поведінкового аналізу і предиктивної аналітики, отримують відчутні результати у вигляді підвищення ефективності виявлення атак, скорочення часу реагування і витрат на організацію безпеки. За даними Capgemini Research Institute, 64% організацій, річний виторг яких складає більше $ 1 млрд, заявляють про те, що технології штучного інтелекту скорочують витрати на виявлення і реагування на загрози національній безпеці, і близько 75% заявляють про скорочення часу реагування (до 12%).

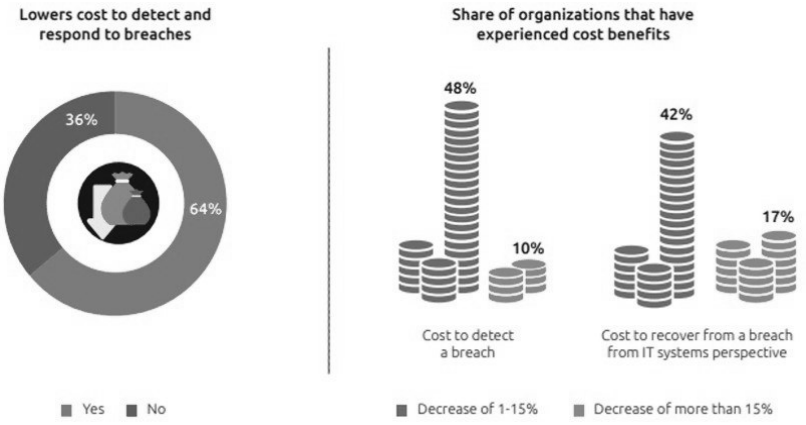


Рисунок 1 – Скорочення витрат на детектування загроз при використанні штучного інтелекту

Підводячи підсумок стосовно застосування штучного інтелекту в інформаційній безпеці робимо наступні висновки:

Штучний інтелект робить достатньо великий внесок в боротьбу з сучасними інформаційними загрозами. Зокрема, в більшості випадків впровадження технологій штучного інтелекту в інформаційній безпеці організації сприяє значному зменшенню часу виявлення проблем та реагування на інциденти, а також зменшує витрати на управління персоналом. Можна відзначати зростання ефективності детектування невідомих загроз, а також швидкості аналізу і виявлення шкідливої активності на кінцевих точках і в додатках.

Також можна відзначати збільшення інвестицій в компанії, які створюють продукти з інформаційної безпеки з застосуванням технологій штучного інтелекту. За останніми даними на кінець 2019 року інвестиції складають $ 3749 мільйонів. При цьому за прогнозом світовий ринок продуктів з інформаційної безпеки з застосуванням технологій II досягне $ 30 млрд в 2025 році з щорічним зростанням на 23%.

Спираючись на це можна однозначно стверджувати, що штучний інтелект є прогресивною галуззю розвитку, зокрема у сфері захисту інформації.

Список використаних джерел

1. *International Telecommunication Union World Telecommunications/ ICT Indicators database. 2019. Режим доступу: https://www.itu.int/en/ITU□D/Statistics/Pages/stat/ default.aspx*
2. *Макс Тегмарк «Життя 3.0. Доба штучного інтелекту» / пер. з англ. Зорина Корабліна. Видавництво «Наш формат», 2019. Розділ 3, підрозділ «Зброя» та «Кібервійна». С. 137–147*

Науковий керівник — кандидат технічних наук, доцент Марченко К. М., доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 519.1

Є. Г. Шевчук
студент, Центральноукраїнський національний технічний університет

Структура графів D_{15} і D_{16} - обструкцій тора

Задача полягатиме у поданні графів-обструкцій роду 2 на 8-ми та 9-ти вершинних, у яких кожне ребро є суттєвим відносно роду при операції видалення ребра, як результат ототожнення по підмножинам множин вершин одного із графів K_5, $K_{3,3}$ та квазізірки з центральним графом G. Наведений [2] повний список 63-х 2-неприведених графів із 9-ма вершинами; 51 із них (48 мінорів) можливо побачити в онлайн PHD-дисертації Hur Suhjin «The Kuratowski covering conjecture for graphs of order less than 10». Граф G називається таким, що неприводиться над S, або $\gamma(G)$-неприведеним (irreducible) для S, якщо для будь-якого власного підграфа H графа G має місце нерівність: $\gamma(H)\le\gamma(S)<\gamma(G)$. Граф G мінімальний (мінор) над S, якщо для будь-якого графа G', отриманого з графа G видаленням або стисканням довільного ребра, має місце нерівність $\gamma(G)\le\gamma(S)<\gamma(G)$. Множину всіх графів мінімальних над S позначимо через Γ_S. Множина всіх графів, що неприводяться над S містить Γ_S характеризує множину всіх графів рід яких не меньше $\gamma(S)+1$.

Лема 1. Для графів D_{15},D_{16} як 9-вершинних графів-обструкцій для тору мають місце наступні φ-перетворення: 1) $\varphi(K_{3,3}+St_{3(2)}(K_{2,3})\cup St_3(9),\sum_{i=1}^{6}(i'\overset{\bullet}{+}i''))\to(D_{15},\{\{i\}_{i=1}^{6})$, де $St_{3(2)}(K_{2,3})\cup St_3(9)=\{i''\}_{i=1}^{6}\cup\{7,8\}$, $St^0{}_3(9)=\{i''\}_{i=1}^{3}$, причому D_5 містить підграф ізоморфний E_3, або E_{18}, що не проективними графами;

2) $\varphi(K_5+St_{1(4)}(K_4),\sum_{i=1}^{4}(i'\overset{\bullet}{+}i''))\to(D_{16},\{\{i\}_{i=1}^{4})$, де $St^0{}_{1(4)}(K_4)=\{i''\}_{i=1}^{4}\cup K_4^0$.

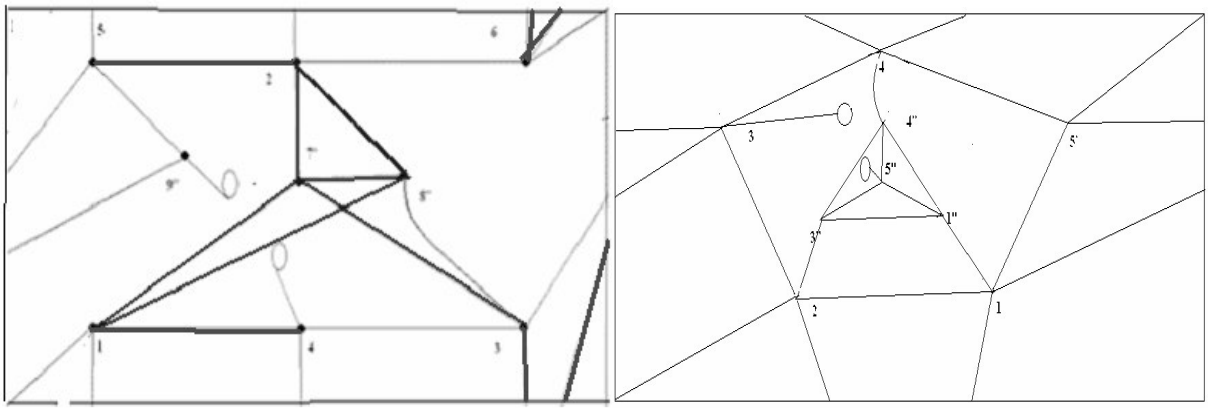


Рисунок 1 – Вкладення графів D_{15},D_{16} в 2-тор

Наведено структуру 9-ти вершинних графів-обструкцій для тору з метою використання при побудові графів-обструкцій для тору.

Список використаних джерел

1. *Хоменко М. П. φ-перетворення графів. Препринт ІМ НАНУ, Київ, 1971,378 с.*
2. *Hur Suhjin «The Kuratowski covering conjecture for graphs of order less than 10». Інтернет-ресурс PhD dissertation,Ohio State University, 2008.*

Науковий керівник — кандидат фізико-математичних наук, доцент Петренюк В. І., доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 04.274

Б. В. Басов
магістрант, ДВНЗ «Донецький національний технічний університет»

Програмна частина системи розумного будинку із голосовим керуванням

Для сучасної людини потрібно створити умови, що дозволяють користуватися смарт-технологіями у повсякденності. Це дозволяє скоротити час, що людина має витрачати кожен день на буденні процеси. Так, об'єктом роботи є створення дешевої системи розумного будинку з голосовим керуванням на базі мікроконтролерів ESP та Arduino, причому в тезах родиться акцент саме на програмну частину такої системи.

Будь-яка система розумного будинку складається з датчиків, центрального модулю, що обробляє інформацію з них, інтерфейсу користувача, та приладів, які керуються системою. Вже навколо цієї основи вибудовуються різні варіації системи розумного будинку. Система складається з серверного модулю (СМ), що отримує інформацію від користувача, та на її основі керує клієнтськими модулями (КМ). До базової схеми було додано діалогову систему, до якої надсилає запити клієнтський смартфон, а вже вона розпізнає, яку команду користувач мав на увазі.

Апаратну частину системи побудовано на платформі мікроконтролерів Arduino Nano, ESP8266 та ESP32, зв'язок між елементами системи виконується через локальну WiFi-мережу завдяки обміну HTTP-запитами від клієнтів до веб-серверу, що розгорнутий на СМ.

Важливим елементом системи є DialogFlow – хмарний сервіс розпізнавання природньої мови від Google [1]. Він дозволяє виділити із звичайної людської мови певні опорні слова, що можуть чітко інтерпретуватися як команди. DialogFlow навчається як на етапі налаштування, так і в процесі її експлуатації, може бути навчена майже будь-чому, особливо на основі типових команд системи розумного будинку.

Алгоритм роботи КМ починається з налаштування EEPROM-пам'яті, тобто її ініціалізації, та підключення до власної WiFi-мережі системи розумного будинку. Потім проводиться читання з пам'яті налаштувань – до цієї інформації входять імена пристроїв та їх стан в системі. Налаштовується UDP-клієнт та починається головний цикл, в якому процес очікує надходження сигналів на UDP-клієнт. В разі наявності пакету на обраному UDP-порту, виконується перевірка, чи є в цьому клієнтському модулі зареєстрований пристрій, для якого цей сигнал - якщо немає, сигнал ігнорується. Якщо один, або більше пристроїв підключених до клієнтського модулю мають таку назву – виконуються команди, що надіслані в цьому повідомленні.

Алгоритм СМ починається з підключення до домашньої WiFi-мережі користувача, ініціалізації власної точки доступу WiFi та не обов'язкового запуску mDNS сервісу. Цей сервіс може використовуватися лише спеціалістом, що знайомий з системою для початкового її налаштування, через власне API. Далі запускається веб-сервер, який буде використовуватися для зв'язку з додатком на клієнтському смартфоні. В основному циклі перевіряється наявність клієнтських модулів та перевірка їх станів. У випадку надходження запиту від користувача, обрані ним команди розповсюджуються на КМ.

Для керування системою з боку клієнта було розроблено мобільний додаток. Схему його роботи наведено на рис. 1. Коли користувач відкриває додаток на смартфоні, додаток перевіряє наявність СМ в домашній мережі користувача. Далі

користувач бачить анімацію та одну кнопку в середині екрану його смартфону – ця кнопка дозволяє почати додатку слухати користувача. Користувач натискає на кнопку, та говорить команду, наприклад “увімкни лампу”. Додаток розпізнає завершення речення та сам перестає слухати користувача.

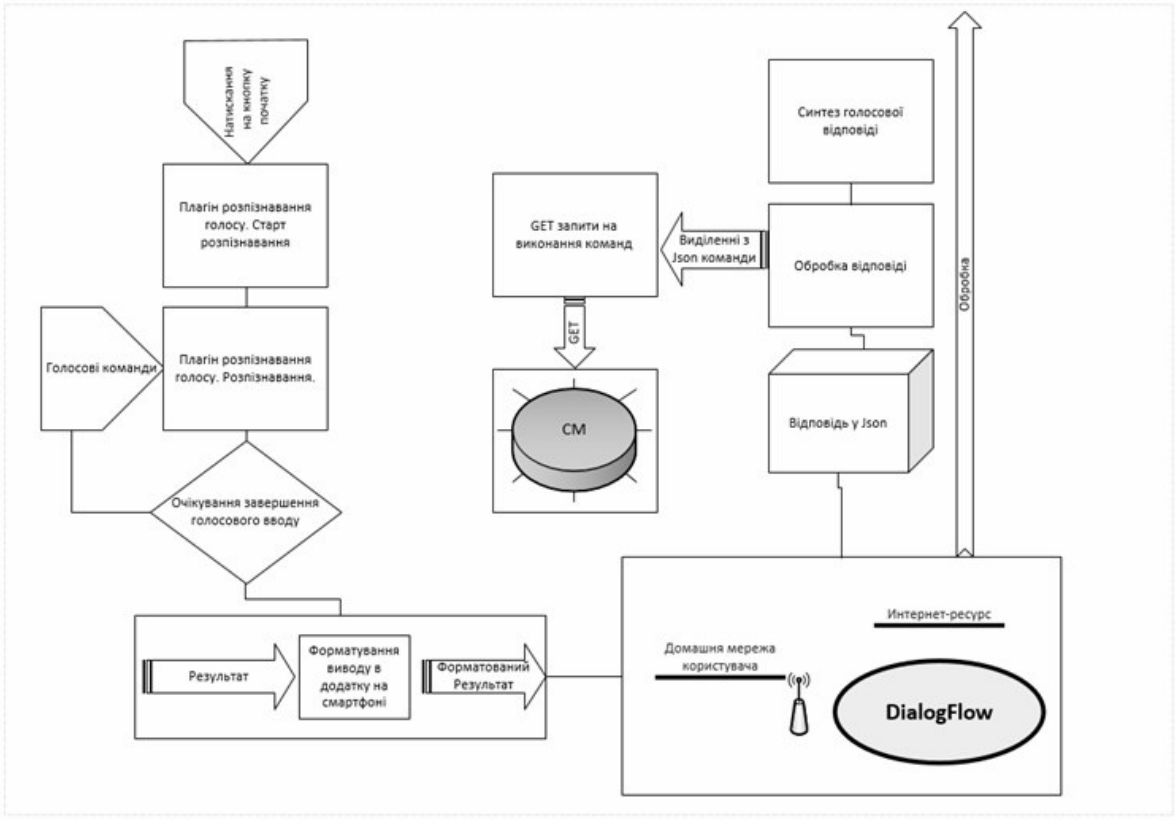


Рисунок 1 – Схема роботи додатку для смартфона

Розпізнаний текст відправляється на аналіз до DialogFlow [1]. Там він розбирається на «сутності» та «значення», які повертаються назад у додаток разом з прийнятною голосовою відповіддю (рис. 2а), що одразу надходить на синтез голосу. Якщо в списку повернених сутностей є одна з команд, що підтримує система, додаток відправляє відповідний цій команді GET-запит на веб-сервер, який розміщений на серверному модулі. В наведеному прикладім випадку буде розпізнано команду на ввімкнення приладу та об’єкт – лампа.

Отже, результатом роботи є програмної частини системи розумного будинку на платформі з мікроконтролерів Arduino Nano, ESP8266 та ESP32. Розроблена система має широкі можливості із вдосконалення та розширення завдяки модульності своєї структури та підтримці веб-запитів на сервері. Такий підхід дозволяє легко створювати засоби керування усіма функціями системи розумного будинку

Список використаних джерел

1. *DialogFlow at Google Cloud Platform [електронний ресурс]. – Режим доступу: https://dialogflow.cloud.google.com/*

Науковий керівник — канд. техн. наук, доцент Цололо С. О., доцент кафедри комп’ютерної інженерії ДВНЗ «Донецький національний технічний університет».

УДК 004.057.4

Р. Е. Бельфер[1], О. С. Савенко[2]
[1]*аспірант, Хмельницький національний університет*
[2]*професор, Хмельницький національний університет*

Архітектура однорангової багаторівневої мережі Layered Peer-to-Peer (LP2P)

При розробці мережі розподіленого реєстру blockchain згідно з протоколом консенсусу "Доказ активності" Proof-of-Activity (PoA) [1], виникла інженерна задача щодо мережевої архітектури яка повинна бути використана при проектування. Класична мережа блокчейн, до прикладу Bitcoin що використовує протокол консенсусу "Доказ роботи" Proof-of-Work [2], базується на архітектурі однорангової Peer-to-Peer мережі. У цьому випадку кожен вузол мережі є рівною одиницею у загальній роботі мережі. Проте для того щоб спроектувати мережу для опрацювання протоколу Proof-of-Activity, потрібно враховувати тип або параметризацію кожного вузла - учасника мережі. Це необхідно для того, щоб слідувати етапам визначеного алгоритму консенсусу у виборі вузла-валідатора.

У проектуванні однорангової блокчейн мережі, яка наслідуватиме протокол консенсусу PoA, необхідною є додаткова деталізація властивостей кожного окремого вузла - саме тому була обрана багаторівнева структура для обробки різних типів та параметрів мережі. Кожен рівень (або шар) містить підмножину вузлів що згруповані за специфічною умовою. Втім мережа досі слідуватиме одноранговому принципу побудови, аналогічно Peer-to-Peer, що робитиме вузли рівними у своїх можливостях. Ця підсилена архітектура може бути класифікована та визначена як багаторівнева однорангова мережа - Layered Peer-to-Peer (LP2P).

Відповідно до кількості та якості активності у мережі, кожен вузол може бути переміщений через рівні, підвищуючи себе та збільшуючи можливість бути обраним до ролі валідатора. Отже відзначимо, що локація вузла у мережі не є статичною та може змінюватися.

Якщо умова $activityIndex(node) \geq index1$ для вузла $node_0K$ правдива, тоді відбувається перетворення: $mode0K \rightarrow node1L+1$. Якщо вузол, розміщений на рівні N, досягає рівня активності, який щонайменше рівний рівню активності $N+1$, цей вузол переміщується до наступного рівня та починає належати до рівня $N+1$. Вузли будуть згруповані базуючись на їхній активності та будуть допущені до участі у виборі вузла для ролі валідатора.

Архітектура багаторівневої однорангової мережі LP2P є структурним шаблоном для проектування мережі що буде використана для розгортання блокчейн системи що слідує протоколу консенсусу Proof-of-Activity. Багаторівнева структура дозволяє розділяти обов'язки вузлів але не обмежує їх можливості для взаємодії. Визначений алгоритм валідації може бути застосований до різних вузлів, які належать різним рівням мережі, з різними визначеними умовами та параметрами. Це дозволяє масштабувати кількість рівнів залежно від вхідних вимог для значної кількості передбачуваних варіантів поведінки.

Список використаних джерел

1. *Belfer R. Proof-of-Activity Consensus Protocol Based on a Network's Active Nodes / R. Belfer, A. Kashtalian, A. Nicheporuk, A. Sachenko, G. Markovsky // Proceedings of the 1st International Workshop on Intelligent Information Technologies & Systems of Information Security. - Khmelnytskyi, Ukraine, June 10-12, 2020. - Pp.239-251.*
2. *Nakamoto, S.: Bitcoin: "A Peer-to-Peer Electronic Cash System". URL:* https://bitcoin.org/bitcoin.pdf. *(дата звернення 17.11.2020).*

Науковий керівник — доктор технічних наук, професор Савенко О. С., декан факультету програмування та комп'ютерних і телекомунікаційних мереж.

УДК 004.7

В. К. Берладін[1], К. О. Буравченко[2]
[1]*магістрант, Центральноукраїнський національний технічний університет*
[2]*старший викладач, Центральноукраїнський національний технічний університет*

Дослідження системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics

Вступна частина. Майбутнє належить флеш-накопичувачам NVMe: уже зараз вони здатні забезпечити набагато більше високі швидкості передачі даних і при цьому порівняно недорогі. А специфікація NVMe over Fabrics відкриває шлях до створення розподілених систем зберігання даних (СЗД) із низьколатентною фабрикою.

Ще в 2011 році була висунута ідея про те, що для роботи із твердотільними накопичувачами потрібний окремий протокол. Спеціально створена галузева група зайнялася стандартизацією функцій, регістрів і набору команд нового протоколу, що одержав назву Non-Volatile Memory Express (NVMe). Якщо відомі протоколи SAS і SATA споконвічно призначалися для механічних пристроїв зберігання даних, то NVMe розроблявся саме для твердотільних накопичувачів NAND. Його поява стала логічним наслідком значно більше високої продуктивності флеш-накопичувачів.

NVMe – протокол для доступу до енергонезалежної пам'яті. Він створювався як один із протоколів для високошвидкісного підключення флеш-накопичувача через шину PCI Express. При її використанні колишній стек на основі SCSI не міг ефективно справлятися з операціями вводу-виводу: занадто багато переривань, тисячі інструкцій центрального процесора на блок даних. Було потрібно не тільки рішення, що дозволило б помітно скоротити число переривань, визволивши процесорні цикли для продуктивної роботи, але й метод передачі даних, що дозволяє по можливості взагалі обійтися без допомоги процесора.

Об'єктом дослідження є процес керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Предметом дослідження є методи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Методи дослідження базуються на методах Big Data, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

–Удосконалено метод керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Основна частина. Якийсь час назад одним з гарячих трендів стало використання SSD-накопичувачів, що підключаються до комп'ютерної шини PCI Express за технологією NVMe, що забезпечує високу продуктивність і низькі затримки. Сьогодні новою точкою росту стає використання специфікації NVMe over Fabrics (NVMe-oF), що, на думку аналітиків, у найближчі роки почне широко впроваджуватися в практику корпоративних рішень. Специфікація NVMe-oF 1.0, що з'явилася в червні 2016 р., по суті є розширенням протоколу NVMe (призначеного для роботи поверх шини PCI Express) на мережі зберігання даних. NVMe-o покликана перенести переваги NVMe у мережі, щоб прискорити перенесення даних між хост-комп'ютерами й системами зберігання даних, що підключаються. Первісний список транспортних опцій NVMe-oF включає RDMA over Converged Ethernet (RoCE) і Fibre Channel (NVMe-FC). В 2016 р.,

були лише перші кроки в освоєнні NVMe-oF, і єдиною областю, де специфікація мала помітну присутність, були пристрою на базі Microsoft Storage Spaces Direct, що використовували NVMe поверх RoCE. Торік на використання NVMe-oF для міжз'єднань стали переходити виробники флеш-масивів, зокрема Kaminario, Pure Storage і куплена Western Digital компанія Tegile.Хоча в питаннях підключень NVMe-oF ще не все пророблено, прогнозується подальше впровадження цієї технології, оскільки пов'язані з нею труднощі полегшуються й нею починають займатися великі вендори. Так, виробники масивів починають брати на озброєння «прискорені» адаптери

NVMe-oF, що дозволяють розвантажити центральні процесори. Іншим важливим напрямком робіт, яким займається фірма NVM Express, є новий транспорт NVMe-TCP для використання NVMe-oF поверх існуючих IP-мереж. Багато хто розділяють більші очікування, що ця розробка значно полегшить застосування NVMe over Fabrics у світі Ethernet. TCP-опція залучить нові кола користувачів, яких раніше, можливо, відштовхували передбачувані складності розгортання NVMe поверх RoCE.

За прогнозами G2M, до 2023 р. ринок NVMe досягне оцінки 60 млрд. дол. завдяки продажам SSD, адаптерів, корпоративних масивів, пристроїв зберігання даних і серверів з урахуванням програмно-обумовлених рішень, розрахованих на використання NVMe. G2M пророкує, що в 2021 р. більшість корпоративних серверів буде оснащене NVMe, а до 2022 р. на NVMe буде базуватися більше 70% флеш-масивів. Поставки адаптерів NVMe-oF до 2023 г. перевищать 1,5 млн. одиниць, і 10% від їхнього числа будуть «прискореними».

Драйвери NVMe-oF для основних ОС поки перебувають у розробці. Тому такі стартапи, як Apeiron Data Systems, E8 Storage і Pavilion Data Systems, часто використовують для підтримки NVMe-oF власні адаптери й драйвери.

Головними сферами використання ранніх продуктів на базі NVMe-oF стали застосунки для аналітики великих даних у реальному часі. Принаймні одне робоче навантаження цього типу, за прогнозами IDC, до 2021 р. буде мати від 60 до 70% організацій зі списку Fortune 2000. Інтерес до NVMe-oF будуть генерувати також власники потужних баз даної, потребуючої низької затримки, зокрема, хмарні вендори, що ущільнюють і консолідують свої ресурси.

