Львівський державний університет безпеки життєдіяльності

Національний університет Львівська політехніка

Департамент кіберполіції Національна поліція України

Львівська міська рада

LVIV IT CLUSTER

softserve

UnderDefense

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції
ІБІТ 2022

30 листопада 2022 року

Міністерство освіти і науки України
Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Національний університет "Львівська політехніка"

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції
ІБІТ 2022

30 листопада 2022 року

Львів
Растр-7
2022

УДК 351.746:007:004
І 74

Інформаційна безпека та інформаційні технології: збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. – Львів: Растр-7, 2022. – 380 с.

ISBN 978-617-8134-79-2

У збірнику опубліковано матеріали IV Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології". На основі теоретичних та експериментальних досліджень представлено інноваційні підходи у сфері кібербезпеки та інформаційних технологій. Обговорено та запропоновано сучасні шляхи щодо захисту інформації як на особистому, так і на державному рівнях.

УДК 351.746:007:004

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

ISBN 978-617-8134-79-2

Zbigniew KOKOSIŃSKI – dr hab. Inż., prof. PK kierownik Katedry Politechnika Krakowska im. Tadeusza Kościuszki;

Volodymyr SAMOTYY – prof. dr hab. inż., professor, Katedra Automatyki i Informatyki Politechnika Krakowska im. Tadeusza Kościuszki;

Sergii TELENYK – prof. dr hab. inż., professor, Department of automatic control and computer engineering Cracow University of Technology;

Володимир РОМАКА – д.т.н., професор, професор кафедри захисту інформації Національного університету "Львівська політехніка";

Іван ОПІРСЬКИЙ – д.т.н., професор, професор кафедри захисту інформації Національного університету "Львівська політехніка";

Любомир СІКОРА – д.т.н., професор, професор кафедри автоматизованих систем управління Національного університету "Львівська політехніка";

Наталя ЛИСА – д.т.н., доцент, доцент кафедри кафедри автоматизованих систем управління Національного університету "Львівська політехніка";

Тетяна ГОВОРУЩЕНКО – д.т.н., професор, завідувач кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету;

Ольга МЕНЬШИКОВА – к.ф.-м.н., доцент, заступник начальника навчально-наукового інституту цивільного захисту Львівського державного університету безпеки життєдіяльності з навчально-наукової роботи;

Андрій Івануса – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валентина ЯЩУК – к.е.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Орест ПОЛОТАЙ – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валерія БАЛАЦЬКА – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Ігор МАЛЕЦЬ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Назарій БУРАК – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Ольга СМОТР – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Юрій БОРЗОВ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Роман ГОЛОВАТИЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Олександр ХЛЕВНОЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

Секція 1

КІБЕРБЕЗПЕКА

Напрям 1

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

UDC 004.02

HYBRID ATTACK RISK ANALYSIS

Bohdan Sakovych[1], Maryna Zharikova[2]

[1]Kherson National Technical University, Kherson, Ukraine
[2]Bundeswehr University Munich, Neubiberg, Germany

Abstract. *The paper reflects on various hybrid threats and attacks spreading all over the earth. The proposed method is able to assist the representatives with the forbearance of mentioned dangers and combating such kinds of attacks.*

Keywords: *hybrid attack, hybrid threat, critical infrastructure, machine learning, random forest, decision trees, Bayesian network.*

Анотація. *Ця стаття висвітлює ступінь гібридних загроз у сучасному світі та пропонує методи їхнього запобігання та попередження у майбутньому.*

Ключові слова: *гібридна атака, критична інфраструктура, машинне навчання, модель випадкових лісів, дерева ухвалення рішень, мережі Байєса.*

Introduction. The contemporary world is inundated with numerous risks and dangers, especially in wartime. This unprecedented Russian invasion of Ukraine has disclosed a plethora of cynical Russian attacks unseen for ages, such as civil infrastructure imperilment, encroachment on residential areas and shopping malls, gas stations and critical infrastructure (CI) objects in particular. The threats can be simultaneous and of different kinds, e.g., cyber threats and air raids. Such threats are known as hybrid attacks and are considered to be quite tricky to deal with. For this reason, it is rather vital to foresee and preclude upcoming attacks.

Literature review. As stated in [1, 2] the hybrid threats represent hostile, subversive activities, and diplomatic, military, economic, and technological methods used in a designed manner either by state or non-state doers to achieve specific goals, while still remaining below the threshold of officially proclaimed war.

Generally, such threats are concentrated on undermining the defence and integrity of a country. Therefore, the EU is devising stated risk assessment methods to properly inform aimed forces about emerging risks of threats. The aim would be to estimate the extent of hybrid threats and forward them to early warning systems and risk assessment mechanisms. Cyberattacks-wise [3], they are extremely wired these days. They can evoke quite lugubrious ramifications,

such as electricity blackouts, disruption of a plant ecosystem, and even atomic explosion prompted by block overheating. Nevertheless, the Council of the European Union informs that terrorism imperils government stability and endangers national security systems around the globe [4]. Thus, there is a strong necessity to timely react to such kinds of imperilments and preclude dire outcomes despite the fact that a lot of regulations and significant actions have already been made to increase resistance to hybrid threats.

Model description. Fortunately, artificial intelligence and machine learning have a major role in the world problem solving, from information technology up to biology and medicine issues. The disparate models and algorithms can solve nearly any issue and generate the optimal solution. Several of them are decision trees, Bayesian networks and Random Forest. The decision tree is a supervised learning method that is utilized for both classification and regression goals. They are aimed at constructing a model that predicts the certain value of the set by learning defined rules derived from data usage. Trees can be viewed as normal tree-like structure, but upside down as its root is located on the top of the tree. The tree increases in depth as more rules are defined which makes the model more accurate. Subsequently, random forests train several decision tree classifiers on different subsamples of a dataset and utilize averaging scores to improve prediction accuracy and preclude overfitting. Ultimately, Bayesian networks portray the probabilistic graphical models of an uncertain area where each node matches an arbitrary variable and each edge represents the tentative liability for the corresponding variables [7−10].

Contribution of this work. The main contribution of this work is to deliver a novel method of analysing the risk of hybrid attacks in comparison with related ones. The proposed risk analysis covers all three main phases of the crisis management cycle such as pre-crisis, response, and post-crisis. As a result, the risk is divided into potential, active, and post-crisis risks, which allows decision-makers to make more informed decisions at every phase of the crisis management cycle.

Risk analysis within the crisis management cycle. We propose a crisis management cycle that is adapted from [11] and divided into three phases such as pre-crisis, response, and post-crisis. The main characteristics of risk in the context of this paper are that it is dynamic and spatially distributed. As for the first one, we presume that for any spatial location, risk will change depending on affecting of hybrid attacks (HA). For the latter, we suppose that risk can be assessed for each area of the territory or for each vulnerable object, which provides its spatial reference.

The subject of risk analysis in the proposed framework is the assessment of the chance of losses as a result of the involvement of the targeted object in the HA. Thus, risk originates from the interaction of hybrid attacks and targeted objects, such as infrastructure, communities, governments etc., affected by this attack and comprises the following dimensions: the likelihood of HA occurrence; characteristics of the targeted object such as object vulnerability,

potential damage, and speed of recovery; the availability of the object for the actors who created the attack. Subsequently, risk assessment can be represented as a combination of the following components: assessment of the likelihood of an attack occurrence *L*; threat potential assessment *T*; availability of targeted object for actor *A*; the vulnerability of targeted object *V*.

Conclusions. The comprehensive approach to support risk-informed decisions at all phases of the crisis management cycle is proffered by bonding relevant tools to prevent, counteract, and recover from the impact of hybrid attacks in a coordinated manner. The division of risk into potential, active, and post-crisis risk allows making decisions corresponding to each of the three phases of the crisis management cycle. Representing risk as a spatially distributed process allows us to highlight the most vulnerable areas that require priority attention.

References

1. Joint Framework on countering hybrid threats a European Union response, European Commission, Document 52016JC0018, 2018. URL: https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52016JC0018

2. V. Sherstjuk, M. Zharikova, S. Pickl, M. Villota, I. Dorovskaja, and D. Chornyi, "Modeling Hybrid Attacks and Operations to Assess the Threats in Early Warning Systems", *in 12th International Conference on Advanced Computer Information Technologies (ACIT)*, pp. 39-44, September 2022.

3. J. Liu, Y. Wang, L. Zha, X. Xie, and E. Tian, "An event-triggered approach to security control for networked systems using a hybrid attack model", *International Journal of Robust and Nonlinear Control*, vol. 31, no.12, 5796-5812, 2021.

4. Strategic Compass. Council of the European Union, 2022. URL: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

5. G. Giannopoulos, H. Smith and M. Theocharidou, "The Landscape of Hybrid Threats: A conceptual model," *Ispra, European Commission*, PUBSY No. 117280, 2021.

6. S. Haji, Q. Tan and R. Soler Costa, "A Hybrid Model for Information Security Risk Assessment," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 1.1, pp. 100–106, 2019.

7. F. Aguessy, O. Bettan, G. Blanc, V. Conan and H. Debar, "Hybrid Risk Assessment Model based on Bayesian Networks", *In Proc. of the 11th International Workshop on Security IWSEC 2016*, Tokyo, Japan, pp. 21–40, 2016.

8. K. Ramya, Y. Teekaraman, and K. R. Kumar, "Fuzzy-based energy management system with decision tree algorithm for power security system", *International Journal of Computational Intelligence Systems*, vol. 12, no.2, 1173-1178, 2019.

9. B. Charbuty, A. Abdulazeez, "Classification based on decision tree algorithm for machine learning" Journal of Applied Science and Technology Trends, vol. 2, no.01, pp. 20-28, 2021.

10. A. Chaudhary, S. Kolhe, and R. Kamal, "An improved random forest classifier for multi-class classification", *Information Processing in Agriculture*, vol. 3, no.4, pp. 215-222, 2016.

11. F. Aligne, J. Mattioli, "The Role of Context for Crisis Management Cycle", In F. Burstein et al. (eds.), Supporting Real Time Decision-Making, *Annals of Information Systems 13*, Springer, New York, pp. 113-132, 2010. doi: 10.1007/978-1-4419-7406-8_6

UDC 004.491.22

COMPUTER VIRUS: WHAT ARE COMPUTER VIRUSES?

Oleksii Polishevskyi[1], Lyudmila Pet'ko[2]

[1]Student at the Department of Software engineering Faculty of Mathematics, Informatics and Physics Dragomanov National Pedagogical University, sity Kyiv, Ukraine

[2]PhD professor, docent at the Department of Foreign languages Dragomanov National Pedagogical University, sity Kyiv, Ukraine

Abstract. *Described the origins of computer viruses and presented their types according to the degree of influence. Given the notion of computer viruses. Analyzed the names of computer viruses, what can be clearly divided into several groups: names of computer viruses by place of origin, by date of activation, by action, by number of bytes, by characteristic text, visual effect, by author, etc.*

Keywords: *computer viruses, Worms, Stoned virus, Marijuana virus, Israeli virus, Dinamo virus, Pakistani virus, Lehigh virus.*

Анотація. *Описано походження комп'ютерних вірусів та наведено їх види за ступенем впливу. Розкрито поняття* "*комп'ютерний вірус*"*. Проаналізувано назви комп'ютерних вірусів, які можна чітко розділити на кілька груп: назви комп'ютерних вірусів за місцем походження, за датою активації, за дією, за кількістю байтів, за характерним текстом, візуальним ефектом, за автором тощо.*

Ключові слова: *комп'ютерні віруси, вірус Worms, завантажувальний вірус Stoned, вірус Marijuana, Ізраїльський вірус, вірус Dinamo, Пакистанський вірус, вірус Lehigh.*

The user of a modern personal computer has free access to all resources of the machine. This opened up the possibility of a danger called a computer virus. I set myself the following goal: to determine what computer viruses are, how to fight them, which programs work better and more effectively, how to protect a device from viruses.

Computer viruses cause damage in billions of dollars each year, causing system critical errors, shutting down large sites and web applications, destroying or modifying files, and increasing response time.

Viruses pose a threat even to users protected by antivirus software, because they can bypass the system of blocking and protecting the program itself. Viruses are also used by hackers to infiltrate the security systems of some web systems to obtain or destroy certain information.

Viruses act only by software. They usually attach to the file or penetrate inside the file. In this case, the file is said to be infected with a virus. The virus enters the computer only together with the infected file. To activate the virus, you need to download the infected file, and only then the virus begins to act

independently. Some viruses become resident (permanently in your computer's RAM) when you run an infected file and can infect other downloaded files and programs. Other types of viruses can cause serious damage immediately after activation, such as formatting the hard disk.

Computer virus – a type of malicious software that can be embedded in the code of other programs, areas of system memory, boot sectors, and distribute their copies through various communication channels (Fig. 1, 2, see the video [13]).

Depending on the location the viruses can be divided into network, file, boot and file- boot. Network viruses are spread on various computer networks. File viruses are implemented mainly in executable modules, i.e. in files with COM or EXE extensions. Boot viruses are introduced into the boot sector of the disk (Boot sector) or into the sector that contains the boot program of the system disk (Master Boot Record). File boot viruses affect both files and boot sectors of disks [6, 11].

According to the degree of influence the viruses can be divided into the following types:

1. Safe, do not disturb the computer's operation, but reduce the amount of free RAM and memory on disks, the actions of such viruses are manifested in any graphic or sound effects.

2. Dangerous viruses that can cause various computer malfunctions.

3. Very dangerous, the impact of which can lead to the loss of programs, data destruction, erasure of information in the system areas of the disk [2].

In more than 80% of computer crimes investigated by the FBI, hackers enter the attacked system via the global Internet. This process can be automated by a virus called a network worm.

Worms are viruses that spread on global networks, infecting entire systems, not individual programs. This is the most dangerous type of virus, as the objects of attack in this case are the information systems of the state scale. With the advent of the global Internet, this type of security breach poses the greatest threat, as it can affect any of the 40 million computers connected to this network at any time (Fig. 3, 4, see the video [3]).

Fig. 1. Computer Virus

Fig. 2. Computer Virus

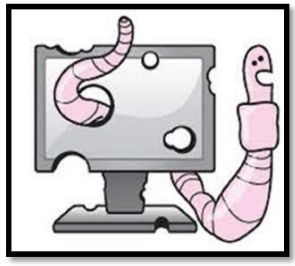


Fig. 3. Virus Worm

Names of computer viruses (Fig. 5). Conditionally, they can be classified as follows according to the following common features:

1) Place of residence:

1. Bootable.
2. File.
3. Boot-file.
4. Network.

2) Level of effects:

1. Relatively safe.
2. Dangerous.
3. Very dangerous.

3) Algorithm features.

1. Invisible viruses
2. Retroviruses
3. Worm-viruses

*4. Trojans Method of infec*tion.

1. Residents
2. Non-residents [10].

Fig. 4. Virus Worm

Mostly the names of computer viruses in modern Ukrainian are borrowed from English, as they have English names, and in Ukrainian they exist as literally translated words or phrases.

Specialists and ordinary PC users make a literal translation of such names into Ukrainian, very rarely giving malware adapted Ukrainian names. Exceptions are viruses created by Ukrainian-speaking or Russian-speaking users, which retain in their names the concepts familiar to such users.

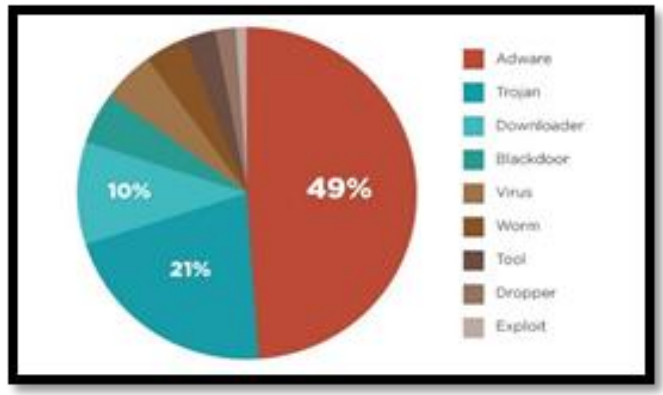


Fig. 5. Rating of the most common computer viruses

Analyzing the names of computer viruses, they can be clearly divided into several groups: names of computer viruses by place of origin, by date of activation, by action, by number of bytes, by characteristic text, visual effect, by author, etc.

Names of computer viruses by date of activation. A separate group of virus names consists of programs that are named after the date when they are activated. For example, the name of the virus ***Black Friday*** is motivated by the fact that if the time of work with infected software falls on Friday the 13th, then infected files are destroyed. Another name for this virus is ***Friday the Thirteenth*** [11], Fig. 6.

The ***Stoned virus*** is so called because when you boot the system, the text '*Your PC is now Stoned'* is simply displayed, after which the work continues (Fig. 7, see the video [1]).

Fig. 6. Friday. The Thirteenth logo

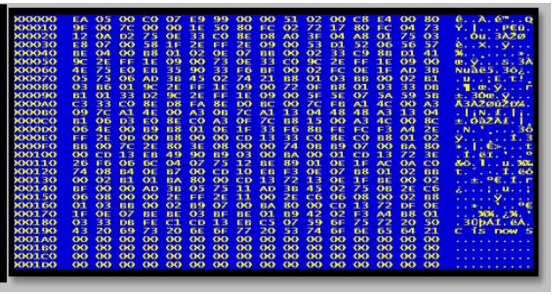


Fig. 7. Stoned virus

The name of the ***Marijuana virus*** is motivated by the phrase *Legalize Marijuana!* which pops up when booting the infected system [11] (Fig. 8).

Fig. 8. Marijuana virus

Fig. 9. Dinamo virus

The Israeli virus (also known as Jerusalem) was first detected at the University of Jerusalem (Israel) in 1987. It is well known in the history of

computer virology for the fact that at one time its spread for the first time became a pandemic among computer systems [10, 5], Fig. 9.

The Jerusalem virus is one of the oldest computer viruses. It infected files in the MS-DOS operating systems that were standard at the time. After DOS operating systems were succeeded by newer types of operating systems, the Jerusalem virus became largely obsolete. The virus also infected executable programs repeatedly until they became too large to run on a computer. Other variants of the Jerusalem virus included additional marginal effects, such as cryptic slogans that would populate the command line interface. Some versions of the virus would apparently restrict the operation of programs during certain days of the week, such as Saturday and Sunday [12].

Dinamo virus displays the phrase: Dinamo (Kiev) – champion !!! – hence the name. Bye! virus name also motivated by the text that follows when booting the system (Fig. 10). The most well-known of these viruses is the Viennese virus. It is one of the first primitive viruses to be discovered in Vienna. When downloaded to computer memory, this virus infects all com programs.

The Pakistani virus (Fig. 11), developed by brothers Amjat and Basit Alvi in 1986, was discovered in the summer of 1987. The malware was supposed to punish local pirates who steal software from their company. The program listed the names, addresses and telephone numbers of the brothers, and this is the first stealth virus (virus-invisible) – when trying to read the infected sector, it substituted its uninfected original [6, 11].

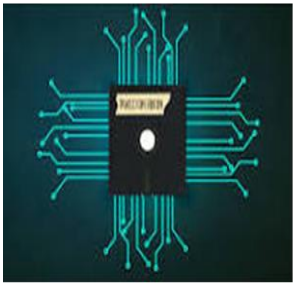


Fig. 10. The Pakistani virus

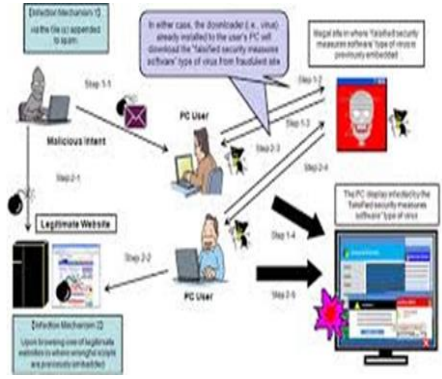


Fig. 11. Types of viruses

The Lehigh virus. Its name is associated with the name Lehigh University (USA), and it was launched in November 1987. Before Thanksgiving 1987, a microcomputcr virus infected several hundred floppy disks at Lehigh University in Bethlehem, PA. The virus was a particularly destructive one; it copied itself

from disk to disk at least four times and then destroyed the contents of the original disk. Each of the copies that were made then went on to do the same thing. This, and the fact that Lehigh University has hundreds of Zenith microcomputers spread all around its campus, on which students shared programs in the form of floppy diskette libraries,proved to bc a rather volatile combination, particularly with Thanksgiving break rapidly approaching. At the time of the viral infection, Lehigh operated approximately 10 microcomputer labs, each one containing an average of between 10 and 15 PCs [4, p. 107].

Within a few days, the virus destroyed the contents of hundreds of floppy disks from the library of the university's computer center and students' personal floppy disks. About four thousand computers were infected during the epidemic [10].

References

1. 500th Video: Virus. Boot Stoned. URL: https://**youtu.be**/kfk4g0iPv74.

2. Cracking: Reversing and Malware Analysis Training Articles. 2012. 60 p. URL: http://index-of.es/Cracking/Malware%20Analysis%20Training_2011_12_Articles.pdf.

3. Malware: Difference Between Computer Viruses, Worms and Trojans. URL: https://youtu.be/n8mbzU0X2nQ.

4. Kenneth R. van Wyk. The Lehigh virus. *Computers & Security*. Vol. 8. Issue 2, April 1989, pp. 107–110. doi: https://doi.org/10.1016/0167-4048(89)90064-3

5. Malwarebytes. URL: https://www.malwarebytes.com/computer-virus.

6. Norton. URL: https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html.

7. Pet'ko Lyudmila. Developing students' creativity in conditions of university // Research: tendencies and prospects: Collection of scientific articles. – Editorial Arane, S.A. de C.V., Mexico City, Mexico, 2017. P. 272−276.

8. Pet'ko L. Multicultural upbringing of students and the formation of professionally oriented foreign language teaching environment // Perspectives of research and development: Collection of scientific articles. – SAUL Publishing Ltd, Dublin, Ireland, 2017. P. 164−170.

9. Pet'ko L. V. Teaching of students' professionally oriented foreign language writing in the formation of professionally oriented foreign language learning environment // Economics, management, law: innovation strategy: Collection of scientific articles. Henan Science and Technology Press, Zhengzhou, China, 2016. P. 356−359.

10. WEBROOT. URL: https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-computer-viruses#:~:text=A%20computer% 20virus%20is% 20a,kind%20that%20makes%20you%20sick.

11. What Are The Different Types Of Computer Viruses? Uniserve. URL: https://uniserveit.com/blog/what-are-the-different-types-of-computer-viruses.

12. What Does Jerusalem Virus Mean? Technopedia Dictionary. URL: https://www.techopedia.com/definition/27875/jerusalem-virus

13. What is a Computer Virus | Tech. URL: https://youtu.be/Ip-u5NZJiwY.

14. What is computer virus? What are various types of viruses? URL: https://www.wired.com/2009/11/1110fred-cohen-first-computer-virus/.

УДК 004.9:378

ІНФОРМАЦІЙНА БЕЗПЕКА

Ілля Гавриленко, Софія Корякіна

Харківський національний університет радіоелектроніки, м. Харків, Україна

Анотація. *Зі стрімким впровадженням новітніх інформаційних технологій у всі сфери діяльності збільшується і кількість цінної інформації, від безпеки якої залежать найважливіші речі. Інформаційна безпека в даний час є актуальною галуззю, оскільки є невід'ємною частиною успіху управління бізнесом, запорукою раціонального вдосконалення всіх взаємопов'язаних процесів. Метою цієї статті є дослідження важливості інформаційної безпеки.*

Ключові слова*: інформаційна безпека, зберігання інформації, інформаційні технології, безпека, Інтернет.*

Abstract. *With the rapid implementation of the latest information technologies in all spheres of activity, the amount of valuable information, the security of which depends on the most important things, is also increasing. Information security is currently a relevant industry, as it is an integral part of the success of business management, a key to the rational improvement of all interrelated processes. The purpose of this article is to explore the importance of information security.*

Keywords: *information security, information storage, information technologies, security, Internet.*

У сучасному бізнес-середовищі, де технології та комунікації розвиваються запаморочливими темпами, захист інформації стає ще важливішим. У захисті інформації виявлення ризиків безпеці та загроз інформаційним активам і контроль відкритих точок у системі потребують серйозних зусиль. Встановлення інформаційної безпеки та забезпечення безперервності контролю залежить від належного встановлення відповідних принципів безпеки та правильного визначення процесів управління.

На разі, наша держава володіє багатими інформаційними ресурсами, які, безумовно, потребують якісного управління та захисту, щоб максимально ефективно використовувати їх для задоволення потреб країни та суспільства. Існує три види інформаційної безпеки, які вказані на рис. 1.

Рисунок 1 – Види інформаційної безпеки

З цієї точки зору підготовка експертів в організаціях з інформаційної безпеки є невід'ємною та важливою частиною національної інформаційної безпеки.

Фахівці з управління такої безпеки здатні вирішувати завдання теоретичного та практичного характеру, що безпосередньо пов'язані з усіма аспектами захисту інформації. Підготовка таких професіоналів спирається на оволодіння сучасними технологіями, фундаментальними та прикладними науковими дисциплінами, що дозволить майбутнім роботодавцям досконало знати конструкцію та принципи функціонування сучасних комп'ютерних систем та мереж, організовувати електронний документообіг, проєктувати системи захисту інформації та системи управління інформаційною безпекою тощо.

Взагалі, система управління інформаційною безпекою (Information Security Management System) – це частина загальної системи управління, що базується на аналізі ризиків, реалізації, контролю, супроводу та вдосконалення заходів в області інформаційної безпеки. Систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

Основними цілями інформаційної безпеки є:

− конфіденційність інформації, тобто необхідність обмеження доступу до інформації певного кола осіб;

− неможливість несанкціонованого доступу до інформації, тобто знання конфіденційної інформації третіх осіб;

− цілісність інформації та пов'язаних з нею процесів (створення, введення, обробки та виведення);

− доступність інформації, тобто можливість забезпечити людям своєчасний і безперешкодний доступ до інформації, що їх цікавить;

− мінімізація ризиків інформаційної безпеки шляхом впровадження компенсаційних заходів;

− облік усіх процесів, пов'язаних з ризиком.

Випускники з кваліфікацією спеціаліста з організації інформаційної безпеки можуть обіймати керівні посади в Державній службі спеціального зв'язку та захисту інформації, Службі безпеки України, а також в органах захисту корпоративної та банківської інформації, а також такі посади: фахівець з питань організації захисту інформації з обмеженим доступом, експерт з системи конфіденційності, експерт з організації захисту інформації та ін.

Адже, з розвитком технологій, штучного інтелекту та інформаційних систем зростають і їхні "темні сторони" – кібератаки та "віруси". Як і біологічні віруси, комп'ютерні "віруси" також мутують і розвиваються.

З 1987 року вони проникли в систему і впливали на дані в ній: вони "з'їдали" дані, шифрували їх, підробляли, маніпулювали ними. Наприклад, вірус, який копіює ваші дані до кінця місця на диску "С", або вірус, який перевантажує процесор на 100%.

Наступний великий стрибок у мутаціях стався у 2012 році: поява вірусу "ivchetoo" або "icon", який фізично спалював жорсткі диски. CNN визнала вірус "найнебезпечнішим".

Чергова мутація та розвиток кібератак сталася нещодавно – WannaCry або Petya. Вірус прославився не тим, що шифрував дані та вимагав біткоїни, а тим, що в 2017 році закрив третину банківської системи країни. Також і віакомпанії, метро, медіа-холдинги, галузеві концерни та великі корпорації зазнали це. Катастрофи такого масштабу можна було б уникнути, якби компанії та їхні співробітники дотримувалися основних правил кібергігієни та кібербезпеки. Проте "незнання" не звільняє від відповідальності.

Необхідний рівень інформаційної безпеки забезпечується комплексом політичних, економічних та організаційних заходів, спрямованих на запобігання, виявлення та усунення ситуацій, факторів і дій, які можуть завдати шкоди або зашкодити реалізації інформаційних прав, потреб та інтересів держави та її громадян. Тому, інформаційна безпека нації – це дуже важлива ступінь захищеності інформаційного середовища, який забезпечує умови для функціонування незалежно від можливих і реальних внутрішніх і зовнішніх загроз.

Інформаційні джерела

1. Про професію "Управління інформаційною безпекою" URL: http://bit.nau.edu.ua/pro-ub (дата звертання 13.11.2022).

2. Система управління інформаційною безпекою підприємства URL: https://stud.com.ua/43080/ekonomika/sistema_upravlinnya_informatsiynoyu_bezpekoyu_ pidpriyemstva (дата звернення 13.11.2022).

3. Інформаційна безпека і кібербезпека – в чому різниця? URL: https://web.archive.org/web/20191017165559/https://indevlab.com/uk/blog-ua/informatsijna-bezpeka-i-kiberbezpeka-v-chomu-riznitsya/ (дата звернення 13.11.2022).

УДК 004.56.53:656.7+614.88

ДО ПИТАННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПРИ ОРГАНІЗАЦІЇ АЕРОМЕДИЧНОЇ ЕВАКУАЦІЇ

Анатолій Гурник, Дмитро Ядченко

Інститут державного управління та наукових досліджень з цивільного захисту, м. Київ, Україна

Анотація. *В роботі запропоновано провести аналіз інформаційної безпеки й комплексне вивчення стану гарантій забезпечення захисту інформації при організації аеромедичної евакуації за наслідками застосування медичних повітряних суден в районі бойового застосування на етапах медичної евакуації поранених, чи наданні допомоги громадянам в зоні надзвичайної ситуації (НС) під час ліквідації наслідків НС.*

Ключові слова: *інформаційна безпека, аеромедична евакуація, воєнні дії, надзвичайна ситуація.*

Abstract. *In the article, it is proposed to conduct an analysis of information security and a comprehensive study of the information protection guarantees state in the organization aeromedical evacuation following the consequences of the use of medical aircraft in the area combat use at the stages of medical evacuation of the wounded or assistance to citizens in the zone of an emergency situation (ES) during the liquidation of the consequences of an emergency.*

Keywords: *information security, aeromedical evacuation, military action, emergency situation.*

Після запущення в роботу проєкту системи аеромедичної евакуації [1] гідно проявляють себе протягом 8 років війни нашої Держави підрозділи Спеціального авіаційного загону (САЗ) Державної служби України з надзвичайних ситуацій при залученні до ліквідації наслідків ведення військових дій у населених пунктах та на територіях, що зазнали впливу засобів ураження [2, ст. 8, п.4].

САЗ виконують польотні завдання для якомога швидкого прибуття медичних бригад авіаційним транспортом до місця надзвичайної ситуації (НС) або ведення бойових дій або обстрілу тощо, з подальшим наданням вчасної медичної допомоги на місці події чи борту залученого повітряного судна (ПС) під час транспортування поранених або хворих (постраждалих) у заклади охорони здоров'я.

У цих умовах діяльність фахівців медичних бригад та підсистеми медичного захисту в Єдиній державній системі цивільного захисту (ЄДСЦЗ), враховуючи досвід зарубіжних країн, неможливо уявити ще й без відповідного оснащення їх підрозділів інноваційними засобами – медичними безпілотними літальними апаратами (БпЛА).

Враховуючи вище викладене, все це в терміновому порядку вимагає суттєвого, більш уважного ставлення до проблем, пов'язаних з інформаційною безпекою, перш за все що стосується захисту від несанкціонованого доступу при застосуванні медичних пілотованих і безпілотних літальних апаратів у зонах бойового застосування на етапах медичної евакуації поранених, чи наданні допомоги громадянам в зоні НС під час ліквідації наслідків НС, і їх безпечної евакуації за межі цих зон.

В умовах ведення війни є необхідність надавати особливого значення вдосконаленню й впровадженню інноваційних інформаційних безпекових технологій і надбань світового досвіду для розвитку системи інформаційної безпеки [3] на всіх етапах заходів організації аеромедичної евакуації за для прихованого виконання польотних завдань.

Якісне, своєчасне і доступне здійснення аеромедичної евакуації в повсякденних умовах війни та в процесі ліквідації медико-соціальних наслідків НС ґрунтується на підході, що враховує ризики умов і управління, пов'язані з використанням інформаційних безпекових систем з метою недопущення порушення конфіденційності, цілісності, автентичності чи доступності інформаційних ресурсів [4] при наданні екстреної медичної допомоги.

В нинішніх умовах неможливо обійтись без удосконалення системи управління інформаційною безпекою, яка вважається успішною інновацією як для забезпечення аеромедичної евакуації, так і для надання екстреної медичної допомоги в цілому.

З метою розробки інноваційних систем управління інформаційною безпекою при організації керування медичними ПС до заданого місця під час виконання польотів і точного й безпечного проходження по заданому маршруту в ручному чи в запрограмованому режимі, за цим напрямком у розвинених країнах здійснюються постійні системні дослідження [5, 6].

Завдяки системі інформаційної безпеки є можливість мати інформацію про ризики, які допомогають приймати фахівцям оптимальне рішення, яке максимально ефективно посприяє визначенню подальших дій з метою

порятунку поранених або потерпілих в складних умовах воєнного стану чи в умовах невизначеності при ліквідації НС відповідно.

Здатність медичних ПС отримувати в масштабі реального часу інформацію про ризики робить їх життєздатними для організації і проведення аеромедичної евакуації на етапах медичної розвідки, надання допомоги пораненим та постраждалим в НС і при пошуку та рятуванні поранених і постраждалих.

Отже, система управління інформаційною безпекою в умовах війни та НС надає можливість під дією зовнішніх дестабілізуючих факторів більш надійно забезпечувати застосування пілотованих і безпілотних літальних апаратів у рамках виконання завдань в інтересах медичного забезпечення в умовах війни та ліквідації її наслідків.

Інформаційні джерела

1. Про затвердження Порядку спільних дій сил цивільного захисту та закладів охорони здоров’я під час здійснення аеромедичної евакуації повітряними суднами Державної служби України з надзвичайних ситуацій : спільний наказ Міністерства внутрішніх справ та Міністерства охорони здоров’я України від 16 серпня 2018 р. № 677/1503 // База даних “Законодавство України” / ВР України. URL : https://zakon.rada.gov.ua/laws/show/z1232-18#Text (дата звернення 15.10.2022).

2. Кодекс цивільного захисту України: Закон України від 2.10.2012№ 5403-VI // База даних “Законодавство України” / ВР України. URL : https://zakon.rada.gov.ua/laws/show/5403-17#Text (дата звернення: 16.10.2022).

3. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19.05.2019 № 518 // База даних “Законодавство України” / ВР України. URL : https://zakon.rada.gov.ua/laws/show/518-2019-%D0% BF#Text (дата звернення: 09.11.2022).

4. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах : постанова Кабінету Міністрів України від 29.03.2006 № 373 // База даних “Законодавство України” / ВР України. URL : https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text (дата звернення: 10.11.2022).

5. Безштанько В. Цикл впровадження системи управління інформаційною безпекою. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні* : наук. журн. 2006. №2(13). С. 123–126.

6. Солодка О.М. Пріоритети удосконалення інформаційної безпеки України. *Інформація і право* : наук. журн. 2015. №3(15). С. 36–42.

УДК 355.244.1(043)

НЕГАТИВНИЙ ВПЛИВ ІНФОРМАЦІЙНОЇ ПРОПАГАНДИ ТА ЗАХИСТ ВІД НЕЇ ПІД ЧАС ВІЙНИ

Діана Іванова, Анна Клєба

Комунальний заклад "Харківська гуманітарно-педагогічна академія" Харківської обласної ради, м. Харків, Україна

Анотація. *У роботі розглянуто проблеми суспільства в умовах інформаційної війни. Висвітлені основні загрози та способи маніпулювання, дезінформування суспільства. Виділенні основні цілі, методи і засоби війни інформацією. Наведені фактори та недоліки інформаційного простору держави, які впливають на інформаційну пропаганду. Розглянуто основні аспекти інформаційних воєн, описано пріоритетні напрями та важливі кроки органів влади в галузі державної інформаційної політики.*

Ключові слова: *інформаційна безпека держави, національний інформаційний простір; мета, методи і засоби інформаційної війни; інформаційні загрози; інформаційно-психологічний вплив; інформаційні ресурси.*

Abstract. *The article examines the problems of society in the conditions of information war. The main threats and methods of manipulation and disinformation of society are highlighted. The main goals, methods and means of information warfare are highlighted. Factors and shortcomings of the information space of the state that affect information propaganda are given. The main aspects of information wars are considered, priority directions and important steps of authorities in the field of state information policy are described.*

Keywords*: information security of the state, national information space; purpose, methods and means of information warfare; information threats; informational and psychological influence; information resources.*

У наш час тема інформаційної пропаганди та захисту від негативних інформаційних впливів є дуже актуальною, оскільки, війна інформацією є однією із основних та найнебезпечніших видів зброї. Інформація – масовий вплив, який є засобом інформування людей, при злих намірах є ключовим аспектом маніпулювання свідомістю та може досягти будь-яких цілей: знищення та усунення конкурента, або навіть розпалу війни.

Інформаційна війна послаблює моральні та матеріальні ресурси противника, пропагуючи негативний вплив на свідомість суспільства в емоційній та ідеологічній галузях. Маніпуляція інформацією є складовою частиною ідеологічної сутички. Війна інформацією наносить руйнування психологічного стану суспільства, за масштабом і за значенням рівна, а інколи і перевищує наслідки збройних війн.