NVMe over Fabrics спочатку, очевидно, буде рости по лінії Fibre Channel, повторюючи аналогічну функціональність, представлену в нинішніх дата-центрах. У міру того, як люди будуть знайомитися з технологією, буде розширюватися й використань опцій на базі Ethernet.

Висновки. Таким чином, у даній роботі було проведено дослідження системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. Визначено актуальність цієї задачі. Напрямком подальшого розвитку вважаємо розроблення вітчизняного продукту керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics, який має більш широкі можливості, на відміну від існуючих аналогів.

Список використаних джерел

1. *Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.*
2. *Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.*
3. *Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.*

УДК 004.771

Д. Ю. Бєліков
магістрант, Донецький національний технічний університет

Віддалений доступ до комп'ютера

Вступ. З розвитком технологій все частіше з'являється необхідність віддаленого доступу до комп'ютера. Воно може знадобитися з будь яких причин: надання допомоги в налаштуванні, адміністрування мережі підприємства, спостереження за діями користувача, отримання необхідних даних. Існує багато програмного забезпечення для отримання віддаленого доступу до комп'ютера, що свідчить про інтерес до цієї проблеми як з боку професійних спеціалістів, так і звичайних користувачів. Метою даної роботи є розробка програмного забезпечення (ПЗ), яке дозволяє отримати віддалений доступ до комп'ютера.

Опис розробки та результати. Розроблене програмне забезпечення працює тільки у локальній мережі та підтримує такі функції як, трансляція екрану, файловий менеджер, передача файлів, текстовий чат. Для спілкування з ПЗ можна обрати одну з мов: англійську, українську або російську.

Програмне забезпечення складається з двох частин. Перша запускається на комп'ютері, який потребує віддаленого доступу (клієнтська частина), а друга - на комп'ютері, що надає відповідні послуги (серверна частина). Функціонально обидві частини ПЗ майже ідентичними, а тому, при необхідності, сервер може «перетворитися» на клієнта та навпаки. Підключення до сервера відбувається за допомогою Ip адреси сервера, tcp порту та паролю встановленого на сервері в режимі налаштування ПЗ. Після запуску серверної частини, відразу запускається прослуховування підключень. Встановлений пароль на серверній частині зберігається у файлі, а тому він може бути завантажений, що виключає необхідність постійного налаштування.

Інтерфейс програмного забезпечення клієнтської та серверної частин практично однаковий. Він складається з функцій обрання мови, введення необхідних даних для мережевої роботи та підключення, текстового чату. Інтерфейс клієнтської частини, крім перерахованих, має додаткові функції, такі як перегляд екрану віддаленого комп'ютера, роботу з файловим менеджером обох комп'ютерів та передачу файлів між комп'ютерами.

Структурно до складу ПЗ входять наступні функціональні компоненти (модулі): інтерфейс, керуючий код, інтерпретатор операцій, визначник операції для виконання (тільки на сервері), модуль трансляції екрану, модуль файлового менеджера, модуль передачі файлів, модуль текстового чату, модуль підключення та відключення.

Модуль інтерфейсу виконує функції взаємодії програмного забезпечення з користувачем. Модуль керуючого коду є проміжною ланкою між інтерфейсом та усіма іншими модулями. Він керує роботою усього програмного забезпечення. Модуль інтерпретації операцій відповідає за декодування (якщо потрібно) операцій, які він отримує від серверної та клієнтської частини, після чого, управління дістає модуль визначення операції на виконання. Декодування являє собою генерацію списку необхідних для виконання операцій або підтвердження виконання певної операції. Даний модуль визначає яка операція може виконуватися для одного клієнта у даний момент часу. Компонент трансляції екрану у серверній частині виконує функції по захвату екрану комп'ютера та передачі клієнту, а у клієнтській частині цей модуль виконує прийом та відображення отриманої трансляції екрану. Модуль файлового менеджера у серверній частині відповідає за зчитування інформації про свої логічні диски та об'єкти файлової системи та передачі цієї інформації клієнтській частині. У клієнтській частині даний модуль виконує аналогічні дії, але без передачі іншому

комп'ютеру. Модуль передачі файлів в обох частинах програмного забезпечення однаковий. Він виконує зчитування інформації про файл та сам файл і подальшу передачу на віддалений комп'ютер (клієнтська або серверна частина). Комп'ютер, який виконує приймання файлу та інформації про нього, виконує створення отриманого файлу у необхідній директорії (рис.1). Модуль текстового чату виконує передачу та отримання текстових повідомлень між комп'ютерами. Модуль підключення/відключення у серверній частині відповідає за прослуховування необхідного tcp порту та реєстрацію клієнта на сервері, якщо клієнт надсилає пароль, який не співпадає з паролем серверу, сервер відмовляє у підключенні. Модуль має інструменти для створення додаткових підключень для зареєстрованого клієнта, а також можливість відключити клієнта. У клієнта даний модуль виконує: ініціювання підключення до сервера, передачу пароля для реєстрації, створення додаткових підключень без передачі пароля, відключення від сервера.

Для забезпечення обміну між сервером та клієнтом було розроблено спеціальний протокол. Основу протоколу складає команда. Одна команда співвідноситься з однією або групою операцій, що потребують виконання. Операції розділені по типам: мережеві, файлового менеджеру, текстового чату, трансляції екрану. Операції різних типів можуть виконуватися «одночасно» для одного або декількох клієнтів. Операції одного типу можна виконувати тільки після отримання підтвердження про виконання поточної операції цього типу. Якщо виконується ланцюг операцій різних типів, то кожній операції прописується тип операції, до якого відноситься сама операція, та додатковий тип або типи, які є у цьому ланцюгу. Ланцюг може розділятися на незалежні частини. Ця можливість необхідна при роботі з більш ніж одним клієнтом. Такий підхід дозволяє рівномірніше розподілити час роботи з кожним клієнтом. Модуль вибору операції на виконання фіксує типи операцій, які на поточний момент виконуються для кожного клієнту та самого серверу.

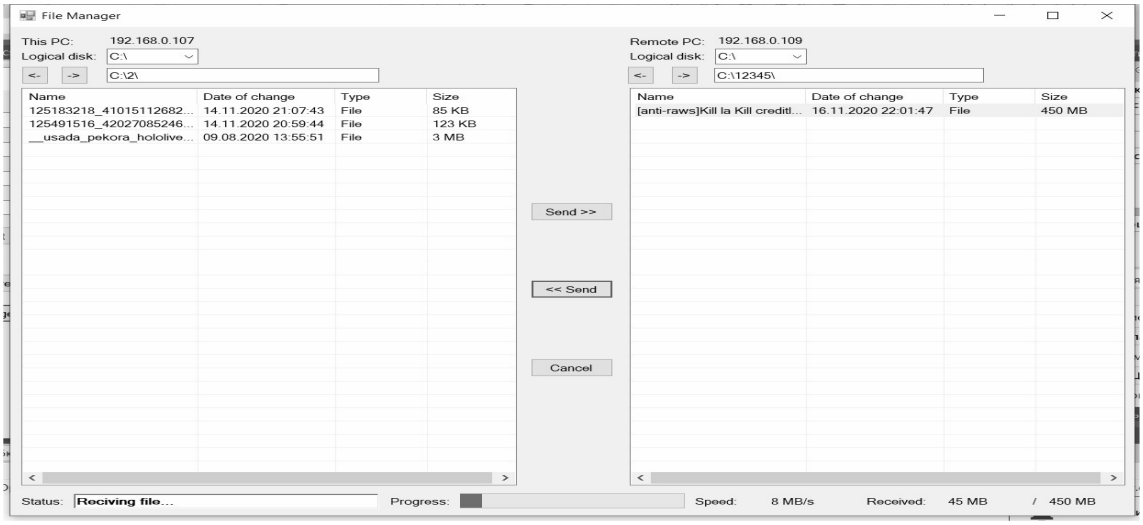


Рисунок 1 – Файловий менеджер, передача файлу

Висновки та перспективи розвитку. Представлене ПЗ віддаленого доступу реалізовано з використанням технології програмування C# , протестоване на апаратно-програмній платформі у складі ПК (процесор AMD Ryzen 7 1700, ОЗП 32Gb, Windows 10 Pro) та ноутбук (процесор Intel Core i3 7100U, ОЗП 8Gb, Windows 10 Pro). Результати тестування підтверджують працездатність ПЗ у відповідності до його функцій. В якості подальшого розвитку пропонується: підтримка шифрування при передачі файлів, реалізація роботи через глобальну мережу.

Науковий керівник — Шевченко О. Г., старший викладач кафедри комп'ютерної інженерії, Донецький національний технічний університет, м. Покровськ.

УДК 004.7

В. І. Головатій[1], К. О. Буравченко[2]
[1]*магістрант, Центральноукраїнський національний технічний університет*
[2]*старший викладач, Центральноукраїнський національний технічний університет*

Дослідження системи моніторингу мережі підприємства на основі комутаторів Nexus 9000

Вступна частина. Проблеми в роботі мережі можуть значно погіршувати якість обслуговування користувачів, знижуючи ступінь їхньої задоволеності мережевими сервісами й породжуючи невдоволення тими, хто надає ці сервіси. Тому надто важливо максимально швидко виявляти, діагностувати й усувати проблеми. Різні системи мережевого моніторингу й діагностичні засоби прискорюють виявлення й аналіз проблем і тим самим сприяють скороченню періоду часу між появою проблеми і її усуненням. Більше того, збираючи й аналізуючи інформацію про роботу мережі, засоби моніторингу дозволяють виявляти можливі проблеми й не допускати їхнього виникнення.

Для забезпечення якості мережевих послуг IT-фахівці усе більше уваги приділяють контролю роботи застосунків і сервісів замість моніторингу стану окремих інфраструктурних мережевих пристроїв. Щоб оцінювати якість роботи сервісів, необхідно захоплювати їх трафік у різних точках мережі (наприклад, до й після балансувальника навантаження, сервера бази даних і ін.) і аналізувати його. Аналіз трафіку здійснюється також для оптимізації роботи мережі, виявлення хакерської активності й в інших цілях.

Підприємства зацікавлені в повному контролі роботи своїх мереж. При цьому збирається й аналізується інформація про обсяги переданого трафіку, що породжують найбільший трафік вузлах, затримках у роботі мережі й застосунків, споживанні смуги пропущення мережі різними додатками й клієнтами й ін. Ці відомості допомагають виявляти ті вузли, які найбільше навантажують мережа й усувати проблеми в роботі застосунків.

Таким чином, виходячи з вищеперерахованого, дослідження системи моніторингу мережі підприємства на основі комутаторів Nexus 9000, є актуальною задачею, яка потребує вирішення у даній роботі.

Об'єктом дослідження є процес моніторингу мережі підприємства на основі комутаторів Nexus 9000.

Предметом дослідження є методи моніторингу мережі підприємства на основі комутаторів Nexus 9000.

Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

–удосконалено метод моніторингу мережі підприємства на основі комутаторів Nexus 9000.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі моніторингу мережі підприємства на основі комутаторів Nexus 9000.

Основна частина. Комп'ютерна мережа є сьогодні практично в кожній процвітаючій фірмі, компанії. Мережа вже не вважається чимсь розкішним, а є прекрасною можливістю ефективно оптимізувати роботу, виробництво, об'єднавши всі комп'ютери в єдину систему.

Стежити за роботою всієї мережі, вчасно реагувати на проблеми допомагає програма моніторингу. З її допомогою керівництво стежить за тим, що відбувається в службових комп'ютерах, як функціонує виробництво, налагоджуються й підтримуються контакти.

Крім цього, програма блокує спам, попереджає вірусні атаки, робить перевірки контенту й файлів, які поступають,. Моніторинг мережі підприємства – це реальна можливість контролювати й убезпечити робочий процес, що пов'язаний з інтернетом і комп'ютерами.

Уже доведено, що неполадки в комп'ютерній мережі легше попередити, ніж потім вирішувати проблеми. Регулярний моніторинг локальної мережі, сервера, мережевих пристроїв дозволяє заздалегідь дізнаватися про можливі неполадки й запобігати їхня поява. Крім того, відслідковуючи історію, адміністратор може дати відомості про частоту появи різних несправностей, що теж є запорукою безпроблемної роботи.

Сьогодні можна виділити два різновиди моніторингу мережі підприємства: оперативний та моніторинг безпеки. На великих підприємствах дані різновиди можуть бути виділені у два процеси, які виконуються окремими фахівцями. У малі ж і середніх фірмах моніторинг звичайно буває загальним. Це правильно, оскільки невелика комп'ютерна мережа не має потреби в скрупульозних оперативних перевірках, вона завантажена не так серйозно й обслуговується простіше. У них немає потреби в докладному аналізі звітів, завдань і тенденцій, які необхідні на великих підприємствах.

Комутатори Nexus серії 9000, представлені в різних типорозмірах, забезпечують високу продуктивність і щільність, низькі затримки й виняткову енергоефективність. Ці комутатори працюють у режимі ПЗ Cisco NX-OS або ACI (інфраструктури, орієнтованої на застосунки) і підтримують передову технологію Cloud Scale ASIC. Вони ідеально підходять для традиційних або повністю автоматизованих центрів обробки даних.

Система моніторингу мережі підприємства на основі комутаторів Nexus 9000 призначена для рішення завдань диспетчеризації й моніторингу об’єктів у комп’ютерній мережі, автоматизованих за допомогою програмно-технічних засобів. Система моніторингу мережі підприємства на основі комутаторів Nexus 9000 виконана в клієнт-серверній архітектурі. Серверна частина системи може бути встановлена на глобальному Інтернет-сервері або локальному сервері. Ніяких спеціальних програм на комп'ютері клієнта (користувача) установлювати не потрібно, досить мати лише Інтернет-браузер і вихід у мережу Інтернет або локальна мережа, залежно від побудови загальної системи моніторингу.

Висновки. Таким чином, у даній роботі було проведено дослідження системи моніторингу мережі підприємства на основі комутаторів Nexus 9000. Визначено актуальність цієї задачі. Напрямком подальшого розвитку вважаємо розроблення вітчизняного продукту моніторингу мережі підприємства на основі комутаторів Nexus 9000, який має більш широкі можливості, на відміну від існуючих аналогів.

Список використаних джерел

1. *Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.*
2. *Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.*
3. *Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.*

УДК 004.7

Л. В. Марченко[1], К. О. Буравченко[2]
[1]*магістрант, Центральноукраїнський національний технічний університет*
[2]*старший викладач, Центральноукраїнський національний технічний університет*

Дослідження системи відеоспостереження на основі бездротових камер і каналів LTE

Вступна частина. Сучасні мережні відеокамери мають убудовані функції відеоаналітики, а програмне забезпечення, здатне вирішувати різноманітні завдання відеоспостереження, містить у собі системи моніторингу й керування записом, а також відеоклієнти з підтримкою різних пристроїв. Сама система відео спостереження – один з найбільше швидкозростаючих сегментів світової галузі ІТ.

Системи відеоспостереження впроваджуються на транспорті, у комунальному господарстві, готельній галузі, промисловості, держустановах, спортивних і розважальних центрах, у комерційних організаціях. Вони використовуються для рішення завдань бізнесу й забезпечення безпеки. По оцінках аналітиків IHS, в 2021 році обсяг світового ринку відеоспостереження становив 13,5 млрд доларів, причому мережне відеоспостереження переважало над аналоговим – зараз біля половини продажів доводиться на мережне відео.

Як очікується, до 2023 року частка останнього перевищить три чверті ринку, а його сукупний обсяг збільшиться до більш ніж 24 млрд доларів. Середньорічні темпи росту можуть досягти 22% по мережному відеоспостереженню й 12% по ринку відеоспостереження в цілому. По даним Intel, світовий ринок IP-відеоспостереження росте в середньому на 24% у рік, ще швидше зростає обсяг генеруємих цими системами даних.

Таким чином, виходячи з вищеперерахованого, дослідження розгалуженої системи відеоспостереження на основі бездротових камер і каналів LTE, є актуальною задачею, яка потребує вирішення у даній роботі

Об'єктом дослідження є процес відеоспостереження на основі бездротових камер і каналів LTE.

Предметом дослідження є методи відеоспостереження на основі бездротових камер і каналів LTE.

Методи дослідження базуються на методах обробки відеоданих, методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод відеоспостереження на основі бездротових камер і каналів LTE.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі відеоспостереження на основі бездротових камер і каналів LTE.

Основна частина. Широке поширення IP-камер з функціями відеоаналітики й зберігання інформації може стати каталізатором росту даного сегмента й консолідації ринку великими гравцями.

Серед технологічних аспектів розвитку систем відеоспостереження можна виділити підвищення продуктивності мікропроцесорів для відеокамер, збільшення ємності кеш-пам'яті й швидкості її роботи. Потужності сучасних процесорів досить для

інтелектуальної обробки зображення й виконання аналітичних додатків безпосередньо в камері.

Відкритість для інтеграції – ще один важливий тренд, що відкриває можливості побудови комплексних систем різного масштабу. Все більшою популярністю користуються мобільні рішення й керування системами відеоспостереження зі смартфонів і планшетів.

Хмарне відеоспостереження (VSaaS) – зберігання відеоархіву в хмарі – дає такі переваги, як резервування, масштабованість і перенос капітальних витрат на поточні операційні витрати. Простота установки, налаштування й експлуатації як апаратної, так і програмної складових систем відеоспостереження – ще одна очевидна тенденція, обумовлене ростом популярності мережних рішень і необхідністю зниження витрат.

Ключовою тенденцією залишається підвищення якості зображення. Сучасні мережні камери навіть в умовах недостатньої освітленості забезпечують відмінну деталізацію й передачу кольору.

Тим часом технології відеоаналітики стрімко розвиваються, відкриваючи можливості для рішення різноманітних завдань. Убудована відеоаналітика дозволяє значно знизити вартість мережної інфраструктури й систем зберігання, а виходить, скоротити бюджет проекту відеоспостереження, адже передавати відео можна лише при виявленні значимих подій, а не транслювати весь відеопотік.

На відміну від сервера, на який надходить безліч відеопотоків, процесору камери досить обробляти всього один потік, причому мова йде про незжатий відео будь-якого розрішення – до 4/8K. Тим самим не тільки підвищується якість виконання аналітичних завдань, але й виключається етап декодування відео на сервері для застосування засобів аналітики. Зараз убудована відеоаналітика застосовується лише в декількох відсотках інсталяцій, але згодом ця частка може вирости до 20-30%, і навіть до 50%. Серверна відеоаналітика залишається важливою технологією для реалізації алгоритмів, які поки не можна реалізувати в програмному забезпеченні камери

Функціонально система складається з наступних блоків:

–Блок функцій оператора розгалуженої системи відеоспостереження на основі бездротових камер і каналів LTE.

–Блок функцій інженера розгалуженої системи відеоспостереження на основі бездротових камер і каналів LTE.

–Блок функцій адміністратора розгалуженої системи відеоспостереження на основі бездротових камер і каналів LTE.

Висновки. Таким чином, у даній роботі було проведено дослідження системи відеоспостереження на основі бездротових камер і каналів LTE. Визначено актуальність цієї задачі. Напрямком подальшого розвитку вважаємо розроблення вітчизняного продукту відеоспостереження на основі бездротових камер і каналів LTE, який має більш широкі можливості, на відміну від існуючих аналогів.

Список використаних джерел

1. *Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.*
2. *Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.*
3. *Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.*

УДК 004.4

Т. В. Селіванов
студент, Центральноукраїнський національний технічний університет

Дослідження застосування віртуальних виділених серверів при розробці та обслуговувані веб-додатків

В даний час сайт компанії є одним з головних інструментів позиціювання її на ринку і надання інформації про поточну діяльність для партнерів і клієнтів. Сайт може складатися з різних файлів: текстових, графічних і т.д., може містити скрипти. Дані файли мають певний обсяг, тому вимагають місце для зберігання. Водночас вони повинні бути постійно доступні користувачеві. Постає задача розміщення файлів в глобальній мережі. Тому буде актуальним дослідити хостинг на недоліки та переваги в порівнянні з іншими способами.

Віртуальний виділений сервер - VPS або VDS - це один з видів хостингових послуг, в рамках яких користувачу надається віртуальний виділений сервер [1]. Управління операційною системою здійснюється таким же чином, як і в ситуації з фізичним виділеним сервером; VPS може бути налаштований довільно. VPS хостинг - це вид хостингу, при якому на одному фізичному сервері створюється кілька віртуальних серверів, які працюють незалежно і за своїми функціями нічим не відрізняються від фізичного сервера, крім обмежень в потужності [2].

Віртуальний виділений сервер характеризується стабільною і надійною роботою. Віртуальні виділені сервери, розташовані на одній хост-машині, працюють незалежно один від одного. Таким чином, несправності функціонування одного сервера не вплинуть на роботу іншого. Збоями в роботі самої хост-машини займаються фахівці майданчика, на якому вона встановлена, усуваючи проблеми в найкоротші терміни. Крім цього, віртуальні виділені сервери гарантують високий ступінь безпеки конфіденційності для розміщуваних даних.

До переваг можна віднести, по-перше, налаштування сервера під умови конкретного веб-проекту [1]: установка необхідного програмного забезпечення, зміна операційної системи і т. д . По-друге, віртуальний виділений сервер незалежний, тобто розташовані на одній хост-машині віртуальні сервери працюють ізольовано один від одного, використовуючи виділені для них ресурси, для кожного надані окремі IP адреси, в той час як на звичайному віртуальному хостингу кілька сайтів нерідко використовують одну IP-адресу.

До недоліків використання VPS можна віднести більш високу ціну в порівнянні з віртуальним хостингом. Вартість оренди віртуального хостингу порівняно нижча, ніж вартість оренди віртуального виділеного сервера.

Таким чином, в даний час послуга VPS - хостингу динамічно розвивається, хоча спочатку спостерігався деякий дефіцит пропозицій щодо її надання. Вибір надійного хостингу з високою якістю сервісу і оптимальною вартістю непросте завдання, яке вирішує керівник веб-проекту, від його рішення в кінцевому підсумку залежить ефективність функціонування сайту.

Список використаних джерел

1. *Уткина Л. И. Возможности виртуального выделенного сервера в поддержке сайта компании // 2017. [Електронний ресурс] // - Режим доступу: https://cyberleninka.ru/article/n/vozmozhnosti-virtualnogo-vydelennogo-servera-v-podderzhke-sayta-kompanii.*
2. *Сорокіна Ю. А. Інформаційно-аналітичне забезпечення у сфері керівництва і бізнесу [Електронний ресурс] // 2013. – № 2. - Режим доступу: http://journal.mrsu.ru/arts/informacionno-analiticheskoe-obespechenie-v-sfererukovodstva-i-biznesa.*

Науковий керівник — Константинова Л. В., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.7

Є. В. Смоляр
магістрант, Центральноукраїнський національний технічний університет

Дослідження системи управління інфраструктурою на основі рішень SD-WAN

Вступна частина. На сучасному рівні існує кілька тенденцій, що визначають нові вимоги до організації територіально розподілених мереж (WAN). Одна з них – перехід до гібридних IT-середовищ, коли необхідні для роботи додатків ресурси можуть перебувати на віддалених площадках, включаючи власні ЦОДи замовника, приватні хмари в комерційних ЦОДах і публічні хмари. При цьому необхідно забезпечити оперативне підключення нових мережних сервісів і нових вузлів (філій), що вкрай складно зробити на основі традиційних технологій WAN. Тому все частіше замовники звертаються до програмно обумовлених рішень SD-WAN, у яких мережна взаємодія підкоряється вимогам з боку додатків. У пропонованого SD-WAN-рішення є ряд унікальних особливостей. Зокрема, ця наявність конвергентного пристрою SD, що сполучить функції шлюзу SD-WAN і WAN-оптимізатора. Шлюзи SD-WAN мають убудовану функціональність міжмережевого екрана й захисту від погроз. Ще одна цікава особливість рішення – можливість об'єднання в програмно обумовленій мережі як WAN-, так і LAN-складових, до останнього ставляться комутатори локальної мережі й точки доступу Wi-Fi. Істотне посилення своєї пропозиції в частині побудови локальних мереж вийшло завдяки використанню унікальних масивів, що містять кілька точок доступу із секторними антенами й убудованим контролером. Такий масив може обслуговувати тисячі користувачів і дуже ефективний там, де необхідні рішення високої щільності. Продукт, крім відмінної масштабованості, відрізняються ще гнучким вибором моделей впровадження: так, система керування може бути розміщена в приватній або публічній хмарі. Таким чином, виходячи з вищеперерахованого, дослідження системи управління інфраструктурою на основі рішень SD-WAN, є актуальною задачею, яка потребує вирішення у даній роботі.