Питання інформаційної війни та захисту від негативних інформаційних впливів привернуло велику увагу багатьох науковців.

Великий вклад в розкриття цієї проблеми зробили В. Балабін [1], І. Валюшко [2], М. Василенко [3], О. Горбань [4], О. Дубас [5], Я. Жарков [6], О. Курбан [7], А. Фісун [8] та інші.

Метою роботи є висвітлення цілей, методів і засобів ведення інформаційної війни.

Аналізуючи різні конфліктні ситуації з активним використанням інформаційних війн можна простежити певну мету та завдання, насамперед це посилення активних бойових дій; домінування між конкуруючими країнами шляхом активного впливу на галузі управління, політики, фінансів, економіки країн, які стали об’єктом агресії; підпорядкування країни шляхом маніпуляції свідомістю громадян.

Інформаційна війна висвітлює подану інформацію окремим об’єктом чи потенційною зброєю, вигідною ціллю. Інформаційна зброя є сукупністю спеціалізованих методів і засобів, які виводять із ладу окремий елемент чи інформаційну інфраструктуру загалом. Основною дією цієї зброї є спотворення або блокування прийнятих інформаційних даних і процесів рішень супротивника.

Наведемо фактори та недоліки інформаційного простору держави які впливають на інформаційну пропаганду: монополізація інформаційної галузі; залежність джерел масової інформації від держави або зацікавлених осіб; обмежена свобода висловлення власної думки журналістів; не рівна за ефективністю інформаційна структура більш розвинених країн та тих, що тільки почали свій розвиток.

Методи і засоби ведення інформаційної війни з часом удосконалюються, тим самим організація безпеки інформаційного простору ускладнюється. На сьогоднішній день можна виділити такі основні методи:

− блокування систем зв’язку і телекомунікацій;
− дезінформація;
− маніпулювання;
− навіювання;
− пропаганда;
− диверсифікація громадської думки;
− залякування;
− психологічний і психотропний тиск;
− поширення чуток.

Основними засобами інформаційної війни є: спотворення, приховування інформації; відволікання уваги неважливим від суттєвого; кількісне збільшення повідомлень якогось певного виду.

Усі ці засоби можна інтерпретувати в різних типах текстових, відео- чи аудіоповідомлень.

Дезінформація у суспільстві здійснюється різними способами: замовчування; оприлюднення неправдивої інформації; поєднання фейкових

і правдивих фактів; подання випадкових подій як систематичних і типових; висвітлення фактів, які були одержані із ненадійних джерел; зміна акцентів у поданні інформації; відвертання уваги суспільства від важливих подій великою кількістю другорядних; активне використання слів-подразників; навішування ярликів та використання штампованих фраз; маніпулювання трагічним чи негативним змістом, залякування військовими, екологічними, економічними проблемами тощо.

Інформаційний вплив за допомогою зображень, відеозаписів або аудіозаписів здійснюється у такий спосіб: оприлюднення уривків минулорічних записів про події які відбувалися в інших країнах для показу актуальних новин у державі інформаційної агресії; спотворення запису, який несе правдивий контент, для маніпулятивного повідомлення; вирізання якихось фрагментів для спотворення змісту; підміна у відео озвучення, перекладу тексту, який не був проголошеним; підміна інформації на відео чи фото для власної вигоди.

Забезпечення інформаційної безпеки – дії та заходи суб'єктів інформаційної безпеки, які спрямовані на досягнення стану захищеності життєво важливих інтересів особистості, суспільства та держави.

Можна виділити такі напрямки захисту інформаційного простору держави:

1. Надання інформаційної безпеки: створення і розвиток галузей держави, які несуть відповідальність за інформаційно-психічну безпеку населення; покращення державних регулюючих органів, що контролюють інформаційний простір держави; своєчасне реагування й усунення інформації, яка несе загрозу; урегулювання роботи засобів масової інформації, видавництв, телерадіоорганізацій, поліграфічних підприємств; притягнення до відповідальності осіб, які взаємодіють з інформаційним простором та пропагують або дезінформують суспільство.

2. Розвиток і забезпечення захисту державного інформаційного простору: сприяння розвитку та популяризації національного аудіовізуального, текстового контенту; надання допомоги для якісного функціонування радіомовлення та телебачення держави; стимулювання у підвищенні медіа-грамотності населення, надання інформації від професійних кадрів медіа-сфери з високим рівнем компетентності; сприяння наданню достовірної, об'єктивної та оперативної інформації населенню, яке проживає на тимчасово окупованих територіях.

3. Прозорість і відкритість влади перед громадянами держави: надання громадянам держави інформації від влади про діяльність органів, сприяння ефективній співпраці з журналістами та засобами масової інформації; залучення суспільства до прийняття рішень органами влади; допомога у формуванні культури суспільної дискусії.

4. Формування позитивного міжнародного іміджу держави: надання актуальної інформації про державу на міжнародній арені; сприяння розвитку публічної дипломатії, культурної та цифрової; створення продуктивного функціонування взаємодії органів влади з громадськістю; виявлення та протидія проти пропагандистської інформації держави-агресора; активна взаємодія з діаспорою держави стимулювання тісної співпраці та впровадження ефективних заходів; прийняття участі у міжнародних культурних заходах для представлення ідентичності та національної культури.

Таким чином, на сьогодні інформаційна війна має великий вплив на суспільство та державу. Впродовж років громадськість аналізує та надає рекомендації, пов’язані з протидією інформаційних загроз, і сприяє інформаційній безпеці держави. Спираючись на вищесказане можна виділити такі заходи: аналіз матеріалу медіа та виявлення неправдивої інформації; надання органам влади результати моніторингу; заохочення суспільства до викриття дезінформуючої, маніпулятивної інформації; надання суспільству правдивої інформації та розвінчання фейків; аналізування досвіду інших держав, щодо протидії негативним інформаційним впливам.

Інформаційні джерела

1. Балабін В. В., Дзюба М. Т., Жарков Я. М., Онищук М. І. Інформаційна безпека сучасного суспільства. Київ: ВІТІ, 2006. 201 с.

2. Валюшко І. О. Еволюція інформаційних війн: історія і сучасність. *Історико-політичні студії. Серія: Політичні науки*: зб. наук. пр. Київ: КНЕУ, 2015. № 2. С. 127–134.

3. Василенко М. К. Фантастичний репортаж-застереження як форма впливу на масову свідомість: новації жанру. *Українське журналістикознавство.* 2001. Вип. 2. С. 41–43.

4. Горбань О. Ю. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України.* 2015. № 1. С. 136–141.

5. Дубас О. П. Інформаційна війна: нові можливості політичного протиборства. *Освіта регіону: політологія, психологія, комунікації.* 2010. № 1. С. 69–73.

6. Жарков Я. М., Присяжнюк М. М. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування. *Вісник Київського національного університету імені Тараса Шевченка. Сер. Військово-спеціальні науки.* 2007. № 14–15. Вип. 14. С. 42–44.

7. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі. Київ: ВІКНУ, 2016. 286 с.

8. Фісун А. Ґенеза поняття “інформаційна війна”. *Гілея (науковий вісник):* зб. наук. праць. Київ: ВІР УАН. 2011. Випуск 49. С. 534–539.

УДК: 378.004

ТЕНДЕНЦІЇ РОЗВИТКУ НОРМАТИВНО-ПРАВОВОЇ БАЗИ УКРАЇНИ У СФЕРІ КІБЕРБЕЗПЕКИ

Зоряна Івануса[1], Андрій Івануса[2]

[1]Львівський державний університет внутрішніх справ, м. Львів, Україна
[2]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *Проведено інформаційний аналіз нормативно-правової бази України у сфері захисту інформації. Встановлено, що в Україні на сьогоднішній день не в повній мірі регламентовано необхідність та порядок захисту інформації у приватному секторі економіки. Запропоновано розробити нормативний документ, який би визначив необхідність захисту інформації приватних підприємств сертифікованими організаціями, які мають досвід роботи у сфері технічного та програмного захисту інформації, з метою покращення рівень кібербезпеки в Україні.*

Ключові слова: *нормативно-правова база, закон, кібербезпека, захист інформації.*

Abstract. *An information analysis of the regulatory and legal framework of Ukraine in the field of information protection was carried out. It has been established that the need and procedure for information protection in the private sector of the economy is not fully regulated in Ukraine today. It is proposed to develop a normative document that would determine the need for information protection of private enterprises by certified organizations with experience in the field of technical and software information protection, with the aim of improving the level of cyber security in Ukraine.*

Keywords: *regulatory framework, law, cyber security, information protection.*

На сьогоднішній день, в еру бурхливого розвитку цифрових технологій та постійного використання баз даних, все більш актуальним стає питання захисту інформації. Щороку кількість атак на об’єкти критичної інформаційної структури як приватної так і державної форм власності збільшуються. Якщо в Україні питання захисту інформації державних інституцій є регламентовано нормативно-правовими актами, то захист інформацією на приватних підприємствах, де участь держави відсутня, не регулюється в повній мірі. Тому необхідно провести детальніший аналіз нормативного правового поля України у сфері захисту інформації з метою виявлення незахищеного інформаційного простору у приватному секторі економіки країни, та запропонувати систему заходів стосовно його удосконалення.

У далекому 1992 році у нашій країні було прийнято Закон України “Про інформацію” [1], який регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. Даний нормативний акт говорить про те, що кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх

прав, свобод і законних інтересів. Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб. У ст. 7 закону [1] сказано, що право на інформацію охороняється законом, а також тещо держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до інформації.

Інший правовий акт [2] регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі – система). Згідно цього правового акту об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації, суб'єктами відносин, пов'язаних із захистом інформації в системах, є: володільці інформації, власники системи, користувачі, спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи. Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом. Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі. Протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування володільці інформації – власники (держателі) державних інформаційних ресурсів можуть укладати договори про технічне адміністрування відповідних реєстрів з іноземними компаніями, організаціями – постачальниками послуг з надання хмарних ресурсів (надавачами хмарних послуг), утвореними відповідно до законодавства інших держав, та/або їх зареєстрованими (акредитованими або легалізованими) відповідно до законодавства України філіями, представництвами та іншими відокремленими підрозділами з місцезнаходженням на території України в порядку, встановленому Кабінетом Міністрів України.

Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу. Власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством. Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

У статті 9 [2] сказано, що відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпе-

чення захисту інформації та контролю за ним. Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган.

Закон України "Про основні засади забезпечення кібербезпеки України" [3] визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Державно-приватна взаємодія у сфері кібербезпеки застосовується з урахуванням встановлених законодавством особливостей правового режиму щодо окремих об'єктів та окремих видів діяльності.

Контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою України в порядку, визначеному Конституцією України.

Як бачимо із аналізу нормативно-правового поля захисту інформації на сьогоднішній день не в повній мірі регламентовано саму необхідність захисту інформації приватних підприємств, що створює загрозу нашій національній безпеці. Тому пропонується розробити нормативний документ, який би визначив необхідність захисту інформації приватних підприємств сертифікованими організаціями, які мають досвід роботи у сфері технічного та програмного захисту інформації, що значно посилить рівень кібербезпеки в Україні.

Інформаційні джерела

1. Про інформацію: Закон України від 02.10. 1992 р. Відомості Верховної Ради (ВВР). 1992. №48. С. 650.

2. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07. 1994 р. Відомості Верховної Ради (ВВР). 1994. №31. С. 287.

3. Про основні засади забезпечення кібербезпеки України: Закон України від 2017 р. Відомості Верховної Ради (ВВР). 2017. №45. С. 403.

УДК 004.056.53

МЕТОДИ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ВЕБ-ДОДАТКІВ

Маргарита Кушнірук, Валентина Ящук, Тарас Репетило

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *Розглянуто теоретичні, науково-методичні та організаційно-функціональні основи тестування на проникнення веб-додатків. Визначено сучасні підходи до управління інцидентами інформаційної безпеки. Наведено методичні підходи до формування концепції удосконалення методики автоматизованого тестування веб-додатків, для забезпечення високого рівня безпеки і мінімізації ймовірності помилок або збоїв в роботі програми. Запропоновані методи проведення тестування на проникнення можуть використовуватись при розробці та тестуванні нових систем захисту інформації, а також оцінюванні ефективності та вдосконаленні вже існуючих систем.*

Ключові слова: *веб-додаток, безпека, тестування на проникнення, веб-сервери, атаки, вразливості.*

Abstract. *The theoretical, scientific-methodical and organizational-functional foundations of penetration testing of web applications are considered. Modern approaches to information security incident management are defined. Methodical approaches to the formation of the concept of improving the methodology of automated testing of web applications are presented, to ensure a high level of security and minimize the probability of errors or failures in the operation of the program. The proposed methods of penetration testing can be used in the development and testing of new information protection systems, as well as in the evaluation of the effectiveness and improvement of already existing systems.*

Keywords: *web application, security, penetration testing, web servers, attacks, vulnerabilities.*

Питання захисту інформації займає провідне місце в процесі проєктування, створення та використання сучасних інформаційних систем. Одним із методів перевірки захищеності інформації є тестування на проникнення. Тест на проникнення (пентест) це симуляція атаки на систему, з метою виявлення вразливостей при реальному нападі. Під час тестування визначається, як система відреагує в разі атаки і яку інформацію можна отримати в системі.

Тестування на проникнення дозволяє виявляти недоліки у сфері інформаційної безпеки (ІБ) із погляду стороннього спостерігача, не враховані при розробці політики безпеки; розкривати внутрішні і зовнішні спроби проникнення в інформаційну систему (ІС) й запобігати їм. Тестування на проникнення може виявити, наскільки безпеці ІТ-систем загрожує атака з

боку хакерів, зловмисників, тощо, а також чи здатні заходи безпеки в даний час забезпечити ІТ безпеку. Воно проводиться з метою виявлення ризику безпеки, який може бути присутнім у системі. Тестування на проникнення зазвичай оцінює здатність системи захищати свої мережі, програми, кінцеві точки та користувачів від зовнішніх або внутрішніх загроз. Воно також намагається захистити засоби контролю безпеки і забезпечує лише авторизований доступ.

Тестування є найбільш широко використовуваним і ефективним підходом для забезпечення якості та надійності програмного забезпечення, включаючи веб-додатки. Однак веб-додатки дуже відрізняються від традиційного програмного забезпечення, оскільки вони включають в себе динамічне створення та інтерпретацію коду, а також реалізацію конкретного режиму взаємодії на основі навігаційної структури веб-програми.

Кіберзлочинці при зломі веб-сайтів зазвичай використовують вразливості веб-додатків, що працюють на сервері або експлуатують деякі вразливості операційної системи, на якій працюють ці додатки. Тестування безпеки необхідне для додатків найрізноманітніших сфер застосування: звичайних веб-додатків; додатків з важливою комерційною або конфіденційною інформацією; різних платіжних систем, де ризик втрати інформації може оцінюватися значними фінансовими втратами; додатків з підвищеними вимогами до цілісності; соціальних мережі.

Сучасні веб-додатки використовують багаторівневу архітектуру, де реалізація розподіляється по різних шарах і запускається на різних машинах. З цієї причини, щоб перевірити загальну поведінку веб-додатків, потрібні наскрізні методи тестування. Безумовно, провівши повний цикл тестування безпеки, не можна бути на 100 % впевненим, що система є абсолютно безпечною. Однак те, що відсоток несанкціонованих проникнень, крадіжок інформації і втрат даних буде в рази меншим, ніж у тих хто не проводив тестування безпеки, гарантовано [1].

Класифікацією вразливостей веб – додатків займається Консорціум з безпеки веб – додатків WASC (Web Application Security Consortium). Згідно даних офіційного веб – сайту Консорціуму WASC, він представляє собою неприбуткову організацію, що складається з міжнародних експертів, фахівців з інформаційної безпеки та безпеки мережі Інтернет [2]. Консорціумом WASC 15 розроблено спеціальний документ, в якому описана класифікація вразливостей веб – додатків – WASC Threat Classification. Згідно документа WASC Threat Classification, вразливості веб – додатків поділяються за наступними етами життєвого циклу програмного забезпечення [2]:

– етап проєктування – охоплює вразливості, які можуть з’явитися внаслідок помилок у проєктуванні веб – додатка;

– етап реалізації – охоплює вразливості, які можуть з’явитися через помилки під час реалізації компонентів веб – додатка, наприклад – написання програмного коду;

– етап розгортання – охоплює вразливості, які можуть виникнути під час налаштування веб – додатка до роботи, наприклад – неправильна конфігурація веб – сервера;

Захищеність веб – додатків від атак зловмисників залежить від технологій та компонентів, які використовуються при побудові веб – додатків, а також від можливих вразливостей у цих компонентах. Існують різні класифікації вразливостей, кожна атака через вразливість має свої особливості, але причина виникнення вразливостей – помилки при проєктуванні, реалізації та застосуванні компонентів веб – додатків, отже виникає необхідність пошуку вразливостей та реагування на інформацію про випадки їх знайдення. Як в Україні, так і в інших країнах світу організовуються команди реагування на надзвичайні події у кібербезпеці, що складаються з експертів та дослідників.

Широкий вибір засобів дозволяє проводити пошук вразливостей, проте ефективність їх використання залежить від алгоритму дій, за яким необхідно проводити цей пошук. Алгоритми дій представлені у вигляді спеціальних методик, які охоплюють широке коло питань кібербезпеки, таких як тестування захищеності фізичного середовища, бездротових мереж, операційних систем, 50 мережевого обладнання та ін. Таким чином, необхідні додаткові витрати часу на аналіз існуючих методик та обрання тих складових, які підходять для тестування веб – додатків. Тому виникає необхідність у розробці такої методики тестування на проникнення, яка враховувала б міжнародні досягнення у тестуванні веб – додатків та містила перелік можливих засобів тестування.

Інформаційні джерела

1. Купріков М. Методи тестування системи на проникнення для забезпечення кібернетичної безпеки / Н. Купріков, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227. С. 80-83.

2. Балацька В.С. Використання сканерів вразливостей для захисту комп’ютерної мережі навчального закладу // В. Балацька, В. Ящук, О. Полотай / матеріали VI Міжнародної науково-практичної конференції “Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи”.

3. Zachko O., Kovalchuk O., Kobylkin D., Yashchuk V. Information technologies of HR management in safety-oriented systems. Materials of 2021 IEEE 16 th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT 2021). V. 2. Lviv, 2021. (Scopus Q2)

УДК: 004.056.5

ОРГАНІЗАЦІЯ ОПЕРАТИВНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ КОМПАНІЇ

Мар'яна-Марія Мних, Ростислав Ткачук, Богдана Федина

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *У роботі розглядається проблема створення та інтеграція Security Operation Center в компаніях. Оптимізація інформаційного захисту систем та динамічного розвитку інфраструктури бізнес-процесів. Фахового реагування на інциденти та їх розслідування.*

Ключові слова: *Security Operation Center, SIEM, компанія, інформаційний захист.*

Abstract. *The work examines the problem of creating and integrating Security Operation Center in companies. Optimization of information protection systems and dynamic development of the infrastructure of business processes. Professional incident response and investigation.*

Keywords: *Security Operation Center, SIEM, company, information protection.*

В Україні за останні роки в рази збільшилася кількість кібер-атак як в корпоративному секторі так і в державному, а самі зловмисники обєднуються у добре організовані групи, які мають відповідне технічне оснащення. Не рідко замовником таких атак є спецслужби ворожої держави які мають у своєму розпоряджені багатомільйонні бюджети.

Сучасний розвиток інформаційних технологій та глобалізація переходу різних сфер діяльності у хмарні технології спонукає фахівців у сфері кібербезпеки активно працювати над створенням єдиних центрів комплексного вирішення проблем щодо реагування на кібератаки та інші інциденти, які пов'язані із несанкціонованим проникненням та витоком інформації, а також можливістю швидкого реагування та подальшого розслідування інцидентів. На наш погляд оптимальним рішенням для вирішення таких задач є створення центру моніторингу та оперативного реагування на кібератаки, який допоможе протистояти атакам в режимі реального часу, а також фахово їх розслідувати.

SOC (Security Operations Center) − центр, основним завданням якого є консолідація всіх подій з різних систем, проведення конкретних аналізів для попередження інженерів з кібербезпеки про інциденти. Виходячи з отриманої інформації, інженери з кібербезпеки проводять кіберрозслідування, щоб виключити можливість повторення інциденту, що в подальшому мінімізує втрати при повторних небажаних подіях. SOC − це еволюція CERT (Computer Emergency Response Team) – це команди інженерів підготовлені для реагування на різні та нестандартні ситуації,

пов'язані з комп'ютерними технологіями. Ключовою відмінністю від CERT є використання новітніх технологій аналітики для оперативного розуміння поточної ситуації в контурі інформаційної безпеки компанії. Security Operation Center (SOC) означає систему, розроблену та побудовану на основі SIEM (Security Information and Event Management), яка призначена для збору та зберігання журналів із пристроїв та додатків для глибокого аналізу та кібер-розслідування інцидентів. В даний час SOC, які створені на базі SIEM, допомагають компаніям вирішувати ключові завдання [1]:

− збирати та зберігати лог-файли в єдиному сховищі;

− визначати активність в мережі підприємства, та сигналізувати коли вона перевищує дозволені параметри;

− виконувати аналаз співвідношення подій між джерелами інформації.

На єтапі розвитку компанії, збільшення обсягів бізнес-процесів, розширення та розгалуження інфраструктури настають необхідні передумови для створити SOC. Власники бізнес-процесів та інфраструктури, мають бути обізнані про виклики, що пов'язані з ризиками повязаними з інформаційною безпекою, та загрозами для бізнесу.

Якщо керівництво компанії приділяє особливу увагу актуальним потребам та вимогам в бізнес-процесах та розкитку інфраструктури, то слід розглянути питання про створення SOC у відповідь на існуючі ризики пов'язані із кібербезпекою.

Витрати інвестовані компанією в кібербезпеку вже в середньотривалій перспективі оправдують затрати, адже сприяють підвищенню ефективності як самих підсистем, так і процесів повязаних із захистом від несанкціонованого проникнення, допомагають оптимізувати та захистити як мережі так і процеси в них. Збільшення витрат також може означати, що компаніям потрібно створити SOC [2].

Створення Enterprise SOC дуже актуальне, особливо коли чисельність співробітників перевищує п'ятсот осіб. Такі компанії, як правило роззосереджені у різних містах та країнах. Отже при наявності високої цінності інформації яку необхідно захищати, великого спектру способів її захисту, широкій територіальній структурі та багаточисельності працівників − це перші передумови для створення власного SOC. Основою будь-якого SOC складають наступні компоненти [3]:

− персонал − інженери, аналітики, директор;

− база − набори співвідношень, норми інцидентів, моделі оповіщення, бази знань про різні загрози та вектори атак;

− процеси − процедури аналізу інцидентів, реагування, звітності, ескалації та протидії інцидентів;

− забезпечення − розміщення SOC, SIEM, інструментів моніторингу продуктивності, сховищ подій, інцидентів, ліцензії на систему SIEM та додаткових модулів.

Для великої компанії, яка хоче побудувати Enterprise SOC з “нуля”, таке впровадження може зайняти досить тривалий час і до того ж без гарантій у кінцевому позитивному результаті. Проблеми в будь якому з елементів (персонал, база, процеси, забезпечення), може значно знизити ефективність SOC, а в окремих випадках звести затрачені ресурси та час на нівець. Тому бізнес постає перед ділемою створювати свою команду (довготривала перспектива) чи наймати фахівців з кіберзахисту.

На наш погляд, у такій ситуації, впровадження SOC-as a service допоможе знизити ризики повязані з безпекою, дозволить запустити моніторинг подій, надасть змогу провести фахову експертизу, команду та базу. При використанні SOC as a service, вирішується кадрова проблема, заповнення контентом SIEM, розробка процесів взаємодії при виявленні, аналізі та протидії на інциденти − всі завдання переходять до аутсорсиру. Постачальник послуг враховує специфіку компанії і внутрішні вимоги. Для компаній які налаштовані на створення Enterprise SOC, в рамках довготривалої співпраці найбільш оптимальним варіантом, може бути, впровадження Hybrid Security Operations Center, що передбачає використання SIEM, яку постачальник послуг забирає на адміністрування та оптимізує її під замовника. Hybrid варіант також вирішує завдання швидкого пошуку команди моніторингу, що дає компанії більше часу на пошук та підготовку власного персоналу.

Впровадження Security Operation Center на підприємстві дозволяє мінімізувати реалізацію можливих загроз та вирішує низку проблем повязаних з інформаційною безпекою, що дає змогу:

− контролювати стан інформаційної безпеки;
− моніторити події інформаційної безпеки;
− проводити аудит дій користувачів;
− відстежувати та управляти вразливостями;
− управляти інцидентами з інформаційної безпеки;
− проводити контроль за дотриманням законодавчих актів;
− впроваджувати кращі міжнародні практики.

Інформаційні джерела

1. What is a SOC (Security Operations Center) [Електронний ресурс]. – Режим доступу: http://securityaffairs.co/wordpress/47631/breaking-news/soc security-operations-center.html.

2. Security Information and Event Management [Електронний ресурс]. – Режим доступу: https://www.gartner.com/en/information technology/glossary/security-information-and-event-management-siem.

3. S. David. A Practical Application of SIM/SEM/SIEM / Automating Threat Identification. SANS Institute, 2006. p.3. [Електронний ресурс]. – Режим доступу: https://www.sans.org/reading-room/whitepapers/logging/practical-%20application sim-sem-siem-automating-threat-identification-1781.pdf.

УДК 004.891.3:004.3

АНАЛІЗ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІТ ПІДПРИЄМСТВА

Андрій Лагун, Аскольд Небельський

Національного університету "Львівська політехніка" м. Львів, Україна

Анотація. *Розглянуто способи оцінки ризиків ІТ підприємства. Особлива увага звертається на вираховування вартості активів, наявних загроз і вразливостей на етапах оцінки ризиків. Наведено перелік дій для зменшення ступеня наявного ризику.*

Ключові слова: *інформаційна безпека, оцінка ризику, загроза, активи підприємства, вразливість.*

Abstract. *Are considered the ways of assessing the IT risks of the enterprise. Special attention is paid to calculating the value of assets, existing threats and vulnerabilities at the stages of risk assessment. Also is given a list of actions to reduce the degree of existing risk.*

Keywords: *information security, risk assessment, threat, enterprise assets, vulnerability.*

Сучасні методи обробки, передавання та збереження інформації сприяють появі загроз і ризиків, пов'язаних з можливістю втрати, перекручування і розкриття даних, які використовуються на підприємствах. Тому забезпечення інформаційної безпеки комп'ютернних систем і мереж є важливим етапом розвитку інформаційннх технологій.

Спочатку варто зазначити, що при розгляді питань інформаційної безпеки, зокрема ризиків реалізації загроз, потрібно звернути увагу на наявність двох протилежних сторін зі своїми цілями: атакуючих, які хочуть отримати, або зламати конфіденційну інформацію; захисників, які хочуть забезпечити неможливість втрати інформації. Питання ризиків інформаційної безпеки, як правило, стосуються дій захисників.

Незалежно від конкретних видів загроз інформаційна система задовольняє потреби її користувачів, якщо забезпечуються такі властивості інформації, як доступність (можливість протягом певного часу отримати інформацію), цілісність (уникнення несанкціонованої зміни інформації), конфіденційність (уникнення несанкціонованого отримання інформації).

Для ІТ підприємств загрози інформаційної безпеки можна класифікувати за названими властивостями інформації, на які вони направлені. Загроза відмова в обслуговуванні (доступність) створюють ситуацій, коли певні дії або блокують доступ до деяких ресурсів ІТ підприємства, або

знижують їх працездатність. Відмова в обслуговуванні шляхом блокування доступу до ресурсу може бути постійною або тимчасовою. Загрози зміни або спотворення інформації (цілісність) призводить до порушення її якості або повного знищення. Ця загроза може бути здійснена навмисно зловмисником, а також в результаті об'єктивних впливів з оточуючого середовища. Ця загроза особливо актуальна для комп'ютерних мереж і систем телекомунікацій ІТ підприємства. Загрози отримання комерційної інформації неповноваженими особами (конфіденційність) спрямовані на розголошення секретної інформації. Загроза порушення конфіденційності виникає при отриманні несанкціонованого доступу до закритої інформації, що зберігається і обробляється на ІТ підприємстві.

Оцінка ризиків інформаційної безпеки ІТ підприємства визначає та оцінює ризики для активів, на які можуть вплинути кібератаки. Спочктку потрібно визначити внутрішні та зовнішні загрози; оцінити їх можливий вплив на конфіденційність, цілісність і доступність даних; оцінити витрати, пов'язані із зміною даних. Маючи такі дані, можна адаптувати засоби керування інформаційною безпекою ІТ підприємства та захистом даних відповідно до фактичного рівня стійкості до ризику компанії.

Для оцінки ризиків інформаційної безпеки потрібно, в першу чергу, визначити та розставте пріоритети активів: сервери, дані клієнтів, конфіденційні документи партнерів, комерційні таємниці. Оскільки технічний працівник може не правильно розуміти цінність активів для бізнесу, то список. активів узгоджується з керівництвом і бізнес-користувачами.

На другому етапі визначають загрози, які розглянули раніше. Загрози визначаються також вразливими місцями. Вразливості можна виявити за допомогою аналізу, процедур тестування та оцінки інформаційної безпеки, аудиторських звітів, тестування на проникнення, бази даних уразливостей NIST, даних постачальника та автоматизованих інструментів сканування вразливостей. Наприклад, якщо ви не повідомити працівників про небезпеку натискання посилань електронною поштою, вразливість від фішингу зростає.

Наступним кроком є аналіз елементів керування на етапі планування для зменшення ймовірності того, що загроза використає вразливість. Технічні засоби контролю повинні виконувати шифрування, механізми виявлення вторгнень, рішення для ідентифікації та автентифікації. Нетехнічні засоби контролю включають політику безпеки, адміністративні дії, фізичні та екологічні механізми.

На останньому етапі потрібно визначити ймовірність інциденту і ймовірність того, що вразливість може бути використана, враховуючи тип вразливості, потужність джерела загрози, наявність різних елементів керування.

Всі етапи оцінки ризиків інформаційної безпеки ІТ підприємства зображено на рис. 1.

Рисунок 1 – Етапи оцінки ризиків інформаційної безпеки

Зокрема оцінюють наслідки інциденту для втраченого або пошкодженого активу, а саме призначення активу та операцій, які залежать від нього, значущість активу для організації, чутливість активу. Для кожної пари загроза/вразливість потрібно вказати рівень небезпеки для системи і можливість того, що загроза використає вразливість, приблизну вартість кожного із заходів, достатність поточних або запланованих засобів контролю безпеки інформаційної системи для усунення або зменшення ризику.

Використовуючи рівень ризику, наведемо перелік дій, необхідних для його зменшення:

− високий – стратегію коригувальних дій розробляють якнайшвидше;

− середній – виправні заходи потрібно розробити з врахуванням впливу ризику;

− низький – визначають, чи прийняти ризик, чи застосувати дисциплінарні заходи.

Основними висновками роботи є те, що основою кібербезпеки є процеси управління ризиками підприємства та оцінка ризиків інформаційної безпеки. Ці процеси створюють основу абсолютної стратегії управління інформаційною безпекою, надаючи відповіді на питання, які загрози та вразливості можуть завдати фінансової шкоди бізнесу, а також як їх можна пом’якшити.

Інформаційні джерела

1. How to perform a cybersecurity risk assessment step by step. [Електронний ресурс] – Режим доступу: https://www.techtarget.com/ searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step

2. Cybersecurity risk management process. [Електронний ресурс] – Режим доступу: https://hyperproof.io/resource/ cybersecurity-risk-management-process/

3. Cybersecurity risk management frameworks. [Електронний ресурс] – Режим доступу: https://www.reflectiz.com/blog/cyber-security-risk-management-frameworks/

УДК 004.621.3

СИСТЕМА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сніжана Ориник, Валентина Ящук, Марія Навитка

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *Розглянуто теоретичні, науково-методичні та організаційно-функціональні засади проєктування системи управління інцидентами інформаційної безпеки. Визначено сучасні підходи до управління інцидентами інформаційної безпеки. Наведено методичні підходи до формування концепції та структури автоматизованої системи управління інцидентами інформаційної безпеки. Запропоновано процедури планування і реагування на інциденти та наведено основні цілі управління інцидентами інформаційної безпеки.*

Ключові слова: *інформаційна безпека, інцидент інформаційної безпеки, система управління інцидентами інформаційної безпеки.*

Abstract. *The theoretical, scientific-methodical and organizational-functional principles of the design of the information security incident management system are considered. Modern approaches to information security incident management are defined. Methodical approaches to the formation of the concept and structure of the automated information security incident management system are presented. Procedures for planning and responding to incidents are proposed and the main goals of information security incident management are given.*

Keywords: *information security, information security incident, information security incident management system.*

Сьогодні темп розвитку сучасних інформаційних технологій значно перевершує темп розвитку рекомендацій на нормативно-правових підставах відповідних документів щодо системи менеджменту управління інцидентами інформаційної безпеки. Навіть найкраща інфраструктура інформаційної безпеки не може гарантувати відсутність вторгнень чи інших шкідливих, зловмисних дій. Система управління інформаційною безпекою (СУІБ) є частиною загальної системи управління, заснованої на оцінюванні бізнес-ризику для створення, впровадження, експлуатації, постійного моніторингу, аналізу, підтримки та вдосконалення інформаційної безпеки (ІБ).

Інцидентом у системі захисту інформації вважається небажана (несподівана) подія або низка подій у системі захисту, які можуть поставити під загрозу бізнес-операції та захист певної інформації. Швидкість, з якою організація може ідентифікувати, аналізувати, запобігати інцидентам і реагувати на них, обмежить завдані збитки та зменшить витрати на відно-

влення. Цей процес виявлення, аналізу та визначення відповіді організації на інцидент комп’ютерної безпеки називається управління інцидентами. Люди, ресурси та інфраструктура, що використовуються для виконання цієї функції, становлять можливості управління інцидентами.

Здатність контролювати інциденти – це здатність забезпечити контроль інцидентів комп’ютерної безпеки. Вона передбачає створення контрольної команди для управління інцидентами безпеки. Крім цього, ця здатність передбачає визначення процесу, якого слід дотримуватися, серед політик і процедур, розподілу ролей і зобов’язань, наявність відповідного обладнання, інфраструктури, інструментів і допоміжних матеріалів, а також наявність кваліфікованого персоналу, визначеного і підготовленого для виконання роботи у високоефективному режимі.

Процедури планування і реагування на інциденти, події чи слабкості систем захисту інформації повинні бути чітко визначені до виникнення інциденту і схвалені керівництвом організації. *ISO/IEC 27001* – це міжнародний стандарт для управління інформаційною безпекою. Цей стандарт детально описує всі вимоги до створення, впровадження, обслуговування та постійного поліпшення системи управління інформаційною безпекою, яка, у свою чергу, спрямована на допомогу організаціям в безпечному здійсненні їх діяльності з інформаційної безпеки.

ISO/IEC 27001 вимагає від менеджменту:

− систематично вивчати ризики інформаційної безпеки організації, враховуючи усі можливі загрози та вразливі місця;

− розробляти і вимагати використання складного набору засобів управління інформаційною безпекою та/або інших форм управління ризиками (таких як уникнення ризику або передбачення ризику) для вирішення тих ризиків, які вважаються неприйнятними;

− прийняти весь процес управління для забезпечення того, щоб контроль інформаційної безпеки задовольняв потреби організації в інформаційній безпеці на постійній основі.

Ефективність процесу системи управління інцидентами інформаційної безпеки залежить від координаційних дій всіх осіб, що беруть безпосередню участь; доступності можливостей для отримання та аналізу інформації, пов’язаної з інцидентом; оперативності та правильності отриманих результатів. Вдосконалення кожного з цих показників значно підвищує ефективність всього процесу і, в свою чергу, дозволяє розділу інформаційної безпеки організації досягти більш значних та ефективніших результатів.

Основні вимоги до процесу управління інцидентами інформаційної безпеки, які містяться в стандартах *ISO/IEC 27001* та *ISO/IEC 27002* включають, у свою чергу: розподіл відповідальності та розробки певних процедур щодо роботи системи (процесів); інформування про інциденти та ура-

зливості інформаційної безпеки; інформування про оцінки та прийняття рішень по інцидентах ІБ; включає реагування на інциденти, витяг певних уроків з них та збір свідчень.

Припущення, що інцидент відбувся в організації, повинне базуватися на таких трьох основних елементах: інформація про інцидент приходить одночасно з декількох джерел; *IDS* сигналізує вже про багаторазовість певних подій; аналіз журнальних файлів автоматизованої системи *(AS)* надає основу для висновку про можливість інциденту.

До основних цілей управління інцидентами відноситься:

− надання інформації, що дозволить оптимізувати процеси підтримки, зменшити кількість інцидентів;

− злагоджена обробка всіх інцидентів та запитів обслуговування;

− відновлення нормальної роботи системи в найкоротший термін;

− мінімізація впливу інцидентів на працездатність організації;

− зосередження ресурсів щодо підтримки найбільш важливих напрямків системи.

Управління інцидентом, це досить важливий процес, який полягає у забезпеченні організації можливості спочатку виявити інцидент, а згодом за допомогою правильно обраних засобів підтримки, якомога швидше вирішити цей інцидент. Але жоден спосіб зниження ризиків інформаційної безпеки не здатен захистити від виникнення в інформаційному середовищі подій, які несуть потенційну загрозу діяльності певної організації.

Інформаційні джерела

1. Incident Management. [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisa.gov/uscert/bsi/articles/best-practices/incident-management/incident-management

2. ISO 27001. Управління інцидентами інформаційної безпеки. [Електронний ресурс] – Режим доступу до ресурсу: https://www.isms.online/iso-27001/annex-a-16-information-security-incident-management/

3. Стандарти ISO/IEC управління інформаційною безпекою. [Електронний ресурс] – Режим доступу до ресурсу: https://studfile.net/preview/5367198/page:3/

4. Драб Ю. Основні підходи до побудови системи управління інформаційною безпекою / Ю.Драб, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С. 29-32).

5. Малькевич Р. Проблеми забезпечення безпеки інформації підприємства в умовах пандемії / Р. Малькевич, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С. 69–72).

УДК: 004.7

КЕРУВАННЯ БЕЗПЕКОЮ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ ІНДЕКСУ ДОВІРИ

Уляна Пановик[1], Сергій Кутас [1], Тарас Брич [2]

[1]Української академії друкарства, м. Львів, Україна
[2]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *Пристрої IoT за допомогою хмарних технологій збирають величезну кількість цінних даних, значна частина яких зберігається в хмарі. Довіра між пристроями IoT та їхніми даними визнана основою створення системи IoT. Підключення до підозрілих пристроїв Інтернету речей може становити загрозу для послуг і роботи системи. Тому дуже важливо аналізувати та керувати інформацією про довіру для пристроїв, а також надавати інформацію про довіру іншим пристроям або користувачам, яким вона потрібна.*

Ключові слова: *Інтернет речей, безпека IoT, довіра; управління довірчою інформацією; індекс довіри.*

Abstract. *IoT devices use cloud technologies to collect a huge amount of valuable data, a large part of which is stored in the cloud. Trust between IoT devices and their data is recognized as the foundation of an IoT system. Connecting to suspicious IoT devices can pose a threat to services and system operation. Therefore, it is very important to analyze and manage trust information for devices, and to provide trust information to other devices or users that need it.*

Keywords: *Internet of things, IoT security, trust; trust information management; confidence index.*

Інтернет речей – одна з найбільш стрімких у розвитку технологій у світі. Пристрої інтернету речей вже використовуються у багатьох галузях діяльності людини, включаючи такі критичні галузі, як енергетика, охорона здоров'я та військова галузь. Глибока інтеграція цих пристроїв допомагає людям швидко та ефективно вирішувати багато проблем, полегшити виконання складних завдань, вивільнити людські ресурси для виконання більш важливих інтелектуальних завдань. В майбутньому планується подальший розвиток технологій інтернету речей, більш глибока інтеграція в усі сфери діяльності людини та виконання інтелектуальними пристроями все більш складних та важливих функцій.

Для бездротової передачі даних особливо важливу роль в побудові Інтернету речей відіграють такі характеристики, як ефективність, відмовостійкість, адаптивність, можливість самоорганізації. Основне зацікавлення в цьому сенсі представляє стандарт IEEE 802.15.4, що управляє доступом

для організації енергоефективних персональних мереж, і є основою для таких протоколів, як ZigBee, WiFi, Bluetooth, 6LoWPAN.

Проте, незважаючи на всі переваги, які інтернет речей приносить у побут людини, він також несе у собі серйозні загрози. Через велику розповсюдженість інтернету речей та важливість функцій, які виконують пристрої IoT, сфера інтернету речей приваблює все більше уваги зловмисників. Втручання у роботу інтелектуальних пристроїв може призвести до фінансових збитків, які нараховують мільярди доларів США, або навіть нести безпосередню загрозу для життя людей.

Встановлено, що за допомогою пристроїв інтернету речей вже відбулося багато інцидентів інформаційної безпеки з отриманням несанкціонованого доступу зловмисників до персональних даних. Через високий ступінь інтеграції в життя та побут людей, ці пристрої мають доступ до великого обсягу персональної інформації. А через низький рівень захищеності пристроїв IoT, ця інформація може потрапити до зловмисників чи компаній, які можуть використовувати цю інформацію для власних потреб.

Спеціалісти OWASP визначили 10 основних проблем інформаційної безпеки, пов'язаних з IoT, до яких відноситься: незахищений вебінтерфейс, недостатній механізм автентифікації/авторизації, незахищені сервіси мережі, відсутність шифрування при передачі даних, порушення конфіденційності, незахищений хмарний інтерфейс, незахищений мобільний інтерфейс, недостатня конфігурація безпеки, ненадійне програмне забезпечення, слабка фізична безпека. Кожна з цих проблем містить додаткові вразливості, які зрештою можуть призвести до модифікації або витоку даних [1].

Для забезпечення загального рівня інформаційної безпеки при використанні об'єктів Інтернету речей будь-якого призначення можна виділити чотири основні складові:

− безпека зв'язку (за допомогою технологій шифрування і перевірки справжності);

− захист пристроїв (забезпечення цілісності програмного коду, наприклад шляхом криптографічного підписання);

− контроль пристроїв (необхідність встановлення патчів та передбачення "безпеки зсередини" – вбудованої функції оновлень "по повітрю" ("over-the-air") на пристроях);

− контроль взаємодії в мережі (періодичні моніторинг, сканування та аналітика мережі на предмет аномалій та загроз).

Унікальним для IoT є те, що пристрої (наприклад, вбудовані датчики) повинні розпізнати інші пристрої. Саме це зменшує ймовірність проникнення чужорідного тіла в системі. Для забезпечення інформаційної безпеки на почтакових етапах "спілкування" з чужорідним пристроєм можна ввести таке поняття як індекс довіри (trust index) для пристроїв IoT [2].

Індекс довіри прямо пропорційний достовірності джерела з точки зору схожості. Чим вищий показник довіри, тим більше шансів для системи, що дані надійдуть від авторизованого пристрою IoT або джерела. На малюнку представлений алгоритм перевірки для підключення в систему (рис. 1).

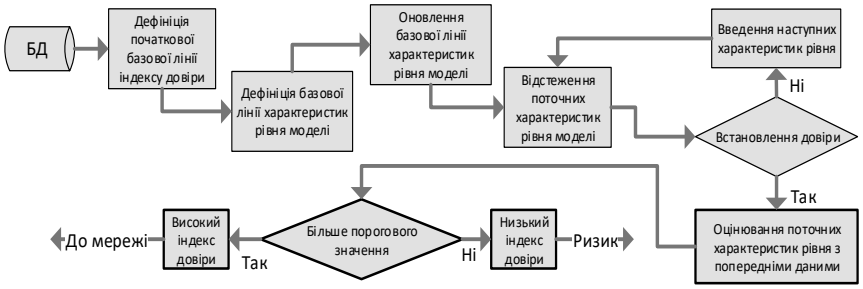


Рисунок 1 – Алгоритм перевірки безпеки

Якщо індекс довіри нижче порогового, то відповідно пристрій не зможе знаходитися в мережі. Система переспрямовує трафік з пристрою на сервіс, який аналізує відповідь і намагається зібрати більше даних про напад.

Ці дані надходять до підсистеми безпеки, і він оновлює параметри характеристик рівня для вивчення та аналізу атаки або зупиняє її на першому ж етапі. Відповідно, для зловмисників буде не легко копіювати дані. Це відбувається з тієї причини, що складність рівня збільшується, і стає важче влізти в систему або створити хибні характеристики. Наприклад, характеристики фізичного рівня, такі як направлення на абонента(angle of arrival) в бездротовому зв'язку. Приймач отримає дані, програмно визначити їх неможливо. Будь-який зловмисник не зможе придумати такі характеристики, доки він не використовуватиме таке ж обладнання чи місцезнаходження.

Такий алгоритм можна застосувати для зменшення ймовірності спуфінга. Система зможе проаналізувати мережу на наявність "чужих" пристроїв та вберегти її від злому, не дозволить зловмиснику проникнути в мережі та забезпечить інформаційну безпеку інформаційної системи IoT.

Інформаційні джерела

1. Um T-W, Lee E, Lee GM, Yoon Y. Design and Implementation of a Trust Information Management Platform for Social Internet of Things Environments. Sensors. 2019; 19(21):4707. https://doi.org/10.3390/s19214707

2. Warsun Najib, Selo Sulistyo, Widyawan. Survey on Trust Calculation Methods in Internet of Things. Procedia Computer Science 161 (2019) 1300–1307. 10.1016/j.procs.2019.11.245.

УДК 004.056

ДОСЛІДЖЕННЯ МЕТОДІВ ЗБОРУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ КІБЕРРОЗВІДКИ ТА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ З МЕТОЮ МОДЕЛЮВАННЯ ДІЙ ЗЛОВМИСНИКА

Ілля Пасічник, Орест Полотай, Тарас Брич

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *Описано методи збору інформації за допомогою кіберрозвідки та соціальної інженерії.*

Ключові слова: *соціальна інженерія, кіберрозвідка.*

Abstract. *Methods of gathering information using cyber intelligence and social engineering are described.*

Keywords: *social engineering, cyber intelligence.*

Майже щодня компанії у галузі кібербезпеки та ЗМІ повідомляють новини про успішні кібератаки, складність та масштаби яких зростають. Також варто зазначити що основним компонентом для будь-якої успішної атаки є розвідка.

Загалом, розвідка спирається на комплексний набір методів і процесів і не повинна вважатися обмеженою інформацією, що характеризує ціль на технологічному рівні, наприклад, використовуване апаратне забезпечення або версія компонентів програмного забезпечення. Зловмисники також прагнуть зібрати деталі, пов’язані з фізичним місцезнаходженням жертви, номерами телефонів, іменами людей, які працюють у цільових організаціях, та їхніми електронними адресами. Насправді будь-яка частина знань може бути використана для розробки програмного експлойту або виявлення слабких місць у захисних системах.

На жаль, розвиток Інтернету, розповсюдження онлайн-соціальних мереж, а також розвиток сервісів для сканування інтелектуальних пристроїв і вузлів Інтернету речей призводять до вибуху джерел, які можуть зробити етап розвідки швидшим, легшим і ефективнішим. Це також може запобігти контакту з жертвою або обмежити його тривалість, що ускладнить раннє виявлення та блокування спроб розвідки. Таким чином, дослідження еволюції методів, що використовуються для кіберрозвідки, є надзвичайно важливим для розгортання чи розробки ефективних заходів протидії.

Щоб проілюструвати найважливіші методи кіберрозвідки та зобразити їх еволюцію, ми можемо їх умовно прокласифікувати, розбивши на 4 компоненти:

− соціальна інженерія: групує методи збору інформації, щоб ввести людину в оману або переконати її поводитися бажаним чином.

− інтернет-розвідка: групує методи, що використовують інформацію, яка є загальнодоступною в Інтернеті, включаючи бази даних, доступні через Інтернет.

− збір інформації з оточення: групує методи для здобуття інформації та інтересів з кругу спілкування жертви та дотичних до неї активностей.

− інші канали: групує методи, що базуються на отриманні ненавмисно злитої інформації жертви про саму себе.

Кожен клас відповідає заданому “ступеню взаємодії” з жертвою, із визнанням того, наскільки тісним має бути зв’язок із джерелом інформації для цілей розвідки. Наприклад, щоб читати екран комп’ютера, потрібно бути поруч із жертвою, отже потенційно мати фізичну взаємодію, тоді як сканування її круку взаємодії може здійснюватися віддалено. Крім того, деякі побічні канали використовують вимірювання, що передбачає фізичну близькість до цілі (наприклад, для вимірювання інтенсивності електромагнітного поля або температури джерела тепла), тоді як отримання даних із соціальної мережі не вимагає взаємодії з активом, яким керує або володіє сама жертва.

Щодо методів протидії кіберрозвідці, то це, перш за все, метод спрямований на навчання та підвищення обізнаності користувачів щодо зниження ефективності соціальної інженерії або запобігання витоку конфіденційної інформації. Для цього необхідно проводити постійні кампанії аудиту та моніторингу загальнодоступної інформації в Інтернеті. Зміна парадигми відбулася, коли розробка контрзаходів перейшла з розгляду переважно технології, а не людини. Перша хвиля стосується реактивних заходів протидії та має на меті пряме реагування на певну техніку розвідки, наприклад, сканування або прослуховування. Остання тенденція стосується проактивних заходів протидії: у цьому випадку зловмиснику постійно заважають або перешкоджають, наприклад, шляхом навмисного поширення даних, що вводять в оману.

Отже, як ми бачимо, в наш час прогресують безконтактні методи кіберрозвідки, і для того щоб мінімізувати ризики потрапляння персональної інформації до рук зловмисників ми повинні дуже чітко розуміти ці ризики та слідкувати за своєю кібергігієною.

Інформаційні джерела

1. Що таке кіберрозвідка та як вона працює. [Електронний ресурс]. Режим доступ з https://www.blumira.com/glossary/reconnaissance/.

2. Кіберрозвідка у розрізі етичного хакінгу. [Електронний ресурс]. Режим доступ з https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_ reconnaissance.htm.

3. Життєві цикли та техніки соціальної інженерії. [Електронний ресурс]. Режим доступ з https://www.imperva.com/learn/application-security/social-engineering-attack/.

4. Фішинг у соціальній інженерії. [Електронний ресурс]. Режим доступ з https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering.

5. Як працює соціальна інженерія та методи захисту від неї. [Електронний ресурс]. Режим доступ з https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html

6. Пасивна та активна розвідка і їх складові. [Електронний ресурс]. Режим доступ з https://www.jigsawacademy.com/blogs/cyber-security/reconnaissance-in-hacking/

7. Основи кібергігієни та інтернет розвідки. [Електронний ресурс]. Режим доступ з https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/basics-footprinting-reconnaissance/

УДК 316.74:378.147

АНАЛІЗ МОТИВАЦІЇ ПОРУШНИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ В ЕЛЕКТРОННОМУ КУРСІ НАВЧАЛЬНОГО СЕРЕДОВИЩА

Орест Полотай, Ольга Меньшикова

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *Описано основні типи порушників інформаційної безпеки електронного курсу навчального середовища закладу вищої освіти, з точки зору їх мотивації.*

Ключові слова: *безпека електронного курсу, дистанційне навчання.*

Abstract. *The main types of information security violators of the electronic course of the educational environment of the higher education institution are described, from the point of view of their motivation.*

Keywords: *electronic course security, distance learning.*

Порушник – це особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби здійснила спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Метою порушника може бути:

− отримання необхідної інформації у потрібному обсязі;

− мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами;

− нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Порушники поділяються на дві основні групи: зовнішні та внутрішні (таблиця 1).

Таблиця 1

Модель порушника за мотивом порушника

Модель внутрішнього порушника			
Категорія порушників		Мотив порушника	Рівень збитків
Технічний персонал	технічний адміністратор	М1, М2, М4	1+2+4=7
Персонал, який обслуговує технічні засоби	основний адміністратор	М1, М2, М4	1+2+4=7
	адміністратор навчального відділу	М3,М4	3+4=7
Користувачі АС	завідувач кафедри	М1, М3	1+3=4
	декан	М1, М3	1+3=4
Керівники різних рівнів посадової ієрархії	адміністратор веб-серверу	М2, М3, М4	2+3+4=9
Співробітники підрозділів розробки та супроводження програмного забезпечення	працівники відділу ТЗІ	М1, М3, М4	1+3+4=8
Модель зовнішнього порушника			
Відвідувачі (запрошені з деякого приводу)		М2, М3	2+3=5
Співробітники закордонних спецслужб або особи, які діють за їх завданням		М2, М3	2+3=5
Хакери		М2, М3	2+3=5

Серед внутрішніх порушників можна виділити такі: користувачі системи; персонал, що обслуговує технічні засоби; співробітники відділів розробки та супроводження програмного забезпечення; співробітники служби безпеки; керівники різних рівнів та посадової ієрархії.

Серед зовнішніх порушників можна виділити такі: клієнти (представники організацій, громадяни); відвідувачі (запрошені з якого-небудь приводу); хакери; особи, які випадково або навмисно порушили пропускний режим (без мети порушити безпеку); будь-які особи за межами контрольованої зони.

Можна виділити також три основних мотиви порушень (М – мотив порушника):

− безвідповідальність (рівень загроз – 1);

− самоствердження (рівень загроз – 2);
− корисливий інтерес (рівень загроз – 3);
− професійний обов'язок (рівень загроз – 4).

При порушеннях, викликаних безвідповідальністю, користувач цілеспрямовано або випадково виробляє руйнуючі дії, які не пов'язані проте зі злим умислом. У більшості випадків це наслідок некомпетентності або недбалості. Деякі користувачі вважають одержання доступу до системних наборів даних значним успіхом, затіваючи свого роду гру заради самоствердження або у власних очах, або в очах колег.

Порушення безпеки інформації електронного курсу (ЕК) навчального середовища може бути викликано корисливим інтересом користувачів даного навчального середовища. У цьому випадку він буде цілеспрямовано намагатися подолати систему захисту для несанкціонованого доступу до інформації в ЕК.

Інформаційні джерела

1. Меньшикова О.В., Полотай О.І. Використання технологій дистанційного навчання в умовах Covid-19 в ЛДУБЖД. Зб. тез доп. VI Міжнар. наук.-практ. конф. "Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи". (м. Львів, 04 листопада 2021 р.). Львів : ЛДУБЖД, 2021.

2. Полотай О.І., Кухарська Н.П. Особливості реалізації політики безпеки дистанційного курсу. Зб. тез доп. VI Міжнар. наук.-практ. конф. "Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи". (м. Львів, 04 листопада 2021 р.). Львів : ЛДУБЖД, 2021.

3. Полотай О.І., Кухарська Н.П. Розроблення електронних курсів у віртуальному навчальному середовищі. Навчальний посібник Львів : СПОЛОМ, 2021. 172 с.

4. Полотай О.І. Зростання індексів розвитку економіки знань – основа ефективного управління освітніми проектами інформатизації. Управління проектами та розвиток виробництва : зб. наук. пр. Луганськ : СНУ ім. В. Даля, 2012. № 3 (43). С. 62–69.

5. Полотай О.І., Ноздріна Л.В. Дослідження передумов запровадження інноваційних освітніх проектів у ВНЗ. CD – ROM : ISBN 978-966-593-624-4. Міжнародна науково-практична конференція "Е-навчання у вищій школі – проблеми й перспективи" (INCEL–08) (м. Одеса, 13–15 травня 2008 р.). Одеса : NTU "KhPI", 2008. С. 1–6.

6. Полотай О.І. Напрями вдосконалення управління проектами запровадження дистанційного навчання у вищому навчальному закладі. Управління розвитком складних систем. 2013. Вип. 13. С. 40–44.

7. Стародуб А.Н., Полотай О.І. Захист контенту електронного курсу навчання (на прикладі віртуального університету ЛДУБЖД). Зб. тез доп. II Міжвуз. наук.-практ. конф. студентів і курсантів "Захист інформації в інформаційно-комунікаційних системах" (м. Львів, 24 листопада 2017 р.). Львів : ЛДУБЖД, 2017. С. 57–58.

УДК 004.91:657.62:640.420

ВАЖЛИВІСТЬ ПРОВЕДЕННЯ IT-АУДИТІВ В УМОВАХ СЬОГОДЕННЯ

Ігор Порожній, Віктор Отенко, Наталія Лужецька

Національний університет "Львівська політехніка", м. Львів, Україна

Анотація. *Описано важливість проведення IT-аудитів. Зазначено основну перевагу IT-аудиту. Наведено основні причини необхідності професійного аудиту IT.*

Ключові слова: *IT-аудит, аудит інформаційних технологій, переваги IT-аудиту.*

Abstract. *The importance of conducting IT-audits is described. The main advantage of IT-audit is indicated. The main reasons for the need for a professional IT-audit are listed.*

Keywords: *IT-audit, information technology audit, advantages of IT-audit.*

Для співіснування будь-якої організації і її конкурування з іншими підприємствами, необхідно інвестувати в "інформаційні технології" [1], які забезпечують доступність, цілісність і конфіденційність даних [2].

Багато організацій витрачають значні суми на інформаційні технології, ігноруючи ризики кібербезпеки. Для зниження цих ризиків купівлі одного рішення недостатньо. Необхідно вибудовувати стратегію кіберзахисту за допомогою створення комплексу внутрішніх IT-контролів, які враховують не тільки технічні аспекти, але й організаційні та адміністративні.

Огляд інформаційної безпеки вкрай важливий для будь-якого бізнесу, оскільки він дає змогу переконатися в тому, що IT-системи й процеси працюють паралельно із системами та процесами інформаційної безпеки, з огляду на кращі світові практики та стандарти для мінімізації ризиків бізнесу [3, 5].

Зі зростанням внутрішніх і зовнішніх загроз, IT-система бізнесу може піддаватися потенційним ризикам. Це одна з основних причин здійснення інвестицій в послуги IT-аудиту.

IT-аудит охоплює широкий спектр IT-процесів та інфраструктуру зв'язку, включно з веб-сервісами, програмними додатками, системами безпеки, операційними системами, клієнт-серверними мережами тощо. Аудит, зазвичай, призначений для виявлення в IT-системі організації помилок, які роблять її уразливою для атаки.

Однією з основних переваг аудиту IT є те, що він може допомогти впоратися з ризиками, пов'язаними з доступністю, цілісністю і конфіденційністю процесів та інфраструктури інформаційних технологій, а також може підвищити надійність, дієвість та ефективність IT-систем, охоплюю-

чи широкий спектр загроз шляхом регулярного виявлення і оцінки ризиків в організації [1].

Впровадження в організації професійного аудиту ІТ дозволяє [4]:

1) удосконалити стратегічне планування.

Кожен бізнес має чітко сформовані стратегічні цілі та бачення подальшого розвитку. Для того, щоб розробити найефективнішу платформу для успішного досягнення цілей, важливо визначити слабкі місця та максимально передбачити потенційні проблеми від самого початку. Сильні та слабкі сторони, виявлені в процесі аудиту ІТ, дозволяють краще спланувати майбутню технічну складову.

2) виявити слабкі місця у кіберзахисті.

Оцінка ризиків кібербезпеки є однією з ключових складових ІТ-аудиту. Вона дозволяє виявити вразливі місця в ІТ-інфраструктурі, внутрішні та зовнішні загрози, які можуть негативно впливати на продуктивність та запропонувати шляхи усунення цих проблем.

3) виявити необхідність підвищення кваліфікації співробітників.

До процесу ІТ-аудиту важливо залучати співробітників організації. Це гарний спосіб черговий раз нагадати всім працівникам про важливість кібербезпеки та ефективного використання робочих інструментів. Також інформація, отримана у процесі спілкування, може бути використана для виявлення кіберзагроз, з якими стикається команда організації. Наприклад, електронні листи з фішингом.

4) оптимально здійснити перерозподіл технічних ресурсів.

В залежності від робочих задач, різні підрозділи компанії мають різні потреби у технологіях, а тому завжди існує ризик неефективного розподілу технічних ресурсів. Наприклад, деяким співробітникам потрібно більше мережевих ресурсів, ніж іншим. Аудит усієї системи допоможе побачити цілісну картину та оптимізувати використання наявних технічних можливостей.

5) передбачити можливі потенційні проблеми.

ІТ-аудит допомагає визначити, чи відповідають технічні ресурси компанії її стратегічним цілям. Якщо компанія планує масштабування бізнесу, її ІТ-складова має бути готова до збільшення навантаження. Важливо чітко розуміти, які інструменти та програми будуть потрібні у майбутньому для забезпечення безперебійного функціонування. Виявлення факторів, які можуть негативно вплинути на продуктивність і розробка стратегії уникнення ризиків, допоможе бізнесу стрімко розвиватися та залишатися на крок попереду конкурентів.

Після проведення ІТ-аудиту, ІТ-відділ організації отримує чітке уявлення про дії, які необхідно зробити для усунення, зниження або простого прийняття ризиків як частини операційного середовища.

Інформаційні джерела

1. Важливість IT-аудиту та його переваги. [Електронний ресурс]. – Режим доступу: https://irpin.com.ua/mistyani-informuyut/trashed.html.
2. Лист НБУ №24-112/365 "Щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України". [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v0365500-11.
3. IT-аудит. [Електронний ресурс]. – Режим доступу: https://www.bdo.ua/uk-ua/services-2/audit/it-audit.
4. Причини потреби IT-аудиту. [Електронний ресурс]. – Режим доступу: https://www.kliksolutions.com.ua/great-info/5-prychyn-chomu-vam-potriben-audyt-it-infrastruktury/.
5. The Importance of IT Audit in an Organisation. [Електронний ресурс]. – Режим доступу: https://www.careersinaudit.com/article/the-importance-of-it-audit-in-an-organisation/.

УДК 004.77; 004.9; 34.342

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ КРАЇНИ

Людмила Рибальченко

Дніпропетровський державний університет внутрішніх справ, м. Дніпро, Україна

Анотація. *Infosec або інформаційна безпека, яка стоїть на захисті цифрових даних, є складовою не одного підприємства, а усієї країни. Інформаційна безпека у XXI столітті стала невід'ємною частиною для будь-якого маленького чи великого бізнесу, який кожен день пов'язує свою діяльність з IT-технологіями та цифровим світом. Комп'ютерна безпека в сфері IT – це не тільки захист персональних даних, але й управління ризиками на підприємстві, забезпечення інформаційної цілісності та гарантії для власних співробітників, це є безпека усього населення держави.*

Ключові слова*: інформаційна безпека, захист персональних даних, інформаційні технології, економічна безпека, кіберзлочини.*

Abstract. *Infosec, or information security, which stands for the protection of digital data, is a component not of one enterprise, but of the entire country. Information security in the 21st century has become an integral part for any small or large business that connects its activities with IT technologies and the digital world every day. Computer security in the field of IT is not only the protection of personal data, but also risk management at the enterprise, ensuring information integrity and guarantees for its own employees, this is the safety of the entire population of the state.*

Keywords*: information security, personal data protection, information technologies, economic security, cybercrimes.*

Загальна мета будь-якої інформаційної безпеки організації – це надання для власних користувачів захищеного простору для роботи та безпека власних ресурсів підприємства в ІТ-середовищі від вторгнення несанкціонованих суб'єктів. Особливо це важливим є під час захисту економічних інтересів підприємства, оскільки, в першу чергу, несанкціоновані дії осіб направлені на спричинення економічної шкоди задля неможливості подальшого ведення підприємницької діяльності шляхом виведення капіталовкладень.

В умовах стрімкого розвитку цифрових технологій, підвищення рівня обізнаності населення в комп'ютерних технологіях та безперебійного доступу до Інтернету питання економічної безпеки підприємства в умовах глобалізації стає дедалі актуальніше. В сучасних умовах інформаційна безпека є складовою економічної безпеки підприємства на якій, в свою чергу, базується підвищення чи спад національної економіки [1].

Як правило, уся діяльність світової спільноти направлена на виявлення основних кіберзагроз, оцінки їх можливого впливу та розроблення методів і засобів захисту інформаційно-комунікаційної системи підприємства.

Все більше видань та центрів дослідження присвячують свої праці вивченню ризиків для підприємства на глобальному рівні. На прикладі дослідження корпоративних ризиків "Барометр ризиків Allianz" зазначено, що одним з головних ризиків, який призводить до перешкод у виробництві ланцюгів поставок є *кібератаки*, *технічні збої* та *геополітична нестабільність*. Стурбованість діяльності ведення бізнесу є потребує ефективних рішень щодо створення безпеки та протидії будь-яким наслідкам чи проявам кібернебезпеки.

Однак, на жаль, не всі підприємці дійсно усвідомлюють небезпеку, яку може в собі нести кіберпростір. Серед причин кібератак на інформаційні ресурси підприємств є недостатні капіталовкладення на створення надійних систем захисту від кіберзлочинства.

З кожним роком питання захисту інформаційних технологій тільки набирає своєї значущості. До актуальних проблем, які розповсюдженні серед опитуваних респондентів, можна віднести захист конфіденційних даних від цільових атак, забезпечення безперебійної роботи критично важливих систем.

Отже, виходячи з цього, можна зрозуміти, що питання інформаційної безпеки має виключне пріоритетне місце у діяльності менеджерів великих національних і світових компаній, керівників середнього і малого бізнесу. Можливість зовнішнього і внутрішнього втручання в інформаційну систему підприємства може вплинути не тільки на цикл виробництва та його

успішність, але й поставити під питання взагалі діяльність. Негативними наслідками у діяльності підприємства може бути:

− збої у функціонуванні систем управління технологічними та управлінськими процесами;

− розголошення відомостей, що становлять комерційну та інші види таємниць;

− порушення достовірності фінансової звітності;

− несанкціонований доступ до бази даних підприємств;

− викривлення публічної інформації тощо.

Результатом такої злочинної діяльності може стати падіння конкурентоспроможності підприємства, фінансові та виробничі втрати, нанесення шкоди підприємству, а й загроза життєдіяльності усієї держави. Загроза порушення функціонування інформаційної системи викликаної проникненням через кіберпростір може спотворити, знищити або спровокувати несанкціоноване використання бази даних. У певних ситуаціях повне ігнорування питання захисту інформації може привести до повної втрати бізнесу.

Таким чином, важливими напрямами захисту та зменшення злочинного впливу кібератак на підприємство та державу можуть бути такі:

− підвищення інформаційної безпеки підприємств через забезпечення високого рівня інформованості персоналу щодо роботи з даними, захисту даних від можливих загроз;

− створення захисту корпоративних даних через застосування методів шифрування;

− обмеження доступу та захист конфіденційних даних від несанкціонованого доступу [2].

Створення високого рівня інформаційної безпеки є важливим як на рівні підприємств, установ чи організацій так і на державному рівні. Дотримання основних таких принципів, як цілісність даних, конфіденційність та захист від несанкціонованого доступу є значно ефективними для стримування та протидії загрозам кібератак у кіберпросторі.

Інформаційні джерела

1. Rybalchenko, L., Ryzhkov, E., Ohrimenco, S. (2021). Modeling economic component of national security. Scientific journal “Philosophy, Economics and Law Review”, 1(1), С. 25−36.

2. Rybalchenko, L., Ryzhkov, E., Ohrimenco, S. (2021). Economic crime and its impact on the security of the state. Scientific journal “Philosophy, Economics and Law Review”, 1(2), С. 67−80.

УДК 004.056.5

ПІДВИЩЕННЯ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ В ОРГАНІЗАЦІЇ

Любомир Романчук, Олег Гарасимчук

Національний університет "Львівська політехніка", м. Львів, Україна

Анотація. *Розглянуто інтенсивне впровадження пристроїв Інтернету Речей в сучасних організаціях. Проаналізовані основні уразливості таких пристроїв. Запропоновані базові підходи, які дозволять правильно захистити пристрої Інтернету Речей.*

Ключові слова: *інтернет речей, уразливість, безпека.*

Abstract. *Intensive introduction of devices of the Internet of Things is considered in modern organizations. The basic to vulnerability of such devices are analysed. Offered base approaches that will allow correctly to protect the devices of the Internet of Things.*

Keywords: *Internet of Things, vulnerability, security.*

На поточному етапі розвитку технологій практично неможливо уявити наше життя без Інтернету Речей (IoT), оскільки він став невід'ємною частиною будь-якого корпоративного середовища. В організаціях може використовуватися один або навіть кілька типів технологій, які базуються на Інтернеті Речей. Більшість із них потрапляє під одну з трьох основних категорій:

1. Технології розумного будинку: ліфти, термостати, системи опалення, вентиляції та кондиціювання, а також розумного освітлення.

2. Технології розумного офісу: зчитувачі маркерів (значків), камери та маршрутизатори.

3. Інтелектуальні бізнес-технології: обладнання для проведення конференцій, Smart-TV, розумні дошки, віртуальні помічники.

Хоча ці пристрої, безумовно, корисні, вони також підвищують уразливість ретельно продуманої мережі через існуючі фактори ризику.

Як показав інцидент із Verkada, IoT-пристрої мають кілька внутрішніх недоліків. Ось кілька основних причин, з яких дана технологія становить великий ризик безпеки:

– відсутність стандартизації створює плутанину серед пристроїв. Пристроям Інтернету Речей не вистачає стандартизованих інтерфейсів та систем управління. Отже, практично неможливо розробити єдину політику безпеки, оновити програмне забезпечення або навіть встановити надій-

ні паролі без спеціального ухвалення рішення щодо забезпечення безпеки Інтернету Речей.

– на відміну від звичного програмного забезпечення, такого як Windows або Android, IoT-пристрої не розроблені з урахуванням вимог безпеки. Зазвичай їх необхідно спеціально обслуговувати і керувати ними.

– застаріла архітектура коду, що не підтримується, прошивка, програмне забезпечення (ПЗ). Наприклад, до половини всіх підключених пристроїв, таких як апарати УЗД та МРТ, працюють на базі застарілих операційних систем. Отже, для них недоступна підтримка безпеки або інших виправлень.

– кожен додатковий пристрій, що використовує мережу, збільшує можливість атаки. Хоча цю вразливість легко контролювати при роботі з більшістю звичних нам пристроїв (телефони, комп’ютери), у випадку з пристроями Інтернету Речей ситуація не така вже і проста.

– медичні пристрої, у свою чергу, не мають сертифікації з кібербезпеки, що іронічно, враховуючи, що безпека медичного обладнання є однією з найсерйозніших областей регулювання у всьому світі.

– більшість організацій, як правило, використовує множину різноманітного обладнання. Через це практично неможливо вручну провести інвентаризацію кожного окремого пристрою та відстежити, що він робить, що підвищує їх вразливість до різноманітних загроз та атак зі сторони зловмисників.

Через ці причини хакери отримують можливість легко зламувати IoT-пристрої в будь-яких установах і завдавати шкоди: викрадати персональні дані клієнтів або співробітників, інтелектуальну власність, контролювати мережу з метою отримання викупу.

Можна застосувати наступні базові підходи, які дозволять правильно захистити пристрої Інтернету Речей.

– *Реалізувати покращення паролів*. Більшість організацій використовують слабкі заводські паролі, які за замовчуванням встановлені на IoT-пристроях. І справа тут не в лінощах, часто буває дуже важко змінити пароль через величезну кількість пристроїв Інтернету Речей, якими доводиться керувати. Також варто враховувати і той факт, що інтерфейс таких пристроїв зазвичай не до кінця зрозумілий чи складний у використанні. У кращому випадку кожен пристрій повинен мати свій унікальний пароль. Тоді, навіть якщо зловмисник отримає доступ до одного пристрою, збитки будуть значно нижчими.

– *Виконати всі можливі оновлення*. Обладнання Інтернету Речей з'являються і замінюються новими досить швидко, що пов'язує розробників оновлень. Тим не менш, підтримка програмного забезпечення або вбудованого програмного забезпечення для певних пристроїв як правило не завжди доступна. Після гучних кібератак із використанням Інтернету Речей ця проблема стала особливо актуальною, і деякі виробники стали оптимізувати та випускати актуальні оновлення.

– *Рух в напрямку до нульової довіри*. Сьогодні багато організацій починають застосовувати модель "Нульової Довіри", яка базується на принципі "Ніколи не довіряй. Завжди перевіряй". Кожен користувач перед тим, як отримати доступ, перевіряється за принципом "найменших привілеїв", тобто отримує доступ лише для досягнення узгоджених бізнес-цілей. Дана модель здатна запобігти атакам на сусідні пристрої навіть у тому випадку, якщо зловмисник зламає мережу. Сегментація мережі – це ще один спосіб заблокувати переміщення ненадійних користувачів або зловмисників через мережу в компанії.

IoT-пристрої, безумовно, є одним із найслабших елементів мережі. Чим більша поверхня атаки (оскільки пристрої Інтернету Речей можуть розташовуватися в громадських місцях, у віддалених областях і т.д.), чим більше пристроїв підключено до системи, тим більше у хакерів можливостей для вторгнення. Ключовий момент полягає в тому, що компаніям необхідно зрозуміти слабкі сторони безпеки IoT для прийняття рішень щодо захисту даних в організації, а виробникам обладнання та іншим хто дотичний до даної технології необхідно серйозно працювати над збільшенням захищеності як пристроїв так і каналів передачі даних в мережі Інтернету Речей.

Інформаційні джерела

1. Жураковський Б.Ю., Зенів І.О. Технології інтернету речей. Навчальний посібник для студ. спеціальності 126 "Інформаційні системи та технології", спеціалізація "Інформаційне забезпечення робототехнічних систем". Київ: КПІ ім. Ігоря Сікорського. 2021. 271 с.

2. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of threats to the Internet of things. IEEE Commun. Surv. Tutor. 2018, 21, 1636–1675.

3. Wei Z., Yan Jia., Anni P., Yuqing Z., PengL.,"The Effect of IoT New Features on Securityand Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved", IEEE Internet of Things Journal, June 2018.