Об'єктом дослідження є процес управління інфраструктурою на основі рішень SD-WAN.

Предметом дослідження є методи управління інфраструктурою на основі рішень SD-WAN.

Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

–Удосконалено метод управління інфраструктурою на основі рішень SD-WAN.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі управління інфраструктурою на основі рішень SD-WAN.

Основна частина. Мережі SD-WAN приходять на зміну застаріваючим традиційним територіально розподіленим мережам, як колись смартфони потіснили звичайні мобільники. Відповідно до досліджень Gartner, більше 36% великих компаній планують почати користуватися SD-WAN до кінця 2020 року. І щороку кількість мереж SD-WAN буде рости в середньому на 65%. Рішення SD-WAN – це перший великий крок у реалізації концепції програмно обумовлених мереж SDN стосовно до територіально розподілених мереж. Ідея програмувальних мереж (Software-Defined Network, SDN) полягає в тому, що функції контролю й керування виконуються не

безліччю мережних пристроїв, а контролером SD-WAN. SD-WAN дозволяє відмовитися від складного керування кожним мережним пристроєм за допомогою командного рядка (Command Line Interface, CLI) на користь централізованого: контролер SD-WAN розсилає налаштування всім пристроям за допомогою спеціального протоколу (SNMP, NETCONF і т.п.) і відслідковує стан маршрутизаторів і каналів зв'язку.

У концепцію SD-WAN споконвічно була закладена підтримка будь-яких каналів: L3VPN, Інтернет, LTE і ін. По-перше, це зручно з погляду моніторингу: адміністратор мережі бачить на панелі управління контролера актуальний стан всіх каналів поза залежністю від їхнього типу. Але ця не найбільша перевага. Вартість каналів Інтернету постійно знижується, а доступна смуга пропущення збільшується. Зараз за ту ж ціну можна орендувати канал із пропускною здатністю в 10 разів більше, ніж 10 років тому, і найчастіше по якості він не буде уступати виділеному L3VPN, для якого оператор надає гарантований рівень обслуговування. Тому з появою SD-WAN стали можливі відмова від оренди дорогих каналів L3VPN і використання каналів Інтернету від різних провайдерів зі збереженням необхідної якості обслуговування. Мережа SD-WAN постійно відслідковує стан всіх каналів по різних параметрах і перемикає трафік критичних додатків з каналу на канал, якщо якість зв'язку виявляється нижче заданого порога.

Функціонально система складається із наступних блоків:

–центрального блоку;

–агентів спостереження.

Центральний блок складається з наступних блоків, які взаємодіють один з одним згідно структурної схеми: Планувальник, який визначає які зв’язки потрібно коригувати, або які вузли необхідно внести. База даних. Блок інтерфейсу ручного вводу. Блок відображення структури та характеристик мережі на основі рішень SD-WAN. Блок обчислення розрахункових значень. Блок виміру параметрів. Блок обробки статистики, передачі трафіку у мережі на основі рішень SD-WAN. Формули розрахунку мережі на основі рішень SD-WAN, які дозволяють на основі використання розробленої математичної моделі мережі на основі рішень SD-WAN, з використанням методів та формул теорії масового обслуговування та теорії статистики, розраховувати навантаження трафіку на кожний вузол мережі на основі рішень SD-WAN.

Висновки. Таким чином, у даній роботі було проведено дослідження системи управління інфраструктурою на основі рішень SD-WAN. Визначено актуальність цієї задачі. Напрямком подальшого розвитку вважаємо розроблення вітчизняного продукту управління інфраструктурою на основі рішень SD-WAN, який має більш широкі можливості, на відміну від існуючих аналогів.

Список використаних джерел

1. *Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.*
2. *Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.*
3. *Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.*

Науковий керівник — доктор технічних наук, професор Смірнов О. А., завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.7

О. О. Юхимчак
магістрант, Центральноукраїнський національний технічний університет

Дослідження системи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture

Вступна частина. Індустріальний інтернет (індустріальний інтернет речей, промисловий інтернет, Industrial Internet of Things, IIoT) – концепція побудови інфокомунікаційних інфраструктур, що припускає підключення до мережі Інтернет будь-яких непобутових пристроїв, устаткування, датчиків, сенсорів, автоматизованої системи управління технологічним процесом (АСУ ТП), а також інтеграцію даних елементів між собою, що приводить до формування нових бізнес-моделей при створенні товарів і послуг, а також їхній доставці споживачам. Ключовим драйвером реалізації концепції «Індустріального інтернету» є підвищення ефективності існуючих виробничих і технологічних процесів, зниження потреби в капітальних витратах. Ресурси компаній, що вивільняються таким чином, формують попит на рішення в сфері Індустріального інтернету. У систему інтернету речей сьогодні утягуються всі необхідні для його функціонування ланки: виробники датчиків і інших пристроїв, програмного забезпечення, системні інтегратори й організації-замовники (причому як B2B, так і B2G), оператори зв'язку. Впровадження індустріального інтернету значно впливає на економіку окремі компанії і країни в цілому, сприяє підвищенню продуктивності праці й росту валового національного продукту, позитивним образом позначається на умовах праці й професійному росту співробітників. Сервісна модель економіки, що створюється в процесі цього переходу, ґрунтується на цифровізації виробництва й інших традиційних галузей, обміні даними між різними суб'єктами виробничого процесу й аналітику великих обсягів даних. Таким чином, виходячи з вищеперерахованого, дослідження системи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture, є актуальною задачею, яка потребує вирішення у даній роботі.

Об'єктом дослідження є процес керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture.

Предметом дослідження є методи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture.

Методи дослідження базуються на методах теорії телетрафіку, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

–Удосконалено метод керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture.

Основна частина. Індустріальний інтернет речей кардинально змінює всю економічну модель взаємодії «постачальник – споживач». Це дозволяє: автоматизувати процес моніторингу й управління життєвим циклом устаткування; організувати ефективні ланцюжки, які самооптимизуються, від підприємств – постачальників до компаній – кінцевих споживачів; перейти до моделей «економіки спільного використання» і багато чого іншого. У найбільш просунутих випадках індустріальний

Інтернет речей дозволяє не тільки підвищити якість технічної підтримки устаткування з використанням розвинених засобів телеметрії, але й забезпечити перехід до нового бізнес-моделі його експлуатації, коли устаткування оплачується замовником по факті використання його функцій. Впровадження мережевої взаємодії між машинами, устаткуванням, будинками й інформаційними системами, можливість здійснювати моніторинг і аналіз навколишнього середовища, процесу виробництва й власного стану в режимі реального часу, передавача функції управління й прийняття рішень інтелектуальним системам приводять до зміни «парадигми» технологічного розвитку, називаної також «четвертою промисловою революцією».

Відповідно до архітектури Industrial Internet Reference Architecture, розробленої Industrial Internet Consortium, система Промислового інтернету піддається декомпозиції на структурні домени. Вони утворять важливі типові будівельні блоки (частково вже існуючі на підприємствах), які можуть застосовуватися в різних галузях. Кожна система Промислового інтернету буде містити принаймні наступні структурні домени:

– Управління – набір функцій рівня АСУ ТП (взаємодія із промисловим устаткуванням, читання даних, створення керуючих команд відповідно до логіки контурів управління й т.п.).

– Експлуатаційний – набір функцій для управління конфігурацією, моніторингу й оптимізації однієї або декількох підсистем доменів управління.

– Інформаційний – набір функцій для збору даних з різних доменів (насамперед з доменів управління), а також для перетворення, збереження й аналізу цих даних з метою одержання інформації більш високого рівня про систему Промислового інтернету (технології Data Lake і т.п.).

– Застосунки – реалізація логіки застосунків, що виконують певні бізнес-функції. Укрупнений рівень управління всією системою Промислового інтернету в довгостроковій перспективі й глобальному масштабі. Цей домен може містити в собі логіку застосунка, правила, моделі й т.д. Його можна представити і як домен аналітики.

– Бізнес – забезпечення наскрізних операцій системи Промислового інтернету шляхом їхньої інтеграції із традиційними або новими типами підсистем управління бізнес-процесами, планування й т.п. Прикладами таких систем можуть бути ERP, CRM, PLM, MES, HRM, управління проектами й багато які інші.

Висновки. Таким чином, у даній роботі було проведено дослідження системи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture. Визначено актуальність цієї задачі. Напрямком подальшого розвитку вважаємо розроблення вітчизняного продукту керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture, який має більш широкі можливості, на відміну від існуючих аналогів.

Список використаних джерел

1. *Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.*
2. *Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.*
3. *Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.*

Науковий керівник — доктор технічних наук, професор Смірнов О. А., завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

UDC 004.738.5:327.8

I. Kolodiazhnyi
Student, Central Ukrainian National Technical University

A Software of Tor and VPN Blocking Implementation

Significant progress and dissemination of information technology, the global nature of mass communication systems have led to the creation of a global information space that forces the world community, each state to navigate and adapt itself into the modern information environment quickly. In this context, the world community has realised that international information security is a problem, the solution of which significantly affects the existence of mankind. That is, with the development and spread of ICT into all spheres of vital importance, the issues of information security recognised in our country as one of the most important components of national security, as a multi-level problem of state information policy, become more significant. Persuasion methods got powerful development during the 20th century. Propaganda, which has a large arsenal of such methods, stimulates socio-political activity of citizens, showing them specific directions and tasks of activity, indicating the ways and means of solving the problems they are facing. According to the public information of the Security Service of Ukraine, hostile propaganda is actively implemented through social networks. Ukraine implemented an approach to resist propaganda in social networks, personal special economic and other restrictive measures (sanctions). The essence is to prohibit the Internet providers to provide an access to Russian-made Internet services: Vkontakte, Odnoklassniki, and many others. However, as practice shows, the approach to ensure the information security of the state proved ineffective. After all, the blocked websites are still among top 10 mostly visited sites in Ukraine, as users actively use VPN, Tor, Opera and other ways to bypass the lock [1].

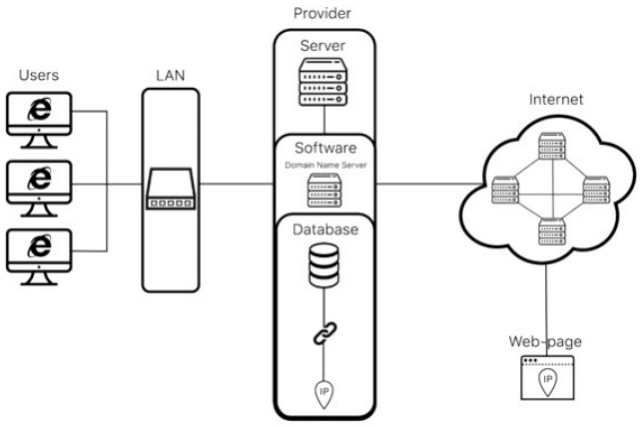


Figure 1 – The software block diagram

The aim of the work is improving the suggested software of Tor entry nodes and servers of VPN providers blocking [2]. The developed software can be improved, since every day more and more web resources spread anti-Ukrainian ideology [3-4].

References

1. *Колодяжний І. О. Вдосконалений підхід до протидії пропаганді сепаратизму та антиукраїнській ідеології в соціальних мережах / І. О. Колодяжний // Комп'ютерна інженерія і кібербезпека : досягнення та інновації : матеріали Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених (м. Кропивницький, 27–29 листоп. 2018 р.) – Кропивницький: ЦНТУ, 2018. – 448 с.*
2. *Kolodiazhnyi, I. Software Tool for Increasing Effectiveness of Countering of Anti-Ukrainian Propaganda on Internet / I. Kolodiazhnyi, O. Dorenskyi // Інформаційні технології – 2020 : зб. тез VII Всеукр. наук.-практ. конф. молодих науковців, 21 трав. 2020 р., м. Київ. – К. : Київ. ун-т ім. Б. Грінченка, 2020. – С. 182-183.*
3. *Kolodiazhnyi I., Dorenskyi O. Increasing Effectiveness of Countering of the Separatism Propaganda and Anti-Ukrainian Ideology in Social Networks. Інформаційні технології в соціокультурній сфері, освіті та економіці : міжнар. наук.-практ. конф. студ. і молодих учених, 18–19 квіт. 2019 р., м. Київ : матеріали конф. Київ : КНУКіМ, 2019. С. 279-280. URL: http://dspace.knukr.ua/jspui/bitstream/123456789/8941/1/ITCKC_Kyiv_2019_279-280.pdf*
4. *Колодяжний І. О., Доренський О. П. Методологічні засади підвищення ефективності протидії антиукраїнській пропаганді в соціальних мережах. Інформаційні технології – 2019 : VI всеукр. наук.-практ. конф. молодих науковців, 16 трав. 2019 р., м. Київ / Київський університеті імені Бориса Грінченка. Київ, 2019. С. 53-54. URL: https://fitu.kubg.edu.ua/images/stories/Departments/kitmd/zbirnuk/zbirn_tez_materialiv_konf_IT_2019.pdf.*

Scientific Supervisor PhD in Information Technology Oleksandr Dorenskyi, Associate Professor, Cybersecurity and Software Academic Department, Central Ukrainian National Technical University.

УДК 330.341.1:004

А. М. Гафіяк[1], Г. С. Гончарова[2], С. Кукоба[2]
[1]*Національний університет «Полтавська політехніка імені Юрія Кондратюка»*
[2]*Науковий ліцей №3 Полтавської міської ради*

Засади правового забезпечення кіберзахисту

Доцільно зауважити, в контексті нашого дослідження, що величчю XXI століття став кіберпростір, який є двигуном зростання економіки, поширення інформації, новою сферою державного співробітництва і суверенітету, соціального управління. Згадуючи, що Кремнієва Долина починалась з «ідеї гуманних технологій», підкреслимо, що сьогодні, в час розвитку інформаційно-комунікаційних технологій, у життя втілено прекрасні ідеї: безперервний обмін інформацією, онлайн навчання й безліч прекрасних можливостей для ефективного особтстісного розвитку. Коли та за яких умов виникла загроза? Вона з'явилася з новими можливостями. Від ери новин перейшли до ери дезінформації, теорій заговорів, фейків, поляризації суспільства, підтасовки виборів, культурних революцій. Суспільство стало більш вразливим до кіберзагроз. Чи захищені ті, хто проводить безліч часу в віртуальному світі, чи захищені люди, банки, компанії, політичні партії, державні лідери і держави від кібератак, від негативних наслідків, до яких сьогодні призвело користування новітніми технологіями? Сьогодні тема безпеки в кіберпросторі є найбільш затребуваною суспільством, оскільки це стосується кожного, хто стикається зі світом інформаційних технологій. Проблема досить актуальна, що доведено в документальному фільмі 2020 року режисера Джеффа Орловскі «Соціальна дилема». Колишні співробітники Google, Instagram, Twitter, YouTube, Tik Tok, Snapchat і Facebook (FB) розповідають про те, як соціальні мережі маніпулюють користувачами. Трістан Гарріс, фахівець з етичного дизайну Google стверджує, що у людей виробляється залежність. Він доводить, що 50 молодих розробників (від 20 до 30 років) ухвалюють рішення, яке потім впливає на 2 мільярди людей. Для цього постійно оновлюються алгоритми, які допомагають сайтам передбачати інтереси користувачів, щоб продавати більше реклами. Дослідники обгрунтовують, як на глобальному рівні використовуються соціальні мережі, щоб дестабілізувати обстановку в країнах, поширювати неправдиву інформацію. Крім цього, Тім Кіндел, який відповідає за монетизацію у FB, називає соцмережі машинами для виробництва грошей. Джерелом грошей є вплив на вчинки представників інформаційного простору, на мислення суспільства. Зі слів авторів, можна зробити висновок, що «продається майбутнє людей, їх увага, час і життя, а платформами соціальних мереж заробляються трильйони долларів» [1, 2, 3].

Справжня дилема для суспільства - це влив платформ на свідомість людей, а осоюливо молоді. Хто їх захистить від шкідливого впливу, де контроль, регулювання в перегляді YouTube та інших ресурсів? На перший погляд невинні кліки в інтернеті, такі як лайки, насправді діють на самооцінку людей, викликають дисфункції психіки. Психологи наводять статистику, що сьогодні стрибок у дитячій тривожності, депресії, самогубствах за останні роки зростає. Не менш важливим є захист від тотального стеження, хакерських атак, вірусів, підробки даних, впливу на роботу й продуктивність співробітників, використовування інформації проти людини, забезпечення конфіденційності та доступності даних, ресурсів, а саме необхідно захистити дані на етапі їх обміну та збереження. Наразі зростає потреба в особистій кібербезпеці, тому що чим далі, тим більше ми "зростаємось" із нашими гаджетами. У 2016 році в Одесі на

конференції Black Sea Summit презентували вперше в Україні вживлений людині чіп у руку, яким вона могла оплачувати рахунки, як банківською картою. З 2018 року чіпи, які би замінювали ключі, карти, ідентифікаційні дані, імплантували в інших країнах. Apple заснували тенденцію на FaceID, завдяки якій вже можна розплачуватися на касі та ідентифікувати людину просто за обличчям [2, 4, 5].

Протидія економічним злочинам, злочинам проти екосистем, ядерних об‘єктів, антимонопольна безпека, захист від крадіжок інтелектуальної власності, шпіонажу -- один з етапів кібербепеки. Ряд судових позовів вказує на недосконаліть захисту в цій сфері. Google вже кілька разів була оштрафована Європейською комісією за порушення антимонопольного законодавства на загальну суму 8,2 млрд євро. У 2014 році компанія «Лабораторія Касперського» спільно з Європолом та Інтерполом розкрила групу Carbanak, яка протягом багатьох років виводила кошти з банків через банкомати або онлайн-банкінг (позов до федерального суду в штаті Каліфорнія США від 2 червня 2020). Google звинуватили в незаконному вторгненні в приватне життя мільйонів користувачів, шляхом відстеження їх дій у випадках, коли вікна браузерів відкривалися в режимі інкогніто. Компанію звинувачують, що вона дізнавалась про хобі користувачів, коханих, звички та інтимні речі, які вони шукають в інтернеті [2, 5].

Україна, як і більшисть країн світу не уникла участі у інформаційній війні, яка характеризується спонуканням до хаосу через соціальні мережі, розповсюдженнямрізноманітних політичних, неекономічнх та соціальних фейків відносно діяльності урядових структур, з використанням мобільних кібератак. Загроза національній безпеці країни потребує створення Стратегії кібербезпеки країни, особливо, з огляду на сучасний політичний стан дерави. Указом Президента України від 15 березня 2016 року було прийнято Закон України «Про основні засади забезпечення кібербезпеки України». На жаль, дія цього Закону не поширюється на послуги, пов’язані зі змістом інформації, що передається, зберігається в соціальних мережах, у мережі Інтернет. 09 травня 2018 року набрала чинності Директива Європейського парламенту і Ради (ЄС) №2016/1148, під назвою «Безпека мереж та інформації» (Network and Information Security). Нормативно правове забезпечення кібербезпеки – складний процес, але це складова успішного бізнесу, захисту особистості і в цілому цивілізації. Світова спільнота якнайшвидше має звернути увагу на удосконалення правового забезпечення кібербезпеки і належної відповідальності за вчинення інформаційних кіберзлочинів проти людства. Світ має стати розумнішим і кращим, чого має прагнути людство.

Список використаних джерел

1. *Алгоритм должен быть разрушен: Netflix выпустил фильм о влиянии соцсетей на человечество [Електронний ресурс]. Режим доступу: https://ms.detector.media/trendi/post/25581/2020-09-25-algoritm-dolzhen-byt-razrushen-netflix-vypustil-film-o-vliyanii-sotssetei-na-chelovechestvo/.*
2. *Espreso.tv. News [Електронний ресурс]. Режим доступу: https://espreso.tv/news/2020/06/05/nimechchyna_maye_dokazy_prychetnosti_rf_do_masshtabnoyi_kiberataky_na_bundestag_maas.*
3. *Ukranews.com [Електронний ресурс]. Режим доступу: https://ukranews.com/ua/news/706732-nimechchyna-dovela-prychetnist-rosiyi-v-kiberatatsi-na-bundestag.*
4. *Суспільне. Новини. [Електронний ресурс]. Режим доступу:* https://suspilne.media/61873-vsesvitnij-den-zapobiganna-samogubstvam-rozvincuemo-posireni-mifi-pro-suicid/.
5. *Відшкодування збитків за порушення конкуренції: національні та світові тенденції private enforcement [Електронний ресурс]. Режим доступу: https://yur-gazeta.com/publications/practice/antimonopolne-konkurentne-pravo/vidshkoduvannya-zbitkiv-za-porushennya-konkurenciyi-nacionalni-ta-svitovi-tendenciyi-private-enforce.html.*

УДК 004.056.55:003.26

О. М. Грищук
молодший науковий співробітник,
Житомирський військовий інститут імені С. П. Корольова

Особливості вибору ключа шифрування для криптосистеми Фредгольма

Вступ. Злам найскла.днішого в світі ключа шифрування RSA-240 групою французьких та американських дослідників [1] черговий раз актуалізує проблему кібербезпеки [2], [3]. Не виключається, що з розвитком квантових комп'ютерів [4] під загрозою буде злам ключів і інших криптоалгоритмів, наприклад AES-256. Таким чином, подальший розвиток стійких до зламу криптосистем залишається актуальним науковим та практичним завданням.

З аналізу відомих публікацій встановлено, що значний внесок у вирішення згаданого завдання внесли ряд вітчизняних [5] та закордонних наукових шкіл [6]. Поряд з тим на сьогодні існує й інший, альтернативний підхід до розвитку криптографічних алгоритмів. Зокрема в [7] запропоновано криптографію нового покоління, яка ґрунтується на інтегральних рівняннях. Вперше прикладні аспекти застосування інтегральної криптографії приведено в [8]. Поряд з тим ні в [7], ні в [8] не приведено методологію вибору ключа шифрування.

Метою даного дослідження є визначення основних особливостей, на які слід звернути увагу при виборі ключа шифрування для криптографічних систем, що ґрунтуються на інтегральних рівняннях Фредгольма першого роду.

Основна частина. У [9] вперше на основі досліджень [7], [8] та ін. за визначеною темою було формалізовано узагальнену модель криптосистеми Фредгольма, де зокрема показано, що згадана модель побудована за класичною моделлю симетричної криптосистеми. При цьому обґрунтовано, що секретним ключем $K(x,s)$ виступає ядро інтегрального рівняння Фредгольма першого роду

$$\int_a^b K(x,s)\, z(s)\, ds = u(x),$$

де $z(s)$ – вихідні дані, які підлягають шифруванню/дешифруванню (відкритий текст), $u(x)$ – зашифровані дані (шифрограма).

У силу некоректності задачі по Ж. Адамару процедура дешифрування також є некоректною і саме від обраного ключа шифрування залежатиме криптостійкість запропонованої в [9] криптосистеми.

Першою особливістю, яка повинна враховуватися при вборі ключа шифрування для криптосистеми Фредгольма повинна бути *вимога до неперервності* ядра інтегрального рівняння, тобто ядро повинно бути неперервним в квадраті $a \le x$, $s \le b$. У формалізованому вигляді дана умова набуває вигляду

$$K(x,s) \in C(a \le x, s \le b). \tag{1}$$

Другою особливістю ключа шифрування для криптосистеми Фредгольма повинна бути *умова виродженості* ядра інтегрального рівняння. Вродженість ядра у формалізованому вигляді зводиться до виразу вигляду

$$K(x,s) = \sum_{l=1}^{m} g_l(x)\, q_l(s). \tag{2}$$

Третьою особливістю ключа шифрування для криптосистеми Фредгольма повинна бути *умова симетричності* ядра інтегрального рівняння, тобто для довільних x та s з множини C при $x, s \in C$ повинна виконуватися рівність вигляду

$$K(x,s) = K(s,x). \quad (3)$$

Таким чином, умови (1)-(3) можна вважати загальними умовами розв'язності зворотної некоректної задачі [10], що описується інтегральним рівнянням Фредгольма першого роду. Іншими словами виконання згаданих умов закладає математичне підґрунтя для дешифрування повідомлень, які шифруються на основі узагальненої моделі криптосистеми Фредгольма.