4. Alrawi O., Lever C., Antonakakis M., Monrose F. SoK: Security Evaluation of Home-Based IoT Deployments – 2018.

УДК 004.891.3:004.3

СТВОРЕННЯ БЕЗПЕЧНОГО ЖИТТЄВОГО ЦИКЛУ РОЗРОБЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Дмитро Савуляк[1] ,Орест Полотай[2], Андрій Лагун[2]

[1]Національний університет "Львівська політехніка", м. Львів, Україна
[2]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *Описано особливості безпечного життєвого циклу розробки програмного забезпечення SSDLC. Розглянуто переваги SSDLC. Показано забезпечення SSDLC. Перераховано основні етапи SSDLC.*

Ключові слова: *розроблення програмного забезпечення, безпека програмного забезпечення.*

Abstract. *Features of the secure life cycle of SSDLC software development are described. Considered the benefits of SSDLC. SSDLC provisioning is shown. The main stages of SSDLC are listed.*

Keywords: *software development, software security.*

Безпека є важливою частиною будь-якої програми, яка включає важливі функції. Це може бути настільки просто, як захистити базу даних від атак зловмисників, або настільки ж складно, як впровадити автоматичний захист та виявлення шахрайства.

Оскільки засоби розробки програмного забезпечення продовжують вдосконалюватися, це відкриває нові можливості для створення досконалішого та складнішого програмного забезпечення з безпрецедентною швидкістю. Написання коду є лише одним із елементів процесу доставки програмного забезпечення, але планування, управління та спілкування однаково важливі. Саме тут життєвий цикл розробки програмного забезпечення (SDLC) відіграє важливу роль.

Безпека повинна застосовуватися на кожному етапі SDLC і має бути в центрі уваги розробників, коли вони розробляють програмне забезпечення згідно вимог.

Усунення проблем безпеки на ранніх етапах розробки, дозволяє зменшити загальну вартість володіння програмами. Пізнє виявлення проблеми в SDLC може призвести до 100-кратного збільшення вартості робіт, необхідних для вирішення цієї проблеми.

Мета безпечного SDLC полягає не в повній ліквідації традиційних перевірок безпеки, таких як тести на проникнення (penetration tests), а в тому, щоб включити безпеку в сферу обов'язків розробників і надати їм можливість створювати безпечні програми з самого початку.

Secure SDLC є найкращим прикладом того, що відомо як ініціатива "shift-left", яка підтримує інтеграцію перевірок безпеки якомога раніше в SDLC.

Це все допомагає командам розробників у належному порядку планувати випуски, полегшуючи виявлення та вирішення проблем, які можуть вплинути на дату випуску нової версії. Це, безсумнівно, краще ніж отримати неприємний сюрприз після розгортання програми в робочому стані. Таким чином, SSDLC підтримує підтримку релізу на шляху.

Забезпечення безпечного SDLC вимагає зосередження як на тому, як працює програма, так і на тому, як розробники перетворюють вимоги в код програми. Під час розробки програми безпека має бути на першому місці. Це може вимагати суттєвих змін у командах, а також автоматизованих процесів і перевірок на кожному етапі розробки програмного забезпечення.

Хоча розробку програмного забезпечення часто вважають простим написанням коду, насправді існує кілька етапів життєвого циклу розробки програмного забезпечення до моменту доставки, з яких програмування є лише одним. Ці етапи включають збір вимог, аналіз, проєктування, розробку, тестування, розгортання та обслуговування.

1. Збір вимог.

Перш ніж приступати до будь-якого проєкту розробки програмного забезпечення, важливо зрозуміти, що насправді потрібно зробити. Нерідко команди розробників та їхні клієнти мають різні уявлення про те, як має виглядати кінцевий результат.

2. Аналіз.

Після вивчення проблеми, яку необхідно вирішити на етапі збору вимог, групі розробників доручається визначити найкращий підхід для досягнення рішення.

3. Дизайн.

Існує багато різних аспектів, які слід брати до уваги під час створення програмного рішення, крім самого коду, включаючи інфраструктуру, архітектуру системи та інтерфейс користувача.

4. Розробка.

Створення самого програмного забезпечення – це щось на зразок мистецтва, яке виходить за рамки простого написання коду. Код працює в інфраструктурі, яка зазвичай включає сервери та мережу або платформу керованого хостингу (наприклад, Azure App Service або AWS Elastic Beanstalk).

5. Тестування.

Розробки програмного забезпечення недостатньо. Перш ніж програмне забезпечення буде доставлено клієнту, команда повинна переконатися, що воно відповідає меті та що з ним немає значних проблем.

6. Розгортання.

Коли програмне забезпечення буде перевірено на відповідність цілям, настав час передати його клієнту.

7. Технічне обслуговування.

Хоча розгортання часто розглядається як останній крок у постачанні частини програмного забезпечення, насправді це лише початок корисного життя цього програмного забезпечення.

Отже, SDLC важливий, тому що безпека програми важлива. Розробники повинні знати про потенційні проблеми безпеки на кожному кроці процесу. Це вимагає інтеграції безпеки у SDLC способами, які раніше не були потрібні. Таким чином, наявність надійного та безпечного процесу SDLC має вирішальне значення для того, щоб програма не піддавалася атакам хакерів та інших зловмисних користувачів.

Інформаційні джерела

1. Agile Project Management for Dummies, 2nd Edition, Layton, M. C., Ostermiller, S. J.

2. Agile Application Security: Enabling Security in a Continuous Delivery Pipeline 1st Edition

3. Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems 1st Edition

4. Kukharska N.,Lagun A., Polotai O. The steganographic approach to data protection using arnold algorithm and the pixel-value differencing method. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020. 2020. Article ID 9204108. P. 174–177.

5. Полотай О.І., Деменко В. Особливості оцінки ризиків загроз інформаційної безпеки. Зб. наук. праць XI Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів “Проблеми та перспективи забезпечення безпеки життєдіяльності” (м. Львів, 24 березня 2016 р.). Львів : ЛДУБЖД, 2016. С. 204–205.

УДК: 004.056.5

ІГРОВІ І СИСТЕМНІ МОДЕЛІ МЕТОДІВ РОЗВ'ЯЗАННЯ КОНФЛІКТНИХ СИТУАЦІЙ ТА КІБЕРБЕЗПЕКА ІНФРАСТРУКТУРИ В УМОВАХ АКТИВНИХ ЗАГРОЗ

Любомир Сікора[1], Валентина Кунченко – Харченко[2], Володимир Сабат[3]

[1]Національний університет "Львівська політехніка", м. Львів, Україна
[2]Кафедра робототехнічних і телекомунікаційних систем та кібербезпеки Черкаського державного технологічного університету, м. Черкаси, Україна
[3]Кафедра інформаційних мультимедійних технологій Української академії друкарства, м. Львів, Україна

Анотація. *У роботі розглядається підхід до розв'язання конфліктних ситуацій в технологічних структурах. Сучасний модельний підхід в побудові алгоритмів і стратегії дозволяє на єдиній методологічній базі розв'язувати задачі аналізу і синтезу систем різної природи орієнтованих на досягнення певних цілей.*

Ключові слова: *конфлікт, система, цілі, системологія, кібербезпека, атаки, інфраструктура.*

Abstract. *The paper considers an approach to resolving conflict situations in technological structures. The modern model approach in the construction of algorithms and strategies allows solving the problems of analysis and synthesis of systems of different nature oriented towards achieving certain goals on a single methodological basis.*

Keywords: *conflict, system, goals, systemology, cyber security, attacks, infrastructure.*

Розв'язання проблеми конфлікту і кризису у внутрішній структурі систем і при взаємодії з зовнішніми об'єктами як учасниками ігри, є актуальною задачею і розв'язати її засобами теорії ігор, дослідження операцій, лінійного програмування не вдається через неповноту понятійного апарату та інструментальних засобів. Системологія цілеспрямованих структур дозволяє обєднати, на основі інформаційно – ресурсної концепції, широку гаму прикладних конструктивних теорій: інформатику, теорію систем, комп'ютерних технологій, системи САПР для аналізу динаміки ігрових систем при визначеній структурі їх організації. Причому аналіз проблемної ситуації спирається на базу знань, побудовану з класів концептуальних моделей систем, сигналів, алгоритмів обробки і оцінювання, алгоритмів прийняття рішень і цільових стратегій, а функціональним об'єднуючим поняттям буде виділення парадигми: "Цільовий простір – формувач образу динамічної ситуації в цільовому просторі – текучий стан системи – цільовий стан – стратегія досягнення цілей – ціна ресурсів – стратегія розв'язання кризи" [1].

В системології цілеспрямованих структур сформовано понятійний апарат розв'язку конфліктних задач, при чому конфлікт трактується як підвищенні витрати або недостача матеріальних, енергетичних, інформаційних, фінансових ресурсів для досягнення цілі при дії збурень або як розвал структури системи при неузгоджених стратегіях гри. Причому методологія розв'язання конфлікту базується на оцінці етапу моменту входження в кризисну ситуацію траєкторії стану, відображену в цільовому просторі системи, а індикатором буде відхилення її стану від прогнозованого. Кризи є стимулом до зміни стратегії поведінки, структури системи, параметричної адаптації і оптимізації як першого етапу стратегії виходу з кризи, зміна або корекція цілі і відповідно стратегій поведінки і структури, як другого етапу.

Методи розв'язання конфлікту при заданій проблемній ситуації в технологічній системі базується на оцінці ситуації відносно цілі. Проводиться оцінка проблемної ситуації в момент входження в окіл цілі траєкторії стану динамічної системи інтелектуальної ієрархічною системою спостереження, при чому формуються критерії та індикатори степеня наближення до цілі (ресурсні, інформаційні). Вибір моделі стратегії розв'язання проблемної ситуації в цільовому просторі системи базується на оцінці внутрішніх і зовнішніх ресурсів і їх достатності для досягнення цілі, уточнення класу локальних стратегій для прийняття рішень, прогнозу траєкторії майбутнього стану. При недостатності внутрішніх матеріальних та інформаційних ресурсів формується принцип взаємин з зовнішніми структурами і критерії оцінки вартості необхідних ресурсів. Розв'язання кризисної ситуації відбувається за рахунок мобілізації ресурсів і зміни локальної стратегії поведінки або в глобальному синтез нової моделі сситеми і її структурна адаптація або режим нового структурування і циклічне повторення позицій в системі з оптимізованою структурою і стратегією, вихід на рівень динамічної рівноваги при зміні внутрішніх і зовнішніх впливів [3].

При невиконанні умов методу розв'язання проблемної ситуації на рівні адаптації і оптимізації, відбувається перехід на слідуючий рівень, де кризисна ситуація є критерієм повноти і непротирічивості приміненої інформаційної та логіко – когнітивної методології, побудови стратегії розв'язання проблемних задач. Основною задачею для розв'язання кризису або конфлікту є синтез цілеспрямованої системи для формування нових знань на основі даних, що отримані у попередній грі і врахуванням нових концепцій і парадигм, які знімають проблему протирічивості методології, синтез на їх основі цільових стратегій подолання кризисів, що знову приводять до глобального аналізу динаміки ресурсів в оновлених структурах (рис. 1).

Позначення: $\{F_S, F_R, F_E\}$ – фактори ресурсно – структурного впливу атаки, F_{KI} – фактор когнітивно – інформаційного впливу, $\{R_m, R_F, R_{KP}\}$ – ресурси матеріальні, енергетичні, когнітивні персоналу, α_{rd} – допустимий

ризик, $\alpha_r(A)$ – ризику від атак, ІІАСУ – інтегрована система з ієрархією, $\langle IS \otimes AS \rangle$ – гра інфраструктури з атакуючою системою, $PR(A)$ – причини комплексної атаки на інфраструктуру.

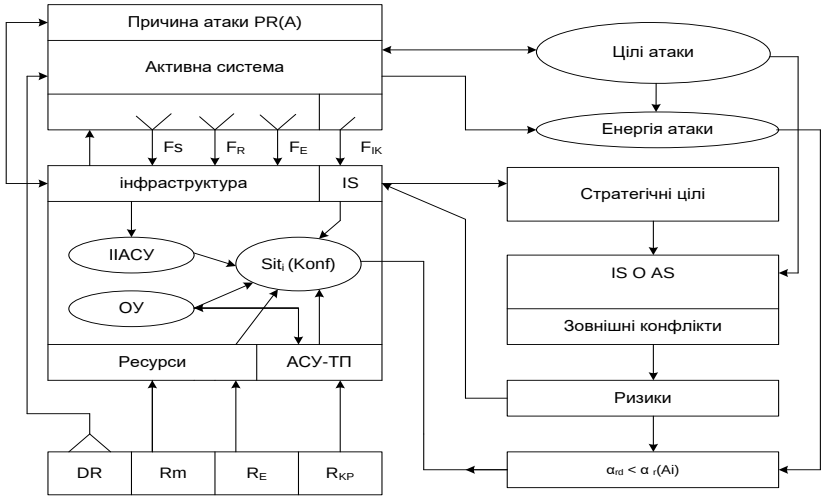


Рисунок 1 – Ігрова модель конфліктної ситуації

Оптимізація режиму системи базується на формуванні функціоналу якості, компонентами якого будуть індикаторні функції економії ресурсів, термінального часу досягнення цілі та точності підтримання функціонального стану. Оптимізація алгоритмів обробки сигналів і стратегій управління базується на вивченні статистичних характеристик траєкторій сигналів і завад, забезпечення їх робастності та інформаційній адекватності. Проблема розвязку конфліктних ситуацій в технологічних структурах вимагає для свого розв'язання створення комплексу концептуальних моделей систем, стратегій управління і оптимізації. А також проведення на їх основі синтезу програмного і комп'ютерного забезпечення, вибору методів протидії атакам як на ресурсному, структурному так і когнітивно – інтелектуальному рівнях підготовки персоналу.

Інформаційні джерела

1. Чикрий А. А. Конфликтно управляемые процессы. – К.: Наук. Думка. 1992 – 384 с.

2. Белман Р. Процессы регулирования с адаптацией. – К.: Наук. Думка. 1964. – 247 с.

3. Васильев В. Иммитационное управление неопределенными огбъктами – К.: Інститут Кібер. АН України. 1986. – 210 с.

УДК: 004.056.5

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ IT – ПРОЄКТІВ З ВИКОРИСТАННЯМ МЕТОДИКИ DEVSECOPS

Денис Смик, Ростислав Ткачук, Андрій Івануса

Кафедра управління інформаційною безпекою
Львіського державного університету безпеки життєдіяльності,
м. Львів, Україна

Анотація. *В роботі розглянуто методологію систематизації існуючих засобів захисту програмного забезпечення, що забезпечують взаємодію команди розробників та фахівців із захисту інформації в межах одного життєвого циклу розробки. Приведена методологія DevSecOps дозволяє максимально оптимізувати процес розроблення та захисту програмного забезпечення.*

Ключові слова: *IT – проєкт, інформаційна безпека, DevOps, DevSecOps.*

Abstract. *The methodology of systematization of the existing means of protection of the software providing interaction of a team of developers and experts on protection of the information within one life cycle of development is considered. The given DevSecOps methodology makes it possible to optimize the software development and protection process as much as possible.*

Keywords: *IT project, information security, DevOps, DevSecOps.*

Методологія розроблення та захисту програмного забезпечення в межах DevSecOps змінила підхід до забезпечення безпеки з реактивного на проактивний, а також підкреслює важливість забезпечення безпеки на всіх рівнях організації. DevSecOps передбачає забезпечення безпеки в розробленні додатків починаючи з початкових стадій і до самого завершення, а також включає в себе автоматизацію деяких шлюзів безпеки з метою запобігання уповільненню робочого процесу DevOps. Вибір правильних інструментів для безперервної інтеграції безпеки сприятиме досягненню поставлених цілей те дасть можливість зекономити час.

Сучасні інструменти автоматизації допомогли підприємствам впровадити більш гнучкі методи розробки, а також відіграли важливу роль у розробленні нових заходів безпеки. Для ефективного захисту DevOps потрібні не тільки нові інструменти, а й зміни на підприємстві процесів DevOps, для пришвидшення інтегрування роботи груп фахівців з безпеки з іншими спеціалістами, що призведе до покращення якості продукту.

DevSecOps – одна з найважливіших тенденцій DevOps. Це підхід до безпеки операцій, що дозволяє використовувати принципи і кращі практики DevOps для забезпечення кращої, швидкості більш безпечної доставки програмного забезпечення. По суті, це означає, що всі вимоги безпеки з

самого початку кодифіковані, а контроль безпеки і розробка здійснюються паралельно, причому безпеку намагаються впровадити в кожну частину процесу agile-розробки. Завдяки цьому DevSecOps може знизити витрати пов'язані з виправленням недоліків безпеки [1].

DevSecOps – це вбудована безпека, а не безпека, яка функціонує як периметр навколо програм та даних. Якщо безпека залишається в кінці конвеєра розробки, організації, що застосовують DevOps, можуть повернутися до довгих циклів розробки, яких вони намагалися уникати в першу чергу.

Зазвичай, методики для оптимізації процесів розроблення програмного забезпечення націлені виключно на підвищення ефективності всередині команди, але в DevSecOps мова йде про застосування автоматизованих інструментів для гарантування комплексного захисту. Варто зазначити, що кожна з доступних методик стрімко прискорює роботу, жертвуючи при цьому безпекою інфраструктури. Більшість компаній може бути не готова до такого стрибка підвищення вимог якості в даній сфері. Саме тому, подальший розвиток DevOps порушив питання інформаційної безпеки. Прискорення роботи команд-розробників створило безперервний потік оновлюваних функцій, а також постійний потік даних з боку сервісів, користувачів та інших додатків [2, 4]. Розгортання коду має відбуватися частіше і завершуватися за менший час. Коротший час циклу є ознакою оптимізованих процесів, в той час як більш тривалий час може бути ознакою того, що необхідно переглянути свої кращі практики або інструменти кодування.

Стратегією DevSecOps є визначення толерантності до ризиків та проведення аналізу ризику. Автоматизація повторюваних завдань є ключовим чинником DevSecOps, оскільки запуск ручних перевірок безпеки в конвеєрі може вимагати багато часу.

DevSecOps дозволяє організації застосовувати попереджуючий підхід до безпеки. Це спонукає розробників програмного забезпечення інтегрувати безпеку в свої повсякденні зусилля. У той же час групи безпеки можуть працювати з розробниками програмного забезпечення, щоб допомогти організації виявити і усунути вразливості безпеки, перш ніж вони вийдуть зпід контролю. DevSecOps змінює безпеку з реактивної на проактивну, а також підкреслює важливість безпеки на всіх рівнях організації, і уповноважує співробітників служби безпеки приймати рішення, які мають позитивний вплив на їхній бізнес [3].

Таким чином, DevSecOps, як концепція і практика, весь час розвивається, зі збільшенням кількості організацій, які впроваджують DevSecOps як рішення для їх проблеми безпеки. Попит на DevSecOps збільшиться в організаціях всіх розмірів і у всіх галузях. У міру того, як все більше організацій шукають способи виявлення та виправлення проблем безпеки на

ранніх етапах процесу розробки програмного забезпечення, попит на інструменти для підтримки DevSecOps відповідно збільшуватиметься.

Підприємство, яке впроваджує інструменти DevSecOps отримує стійку конкурентну перевагу. Надаючи розробникам програмного забезпечення і командам безпеки зручні та ефективні інструменти DevSecOps, підприємство розвиває культуру співпраці, спілкування, прозорості та відкритості. В результаті організація створює середовище, в якій розробники та групи безпеки постійно удосконалюються.

Переваги, які DevSecOps приносить компаніям це – зниження витрат, збільшення швидкості доставки, швидкості відновлення, відповідність в масштабі і пошуку загроз. Сукупний ефект цих переваг – це підвищення ділової репутації та більш плавна бізнес-модель. DevSecOps успішно видалить бар'єри між DevOpsi Security, яка заважають їм працювати як єдине ціле. DevSecOps матиме можливість знаходити і виправляти проблеми безпеки на початку процесу розробки, тим самим значно скорочуючи витрати, пов'язані з їх виявленням і виправленням. Важливо включити гарантування безпеки в життєвий цикл розробки Agile. Завдяки DevSecOps розробники можуть краще зрозуміти критичність уразливостей, які існують у їхньому коді, і виправити ці вразливості, надаючи швидкі, але безпечніші продукти або рішення. Оскільки підхід DevSecOps автоматизований, тому команді розробників більше не потрібно записувати правила безпеки у свій код. DevSecOps знижує ризик перенапруження даних, оптимально застосовуючи ресурси.

Висновки. Розглянута методологія систематизації існуючих засобів захисту програмного забезпечення, яка дозволяє забезпечити взаємодію команди розробників та фахівців із захисту інформації в межах одного життєвого циклу розробки. Такий підхід дозволяє значно скоротити час циклу розробки програмного забезпечення та оптимізувати його захист.

Інформаційні джерела

1. IT – безпека [Електронний ресурс] Режим доступу до ресурсу: https://astwellsoft.com/uk/blog/software-security.html.

2. Чим займається DevOps – інженер [Електронний ресурс] // Режим доступу до ресурсу: https://vc.ru/hr/51144-kto-takoy-devops-inzhener-i-chem-on-zanimaetsya.

3. Що таке DevSecOps [Електронний ресурс] // Режим доступу до ресурсу: https://itfb.com.ua/chto-takoe-devsecops/

4. Britvin A., Alrawashdeh J. H., Tkachuk R. Client-Server System for Parsing Data from Web Pages. Advances in Cyber-Physical Systems Volume 7, Number 1, 2022. P. 8–13.

УДК 005.5:004.056

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА НА ОСНОВІ СУЧАСНИХ ТЕХНОЛОГІЙ АУТЕНТИФІКАЦІЇ

Наталія Фединець

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *Проблема управління інформаційною безпекою підприємства завжди була актуальною. Особливо це стосується середнього та великого бізнесу, що успішно функціонує та реалізовує бізнесові проєкти, ідеї та рішення яких є цікавими для інших гравців на ринку відповідної сфери.*

Ключові слова: *інформаційна безпека, аутентифікація, технології, захист інформації.*

Abstract. *The problem of information security management of the enterprise has always been relevant. This especially applies to medium and large businesses that successfully operate and implement business projects, the ideas and solutions of which are interesting for other market players in the relevant field.*

Keywords: *information security, authentication, technologies, information protection.*

Вкрай важливим є питання інформаційної безпеки в умовах війни, оскільки посилюються зовнішні загрози, зростає рівень конкуренції та соціальної напруги в суспільстві. Перед керівництвом підприємств гостро постає завдання у швидкому та надійному захисті інформації, чіткому визначенні осіб, що мають до неї доступ.

Аутентифікація – встановлення достовірності користувача, що представив ідентифікатор або перевірка того, що особа або пристрій, що повідомив ідентифікатор є дійсно тим, за кого воно себе видає.

Основними критеріями вибору певної технології аутентифікації є вартість, надійність, швидкість реалізації, можливість вирішення поставлених завдань.

Зазвичай користувачі ідентифікуються за ідентифікатором користувача плюс фактором аутентифікації знань, наприклад паролем. Однак, оскільки паролі за своєю суттю є незахищеними, аутентифікація перейшла та розвинулася до таких технологій:

1. Біометрія пристрою. Біометрія пристрою відноситься до біометричних технологій, вбудованих у сам кінцевий пристрій. Сьогодні це в основному камери для розпізнавання обличчя та сканери відбитків пальців, доступні в мобільних пристроях, ноутбуках і настільних комп’ютерах. Ці

технології аутентифікації, незважаючи на те, що вони відносно безпечні, надійні та зрілі, все ще не досконалі. Часто присутні помилки розпізнавання обличчя або відбитків пальців на своїх пристроях через різні обставини, що призводить до повернення до пароля або іншого способу аутентифікації. Незважаючи на ці недоліки безпеки, біометрія пристрою, здається, буде провідним варіантом заміни пароля в майбутньому. Фахівці з корпоративної безпеки та IT-спеціалісти повинні звернути пильну увагу на різноманітні зміни в API та технологіях, випущених кожним постачальником, особливо Apple на iOS і MacOS, Microsoft і Google.

2. Голосова біометрія. Голосова біометрія демонструє цікавий потенціал, особливо в голосових каналах, таких як кол-центр і служби голосової допомоги. Існують різні алгоритми для виявлення та аутентифікації голосу залежно від каналу та використання. Спроби поширити голосову біометрику на онлайн-канали поки що не мали великого успіху, однак вона має багато важливих переваг перед біометрією пристрою. Одним із прикладів цього є голосова аутентифікація за допомогою централізованого голосового друку. Оскільки ця та інші голосові біометричні технології стануть більш зрілими, вони відкриють нові можливості для організацій для захисту своїх користувачів на багатьох пристроях і каналах.

3. Апаратні ключі безпеки. Ключі безпеки стосуються апаратного пристрою, який можна використовувати як “щось, що у вас є” для аутентифікації користувача в різних онлайн-сервісах. Це апаратне забезпечення може бути спеціальним, як-от рішення від YubiKey і Google Titan, або може бути просто самим мобільним пристроєм користувача. Залежно від технології апаратне забезпечення може підключатися за допомогою USB, BLE, NFC, WiFi або одноразових кодів (TOTP), які користувач копіює з пристрою. Ми бачимо деякі цікаві зміни щодо ключів безпеки із запровадженням протоколів FIDO2 CTAP, які стандартизують зв’язок між ключами безпеки та іншими пристроями, такими як настільні комп’ютери та ноутбуки. Ми також відзначаємо значний прогрес у тому, що мобільні пристрої стають безпечними глобальними аутентифікаторами.

4. Поведінкова біометрія Те, як ви взаємодієте з пристроєм, від того, як його тримаєте, до того, як ви друкуєте чи рухаєте мишею, було важливою областю досліджень протягом багатьох років. Завдяки появі більшої кількості датчиків на кінцевих пристроях у поєднанні з прогресом у профілюванні та алгоритмах машинного навчання ці технології аутентифікації стають дедалі точнішими. Хоча вони все ще не здатні повністю аутентифікувати користувача з високим ступенем точності, їх можна використовувати для виявлення підозрілих подій і поведінки, які потребують осо-

бливої уваги з боку команд безпеки. Ми очікуємо, що ця технологія продовжуватиметься та вдосконалюватиметься в майбутньому, щоб забезпечити більше випадків використання.

5. Технології ідентифікації пристрою Кожен пристрій має набір характеристик і ідентифікаторів, які можна використовувати для однозначної ідентифікації без будь-якої взаємодії з користувачем. Якщо відомо, що пристрій раніше був пов'язаний з користувачем, це не може гарантувати дійсність користувача, однак його можна використовувати як надійний елемент для багатофакторної аутентифікації в поєднанні з чимось, наприклад, скануванням обличчя чи відбитків пальців. Технології ідентифікації пристрою покладаються на елементи, надані виробниками пристроїв і постачальниками програм веб-браузера. Вони можуть змінюватися з багатьох причин через нормативні вимоги та прогрес у технологіях кінцевих пристроїв. Оператори мобільних мереж також надають інформацію, яку можна об'єднати, щоб забезпечити додаткові рівні ідентифікації, що ще більше підвищує довіру пристрою та, зрештою, користувача.

В багатьох випадках традиційної аутентифікації користувачів вже недостатньо й виникає потреб в аутентифікації, що передбачає додаткові рівні захисту: 2FA (передбачає введення від користувача коду підтвердження, отриманого у текстовому повідомленні на попередньо зареєстрованому мобільному телефоні чи мобільному пристрої, або код, згенерований програмою аутентифікації), MFA (вимагає від користувачів автентифікації за допомогою кількох факторів автентифікації, включаючи біометричний фактор, такий як відбиток пальця або розпізнавання обличчя, фактор володіння, як брелок безпеки; або маркер, створений програмою автентифікації).

Аутентифікація дозволяє організаціям підтримувати безпеку своїх мереж, дозволяючи лише аутентифікованим користувачам або процесам отримувати доступ до їхніх захищених ресурсів. Це може включати комп'ютерні системи, мережі, бази даних, веб-сайти та інші мережеві програми чи служби.

Інформаційні джерела

1. IT-портал компанії "Інфосистеми джет". URL: http://www.jetinfo.ru/stati/biometricheskie-metody-autentifikatsii.

2. Резнік Н., Полотай О.І. Методи біометричної аутентифікації та загрози їх зламу. Матеріали XIII Міжнародної науково-практичної конференції молодих вчених, курсантів та студентів. "Проблеми та перспективи розвитку системи безпеки життєдіяльності". С. 237−238.

УДК 004.056.5:005

ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Валентина Ящук, Ростислав Ткачук, Андрій Івануса

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *Розглянуто теоретичні, науково-методичні та організаційно-функціональні основи оцінювання ризиків кібербезпеки об'єктів критичної інфраструктури. Визначено сучасні підходи до оцінювання ризиків кібербезпеки об'єктів критичної інфраструктури. Наведено методичні підходи до формування концепції оцінювання ризиків кібербезпеки об'єктів критичної інфраструктури. Запропоновано етапи вирішення науково-практичної проблеми, пов'язаної з підвищенням рівня захисту інформаційних систем критичної інфраструктури шляхом розроблення методології забезпечення кібербезпеки об'єктів критичної інфраструктури.*

Ключові слова: *захист інформації, кібербезпека, оцінювання ризиків, комплексний ризик, об'єктивний ризик, суб'єктивний ризик, інформаційна система, управління ризиком.*

Abstract. *The theoretical, scientific-methodical, and organizational-functional bases of cyber security risk assessment of critical infrastructure objects are considered. Modern approaches to cyber security risk assessment of critical infrastructure facilities are defined. Methodical approaches to the formation of the concept of cyber security risk assessment of critical infrastructure objects are given. The stages of solving the scientific and practical problem associated with increasing the level of protection of information systems of critical infrastructure by developing a methodology for ensuring cyber security of critical infrastructure objects are proposed.*

Keywords: *information protection, cyber security, risk assessment, complex risk, objective risk, subjective risk, information system, risk management.*

Події останніх місяців в Україні і у світі показали нагальну необхідність забезпечення безпеки об'єктів критичної інфраструктури, особливо енергетичного сектору. Сьогодні, коли ворог завдає ракетних ударів по об'єктам критичної інфраструктури та атакує інформаційні системи об'єктів китичної інфраструктури, питання забезпечення безпеки об'єктів критичної інфраструктури шляхом оцінювання ризиків є актуальним.

Проводячи аналіз норм законодавства у сфері критичної інфраструктури, в тому числі Закону України "Про критичну інфраструктуру" [1], можна зазначити, що в цілому норми Закону спрямовані на впорядкування питань, пов'язаних з об'єктами КІ, та є першим кроком до розвитку зако-

нодавства у цій сфері. В той же час, більшість норм та механізмів, що передбачені цим Законом, – просто не працюють станом на сьогоднішній день. В першу чергу це відбувається через збройну агресію зі сторони російської федерації, під час якої уряд має більш пріоритетні задачі щодо забезпечення функціонування держави, у зв'язку з чим всі строки порушились. Закон набув чинності в середині червня 2022 року та не пройшов практичного застосування. Уповноважений орган у сфері ЗКІ, який повинен був бути створений ще в березні 2022 року, – "документально утворений" у липні поточного року, але реально не функціонує. Також не затверджені окремі порядки, які стосуються, зокрема, Реєстру та паспортизації об'єктів КІ.

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" забезпечення кібербезпеки об'єкту критичної інфраструктури, у тому числі енергетичного сектору, досягається створенням системи управління інформаційною безпекою (СУІБ) у відповідності до міжнародного стандарту ISO/IEC 27001:2013 або створенням комплексної системи захисту інформації (КСЗІ) у відповідності до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах". Одним з основних етапів побудови СУІБ, КСЗІ є створення системи управління ризиками.

Не зважаючи на значну кількість підходів та методів до вирішення проблеми оцінювання ризиків кібербезпеки інформаційних систем, у тому числі об'єктів критичної інфраструктури, а також програмні продукти управлінням такими ризиками проблема залишається актуальною не тільки для України, але і для всієї світової спільноти. Існуючі методи не дають можливості вирішувати задачі, пов'язані із можливістю визначення суми ризиків, що дало би змогу здійснення кількісного оцінювання ризику проєкту у цілому або вибраного напряму розвитку процесу, а також обчислення комплексного ризику, що враховував би вплив людського чиннику. Оцінювання ризику кібербезпеки здійснюється з достатньою точністю, як правило, на підставі статистичних даних кіберінцидентів за певний проміжок часу. Разом з тим, за низкою ризиків, зокрема, об'єктів критичної інфраструктури, такі дані відсутні, а величина збитків занижена.

Вирішення науково-практичної проблеми, пов'язаної з підвищенням рівня захисту інформаційних систем критичної інфраструктури шляхом розроблення методології забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури ми пропонуємо здійснювати за такими етапами:

– проаналізовати сучасні методи, методики, методології оцінювання ризиків кібербезпеки інформаційних систем, у тому числі об'єктів крити-

чної інфраструктури, а також програмні продукти управлінням такими ризиками.

– обґрунтувати поняття комплексного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури, здійснити його змістовну інтерпретацію та розглянути основні властивості.

– розробити методи обчислення сумарного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури з використанням значення максимальних наслідків.

– розробити методологію оцінювання ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури з використанням розроблених методів.

– розробити структурні рішення обчислювальних систем для розрахунку сумарного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури з використанням розроблених методів.

– розробити алгоритмічне та програмне забезпечення обчислювальних систем для розрахунку сумарного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури з використанням розроблених методів.

– провести експериментальні дослідження з метою підтвердження теоретичних положень та практичних розробок дослідження.

Отже, реалізація запропонованих етапів підвищення рівня захисту інформаційних систем критичної інфраструктури надасть можливість побудувати ефективну систему оцінювання ризиків кібербезпеки об’єктів критичної інфраструктури. Розроблені та обґрунтовані практичні рекомендації з побудови та функціонування систем оцінювання ризиків кібербезпеки об’єктів критичної інфраструктури сприятимуть підвищенню ефективності управління кібербезпекою об’єктів критичної інфраструктури.

Інформаційні джерела

1. Закон України “Про критичну інфраструктуру” (1882-IX від 16.11.2021), який набрав чинності 15.12.2021, але почав діяти тільки 15.06.2022 [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1882-20#n20

2. Постанова КМУ від 09.10.2020 № 1109 “Деякі питання об’єктів критичної інфраструктури”, зі змінами від 29.12.2021, яка набула чинності 31.12.2021 [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

3. Драб Ю. Основні підходи до побудови системи управління інформаційною безпекою / Ю. Драб, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С. 29–32).

Напрям 2

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

УДК 654.071

СИСТЕМА ЕЛЕКТРОННОГО УПРАВЛІННЯ НА ОСНОВІ БЛОКЧЕЙНУ

Святослав Василишин, Іван Опірський

Кафедра захисту інформації Національного університету "Львівська політехніка", м. Львів, Україна

Анотація. *В реаліях захисту інформації у кіберпросторі існує багато засобів та підходів до безпеки урядового, бізнес та приватних секторів, одним з яких цілком ймовірно можуть стати системи побудовані на основі блокчейну. В даних тезах пропонується система безпеки урядових, приватних та бізнес секторів побудованих з використанням даної технології.*

Ключові слова*: блокчейн, захист інформації, конфіденційність, вузли зв'язку.*

Abstract. *In the realities of protecting information in cyberspace, there are many means and approaches to the security of the government, business, and private sectors, one of which is likely to be systems built on the basis of blockchain. These theses propose a security system for government, private and business sectors built using this technology.*

Keywords: *blockchain, information protection, privacy, communication nodes.*

Система електронного урядування на основі блокчейну. Запропонована структура електронного урядування на основі блокчейну проілюстрована на рис. 1. На цьому малюнку двонаправлена стрілка УДУ показує взаємодію, що відбувається між державними департаментами та організаціями, що дозволяє здійснювати одноранговий (p2p) обмін (широкомовлення) та перевірку даних, які надаються особами. Подвійна стрілка УДГ позначає обмін інформацією між громадянами та урядом, як-от заповнення податкових форм, свідоцтв про шлюб, дозволів на ведення бізнесу, свідоцтв про народження, віз або паспортів. Подвійна стрілка УДБ вказує на обмін інформацією, як-от електронні закупівлі, податкові та страхові форми, а також електронні аукціони між державними та діловими організаціями (підприємствами) як головне джерело економічного зростання [1].

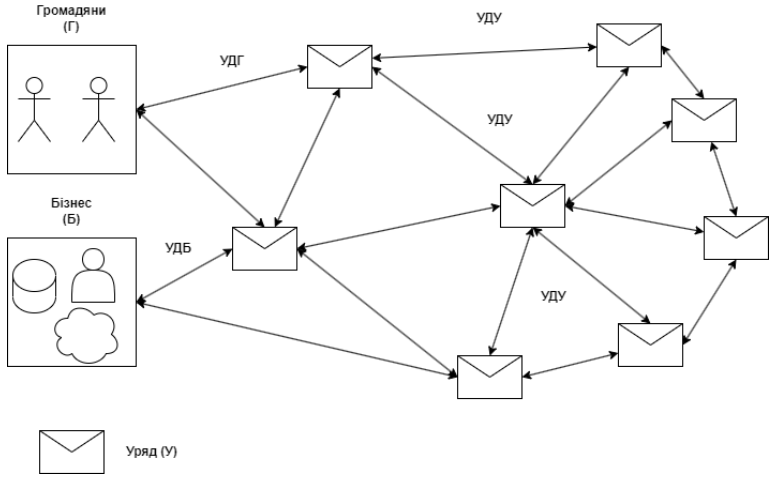


Рисунок 1 – Пропонована мережа електронного урядування на основі блокчейну

Приєднання будь-якого нового вузла електронного уряду (У) або вузла користувача (Г або Б) до мережі блокчейн перевіряється однорангови-ми користувачами в мережі, і токени електронного уряду призначаються для налаштування його мережевого вузла, що призводить до отримання дозволу [2].

Створення нового вузла. Процес реєстрації нового вузла в запропонованій мережі електронного уряду підсумовано в “Алгоритмі 1”. Будь-який відділ електронного урядування може приєднатися до мережі блокчейн, налаштувавши повний мережевий вузол, тоді як інші користувачі можуть налаштувати лише легкі вузли [3].

Алгоритм 1: Додавання нової гілки в мережу електронного уряду

If (the request is from government) then
Create a node n;
else
Create a lightweight node n;
end if
$(K_{pub}, K_{pr}) \leftarrow$ generateKeys( );
Addr $\leftarrow$ createBlockchainAdress() + (K_{pub}, K_{pr});
Walt $\leftarrow$ createBlockchainWallet() + (K_{pub}, K_{pr});
safetyStorePrivateKey( );
Addr $\leftarrow$ Addr + tokens;
$\alpha \leftarrow$ selectDelegate (S);
for each m $\in$ $\{S - \alpha\}$ do

distrReg (m,n);
end for
n ← verNewNODE( );

Генерація нового блока. Кожен блок створюється одним активним свідком, який вибирається випадковим чином більшістю однорангових користувачів зі списку активних делегатів [4].

Алгоритм 2: створення та додавання нового блоку в блокчейн

initialize an empty set of transaction G = { };
$\alpha \leftarrow$ WitnesElect(S);
while treansaction$_t$ < T_c do
for each m $\in$ {S − α} do
G ← G + GetTransactionfromNode(m);
end for
end while
$b_{m+1} \leftarrow$ createBlock(b_m, G);
for each m $\in$ {S − α} do
signBlock(b_{m+1}, m);
end for
B′ ← B + b_{m+1};
for each m $\in$ S do
distributeBlockchain (B′, m);
end for

Висновки. У цьому документі пропонується структура електронного урядування, яка може забезпечити безпеку та конфіденційність у державному секторі за допомогою технології блокчейн. Теоретичний і якісний аналіз безпеки та конфіденційності фреймворку показує, що криптографія, незмінність і децентралізоване управління та контроль, запропоновані технологією блокчейн, можуть забезпечити необхідну безпеку та конфіденційність у системах електронного урядування.

Інформаційні джерела

1. Lafaille, C. What is Blockchain Technology. 2018. Available online: https://www.investinblockchain.com/ what-is-blockchain-technology/

2. CoinDesk. How Bitcoin Mining Works. 2018. Available online: https://www.coindesk.com/information/ how-bitcoin-mining-works

3. Tuwiner, J. What Is Bitcoin Mining and How Does It Work? 2019. Available online: https://www. buybitcoinworldwide.com/mining/

4. Gautham. PoW Blockchain Could Be Vulnerable to Balance Attack. 2017. Available online: https: //www.newsbtc.com/2017/01/29/pow-blockchain-balance-attack/

УДК 004.722

ПІДВИЩЕННЯ РІВНІ БЕЗПЕКИ КОРИСТУВАЦЬКИХ ДАНИХ ЗА ДОПОМОГОЮ ПЕРЕХОДУ НА HTTPS ПРОТОКОЛ ПЕРЕДАЧІ ДАНИХ

Віктор Дебре, Данило Гречишкін

Харківський Націолнальний університет радіоелектроніки
м. Харків, Україна

Анотація. *В цих тезах розглядається важливість переходу від HTTP протоколу до HTTPS та яким чином шифрувальні механізми SSL і TLS допомагають у розвитку безпечного інтернету та захисту конфіденційних даних користувачів від зловмисників.*

Ключові слова: *HTTPS протокол, SSL, TLS, веб-безпека, cookie, інтернет порти.*

Abstract. *These theses consider the importance of the transition from the HTTP protocol to HTTPS and how SSL and TLS encryption mechanisms help in the development of a secure Internet and the protection of confidential user data from attackers.*

Keywords: *HTTPS protocol, SSL, TLS, web security, cookie, net port.*

In connection with the expansion of the global Internet network, the risks associated with the protection of information are constantly increasing. Accordingly, new ways of ensuring security in networks and data transmission are created. One of the main ways of transferring information over networks is the HTTP protocol [1], but it is not secure and cannot provide the confidentiality of transmitted data. For enlarge the level of protection, the HTTPS protocol was created, which protects HTTP data transmission through encrypted transport mechanisms SSL and TLS [2]. It is in effecting to malformed attacks based on eavesdropping on the network connection sniffer and man-in-the-middle attacks, due to provided encryption tools are used and the server's certificate is verified and trusted.

Moreover, we have to know which system sends the information and which system receives it. HTTP protocol covers these particular problems and relies on the following parts that can be divided into three groups:

− servers − it is the main service provider, that can store and process data

− clients – end service consumers for example sending requests,

− proxies – intermediate nodes that cover transport services.

The binary fragmentation mechanism in HTTP/2 is designed so that no changes need to be made to existing APIs and configuration files: it is quite

transparent to the user. HTTP requests and responses have a close structure. They consist of:

1. A start line that describes the request, or status. This is always a single string.

2. A random set of HTTP headers defining the request or describing the message body.

3. An empty string indicating that all meta information has been sent.

4. An arbitrary body containing the data sent with the request (for example, the contents of an HTML form) or the document sent in response. The presence and size of the body are determined by the start string and HTTP headers.

HTTPS is not a separate data transfer protocol but is an extension of the HTTP protocol with an encryption add-on. On HTTP, all sensitive data shared between computer applications over a network is not encrypted but in plain text. As such, users' passwords, names, addresses, and credit card numbers become vulnerable to man-in-the-middle attacks.

In HTTP:

− URL begins with "http://"

− It uses port 80 for communication.

− No encryption.

Therefore, HTTPS is a combination of Hyper Text Transfer Protocol and Secure Sockets Layer. SSL is currently the most frequently used method for providing security for Internet communications, so HTTPS is a more secure way for transmitting and receiving information across the Internet. This kind of communication is used for accessing those websites where security is required. Banking websites and payment gateway are some great examples where HTTPS protocols are used.

On the other hand in HTTPS:

− URL begins with "https://"

− It uses port 443 for communication.

− Encryption is present.

However, the HTTPS transaction is a bit slow and time is required for decrypting and encrypting.

By default, browsers communicate with the server via HTTP. To perform migration to HTTPS, the site owner must install an SSL certificate on the hosting. When a site owner installs an SSL certificate, a lock icon appears in the browser's address bar and HTTP changes to HTTPS. This literally means that this site is safe for inputting some personal information. If HTTPS traffic is intercepted, the message will appear as a set of random characters. You need a

key to read it. Nevertheless, they are specially made so long that even the most powerful computer would take years of continuous work to pick them up.

Online businesses, corporations, and even governments rely on the Security Socket Layer called SSL 256-bit. It is a standard specification for SSL encryption. It means that the key, which is used to decrypt the messages that have been previously encrypted, is a string of 256 characters, all ones, and zeros. Taking into account that each element of the 256 digits string has two possibilities (1 or 0), there are 2256 possible combinations [3].

For instance, given a high-performance GPU computer that can perform approximately 2 billion calculations per second. As long as provided a 1 billion computers similar to mentioned previously, which all are connected in a massive parallel and efficient system, only then they are capable of performing 2e18 computations per second.

By estimation, this number of years for calculation that must pass appears per year group of 1 billion computers can perform estimably: 2e18 * 31 556 952 = 6.3113904e25. Consequently, the result is 25 rank number. Now we can make further calculations to see how many years we need to crack the SSL code.2^225 / 6.3113904^25 = 9.1732631e50 years.

Despite the billions of years needed to go over every possible combination, 1 billion GPUs will require electricity from 150 nuclear power plants. That covers 30% of the world's nuclear energy system capacity. In addition, it will contribute to the expenses of trillions of dollars. With this in mind, cracking an SSL encryption is impossible with current computing power thresholds. It would take slightly longer for somebody to try to do this and would require very much resources and finances. Since hackers fail to break the SSL Certificates, they will explore vulnerabilities in other areas that are related to the SSL Certificates. The most common server backdoor problems that are related to SSL Certificates are Heartbleed, BREACH and BEAST. These allow attackers to bypass the strength of an SSL Certificate.

Інформаційні джерела

1. James Ll. What does 'https' mean, and why is it necessary? URL: https://www.quora.com/What-does-https-mean-and-why-is-it-necessary (дата звернення: 04.09.2022)

2. What is SSL? URL: https://www.ssl.com/faqs/faq-what-is-ssl/ (дата звернення: 23.09.2022)

3. Baptiste Assmann Benchmarking SSL Performance URL: https://www.haproxy.com/blog/benchmarking_ssl_performance/ (дата звернення: 15.10.2022)

УДК 004.457

СТВОРЕННЯ ФІКТИВНИХ ВЕБСЕРВЕРІВ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ КІБЕРБЕЗПЕКИ

Тетяна Лаврик, Дмитро Кіхтенко

Сумський державний університет, м. Суми, Україна

Анотація. *Розробники і тестувальники для вирішення завдань кібербезпеки використовують різний набір програмних засобів та інструментів. Створення програмного засобу для імітації вебсерверів дозволяє оптимізувати реалізацію певних завдань кібербезпеки за критерієм часу.*

Ключові слова: *кібербезпека, вебсервер, імітація вебсерверу, програмна утиліта.*

Abstract. *Developers and testers use a variety of software tools to solve cyber security tasks. The creation of a software tool for imitation web servers allows them to optimize the implementation of certain cyber security tasks according to the time criterion.*

Keywords: *cyber security, web server, web server imitation, utility program.*

Розробники програмного забезпечення, тестувальники, системні адміністратори у процесі розробки, розгортання чи налаштування деяких компонентів, що працюють на основі протоколу HTTP/HTTPS і виступають у ролі клієнта, стикаються із завданням перевірки коректності їх роботи. Особливо це стосується додатків, що побудовано на базі мікросервісної архітектури. Здебільшого подібний проєкт складається з кількох мікросервісів, кожен з яких взаємодіє з іншим за HTTPS протоколом. Кожен елемент такого проєкту розробляється окремо від інших, але для підсистем-адаптерів (*частин мікросервісу, що виконують функцію зв'язку з іншими мікросервісами*) необхідно зімітувати інші залежні мікросервіси для тестування і відлагодження адаптерів. З цією метою у переважній більшості випадків здійснюється повне розгортання усіх компонентів проєкту, на що витрачається значна частина часу і потужностей обчислювальної техніки. Тобто, виникає необхідність для перевірки працездатності та відлагодження компонентів проєкту використовувати такий програмний засіб, який зміг би імітувати будь-яку кількість веб-серверів.

Для проведення тестів на проникнення фахівці досить часто використовують у своїй практиці атаки типу "людина посередині" для HTTP/HTTPS серверів. Такий підхід має на меті створення копії вебсерверу і підміни ним оригінального ресурсу для прослуховування HTTP-запитів на випадок конфіденційної інформації. Для тестувальника на проникнення у цьому випадку важливим критерієм залишається час здійснення атаки: чим меншим буде витрачений час, тим меншою буде ймовірність того, що "зловмисника" буде помічено в системі. Для реалізації зазначеного завдання кібербезпеки основним критерієм також є час, витрачений на

створення такого серверу-посередника, що імітує оригінальний сервер. Як і в першому прикладі, постає необхідність програмного засобу для імітації вебсерверів.

Проведена пошукова та аналітична робота щодо наявних програмних рішень, які хоча б частково дозволяли вирішувати поставлену проблему, свідчить, що такі інструменти існують лише для завдання здійснення атаки типу “людина посередині”. Програмних рішень для відлагодження чи тестування під час створення нового продукту не виявлено.

Атаки типу “людина по середині” для протоколів HTTP/HTTPS реалізуються різними способами. Загалом можна виділити два основних сценарії здійснення такої атаки: 1) використання прослуховування незахищеного каналу зв’язку; 2) використання додаткового вебсерверу посередника між цільовими клієнтом і сервером. Перший спосіб реалізується за допомогою поширених утиліт Wireshark, tcpdump, mitmproxy, але лише для тих випадків, коли канал зв’язку не шифрується, тобто для протоколу HTTP. Другий спосіб застосовується як для HTTP-протоколу, так і для HTTPS-протоколу. Реалізується він за допомогою створення і розгортання вебдодатку посередника, який для клієнта видає себе за легітимний ресурс, а для цільового сервера видає себе за легітимного клієнта. Сервер-посередник повинен частково або повністю копіювати оригінальний сервер.

Слід враховувати, що створити програмний засіб для імітації вебсерверів можна для двох принципово різних бекенд вебдодатків: вебсайтів та вебсервісів.

Для копіювання вебсервісів необхідно використовувати фреймворки побудови вебсервісів: Spring Frawework, Python Jango, ASP.NET core, Laravel, Ruby on Rails, Fiber framework, Python Flask, Python FastApi тощо. Використовуючи одну із цих технологій, залежно від цільового сервісу, фахівець з кібербезпеки може розробити потрібний йому сервер для імітації цільового ресурсу і перехоплення запитів користувачів. Ці інструменти надають можливість реалізації будь-якого функціоналу і через це вимагають багато часу. Програмних рішень для автоматизації процесу копіювання вебсервісу не виявлено, оскільки це доволі складна задача, що залежить від архітектури цільового додатку.

Для копіювання вебсайтів можна використовувати звичайні сервери для побудови вебсайтів і їх запуску: Apache HTTP Server, NGINX тощо. Копіювання самого ресурсу можна виконати вручну, що також займає достатньо часу. А оскільки вебсайти є більш простими додатками і зазвичай мають шаблонну архітектуру, для них існує інструмент для автоматизації копіювання – утиліта HTTrack. HTTrack – це консольний інструмент, що дозволяє рекурсивно скопіювати всі файли вебсайту зі збереженням дерева каталогів. Із локальної копії даних можна запустити вебсайт, отримавши таким чином повну його копію.

Створити універсальний інструмент для здійснення копіювання і вебсайтів, і веб-серверів будь-якої складності є достатньо складним і трудомістким завданням, оскільки програмний засіб має містити потужний функціонал. У порівнянні з таким рішенням вважаємо, що найпростішим у реалізації буде створення копії ресурсу за допомогою стандартних вебтехнологій розробки.

Проведений аналіз дозволив сформулювати завдання для подальшої програмної реалізації. Заплановано створити програмну утиліту для імітації вебсерверів з такими функціональними можливостями:

− приймає HTTP-запити, імітуючи вебсервер;

− формує HTTP-відповіді на HTTP-запити, імітуючи вебсервер;

− прослуховує декілька різних сокетів HTTP серверу;

− підтримує протоколи HTTP і HTTPS;

− має налаштування SSL сертифікату;

− здійснює за допомогою конфігурації користувача імітацію будь-якої вебсерверної технології;

− дозволяє налаштовувати коди відповіді, заголовків й тіла відповіді для кожного окремого запиту за критерієм директорії запиту (мапінгу);

− показує або зберігає метод, URL, параметри, заголовки й тіло HTTP запитів.

УДК 122.2

ВИКОРИСТАННЯ МЕХАНІЗМІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АУТЕНТИФІКАЦІЇ ВАНТАЖНИХ ЗАЛІЗНИЧНИХ ВАГОНІВ

В. Пашук, І. Жуковицький

Дніпровський інститут інфраструктури та транспорту Українського державного університету науки і технологій, м. Дніпро, Україна

Анотація. *Раніше використовувалися інтелектуальні технології транспортних процесів, які містять ряд елементів автоматичного збору даних про умови транспортування, моделювання процесів у порівнянні з шаблонами або регламентами, розпізнавання надзвичайних ситуацій або умов і можливостей їх виникнення, прогнозування транспортних систем і транспортування. планування.*

Зараз для завдання розпізнавання номерів вантажних вагонів найкраще підходить механізм використання згорткових нейронних мереж (CNN).

Ключові слова*: аутентифікація, ідентифікація, штучний інтелект, автоматизація, нейронні мережі, згорткові нейронні мережі, піксель, шар, зображення, CNN.*

Abstract. *Previously, intelligent technologies of transportation processes were used, which contain a number of elements of automatic data collection on transportation conditions, process modeling, compared to templates or regulations, recognition of emergencies or conditions and opportunities for their occurrence, forecasting transport systems and transportation planning.*

Now, for the task of recognizing freight car numbers, the mechanism of using convolutional neural networks (CNN) is best suited.

Keywords: *authentication, identification, artificial intelligence, automation, neural networks, convolutional neural networks, pixel, layer, image, CNN.*

На даний момент в системах залізничного транспорту потребується ідентифікація номерів вантажних вагонів, що дозволяє оперативно отримувати інформацію про параметри (номер, тип та ін.) вагонів, локомотивів та іншого рухомого складу в реальному режимі часу. Завдяки цьому стає можливим впровадження нових концепцій системи технічного обслуговування та ремонту. При цьому існує ряд недоліків та проблем:

– ненадійне зчитування на забрудненому номері вагону рухомого складу;

– несприятливі погодні умови;

– слабке або нечітке освітлення прожекторів у темну годину доби;

– недостатньо потужна робота датчиків та відеоадаптерів під час безпосереднього зчитування номера вагону.

Зупинимося на проблемах стеження за рухом вантажів: відстеження товарів передбачає в будь-який час в режимі "реального часу" можливість отримання інформації про стан транспортних засобів, що перевозять товари та/або про становище самих товарів або їх контейнерів, а також про умови перевезення. Моніторинг має логічний зв'язок з попередженням аварій.

Раніше застосовувалися інтелектуальні технології процесів перевезень, які містять ряд елементів автоматичного збору даних про умови перевезень, моделюванні процесів, порівняно з шаблонами або ж з нормативами, розпізнавання позаштатних ситуацій або умов і можливостей їх виникнення, прогнозування станів транспортних систем і планування перевезень та ін.

Зараз же для задачі розпізнавання номерів вантажних вагонів найкраще підійде механізм використання згорткових нейронних мереж (CNN).

Згорткові нейронні мережі – це досить широкий клас архітектур, основна ідея яких полягає в тому, щоб перевикористати одні й ті ж частини нейронної мережі для роботи з різними маленькими, локальними ділянками входів.

Головна ідея, яка лежить в основі згорткових нейронних мереж, полягає в тому, що цілком достатньо локального осмислення зображення. Практична перевага згорткових нейронних мереж така, що, маючи декілька параметрів, можна значно скоротити час на навчання, а також об'єм даних, необхідних для навчання моделі.

Замість повнозв'язних мереж із вагами від кожного пікселя CNN має достатню кількість ваг, необхідних для перегляду невеликого фрагменту

зображення номера вагону. Це все одно що наприклад читати книгу з лупи: в кінцевому рахунку ви прочитуєте всю сторінку, але в будь-який момент дивитесь тільки на невеликий її фрагмент.

Привабливість цих мереж полягає в тому, що число використаних моделлю параметрів не залежить від розміру початкового зображення. Наприклад, можна виконати одну й ту саму згорткову нейронну мережу на зображення розміром 300×300, і число параметрів у згортковому шарі не зміниться.

Для роботи із зображеннями номерів вагонів будемо використовувати формат файлів bmp. Конвертувати в формат BMP можна файли наприклад таких форматів як JPG, PNG, GIF. Оскільки будь-яке зображення (в нашому випадку це зображення номера вагону), яке завантажується з графічного файлу, є набором кольорових точок (пікселів), то інформацію про кожну таку точку доцільно зберігати в бітах.

BMP – це формат файлу зображення, який не має нічого спільного з апаратними пристроями та широко використовується. Він використовує формат зберігання растрових зображень, за виключенням необов'язкової глибини зображення, не використовує ніякого другого стиснення, а тому BMP файл займає багато місця. Файлова структура BMP складається з чотирьох частин:

1) структура даних заголовка растрового файлу;
2) структура растрових інформаційних даних;
3) палітра;
4) растрові дані.

Інформаційні джерела

1. Скалозуб В. С. Економіко-математичне обгрунтування потреби в вагонних парках операторів залізничного транспорту / В. С. Скалозуб, М. С. Чередниченко // Вісник Дніпровського інституту інфраструктури та транспорту Українського державного університету науки і технологій. – Дніпропетровськ, 2010, Вип.31 – С. 240−248.

2. Modern Transport Telematics / Ed. Jerzy Mikulski // 11 th International Conference on Transport Systems Telematics, TST 2011. Katowice-Ustron, Poland, October 19-22, 2011. – 418 p.

3. Жуковицький І.В., Автоматизована ідентифікація рухомих одиниць та потяга в цілому / І.В. Жуковицький, О.Й. Єгоров // Інформаційно – керуючі системи на залізн. трансп. – 2012. – №6. – С.77−82.

4. Graves A., Schmidhuber J. Framewise Phoneme Classification with Bidirectional LSTM and Other Neural Network Architectures // Neural Networks, 2005, vol. 18, no. 5−6. – P. 602–610.

5. Graves A., Wayne G., Danihelka I. Neural Turing Machines // arXiv, 2014. http://arxiv.org/ abs/1410.5401.

6. Nishant Shukla. Machine Learning with Tensor Flow / N. Shukla, K. Fricklas // СПб.: Пітер, 2019. – 336 с.: іл. – (Серія "Бібліотека програміста").

7. Сайт Олександра Клімова: [Електронний ресурс]. URL: https://developer.alexanderklimov.ru/android/catshop/bitmap.php. (Дата звернення: 09.11.2022).

УДК 004:001.102-049.5

РОЛЬ ЦЕНТРІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЗАХИСТІ IT-ІНФРАСТРУКТУРИ КОМПАНІЙ

Станіслав Петько

Доцент кафедри міжнародного менеджменту
КНЕУ імені Вадима Гетьмана, м. Київ, Україна

Анотація. *Проаналізовано роль центрів інформаційної безпеки у захисті IT-інфраструктури компаній та їх основні принципи функціонування в корпоративному бізнес середовищі. Визначено мету створення центрів інформаційної безпеки, основні обов'язки та підходи персоналу щодо вирішення питань кібербезпеки компаній при потенційних загрозах. Доведено, що менеджери четвертого рівня таких центрів виступають основним елементом комунікації з іншими підрозділами компанії задля запобігання потенційної кіберзагрози та вчасної передачі інформації.*

Ключові слова: *центр інформаційної безпеки, ІКТ, компанія, IT-інфраструктура, кібербезпека.*

Abstract. *Analyzed the role of security operations center in the company's IT-infrastructure protection and its basic principles of functioning in the corporate business environment. Determined the main purpose of the security operations centers creating, main responsibilities and approaches company's staff of solving cybersecurity issues in case of potential threats.*

It has been proven that the fourth-level managers of such centers are going as the main element of communication with other divisions of the company in order to prevent a potential cyber threat and timely transfer of information.

Keywords*: security operation center, ICT, company, IT-infrastructure, cybersecurity.*

Із цифровізацією бізнес середовища й інтеграцією ІКТ у виробництво та сферу послуг набула потреба в захисті IT-інфраструктури компаній. Поява глобальної мережі Internet та подальший бурхливий розвиток ІКТ спричинило появу кіберзлочинності, хакерських атак, веб-підробок, вірусів, витоку корпоративної інформації, що заважає ефективно функціонувати компанії та знижує її конкурентоспроможність. І це не важливо до якої форми власності відноситься компанія – страждають від кіберзлочинності та атак як державні, так і приватні компанії.

Починаючи з 1970 рр. починають виникати центри інформаційної безпеки (SOC – security operations center) у США, а потім в Японії, Вели-

кобританії, Західній Німеччині, Республіці Корея, які з часом стали невід'ємними частинами будь-якої компанії або державної організації. За своєю суттю центр інформаційної безпеки – це група ІТ-фахівців, які моніторять 24/7 інформаційний стан компанії від потенційних внутрішніх та зовнішніх кіберзагроз. Мета створення центрів інформаційної безпеки полягає в своєчасному запобіганні потенційних кіберзагроз, підвищенні рівня захисту корпоративної мережі, зниження ризиків, а у випадку виникнення кіберзагрози – швидко її встановити та знищити.

Основні обов'язки фахівців таких центрів полягають у:

1) перевірці мереж компанії на вразливість та аналіз їх кібербезпеки;

2) постійному моніторингу та аналізі кіберзагроз;

3) фільтрації фейкових обробок та швидкій реакції на підтверджені кіберзагрози;

4) підготовці звітів щодо реального стану ІТ-інфраструктури компанії, кількості хакерських атак та ідентифікованих загроз.

Персонал центру інформаційної безпеки складається з аналітиків великих даних, криптографів, інженерів кібербезпеки та мережевої інженерії. Іншими словами, – це професіонали, які спеціально навчені відстежувати та керувати потенційними кіберзагрозами, допомагають створювати та підтримувати безпечну ІТ-архітектуру компанії. Вони не лише вміють користуватися різноманітними інструментами безпеки, але й знають конкретні дії, яких слід дотримуватися у разі зламу ІТ-інфраструктури компанії. Фахівці центру використовують низку інструментів, які збирають дані з мереж та апаратного обладнання, відстежують аномалії та сповіщають персонал компанії про потенційні кіберзагрози.

Більшість центрів інформаційної безпеки у глобальних ТНК використовують ієрархічний підхід до вирішення питань кібербезпеки, де фахівці центру розподіляються на основі їхнього набутого практичного досвіду. Класична команда центру може бути структурована наступним чином:

Рівень 1. "Гаряча лінія" служб реагування на потенційну загрозу. Спеціалісти з безпеки спостерігають за сповіщеннями та визначають терміновість кожного сповіщення та час для його переведення на рівень 2. Спеціалісти першого рівня мають змогу управляти засобами безпеки та надавати регулярні звіти.

Рівень 2. Персонал другого рівня більш досвідчений за колег з першого рівня, тому вони можуть швидше знайти загрозу та оцінити частину ІТ-

інфраструктури компанії, яка піддалася кібератаці. Фахівці дотримуються спеціальних процедур для усунення кіберзагрози, а також визначають знайдену загрозу для її подальшого дослідження.

Рівень 3. На даному рівні персонал складається з провідних експертів-аналітиків кібербезпеки, які активно шукають вразливі місця в мережі. Спеціалісти використовують широкий арсенал інструментів задля виявлення кіберзагрози, здійснюють карантинне діагностування слабких місць мережі задля розробки рекомендацій щодо підвищення рівня загальної кібербезпеки компанії.

Рівень 4. Четвертий рівень складається з топ-менеджерів з найбільшим досвідом роботи, яким підпорядковується уся команда центру інформаційної безпеки. Вони займаються HR-діяльністю, навчанням молодого персоналу, оцінюють індивідуальну та загальну продуктивність спеціалістів нижчих рівнів. Спеціалісти четвертого рівня втручаються в діяльність центру в самих кризових ситуаціях, який можна характеризувати як гармонічний взаємозв’язок центру з іншими підрозділами компанії.

Інформаційні джерела

1. Петько С. М. Вплив цифровізації державного апарату на розвиток демократії в Республіці Корея. Пріоритетні напрями досліджень в науковій та освітній діяльності: проблеми та перспективи: тези ІІ Всеукраїнської науково-практичної конференції з міжнародною участю (м. Рівне, 12–13 жовтня 2022). КЗВО “Рівненська медична академія. Рівне, 2022.

2. Петько С. М. Електронна комерція в цифровій екосистемі Республіки Кореї. *Економічний вісник Національного технічного університету України “Київський політехнічний інститут”*. 2022. № 23. С. 61−67. doi: https://doi.org/10.20535/2307-5651.23.2022.264630

3. Петько С. М. Республіка Корея в індексах цифрової економіки. Цифрова економіка та економічна безпека. 2022. № 1 (01). С. 66−73. doi: 66-73. https://doi.org/10.32782/dees.1-11

4. Петько С. М. Цифровий прорив Республіки Корея у сфері державного урядування. Економіка та суспільство.2022. № 42. doi: https://doi.org/10.32782/2524-0072/2022-42-47

5. Петько С. М. Цифровий техноглобалізм у становленні Республіки Корея на глобальному ринку напівпровідників. *Науковий вісник Полтавського університету економіки і торгівлі. Серія “Економіка”*. 2022. Випуск 1 (65). С. 91−99.

УДК 004.413

АНАЛІЗ ЗАГРОЗ ПРИВАТНОСТІ У ПРОГРАМАХМИТТЄВОГО ОБМІНУ ПОВІДОМЛЕННЯМИ НА ПРИКЛАДІ ПОПУЛЯРНХ МЕСЕНДЖЕРІВ В УКРАЇНІ

Василь Побережник, Іван Опірський

Національний Університет "Львівська політехніка", м. Львів, Україна

Анотація. *У даній роботі розглядаються загрози у програмах миттєвого обміну повідомленнями у контексті популярних, серед українських користувачів, месенджерів. Зокрема розглянуті як загальні загрози identity spoofing, загрози витоку персональної інформації та несанкціонованого доступу до приватних переписок.*

Ключові слова: *приватність, месенджери, спуфінг, витік даних, персональні дані.*

Abstract. *This work examines threats in instant messaging programs in the context of popular, among Ukrainian users, messengers. In particular, they are considered as general threats of identity spoofing, threats of leakage of personal information and unauthorized access to private messages.*

Keywords: *privacy, messengers, spoofing, data breach, personal data.*

На цей час різні месенджери стали невід'ємною частиною життя людей, наприклад Messenger був завантажений 1,3 мільярди разів, а WhatsApp має 2 мільярди завантажень[1]. За результатами Київського міжнародного інституту соціології найбільш розповсюдженим месенджером в Україні став Viber, яким користується 73,6% опитаних. Далі за популярністю йдуть Messenger – 42,7%, Telegram – 31,6% та WhatsApp – 25,3%[2]. Також, дані даного опитування демонструють, що послугами месенджерів користуються всі вікові групи населення країни, що дає змогу зробити висновок, що даними додатками користується переважна більшість населення України.

Загроза витоку персональних даних. Дані сервіси можуть збирати персональну інформацію про користувачів, наприклад месенджер Telegram [3] може збирати такі типи даних: номер телефону, електронну скриньку, інформацію про покупки, геолокацію, список контактів, фінансові дані, контактні дані, медіа-контент, ідентифікатори. WhatsApp [4] та Viber [5] на додачу до згаданих даних також збирає діагностичні дані та дані про використання. Втім, найбільше даних збирає Messenger [6]. Окрім згаданих вище, в його список входять: дані про здоров'я, історія пошуку, історія перегляду, чутливі дані та інше. Зберігання таких даних створює загрозу витоку даних з персональною інформацією, що і сталося у 2019 році, коли через вразливість Facebook (тепер Meta), якій належить Messenger, було викрадено персональні дані 533 мільйонів користувачів [7]. Іншим прикладом можливого витоку даних, є виявлені вразливості у WhatsApp у

2022 році [8], які дозволяла отримати зловмиснику доступ до віддаленого виконання коду, що могло дати можливість для викрадення персональних даних користувача. Витоки таких даних, дають можливість зловмисникам проводити персоналізовані SPAM-атаки, які є ефективнішими за простий SPAM, вимагати викуп за нерозголошення інформації чи створювати фейкові сторінки на основі викрадених даних.

Identity spoofing. Системи обміну миттєвими повідомленнями дозволяють корис-тувачам створювати анонімні аккаунти, які можна створити, навіть якщо пов’язані з ними особи, компанії, домени і т.д. не належать цьому користувачу, наприклад можна створити профіль та назвати його “Microsoft” чи іменем якогось відомого активіста, що створює загрозу, оскільки такі ідентифікатори можуть використовуватися зловмисно, для отри-мання персональних даних, важливої інформації, заманювання користувачів у фейкові чати і т.д. Прикладом є випадки зафіксовані у 2020 році в месенджері Telegram, коли зловмисники створювали фейкові акаунти з іменем “Saved messages” [9] та надсилали жертві повідомлення, одразу стираючи його чим виводили фейковий чат вгору списку контактів. Зважаючи на те, що оригінальний чат “Saved messages” може слугувати своєрідним архівом для користувача, де він зберігає різну інформацію, надсилання повідомлення зловмиснику з необачності, може стати джерелом витоку різного роду інформації, включаючи персональні дані, паролі і т.д.

Telegram. Даний месенджер є кросплатформенним хмарним застосунком з відкритим вихідним кодом для клієнтської частини. Хоч розробники заявляють про відкритість його коду, сам клієнт використовує для шифрування власний криптографічний алгоритм MTProto [10], який не використовується іншими розробниками, що значно знижує можливість знаходження вразливостей через неможливість його дослідження широким колом фахівців та підвищує шанси наявності вразливості нульового дня. Також, попри те, що він має e2e-шифрування, за замовчуванням Telegram використовує обмін повідомленнями із збереженням історії на сервері, що дозволяє отримати доступ до всієї історії, при компрометації хоча б одного із пристроїв користувача, яка стосується звичайних чатів, оскільки використання e2e-захисту вимагає створення окремого “секретного” чату.

Viber та WhatsApp. Дані месенджер одразу використовують e2e-шифрування пові-домлень [11, 12] і навіть якщо повідомлення не може бути доставлене одразу отримувачу, воно буде зберігатися на сервері у зашифрованому вигляді, оскільки можливість розшифрувати його, має лише отримувач. Втім, загроза у Viber полягає в тому, що при отриманні повідомлення воно розшифровується, а база даних із історією повідомлень зберігається на пристрої у відкритому вигляді і при отриманні доступу до пристрої всю історію, наявну на даний момент, можна викрасти, після чого переглянути без особливих труднощів, наприклад за допомогою утиліти “DB Browser for SQLite”. Що стосується WhatsApp, то історія зберіга-

ється у відкритому вигляді на пристрої і також може зберігатися у хмарних сховищах Google Drive та iCloud і відповідно їхня компрометація дасть змогу прочитати історію чатів.

Більшості загроз можна запобігти використовуючи всім відомі правила: не використовувати реальні імена та прізвища для реєстрації, регулярне оновлення програмного забезпечення та використання захищених чатів. Також можна виділити вибір більш безпечних програм, таких як Signal, який не збирає даних користувача і використовує номер телефону лише для реєстрації. Втім, залишається загроза витоку даних з боку розробників і єдиним способом захисту від цього залишається ретельне слідкування за даними, які програма збирає, використання e2e-захищених чатів, та заборона на доступ до будь-яких даних, які не потрібні для функціонування основного функціоналу, тобто обміну повідомленнями.

Інформаційні джерела

1. WhatsApp, wechat and meta messenger apps – global usage of messaging apps, penetration and statistics. MessengerPeople by Sinch. URL: https://www.messengerpeople.com/global-messenger-usage-statistics/ (дата звернення: 08.11.2022).

2. Прес-релізи та звіти – Які мобільні додатки є найбільш популярними? Домашня сторінка КМІС. URL: https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1072&page=1 (дата звернення: 08.11.2022).

3. Telegram messenger. App Store. URL: https://apps.apple.com/app/telegram/id686449807 (дата звернення: 09.11.2022).

4 WhatsApp messenger. App Store. URL: https://apps.apple.com/ua/app/whatsapp-messenger/id310633997 (дата звернення: 08.11.2022).

5. Viber messenger: chats & calls. App Store. URL: https://apps.apple.com/us/app/viber-messenger-chats-calls/id382617920 (дата звернення: 09.11.2022).

6. Messenger. AppStore. URL: https://apps.apple.com/app/messenger/id454638411 (дата звернення: 08.11.2022).

7. Holmes A. 533 million Facebook users' phone numbers and personal data have been leaked online. Business Insider. URL: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 (дата звернення: 09.11.2022).

8. Critical WhatsApp vulnerabilities patched: check you've updated!. Malwarebytes. URL: https://www.malwarebytes.com/blog/news/2022/09/critical-whatsapp-vulnerabilities-patched-check-youve-updated (дата звернення: 09.11.2022).

9. Шахрайство в Telegram: набирають популярність фейкові акаунти "Вибране". 24 Канал. URL: https://24tv.ua/tech/shahraystvo-telegram-nabirayut-populyarnist-novini-tehnologiy_n1391752 (дата звернення: 09.11.2022).

10. End-to-End encryption, secret chats. Telegram APIs. URL: https://core.telegram.org/api/end-to-end (дата звернення: 08.11.2022).

11. Viber Support. Viber Support. URL: https://help.viber.com/en/article/end-to-end-encryption-in-chats (дата звернення: 08.11.2022).

12. About end-to-end encryption | WhatsApp Help Center. WhatsApp Help Center. URL: https://faq.whatsapp.com/820124435853543 (дата звернення: 09.11.2022).

УДК 004.056

БЕЗПЕЧНА РЕАЛІЗАЦІЯ ПРОТОКОЛУ OAuth 2.0

Анастасія Толкачова, Олег Гарасимчук

кафедра захисту інформації Національного університету "Львівська політехніка"

Анотація. *Описана реалізація протоколу OAuth 2.0. Виділені основні вразливості. Розроблені рекомендації щодо імплементації протоколу у веб додатках.*

Ключові слова: *вразливості, протокол OAuth 2.0.*

Abstract. *The implementation of OAuth 2.0 protocol were described. The public vulnerabilities were mentioned. Recommendations for the implementation of the protocol in web applications are developed.*

Keywords: *vulnerabilities, OAuth 2.0 protocol.*

Останнім часом OAuth 2.0 використовує все більше застосунків і це розширює поверхню атаки для зловмисників. Протокол дуже зручно використовувати для авторизації, але, на жаль, не завжди це безпечно. І чим більше користувачі будуть використовувати авторизацію через інші додатки, тим більше хакерів буде зацікавлено в тому щоб заволодіти даними.