Висновки з дослідження та перспективи подальших розвідок у даному напрямку. У тезах доповіді вперше розкриті особливості вибору ключа шифрування для криптосистеми Фредгольма. Урахування зазначених вимог дозволить практично реалізувати процедури шифрування та дешифрування повідомлень на основі нових та перспективних, з точки зору криптостійкості, криптосистем.

Перспективним напрямом подальших досліджень є вибір ключа шифрування у формалізованому вигляді, виходячи із запропонованих умов (1)-(3) та, власне, реалізація процедури шифрування та дешифрування повідомлень з використанням криптосистеми Фредгольма.

Список використаних джерел

1. *Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment [Електронний ресурс] / [F. Boudot, P. Gaudry, A. Guillevic та ін.] // Cryptology ePrint Archive, Report 2020/697. – 2020. – Режим доступу до ресурсу: https://arxiv.org/pdf/2006.06197.pdf.*
2. *Грищук Р.В. Основи кібернетичної безпеки: монографія / Р.В. Грищук, ЮГ. Даник; за заг. ред. проф. Ю.Г. Даника. – Житомир: ЖНАЕУ, 2016. – 636 с.*
3. *Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти : монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька ; за заг. ред. Р. В. Грищука. – Житомир : ЖНАЕУ, 2019. – 280 с.*
4. *Foy K. MIT partners with national labs on two new National Quantum Information Science Research Centers [Електронний ресурс] / K. Foy, S. Wilcox // MIT. – 2020. – Режим доступу до ресурсу: https://news.mit.edu/2020/mit-partners-national-labs-new-national-quantum-information-science-research-centers-0831.*
5. *Results of Ukrainian National Public Cryptographic Competition / R.Oliynykov, I. Gorbenko, V. Dolgov, V. Ruzhentsev. // Tatra Mt. Math. Publ.. – 2010. – №4. – С. 99–113.*
6. *Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Б. Шнаєрю – М : Триумф, 2003, 806 с.*
7. *Криптография нового поколения: Интегральные уравнения как альтернатива алгебраической методологии / Г. Броншпак, И. Громыко, С. Доценко, Е. Перчик // Прикладная электроника. – 2014. – №3. – С. 337–349.*
8. *Глинская Е. В. Информационная безопасность открытых каналов передачи проектной документации, продуцируемой в САПР / Е. В. Глинская, Н. В. Чичварин. // Вопросы кибербезопасности. – 2014. – №4. – С. 11–22.*
9. *Грищук О. М. Узагальнена модель криптосистеми Фредгольма / О. М. Грищук, Р. В. Грищук. // Кібербезпека: наука, освіта, техніка. – 2019. – №4. – С. 14–23.*
10. *Тихонов А. Н. Методы решения некорректных задач / А. Н. Тихонов, В. Я. Арсенин. – М.: Наука, 1986. – 288 с.*

Науковий керівник – доктор технічних наук, професор Молодецька К. В., керівник навчально-наукового центру інформаційних технологій Поліського національного університету МОН України.

УДК 004.056

Б. Є. Золотухін
студент, Центральноукраїнський національний технічний університет

Проблеми безпеки при використанні веб-сервісів в Інтернет-покупках

У цифровій безпеці одних лише технологічних рішень недостатньо, щоб захистити користувача від втрати інформації чи грошей. Це рішення є комплексним.

Багато користувачів, наприклад, встановлюють антивірус на свій комп'ютер і вважають, що цього достатньо. Але для того, щоб антивірус працював, потрібно постійно його оновлювати, завантажувати та встановлювати необхідні програми з офіційних сайтів тощо. Якщо антивірусна програма каже, що програма «підозріла» - краще відмовитися від інсталяції і не ігнорувати попередження або перевіряти іншими антивірусними програмами, треба шукати альтернативну програму, яка «підійде» вашому антивірусу.\, тобто, вживати альтернативні заходи, щоб захистити себе.

Ще одним підтвердженням цього є закриття «Новою поштою» служби «Сейф-сервіс», яка мала забезпечити користувачів покупками через Інтернет. Служба працювала трохи більше місяця і була припинена з формулюванням "На жаль, ми бачимо, що службою почали зловживати шахраї". Тобто служба, яка мала захищати клієнтів від шахраїв, стала послугою, яка шахраям, навпаки, сподобалася і почала успішно працювати для них.

Звичайно, користувачі думають, що це окрема супер надійна послуга (власне, послуга себе так і позиціонувала). Ось фрагмент: "Нова пошта запустила послугу для безпечних онлайн-транзакцій між продавцями та покупцями - "Сейф-сервіс". Нова послуга допомагає захистити відправника та одержувача від шахрайства.

Усі користувачі цього сервісу були впевнені, що якщо вони ним скористаються - будуть на 100% захищені і що ви можуть робити покупки за допомогою цього сервісу на великі суми. Чим, власне, шахраї із задоволенням скористались. Впевненість користувачів у повній надійності послуги, неуважність та відсутність здорової підозри призвели до того, що їх почали «роззувати» на кругленькі суми. За словами постраждалих користувачів, суми становлять від 1000 до 10 000 гривень і вище.

Найпростіший спосіб обдурити користувачів - це фішинг. Шахраї надсилали довірливим клієнтам посилання на сайт, схожий на офіційний для "безпечного" платежу. І дуже мала кількість людей насторожувалася, отримавши посилання на сайт не в зоні .ua, а, наприклад, .ch. Ніхто не запитував себе, чому цей сайт знаходиться не в доменній зоні України, а в зоні Швейцарії? І майже нікого не бентежили неточності дизайну та інші помилки.

Так, не всі знають, як виглядає офіційний веб-сайт Нової пошти, не всі знають, що .ch - це швейцарська доменна зона тощо, але всі точно можуть зайти в Google. Просто скопіюйте посилання та вставте його в рядок пошуку - ми отримаємо перший результат - посилання на офіційний сайт "Нової пошти" та попередження про те, що це єдиний офіційний сайт - у зоні .ua. Всього цього достатньо, щоб поставитись питанням і не стати жертвою шахрайства.

Звичайно, поштовий перевізник випустив «сирий продукт» та не всі користувачі - ІТ-гуру, але в сучасному світі вам потрібно вивчити для себе: 100-відсоткової безпеки не існує навіть у теорії; одних лише технологічних рішень недостатньо; перекласти відповідальність за свою цифрову безпеку на когось чи щось - замало.

Науковий керівник — кандидат технічних наук, доцент Марченко К. М., доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.56.5

А. С. Мороз
студент, Центральноукраїнський національний технічний університет

Компоненти інформаційної безпеки

Інформаційна безпека - це набір практик, призначених захистити дані від несанкціонованого доступу, як при зберіганні так і під час передачі даних.

Основні компоненти інформаційної безпеки найчастіше узагальнює так звана тріада CIA (Confidentiality, Integrity, Availability): конфіденційність, цілісність та доступність.

Конфіденційність - це, мабуть, той елемент тріади, який найбільш відразу спадає на думку, коли ти думаєш про інформаційну безпеку. Дані є конфіденційними, коли до них мають доступ лише авторизовані користувачі. Щоб забезпечити конфіденційність, ви повинні мати можливість визначити, хто намагається отримати доступ до даних, і блокувати спроби тих, хто не має дозволу. Паролі, шифрування, автентифікація та захист від атак проникнення - це всі методи, призначені для забезпечення конфіденційності.

Цілісність означає підтримку даних у коректному стані та запобігання їх несанкціонованому зміненню, випадковому чи зловмисному. Багато методів, що забезпечують конфіденційність, також захищають цілісність даних - врешті-решт, хакер не може змінювати дані, до яких він не має доступу. Але існують інструменти, які допомагають забезпечити глибокий захист цілісності: контрольні суми можуть допомогти вам перевірити дані на цілісність, програмне забезпечення для контролю версій та часті резервні копії можуть допомогти вам відновити дані до правильного стану, якщо це необхідно. Цілісність також охоплює поняття відмови: ви повинні мати можливість довести, що зберегли цілісність своїх даних, особливо в юридичному контексті.

Доступність - це дзеркальне відображення конфіденційності: хоча вам потрібно переконатись, що неавторизовані користувачі не можуть отримати доступ до ваших даних, вам також потрібно забезпечити доступ до них тим, хто має належний дозвіл. Забезпечення доступності даних означає узгодження мережевих та обчислювальних ресурсів з обсягом доступу до даних, та впровадження належної політики резервного копіювання для цілей аварійного відновлення.

В ідеальному світі ваші дані завжди повинні залишатися конфіденційними, у правильному стані та доступними; на практиці, звичайно, часто потрібно робити вибір, які принципи інформаційної безпеки більш пріоритетні у конкретній інформаційній системі, а для цього потрібно правильно оцінити бізнес цілі вашої системи.

Наприклад, якщо ви зберігаєте конфіденційну медичну інформацію, ви зосередитесь на конфіденційності, тоді як фінансова установа може наголосити на цілісності даних, щоб переконатися, що нічий банківський рахунок не кредитується або дебетується неправильно, якщо ж у вас серверний додаток з великою кількістю користувачів та вимогами з передачі великих обсягів даних більш пріоритетним може бути доступність.

Тож детальний аналіз структури та бізнес цілей вашої інформаційної системи дозволить правильно обрати пріоритет компонентів інформаційної безпеки і забезпечити баланс цих компонент на належному рівні.

Науковий керівник — Бісюк В. А., викладач кафедри кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет.

УДК 343.3/7:004

Д. О. Радін
студент, Центральноукраїнський національний технічний університет

Аспекти проблеми інформаційної безпеки України

У сучасному суспільстві при бурхливому розвитку інформаційно-комунікаційних технологій підсилення проблеми захисту даних від викрадення, втрати, пошкодження викликає посиленої уваги, особливо у банківської сфері. Ігнорування цих проблем може привести до появи проблем у прийнятті важливих економічних, політичних та соціальних рішень, що можуть прямо вплинути на якість життя населення. Нажаль, нині в Україні немає реальних гарантів її інформаційної безпеки, відсутній комплекс нормативно–правових актів щодо захисту інформаційних ресурсів та інформаційної інфраструктури, а відповідальність за такі злочини не відповідає стандартам міжнародної конвенції про кібербезпеку[1].

Кібервійни та кібертероризм набувають глобального характеру та становлять ще більшу загрозу за рахунок неперервного розвитку технологій та більш складних способів атак, що ускладнює їх виявлення та можливості їх протидії.

Процес інформатизації має некерований стихійний характер, з використанням засобів інформатизації іноземного виробництва, що приводить до необхідності в комплексному та ефективному підході до процесу забезпечення безпеки національного інформаційного простору[2].

У зв’язку з вищевикладеним випливає, що перед державою постає задача посилення інформаційної безпеки, а саме створення захищеного інформаційного простору, захист національних інтересів, економічного потенціалу України в умовах формування світових інформаційних мереж, захист від незаконного використання інформаційних ресурсів. Вирішення даної проблеми підвищить забезпечення інформаційної безпеки не тільки всієї держави, але й організації і окремої особистості.

Заходи із забезпечення безпеки інформаційної системи повинні ґрунтуватися на перевірених практикою прийомах і методах та носити комплексний характер.

Організація управління інформаційними ресурсами передбачає створення норм і механізмів, що забезпечують: координацію діяльності щодо формування регіональних інформаційних ресурсів; визначення повноважень і відповідальності за інформаційні ресурси органів державного та регіонального управління; організацію реєстрації й обліку інформаційних ресурсів; контроль використання захисту і збереження інформаційних ресурсів.

Але основні труднощі полягають не в створенні і розборі комплексних систем дій спрямованих на рішення проблеми, а в самому її визначенні. Це пов'язано з тим, що кібертероризм не постійний. Він не має чіткої і кінцевої форми, а багато його проявів мають суто індивідуальний характер. Кібертероризм, як новий вид тероризму, потребує детального та поглибленого дослідження в контексті шляхів його протидії та запобігання.

Список використаних джерел

1. *Косогов О. М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору / О. М. Косогов // Збірник наукових праць Харківського університету Повітряних Сил. – 2014. – № 3. – С. 127–130.*
2. *Грицюк Ю. І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання / Ю. І. Грицюк // Науковий вісник НЛТУ України. –2016. – №. 26.8. – С. 327-337.*

Науковий керівник — Ладигіна О. А., викладач кафедри кібербезпеки та програмного забезпечення.

УДК 004.56.5

Я. В. Федюк
студент, Центральноукраїнський національний технічний університет

Інформаційна безпека національного сегмента кіберпростору та боротьба з кіберзлочинністю

Сьогодення яскраво демонструє те, наскільки актуальними є кібератаки та їх еволюція. Більшість організацій та проектів перейшли у мережу Інтернет та ці атаки набувають більшого і більшого сенсу у 21 столітті. Як відомо, за недавні часи в Україні було підвищено рівень кібербезпеки та боротьби із кіберзлочинністю. Значними кроками до цього було заснування нової кіберполіції 5 жовтня 2015 р. та написання законів "про основні засади забезпечення кібербезпеки України" №2163 - VIII 5 жовтня 2017 р.

Все частіше можна почути про кіберзлочини по всьому світу. Нажаль це явище присутнє і в Україні. Головною проблемою та основним джерелом цього є несерйозне ставлення людей, зокрема держави, до особистої та державної безпеки у кіберпросторі. Що надає наша держава, щодо даної проблеми:

1. Розробка безпечного, стійкого та надійного кіберпростору;
2. Кібербезпека державних електронних інформаційних ресурсів;
3. Кібербезпека критичної інфраструктури;
4. Розвиток потенціалу кібербезпеки в оборонному секторі;
5. Боротьба з кіберзлочинністю.

Не можна не сказати і про все ще низький рівень кібербезпеки у нашій державі. Об'єкти критичної інфраструктури та державних органів досі схильні і піддаються кібератакам злочинців. Звісно, що з моменту появи нової кіберполіції, дані злочини стали з'являтися дещо рідше, але це все ще не бажаний і не найнебезпечніший результат їх роботи. Серед усіх, відзначено саме такі недоліки і факти, що впливають на загальну безпеку кіберпростору України:

1. Низька якість аудиту кібербезеки;
2. Кіберрозвідка потребує покращення;
3. Потреба у переході на міжнародні стандарти кібербезпеки;
4. Впровадження кібербезпеки вимагає трансформаційного підходу;
5. Низька готовність реагувати на кібератаки.

Отже, як ми бачимо, нова поліція і кіберполіція у тому числі, несе за собою багато різних реформ і закони, в яких є як переваги, так і недоліки. На сьогоднішній день кіберполіція успішно затримує злочинців, що порушують закон і ховаються у мережі Інтернет. У наші дні, технології ростуть дуже швидко, з чим ростуть і потреби людини у Інтернеті. Кількість злочинців і їх потреби, нажаль, теж не стоять на місці. Саме тому нашій кіберполіції і поліції варто швидше робити значні кроки до покращення роботи і розширення зон відповідальності.

Список використаних джерел

1. *Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради України. –2015. №2163 - VIII.*

Науковий керівник — Бісюк В.А., викладач кафедри кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет.

УДК 004.05

Ю. І. Хлапонін[1], П. І. Драгунов[2]
[1]*завідувач кафедри, Київський національний університет будівництва і архітектури*
[2]*студент, Київський національний університет будівництва і архітектури*

Кібербезпека в Україні та стратегія протидії кіберзлочинності

Під терміном “кіберзлочинність” прийнято мати на увазі будь-який злочин, здійснений за допомогою віртуального простору і комп'ютерів. У реальному світі кібератаки паралізують діяльність важливих фірм, державних установ, громадяни втрачають гроші завдяки різним шахрайським схемам. Багато фірм яким важлива репутація не називають точні суми своїх збитків, особливо це стосується випадків витоку даних, оскільки інші компанії мають можливість використати цю інформацію у своїх цілях. Деякі з компаній навіть не підозрюють, що на них здійснювались напади з боку кіберзлочинців, тому точну суму збитків визначити неможливо. Більшості світових лідерів стурбовані безпекою кіберпростору тому інвестують у цю сферу фінансове забезпечення. Боротьба з кіберзлочинністю неможлива без глибокого розуміння правових основ щодо використання інформаційних мереж. Одна із проблем протидії кіберзлочинам — це потреба якісних спеціалістів у сфері кібербезпеки. Більшість кіберзлочинців мають великі знання в областях інформаційних технологій і електроніки, і тому протидіяти їм непросто. Протизаконні дії кіберзлочинів не обмежуються рамками одного міста або однієї країни. І хоча Кримінальний кодекс України передбачає обмеження свободи на строк до 3 років або позбавлення волі на строк до 12 років для тих, хто займається інформаційним шахрайством та втручанням у системи обчислювальної техніки. Але це не зупиняє шахраїв та кіберзлочинців, внаслідок це призводить погіршенню фінансовому стану, так і діловій репутації. Сьогодні економічна та політична репутація є одними з найбільш важливих аспектів для комерційних і державних структур. На цьому ґрунтується довіра людей на світовому рівні.

У МВС України створено Управління по боротьбі з кіберзлочинністю. Основним завданням якого є організаційне і практичне забезпечення по попередженню і протидії злочинам і правопорушенням, що здійснюються з використанням інформаційних технологій і телекомунікаційних мереж. Задля належної розробки відповідних заходів протидії злочинності, в тому числі кіберзлочинності, є необхідною належна організація діяльності як правоохоронних органів, так і вищих органів держави, яка відповідає вимогам, що висуваються до правової, незалежної та демократичної держави. Крім того, необхідно усувати фактори, що позитивно впливають на існування та розвиток злочинності. Але з урахуванням вищесказаного, на жаль, в Україні на сьогодні відсутня потужна протидія кіберзлочинів та ефективне законодавство у сфері боротьби з кіберзагрозами і кіберзлочинами. Навіть законопроект №2483 “Проект Закону про внесення змін до Закону України “Про основи національної безпеки України” щодо кібернетичної безпеки України” триває близько декілька років і в результаті законопроект не ухвалений.Безперечно, цей напрямок діяльності поліції є важливим, оскільки економічні втрати вже досягли широких масштабів, деякі злочинці діють на міжнародному рівні організованою групою. Враховуючи, що завдання, які стоять перед підрозділами поліції з боротьби з комп’ютерною злочинністю, носять міжнародний характер і не є специфічними, вони активно співпрацюють з іншими країнами та Інтерполом з боротьбою зі злочинністю, в тому числі кіберзлочинністю, забезпеченням дотримання прав людини, забезпеченням захисту федеральних державних комп’ютерних центрів, приватного сектора.

Основними заходами запобігання кіберзлочинності, що повинні реалізовувати ОВС та Національною поліцією (в особі Департаменту кіберполіції), слід визнати такі: розроблення та затвердження МВС Стратегії протидії кіберзлочинності, що повинна містити концепцію кримінально-превентивої діяльності, науково обґрунтовані стратегічні й тактичні заходи антикримінального впливу й моніторингові механізми

забезпечення якостіостаннього; збільшення кількості планових і позапланових перевірок відповідними органами поліції підприємств, установ та організацій, діяльність яких прямо пов'язана з використанням комп'ютерних технологій або наданням інформаційних послуг, з метою виявлення випадків використання нелегального (нерегламентованого) програмного забезпечення; посилення відповідальності уповноважених осіб підприємств, установ або організацій, діяльність яких пов'язана із зазначеною сферою, які за своїми посадовими або функціональними обов'язками відповідають за безпеку функціонування комп'ютерів та комп'ютерних мереж.

Напрямом діяльності щодо протидії вчиненню кіберзлочинів слід також визначити виявлення осіб, які вчиняють або схильні до вчинення кіберзлочинів, індикаторами поведінки яких є систематичний перезапис даних без необхідності, заміна або видалення даних, поява фальшивих записів, випадків, коли оператор системи без об'єктивних підстав починає працювати наднормово, персонал заперечує проти здійснення контролю за записом даних, фіксуються постійні скарги користувачів баз даних або власників щодо помилок та затримок у роботі системи тощо.

Рівень кіберзлочинності у 2017 р. склав 2573 злочинів і має тенденцію до зростання. Показники динаміки кіберзлочинності в цілому відповідають показникам загальної злочинності в країні, що свідчить про специфічність детермінаційного комплексу кіберзлочинності та про відставання можливостей правоохоронних органів від сучасного рівня технологічного та програмного забезпечення кримінальної активності. Найбільш ефективними заходами, безпосередньо спрямованими на протидію кіберзлочинності, є такі: збільшення кількості планових і позапланових перевірок; установлення жорсткого контролю за обігом технічних засобів, заборонених або обмежених у вільному цивільному обігу; перейняття досвіду діяльності правоохоронних органів інших країн у цій сфері; співробітництво з відповідними органами інших країн щодо розкриття, розслідування та запобігання злочинам в аналізованій сфері, обмін досвідом правозастосування; виявлення осіб, схильних до вчинення злочинів в аналізованій сфері, тощо. Указані заходи потребують подальших наукових розробок для створення дієвих інструментів протидії сучасним викликам кіберзлочинності. Ефективна боротьба із комп'ютерною злочинністю вимагає більш дієвого та ефективно функціонуючого співробітництва правоохоронних органів різних країн, у тому числі в межах Інтерполу.

Сучасний етап становлення громадянського суспільства визначається входженням України до провідних технологічно розвинутих країн світу, до глобального інформаційного простору. Саме тому ми маємо використовувати досвід країн, що вже мають досить серйозні напрацювання у сфері забезпечення інформаційної безпеки. Оскільки вона є невід'ємним напрямком побудови інформаційного суспільства, розвиток якого повинен йти не лише через нарощування технологічних можливостей здійснення інформаційного обміну, а й через глибоке усвідомлення всіма суб'єктами інформаційних відносин власниками інформації та її користувачами, виробниками інформаційних технологій і засобів, постачальниками послуг, державою необхідності здійснення всіх заходів щодо захисту інформаційних ресурсів та забезпечення безпеки держави, у тому числі враховуючи зарубіжний досвід протидії кіберзлочинності в сфері адміністративно-правового забезпечення. Тільки скоординованими зусиллями організацій та відомств незалежно від форм власності, шляхом налагодження міжнародного співробітництва, використовуючи сучасні технології захисту інформації можна отримати переваги не лише електронного бізнесу, а й інформаційної революції в цілому, не забуваючи про інформаційну безпеку держави та окремих громадян. Слід зазначити, що удосконалення адміністративно-правового забезпечення протидії кіберзлочинності в Україні має відбуватися з урахуванням національних культурно-історичних, соціально-економічних особливостей країни на підставі детального наукового аналізу міжнародного законодавства та досвіду інших країн у сфері боротьби з кіберзлочинністю.

УДК 004.056.2

Я. Білорус
студент, Центральноукраїнский національний технічний університет

Штучні імунні системи як засіб самозахисту

Вступ. Системи, що запозичують у природи принцип імунітету, називають штучними імунними системами (AIS - Artificial Immune System) .

Фахівці, що працюють в області AIS, відзначають три основних властивості імунної системи людини: вона є розподіленою, самоорганізованою, легковаговою, тобто не особливо вимогливою до обчислювальних ресурсів. Саме цими властивостями, на думку багатьох експертів, повинна володіти система виявлення вторгнень в мережу (IDS - Intrusion Detection System), яка за своїми характеристиками наближалася б до максимально ефективної. IDS для одного сегмента мережі, побудована на принципах штучної імунної системи, підрозділяється на основну та набір вторинних. В основній IDS на базі AIS реалізуються, а точніше імітуються, два процеси - еволюція генної бібліотеки і негативна селекція даних.

Основна частина. На етапі еволюції генної бібліотеки відбувається накопичення інформації про характер аномалій мережевого трафіку. Генна бібліотека штучної імунної системи повинна містити гени (дані про характерну кількість пакетів, їх довжину, структуру і типові помилки), на підставі яких будуть генеруватися особливі програмні агенти - детектори, які служать аналогами лімфоцитів. Початкові дані для формування генної бібліотеки вибираються виходячи з особливостей застосовуваних мережевих протоколів, зокрема, їх слабких з точки зору захисту місць. Надалі при виявленні детекторами аномальної активності в мережі в бібліотеку будуть додаватися відповідні цим проявам нові гени. Слід зауважити, що розмір генної бібліотеки обмежений, в ній зберігаються гени які найчастіше проявляються.

На другому етапі шляхом довільного комбінування генів відбувається генерування так званих предетекторів, які потім за допомогою механізму негативної селекції перевіряються на сумісність або на несумісність з нормальним мережевим трафіком. При цьому використовуються дані про характер такого трафіку (профіль), що формуються так званим автоматичним профайлером, який постійно аналізує потік даних, що надходить від маршрутизатора на вході в мережевий сегмент.

При виявленні аномалії відповідний їй детектор розмножується і розсилається на всі вузли. Остаточне рішення про те, чи відбувається вторгнення в мережу чи ні, приймається на підставі даних від декількох вузлів. Кожен вузол, а також основна IDS забезпечені ще одним компонентом - комунікатором, який, зокрема, оперує таким параметром, як рівень ризику. У разі, якщо на якомусь вузлі помічена підозріла активність, комунікатор піднімає свій рівень ризику і відсилає відповідне повідомлення комунікаторам інших вузлів і основну IDS, які теж піднімають свої рівні ризику. При появі аномалій відразу на декількох вузлах протягом короткого проміжку часу цей рівень дуже швидко зростає, і, якщо буде досягнуто заданий поріг, адміністратор мережі отримає сигнал тривоги.

Висновок. Варто відзначити, що розроблені на сьогоднішній день алгоритми негативної селекції оперують імовірнісними характеристиками - замість точної відповідності використовується часткова, ступінь якої може довільно змінюватись. Її зміна в кінцевому підсумку повинна приводити до зменшення або збільшення частоти помилкових спрацьовувань.

Науковий керівник — Савеленко О. К., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.056

А. А. Вітряченко[1], І. С. Касяненко[1]
[1]*студент, Центральноукраїнський національний технічний університет*

Дослідження систем виявлення аномалій мережевого трафіку

Здатність виявлення аномалій мережевого трафіку - є важливою вимогою, що пред'являються до систем виявлення і попередження шкідливих вторгнень в сучасні мережеві інфраструктури. Щоб побудувати таку систему актуальним буде розглянути існуючі на даний момент системи моніторингу та технології, на яких вони побудовані.

З найбільш популярних систем моніторингу можна виділити такі [1]: 1) Cacti - веб-додаток дозволяє проводити збір статистичних даних за певний проміжок часу з відображенням їх у вигляді графіків; 2) Zabbix - система моніторингу серверів, комп'ютерних мереж, мережевого обладнання, поширюється на безкоштовній основі. Підтримує декілька видів моніторингу: ZABBIXagent, Simplechecks, externalcheck; 3) Nagios - здійснює такі операції: моніторинг мережевих служб, спостереження за станом хостів, віддалений моніторинг за допомогою шифрованих тунелів SSLi SSH; 4) Ganglia - система, призначена для моніторингу кластерів паралельних обчислень, а також хмарних систем з ієрархічною структурою; 5) PRTG - програма спостереження за станом мережі. Здійснює збір даних про протоколи, з можливістю збереження їх в базі даних і переглядом у вигляді таблиць і графіків; 6) Snort - мережева система запобігання й виявлення вторгнень з відкритим вихідним кодом, що виконує реєстрацію пакетів за певними ознаками та в реальному часі здійснює аналіз трафіку в IP мережах.

У розглянутих системах немає можливості (або вони обмежені) тонкої настройки системи й керування процесом розбирання пакетів, що ускладнює їх використання та аналіз. З цієї причини в [1] пропонується спосіб побудови найбільш гнучкої моделі виявлення мережевих аномалій на принципах модульності й розширюваності.

Досить поширеними є системи виявлення вторгнень, засновані на аналізі сигнатур, які виявляють аномалії, пов'язані з атаками й вторгненнями, наприклад RealSecure і NetRanger [2]. Однак сигнатурний метод має недоліки: неможливість виявляти нові несанкціоновані дії, що не зустрічалися раніше; нестійкість до модифікацій відомих атак; нездатність визначати розподілені в часі атаки й аномалії.

Для побудови систем виявлення аномалій велика увага приділяється вивченню методів біологічного моделювання штучного інтелекту, таких як штучні нейронні мережі й штучні імунні системи, що є одним з перспективних підходів до вирішення завдань виявлення аномалій [3] в комплексі з іншими методами. З проаналізованих нейронних мереж найбільш доцільними для застосування в засобах виявлення аномалій є багатошаровий персептрон і самоорганізована карта ознак. Результати роботи будуть застосовані для розробки програмного забезпечення, призначеного для адміністраторів комп'ютерних мереж.

Список використаних джерел

1. *Левоневский Д.К., Р.Р. Фаткиева Р.Р. Разработка системы обнаружения аномалий сетевого трафика // Научный вестник НГТУ Scientific Bulletin of NSTU том 56, № 3, 2014, с. 108–114*
2. *Сухов В.Е. Система обнаружения аномалий сетевого трафика на основе искусственных иммунных систем и нейросетевых детекторов // Вестник РГРТУ. 2015. №54. Часть 1 С. 84-90.*
3. *Селеменев А. В., Астахова И. Ф., Трофименко Е. В. Применение искусственных иммунных систем для обнаружения сетевых вторжений // Вестник ВГУ, серия: системный анализ и информационные технологии, 2019, № 2 С. 49-56.*

Науковий керівник — Константинова Л. В., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.056.53(045)

А. В. Ільєнко[1], М. К. Герасименко[2]
[1]*доцент, Національний авіаційний університет*
[2]*студентка, Національний авіаційний університет*

Практичні аспекти використання нейронних мереж в криптографії

Захист інформації завжди посідав важливе місце в усіх сферах життя суспільства. З кожним днем потреба в інтегруванні криптографічних систем для захисту інформації як на підприємствах, так і в фінансових установах зростає. Причина полягає у тому, що криптографія це потужний засіб для забезпечення контролю цілісності та конфіденційності.

Виділяють два види методів криптографічного захисту інформації за швидкістю криптографічних перетворень: *Симетричні методи.* Особливість полягає у використанні єдиного ключа для виконання операцій шифрування та дешифрування. *Асиметричні методи.* Особливість полягає у використанні відкритого ключа для шифрування та секретного для дешифрування.Використання різних ключів для шифрування/дешифрування виступає однією з переваг асиметричних методів над симетричними, оскільки дозволяє вирішити проблему розподілення ключів між користувачами. Рішенням проблеми передачі ключа шифрування/дешифрування є використання нейронних мереж. Для цього використовуються такі їх можливості: самостійне навчання, взаємне навчання, стохастична поведінка, низька чутливість до неточностей (спотворення даних, вагових коефіцієнтів та помилок в програмі). Це дозволяє вирішувати проблеми з відкритим ключем, їх розподіленням, хешуванням та генерацією псевдовипадкових чисел. Основна ідея використання нейронних мереж в симетричній криптографії – можливість синхронізації двох систем з випадковим початковим набором вагових коефіцієнтів, в результаті чого створюється спільний для двох систем вектор значень, який може бути використаний в якості секретного ключа в системах шифрування. Отже, користувачі повинні синхронізувати свої мережі. Для цього відправник дотримується такого алгоритму [1] рис. 1: Ініціалізація нейронної мережі; Генерування вхідного вектору для нейронної мережі із випадкової послідовності чисел; Перевірка рівності вхідних векторів нейромереж відправника і отримувача; Корегування вагових коефіцієнтів нейронної мережі; Генерування ключа шифрування/дешифрування на основі вагових коефіцієнтів нейронної мережі (при умові рівності виходів нейронних мереж відправника і отримувача).

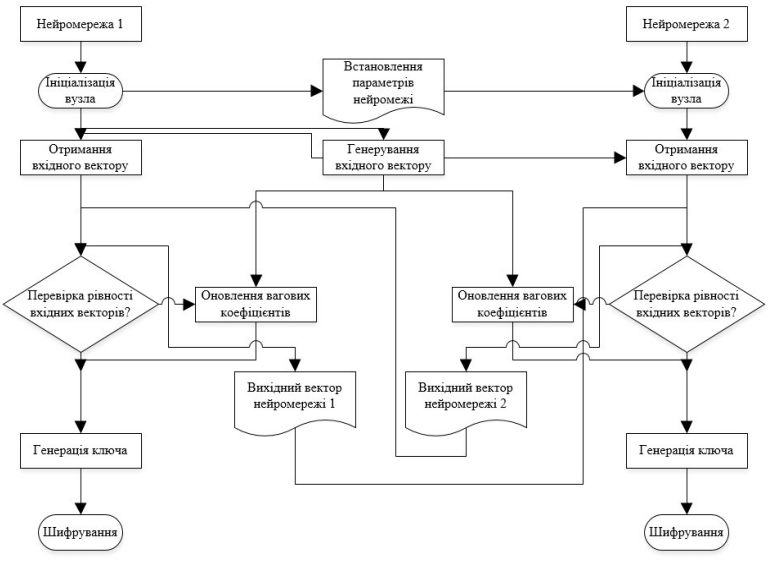


Рисунок 1 – Алгоритм синхронізування нейромереж

При використанні блочних шифрів текст розбивається на блоки фіксованої довжини. Такий спосіб має невисоку криптостійкість. До того ж, накопичення шифротекстів одного коду призводить до створення можливості розкриття секретного ключа.

Для підвищення криптостійкості блочних шифрів використовується нейромережа, яка дозволяє згенерувати ідентичні ключі, а також здійснити

перетворення інформації за правилами, відомими тільки абонентам, що забезпечує конфіденційність. Але недоліком такого підходу знову виступає можливість розкриття інформації при великому об'ємі повідомлення. Рішенням цієї проблеми є використання нейромережі з генерацією нового ключа для кожного блоку даних [2]: нейромережі синхронізуються; на вхід і вихід подається бінарна послідовність; використання 2-3 робочих шарів в нейромережі і одного коректуючого.

Як приклад інтеграції нейронних мереж в криптографії, можна розглянути також використання НС в функції хешування з трьома шарами [3]: вхідним, вихідним та прихованим. Вагові коефіцієнти та керуючі параметри для кожного шару створюються за допомогою генератора ключів. Ітерації проводяться тільки на вхідному та вихідному шарах для зменшення числа операцій, необхідних для обчислення функції хешування. Алгоритм переводить дані в довільної довжини в 128-бітне значення хеш-функції. Хоча така система володіє властивістю однобічності та більшою швидкодією за рахунок зменшення кількості операцій, вона має і ряд недоліків. Для роботи цього алгоритму необхідна генерація ключів, тобто статичних параметрів для нейромережі, які порушать вимогу до однобічності перетворення. Також при перевірці хеш-значення даних необхідно знати той самий ключ, використаний для шифрування.

Проектування архітектури нейромережі відбувається наступним чином: визначення кількості шарів (мінімальна кількість два шари – вхідний та вихідний, при збільшенні кількості шарів збільшується точність результату), визначення кількості нейронів кожному шарі, вибір типу зв'язків між нейронами, вибір функції активації (рис. 2).

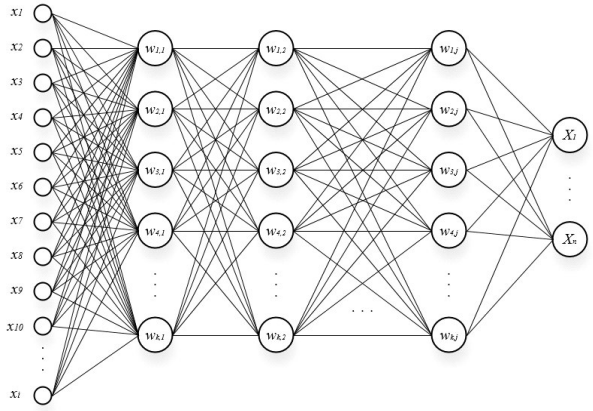


Рисунок 2 – Приклад архітектури нейронної

Загальна система нейронної мережі складається з вхідного набору даних (вхідного вектору $x_1 \dots x_i$), з прихованих шарів, кількість яких встановлюється дослідним шляхом для збільшення точності результату, та з вихідного вектору даних: Вхідний вектор подається як бінарна послідовності із 0 і 1. Зв'язок між нейронами визначається ваговими коефіцієнтами $w_{1,1} \dots w_{i,j}$ (для корекції коефіцієнтів $w_{i,j}$ використовується метод зворотнього поширення помилки), представлених матрицею, зсувом активації для контролю коректності результату $b_1 \dots b_i$, рівнем активації W та функцією активації $f(W)$, яка визначається відповідно до криптосистеми, яка використовується.

$$\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = \prod_i f\left(W = \begin{pmatrix} w_{1,1} & \cdots & w_{1,j} \\ \vdots & \ddots & \vdots \\ w_{i,1} & \cdots & w_{i,j} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_i \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_i \end{pmatrix} \right),$$

де i – кількість біт на вході, j – кількість шарів в НС, n – розрядність вихідного потоку даних.

Таким чином, нейронні мережі використовується для підвищення криптографічної стійкості системи та створення «захищеного каналу» між відправниками. До того ж, враховуючи те, що будь-яка функція може бути представлена нейромережею, існує можливість створювати нові типи атак на криптографічні алгоритми. Тому з огляду на властивість нейронних мереж досліджувати множину рішень, вони використовуються також і в криптоаналізі.

Список використаних джерел

1. *Ємел'янов В. О. Алгоритм передачі ключа в симетричному шифруванні.*
2. *Добриця В. П., Верютіна К. Г. Блочное шифрование с переменными ключами. стр. 4. https://esa-conference.ru/wp-content/uploads/2018/06/esa-may-2018-part1.pdf.*
3. *Shiguo Lian, Jinsheng Sun, Zhiquan Wang. One-way Hash Function Based on Neural Network. https://arxiv.org/ftp/arxiv/papers/0707/0707.4032.pdf.*

УДК 004.56.5

Д. С. Головко
студент, Центральноукраїнський національний технічний університет

Зміна напрямків розвитку кібербезпеки через COVID-19

Пандемія COVID-19 значно вплинула на всі сфери життя нашого суспільства, за результатами глобального опитування компанія Microsoft виділила п'ять пріоритетних напрямків розвитку ринку, які були визначені саме через пандемію.

Цифрова емпатія. Під час пандемії компанії визнали, що додатки для спільної роботи дійсно збільшують продуктивність і повинні стати пріоритетом при створенні здорового віддаленого робочого середовища. Microsoft назвала це явище «цифрова емпатія». Однак для її створення потрібно розширити політики безпеки, щоб співробітники могли використовувати якомога більше додатків для віддаленої роботи з домашніх комп'ютерів. Включення багатофакторної аутентифікації стало основою для подальших розробок і пріоритетним напрямком інвестицій під час пандемії для 41% керівників.

Нульова довіра. Zero Trust перетворилася в пріоритетний напрямок бізнесу, оскільки під час пандемії керівники намагалися впоратися з припливом нових, потенційно незахищених пристроїв, що підключаються до корпоративних мереж. Більше половини (51%) керівників прискорили розгортання Zero Trust і вважають, що з часом його використання стане галузевим стандартом. В цілому про плани розгортання нових можливостей Zero Trust повідомили 94% компаній, які брали участь в опитуванні Microsoft.

Нові інструменти боротьби з шахраями. За даними Microsoft, 54% керівників служби безпеки повідомили про приріст числа фішингових атак з початку пандемії. Боротися з ними дозволила розгорнута мережа хмарних інструментів і наборів даних. Microsoft заявила, що щодня відстежує більше восьми трильйонів повідомлень про погрози, використовуючи різноманітні продукти, послуги і канали. При цьому компанія комбінує автоматизовані інструменти та аналітичні здібності співробітників, щоб захистити кінцевих користувачів.

Кіберстійкість - основа бізнес-операцій. В умовах пандемії і роботи більшості співробітників на дому підприємства повинні турбуватися проблемою кібербезпеки, щоб регулярно оцінювати свої ризики і здатність реалізації нових планів. За даними Microsoft, хмарні технології можуть полегшити оцінку ризиків кібербезпеки і створення планів дій на випадок надзвичайних ситуацій. Більше половини «хмарних» і гібридних компаній в опитуванні Microsoft повідомили, що розробили стратегію кіберстійкості для більшості сценаріїв ризику, тоді як серед переважно локальних організацій ця частка склала лише 40%.

Хмара - запорука безпеки. Дослідження Microsoft показало, що про успішні фішингові атаки значно частіше повідомляли організації, які використовували локальні (36%), а не хмарні ресурси. У той же час майже 40% підприємств заявили, що віддають пріоритет інвестицій в хмарну безпеку, щоб знизити ризик злому. Слідом ідуть безпека даних і інформації (28%) і засоби захисту від фішингу (26%). В цілому, як вважає Microsoft, пандемія COVID-19 показала, що підприємствам необхідна інтегрована система безпеки, що охоплює кінцеві точки в хмарній сфері.

Науковий керівник — Бісюк В. А., викладач кафедри кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет.

УДК 621.396.2:004.056

І. Д. Гриценко
студент, Національний університет «Запорізька Політехніка»

Дослідження криптографічних механізмів захисту інформації в мережах LTE

В епоху всеохоплюючої діджиталізації сучасного світу, стільникові мережі зв'язку являються одними із найголовніших елементів в системі надання електронних сервісів. Останнім технологічним рішенням, яке знайшло широкого поширення, є LTE (Long Term Evolution) - стандарт високошвидкісного бездротового зв'язку передачі даних. Стандарт LTE відіграє ключову роль у взаємодії мереж різних поколінь так як є пограничним (проміжним) між мережами третього (3G) і п'ятого (5G) покоління.

В даній роботі досліджуються криптографічні засоби захисту в мережах 4G LTE в контексті забезпечення конфіденційності, цілісності та доступності інформації.

Вимоги безпеки до ядра мережі EPS (Evolved Packet Core) забезпечуються використанням технології безпечної доменної зони (NDS - Network Domain Security) на мережному рівні , а можливість використання UMTS та перехід із стандарту 3G на стандарт LTE, можливий завдяки механізму автентифікації та узгодження ключів AKA (Authentication and Key Agreement).

Відповідно до специфікацій консорціуму 3GPP (3rd Generation Partnership Project) для забезпечення цілісність даних використовується механізми цілісності шарів без доступу NAS (Non-Access Stratum) та шарів доступу AS (Access Stratum). Після завершення автентифікації та механізму узгодження ключів користувацького інтерфейсу UE (User Equipment) та модуля управління мобільністю MME (Entity Management Mobility) генерується спільний ключ «K_{ASME}», який використовується для генерації ключів цілісності AS та NAS (K_{UPint} та K_{NASint}, відповідно) [1], рис 1.

Під час генерації «K_{ASME}» використовується код розпізнавання автентифікації повідомлень HMAC. Для визначення HMAC використовується криптографічна хеш-функція на базі алгоритмів MD5 або SHA-1, та статичний ключ K, що зберігається на USIM та у центрі автентифікації AuC (Authentication Centre).

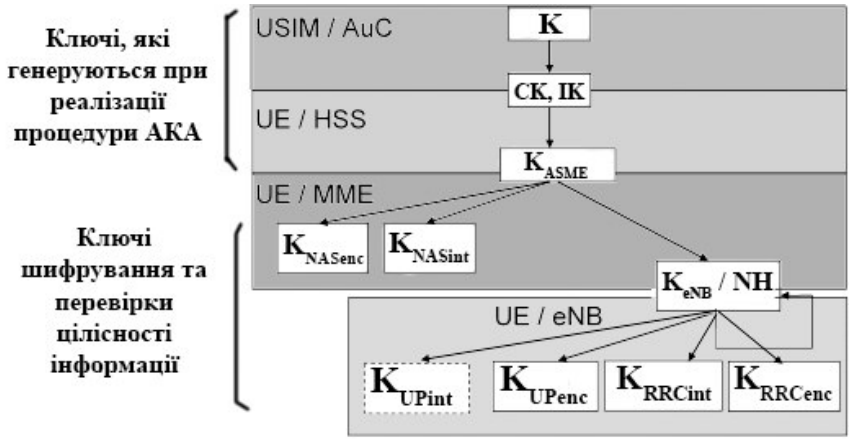


Рисунок 1 – Ієрархія ключів LTE

Довжина ключів K_{ASME} та K_{eNB} -256 біт, а усіх інших - 128 біт [2].

3GPP TS дає таке визначення кожному с цих ключів [2]:

– CK, IK – ключі отримані в AuC та USIM під час AKA;

– K_{ASME} – ключ управління захистом доступу (access security management entity);
– K_{NASenc} – ключ шифрування NAS сигнального трафіку;
– K_{UPenc} – ключ шифрування трафіку користувача;
– K_{eNB} – проміжний ключ для обчислення K_{UPenc} та K_{UPint};
– K_{RRCint} – ключ контролю цілісності сигнального трафіку;
– K_{RRCenc} – ключ шифрування сигнального трафіку;

Оскільки пакетна система нового покоління EPS (Evolved Packet System) була розроблена для довгострокової еволюції, 3GPP запровадив модульний механізм відбору доступних алгоритмів захисту цілісності. UE та eNB (eNodeB - вдосконалена базова станція) вибирають найкращий алгоритм, що підходить для них обох, спільно використовуючи код підтримуваного EIA (EPS Itegrity Algorithm - алгоритм цілісності EPS).

В EPS (EIA) визначені два обов'язкові алгоритми:
– 128EEA1 і 128-EIA1 - на основі SNOW 3G;
– 128EEA2 і 128-EIA2 - на основі AES.

Вказані алгоритми також використовуються для забезпечення конфіденційності інформації на усіх рівнях мережі LTE [1], рис 2:

– AS-трафік забезпечує конфіденційність між UE та eNB за допомогою K_{UPenc};
– NAS-трафік забезпечує конфіденційність між UE та MME за допомогою K_{NASenc};
– конфіденційність потоку даних між eNB та обслуговуючим шлюзом S-GW (Serving Gateway) / MME забезпечується за допомогою протоколу IPSec.

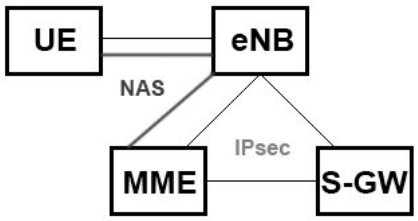


Рисунок 2 – Забезпечення конфіденційності на різних рівнях

Проведене дослідження криптографічних засобів захисту в стандарті LTE показало наявність достатньої кількості інструментів для забезпечення належного рівня захищеності конфіденційної інформації на всіх рівнях мережі.

Однак, існують ризики несанкціонованого доступу до інформації непов'язані з криптоаналізом – атаки на основні вузли мережі (MME, eNB, S-GW та ін.), – в разі успішності яких, зловмисник може отримати повний доступ до всіх критичних даних.

Варто зазначити, що мінімізація вразливостей від атак на ключову інформацію, безпосередньо пов'язана з наявністю безпечного середовища, в якому відбувається виконання таких чутливих операцій, як шифрування і розшифрування даних користувачів, зберігання ключів тощо. Крім того, обмін конфіденційними даними повинен проходити в межах цього безпечного середовища.

Список використаних джерел

1. *Abdo, J. B., Chaouchi H., Demerjian J. Security in Emerging 4G Network. Next-Generation Wireless Technologies: 4G and Beyond. London: Springer. 2013. P. 243-272.*
2. *3rd Generation Partnership Project, 3GPP TS 33.401 V11.2.0 (2011-12), 3GPP System Architecture Evolution (SAE); Security architecture (Release 11).*

Науковий керівник — Куцак С. В., старший викладач кафедри захисту інформації НУ "Запорізька політехніка".

УДК 004.056

Б. С. Клименко[1], С. А. Смірнов[2]
[1]*магістрант, Центральноукраїнський національний технічний університет*
[2]*доцент, Центральноукраїнський національний технічний університет*

Дослідження системи реалізації DLP-агенту

Вступна частина. Сьогодні ринок DLP-систем є одним із самих швидкоростучих серед всіх засобів забезпечення інформаційної безпеки. Втім, вітчизняна ІБ-сфера поки не зовсім устигає за світовими тенденціями, у зв'язку із ніж у ринку DLP-систем у нашій країні є свої особливості.