OAuth 2.0 – це протокол делегування, засіб, що дозволяє людині, що контролює ресурс, дозволити програмному додатку доступ до ресурсу від свого імені, не видаючи себе за нього.

Програма запитує авторизацію у власника ресурсу та отримує маркери або токени, які він може використовувати для доступу до ресурсу. Все це відбувається без необхідності додатку видавати себе за людину, яка контролює ресурс, оскільки токен явно представляє делеговане право доступу.

OAuth має на меті отримання право доступу від одного компонента системи до іншого. Зокрема, у світі OAuth клієнтська програма хоче отримати доступ до захищеного ресурсу від імені власника ресурсу (зазвичай кінцевий користувач). Специфікація OAuth визначає чотири ролі:

1. Власник ресурсу – має доступ до API і може делегувати доступ до цього API. Власником ресурсу, як правило, є особа, і зазвичай передбачається, що вона має доступ до веб-браузера.

2. Захищений ресурс – це компонент, до якого має доступ власник ресурсу. Він може приймати багато різних форм, але здебільшого це якийсь Web API. Хоча назва "ресурс" звучить так, ніби це щось для завантаження. API може дозволяти читання, запис та інші операції.

3 Клієнт – це частина програмного забезпечення, яка отримує доступ до захищеного ресурсу від імені власника ресурсу. Якщо ви Web-розробник, ви можете подумати, що ім'я "клієнт" означає Web-браузер, але цей термін тут використовується не в цьому сенсі. Якщо ви розробник біз-

нес-додатків, ви можете думати про “клієнта” як про людину, яка оплачує ваші послуги, але тут мова йде не про це. У OAuth клієнтом є будь-яке програмне забезпечення, яке використовує API, що надає захищений ресурс.

4 Сервер авторизації – цей сервер надає клієнту маркери доступу після успішної автентифікації власника ресурсу та отримання авторизації.

Наразі виділяють декілька типів реалізації протоколу в залежності від типу застосунку. Це може бути Web додаток, user-agent застосунок або нативний додаток. Вразливості автентифікації OAuth частково виникають через документацію щодо реалізації OAuth. Вимоги є відносно розмитими та гнучкими. Хоча існує декілька обов’язкових компонентів, необхідних для базової функціональності кожного типу гранту, переважна більшість реалізацій є абсолютно необов’язковою. Сюди входить безліч налаштувань необхідних для захисту даних користувачів.

Протокол OAuth 2.0 може бути реалізований в чотири різні способи:

– authorization code grant;

– implicit grant type;

– resource owner password credentials grant;

– client credentials grant.

Мета цих реалізацій – це інтегрувати сервіс одного ресурсу у другий. Наприклад, у вас є банківський додаток і ви хочете реалізувати інтеграцію пошти. У цьому випадку перший сервіс матиме доступ до даних користувача у другому сервісі. Для зловмисника це відкриває можливість скомпрометувати одразу два додатки та отримати дані користувача з пошти через банківський застосунок.

На сьогодні відомими вразливостями у OAuth 2.0 є:

– вразливості в застосунку (Такі як XSS, SQL injection);

– відсутність CSRF захисту;

– вразливості в the OAuth 2.0 сервері для автентифікації;

– розкриття кодів авторизації та токенів доступу;

– область застосування (параметр state) мав більше прав доступу, ніж було необхідно.

Міжнародні методології виділяють найкращі практики реалізації для запобігання атак на протокол OAuth 2.0. Важливо відзначити, що уразливості можуть виникати як на стороні клієнтського додатку, так і на стороні самого OAuth-сервісу. Існують рекомендації і для тих, і для інших.

Рекомендації для провайдерів OAuth-сервісів:

– Необхідно запитувати від клієнтських додатків реєстрації білого списку дійсних redirect_uris посилань, які використовуються при перенаправленні користувача. Де це можливо, необхідно використовувати суворе побайтове порівняння для перевірки URI в будь-яких вхідних запитах.

– Необхідно використовувати параметр state. Його значення також повинно бути прив’язане до сеансу користувача, включаючи деякі непе-

редбачувані, специфічні для сеансу дані, такі як хеш, що містить сеансовий файл cookie. Це допомагає захистити користувачів від CSRF атак.

– На сервері ресурсів необхідно переконатися, що токен доступу був виданий тому самому client_id, який робить запит.

Рекомендації для клієнтських додатків OAuth:

– Необхідно відправляти параметр redirect_uri не тільки на кінцеву точку /authorization, але і на кінцеву точку /token.

– Варто бути обережним з кодами авторизації – вони можуть бути розкритими через заголовки Referer при завантаженні зовнішніх зображень, скриптів або CSS-контенту. Також важливо переконатися, що їх нема в динамічно згенерованих файлах JavaScript, оскільки вони можуть бути використані з зовнішніх доменів через теги <script>.

Інформаційні джерела

1. Kiani, K.: Four Attacks on OAuth – How to secure your OAuth implementation.SANS – Working Papers in Application Security (2016)

2. Pai, S., Sharma, Y., Kumar, S., Pai, R.M., Singh, S.: Formal verification of OAuth2.0 using alloy framework. In: Proceedings of the 2011 International Conference on Communication Systems and Network Technologies, CSNT 2011. IEEE ComputerSociety, Washington (2011) OAuth 2.0 Cookbook by Adolfo Eloy Nascimento 1st Edition

3. Lodderstedt, T., McGloin, M., Hunt, P.: OAuth 2.0 threat model and security considerations. RFC 6819 (Informational), January 2013

4. OAuth 2 in Action by Justin Richer and Antonio Sanso 1st Edition

УДК 004.4

МЕТОДИ ЗАХИСТУ ВІД DDOS-АТАК НА ВЕБ-СЕРВІСИ

Віталій Фарбітник, Орест Полотай

кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Описано основні види DDOS-атак на веб-сервіси та основні методи захисту від них.*

Ключові слова: *DDOS-атаки, веб-сервіси.*

Abstract. *The main types of DDOS attacks on web services and the main methods of protection against them are described.*

Keywords: *DDOS attacks, web services.*

DDoS-атака – це злочиний спосіб порушити звичну роботу трафіку веб-ресурсу, що ускладнює користувачам доступ до нього, або повністю

його блокує. Якщо пояснювати простіше, то DDoS-атака виглядає, штучно створені затори, щоб не дозволити іншим водіям спокійно рухатись. Зазвичай для проведення DDoS-атак використовується мережа взламаних комп'ютерних систем (ботнет), які надсилаються велику кількість запитів, що і призводить до засмічення трафіку.

Хоча майже всі атаки DDoS передбачають перевантаження цільового пристрою або мережі трафіком, атаки можна розділити на три категорії. Зловмисник може використовувати один або кілька різних векторів атаки або циклічні вектори атаки у відповідь на контрзаходи, які вживає ціль.

Атаки прикладного рівня – іІнколи їх називають DDoS-атакою 7-го рівня (посилання на 7-й рівень моделі OSI), мета цих атак – вичерпати ресурси цілі, щоб створити відмову в обслуговуванні.

HTTP-flood – ця атака схожа на повторне натискання оновлення у веб-браузері на багатьох різних комп'ютерах одночасно – велика кількість HTTP-запитів переповнює сервер, що призводить до відмови в обслуговуванні.

Протокольні атаки – також відомі як атаки вичерпання стану, викликають порушення роботи служби через надмірне споживання ресурсів сервера та/або ресурсів мережевого обладнання, таких як брандмауери та балансувальники навантаження. Протокольні атаки використовують слабкі місця в рівнях 3 і 4 стеку протоколів, щоб зробити ціль недоступною.

SYN-flood – ця атака використовує з'єднання TCP – послідовність комунікацій, за допомогою яких два комп'ютери ініціюють мережеве з'єднання – шляхом надсилання цілі великої кількості SYN-пакетів TCP "Початковий запит на підключення" з підробленими вихідними IP-адресами.

Volumetric attacks – ця категорія атак намагається створити перевантаження, споживаючи всю доступну пропускну спроможність між цільовим елементом і сервером. Великі обсяги даних надсилаються до цілі за допомогою форми посилання або іншого засобу створення масивного трафіку, наприклад запитів від ботнету.

Ключовою проблемою для пом'якшення DDoS-атаки є розмежування між трафіком атаки та звичайним трафіком.

Наприклад, якщо у день випуску продукту веб-сайт компанії переповнений зацікавленими клієнтами, відключення всього трафіку є

помилкою. Якщо у цієї компанії раптом виникне сплеск трафіку від відомих зловмисників, ймовірно, потрібні зусилля, щоб пом’якшити атаку.

Взагалі кажучи, чим складніша атака, тим більша ймовірність того, що трафік атаки буде важко відокремити від звичайного трафіку – мета зловмисника полягає в тому, щоб якомога більше злитися, роблячи зусилля з пом’якшення якомога неефективними.

Спроби пом’якшення, які передбачають невибіркове припинення або обмеження трафіку, можуть викинути хороший трафік із поганим, а також атака може змінити й адаптуватися, щоб обійти контрзаходи. Щоб подолати складну спробу зриву, найбільшу користь дасть багатошарове рішення:

− Одним із рішень, доступним практично всім адміністраторам мережі, є створення примарного маршруту і перенаправлення трафіку на цей маршрут. У найпростішій формі, коли фільтрація реалізується без певних критеріїв обмеження, як легітимний, так і шкідливий мережевий трафік направляється на примарний маршрут та вилучається з мережі.

− Обмеження кількості запитів, які сервер приймає протягом певного періоду часу, також є способом пом’якшення атак відмови в обслуговуванні. Хоча обмеження швидкості є корисним для уповільнення крадіжки вмісту веб-сервісу та для пом’якшення спроб грубого входу в систему, одного цього, ймовірно, буде недостатньо для ефективної обробки складної DDoS-атаки. Тим не менш, обмеження швидкості є корисним компонентом ефективної стратегії пом’якшення DDoS.

− Web Application Firewall (WAF) – це інструмент, який може допомогти пом’якшити DDoS-атаку рівня 7. Поміщаючи WAF між інтернетом і вихідним сервером, WAF може діяти як зворотний проксі, захищаючи цільовий сервер від певних типів шкідливого трафіку.

− Розповсюдження мережі Anycast – підхід пом’якшення, який використовує мережу Anycast для розсіювання трафіку атаки по мережі розподілених серверів до точки, де трафік поглинається мережею. Подібно до потоку по окремим меншим каналам, цей підхід поширює вплив розподіленого трафіку атаки до точки, де він стає керованим, поширюючи будь-які руйнівні можливості. Надійність мережі Anycast для пом’якшення DDoS-атаки залежить від розміру атаки, розміру та ефективності мережі. Важливою частиною пом’якшення DDoS є використання розподіленої мережі Anycast.

− Транзитний потенціал. При проєктуванні програм необхідно переконатися, що постачальник послуг хостингу надає надмірну пропускну здатність підключення до інтернету, яка дозволяє обробляти великі обсяги трафіку. Оскільки кінцева мета DDoS-атак – вплинути на доступність ресурсів або додатків, необхідно розміщувати їх поряд не тільки з кінцевими користувачами, але і з великими вузлами міжмережевого обміну трафіком, які легко забезпечать вашим користувачам доступ до програми навіть за великого обсягу трафіку.

Продуктивність сервера. Більшість DDoS-атак є об'ємними та споживають багато ресурсів, тому важливо мати можливість швидко збільшувати чи зменшувати обсяг своїх обчислювальних ресурсів. Це можна забезпечити, використовуючи надмірний обсяг обчислювальних ресурсів або ресурси зі спеціальними можливостями, такими як продуктивні мережеві інтерфейси або покращена мережна конфігурація, що дозволяє підтримувати обробку великих обсягів трафіку.

Щоразу, коли виявляється підвищення обсягу трафіку, що потрапляє на хост, як орієнтир можна брати максимально можливий обсяг трафіку, який може обробити хост без погіршення його доступності. Така концепція називається обмеженням швидкості. Більш просунуті методи захисту відповідно мають додаткові можливості і можуть інтелектуально приймати тільки трафік, який дозволено, аналізуючи окремі пакети. Для використання подібних засобів необхідно визначити характеристики хорошого трафіку, який зазвичай отримує цільовий об'єкт, та мати можливість порівнювати кожен пакет із цим еталоном.

Отже, для забезпечення надійної роботи веб-сервісів, адміністратори повинні враховувати всі можливі види DDOS-атак та бути готовими до їх нейтралізації.

Інформаційні джерела

1. "DDoS npn" [Електронний ресурс]: – режим доступу: https://www.npmjs.com/package/ddos.

2. "What is a DDoS attack?" [Електронний ресурс]: – режим доступу: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

3. Балацька В.С., Полотай О.І., Ящук В.І. Вразливість комп'ютерної мережі як проблема закладів вищої освіти. Зб. тез доп. VI Міжнар. наук.-практ. конф. "Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи". (м. Львів, 04 листопада 2021 р.). Львів : ЛДУБЖД, 2021

УДК 004.056.53

ВИКОРИСТАННЯ ХАНІПОТІВ ДЛЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК

Єлизавета Шаєц, Ольга Лунгол

Донецький державний університет внутрішніх справ, м. Кропивницький, Україна

Анотація. *Виявлення вторгнень є важливою складовою інформаційної безпеки. Системи виявлення мережевих вторгнень використовується для моніторингу мереж на наявність атак або вторгнень, щоб вжити відповідних заходів для їх попередження та уникнення. Одним із способів виявлення мережевих атак є використання ханіпотів.*

Ключові слова: *ханіопти, інформаційна безпека, технологія обману, мережеві атаки.*

Abstract. *Detection of intrusions is an important component of information security. Network intrusion detection systems are used to monitor networks for attacks or intrusions in order to take appropriate measures to prevent and avoid them. One of the ways to detect network attacks is the use of honeypots.*

Keywords: *honeypots, information security, deception technology, network attacks.*

З розвитком мережевих технологій і додатків та зважаючи на те, що ми живемо в період гібридної війни, фактор виявлення мережевих атак є надзвичайно актуальним. Кількість і серйозність мережевих атак на території України значно зросла з початку 2022 року. Як ключовий метод у сфері мережевої безпеки, система виявлення мережевих атак відіграє надзвичайно важливу роль у захисті як персональних даних, так і даних організацій та установ, в тому числі державного рівня. Навколишнє середовище постійно розвивається та змінюється завдяки новим технологіям та Інтернету [1]. Продукти виявлення вторгнень – це інструменти, які допомагають керувати загрозами та вразливими місцями в цьому мінливому інформаційному середовищі.

Мережеві атаки будемо розглядати як спробу зловмисників отримати несанкціонований доступ до мережі організації або установи з метою викрадення, пошкодження даних, спостережень за діями користувачів мережі або виконання інших шкідливих дій. Наслідком пасивної мережевої атаки є отримання зловмисниками доступу до мережі з контролем або викраденням конфіденційної інформації, але не змінюючи дані, залишаючи їх недоторканими. У випадку активної мережевої атаки зловмисники не лише отримують неавторизований доступ, але й можуть змінювати дані, видаляючи, шифруючи чи іншим чином пошкоджуючи їх. Отримання зловмисниками неавторизованого доступу до пристроїв користувачів, організацій чи

установ, відбувається часто з їх компрометацією шляхом зараження шкідливим програмним забезпеченням. Зараження шкідливим програмним забезпеченням дозволяє зловмисникам скомпрометувати системи, викрасти дані та завдати значної шкоди користувачу чи групі користувачів [2].

Існують різні методи захисту мереж, такі як поділ мережі на зони відповідно до вимог безпеки, регулювання доступу до мережі Інтернет через проксі-сервер, розміщення брандмауера на кожному з'єднанні мережевих зон, використання трансляції мережевих адрес, що дозволяє переводити внутрішні IP-адреси в адреси, доступні в загальнодоступних мережах, відстеження вхідного, вихідного та внутрішнього мережевого трафіку з можливістю автоматичного виявлення загроз і розуміння їх контексту та впливу, застосування технології обману, тобто створення приманок у власній мережі, спокушаючи зловмисників скористатися ними тощо. Ідея створення приманок полягає у тому, що зловмисників навмисно перенаправляють в спеціально створене ІТ-середовище ще до того, як вони змогли проникнути в реальну інформаційну інфраструктуру організації чи установи. У цьому фіктивному середовищі фахівці служби кібербезпеки мають змогу спостерігати за зловмисниками, щоб визначити їхню мотивацію, методи та, в деяких випадках, навіть особу та замовників. Однією з технологій обману є використання приманки, або ханіпоту (honeypot). Він має вигляд справжньої комп'ютерної системи з програмами та даними, що змушує злочинців ІТ-простору вважати, що це реальна ціль. Наприклад, ханіпот може представляти собою систему виставлення рахунків клієнтам певної організації, що є улюбленою мішенню для кібератак злочинців, які хочуть заволодіти даними кредитних карток. Коли хакери використовують приманку, їх можна відстежити та вивчити, спрогнозувати поведінку, щоб зробити реальну мережу більш безпечною. Інший спосіб зацікавлення кіберзловмисника, це навмисне створення вразливостей у мережі. Наприклад, ханіпот може мати порти, які відповідають на сканування портів або слабкі паролі. Вразливі порти можуть бути залишені відкритими, щоб спонукати зловмисників проникнути до середовища ханіпот, а не до реальної мережі певної організації. Отже, ханіпоти у виявленні мережевих атак являються тим інформаційним інструментом, який може допомогти користувачу або спеціалістам із захисту мережі зрозуміти існуючі загрози та можливі загрози для певної організації.

Ханіпоти класифікують на основі їхнього розміщення та участі кіберзловмисника [4]:

– дослідницькі, які використовуються для аналізу хакерських атак і застосування різних способів запобігання цим атакам;

– виробничі, які розміщуються у виробничих мережах разом із сервером. Ці приманки діють як зовнішня пастка для зловмисників, що склада-

ється з неправдивої інформації та дає час адміністраторам на усунення ймовірної вразливості.

Залежно від взаємодії ханітопи можна поділити на:

− приманки з низьким рівнем взаємодії, які дають кіберзловмиснику дуже мало інформації про мережу. Цей ханітоп лише імітує послуги, які часто запитують зловмисники. Основна операційна система не задіяна в системах з низьким рівнем взаємодії. Такі приманки не потребують багато ресурсів і їх легко можна розміщати. Єдиним недоліком цих приманок є те, що досвідчені хакери можуть легко ідентифікувати подібні приманки та уникнути їх використання;

− приманки із середньою взаємодією дозволяють кіберзловмиснику виконувати більше дій порівняно з попереднім варіантом;

− приманки з високою взаємодією спрямовані на те, щоб кіберзловмисник витратив багато часу на роботу з ханітопом, у цей час фахівці з безпеки отримують багато інформації про самих хакерів. Ці приманки включають операційну систему в реальному часі, тому вони є порівняно ризикованими, якщо хакер ідентифікує ханіпот [4]. Недоліком таких приманок також є те, що вони є досить дорогими у вартості та складними у реалізації.

До переваг використання приманок ханітопів при виявленні мережевих атак можна віднести: ханітопи збирають дані лише тоді, коли із ними хтось взаємодіє; у ханіпотів немає помилкових спрацьовувань, тому що будь-яка діяльність з ними є несанкціонованою, зважаючи на мету їх створення; вони не потребують багато ресурсів; не має значення, чи використовує зловмисник шифрування, оскільки діяльність з приманкою в будь-якому випадку буде зафіксовано.

Інформаційні джерела

1. Meeragandhi, G. & K.Srivatsa,. (2018). Detecting and preventing attacks using network intrusion detection systems. International Journal of Computer Science and Security.

2. Network Attacks and Network Security Threats. URL: https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/ (Дата звернення: 17.11.2022).

3. What is deception? Deception Technology from Austria. URL: https://cybertrap.com/en/deception-technology/ (Дата звернення: 15.11.2022).

4. What is Honeypot? Geeksforgeeks. URL: https://www.geeksforgeeks.org (Дата звернення: 19.11.2022).

5. Honeypots: The sweet spot in network security. John Harrison, Symantec Corp. URL: https://www.computerworld.com/article/2573345/honeypots--the-sweet-spot-in-network-security.html (Дата звернення: 19.11.2022).

Напрям 3

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

АНАЛІЗ ПРОТОКОЛІВ КВАНТОВОГО ПРЯМОГО БЕЗПЕЧНОГО ЗВ'ЯЗКУ

Сергій Дорожинський

Національний авіаційний університет, м. Київ, Україна

Анотація. *Розвиток сучасних обчислювальних технологій ставить під загрозу конфіденційність інформації, що майже завжди забезпечується традиційними криптографічними засобами. Ця обставина змушує шукати нові методи захисту. У статті проведено аналіз нових методів та протоколів, а також представлено їх переваги та недоліки. В результаті представлено висновки щодо використання протоколів та підвищення рівня їх ефективності.*

Ключові слова*: квантова криптографія, класифікація, квантовий прямий безпечний зв'язок, квантовий розподіл ключів.*

Abstract. *The development of modern computer technologies threatens the confidentiality of information, which is almost always ensured by traditional cryptographic means. This circumstance forces to look for new methods of protection. The article analyzes new methods and protocols, as well as presents their advantages and disadvantages. As a result, conclusions are presented regarding the use of protocols and increasing the level of their effectiveness.*

Keywords: *quantum cryptography, classification, quantum direct secure communication, quantum key distribution.*

Вступ. Квантовий прямий безпечний зв'язок (QSDC) – це один з напрямків квантової криптографії, який пропонує безпечне спілкування без будь-якого спільного ключа. Характерною особливістю даного методу є відсутність криптографічних перетворень, відповідно відсутня і проблема розподілу ключів шифрування. ***Метою*** даної роботи є узагальнена характеристика протоколів квантової криптографії, знаходження їх слабких сторін для подальшого опрацювання та покращення.

Основна частина. В QSDC протоколах Аліса (адресант) кодує секретне повідомлення, що складається з декількох кубітів, використовуючи попередньо обране правило кодування та надсилає їх Бобу (адресату) [2]. Щоб уникнути підслуховування, законні сторони повинні перевіряти легітимність інших сторін, що вимагається протоколами квантової автентифікації.

Перший протокол QSDC з автентифікацією був запропонований у 2006 році, і з тих пір багато дослідників працювали в цій галузі. Існує кілька протоколів квантової криптографії, які доведено невразливими до різноманітних поширених атак. Це активні атаки, тобто перехоплювач може отримати доступ до кубітів, що передаються в квантовому каналі між законними сторонами, і брати активну участь у протоколі. Деякі пасивні атаки також можуть викликати проблеми з витоком інформації в протоколах зв'язку.

У 2020 році був представлений протокол QSDC на основі одного фотона та пари EPR, а також була досягнута взаємна автентифікація. Для простоти його називають протоколом YZCSS (Yan, Zhang, Chang, Sun, Sheng protocol) [3]. У ньому є дві сторони, а саме Аліса та Боб з їхніми відповідними ідентифікаторами ID_A та ID_B відповідно, де ID_A, $ID_B \in \{0, 1\}^N$. Алісі потрібно надіслати секретне повідомлення $M \in \{0, 1\}^N$ до Боба за допомогою окремих фотонів і станів Белла, де Белл-стани (пари EPR) визначаються як:

$$\left|\phi\pm\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle or \left|\phi^-\right\rangle\right),$$

$$\left|\varphi\pm\right\rangle = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle \pm \left|10\right\rangle\right).$$

Етапи протоколу такі:

1 етап. Аліса та Боб мають спільні ідентифікатори ID_A та ID_B, використовують деякі QKD для обміну даними.

2 етап. Після того, як Боб отримує S, він знає точне положення фотонів-приманок, що відповідають його ідентифікатору ID_B. Боб вимірює ці фотони-приманки в належних базисах, відповідно до ID_A.

3 етап. Боб просить Алісу оголосити початкові стани пар кубітів S_A для перевірки безпеки.

4 етап. Боб отримує всі біти секретного повідомлення з результатів вимірювання пар кубітів S_M. Щоб перевірити цілісність секретного повідомлення, Аліса і Боб публічно порівнюють деякі частини повідомлення.

Протокол YZCSS захищений від різного роду атак, таких як атака імітації, атака перехоплення та повторного надсилання, атаки "людина всередині" і т.д. Однак підслухувач може розробити стратегію, яка дозволяє йому ефективно виконувати атаку перехоплення та повторного надсилання.

Нещодавно було запропоновано два дуже цікаві протоколи DSQC [4], засновані на перевпорядкуванні частинок. Протокол Юаня застосовує чотирикубітовий симетричний стан W для зв'язку, тоді як протокол Цая використовує щільне кодування чотирьох станів кластера кубітів. GHZ-подібні стани корисні для контрольованої квантової телепортації. Також

можна сформувати ортонормований базисний набір у 2^3 тривимірному Гільбертовому просторі з 8 станів, які можна використовувати для щільного кодування та DSQC. Таким чином, стани створюються як корисний ресурс для квантової обробки інформації. Аналогічний протокол DSQC, заснований на перегрупуванні частинок, був нещодавно запропонований Юанем та іншими [5]. У своїй роботі вони використовували чотирикубітний симетричний стан W для безпечної передачі 2 бітів класичної інформації. Їхній протокол також використовує 4-кубітні W-стани для DSQC, але кожен із цих W-станів можна використовувати лише для передачі одного біта класичної інформації.

Узагальнюючи, можна продемонструвати слабкі позиції для кожного зі згаданих протоколів, а також показати, до яких кібератак вони є абсолютно стійкими.

Таблиця 1

Презентація стійкості протоколів до різних видів кібератак,
де "+" означає стійкість, а "–" вказує на вразливість до таких атак

Протоколи QSDC	Основні види кібератак								
	C	NC	MiM	DoS	TC	FS	PBS	PNS	TH
Ping-pong, DLL, PP^{GV}	+	–	–	–	+	+	+	+	–
Переплутані кубіти групами	+	+	–	–	+	+	+	+	–
З групами переплутаних кудитів	+	+	–	–	+	+	+	+	–
З одиничними кубітами	+	+	–	–	+	+	+	+	–
YZCSS	+	+	–	–	+	+	+	+	–
з використанням GHZ-подібних станів	+	+	–	–	+	+	+	+	–
з використанням GHZ-подібних станів без використання щільного кодування	+	+	–	–	+	+	+	+	–

Висновки. Таким чином, у цій роботі проведено аналіз сучасних протоколів квантової криптографії (визначено їх переваги і недоліки), їх існуючі класифікації. На підставі часткових узагальнень теоретичних положень та практичних досягнень у галузі квантової криптографії, розроблено узагальнену класифікацію. За рахунок порівняння різних факторів роботи протоколів, їх стійкості до певних кібератак, ми маємо можливість виявити низку проблем у цій галузі та розширити можливості щодо вибору відповідних методів для побудови сучасних квантових систем захисту інформації.

Інформаційні джерела

1. Zhmurko T., Kinzeryavyy V., Yubuzova Kh., Stojanovic A. Generalized classification of modern quantum cryptography and communication methods. Ukrainian Scientific Journal of Information Security, 2015, vol. 22, issue 3, p. 287-293.
2. Banerjee A., Pathak A. Efficient protocols for deterministic secure quantum communication using GHZ-like states. Quantum Physics, 2018.
3. Lili Yan, Shibin Zhang, Yan Chang, Zhibin Sun, and Zhiwei Sheng. Quantum secure direct communication protocol with mutual authentication based on single photons and Bell states. Computers, Materials & Continua, 63(3):1297–1307, 2020.
4. Banu N., Ghosal P. and Panigrahi P. K., "Quantum information splitting of an unknown two qubit state by using two three qubit GHZ like states, " 2014 International Conference on Electronics and Communication Systems (ICECS), 2014, pp. 1-4, doi: 10.1109/ECS.2014.6892773.
5. Shukla Ch., Banerjee A., Pathak A. Improved Protocols of Secure Quantum Communication Using W States. International Journal of Theoretical Physics, 2018, vol. 52, pp. 1914–1924.

УДК 004.6

КІБЕРЗАХИСТ В ІНТЕГРОВАНИХ СИСТЕМАХ САНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ

Андрій Рудик, Юрій Рудик, Наталія Федінець

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Розглядаються рівні хмарних обчислень та кібербезпеки. Наведено підходи до інформаційної безпеки хмарного хостингу. Їх суть заснована на принципі: безпека хмари – це відповідальність провайдера, безпека в хмарі – це відповідальність клієнта. Тому питання підвищення безпеки хмарних сервісів та хостингу потребує різноманітної уваги.*

Ключові слова: *хостинг, кібербезпека, вразливість, хмарні обчислення, безпека, якість.*

Abstract. *The levels of cloud computing and cyber security are considered. Approaches to information security of cloud hosting are given. Their essence is based on principle: the security of the cloud – is the responsibility of the provider, the security in the cloud – is the responsibility of the client. Therefore, the issue of improving the safety of cloud services and hosting requires a variety of attention.*

Keywords: *hosting, cyber security, vulnerability, cloud computing, safety, quality.*

Президент росії оголосив про початок “спецоперації” з метою “демілітаризації і денацифікації України” вранці 24 лютого. Цей день став початком повномасштабної війни проти України. Цілі “спецоперації” неодноразово змінювалися і зрештою трансформувалися у “захист населення Донбасу”. На сьогодні, в умовах військової повномасштабної агресії росії в Україні всі завдання цивільного захисту і безпеки громадян перебувають в нових вимірах [1–3].

Нині нашою головною метою є вдосконалення діяльності підрозділів ДСНС України, оснащення рятувальників сучасними технічними засобами та налагодження тісної взаємодії з органами місцевої влади у процесі забезпечення цивільного захисту населення. Російські інформаційні операції виявилися незграбними й були спростовані оприлюдненням розвідданих. А спроби росіян зруйнувати цифрову інфраструктуру України та посіяти розбрат за допомогою кіберможливостей були зустрінуті стійким, професійним та ефективним українським кіберзахистом. Це новий фронт війни в Україні, і його наслідки продовжуватимуться і після її завершення. У системах кіберзахисту слід вжити заходів, щоб протистояти організованим державним кампаніям з дезінформації та домогтися того, щоб їм не вдалося приглушити міжнародне обурення діями Росії [4–5].

У всіх цих сферах спостерігаються спроби російської держави узгодити та скоординувати кібернетичні можливості з більш традиційними аспектами військової потуги. На сьогодні ці гібридні наміри не мали успіху – їхній вплив виявився меншим, ніж очікували. Почасти це пояснюється тим, що Україна зарекомендувала себе надзвичайно ефективним кіберзахистом. Після анексії Криму у 2014 році в різних сферах і галузях створювали цифрову фортецю. Поряд із героїчною обороною українських військових, в інтернеті, можливо, була найефективніша оборонна кіберактивність дотепер. Діючи під постійним тиском проти дуже здібного противника, ця команда з представників бізнесу, розвідки, служб безпеки, а в деяких випадках і громадян, працювала пліч-о-пліч, попереджаючи, реагуючи та усуваючи наслідки.

У відповідь на стрімкий розвиток засобів несанкціонованого доступу до інформації в результаті загального прогресу сучасних інформаційних та комп’ютерних технологій є необхідність підтримки актуальності систем захисту підприємств від несанкціонованого доступу та контролю за працівниками [6].

Загроза безпеки активів об’єкту інформаційної діяльності складається з безлічі пов’язаних і автономних елементів. Розглядаючи загрозу безпеки, як комплекс, виникає ідея пошуку комплексного рішення до потенційної загрози.

Розробляючи комплексну систему санкціонованого доступу потрібно прослідкувати за вдосконаленням вже існуючих та появу нових організаційних, програмних та технічних способів, які б допомогли в побудові комплексної систем санкціонованого доступу та захисту інформації [7].

Саме правильне проведення процесу розробки комплексної системи санкціонованого доступу дозволяє оптимізувати як процес реалізації комплексу на практиці, так і гарантувати його максимальну ефективність під час експлуатації.

Підбір компонентів комплексу здійснено враховуючи характеристики об'єкту інформаційної діяльності, елементи якої формували зокрема і просторові та бюджетні вимоги [8].

Підійшовши до спроєктованої системи у ролі зловмисника вдалось сформувати картину вразливостей об'єкту під захистом комплексу, та запропонувати способи їх вирішити. З повторенням цієї процедури можна отримати кілька ітерацій комплексу, з різним рівнем захисту, який буде пропорційним до затрат на його реалізацію та підтримку. Вибір варіанту варто здійснювати оцінюючи ризики.

Інформаційні джерела

1. Три сценарії розвитку війни в Україні URL: https://texty.org.ua/tag/khid-vijny/

2. Парламентська асамблея НАТО визнала Росію державою-терористом URL: https://www.radiosvoboda.org/z/16697

3. Найкоротша історія російсько-української війни URL: https://www.radiosvoboda.org/a/31382202.html

4. Ткачук Р.Л., Сікора Л.С., Лиса Н.К., Навитка М.Л., Сабат В.І., Федина Б.І., Тупичак Л.Л. Інформаційні технології формування стратегій прийняття рішень інтелектуальним агентом в техногенних системах за умов когнітивних збоїв, НУЛП, 2020.

5. Полотай О.І. Важливість комплексної системи захисту інформації у забезпеченні інформаційної безпеки ГО "Наукова спільнота"; WSSG w Przeworsku. – Тернопіль, 2022 https://sci.ldubgd.edu.ua/jspui/handle/123456789/11113

6. Лагун А., Рудик А., Рудик Ю. Аналіз виявлення вразливостей сучасного хостингу при тестуванні на проникнення, Захист інформації в інформаційно-комунікаційних системах, Львів, 2019. С.53-55.

7. Полотай О.І., Масюк Н. Профілі можливостей порушників інформаційної безпеки структурних підрозділів безпекових структур Національна Академія Служби Безпеки України, 2021.

8. Ткачук Р.Л., Боднар О., Лагун А. Е. Виявлення небезпечних входжень у комп'ютерну мережу за допомогою систем виявлення вторгнень, ЛДУБЖД, 2021.

УДК 342.951:34.03(477)

ДО ПИТАННЯ ПЕРЕВАГ СИСТЕМ ВІДЕОНАГЛЯДУ У ГРОМАДСЬКИХ МІСЦЯХ

Максим Смілевський

Управління безпеки департаменту міської мобільності та вуличної інфраструктури Львівської міської ради, м. Львів, Україна

Анотація. *Встановлення відеоспостереження у громадських місцях слугує для забезпечення безпеки оточуючих. Статтею 307 Цивільного кодексу України передбачено, що на вулиці, у громадських місцях, на публічних заходах дозволяється відкрита зйомка осіб, які потрапляють в кадр. Законодавство у сфері забезпечення безпеки та законодавство, що охороняє право на приватне життя як в Україні, так і в інших країнах завжди є дуже динамічним, у залежності від суспільних потреб, баланс схиляється то у бік безпеки, то у бік приватності. Зазвичай, нормативні документи, які регламентують правила відеонагляду, розробляються місцевою владою.*

Ключові слова: *системи відеоспостереження, безпека, цифрові дані, аналітика відеонагляду, розумні міста, розпізнавання обличчя.*

Abstract. *Installation of video surveillance in public places serves to ensure the safety of people. Article 307 of the Civil Code of Ukraine stipulates that on the street, in public places, at public events, open filming of persons who fall into the frame is allowed. Legislation in the field of ensuring security and legislation protecting the right to private life both in Ukraine and in other countries is always very dynamic, depending on public needs, the balance tilts either in the direction of security or in the direction of privacy. Usually, regulatory documents that regulate the rules of video surveillance are developed by local authorities.*

Keywords: *video surveillance systems, security, digital data, video surveillance analytics, smart cities, facial recognition.*

Багато країн використовують камери спостереження в громадських місцях як основний інструмент для відстеження переміщень населення і запобігання злочинності та тероризму як у приватному, так і в державному секторах.

Загальна фізична безпека життя, майна та обладнання, як і завжди є важливою та обумовлює еволюцію відеоспостереження, цифрового відеонагляду, а також те, як інтелектуальніші системи допомагають операторам у роботі. На даний час у розумних містах впроваджується дедалі більше систем відеоспостереження.

За останнє десятиліття можливості камер відеоспостереження змінилися завдяки фундаментальним змінам у способах збирання, аналізу, спільного використання та зберігання цифрових даних. Камери відеоспостереження вже відіграють ключову роль у розвитку розумних міст і промислового інтернету речей, що бурхливо розвивається. Глибоке навчання та штучний інтелект стають все більш поширеними, оскільки камери можуть точніше збирати дані та робити прогнози на основі інтегрованого аналітичного програмного забезпечення, розробленого виробниками.

Переваги камер спостереження у громадських місцях:

– Камери спостереження мають бути встановлені у громадських місцях, оскільки вони забезпечують громадську безпеку. Мало хто спробує завдати вам шкоди, знаючи, що його дії записуються на камеру. Камери захищають вас та ваше особисте майно.

– Поліція може ідентифікувати злочинців, зафіксованих камерами. За допомогою камер спостереження поліція може не лише запобігати злочинам, а й оперативно розкривати кримінальні справи з речовими доказами.

– Камери відеоспостереження захищають від крадіжки майна та вандалізму. Дуже складно вкрасти щось, якщо вас знімають камери. Камери спостереження зловлять злодія до або в процесі злочину.

– Якщо ніхто не знає про злочин, доки його не було здійснено, відеозаписи з камер спостереження завжди є важливим доказом під час поліцейського розслідування. Камери спостереження розкривали і розкриватимуть багато злочинів.