Перш ніж говорити про ринок DLP-систем, необхідно визначитися з тим, що, власне кажучи, мається на увазі, коли мова йде про подібні рішення. Під DLP-системами прийнято розуміти програмні продукти, що захищають організації від витоків конфіденційної інформації. Сама абревіатура DLP розшифровується як Data Leak Prevention, тобто, запобігання витоків даних.

Подібного роду системи створюють захищений цифровий «периметр» навколо організації, аналізуючи всю вихідну, а в ряді випадків і вхідну інформацію. Контрольованою інформацією повинен бути не тільки інтернет-трафік, але й ряд інших інформаційних потоків: документи, які виносяться за межі контуру безпеки, що захищається, на зовнішніх носіях, що роздруковуються на принтері, що відправляються на мобільні носії через Bluetooth і т.д.

Оскільки DLP-система повинна перешкоджати витокам конфіденційної інформації, то вона в обов'язковому порядку має убудовані механізми визначення ступеня конфіденційності документа, виявленого в перехопленому трафіку. Як правило, найпоширеніші два способи: шляхом аналізу спеціальних маркерів документа й шляхом аналізу вмісту документа. У цей час більше розповсюджений другий варіант, оскільки він стійкий перед модифікаціями, внесеними в документ перед його відправленням, а також дозволяє легко розширювати число конфіденційних документів, з якими може працювати система.

Об'єктом дослідження є процес реалізації DLP-агенту.

Предметом дослідження є методи реалізації DLP-агенту.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

–Удосконалено метод реалізації DLP-агенту.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі реалізації DLP-агенту.

Основна частина. Крім свого основного завдання, пов'язаного із запобіганням витоків інформації, DLP-системи також добре підходять для рішення ряду інших завдань, пов'язаних з контролем дій персоналу. Найбільше часто DLP-системи застосовуються для рішення наступних неосновних для себе завдань: контроль використання робочого часу й робочих ресурсів співробітниками; моніторинг спілкування співробітників з метою виявлення «потаємної» боротьби, що може нашкодити організації; контроль правомірності дій співробітників (запобігання печатки підроблених документів та ін.); виявлення співробітників, що розсилають резюме, для оперативного пошуку фахівців на посаду, що звільнилася.

За рахунок того, що багато організацій думають, що ряд цих завдань (особливо контроль використання робочого часу) більше пріоритетними, ніж захист від витоків

інформації, виник цілий ряд програм, призначених саме для цього, однак здатних у ряді випадків працювати і як засіб захисту організації від витоків. Від повноцінних DLP-систем такі програми відрізняє відсутність розвинених засобів аналізу перехоплених даних, що повинен вироблятися фахівцем з інформаційної безпеки вручну, що зручно тільки для зовсім невеликих організацій (до десяти контрольованих співробітників).

Головною тенденцією, як думають експерти, є перехід від «заплаткових» систем, що складаються з компонентів від різних виробників, що вирішують кожного своє завдання, до єдиних інтегрованих програмних комплексів. Причина подібного переходу очевидна: комплексні інтегровані системи рятують фахівців з інформаційної безпеки від необхідності вирішувати проблеми сумісності різних компонентів «заплаткової» системи між собою, дозволяють легко змінювати налаштування відразу для великих масивів клієнтських робочих станцій в організаціях, а також дозволяють не випробовувати складностей при перенесенні даних з одного компонента єдиної інтегрованої системи в іншій. Також рух розроблювачів до інтегрованих систем іде в силу специфіки завдань забезпечення інформаційної безпеки: адже якщо залишити без контролю хоча б один канал, по якому може відбутися витік інформації, не можна говорити про захищеність організації від подібного роду погроз.

Ще однією важливою тенденцією в сфері DLP є поступовий перехід до модульної структури, коли замовник може самостійно вибрати ті компоненти системи, які йому необхідні (наприклад, якщо на рівні операційної системи відключена підтримка зовнішніх пристроїв, те немає необхідності доплачувати за функціональність по їхньому контролі). Важливу роль на розвиток DLP-систем буде робити й галузева специфіка – цілком можна чекати появу спеціальних версій відомих систем, адаптованих спеціально для банківської сфери, для держустанов і т.д., що відповідають запитам самих організацій.

Немаловажним фактором, що впливає на розвиток DLP-систем, є також поширення ноутбуків і нетбуків у корпоративних середовищах. Специфіка лептопів (робота поза корпоративним середовищем, можливість крадіжки інформації разом із самим пристроєм і т.д.) змушує виробників DLP-систем розробляти принципово нові підходи до захисту портативних комп'ютерів. Варто відзначити, що сьогодні лише деякі вендори готово запропонувати замовникові функцію контролю ноутбуків і нетбуків своєю DLP-системою.

Висновки. Таким чином, у даній роботі було проведено дослідження системи реалізації DLP-агенту. Визначено актуальність цієї задачі. Напрямком подальшого розвитку вважаємо розроблення вітчизняного продукту реалізації DLP-агенту, який має більш широкі можливості, на відміну від існуючих аналогів.

Список використаних джерел

1. *Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I.,Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 166-171.*
2. *Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.*
3. *Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.*
4. *Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.*

УДК 004

С. М. Копаніцький
студент, Центральноукраїнський національний технічний університет

Захист даних користувача при розробці мобільних додатків для iOS

З кожним роком кількість користувачів мобільних телефонів у світі зростає. Адже сучасні смартфони досить потужні і можуть обробляти та зберігати велику кількість інформації. Один із напрямів для розробки є операційна система iOS, яка працює на пристроях від компанії Apple. Хоч платформа і має значно меншу кількість аудиторії в порівнянні з Android, але прибуток від продажу додатків отримує більший. Це обумовлено тим, що користувачі смартфонів на базі iOS більш платоспроможні. Велика платоспроможність приваблює розробників з усього світу, які створюють мобільні додатки для спрощення повсякденного життя людей.

Одним із ключових пунктів при розробці мобільного програмного забезпечення є захист користувацьких даних: номера кредитних карток, пін-коди, логіни, паролі і т.д. Щоб зловмисники не змогли отримати доступ до цієї інформації, треба вибрати правильне сховище. Всього в iOS є один фреймворк для управління базою даних та два системні сховища, з якими найчастіше доводиться працювати розробникам: core data; user defaults; keychain.

Core data - це фреймворк, який керує базою даних і дозволяє зберігати інформацію локально на пристрої. Інформація на вибір може зберігатися в: кеш-пам'яті, XML-файлі, бінарному вигляді або в SQLite. Фреймворк використовується для збереження основної інформації, якою оперує додаток.

User defaults - це сховище, яке використовується для збереження користувацьких налаштувань. Призначене для зберігання невеликих обсягів даних, котрі часто запитуються та рідко змінюються. Інші способи використання можу призвести до повільної роботи або більшого споживання пам'яті.

Keychain - це спеціалізоване сховище, призначене для зберігання метаданих та конфіденційної інформації. Для шифрування даних використовується 256-бітний алгоритм AES, який забезпечує безпечне зберігання інформації.

З вище перелічених сховищ можна виділити тільки одне, яке задовольняє потребам захисту даних користувача, і це keychain. Keychain в мові програмування Swift має застаріле API, що значно ускладнює роботу з ним. Для розв'язання цієї проблеми можна використовувати бібліотеки, які спрощують взаємодію зі сховищем: KeychainAccess, SwiftKeychainWrapper, KeychainSwift.

Попри те, що для збереження інформації використовується спеціалізоване сховище, для підвищення безпеки усі дані треба шифрувати за допомогою хеш-функцій. Мова програмування Swift надає пакет Swift Crypto, який містить набір криптографічних операцій. Однією із бібліотек в цьому пакеті є Crypto Kit, вона забезпечує розробників актуальними функціями хешування: md5; sha1; sha256; sha384; sha512.

Усі вживані заходи значно підвищують безпеку даних, і зводять до мінімуму ймовірність отримання їх зловмисниками. Напрям захисту персональних даних постійно розвивається і вносить нові підходи. Тому розробникам потрібно слідкувати за актуальною інформацією, і постійно підвищувати безпеку своїх додатків.

Науковий керівник — Ладигіна О. А., викладач кафедри кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет.

УДК 004.05

О. В. Мацола[1], Д. Ю. Хлапонін[2]
[1]*студент, Київський національний університет будівництва та архітектури*
[2]*доцент, Державний університет телекомунікацій, м. Київ*

Способи захисту інформації при використанні інтернету речей

Сьогодні пристрої Інтернету речей не лише масово використовуються у щоденному вжитку, але й у сучасному бізнес-середовищі.. Поступово пристрої IoT стають невід'ємною частиною багатьох бізнес-процесів, і зростання їх кількості спричиняє виникнення нових проблем безпеки.

Не існує точних рамок або списку приладів, де можна застосувати систему Інтернету речей. На практиці IoT можна запровадить навіть в приватному будинку, оскільки практично будь-який фізичний об'єкт можна перетворити в "розумний". Але якщо розібратися більш детально, то Інтернет речей можна впровадити:

– розумний будинок - з розумною системою кондиціонування або обігріву, розумним чайником або кавоваркою тощо;

– промисловість - програмні системи, сенсори, аналіз даних, розумні машини і обладнання;

– охорона здоров'я - медичні дрони, відкриття в генетиці, індивідуальний підхід до пацієнтів, аналіз роботи лікаря;

– рітейл - найпопулярніше це безконтактна оплата і спеціальні програми для покупок і доставки онлайн.

Крім перерахованих сфер, IoT також можна застосувати в енергетиці, для автомобілів, смартфонів і гаджетів, системи безпеки (в тому числі камери відеоспостереження) і звичайно ж - побудувати розумний місто.

Основні загрози для IoT:

1. Небезпечні мережеві сервіси;
2. Фізична незахищеність;
3. Витік конфіденційність даних;
4. Незахищені мобільні додатки;
5. Неякісна або застаріла прошивка або ПЗ.

Атаки зазвичай проходять в таких етапах:

Етап 1: Розвідка - дослідження цілі, до того, як вона буде уражена. Вона може бути пасивною без прямої взаємодії з ціллю. Онлайн-ресурси, наукові праці, веб-сайти, наявна документація, соціальна інженерія тощо, використовуються на цьому етапі.

Етап 2: Пошук вразливих місць - коли зібрано достатньо інформації розвідка за допомогою певних інструментів, таких як порти або інші сканери вразливості, хакери намагаються зібрати інформацію про особливості системи та знайти інші вразливі місця. Будь-яка вразливість дозволяє створити новий вектор атаки.

Етап 3: Атака - коли вразливі місця виявленні, тоді атаки спрямовуються проти їх. Існує досить багато варіантів атак. Новою специфічною атакою IoT є прокатні коди (rolling codes), які широко використовуються в галузі автоматизації (замки на ключі тощо). Це робиться з допомогою різних інструментів, таких як RF-Crack, глушителів сигналу, сканерів, чи повторних програвачів, тощо.

Етап 4: Отримання доступу – зловмисники проникають в систему через недостатньо захищені мережі, вразливі чи переписані ОС, або програми.

Етап 5: Забезпечення постійного доступу, утримання анонімності - підтримка доступу так само важлива як отримання доступу. Отже, хакери докладають багато зусиль, щоб досягти повного контролю над (PWN) системи.

IoT щодня наражає користувачів на підвищений ризик. Превентивні заходи повинні бути задіяні прямо зараз. Справа не лише у використанні найнадійніших паролів чи просто використання програм, які шифрують свої данні. Ми можемо зробити більше, нам потрібно навчитися виявляти шкідливе програмне забезпечення та програми-вимагачі, та інвестувати в програмне забезпечення, яке може захистити дані користувачів та систем шляхом впровадження найкращих практик та використання найкращих інструментів від лідерів ринку.

Є кілька дуже корисних практик, які можуть бути застосовані не лише для IoT систем, але і для всіх систем, які використовують Інтернет чи покладаються на віддалений доступ, їх використання може вберегти нас від багатьох проблем. Необхідно завжди змінювати облікові дані за замовчуванням і ніколи не покладатись налаштування за замовчуванням, переконуватись, що пристрої використовують надійну аутентифікацію, ізолювати IoT мережі від інших виробничих та промислових мереж, якщо це можливо, використовувати системи захисту / виявлення вторгнень, використовувати PKI / End-2-End шифрування та VPN (Virtual Private Network) разом з білим списком IP, слідкувати за telnet та портом 48101, вимикати UPnP (універсальний plug and play). Оновлювати не тільки шлюзи, а також пристрої, тому що багато атак можна зупинити, якщо встановити останні патчі безпеки та оновлення вчасно. Обмежити фізичний доступ до системи та пристроїв, якщо зловмисник має фізичний доступ до вашого пристрою, ви більше не володієте цим пристроєм.

Бажано використовувати функцію дистанційного блокування, коли немає необхідності у віддаленому доступі до пристрою. Вимкнути незадійяні послуги, порти, програми та налаштування. Функція безпечного завантажувального ланцюга (secure boot chain) захищає пристрій від запущення фальсифікованої версії програмного забезпечення шляхом перевірки її оригінальності.

IoT швидко зростає, і різні галузі все більше покладаються у своєму бізнесі на пристрої, які підключені до Інтернету. Дослідження в цій галузі переважно орієнтовані на збір даних у режимі реального часу, маніпулюванням даними на місці, ефективним виявленням даних та візуалізацію в режимі реального часу. Дані, що генеруються різними IoT джерелами відкривають нові можливості для інноваційних додатків у різних галузях. Але ці можливості не повинні ставити під загрозу безпеку.

Список використаних джерел

1. *Varga E., Draskovic D., Mijic D. Scalable Architecture for the Internet of Things. O'Reily. 2018*
2. *Bhuvaneswari V., Porkodi R. The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview. International Conference on Intelligent Computing Applications, pp 324. – 329, 2014.*
3. *Stalling W., Operating Systems: Internals and Design Principles. Pearson. 2018*
4. *Dineva K., Atanasova T. Computer System Using Internet of Things for Monitoring of Bee Hives, 17th International Multidisciplinary Scientific GeoConference SGEM 2017, Vienna GREEN Conference Proceedings, Vol. 17, Issue 63, pp 169-176, 2017.*
5. *Dominguez S., The Target Breach – Case Study, Lessons Learned and the Lockheed Martin Intrusion Kill Chain Model, IBM Lab Services, , 2016.*
6. *Alexandrov A., Monov V., ZigBee smart sensor system with distributed data processing, Proc. of the 7-th IEEE International Conference Intelligent Systems IS'2014, Vol. 2: Tools, Architectures, Systems, Applications, Warsaw Poland, Advances in Intelligent Systems and Computing, Springer, Vol. 323, pp 259-268, 2014.*

Науковий керівник — д.т.н., професор Хлапонін Ю. І., завідувач кафедри кібербезпеки та комп'ютерної інженерії, Київський національний університет будівництва та архітектури.

УДК 004.056.55

Д. Ю. Микитенко
студент, Центральноукраїнський національний технічний університет

Використання простих чисел для криптографічного захисту інформації

Актуальність роботи: На сучасному етапі розвитку суспільства однією з найбільших цінностей стала інформація. Важливим питанням є захист інформації. Існує декілька напрямків та підходів до захисту інформації, і один із них це криптологія, тобто захист математичними методами. Розвиток комп'ютерної техніки та математичного апарату дає зловмисникам все більше можливостей для дешифрування інформації. З плином часу до алгоритмів шифрування висуваються все більш суворі вимоги, а кожний новий запропонований метод перевіряється все більш детально на велику кількість вразливостей.

Одним із методів криптографічного захисту конфіденційності інформації є алгоритм шифрування RSA (Rivest, Shamir, Adleman). На сьогодні відомо багато таких шифрів, які щодня захищають велику кількість інформації. Тому питання про їхню стійкість турбує криптографічну спільноту й є як ніколи актуальним.

Принцип безпеки алгоритму RSA базується на складній факторизації. Застосовуються відкритий та закритий ключі, які разом утворюють пари ключів. Відкритий ключ використовується для шифрування даних і не зберігається в таємниці. Його можна повідомити іншому учаснику або десь опублікувати. Але якщо цим відкритим ключем зашифрувати повідомлення, то тільки відповідним закритим ключем можна розшифрувати це послання, який зберігається в секреті.

RSA дозволяє зашифрувати і розшифрувати повідомлення, передане між користувачами. В основі RSA лежить завдання факторизації множення двох простих великих чисел. І з пари цілих чисел складаються відкритий і закритий ключі. Для шифрування використовується проста операція піднесення до степеню за модулем N. Для розшифрування ж необхідно обчислити функцію Ейлера від числа N, для цього необхідно знати розкладання числа n на прості множники. Головною перевагою саме цього алгоритму є простота реалізації і висока швидкість роботи за рахунок використання більш простих операцій. Однак якщо один з ключів буде скомпрометований, будь-яка спроба захистити секретну інформацію втратить свій сенс. Така проблема вирішується в асиметричних криптосистемах за допомогою спеціальних алгоритмів. У таких системах дуже складно обчислити з одного ключа інший, тому поки комп'ютери не володіють високою продуктивністю (тобто не є квантовими), користувачі можуть бути спокійні за секретність своїх даних.

В умовах низької швидкості шифрування повідомлення слід застосовувати симетричні алгоритми з сеансовим ключем, тобто випадковим. В цьому випадку алгоритмом RSA шифрують сеансовий ключ.

Області застосування систем з використанням RSA досить широкі: для захисту програмного забезпечення; в схемах цифрового підпису; у відкритих системах шифрування PGP; в системах шифрування в поєднанні з симетричними алгоритмами.

Розглянемо приклад: шифрування повідомлення. Для наочності обчислення, будемо використовувати невеликі числа. Але на практиці використовують дуже великі числа (довжиною 200-300 десяткових розрядів).

Дії об'єкта B: Для простого P=5 і простого Q=7 знаходить модуль $N=P\times Q=5\times 7=35$. Обчислює значення функції Ейлера при N=35:

$$\varphi(N)=(P-1)\times(Q-1)=4\times 6=24.$$

В якості відкритого ключа Кв використовується довільне число з урахуванням умови: 1<Кв≤φ(N), НСД (Кв, φ(N))=1, тобто Кв і φ(N) є взаємо простими, нехай Кв=7. Знаходимо значення секретного ключа кв, використовуючи алгоритм Евкліда: кв ≡ = 1. Об'єкт В передає об'єкту А пару чисел (N = 35, Кв = 7).

Дії об'єкта А: Формує зашифроване повідомлення як послідовність цілих чисел в діапазоні 0 ... 32. Нехай літера А шифрується як число 1, літера В це 2 і т.д. Припустимо, що повідомлення AFOODE можна показати як послідовність чисел 1,6,15,15,4,5, тобто відкритий текст: $M_1=1$, $M_2=6$, $M_3=15$, $M_4=15$, $M_5=4$, $M_6=5$. Шифрує повідомлення М, використовуючи ключ Кв=7 і N=35 за формулою: $Ci=Mi^{Кв}(\text{mod } N)=Mi^7(\text{mod } 35)$.

$$\text{Тобто } C_1=1^7(\text{mod } 35)=1(\text{mod } 35) = 1,$$
$$C_2=6^7(\text{mod } 35) = 279936(\text{mod } 35) = 6,$$
$$C_3=15^7(\text{mod } 35)= 170859375 (\text{mod } 35) = 15,$$
$$C_4=15^7(\text{mod } 35)= 170859375 (\text{mod } 35) = 15,$$
$$C_5=4^7(\text{mod } 35) = 16384(\text{mod } 35) = 4,$$
$$C_6=5^7(\text{mod } 35)= 78125 (\text{mod } 35) = 5.$$

Передає об'єкту В криптограму: $C_1, C_2, C_3, C_4, C_5, C_6 = 1, 6, 15, 15, 4, 5$.

Дії об'єкта В: Розшифровує прийняту криптограму $C_1, C_2, C_3, C_4, C_5, C_6$ використовуючи секретний ключ кв ≡= 3 за формулою: $M_i=C_i^{кв}(\text{mod } N) = C_i^3(\text{mod } 85)$.

$$\text{Тобто } M_1=1^1(\text{mod } 35) = 1 (\text{mod } 35) = 1,$$
$$M_2=6^1(\text{mod } 35)= 6 (\text{mod } 35) = 6,$$
$$M_3 = 15^1 (\text{mod } 35) = 15 (\text{mod } 35) = 15,$$
$$M_4 = 15^1 (\text{mod } 35) = 15 (\text{mod } 35) = 15,$$
$$M_5 = 4^1 (\text{mod } 35) = 4 (\text{mod } 35) = 4,$$
$$M_6= 5^1 (\text{mod } 35) = 5 (\text{mod } 35) = 5.$$

Об'єкт В отримав початкове повідомлення, яке послав об'єкт А – це AFOODE, при шифруванні якого використовувався відкритий ключ, а при дешифруванні – закритий (секретний).

Оскільки в даному прикладі використано маленькі прості числа 5,7, то для подальших досліджень планується скористатися великими простими числами. Так було написано програму на C#, яка за допомогою алгоритму Гордона згенерувала сильне просте число 154832679977. Хоча воно і має лише 12 цифр (для прикладу останнє знайдене в 2018 році надвелике просте число Мерсенна має 23249425 цифр) та є обнадійливим в майбутньому.

Хоча на сьогодні шифрування RSA й застосовується у великій кількості сфер, але й досі цей метод має свої недоліки, тож у планах подальших досліджень є формування підходу до оптимізації роботи RSA та формування підходу до виправлення недоліків.

Список використаних джерел

1. *ISO / IEC 9796 RSA. Cryptographic Token Interface Standard.*
2. *The Largest Known Prime Number. Slate: веб-сайт. URL https://slate.com/technology/2018/01/the-worlds-largest-prime-number-has-23249425-digits-heres-why-you-should-care.html (дата звернення: 17.11.2020).*
3. *Захарченко М. В. Асиметричні методи шифрування в телекомунікаціях: навч. посіб. / М. В. Захарченко, О. В. Онацький, Л. Г. Йона, Т. М. Шинкарчук. – Одеса: ОНАЗ ім. О. С. Попова, 2011. – 184. – (Криптографічні методи захисту інформації в телекомунікаційних системах та мережах: модуль 2 з дисципліни „Захист інформації в телекомунікаційних системах та мережах").*

Науковий керівник — Поліщук Л. І., старший викладач кафедри кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет.

УДК 004.056

М. М. Мулярчук
магістрант, Центральноукраїнський національний технічний університет

Дослідження системи кібербезпеки, побудованої на використанні Cyber Threat Hunting та Data Science

Вступна частина. Штучний інтелект і пов'язані з ним терміни машинне навчання й нейромережі сьогодні активно використовують для просування нового покоління інформаційних систем. Терміни «самонавчаємий», «інтелектуальний» стали маркетинговими «мемами», як колись слово smart («розумний»), згадайте – смартфон, розумні годинники, розумний будинок і т.д., тому ними користуються зайво часто. «Інтелектуальний», як і «розумний», – завжди дорожче, ніж звичайний, тому важливо відрізняти, де це слово означає технології, що створюють принципово нову якість, а де тільки обгортка й маркетинг. Особливо це важливо в інформаційній безпеці, де часто помилка – це прямий збиток. Специфіка інформаційної безпеки, на відміну від інших інформаційних технологій, у тому, що навчання на старих даних не ефективно. Якщо справа стосується розпізнавання осіб, планування товарних запасів або машинного перекладу текстів – то навчання на старих паттернах – основа успіху таких алгоритмів машинного навчання. Чим більше правильно розпізнаних осіб, правильно перекладений текст, правильно спланованих запасів – тим краще алгоритми будуть працювати в майбутньому – об'єкт вивчення не буде сильно мінятися й можна усе більше заглиблюватися в деталі – адже не можна очікувати, що в людей з'явиться третє око або в мові радикально зміниться морфологія або синтаксис. Cyber Threat Hunting (тут і далі – також хантинг) – це процес проактивного й ітеративного пошуку й виявлення просунутих погроз, які неможливо виявити традиційними засобами захисту. Даний процес розпадається на ряд загальновизнаних технік хантингу. Data Science – наука про дані, відповідальна за обробку й добування корисної інформації з масивів структурованих або неструктурованих даних.