– Є певні думки що камер спостереження у громадських місцях не повинно бути. Основна теза – камери втручаються у приватне життя. Однак, є контраргумент – навіщо бути на публіці, якщо вам потрібна конфіденційність? Камери спостереження призначені для того, щоб охороняти вас та інше майно, а не переслідувати вас. Камери існують не для того, щоб втручатись у приватне життя людини, а для того, щоб захищати громадськість, стримуючи злочинну діяльність та надаючи речові докази, коли злочин було знято на камеру. Відеонагляд має відповідати світовим стандартам безпеки, до прикладу, як розроблений британцями стандарт “Безпека за замовчуванням” [1].

– Злочинці з меншою ймовірністю вчинять злочини в цьому районі, якщо знатимуть, що їх весь час зніматимуть. Несумлінні дії, такі як магазинні крадіжки, навряд чи варті можливості потрапити до в’язниці [2].

– Наявність камер у громадських місцях дозволяє людям відчувати себе у безпеці. Люди почуваються у більшій безпеці, знаючи, що потенційного грабіжника чи зловмисника відлякує присутність камери.

− Камери за допомогою відеоаналітики тепер можуть збільшувати масштаб, розпізнавати обличчя та автомобільні номери, щоб розкрити чиюсь особу, що може бути корисним для запобігання злочинам при правильному використанні. Злочинця може бути затримано швидко.

− Розвиток розпізнавання осіб та аналітичного програмного забезпечення дозволяє набагато краще прогнозувати злочинну поведінку та створювати точніші звіти.

Як яскравий приклад – ради, правоохоронні органи та фахівці з управління безпекою [3] у Великій Британії значною мірою покладаються на відеоспостереження як на інструмент боротьби зі злочинністю та запобігання тероризму. В даний час підраховано, що у Великій Британії налічується близько 5,2 мільйона камер відеоспостереження [4], по одній камері на кожні 13 осіб – ця кількість охоплює все, від громадського спостереження до камер, встановлених приватними підприємствами, і навіть камер дверних дзвінків.

Залежно від кількості камер безпеки та їх розташування, одночасний перегляд прямого та архівного відео може підтвердити будь-яку незаконну діяльність до того, як підозрюваного затримають відповідні органи. Досвід встановлення камер відеонагляду показав, що один оператор, який стежить за живим та архівним відео, може охопити набагато більшу територію, ніж офіцер, що патрулює на вулиці. Сучасні системи тепер мають “феноменальні можливості”, які викликають зрозумілі побоювання з приводу ризику для конфіденційності та потенційних зловживань, які створюють такі можливості. Саме тому індустрія відеоспостереження повинна забезпечити встановлення тільки апаратного та програмного забезпечення, що відповідає відповідним стандартам.

Інформаційні джерела

1. Secure by Default. National Cyber Security Centre : веб-сайт. URL: https://www.ncsc.gov.uk/information/secure-default (дата звернення: 15.11.2022).

2. IP video will ‘stamp out’ self-service checkout theft. IFSEC Global : веб-сайт. URL: https://www.ifsecglobal.com/uncategorized/ip-video-will-stamp-out-self-service-checkout-theft/ (дата звернення: 15.11.2022).

3. A security management guide: the role, training, certification, degrees and standards. IFSEC Global : веб-сайт. URL: https://www.ifsecglobal.com/global/security-management-guide-role-training-certification-degrees-standards/ (дата звернення: 15.11.2022).

4. Jonathan Ratcliffe. Number of CCTV Cameras in the UK reaches 5.2 million. URL:https://www.cctv.co.uk/number-of-cctv-cameras-in-the-uk-reaches-5-2-million/ (дата звернення: 15.11.2022).

УДК: 004.05

ВПРОВАДЖЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕХНОЛОГІЯХ РОЗУМНОГО БУДИНКУ

Тарас Стефанів, Ростислав Ткачук, Валерія Балацька

Кафедра управління інформаційною безпекою
Львівського державного університету безпеки життєдіяльності,
м. Львів, Україна

Анотація. *У роботі розроблено захищену систему з використанням Internet of Things на прикладі розумного будинку. Визначено переваги та недоліки використання Інтернет речей. Досліджено що сновними уразливостями IoT слід вважати відсутність стандартизації, шифрування трафіку, встановлення дефолтних паролів за замовчуванням.*

Ключові слова: *IoT, мережа, розумний будинок, VPN, WPA2-PSK, ASA5505, ACL, актуатор.*

Abstract. *The paper developed a secure system using the Internet of Things using the example of a smart house. The advantages and disadvantages of using the Internet of Things are defined. The main vulnerabilities of IoT can be considered the lack of standardization, encryption of traffic, setting of default passwords by default.*

Keywords: *IoT, network, smart home, VPN, WPA2-PSK, ASA5505, ACL, actuator.*

Розумний будинок (smart home, digital house, intelligent house) – комплекс датчиків, проводів, контролерів і інших девайсів що дають можливість домовласнику керувати системами що забезпечує комфорт, безпеку, ресурсозбереження і інші властивості будинку, автоматизувати їх. Система повинна вміти розпізнавати конкретні ситуації, що відбуваються в будівлі, і відповідним чином на них реагувати: одна з систем може управляти поведінкою інших за заздалегідь виробленим алгоритмам [4].

Сьогодні споживачам доступне надзвичайно широке коло контролерів, датчиків, виконавчих пристроїв й інших гаджетів для розумного дому. Для того щоб розібратися у цій величезній кількості техніки від багатьох фірм що виходять на ринок з даною продукцією спробуємо класифікувати дану техніку і накреслити деяку стратегію побудови розумного дому. Отже бувають провідний і безпровідний спосіб управління системою розумного будинку.

Переваги провідних систем у тому що вони надійні (сигнал що йде по спеціально прокладеними проводам), постійне джерело живлення (не потрібна заміна батарейок в пристроях), висока швидкість відгуку. Провідні системи не обмежуються радіусом дії радіосигналу, не схильні до впливу різних перешкод, мають гарну захищеність мережі з точки зору кібербез-

пеки і не вимагають подальшого обслуговування. Крім того, такі технології мають високу швидкість передачі даних [4].

Недоліки даної системи полягають у тому, що її необхідно запроєктувати та встановити на початковому етапі будівництва, реконструкції чи ренонту. Також прокладання та підєднання каберів потребує певного досвіду та відповідних знань і навиків.

Безпровідний – це коли зв'язок і управління з датчиками і виконавчими механізмами здійснюється за допомогою радіохвиль (wi-fi, bluetooth, z-wave, ZigBee, EnOcean і інші). Це дозволяє скоротити кількість кабелів, а також час на інсталяцію системи. Ці системи можна монтувати на об'єктах із завершеним ремонтом. Її можна встановити і налаштувати за інструкцією і звичайний користувач. Недоліки безпровідної системи полягають у тому, що інформаційні та управляючі сигнали між пристроями мають обмежений радіус дії. Також необхідно слідкувати за джерелом автономного живлення пристроїв, адже час їх дії обмежений. При застосуванні бездротових пристроїв системи автоматизації треба враховувати цілу низку особливостей (перешкоди сигналу, живлення, сумісність і.т.п).

Провідні технології – безальтернативні для автоматизації великих об'єктів, заміських резиденцій, офісних і промислових будівель, багатоквартирних житлових будинків. Вони забезпечують більшу надійність, безпеку і комфорт у порівнянні з бездротовими технологіями.

Оптимальна побудова системи автоматизації "розумний будинок" виконується на провідній основі, а згодом, по мірі необхідності, доповнюється бездротовими пристроями. У загальному випадку, система домашньої автоматизації, тобто розумного будинку складається з трьох основних компонентів: датчиків, актуаторів і центрального контролера.

Датчики або сенсори призначені для того, щоб збирати інформацію про стан навколишнього середовища. Виконавчі пристрої або актуатори служать для того, щоб управляти реальними фізичними об'єктами і пристроями, чи змінювати будь-яким способом стан навколишнього середовища.

Центральний контролер або хаб розумного будинку приймає інформацію від датчиків і посилає сигнали актуаторами. Саме в хабі зосереджений весь інтелект "розумного будинку". В абсолютній більшості випадків, хаб виступає мостом між розумним будинком, тобто мережею датчиків, актуаторів і звичайною домашньою провідною або Wi Fi мережею інтернету. Найчастіше, в центральному контролері є свій невеликий веб-сервер, завдяки якому доступ до управління розумним будинком можна отримати з будь-якого веб-браузера, з ПК, ноутбука, планшета чи смартфона – як "всередині", з домашньої мережі так і "зовні", через інтернет.

Можливості центрального контролера багато в чому залежать від того, наскільки "просунуте" ПО в ньому встановлено. Деякі бюджетні продукти просто надають інтерфейс для того, щоб можна було дистанційно

включати і вимикати світло, посилати прості команди на актуатори, підключені до мережі домашньої автоматизації або переглядати параметри середовища в квартирі за допомогою мобільного пристрою або інтернет-браузера. Найбільш "просунуті" контролери мають штучний інтелект, який дозволяє виконувати певні сценарії без участі людини, підлаштовуючись під її поведінку. Часто для цього контролери підключаються до хмарних сервісів, де збираються десятки тисяч різних сценаріїв і на підставі аналізу великих обсягів даних виділяються характерні особливості поведінки користувачів, складаються найбільш оптимальні шаблони управління домашньою інфраструктурою. При цьому може бути задіяна й інша інформація, не тільки та, що надходить від датчиків розташованих всередині об'єкта. Слід зазначити, що досить часто, "просунутому" програмному забезпеченню для управління "розумним будинком" неважливо, яка технологія зв'язку датчиків і актуаторов використовується на фізичному рівні. Достатньо лише, щоб були в наявності високорівневі драйвера, які б передавали в інтерфейс потрібні дані [2].

Усі "розумні" пристрої що підключені до мережі та передають через неї дані, можуть стати потенційною мішенню для кіберзлочинців.

Чим більше способів підключення пристроїв, тим більше можливостей у зловмисників для їх перехоплення. Такі протоколи, як HTTP та інтерфейс прикладного програмування (API), є лише деякими з каналів, які використовують пристрої IoT і які можуть бути перехоплені хакерами. Пристрої IoT можуть піддаватися різним потенційним загрозам, як наприклад вразливість сеансу/файлів cookie та використання вразливого OAuth та інші [1, 3].

Висновки. Комплексний захист систем IoT можливий лише при забезпеченні надійного мережевого, програмного та технічного захисту пристроїв, обладнання та комунікацій з яких складаються ці системи. Враховуючи те, що вищезазначені об'єкти та методи їх захисту можна об'єднати в окрему захищену систему розумного будинку, її розробка є актуальною теоретичною та практичною задачею кібербезпеки.

Інформаційні джерела

1. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6165453.

2. Internet of things (IoT). URL: https://internetofthingsagenda.techtarget.com/definition/Internetof-Things-IoT#.

3. Britvin A., Alrawashdeh J. H., Tkachuk R. Client-Server System for Parsing Data from Web Pages. Advances in Cyber-Physical Systems Volume 7, Number 1, 2022. P. 8–13.

4. Coetzee and J. Eksteen. The Internet of Things-promise for the future? An introduction. ISTAfrica Conference Proceesing, 2011. P. 1–9.

УДК 004.621.3

МОДЕЛЬ СИСТЕМИ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Юрій Тичина, Валентина Ящук, Орест Полотай

Кафедра управління інформаційною безпекою
Львівського державного університету безпеки життєдіяльності,
м. Львів, Україна

Анотація. *Розглянуто теоретичні, науково-методичні та організаційно-функціональні основи моделювання системи управління інцидентами інформаційної безпеки. Визначено сучасні підходи до управління інцидентами інформаційної безпеки. Наведено методичні підходи до формування концепції та структури автоматизованої системи управління інцидентами інформаційної безпеки. Запропоновано модель управління інцидентами інформаційної безпеки та наведено методику розслідування інцидентів інформаційної безпеки.*

Ключові слова: *інформаційна безпека, інцидент інформаційної безпеки, система управління інцидентами інформаційної безпеки, модель системи управління інцидентами.*

Abstract. *The theoretical, scientific-methodical, and organizational-functional bases of modeling the information security incident management system are considered. Modern approaches to information security incident management are defined. Methodical approaches to the formation of the concept and structure of the automated information security incident management system are given. The information security incident management model is proposed and the method of investigation of information security incidents is given.*

Keywords: *information security, information security incident, information security incident management system, incident management system model.*

Управління інцидентами є однією з найважливіших процедур управління інформаційною безпекою (ІБ). Основною метою створення системи інформаційної безпеки (ІБ) організації є зниження ризиків щодо інформаційних активів і зменшення негативних наслідків від можливих інцидентів ІБ. Процес управління інцидентами інформаційної безпеки (УІІБ) – ключовий процес у системі інформаційної безпеки. Саме цим зумовлені теоретична значущість, практична спрямованість та новизна теми кваліфікаційної роботи, його мета і сукупність завдань.

Для управління ІІБ необхідно організувати комплекс методів та засобів управління інцидентами (УІ), забезпечити його належними ресурсами,

відповідною нормативно-розпорядчою і робочою документацією, технічними засобами забезпечення механізмів контролю.

Управління інцидентами інформаційної безпеки (УІІБ) є важливим процесом, який забезпечує організацію можливістю своєчасного виявлення інциденту та якомога швидшого реагування на нього за допомогою адекватних засобів підтримки. Для опису процесу формування СМІІБ в роботі використовується класична модель безперервного удосконалення процесів (рисунок на слайді), що отримала назву від циклу Шухарта-Демінга – модель PDCA (Плануй, Plan – Виконуй, Do – Перевіряй, Check – Дій, Act).

Проблеми інформаційної безпеки істотно залежать від типу інформаційних систем і сфери їх застосування. У локальних системах малого масштабу систему захисту побудувати набагато простіше, ніж в системах розподіленого типу, що пояснюється особливостями цих систем. Саме тому запропонована структурна модель інформаційної безпеки систем розподіленого типу (рис. 1). Структурна модель передбачає, що рішення проблеми безпеки в інформаційних системах розподіленого типу полягає в аналізі таких основних компонентів: визначення основних завдань захисту інформації, визначенні суб'єктів інформаційних процесів, класифікації основних можливих загроз безпеки, визначенні рівнів вразливості інформаційних систем, визначенні джерел інформації, ознайомленні з особливостями джерел загроз, дослідженні способів та напрямів захисту та звичайно цілей захисту.

Формалізуючи модель системи інцидентів інформаційної безпеки у математичному вигляді, доцільно визначити її функціональну залежність від завдань захисту інформації, суб'єктів інформаційних процесів, загроз безпеки, рівнів вразливості інформаційних систем, джерел інформації, джерел загроз, способів захисту, напрямів захисту, цілей захисту:

Роботи із впровадження СУІІБ нами пропонується проводити у декілька етапів: обстеження об'єкту; розробка процедур та процесів системи управління, написання відповідних документів; впровадження СУІІБ; впровадження АС моніторингу й управління інцидентами ІБ.

Проведений аналіз вітчизняного ринку програмних продуктів для оброблення подій дозволив визначити один із кращих СУІІБ – netForensics nFX Open Security Platform. Система netForensics призначена для роботи з гетерогенним середовищем продуктів забезпечення ІБ і реалізує безперервний збір, обробку та відображення подій безпеки. Система може працювати на платформах Windows, Linux або Solaris, використовуючи в якості сховища даних повнофункціональну СУБД Oracle.

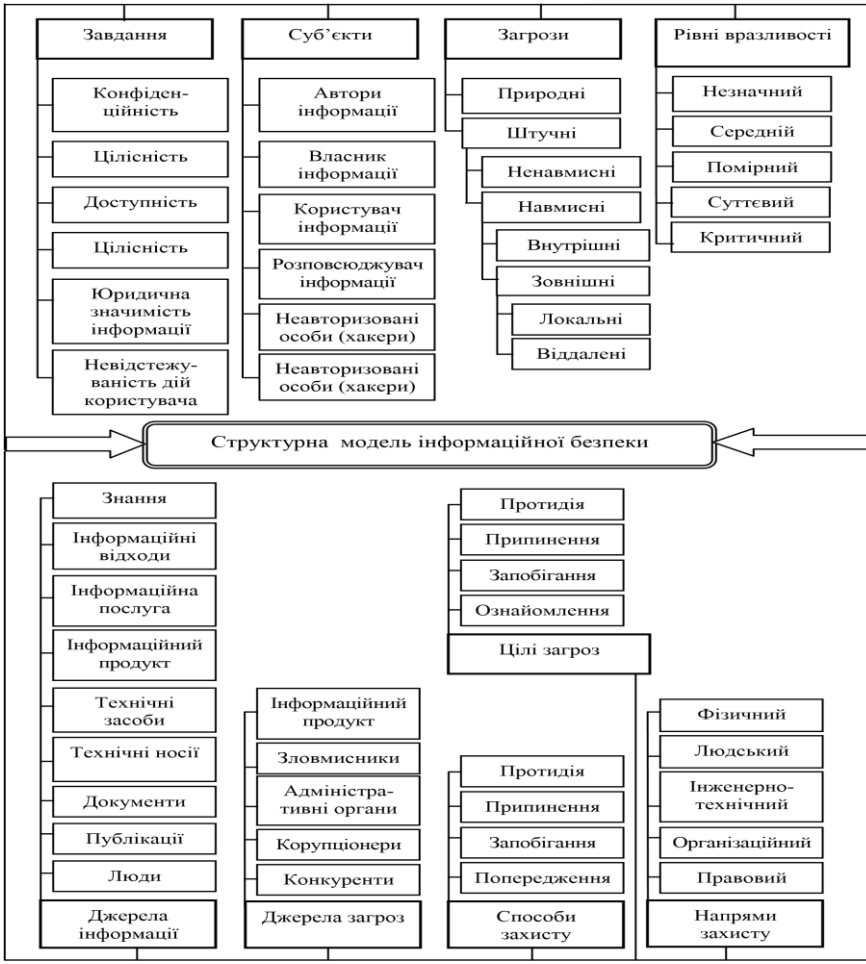


Рисунок 1 – Структурна модель інформаційної безпеки систем розподіленого типу

Отже, запропонована вдосконалена структурна та математична модель управління інцидентами інформаційної безпеки надала можливість побудувати ефективну систему захисту інформації, застосувати адекватні засоби і методи безпеки на всіх рівнях інформаційних процесів. Розроблені та обґрунтовані практичні рекомендації з побудови та функціонування систем управління інцидентами інформаційної безпеки сприятимуть підвищенню ефективності управління інцидентами інформаційної безпеки підприємств.

Інформаційні джерела

1. Драб Ю. Основні підходи до побудови системи управління інформаційною безпекою / Ю.Драб, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.29–32).

2. Малькевич Р. Проблеми забезпечення безпеки інформації підприємства в умовах пандемії / Р. Малькевич, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.69–72).

3. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – [Чинний від 2010-07-01]. – К.: Національний банк України 2010. – 163 с. – (Галузевий стандарт України).

УДК: 004.05

ПОТЕНЦІЙНІ ВРАЗЛИВОСТІ БРАНДМАУЕРА

Богдан Філіпчук, Ростислав Ткачук, Тарас Репетило

Кафедра управління інформаційною безпекою
Львівського державного університету безпеки життєдіяльності,
м. Львів, Україна

Анотація. *У роботі розглядається проблеми налаштування та використання брандмауера (міжмережевого екрану). Описані основні потенційні проблеми користувачів, які пов'язані із вразливостями брандмауера. Запропоновані базові рекомендації щодо захисту інформації від несанкціонованого проникнення через брандмауер.*

Ключові слова: *міжмережевий екран, фаєрвол, брандмауер, інформаційний захист, інтернет.*

Abstract. *The work considers the problems of configuring and using a firewall (internet screen). Describes the main potential user problems that are related to firewall vulnerabilities. Basic recommendations for protecting information from unauthorized access through the firewall are offered.*

Keywords: *internet screen, firewall, information protection, Internet.*

Інтенсивний розвиток та широке використання віртуального середовища у різних сферах діяльності передбачає: збереження, опрацювання та використання великих обсягів інформації. Досить часто ця інформація носить конфіденційний характер, а частина її стосується критичних сфер діяльності, які пов'язані з промисловою, фінансовою, енергетичною та

іншими сферами діяльності. Загрози можуть становити велику низку проблем пов'язаних не тільки з фінансовими втратами, але й з репутаційними. Брандмауери – це один із інструментів, які використовують організації та окремі особи для захисту від кібератак і підтримки контролю над своєю системою [1–3].

Брандмауери вперше почали використовувати ще двадцять п'ять років тому. Вперше їх використовували як початкову лінію захисту в мережевій безпеці. На даний момент вони все ще дуже корисні з точки зору підвищення безпеки комп'ютера, який підключено до таких мереж, як Інтернет або локальної мережі. Брандмауер – це система безпеки, створена для ізоляції внутрішньої мережі від Інтернету з метою захисту від шкідливого Інтернет-трафіку. Брандмауери здійснюють моніторинг і контроль усього вхідного та вихідного трафіку на основі певних правил. Ці правила визначатимуть, чи дозволено певному Інтернет-трафіку дістатися до місця призначення чи блокувати та обмежувати доступ. Брандмауер може бути апаратним, програмним чи комбінованим. Завдяки брандмауеру організація може захистити свою мережу від атак та контролювати трафік користувачів чи певних підмереж, що добре забезпечує внутрішню комунікацію (рис. 1). Брандмауер може використовуватися окремими особами для захисту свого комп'ютера, так як це відбувається у випадку із Windows Defender [4]. Його також можна використовувати у великому масштабі, як це відбувається у випадку Великого китайського брандмауера, який використовується для моніторингу веб-трафіку тих, хто живе в Китаї.

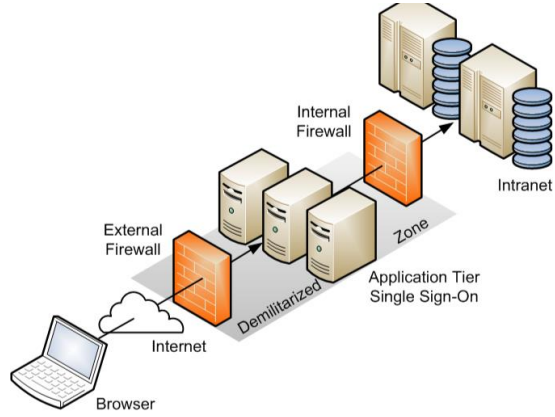


Рисунок 1 – Типова конфігурація під'єднання до мережі із використанням каскаду брандмауерів

Оскільки брандмауери захищають комп'ютерну мережу, вони часто стають суттєвою перепоною для співробітників, яким важко отримати доступ до обраних ними сайтів, таких як потокові сервіси, платформи соціальних мереж тощо.

Зашифровані ін'єкційні атаки зазвичай здійснюються за допомогою фішингових листів. Такі електронні листи обманюють користувачів, зму-

шуючи їх переходити за певним посиланням, яке вводить зашифрований код у комп’ютер. Це може бути звичайне зловмисне програмне забезпечення, шкідливе програмне забезпечення без файлів або будь-який бекдор для доступу до даних [5–6]. Фішингові посилання також можуть запитувати користувачів облікові дані для входу (або іншу конфіденційну інформацію) і пересилати зашифровані чутливі дані. Старі програмні системи не здатні належним чином перевіряти та фільтрувати зашифрований трафік. Але й навіть найновіші моделі брандмауерів із підтримкою DPI, що з великою ймовірністю впораються із шкідливим трафіком, можуть проігнорувати загрози, які відносяться до типу “нульового дня” [7].

SQL-ін’єкція – це метод, за допомогою якого зловмисники оминають брандмауер системи користувача або бази даних, впроваджуючи шкідливий код (команди) SQL. Це найпоширеніший метод веб-злому, який використовується зловмисниками. Завдяки атакам з використанням SQL-ін’єкцій зловмисники можуть отримати «чутливі» дані користувача, які є в базі даних, наприклад, інформацію про кредитну картку. Зловмисники також можуть змінювати, видаляти чи шифрувати дані. Вони розробляють інструкції SQL для обходу баз даних або брандмауерів користувачів систем. Зловмисники застосовують цю шкідливу інструкцію SQL, коли веб-сервер взаємодіє із сервером бази даних.

Некоректно налаштоване програмне забезпечення чи сервер може призвести до витоку трафіку в обхід брандмауеру, тому навіть при наявності сучасних систем захисту суттєве значення має конфігурація налаштувань правил обміну даними та під’єднаними сервісами. Зловмисники досліджують налаштування системи, виявляють слабкі місця, в тому числі, і пов’язані з налаштуваннями мережі та використовують їх у своїх цілях [8]. Тому є дуже важливо своєчасно виправляти будь-які програмні помилки чи гіпотетичні вразливості, щоб захистити систему від несанкціонованого проникнення.

Як уже не раз зазначалося, традиційні засоби, до яких можна віднести і міжмережеві екрани, були побудовані на основі моделей, розроблених в той час, коли мережі не отримали широкого розповсюдження і способи атак на ці мережі не були так розвинені, як зараз. Щоб на належному рівні протидіяти цим атакам, необхідно застосування нових технологій. А особливо тих що стосуються персоналу компаній, адже найбільша загроза, нажаль і на сьогодні, стосується людського фактору.

Щоб підняти рівень безпеки в організації, захистити її від можливих мережних атак з її персоналом потрібно проводити регулярні навчання,

оновлювати конфігурацію сервера, програмне забезпечення та операційну систему, ніколи не відкривати вкладення в електронних листах від невідомих відправників та уникати завантаження різних типів невідомих файлів, таких як архівні файли (.zip, .rar) і т.д., оскільки зловмисники приховують шкідливий код у файлах з таким розширенням.

Висновки. Міжмережеві екрани не забезпечують достатнього рівня захищеності корпоративних мереж. Хоча ні в якому разі від них не можна відмовлятися. Вони забезпечують необхідний, але нажаль недостатній рівень захисту корпоративних мереж.

Інформаційні джерела

1. Філіпчук Б. Ю., Ткачук Р. Л. Захист персонального комп'ютера від шкідливого програмного забезпечення. Зб. наук. праць Всеукраїнської науково-практичної конференції з міжнародною участю. "Актуальні проблеми пожежної безпеки та запобіганням надзвичайним ситуаціям в умовах сьогодення". – Львів: ЛДУ БЖД, 2022. С. 478–481.

2. Захист даних за допомогою брандмауерів нового покоління [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/347901156_Data_protection_by_means_of_firewalls_of_new_generation

3. Брандмауер [Електронний ресурс] – Режим доступу до ресурсу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/brandmauer/

4. Windows Defender [Електронний ресурс] – Режим доступу до ресурсу: https://www.microsoft.com/uk-ua/windows/comprehensive-security

5. Мельцов В. В., Ткачук Р. Л. Організація захисту сайту створеного за технологіями: MONGODB, ANGULAR 12, HTML5, CSS3, JAVASCRIPT, NESTJS. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції "Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України" (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М. П. Драгоманова, 2022. С. 84–85.

6. Шахуб С. М., Ткачук Р. Л. Дослідження методів і засобів при запроваджені концепції BYOD на підприємстві. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції "Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України" (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М. П. Драгоманова, 2022. С. 149–150.

7. Загальні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення. [Електронний ресурс] – Режим доступу до ресурсу: https://cert.gov.ua/recommendation/2502

8. Впровадження систем firewall [Електронний ресурс] – Режим доступу до ресурсу: https://studfile.net/preview/6214746/page:6/

Напрям 4

БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ

УДК: 378.004

THE GROWTH OF CLOUD COMPUTING IN THE EDUCATIONAL PROCESS UNDER TODAY'S CONDITIONS

Ulyana Panovyk[1], Amiran Sharadze[2]

[1]Department of Automation and Computer Technologies of the Ukrainian Academy of Printing, Lviv, Ukraine
[2]Batumi Shota Rustaveli State University, Batumi, Georgia

Abstract. *Today in Ukraine, the urgent issue of distance learning is training qualified specialists in various specialties. The article examines the problems and prospects of using cloud technologies and services in the educational process. Examples and advantages of well-known cloud platforms used in education are considered.*

Keywords: *cloud technologies, cloud services, cloud platforms, cloud storage, virtual computer laboratory.*

Анотація. *Сьогодні в Україні важливим питанням при дистанційному навчанні є підготовка кваліфікованих фахівців різних спеціальностей. У статті досліджуються проблеми та перспективи використання хмарних технологій та сервісів у навчальному процесі. Розглядаються приклади та переваги відомих хмарних платформ, які застосовуються в освіті.*

Ключові слова: *хмарні технології, хмарні сервіси, хмарні платформи, хмарні сховища, віртуальна комп'ютерна лабораторія.*

During the coronavirus pandemic and the military aggression of the Russia against Ukraine, the education system of Ukraine found itself in new realities of functioning, and the organizers of the educational process faced such questions that no one has solved until today. Today's realities have shown that the education system needs the introduction of innovative teaching styles. Technology, especially cloud computing technologies such as cloud tools and cloud storage options, should play a greater role in student learning. Educational institutions should use cloud computing and cloud communications. Only by using the modalities of virtual interaction, educational institutions will be able to remain relevant. Higher education especially needs the use of cloud technologies and virtual (electronic) learning.

Today, cloud computing and e-learning have become more important than at any time in recent history. Educational institutions introduce online learning for students. Online engineering and programming courses are also becoming

increasingly popular. Technology is a tool and catalyst for educational change, solving today's problems. Cloud computing offers the benefits of increased efficiency for both educators and students (Fig. 1).

When using cloud technology in the educational process, all types of services can be used – IaaS, PaaS, and SaaS. The most famous in the world are free cloud platforms Microsoft Live@edu, Google Apps Education Edition, and cloud services based on them [1].

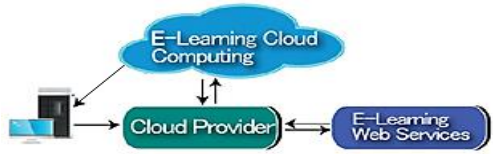


Fig. 1. Architecture of e-learning

Cloud platforms Microsoft Live@edu, and Microsoft Office 365 provide opportunities for the practical study of well-known office applications through a web browser based on cloud technologies. These tools include a set of functions such as the use of e-mail, a calendar, a web conferencing service with the possibility of video communication, the presence of a virtual whiteboard and compatible access to the desktop; creating and maintaining your own website; creation and editing of Word, PowerPoint, Excel, OneNote documents of any complexity. Open access to office applications is possible when using the free SkyDrive cloud file storage.

The main tools that students and teachers can use when using the Google Apps Education Edition cloud platform are Gmail e-mail with Google Talk and video chat; Google calendar; Google Drive; Google Docs; Google sites. Google Apps Education is constantly expanding services for educational institutions, namely additional services are Apps Marketplace; Google Moderator; Google Apps application script (JavaScript cloud scripting language for task automation), etc [2].

Another option for developing your online educational applications is to use the Microsoft Windows Azure cloud platform,: local development environment, Windows Azure computing emulator, Windows Azure storage, Microsoft SQL Azure service of relational databases, Windows Azure Connect interface for configuration of secure IPsec connections, Windows Azure service bus for data exchange, Windows Azure Access Control cloud service for authentication and authorization, Windows Azure Content delivery network, Windows Azure cache service, connection to the Windows Azure Marketplace online store. The most important component of the Windows Azure cloud platform for the development of educational applications is a local development environment with the possibility of using Visual Studio, Java programming languages [3].

The most famous cloud storages are SkyDrive, Apple iCloud, Google Drive, Dropbox, and others. Students can use Apple iCloud cloud storage as storage for any files transferred from Apple devices to remote Apple servers. The iCloud cloud service allows you to use the calendar to plan events and remind them, edit

documents with an automated backup function, use mail, etc.The advantage of SkyDrive cloud storage is the integration with Microsoft Office Web Apps, which enables users of SkyDrive cloud storage to study Word, Excel, PowerPoint, and OneNote office applications in a browser window.

For universities, there is an opportunity to create a private cloud (private cloud) and an educational cloud (educational cloud). Private cloud and educational cloud provide access to remote processors, software and data storage (resources), and infrastructure. However, the private cloud is the space of one university, and the educational cloud combines universities with their resources into one single space.

Well-known manufacturers of IT services offer certain cloud services for educational purposes: Blue Cloud from IBM – tools for supporting data migration from traditional IT infrastructure to the cloud called IBM Cloud Academy; App Engine from Google that is the Google Apps for Education program to support educational institutions; Microsoft Windows Azure that is the cloud solutions for educational institutions.

A separate direction in the application of cloud technologies is the use of virtual computing laboratories (VCL). A virtual computer lab is a technology that is used to deploy distributed small data centers and IT services for educational institutions to support the collaborative work of a team of programmers on code development. Currently, cloud versions of well-known manufacturers of service providers are appearing, including Sage MathCloud, Maple, MATLAB, Maple Net, MATLAB web server, WebMathematica, Calculation Laboratory, etc.

Conclusions. The implementation of cloud technologies in education has special advantages: cloud services provide the possibility of instant processing of huge amounts of information with low cost of computing resources and the possibility of its instant distribution and exchange of analysis results; cloud technologies create an opportunity for continuous learning with the support of mobile technologies and make the learning process itself interactive; cloud technologies make it possible to conduct interactive online counseling of students with the teacher and instantly receive answers to their questions; cloud technologies make it possible to save data in the clouds without the need to transfer them from one device to another, i.e., there is hardware independence from the equipment.

It is unclear how long and to what extent e-learning will be a part of higher education. It is necessary to find new ways of spreading knowledge. These alternative pathways must be able to cross borders and reach all parts of society.

Інформаційні джерела

1. Baharuddin et al. (2021). Implementation of cloud computing system in learning system development in engineering education study program. IJEMST, 9(4), 728–740.

2. Google for Education. [online] Available at: https://cloudfresh.com/ua/produkty/google-for-education/ (accessed October 15, 2022).

3. Platform Microsoft Azure [online] Available at: https://techexpert.ua/it-products/platforma-microsoft-azure/ (accessed November 10, 2022).

УДК 004.75

БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ

Владислав Горон[1], Орест Полотай[2], Уляна Пановик[2]

[1]Кафедра безпеки інформаційних технологій Національного університету "Львівська політехніка", м. Львів, Україна
[2]Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Описано хмарні сховища, типи хмар та способи захисту інформації в марних сховищах.*
Ключові слова: *хмарні сховища, хмарна безпека.*

Abstract. *Describes cloud storage, types of clouds and ways to protect information in useless storage.*
Keywords: *cloud storage, cloud security.*

Хмарне сховище – це модель комп'ютерного сховища даних, у якій цифрові дані зберігаються в логічних пулах, які називаються "хмарою". Фізичне сховище охоплює кілька серверів, а фізичне середовище, як правило, належить і керується хостинговою компанією.

Зазвичай використовуються три типи хмар:

1. Громадські хмари – це хмарні ресурси, такі як обладнання, сховище та мережеві пристрої, належать і керуються стороннім постачальником хмарних послуг і надаються через інтернет.

2. Приватні хмари – використовуються виключно однією організацією та можуть бути фізично розташовані в локальному центрі обробки даних або розміщені стороннім постачальником хмарних послуг.

3. Гібридні хмари – це поєднання приватної хмари з публічною хмарою. У гібридній хмарі дані та програми можуть переміщатися між приватною та загальнодоступною хмарами для більшої гнучкості та додаткових можливостей розгортання.

В наш час людям набагато зручніше користуватися хмарними сховищами. Вони не займають зайве місце, до них легко доступитися в любий момент, потрібен тільки Інтернет. Також компаніям краще використовувати хмари, тому що легше виділити місце у хмарі, а між зберігати дані, наприклад, на флешках або дисках. Тому все більше і більше компаній задумують над тим як покращити безпеку інформації у хмарних сховищах.

Хмарна безпека – це набір політик, технологій, програмного забезпечення та програм, які захищають ваші дані, що зберігаються не на вашому комп'ютері, а в Інтернеті.

Хмарна безпека є дуже важливою, тому що все більше і більше інформації зберігається у хмарі і це дає можливість зловмисникам отримати її, якщо хмара є недостатньо захищеною. Якщо дехто зберігає в хмарі тільки свої сімейні фотографії і відео, щоб вони не займали місце на комп’ютері і втрата таких даних не буде критичною, то компанії зберігають свої документи і важливі дані своїх працівників, втрата цих даних може призвести до великих фінансових втрат.

Так як зараз багато роботи робиться дистанційно, то ризики викрадення інформації з хмари збільшуються. В таких випадках безпека мобільних пристроїв має особливе значення. В компанії може бути прекрасний захист системи, але якщо працівник має можливість зайти в систему зі свого пристрою, то ризик викрадення інформації є дуже великим. Для таких випадків є політика Bring-Your-Own-Device (BYOD. Це політика, згідно з якою співробітникам дозволено або рекомендується використовувати особисті мобільні пристрої (телефони, планшети, ноутбуки) для доступу до корпоративних даних та систем, але вони мусять дотримуватися певних правил для того, щоб зменшити ризик викрадення інформації.

Є декілька способів покращення безпеки хмари:

1. Підключення багатофакторної автентифікації (MFA). З кожним днем зловмисники знаходять все нові і нові способи отримати доступ до вашого аккаунту. Тому зараз комбінації імені користувача та пароля недостатньо. MFA є одним із найдешевших, але найефективніших засобів контролю безпеки, які запобігають доступу потенційних хакерів до ваших хмарних програм.