Таким чином, виходячи з вищеперерахованого, дослідження системи кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science, є актуальною задачею, яка потребує вирішення у даній роботі

Об'єктом дослідження є процес кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science.

Предметом дослідження є методи кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

–Удосконалено метод кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science.

Основна частина. Термін «Data Science» у контексті Cyber Threat Hunting розкривається як набір технік і прийомів, за допомогою яких здійснюється хантинг і які несуть у собі специфічні принципи роботи з даними. Далі розглянемо кожну з технік.

Техніки *Cyber Threat Hunting*:

– Базовий пошук.

– Статистичний аналіз.
– Техніки візуалізації.
– Прості агрегації.

Машинне навчання

Алгоритми машинного навчання (Data Mining), у якості ще однієї техніки Cyber Threat Hunting, успішно застосовні при фільтрації спаму, виявленні шкідливого трафіку й детектувані шахрайських дій. Успішно впроваджені в процес хантингу алгоритми здатні істотно підвищити ефективність захисту інформації. Зазначені алгоритми можна впроваджувати в засоби захисту інформації, які вимагають серйозної ресурсної й організаційної підготовки, як в IT, так і в ІБ-секторі. Дані алгоритми підрозділяються на два типи: «навчання із вчителем» і «навчання без вчителя».

Розроблена схема кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science включає в себе симетричну нейросистему, що реалізує нейромережевий алгоритм шифрування. Система характеризується простотою використання внаслідок автоматичності процесів налаштування параметрів нейроної мережі та швидкодією за рахунок використання блокової структури. Вхідною інформацією (блок "Джерело повідомлень") служать файли даних, ефективна обробка яких забезпечується шляхом оперування побітовим машинним кодом. Внутрішні параметри програмних модулів (для алгоритму кодування, генерації ключа та ін.) можуть вводитись в інтерактивному режимі або встановлюватись з попередньо створених бібліотек. Для експериментальних досліджень і подальшого гнучкого функціонування в програмних модулях передбачена можливість зміни параметрів, таких як рівень завад в каналі зв'язку та довжина ключа. Наведено дані щодо застосування створених спеціалізованих програмних реалізацій для розв'язування практичних завдань. Кожна компонента наведеної схеми містить елементи, що передбачають використання нейромережі та реалізують задачі підтримки інформаційних характеристик з наперед обумовленим ступенем захисту. В залежності від вибраної задачі (забезпечення цілісності, конфіденційності) в процесі роботи використовується відповідний модуль схеми і певна конфігурація кожної складової.

Висновки. Таким чином, у даній роботі було проведено дослідження системи кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science. Визначено актуальність цієї задачі. Напрямком подальшого розвитку вважаємо розроблення вітчизняного продукту кібербезпеки побудованої на використанні Cyber Threat Hunting та Data Science, який має більш широкі можливості, на відміну від існуючих аналогів.

Список використаних джерел

1. *Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I.,Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 166-171.*
2. *Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.*
3. *Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.*
4. *Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.*

Науковий керівник — доктор технічних наук, професор Смірнов О. А., завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.056.57:004.492

А. В. Небесний
студент, Центральноукраїнський національний технічний університет

Дослідження ефективності найпопулярніших антивірусних программ з використанням справжніх вірусних загроз

В наш час, неможливо уявити життя без інформаційних технологій. Основним джерелом знань сьогодні є інтернет. Дуже корисна річ! Легко ж відкрити сторінку браузера та знайти щось потрібне. І мабуть безпечно. Але це не так. Кожного разу, відкриваючи веб-сайт, ми ризикуємо натрапити на шкідливе програмне забезпечення, що так і мріє потрапити на наш девайс та покопатися в його пам'яті. Це шкідливе програмне забезпечення носить назву – вірус. Ми вже починаємо забувати про них, вважаємо що вони вже пішли в минуле. Але, як мовлять "ворог не дрімає". Виникає запитання, а що там з захистом. Що трапилося з галуззю інтернет-захисту? Актуальність цієї проблеми і стала причиною написання цієї праці.

Вже дуже рідко можна натрапити на веб-ресурс з зараженим програмним забезпеченням. Їх залишилося дуже мало, й більшість з них перейшли в чорний список. Основним джерелом розповсюдження були рекламні банери, але більшість людей вже їх не помічає, так як встановили adblock. Але, якщо комусь вдалося натрапити на вірус, то цій людині буде гірко. Адже хоч вони і рідкість, вони є дуже агресивними і обережними. Основними є:

1. Вірус завантажувального сектора: вірус даного типу проникає в середину основного завантажувального сектора на жорсткому диску. Звідти він отримує інструкції завантаження системи та вносить себе в цей розділ. Потім під час завантаження, вірус виділяє собі місце в оперативній пам'яті та починає звідти керувати системою.
2. Винищувач файлів – даний вірус потрапляючи в систему, починає шукати та видаляти важливі файли системи або дані користувача.
3. Вірус Mass Mailer – даний вірус шукає в системі месенджери. Потім він проникає в середину адресної бази та зчитує усі відомі месенджеру email адреси. Під кінець, він розповсюджується на інші системи, використовуючи заражене ПЗ та отримані email адреси.
4. Макро віруси – це шкідливе програмне забезпечення, що розповсюджується ховаючись всередині office документів. Написані мовою програмування Macro або VBA.
5. Поліморфні віруси – вірусне програмне забезпечення, що постійно маскує себе змінюючи свій код кожного разу, коли заражають нову систему або програму. Це ускладнює завдання антивірусу, знайти та знищити. Також має здатність мутувати.
6. Броньований вірус: розробляється для ускладнення процесу виявлення шкідливого ПЗ у системі. Під час видалення має здатність захищатися.
7. Стелс-вірус: приховує свою присутність від антивірусів шляхом зміни розміру файлів та каталогу. Має антиевристичну природу, що допомагає сховатися від евристичного виявлення.
8. Ретровірус – вірус, завдання якого вивести з ладу антивірус. Він проникає в систему та припиняє роботу антивірусної програми або руйнує її базу даних.
9. Універсальний – має властивості кожного з вище перелічених. Є найнебезпечнішим.

Тепер перейдемо до основної мети. Дізнатися про ефективність антивірусних програм в наш час. Спочатку для того, щоб дізнатися думку експертів та інших користувачів, було відвідано декілька веб-сайтів, на яких описувалися основні недоліки

та переваги. Список топ антивірусів був досить сумнівним, адже в ньому зустрічалися вже перевірені особисто екземпляри. Тому було вирішено провести власний експеримент.

Для проведення експерименту було створено віртуальну машину, досить слабку, щоб перевірити оптимізацію програмного забезпечення для захисту системи. Далі було завантажено архів з вірусами та встановлено декілька антивірусних програм. Серед них були найпопулярніші, а саме: Avast, Avira, Dr.Web, Eset, Kasperskiy, а також стандартний Захисник Windows.

Першим було перевірено антивірус Avira. Дана антивірусна програма була досить ефективною, так як їй вдалося помітити загрозу ще в архіві. Потім програма помістила небезпечне програмне забезпечення в карантин та вивела повідомлення про загрозу на екран. У вікні антивірусу надається можливість видалити файли або повернути їх на місце. Недоліками Avira є довгий процес інсталяції та відсутність можливості відмінити дію, що призводить до помилок при 4 запущених процесах.

Наступним став Avast. Варто відмітити, що в 2019 році Avast став одним з найкращих антивірусних програм. Але під час мого дослідження він показав найгірші результати. Avast видаляє загрози одразу, як тільки помічає їх. Він нераз відправляв в карантин архів з вірусами. Але коли на основному диску опинилося декілька вже розпакованих вірусів, Avast їх навіть не знаходив. Він помітив представлену небезпеку в системі, лише після вказання на неї.

Потім було протестовано антивірус NOD 32. Даний антивірус було перевірено досить ретельно, так як він включає в себе не лише захист системи, а й захист користувача від небезпек в інтернеті. Антивірус NOD 32 блокує усі підозрілі веб-сайти і не дає користувачу можливості відвідати їх. Також він повідомляє про загрозу, що з'явилася в системі, але сам він вирішити усі питання не здатний. Йому обов'язково необхідно дати дозвіл. Одного разу, NOD 32 не вивів повідомлення про небезпеку, тому її не було помічено. В результаті постраждала уся система в тому числі й антивірус. Виявилося, що на систему було встановлено маскувальник і декілька троянів. Так би мовити, NOD 32 не здатний ідентифікувати антивіруси типу стелс. Виникали проблеми під час інсталяції на слабкій конфігурації системи.

Далі було перевірено антивірус Kasperskiy, що є найефективнішим за даними з перевірених сайтів. Він здатний сканувати систему без участі користувача та поміщати загрози в карантин. Також він забезпечує безпеку під час пошуку інформації в інтернеті, блокуючи банери та підозрілі веб-ресурси.

Dr.Web – гарний супротивник антивірусу Kasperskiy. Він також здатний блокувати веб-ресурси з підозрілим або небезпечним вмістом, сканувати систему на наявність загроз та видаляти їх без участі користувача. Антивірус має можливість відновлювати свою базу після ушкоджень самостійно, без повторної інсталяції і використання сервісної служби. Окрім цього, Dr.Web єдиний з перелічених антивірусів, якому вдалося виявити та видалити вірус типу стелс. На додачу до своєї ефективності, ще й не використовує багато ресурсів та не має збоїв.

Захисник Windows – антивірус, що має багато недоліків. Він не здатний сканувати систему на наявність небезпечного програмного забезпечення автоматично. Постійно блокує безпечні дії користувача та використовує занадто багато ресурсів представлених системою.

Отже, як висновок, можна сказати, що більшість антивірусів не здатні підтвердити свій високий рейтинг.

Науковий керівник — Поліщук Л. І., старший викладач кафедри кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет.

УДК 004.56:004.93

Д. І. Орловський
студент, Національний університет «Запорізька політехніка»

Використання цифрового відбитку браузера для ідентифікації користувача у мережі

За останнє десятиліття відбулися суттєві зміни у підходах до розробки веб-додатків, які пов'язані з переходом на мікро-сервісну архітектуру. Зросла кількість програмного коду клієнтської складової додатку. Такі зміни в архітектурі програмного забезпечення торкнулись й систем автентифікації та авторизації. Тепер система авторизації становить складову частину REST (Representational State Transfer) – стилю з передачею репрезентативного стану веб-платформи – і має риси мікро-сервісу, що зобов'язаний займатися питанням надійного розмежування доступу до мережних ресурсів. Разом з відомими на сьогодні методами ідентифікації, автентифікації та авторизації (логіни-паролі, токени, виділені IP-адреси тощо) широке використання отримав новий підхід, що базується на цифрових відбитках (ЦВ).

В даній роботі був проведений огляд та запропонована реалізація механізму ідентифікації користувачів в мережі Internet, що базується на цифровому відбитку браузера (Browser fingerprint).

Browser fingerprint створюється шляхом визначення унікального хешу (ідентифікатора) користувача за допомогою математичних перетворень технічної інформації про його браузер та комп'ютер. За аналогією з відбитком пальця людини, кожен гаджет має унікальний, незмінний цифровий відбиток, використовуючи який, можливо однозначно визначати кожний пристрій в мережі. Дослідження [1] показало достатньо високу унікальність відбитків, яка для 118934 зразків складає 81% на мобільних девайсах і 90% на персональних комп'ютерах.

Основними параметрами, на базі яких формується ЦВ є: часовий пояс, заголовки браузера, User-agent (браузер, версія операційної системи (ОС), тип пристрою користувача, і т.д.), роздільна здатність монітора, конфігурацію Cookies, системні шрифти, додатки до браузеру, журнал користування браузером тощо.

Значення розходження та стабільності цифровому відбитку браузера залежить від таких факторів:

1. Фактор розходження: не існує декількох пристроїв з повністю однаковими технічними характеристиками, log-файлами браузера, Cookies, тощо. Однак можлива ситуація, коли велика кількість пристроїв мають однакові налаштування і відповідно – однакові відбитки. Особливо актуальна ця проблема для встановлених на підприємствах комерційних ОС (наприклад: Windows LTS). Одним із засобів збору відбитків є використання скриптових мов на рівні клієнтської частини веб-застосунку, які будуть збирати більшу кількість параметрів. Проте, відбиток, зібраний з великої кількості даних, більш вразливий до зміни налаштувань комп'ютера та є нестабільним.

2. Фактор стабільності: відбиток браузера без зміни конфігурації браузера та комп'ютера ніколи не зміниться. Однак, якщо системний адміністратор при використанні хешу цифрового відбитку під час авторизації буде повністю довіряти лише конфігурації браузеру, то може відбутися «витік» хешу. Таким чином, постає необхідність формування цифрового відбитку з параметрів, які не змінюються на більшості браузерів.

У роботі був реалізований алгоритм визначення цифрового відбитку браузера на мові JavaScript за допомогою бібліотеки fingerprintjs2 [2], яка користується нововведеннями стандарту HTML5 (HTML-тег «canvas», підтримка Emoji) та ES2017. Під час відвідування користувачем сторінки, сценарій створення відбитків пальців

малює текст кирилицею та латиною з використанням символів Unicode(зокрема Emoji) та системним шрифтом у розмір екрану. Позаду тексту додається кольоровий задній фон, анімовані геометричні фігури у тезі «canvas». Потім, за допомогою JavaScript, отримане «полотно» перетворюється в рядок у форматі Base64, доповнюючи отриманий хеш іншою інформацією щодо конфігурації браузера, конфігурації ПК, часової зони, наявності розширень браузеру та засобів анонімізації тощо. Отриманий у результаті хеш стає цифровим відбитком браузера [3]. Реалізації алгоритму визначення цифрового відбитку браузера зображена на схемі (рис. 1).

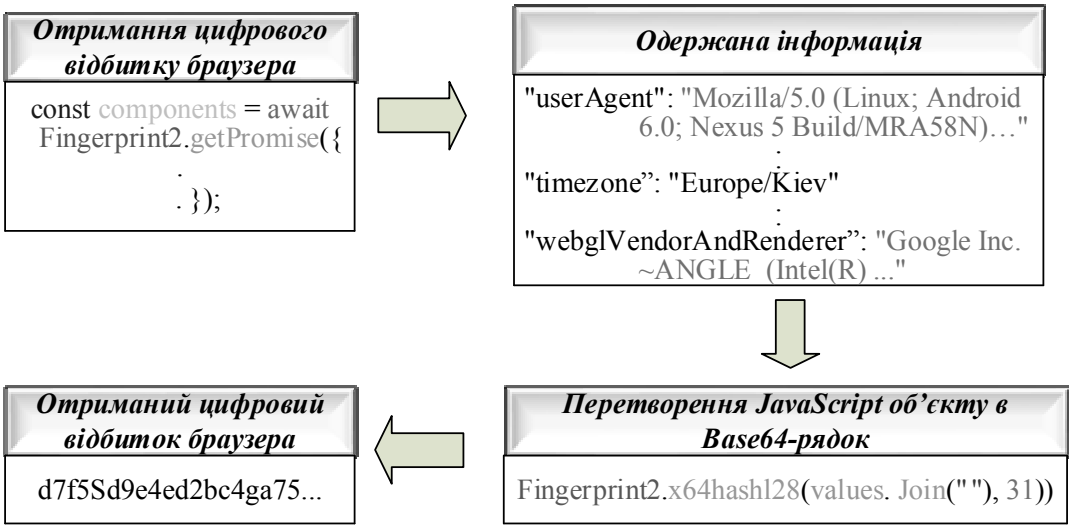


Рисунок 1 – Схема перетворення хешу

Основним призначенням цифрового відбитку браузера є [3]:

– виявлення у мережі ботів і «небажаного» трафіку: використовується для веб-сайтів фінансових організацій, державних установ, даючи можливість відокремити поведінку легального користувача від активності зловмисників;

– визначення користувачів VPN, TOR, proxy на веб-сайті: спеціальні служби можуть використовувати цей метод для відстежування інтернет-користувачів з прихованими IP-адресами задля їх персоналізації.

Таким чином, технологія відбитків браузера, маючи велику унікальність, точність та інформативність у порівнянні зі звичайною ідентифікацією за IP-адресою є дієвим методом для ідентифікації користувача у мережі Інтернет. Використання цифрових відбитків фахівцями з інформаційної безпеки може значно підвищити якість систем захисту веб-застосунків та запобігти використання користувачем засобів анонімізації. Також, цифровими відбитками можуть користуватися аналітики, спеціалісти з Data Mining (збір та агрегації неупорядкованих даних) з метою організації та проведення рекламних, агітаційних компаній у мережі.

Список використаних джерел

1. *Pierre Laperdrix, Walter Rudametkin, Benoit Baudry «Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints». INSA-Rennes & INRIA. Rennes, France, 2016. – С. 12–13. – URL: https://hal.inria.fr/hal-01285470v2/document. (дата звернення: 22.11.2020).*
2. *Fingerprintjs/fingerprintjs URL: https://github.com/fingerprintjs/fingerprintjs. (дата звернення: 22.11.2020).*
3. *Browser Fingerprinting. What Is It and What Should You Do About It? URL: https://pixelprivacy.com/resources/browser-fingerprinting/. (дата звернення: 22.11.2020).*

Науковий керівник — Куцак С. В, старший викладач.

УДК 004.932

А. О. Поліщук
студент, Центральноукраїнський національний технічний університет

Доцільність використання захисту інформації, залежно від рівнів

В теперішній час життя без комп'ютерів стало неможливим та разом з цим з'явилося багато питань з приводу захисту інформації. Зловмисники мають різні наміри щодо вашої інформації: є викрадення комп'ютерних даних; блокування ; спотворення чи знищення інформації. Відомо, що програмного забезпечення, яке гарантує безпечність та цілісність даних на 100% - не існує. З цього виникає питання, як захиститися від можливого проникнення зловмисників в комп'ютерну систему або мережу?

Перш за все потрібно знати, що в комп'ютерних системах і мережах захист ділиться на два рівня: низький та високий.

Високий рівень захисту – цей рівень охоплює не лише безпеку програм та даних , а і будівлю, кімнату та місце де вони знаходяться. Для забезпечення високого рівня захисту здійснюються такі заходи:

– охорона території або споруди за допомогою спеціального обладнання та персоналу;

– моніторинг приміщень;

– перевірка операційної системи.

Низький рівень захисту – це наявність алгоритму обмеження доступу до даних в комп'ютерних системах або мережах. Мається на увазі, що користувач проходить ідентифікацію перед входом у комп'ютерну систему або мережу(відбувається введення пароля, ключа).

Розповсюдженим методом захисту даних стала саме ідентифікація користувача. Тобто, при вході у систему запрошується ввести пароль, який вже раніше був визначений самим користувачем. Максимальна кількість символів може бути різною, але рекомендовано від 4 до 12. Не рекомендується використовувати один пароль тривалий час, так як він може бути вгаданий сторонньою людиною.

Також можна використовувати метод біометрії як захист програм та даних. Біометрія - метод ідентифікації, заснований на фізіологічній характеристиці особи. Біометрія має деякий ряд переваг над іншими методами захисту:

– не потребує зайвої інформації окрім фізіологічних даних особи;

– фізіологічні дані особи не можуть бути підробленими або викраденими.

Але щоб підвищити надійність ідентифікації особистості людини за допомогою біометрії потрібно використовувати декілька способів ідентифікатора системи - інформаційно-смисловий і біометричний. Тоді і виходить бажаний критерій «вартість / ефективність». Серед біометричних ідентифікаторів найбільш привабливі системи, що використовують не менше двох методів ідентифікації з включенням біометрії за будовою вен пальця і руки. Серед речових ідентифікаторів слід приділити увагу безконтактним ідентифікаторам на базі RFID з обов'язковим захистом інформації від копіювання та несанкціонованого перезапису.

Отже, розглянуті різні методи мають свої переваги, але мають і недоліки. Щодо захисту даних в комп'ютерних системах і мережах, то метод Біометрії є найкращим, так як підробка даних зловмисником майже неможлива і саме цей фактор робить цей метод найпотужнішим серед усіх інших.

Науковий керівник — Конопліцька-Слободенюк О. К., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.02 :004.056.5

І. Д. Попович
студент, Харківський національний університет радіоелектроніки

Дослідження методів глибинного машинного навчання для вирішення задачі побудови системи виявлення вторгнень

Забезпечення інформаційної безпеки є одним з найважливіших завдань, яке розв'язується у ході проектування сучасних систем [1]. В реальних умовах практично неможливо мати систему, яка повністю захищена від зловмисних дій, але вона повинна хоча б своєчасно реагувати, а для цього якнайшвидше визначати загрозу.

Мережева система виявлення вторгнень (англ. Network Intrusion detection system – NIDS) – це програмне забезпечення, призначене для аналізу мережевого трафіку та виявлення зловмисних інцидентів у ньому [2]. NIDS поділяють на системи, які базуються на основі підписів та на основі аномалій. Перші відстежують мережевий трафік на предмет підозрілих зразків у пакетах даних за допомогою бази даних підписів відомих вторгнень у мережу [2]. NIDS на основі аномалії використовує системи у звичайному стані, щоб відстежувати, чи відбувається незвична або підозріла діяльність.

Формально NIDS на основі аномалій виконує функцію класифікації трафіку на шкідливий і звичайний [2]. Зараз завдання класифікації досить ефективно вирішують за допомогою методів машинного навчання. Для розв'язання задачі виявлення аномалій існує багато методів класичного машинного навчання, такі як нейронні мережі, байєсівські мережі, метод опорних векторів тощо. Наразі, активно використовують більш ефективні підходи глибинного навчання, зокрема нейронні мережі.

Отже, було поставлено задачу дослідити методи машинного навчання, зокрема різні типи архітектур нейронних мереж, а саме, натренувати моделі, визначивши їх оптимальні параметри на основі даних для навчання, та порівняти їх ефективність. Найбільш ефективні моделі використати для створення системи виявлення вторгнень.

Для проведення дослідження були обрані архітектури наступних мереж: згорткова нейрона мережа (англ. Convolutional neural network – CNN), рекурентна нейронна мережа (англ. Recurrent neural network – RNN), а саме її різновиди: довга короткочасна пам'ять (англ. Long short-term memory – LSTM) та керуючий рекурентний блок (англ. Gated recurrent unit – GRU) [3].

Особливість методу CNN полягає у тому, що за основу береться математична операція, яка називається згорткою – спеціалізований вид лінійних операцій [3]. CNN зазвичай використовують для вирішення завдань класифікації зображень, але в випадку спеціальної обробки даних перед тренуванням та при використанні особливої оптимізації ця архітектура може бути використана для виявлення аномалій.

Нейроні мережі, які засновані на архітектурі LSTM активно використовуються для аналізу природної мови [3]. Клітина LSTM запам'ятовує значення через довільні інтервали часу, тому такі мережі також добре підходять для класифікації, обробки та виявлення аномалій на основі даних часових рядів, оскільки важливі події можуть виникати через невизначені проміжки. Тобто LSTM може досить ефективно вирішувати завдання визначення зловмисного трафіку у мережі.

Архітектура GRU фактично є більш простою версією LSTM, але її одиниця мережі має на один шар менше [3]. Це дозволяє отримати більш високі результати у випадку, якщо кількість інформації є порівняно невеликою, а у випадку аналізу мережевого трафіку зазвичай доступні дані за період до одного тижня.

Також було вирішено дослідити доцільність використання комбінації підходів LSTM та методу SVM, який був використаний у якості класифікатору.

У якості датасету обрано набір даних, розроблений Канадським університетом з кібербезпеки [4] шляхом емуляції найбільш поширених атак, та збирання даних мережевого трафіку впродовж п'яти днів у стандартному форматі pcap. Для подальшого його використання для тренування моделей, датасет було перетворено до формату XML. З XML файлу виділено параметри мережі та сконвертовано до масиву, а також застосовано операцію one hot encoding [3] для отримання бінарних значень параметру (присутній або ні). Отримані дані було розділено на частини для тренування та для тесту. У ході роботи кожна модель натренована за допомогою методу градієнтного спуску на першій частині даних, тобто були отримані оптимальні важелі параметрів нейроної мережі, а після цього протестовано на другий частині даних. Ефективність моделей визначалася за допомогою наступних критеріїв:

– точність – процент правильно визначених загроз;

– вірні позитивні відповіді – процент правильно визначених аномалій;

– невірні позитивні відповіді – процент неправильно визначених аномалій.

В ході дослідження отримано результати, які наведені у таблиці 1.

Таблиця 1 – Результати дослідження

	Точність (%)	Вірні позитивні відповіді (%)	Невірні позитивні відповіді (%)
CNN	95,4	93,6	3,3
LSTM	96,8	94,9	2,5
GRU	96,4	95,2	3.1
LSTM+SVM	96,1	94,7	2,7

Отримані результати дозволяють зробити висновки, що архітектура GRU та LSTM є ефективнішими за CNN. При цьому LSTM показує дещо більш високу точність, але GRU має менше невірних позитивних відповідей. Комбінації методів LSTM + SVM значно не покращила ефективність мережі.

На базі отриманих результатів для реалізації було обрано модель на архітектурі GRU, за допомогою якої реалізовано демонстраційну систему виявлення вторгнень. Розроблена система забезпечує наступний функціонал: перегляд підозрілих подій у системі, відображення статусу підозрілих на аномалію подій, сортування подій за різними критеріями, будування графіків аномалій у залежності від часу, тощо.

Запропоновану модель можна використати для побудови NIDS або різноманітних аналізаторів мережі. Розроблений прикладний додаток може застосовуватись для моніторінгу мережі хмарних серверів, кластерів або локальних мереж та виявлення кібератак різних типів.

Список використаних джерел

1. *Бобало Ю.Я. Інформаційна безпека / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарєв та ін. – Львів: Львівська політехніка, 2019. – 580 с.*
2. *Newman R. Computer Security, Protecting Digital Resources. – New York: Jones & Bartlett Learning, 2009. – 326 p.*
3. *Raghavendra Chalapathy, Sanjay Chawla. Deep Learning for Anomaly Detection: A Survey. – University of Sydney, 2019. – 48 с.: ил.*
4. *Canadian Institute for Cybersecurity datasets URL: https://www.unb.ca/cic/datasets/ (дата звернення: 29.10.2020).*

Науковий керівник — кандидат технічних наук, доцент Мазурова О. О., доцент кафедри програмної інженері Харківського національного університету радіоелектроніки.

УДК 004.056

Р. А. Рудяк[1], С. А. Смірнов[2]
[1]*магістрант, Центральноукраїнський національний технічний університет*
[2]*доцент, Центральноукраїнський національний технічний університет*

Дослідження системи автоматизованого захисту корпоративної мережі

Вступна частина. Для деяких процесів удалося радикально підвищити точність визначення атак, причому настільки, що досягнута точність перевищила показники людини. Процеси легко автоматизують, коли вони однозначні й повторювані. Наприклад антивіруси – їх треба було тільки встановити, інше вони робили самі: скачували відновлення баз даних, визначали й блокували віруси, іноді запитуючи підтвердження. Визначення вірусів, сигнатури атак і інших простих методів захисту працювали безвідмовно доти, поки атаки не стали персоніфікованими. Інакше кажучи, зловмисники стали враховувати особливості конкретного об'єкта захисту й саму систему захисту. Виявляти віруси й атаки за допомогою вже відомих зразків тепер вдавалося не завжди, що змусило вдатися до набагато менш точного способу – поведінкового аналізу: ні на один відомий вірус це не схоже, але веде воно себе як вірус. Перші системи такого роду викликали протести користувачів: кількість помилкових спрацьовувань у порівнянні зі старими технологіями було неприйнятним, користувачеві доводилося постійно відволікатися від роботи, щоб розбиратися з повідомленнями антивірусу. Поступово всі зійшлися на тому, що заради захисту прийде упокоритися з помилковими спрацьовуваннями, але відрізнити фіктивну тривогу від реальної атаки може не кожний. Так з'явилися професійні оператори систем захисту, які аналізували повідомлення систем безпеки й дозволяли колізії. «Системи захисту» – устояний, але неправильний термін, адже по суті мова йде про системи моніторингу, оскільки така система лише повідомляє оператора про підозрілу активність, а ті або інші міри приймає людина, від кваліфікації якого багато в чому залежить їхня ефективність.

Таким чином, виходячи з вищеперерахованого, дослідження системи кібербезпеки для автоматизованого захисту корпоративної мережі, є актуальною задачею, яка потребує вирішення у даній роботі

Об'єктом дослідження є процес автоматизованого захисту корпоративної мережі.

Предметом дослідження є методи автоматизованого захисту корпоративної мережі.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

–Удосконалено метод автоматизованого захисту корпоративної мережі.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі автоматизованого захисту корпоративної мережі.

Основна частина. Безпека даних – одне з головних завдань, розв'язуваних IT-відділами компаній. Причому мова йде не тільки про запобігання витоку корпоративної інформації, зниженні обсягів паразитного трафіку й відбитті атак на ресурси компанії, але й про оптимізацію роботи системи в цілому. Знайти універсальне рішення в даному питанні практично неможливо: неоднорідність сфер діяльності й структур організацій переводить завдання в категорію потребуючого індивідуального підходу. Однак для грамотних фахівців нерозв'язних проблем не існує. У цій роботі ми поговоримо про

ключові підходи, методи й засоби інформаційної безпеки, а також оцінимо вартість конкретних рішень.

Забезпечення інформаційної безпеки актуально насамперед для корпорацій зі складною, територіально-розподіленою, багаторівневою структурою: великих банків, транснаціональних і державних компаній. Найчастіше корпоративні мережі подібних організацій побудовані з використанням устаткування різних поколінь і від різних виробників, що помітно ускладнює процес керування ІТ-системою.

Крім того, інформаційні структури корпорацій відрізняються різнорідністю, вони складаються з різних баз, наборів розподілених і локальних систем. Це робить ресурси корпоративного рівня особливо уразливими.

У процесі обміну даними між користувачами організації й зовнішнім миром мережі можуть бути уражені шкідливими програмами, які руйнують бази даних і здійснюють передачу відомостей третім особам. Однак сказати, що завдання забезпечення інформаційної безпеки неактуальна для середнього й малого бізнесу, теж було б невірно. Особливо сьогодні, коли бізнес-процеси активно переходять у віртуальний простір: оплата товарів і послуг через Інтернет, електронна пошта, IP-телефонія, хмарні сховища, віртуальні сервера – все це стало типово для сучасних фірм середньої руки, як і атаки хакерів, витік конфіденційних даних, у тому числі фінансових і т.д. Отже, що ж ставиться до головних погроз корпоративної мережі? На думку фахівців, найбільш серйозну небезпеку для ІТ-інфраструктури сьогодні представляють віруси (троянське ПЗ, хробаки), шпигунське й рекламне програмне забезпечення, спам і фішінг-атаки типу «відмова в обслуговуванні», підміна головної сторінки інтернет-ресурсу й соціальний інжиніринг. Причому джерелом погроз можуть бути як зовнішні користувачі, так і співробітники (часто ненавмисно). Реалізація шкідливих алгоритмів може привести як до паралізації системи і її збоїв, так і до втрати, підміні або витоку інформації. Все це чревате величезними імиджевими, часовими й фінансовими втратами для компанії.

Таким чином, головними завданнями будь-якої системи інформаційної безпеки є: забезпечення доступності даних для авторизованих користувачів – можливості оперативного одержання інформаційних послуг; гарантія цілісності інформації – її актуальності й захищеності від несанкціонованої зміни або знищення; забезпечення конфіденційності відомостей.

Для рішення позначених цілей сьогодні застосовуються такі методи захисту інформації, як реєстрація й протоколювання, ідентифікація й автентифікація, керування доступом, створення міжмережевих екранів і криптографія.

Висновки. Таким чином, у даній роботі було проведено дослідження системи автоматизованого захисту корпоративної мережі. Визначено актуальність цієї задачі. Напрямком подальшого розвитку вважаємо розроблення вітчизняного продукту автоматизованого захисту корпоративної мережі, який має більш широкі можливості, на відміну від існуючих аналогів.

Список використаних джерел

1. *Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.*
2. *Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.*
3. *Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.*

УДК 004.056

А. Р. Сароян[1], С. А. Смірнов[2]
[1]*магістант, Центральноукраїнський національний технічний університет*
[2]*доцент, Центральноукраїнський національний технічний університет*

Дослідження системи аналізу додатків рівня L7 у Firewall

Вступна частина. Skype, TOR, Ultrasurf, TCP-over-DNS і ще кілька сотень застосунків і тунелів спокійно проходять крізь statefull inspection firewall і HTTP проксі. Багато засобів захисту відкривають з'єднання, але не перевіряють, що ходить усередині них. Пропоную розібратися, як контрольовано дозволяти з'єднання застосунків у новому поколінні firewall, де правила пишуться по іменах застосунків, що відповідає 7 рівню моделі OSI ISO. Такі міжмережеві екрани мають назву Next Generation Firewall – міжмережевий екран нового покоління або просто NGFW. Адміністраторові міжмережевого екрана потрібно не тільки дозволити з'єднання, а ще гарантувати, що усередині дозволеного з'єднання ходить те, що ви хотіли, включаючи перевірки переданих файлів. Це називається безпечний дозвіл застосунків. Існує кілька важливих відмінностей у роботі із трафіком, які розумієш лише коли переходиш на реальне використання правил, де критерієм є застосунок 7 рівня моделі ISO OSI: IT адміністратор бачить, що NGFW зручніше у візуалізації мережевого трафіку й показує вміст поля даних пакетів по кожному користувачі й сервісу: який застосунок працюють і які файли передає. IT безпека бачить, що NGFW забезпечують безпечний дозвіл застосунків, оскільки більше глибокий аналіз даних у пакеті дозволяє побачити віруси, підключити відправлення невідомих файлів у пісочницю, перевірити тип файлу, ключові слова для DLP, перевірити категорію URL, перевірити що йде усередині SSL і SSH, зрівняти із уже відомими усьому світу індикаторами компрометації, включити DNS фільтр і інші сучасні техніки. Таким чином, виходячи з вищеперерахованого, дослідження системи аналізу додатків рівня L7 у Firewall, є актуальною задачею, яка потребує вирішення у даній роботі

Об'єктом дослідження є процес аналізу додатків рівня L7 у Firewall.

Предметом дослідження є методи аналізу додатків рівня L7 у Firewall.

Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

–Удосконалено метод аналізу додатків рівня L7 у Firewall.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі аналізу додатків рівня L7 у Firewall.

Основна частина. Міжмережевий екран (MME), Firewall, NetworkFirewall – це мережевий пристрій, що ділить мережу на сегменти з різними політиками безпеки й контролюють ці політики. Наприклад, сегмент Інтернет – там можна всі що завгодно. І сегмент вашого ЦОД – там можна працювати тільки виділеному списку співробітників по дозволених застосунках. Усередині одного хоста VMware може бути кілька віртуальних мереж з віртуальними машинами й різними політиками доступу до них.

Політика безпеки firewall містить правила, які пускає в хід програмний код пристрою, аналізуючи кожний фрейм і пакет що прийшов і виходить із firewall. У правилах firewall задаються критерії перевірки (кваліфікатори), по яких приймається рішення пропускати або блокувати трафік. Прикладами кваліфікаторів у правилах є: адреса, порт, застосунок, користувач, зона. Міжмережевий екран послідовно, правило за правилом, зверху внизу за списком переглядає критерії і якщо вхідний трафік

відповідає всім критеріям правила, (логічна операція «И» між критеріями) те застосовується зазначена дія: заблокувати або пропустити. Дія виконується як для першого пакета, так і для всіх наступних пакетів одного TCP/IP з'єднання.

L7firewall – це міжмережевий екран, що пропускає через себе IP трафік мережі й перевіряє й заголовки 4 рівні й сегмент даних кожного IP пакета, тобто розуміє L7 трафік рівня застосунків, аж до того які файли передаються й у якому напрямку. Оскільки аналізується більше даних, те й критеріїв перевірки в правилах L7 firewall більше: ім'я користувача, застосунок, URL категорія, стан софта на комп'ютері користувача. Навантаження на L7 firewall набагато вище, оскільки його процесор повинен постійно аналізувати мегабайтів даних, які передає застосунок, у той час як L4 firewall перевіряє тільки трохи байт заголовка з адресами джерела й одержувача й портами. Розмір буфера для зберігання стану кожного застосунку потрібно набагато більше, оскільки даних на L7 передається більше, ніж просто в заголовку TCP/IP. Через виросліий розмір буфера при використанні аналізу застосунків, кількість одночасно збережених у пам'яті сесій в L7 firewall менше L4 firewall при тім же обсязі пам'яті. Оскільки L7 firewall бачить по контенту що за застосунок йде мережею, то номер порту не несе особливого змісту й правила можна писати за іменем застосунку L7. Крім того сучасні застосунки генерують багато з'єднань і всіх цих з'єднань є частиною одного застосунку. Цей вид firewall дозволяє повернути контроль за сучасними динамічними застосунками, що працюють по будь-якому порту, наприклад, teamviewer, bittorent, tor, про які L4 firewall нічого не знає. Тобто L7 firewall у сучасних реаліях потрібний, якщо в мережі потрібна безпека.

NGFW – це мережевий пристрій, усередині якого реалізований L7 firewall. Оскільки кваліфікатором основним стає ім'я застосунку L7, те в такий спосіб правила пишуться по-іншому. В NGFW працює динамічне зіставлення IP адрес користувачі мережі, тому ім'я користувача теж стає кваліфікатором. NGFW містить у собі функції розшифрування SSL і SSH для розпізнавання застосунків і атак усередині них, IPS, антивірусу, URL фільтрації.

Через те, що NGFW виконує кілька функцій одночасно, іноді вважають NGFW підкласом пристроїв UTM. Відмінність у тім, що в NGFW функції безпеки контенту застосунків (IPS, антивірус, URL фільтрація) прискорені на спеціалізованих апаратних чипах: тобто IPS працює на своєму чипі, антивірус на своєму, розшифровані SSL на своєму й так далі. Поділ функцій по різних процесорах дає можливість запускати їх паралельно й не чекати, коли закінчить працювати попередня функція, як в UTM. Також NGFW містять єдиний програмний інтерфейс керування всіма функціями одночасно.

Висновки. Таким чином, у даній роботі було проведено дослідження системи аналізу додатків рівня L7 у Firewall. Визначено актуальність цієї задачі. Напрямком подальшого розвитку вважаємо розроблення вітчизняного продукту аналізу додатків рівня L7 у Firewall, який має більш широкі можливості, на відміну від існуючих аналогів.

Список використаних джерел

1. *Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.*
2. *Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.*
3. *Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.*

УДК 004.056.5

Д. В. Фесечко
студент, Центральноукраїнський національний технічний університет

Методика вибору оптимального захисту інформації на підприємствах

На сьогоднішній день існує велика кількість підприємств, організацій, компаній, які зберігають велику кількість інформації. Необхідність захисту цієї інформації може бути спричинена комерційною таємницею, банківською таємницею або законом про персональні дані. Щоб виключити неправомірний доступ до інформації застосовують такі засоби, як ідентифікація і аутентифікація. При цьому об'єктом аутентифікації може бути не тільки людина, але і технічний засіб.

Ідентифікація - процедура розпізнавання суб'єкта за його ідентифікатором. У процесі реєстрації суб'єкт надає системі свій ідентифікатор і вона перевіряє його наявність у своїй базі даних. Суб'єкти з відомими системі ідентифікаторами вважаються легальними (законними), інші суб'єкти відносяться до нелегальних.

Авторизація - процедура надання суб'єкту певних прав доступу до ресурсів системи після проходження ним процедури аутентифікації. Для кожного суб'єкта в системі визначається набір прав, які він може використовувати при зверненні до її ресурсів.

Аутентифікація - процедура перевірки прав суб'єкта, яка дозволяє достовірно переконатися в тому, що суб'єкт, який надав ідентифікатор, насправді являється тим суб'єктом, ідентифікатор якого він використовує. Для цього він повинен підтвердити факт володіння певною інформацією, яка може бути доступна тільки йому одному (пароль, ключ).

При використанні простої аутентифікації в якості ідентифікатора використовується пароль. При складній аутентифікації, захист якої набагато надійніший, ідентифікатор створюється з використанням криптографічних алгоритмів.

В даний час використання однофакторної або простої аутентифікації на підприємствах вже недостатньо, так як вона не завжди здатна забезпечити необхідний рівень безпеки. Застосування багатофакторної аутентифікації призначене для забезпечення більш високого рівня безпеки.

Для аутентифікації використовуються як програмні, так і апаратні засоби. Якщо компанія велика, вона може мати кілька інформаційних систем і джерел інформації, які потребують надійного захисту. До апаратних засобів, що використовуються для аутентифікації, відносяться апаратні токени, до програмних засобів - паролі і цифрові сертифікати. Цифрові сертифікати зручно використовувати при великій кількості користувачів, наприклад вони захищають внутрішні сервери та веб-додатки.

Забезпечення безпеки повинно грунтуватися на одночасному застосуванні всього комплексу заходів, передбачених законом або пропонованих фахівцями. Технічні та організаційні заходи необхідно співставляти з можливостями організації та інформаційної системи.

Список використаних джерел

1. *"Основні захисні механізми. Ідентифікація та аутендифікація користувачів. URL:*
2. *Економічна безпека підприємств, організацій та установ. Методи і способи захисту інформації URL: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/rozdil7.html*
3. *Інформаційна безпека. Системи ідентифікації, аутентифікації і авторизації. URL: https://alfa-tex.com/uslugi/guard/upravlenie-dostupom/sistemy-identifikacii-autentifikacii-i-avtorizacii*

Науковий керівник — Конопліцька-Слободенюк О. К., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

УДК 004.3.052

О. Чумак
студент, Центральноукраїнский національний технічний університет

Методи побудови відмовостійких систем

Вступ. На сьогоднішній день не існує системи, яка гарантує 100% відмовостійкість. Іншими словами, не існує системи, яка гарантує 100% ймовірність безвідмовної роботи протягом заданого проміжку часу (100% доступність).

Основна частина. Існує два основних напрямки при побудові відмовостійких систем. Перший спосіб - використання тільки відмовостійких компонентів. Другий спосіб розробка методів, що гарантують побудову відмовостійкої системи з компонентів, які не є відмовостійкими. При реалізації цього напрямку кожен компонент системи може продовжувати своє функціонування, навіть якщо один / кілька підкомпонентів системи, виходять з ладу. Другий спосіб розробка методів, що гарантують побудову відмовостійкої системи з компонентів, які не є відмовостійкими. В таких системах відмовостійкість реалізована за рахунок введення надмірності і розробки спеціального програмного забезпечення, елементних взаємозв'язків і алгоритмів функціонування.

Внесення відмовостійкості в систему або окремо взятий компонент завжди потребує появи деякої надмірності. Надмірність - це наявність в структурі пристрою можливостей понад ті, які могли б забезпечити його нормальне функціонування. В основному використовується чотири види надмірності.

Апаратна надмірність (Hardware Redundancy, більш відома як резервування). Існують методи постійного резервування (синтез надлишкових пристроїв, нечутливих до певної кількості помилок) і методи резервування заміщенням (використання системи контролю, яка може діяти безперервно або періодично, в цьому випадку говорять, про так званому функціональному діагностуванні).

Програмна надмірність (Software Redundancy) використовується для контролю і забезпечення достовірності найбільш важливих рішень з управління та обробки інформації. Вона полягає в зіставленні результатів обробки однакових вихідних даних різними програмами і виключення спотворення результатів, обумовлених різними аномаліями. Виключаючи навіть короткочасний простий, постійне резервування має відносну перевагу в порівнянні з другою групою методів, системи при відмовах.

Інформаційна надмірність (Information Redundancy) найбільш притаманна телекомунікаційним системам, в яких інформація передається багато разів. Інформаційна надмірність полягає в дублюванні накопичених вихідних і проміжних даних.

Тимчасова надмірність (Time Redundancy) полягає у використанні певної частини продуктивності комп'ютера для контролю за виконанням програм та відновлення (рестарту) обчислювального процесу (запас часу для повторного виконання операції (наприклад, з подвійним або потрійним прорахунку на обчислювальній машині).

Досить поширені методи, коли з метою підвищення надійності, система забезпечується схемою внутрішнього контролю (СВК / тестер), призначення якої полягає в ініціалізації «сигналу відмови» при наявності несправностей або зміни функціональності, і як наслідок, невідповідність вихідних сигналів. В цьому випадку, сигнал про помилку використовується для відключення несправного пристрою від об'єкта управління. Також цей сигнал може бути паралельно використаний для активізації команди підключення резервного або дублюючого устрою.

Розглянемо основні методи розробки відмово стійкої системи (fault-tolerant system). Розробка відмовостійкої системи або відмовостійка експлуатація останньої, повинні ґрунтуватися на знанні і розумінні природи тих видів відмов, ймовірність яких, за даних умов експлуатації пристрою, мають максимально велику ймовірність виникнення. За часом впливу на об'єкт відмови підрозділяються на постійні (permanent fault - одноразова дія без можливості подальшого використання системи), що перемежовувалися відмови (intermittent fault - багаторазове повторення ситуації без можності визначення її закономірності) і прохідні відмови (transient fault - одноразовий короткочасний відмова без можливості його повторення при рестарт системи).

Важливо зрозуміти, що відмови можуть виникати раптово (без попереднього погіршення вихідних характеристик), або заздалегідь прогнозуватися поступовою зміною вихідних характеристик. Тому для оцінки відмовостійкості нової системи і її надійності, важливий регулярний аналіз статистичної інформації і як наслідок аналізу, прагнення зменшити вплив певних несприятливих впливів.

При розгляданні відмово стійких систем не можна не сказати про таке поняття як інтенсивність відмов системи захисту від НСД (несанкціонований доступ). Під інтенсивністю відмов системі слід розуміти інтенсивність виявлення в ній каналів НСД к інформації в одиницю часу. При розрахунку надійності приймається, що інтенсивність відмов являється постійною в часі величиною. Якщо допустити, що загрози НСД взаємонезалежні і будь яка *i*-а (*i*= 1,…,*I*) загроза приймає катастрофічний характер, надаючи зловмиснику несанкціонований доступ до інформації, то інтенсивність відмов систем захисту дорівнює сумі інтенсивності загроз НСД до відповідної системи захисту:

$$\lambda = \sum_{i=1}^{I} \lambda_i,$$

де λ - середнє число відмов за одиницю часу.

Тоді імовірність справної роботи системи захисту протягом довільного інтервалу часу *t* визначається наступним чином:

$$p(t) = e^{-\lambda t}.$$

Відповідно, зворотня величина інтенсивності відмов дорівнює середньому проміжку часу між двома відмовами і називається часом напрацювання на відмову:

$$T = 1/\lambda.$$

Інтенсивність відмов системи визначається рядом параметрів, в тому числі , складністю дослідження захисних механізмів в системі, аваліфікацією зловмисника, і тимчасовим інтервалом експлуатації захисної системи. Тимчасовий інтервал експлуатації системи- є важливим аспектом, який впливає на інтенсивність відмов.

Висновок. Відмінними перевагами відмовостійких систем є: їх висока безвідмовність, безперебійність роботи системи при наявності відмов і більш тривалий життєвий цикл експлуатації. Відмовостійкі системи крім переваг мають і ряд специфічних характеристик, а саме: складність дизайну і висока вартість розгортання, підвищення енергоспоживання, ускладнення системи.

Список використаних джерел

1. *Торошанко Я. І. Ключові параметри ефективності безпроводових телекомунікаційних мереж та методи їх ідентифікації / Я. І. Торошанко, В. П. Грушевська, В. С. Шматко, М. С. Височіненко // Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – №4(32). – С.28-33.*
2. *Василевський О. М. Нормування показників надійності технічних засобів [Текст] : навчальний посібник / О. М. Василевський, О. Г. Ігнатенко. – Вінниця : ВНТУ, 2013. – 160 с.*

Науковий керівник — Савеленко О. К., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

Наукове видання

КОМП'ЮТЕРНА ІНЖЕНЕРІЯ І КІБЕРБЕЗПЕКА: ДОСЯГНЕННЯ ТА ІННОВАЦІЇ

Матеріали ІІ Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених

м. Кропивницький, 25-27 листопада 2020 р.

Технічний редактор *О. П. Доренський*

Підписано до друку 27.11.2020. Формат 60х84/8. Папір офсетний.
Надруковано на ризографі. Тираж 97 прим.