2. Керувати доступом користувачів, щоб покращити безпеку хмарних обчислень. Більшості співробітників не потрібен доступ до кожної програми, кожної інформації чи кожного файлу у вашій хмарній інфраструктурі. Встановлення відповідних рівнів авторизації гарантує, що кожен співробітник може переглядати або маніпулювати лише тими програмами чи даними, які необхідні йому для виконання роботи.

3. Відстежування дій кінцевих користувачів за допомогою автоматизованих рішень для виявлення зловмисників. Моніторинг у режимі реального часу та аналіз дій кінцевих користувачів можуть допомогти вам виявити порушення, які відрізняються від звичайних шаблонів використання, наприклад, вхід із раніше невідомої IP-адреси або пристроїв.

4. Створення комплексного процесу виходу працівника з системи. Коли співробітники залишають вашу компанію, переконайтеся, що вони більше не мають доступу до вашого хмарного сховища, систем, даних, інформації про клієнтів та інтелектуальної власності.

5. Регулярне проведення навчань співробітників із захисту від фішингу. Хакери можуть отримати доступ до захищеної інформації, викравши облікові дані співробітників за допомогою методів соціальної

інженерії, таких як фішинг, підробка веб-сайтів і шпигунство в соціальних мережах. Пропонувати постійне навчання – найкращий спосіб запобігти тому, щоб співробітники стали жертвами цих шахраїв і скомпрометували конфіденційні дані вашої компанії.

Як підсумок можна сказати, що хмарне середовище є дуже зручним і на сьогоднішній день захищеним, але немає гарантії, що ваші дані захищені на всі сто відсотків, тому що хакери кожен раз придумують щось нове для того, щоб отримати персональну інформацію працівників. Також кожен працівник мусить дотримуватися певних правил для того, щоб зменшити ризики витоку даних. Компанія може мати дуже хороший захист, але якщо їх працівники не дотримуються правил безпеки, то хакери зможуть обійти любий захист.

Інформаційні джерела

1. Стаття “Cloud storage” на сторінці вікіпедії – https://en.wikipedia.org/wiki/Cloud_storage.

2. Belej O., Nestor N., Panchak S., Polotai O.I. Developing a Model of Cloud Computing Protection System for the Internet of Things. 2020 IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 – Proceedings, 2020, pp. 53–58.

УДК 514.18:004.056

ЗБЕРЕЖЕННЯ КРЕСЛЕНИКІВ У ВЕКТОРНІЙ ГРАФІЦІ

Олена Гумен, Ірина Селіна, Артем Василенко

Національний технічний університет України
Київський політехнічний інститут імені Ігоря Сікорського, Київ, Україна

Анотація. *Необхідність забезпечення збереження інформації, зокрема креслеників та інших документів, є наразі дуже актуальною. Все ширше застосування набувають для цього хмарні сховища. Головною перевагою векторної графіки є можливість зміни розмірів зображення без втрати якості картинки, що значно спрощує роботу з графікою і підвищує якість кінцевого результату.*

Ключові слова: *векторна графіка, хмарні документи, кресленики.*

Abstract. *The need to ensure the preservation of information, in particular blueprints and other documents, is currently very urgent. Cloud storage is increasingly used for this purpose. The main advantage of vector graphics is the ability to change the size of the image without losing image quality, which greatly simplifies work with graphics and improves the quality of the final result.*

Keywords: *vector graphics, cloud documents, drawings.*

Векторна графіка – це спосіб зображення об’єктів у комп’ютерній графіці, що базується на математичному описі елементарних геометричних об’єктів, які зазвичай називають примітивами, наприклад, сплайни, криві Без’є, кола, еліпси, багатокутники [1, 2].

Коли виконано кресленик, є необхідність його збереження для того, щоб не відбулася втрата даних за виникнення непередбачуваних ситуацій, наприклад, при збої живлення. Працюючи з кресленником, рекомендується періодично зберігати його. Так, у AutoCAD збереження файлів креслеників відбувається у .dwg, і якщо користувач не змінить формат файла, в котрому зберігаються кресленики, вони зберігатимуться в останньому заданому форматі файла кресленика. Цей формат має високий ступінь стиснення і добре підходить для роботи в мережі. Довжина імені файлу .dwg не може перевищувати 256 символів.

Для збереження кресленика також використовуються команди Block Palette (блокова палітра) (рис. 1).

Рисунок 1 – Блокова палітра AutoCAD

Команда BLOCK у AutoCAD дуже значущий інструмент, що дозволяє на основі даних об’єктів створювати інший об’єкт (блок), зберігати його під вказаним іменем і потім знову вставляти в кресленик. Крім того, ці блоки, що вставляються, можна масштабувати окремо по осі *x* і по осі *y,* а також повертати на певний заданий кут. Це подібно до трафарету або шаблону. При цьому його можна трансформувати такими командами як MOVE, COPY, ERASE, ROTATE, ARRAY, MIRROR, і він сприймається програмою, як окрема одиниця. Блоки можна експортувати і зберігати, також з них можна створювати бібліотеки і використовувати в інших кресленнях. Все це значною мірою спрощує роботу з кресленнями.

Крім зазначеної вище, є й інші програми для векторної графіки, серед яких CorelDRAW, Adobe Illustrator, Adobe Fireworks та інші [3]. У всіх програмах зображення складаються із відрізків прямих ліній, фігур і інших компонентів зображення. Збереження векторних зображень здійснюють не лише в DWG (для AutoCAD), але і в наступних векторних форматах файлів для інших програм, а саме: EPS, SVG, AL (рис. 2).

При використанні векторних даних зображення зберігається в пам’яті як база даних описів примітивів – точка, пряма, крива Без’є, коло, еліпс, багатокутник. А ще збереження файлів можна проводити у хмарі [4].

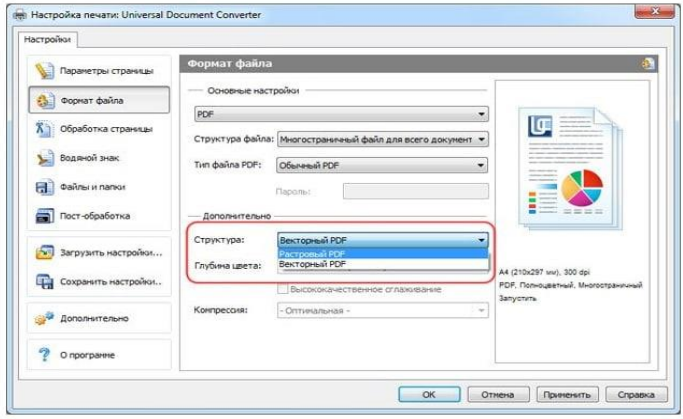


Рисунок 2 – Керування хмарними документами Illustrator

Хмарні документи зберігаються з розширенням .aic і відображаються із символом хмари на вкладці з назвами документів, за яким їх можна легко відрізнити від локально збережених документів (рис. 3). Хмарні документи зберігаються автоматично під час роботи. Завдяки цьому забезпечується доступ до актуальної версії хмарного документа на будь-якому пристрої, на якому встановлено відповідну програму.

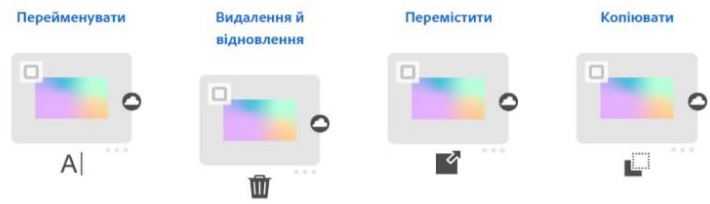


Рисунок 3 – Керування хмарними документами Illustrator

Головною перевагою векторної графіки є можливість зміни розмірів зображення без втрати якості картинки. Це значно спрощує роботу з графікою і підвищує якість кінцевого результату.

Інформаційні джерела

1. Графічний дизайн і реклама на комп'ютері. Векторна графіка. https://www.williamspublishing.com.
2. Векторна графіка. uk.wikipedia.org/wiki/Векторна_графіка.
3. Adobe Illustrator. helpx.adobe.com/ua/illustrator.html.
4. Cloud documents and how to use them / Adobe Creative Cloud. https://youtu.be/CwRjUnWxfhg.

УДК 004.738.5

ОСНОВНІ ПРОБЛЕМИ БЕЗПЕКИ ХМАРНОЇ ІНФРАСТРУКТУРИ

Назарій Дацків, Орест Полотай

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Перераховано типи хмарних сервісів. Описано різні класифікації загроз безпеки інформації сервісів хмарної інфраструктури.

Ключові слова: *хмарна інфраструктура, бепека інформації, загрози.*

The types of cloud services are listed. Various classifications of information security threats of cloud infrastructure services are described.

Keywords: *cloud infrastructure, information security, threats.*

Хмарні обчислення – це надання обчислювальної техніки, де надаються широкомасштабовані можливості на основі IT, як послуги для клієнтів Інтернету. Цей термін ефективно зосереджує різні аспекти парадигми хмарних обчислень, які можна знайти на різних рівнях інфраструктури. Існує три типи послуг, що надаються архітектурою хмарних обчислень, а саме SaaS, PaaS, IaaS (рис. 1).

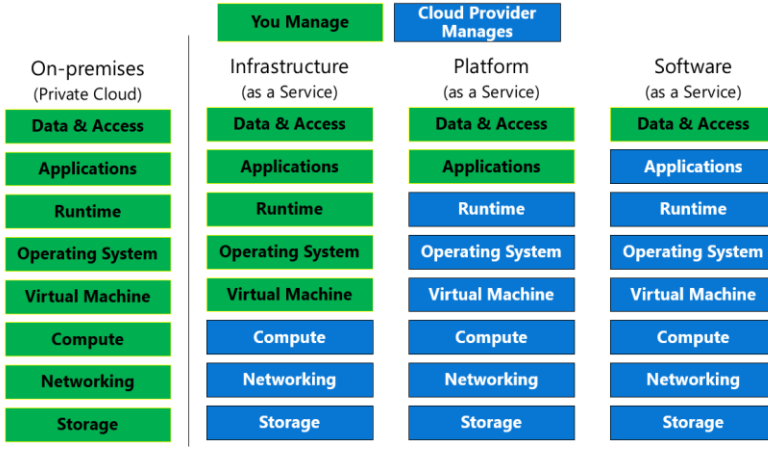


Рисунок 1 – Типи хмар

Основною перевагою такого роду послуг є те, що вони замінюють капітальні витрати на операційні (парадигма низької вартості). AWS надає масштабовану, надійну та недорогу інфраструктуру в хмарі, яка

забезпечує тисячі компаній по всьому світу. AWS надає обчислювальні послуги та різні інші послуги, які допомагають розвивати організацію. Служби засновані на кількох протоколах, таких як протоколи HTTP, REST і SOAP.

Проблема безпеки зіграла важливу роль у перешкоджанні прийняття хмарних обчислень. У хмарі можливі різні проблеми безпеки, такі як:

− угода про рівень обслуговування (SLA);
− шифрування даних;
− управління та безпека хмарних даних;
− міграція віртуальних машин;
− сумісність;
− контроль доступу;
− енергетичний менеджмент;
− багатоквартирне користування (multi-tenancy);
− консолідація серверу;
− надійність та доступність послуги;
− управління платформою.

Хмара керується угодою про рівень обслуговування, яка дозволяє за потреби реплікувати декілька екземплярів однієї програми на кількох серверах; це залежить від схеми пріоритетів. Специфікація SLA краще відображає потреби клієнтів, якщо вони вирішують потрібну проблему в потрібний момент.

Шифрування – це ключова технологія безпеки даних. Наприклад, API веб-сервісів, які ми використовуємо для доступу до хмари, програмно або з клієнтами, записаними на ці API, забезпечують шифрування SSL для доступу, це зазвичай вважається стандартом.

Управління хмарними даними є важливою темою дослідження в хмарних обчисленнях. Оскільки постачальники послуг зазвичай не мають доступу до системи фізичної безпеки центрів обробки даних, вони повинні покладатися на постачальника інфраструктури для досягнення повної безпеки даних.

Основна перевага міграції віртуальних машин полягає в уникненні гарячих точок, однак це непросто. Віртуалізація може забезпечити значні переваги в хмарних обчисленнях, дозволяючи міграцію віртуальних машин збалансувати навантаження в центрі обробки даних. Крім того, міграція віртуальних машин забезпечує надійне та високочутливе надання в центрах обробки даних.

Сумісність – це здатність двох або більше систем працювати разом, щоб обмінюватися інформацією та використовувати цю інформацію.

Відсутність інтеграції між цими мережами ускладнює для організацій об’єднання своїх IT-систем у хмарі та досягнення підвищення продуктивності та економії витрат.

Існує ряд типів хмарних додатків, до яких користувач може отримати доступ через Інтернет, від невеликих інтернет-віджетів до великих корпоративних програм, які мають підвищені вимоги до безпеки залежно від типу даних, що зберігаються в інфраструктурі постачальника програмного забезпечення. Ці запити додатків вимагають багатоквартирного користування з багатьох причин, найголовнішою є вартість. Для багатоорендного прикладного рівня ресурси розподіляються на кожному рівні інфраструктури та мають серйозні проблеми з безпекою та продуктивністю.

Консолідація серверів – це ефективний підхід для максимального використання ресурсів при мінімізації споживання енергії в середовищі хмарних обчислень. Збільшене використання ресурсів і зниження потреби в живленні й охолодженні, досягнуті завдяки консолідації серверів, тепер поширюються на хмару.

Надійність виявляється, коли хмарний постачальник надає програмне забезпечення на вимогу як послугу. Більшість програмного забезпечення забезпечує якість надійності, тому користувачі можуть отримати до нього доступ за будь-яких умов мережі. Через ненадійність програмного забезпечення на вимогу виявлено кілька випадків. Наприклад: хмарна служба Apple MobileMe, яка зберігає та синхронізує дані на кількох пристроях.

Одна з найважливіших частин хмарних платформ надає розробникам різного роду платформу для написання програм, які працюють у хмарі, або використовують послуги, що надаються з хмари, або і те, і інше. Існує багато проблем із забезпеченням можливостей проміжного програмного забезпечення для створення, розгортання, інтеграції та керування додатками в багатоорендному, еластичному та масштабованому середовищі.

Популярними цілями хакерів при атаці на хмари є:

– Незаконний майнінг. Хакери використовують обчислювальну потужність хмар для майнінгу криптовалют, що буде досить дорого коштувати підприємству, оскільки рахунок сервіс-провайдер направить саме йому.

– E-skimming. Хакери отримують доступ до веб-додатків підприємства для введення зловмисного коду, який збирає фінансову інформацію.

– Несанкціонований доступ (НСД), що призводить до модифікації, порушення, втрати чи ексфільтрації. Цілі різні – від доступу до баз даних про клієнтів (потім їх продають у даркнеті) до викрадення інформації, що становить комерційну таємницю.

Підсумовуючи, всі загрози безпеки технологій хмарної інфраструктури можна об'єднати в дві групи: загрози безпеки інформації для споживача хмарних послуг та загрози безпеки інформації для постачальників хмарних послуг.

Загрози безпеки інформації для споживача хмарних послуг:

− загрози безпеки інформації, пов'язані з невизначеністю відповідальності;

− загрози безпеці інформації, пов'язані з втратою управління;

− загрози безпеки інформації, пов'язані з втратою довіри;

− загрози безпеки інформації, пов'язані з здійсненням НСД з боку споживачів хмарних послуг;

− загрози безпеки інформації, пов'язані з недоліком управління хмарними ресурсами;

− загрози, пов'язані зі зловживаннями з боку споживачів хмарних послуг.

Загрози безпеки інформації для постачальників хмарних послуг:

− загрози, пов'язані з невизначеністю при розподілі відповідальності;

− загрози, пов'язані з неузгодженістю політик безпеки;

− загрози, пов'язані з використанням технологій віртуалізації.

Інформаційні джерела

1. Belej O., Nestor N., Panchak S., Polotai O. Developing a Model of Cloud Computing Protection System for the Internet of Things. International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020. 2020. Article ID 9109456. P. 53–58.

2. Нікішин Д., Федюшин О. Ризики інформаційної безпеки в хмарних сервісах. "Global Cyber Security Forum 2019" 14 – 16 листопада 2019, Харків, Україна. С. 80–81.

3. Документ України щодо обробки інформації в системах хмарних обчислень [Електронний ресурс] – Режим доступу з: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=58527

4. Хмарна безпека: ключові поняття, загрози та рішення. [Електронний ресурс] – Режим доступу з: https://sgs4business.com/news/khmarna-bezpeka-kliuchovi-poniattia-zahrozy-ta-rishennia.html

УДК: 004.056.5

ЗАСОБИ ЗАХИСТУ ДАНИХ У ВЕБ-СИСТЕМАХ

Валерій Клочков, Андрій Вахула, Ігор Горак

Кафедра електронних обчислювальних машин
Національного університету "Львівська політехніка", м. Львів, Україна

Анотація. *У цій роботі аналізуються можливі загрози для комп'ютерних мереж і способи їх захисту за допомогою технологій VPN. Розглянуто питання несанкціонованого доступу до мережі, кілька методів і засобів захисту від зловмисників. Наведено типові загрози комп'ютерним мережам, проведено аналіз особливостей методів і технологій захисту. Результати дослідження можуть бути використані для прийняття обґрунтованих рішень щодо вибору методів захисту для мереж різного призначення та з різними вимогами до захисту інформації.*

Ключові слова: *безпека, веб-системи, TCP/IP, VPN.*

Abstract. *This paper analyzes possible threats to computer networks and ways of securing them using VPN technologies. The issue of unauthorized access to the network was considered, several methods and means of protection against intruders were selected. threats to computer networks are given, and an analysis of the features of protection methods and technologies is carried out. The results of the study research can be used to make informed decisions about the choice of protection methods for networks of different purposes and with varying requirements for information protection.*

Keywords: *security, web systems, TCP/IP, VPN.*

З ростом глобальної мережі зростає і кількість її користувачів. І чим більше користувачів, тим більше людей хочуть отримати вигоду від публічності Інтернету. Використання публічного каналу інформації стає небезпечнішим, ніж будь-коли.

Згідно з попереднім дослідженням OWASP, проведеним у 2021 році [1], існує десять найбільш критичних ризиків для безпеки веб-додатків:

− порушений контроль доступу;
− криптографічні збої;
− ін'єкція;
− небезпечний дизайн;
− неправильна конфігурація безпеки;
− вразливі та застарілі компоненти;
− помилки ідентифікації та автентифікації;
− порушення цілісності програмного забезпечення та даних;
− помилки реєстрації та моніторингу безпеки;
− підробка запитів на стороні сервера.

Усі описані загрози значно впливають на веб-сервіси, тому розробники та власники намагаються мінімізувати ризики. За останні десять років було досягнуто значного прогресу. Більшість веб-сервісів почали викорис-

товувати протокол HTTPS замість старого HTTP. Це допомагає безпечно та надійно передавати дані між службами та користувачами.

У протоколі TCP/IP інформація передається у вигляді послідовності дейтаграм. Одне повідомлення може передаватися як серія дейтаграм, які збираються в повідомлення в місці отримання.

Верхній рівень TCP/IP включає протокол HTTPS. HTTPS розшифровується як Hyper Text Transfer Protocol Secure. Це розширена та безпечна версія HTTP [2]. Це дозволяє створювати багато безпечних транзакцій, шифруючи весь зв'язок за допомогою SSL. За своєю суттю HTTPS є комбінацією протоколів SSL/TLS і HTTP. Він забезпечує зашифровану та безпечну ідентифікацію мережевого сервера (рис. 1).

HTTPS також дозволяє створити безпечне зашифроване з'єднання між сервером і браузером. Він забезпечує двосторонню безпеку даних. Це допоможе захистити потенційно конфіденційну інформацію від крадіжки.

У HTTPS транзакції SSL узгоджуються за допомогою алгоритму шифрування на основі ключа. Ці ключі, які використовують принцип факторизації, зазвичай мають 64 або 128 біт [3]. Деякі транзакції можна здійснити з посиленою безпекою та ключами 256, 512 або навіть 2048 біт (рис. 1).

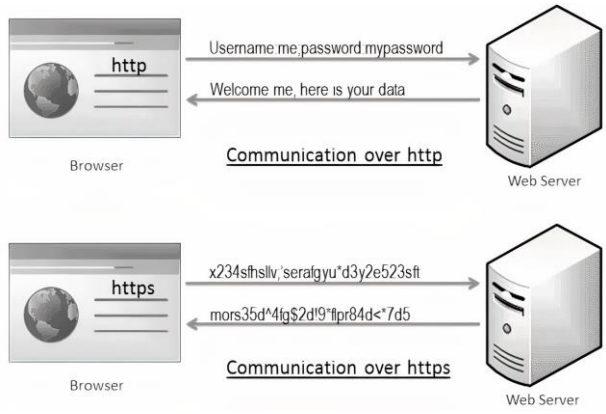


Рисунок 1 – Порівняння незахищеного HTTP та зашифрованого зв'язку HTTPS

На жаль, протоколи в стеку TCP/IP за замовчуванням не можуть забезпечити безпеку веб-служб від усіх типів атак. Хоча це дозволяє перевіряти користувачів, приховувати деякі вразливі дані та робити з'єднання більш надійним, хакери всеодно можуть викрасти деякі дані з мережі або серверів за допомогою атак, таких як ін'єкції, XSS, CRFS тощо.

Допомогти усунути це недолік може протокол VPN, який точно визначає, як система VPN взаємодіє з усіма системами в Інтернеті та рівень безпеки трафіку. Причиною є використання шифрування між двома кінце-

вими вузлами. Якщо ж інформація не захищена, зловмисник може перехопити ключі та розшифрувати трафік.

Щоб створити VPN за допомогою апаратного та програмного забезпечення, важливо дотримуватися стандартного механізму, заснованого на протоколі безпеки протоколу Інтернету (IPSec). Тут детально описано методи ідентифікації для ініціалізації тунелю та методи шифрування. Недоліками є орієнтація на використання IP-адреси.

Ще один протокол, який використовується для побудови VPN, – протокол тунелювання “точка-точка” (PPTP), переадресація рівня 2 (L2F) і протокол тунелювання рівня 2 (L2TP), який поєднує в собі два описані вище протоколи. Але вони не є комплексними і повністю функціональними.

Інший протокол Internet Key Exchange (IKE) забезпечує передачу інформації через тунель, виключаючи втручання ззовні. IKE автоматизує процес передачі ключа за допомогою механізму шифрування з відкритим ключем. IKE змінює ключ підключення і дозволяє підвищити конфіденційність інформації, яка передається. При цьому інкапсуляція забезпечує мультиплексування кількох транспортних протоколів одним каналом.

Протокол керування з’єднанням (LCP) – протокол “точка-точка” (PPP) визначає гнучкий LCP для встановлення, налаштування та перевірки з’єднання. LCP узгоджує формат інкапсуляції, розмір пакета, параметр налаштування, дії при розриві з’єднання та параметри автентифікації.

Зазвичай, для створення VPN-тунелів використовуються протоколи PPTP, L2TP, IPsec і OpenVPN.

Висновки. У результаті досліжеггя отримано опис веб-атак і рекомендації щодо захисту веб-сервісів. Аналіз сучасних загроз дав розуміння сучасних проблем безпеки. Деякі вразливості, згадані в дослідженні OWASP, можна уникнути за допомогою надійних протоколів із стеку TCP/IP, який використовує шифрування, цифровий підпис і авторизовані сертифікати. Але одним із найкращих способів захисту зв’язку є використання протоколу VPN. У процесі підготовки матеріалів були проаналізовані загальні характеристики VPN, протоколи VPN, функції та компоненти VPN, виявлені мережі VPN та проблеми їх безпеки.

Інформаційні джерела

1. OWASP Top Ten (2021). [Електронний ресурс]. – Режим доступу: https://owasp.org/www-project-top-ten/. (Перевірено: 2 жовтня, 2022).

2. HTTP Over TLS, RFC 2818, IETF (травень 2000). DOI: 10.17487/RFC2818.

3. Prasetyo, Deny; Widianto, Eko Didik; Indasari (2019). “Short Message Service Encoding Using the Rivest-Shamir-Adleman Algorithm”. Jurnal Online Informatika. 4 (1): ст 39. DOI:10.15575/join.v4i1.264.

УДК 004.056.53

МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПРОЄКТУВАННІ WEB-ДОДАТКА УНІВЕРСИТЕТУ

Катерина Пожичкевич, Валентина Ящук, Наталія Федінець

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Розглянуто теоретичні, науково-методичні та організаційно-функціональні основи захисту інформації при проєктуванні web-додатка університету. Визначено сучасні підходи до захисту інформаційної безпеки на прикладі проєктуванні web-додатка університету. Наведено методичні підходи до формування концепції та структури автоматизованої системи управління захистом інформаційної безпеки. Проаналізовано стандарти, рекомендації, етапи щодо попередження загроз інформаційної безпеки. Запропоновано модель захисту веб-додатку від хакерських атак та наведено методику взлому платформи. Розроблено та візуалізовано веб-додаток для ldubzhd.*

Ключові слова: *інформаційна безпека, захист інформації, загрози, проєктування веб-додатка.*

Abstract. *The theoretical, scientific-methodical and organizational-functional foundations of information protection during the design of the university's web application are considered. Modern approaches to the protection of information security have been determined using the example of designing a university web application. Methodical approaches to the formation of the concept and structure of the automated information security protection management system are presented. The standards, recommendations, stages for the prevention of threats to information security have been analyzed. A model for protecting a web application from hacker attacks is proposed and a methodology for hacking the platform is given. A web application for Ldubzhd was developed and visualized.*

Keywords: *information security, information protection, threats, web application design.*

Безпека веб-ресурсів являє собою важливий напрямок інформаційної безпеки. Кількість веб-ресурсів постійно зростає, разом з цим зростає як кількість приватної інформації, що зберігається на серверах віддаленого доступу, так і кількість атак на веб-ресурси з метою заволодіння такою інформацією. Подібного роду атаки потенційно можуть привести до великих негативних наслідків, економічних і репутаційних. Однак зацікавленість в здійсненні таких атак і захисту від них не обмежується сферою економіки. На сьогодні вразливість від атак може бути пов'язана з політичними мотивами, її використовують у гібридних війнах, вона стає чинником зростання терористичних загроз. Через це актуальність даної роботи полягає в зменшенні кібер-вразливості веб-застосунку.

Нами сформовано низку вимог, яким має веб-додаток для університету. Перш за все, додаток має бути кроссплатформеним. Оскільки в наш час багато додатків працює лище на платформі iOS чи Android. Другим та не менш важливим критерієм є зрозумілість інтерфейсу. Також потрібно забезпечити коректну роботу додатку при слабому зв’язку або відсутності мережі Інтернет. Додаток мусить містити 3 інтерфейси: адмін, студент та викладач. Розглянемо детальніше: інерфейс адміна дає змогу створити студента та викладача, створити опитувальник та репорт. Додаток мусить містити інтерфейси авторизації, автентифікації та відновлення паролю. Так як продукт націлений не тільки на уранський маркет, сайт має підтримувати інтернаціоналізацію (українську та англійську мову). Таким чином, можна узагальнити вищезгадані вимоги:

1. Кроссплатформенність.
2. Робота при відсутності марежі Інтернет.
3. Підтримка інтернаціоналізації.
4. “User friendly” інтерфейс.
5. Обмін документами.

Отже, розглянуто зазначені вимоги, згідно з якими проведено детальний порівняльний аналіз існуючих програмних рішень. Також враховано їх переваги та недоліки при розробленні програмного застосунку. Приклад візуалізації додатка наведено на рис. 1.

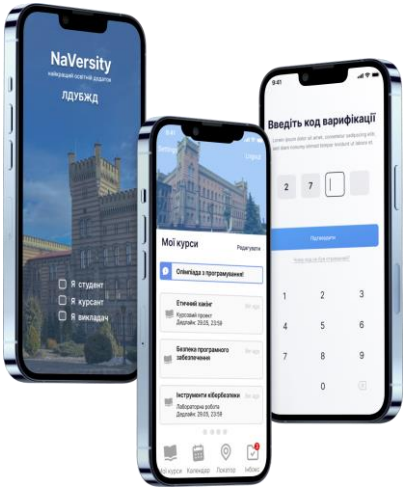


Рисунок 1 – Приклад візуалізації додатка

Програмно-технічний рівень протидії загрозам ІБ передбачає такі механізми безпеки як аутентифікація користувача, протоколювання, крипто-

графію, екранування каналів зв'язку. До атак, які загрожують додаткам відносять сукупність умов і факторів, що створюють небезпеку. Загроза інформації розглядається як порушення конфіденційності, цілісності або доступності даних, а також втрату або знищення даних. Класифікація загроз здійснюється за багатьма ознакам, що дозволяє добирати та застосовувати ефективні методи та засоби захисту. Витік інформації означає незаконне отримання даних, що не мають бути поширені. Досліджено та створено чіткий структурований підхід до проєктування користувацьких інтерфейсів, які забезпечують винятковий досвід роботи з додатками для мобільних телефонів, враховуючи потреби та бажання користувачів. Це було зроблено, дотримуючись принципів і процесів User Experience (UX) та User Interface (UI).

Проведений аналіз конкурентів дозволив оцінити різні стратегії взаємодії з користувачем, прийняті конкурентами, визначити їх сильні та слабкі сторони. Дослідження користувачів було розпочато проводячи інтерв'ю та опитування, щоб зрозуміти, чи має визначена ціль однакові чи різні потреби та проблеми, які були висунуті на етапі концепції. Крім того, створено профілі користувачів, які називаються персонами користувачів, щоб мати змогу ідентифікувати користувачів, їхні потреби, розчарування та очікування. Проаналізовано досвід користувачів, створюючи шляхи користувачів та зосереджуючи увагу на діях, цілях, думках та емоціях користувачів. Ці елементи були ключем до розроблення вирішень можливих проблем, з якими могли зіткнутися користувачі. Це також допомогло в процесі проєктування, оскільки дозволяло використовувати різноманітні типи користувачів.

Інформаційні джерела

1. Балацька В.С. Використання сканерів вразливостей для захисту комп'ютерної мережі навчального закладу // В. Балацька, В. Ящук, О. Полотай / матеріали VI Міжнародної науково-практичної конференції "Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи".

2. Купріков М. Методи тестування системи на проникнення для забезпечення кібернетичної безпеки / Н. Купріков, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.80–83).

3. Zachko O., Kovalchuk O., Kobylkin D., Yashchuk. Information technologies of HR management in safety-oriented systems. Materials of 2021 IEEE 16th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT 2021). V. 2. Lviv, 2021. (Scopus Q2).

УДК 004.946

АКТУАЛЬНІСТЬ ВИКОРИСТАННЯ ВІРТУАЛЬНИХ ТА ХМАРНИХ ТЕХНОЛОГІЙ

Іванна Рошинець, Валентина Ящук, Богдана Федина

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Розглянуто теоретичні, науково-методичні та організаційно-функціональні основи використання віртуальних та хмарних технологій. Визначено сучасні підходи до впровадження віртуальних та хмарних технологій у галузь освіти, медицини, фінансів, юриспруденцію, економіку. Наведено методичні підходи до формування концепції використання хмарних технологій. Проаналізовано переваги та недоліки використання віртуальних та хмарних технологій у різних галузях господарства.*

Ключові слова: *хмарні технології, хмарний сервіс, хмарні обчислення, віртуальні технології, хмарні бази даних.*

Abstract. *The theoretical, scientific-methodical and organizational-functional bases of the use of virtual and cloud technologies are considered. Modern approaches to the implementation of virtual and cloud technologies in the field of education, medicine, finance, jurisprudence, economy are defined. Methodical approaches to the formation of the concept of using cloud technologies are given. The advantages and disadvantages of using virtual and cloud technologies in various branches of the economy are analyzed.*

Keywords: *cloud technologies, cloud service, cloud computing, virtual technologies, cloud databases.*

Сьогодні, в еру інформаційного прогресу, постійного оновлення програмного забезпечення та оцифровування інформації все більшою популярністю користуються хмарні технології. Раніше вони використовувалися у вузькому колі IT-спеціалістів, а вже сьогодні дана технологія є доступною для всіх користувачів.

Хмарні технології (англ. cloud technologies) – це кардинально новий сервіс, який дозволяє віддалено використовувати засоби обробки й зберігання даних [1]. Найпоширенішими хмарними сервісами, які призначені для роботи з web-сервісами та звичайними різного роду документами. Серед них, до прикладу, найбільш поширена у використанні студентами та викладачами, хмарна платформа Google Apps Education Edition, якої основними інструментами є: електронна пошта Gmail (перевагами якої є підтримка текстового, а також голосового чату Google Talk, та навіть відеочату); календар Google; диск Google – сховище для зберігання власних файлів та можливістю настройки прав доступу до них; Google Docs – сервіс для створення документів, таблиць і презентацій з можливістю надання прав

спільного доступу декільком користувачам. Інтеграція з фізичних серверів у хмарні дозволить зменшити кількість витрат на їх утримання [1].

Стрімко зростає впровадження хмарних технологій в навчальний процес, завдяки технологіям освіта стає ще доступнішою, навчатися можна скрізь: в освітніх закладах або ж вдома. Всі потрібні матеріали для навчання, що знаходяться у віртуальному середовищі доступні з будь-якого місця, що дуже актуально за умов війни, або ж коли у світі панувала епідемія вірусу "Covid-19". Переважна більшість навчальних закладів лише почала впроваджувати та практикувати хмарні технології у своїх освітніх процесах. Наприклад, при пандемії, коли через небезпеку поширення вірусу, було рекомендовано перевезти більшість навчальних закладів освіти на дистанційне навчання.

Впровадження хмарних технологій в освітній процес є досить новим напрямом, що стрімко розвивається. Хмарні технології дають можливість проводити онлайн-консультації, наради, конференції та швидко отримувати коментарі та відповіді на питання. Що ж до перспектив розвитку хмарних технологій в напрямку освіти, то до них можна віднести навчальні онлайн-додатки, розробка нових та вдосконалення вже наявних додатків, а також перенесення таких відомих систем, як Moodle та Blackboard, у хмари [1–3].

Зокрема, для юристів, економістів, фінансистів хмарний сервіс надає можливість створювати юридичні документи, здійснювати обробку фінансових операцій, оформлювати звіти для бізнес-планів, зберігати всі свої документи в цифровому вигляді, за потреби навіть надавати дозволу своїм колегам переглядати свої документи чи редагувати спільні звіти та багато іншого [3].

Сфера медицини не виняток розвитку віртуальних технологій. Бельгійські медики провели дослідження і виявили, що віртуальні технології можна використовувати у хірургії замість вживання різних седативних препаратів. Такій методиці лікарі дали назву "віртуальний гіпноз". Особливістю є те, що під час операції на пацієнта одягаються навушники, VR-окуляри та вмикається заспокійливе відео про життя підводних тварин під час трансляції, де все коментується приємним заспокійливим голосом [4].

Використання хмарних серверів у галузі медицини надає зручності для лікарів. В минулому всі медичні документи про стан здоров'я були тільки в паперовому вигляді, але вже зараз більшість таких документів оцифрували та заносять в бази даних для зберігання. Для зменшення серверів зберігання всіх даних, і для фінансової вигідності можна використовувати хмарні бази даних. Однак, небезпека витоку даних – це основна проблема, з якою стикаються медична сфера при виборі хмарного рішення. Для подолання цих проблем медичні підприємства повинні вибирати надійних постачальників хмарних послуг, які діють у повній відповідності до положень медичної таємниці, конфіденційності, порушення зберігання

та втрати даних. Ризик витоку конфіденційних даних – і, як наслідок, кримінальна відповідальність та втрата довіри громадян – повинна бути мотивацією зосередити всі зусилля на захисті цифрових даних [4].

Серед можливостей хмарних обчислень можна виділити: легкий доступ до особистої або корпоративної інформації з будь-якого пристрою, що підключений до Інтернету; можливість працювати з інформацією з різних пристроїв, це може бути ПК, планшети, телефони та багато іншого; незалежність від операційних систем комп'ютерів користувачів; одну інформацію можна переглядати або редагувати одночасно на різних пристроях; запобігання втрати будь-якої інформації, тому що вона зберігається в хмарних сховищах; можливість об'єднання інформації з іншими користувачами; завжди актуальність web-додатків, постійне оновлення та підтримка програми; можливість ділитися інформацією з будь-якими людьми не залежно де ви знаходитесь.

До недоліків хмарних обчислень слід зазначити: необхідність постійного з'єднання зі Інтернет, без нього неможливо зв'язатись з сховищем; конфіденційність даних, не рекомендується зберігати цінні документи на публічних "хмарах"; небезпека проникнення в "хмару", зловмисники відразу отримують доступ до величезного сховища даних; використання систем віртуалізації в яких, як гіпервізор, використовуються ядро стандартних ОС, що дозволяє використовувати вразливості системи; для побудови власної хмари необхідно виділити значні матеріальні ресурси, що не вигідно для нових та малим компаніям; монетизація ресурсу.

Інформаційні джерела

1. Вакалюк Т.А. Хмарні технології в освіті. Навчально-методичний посібник для студентів фізико-математичного факультету. – Житомир: вид-во ЖДУ, 2016. – 72 с.

2. Продукти Google [Електронний ресурс] – Режим доступу до ресурсу: https://about.google/intl/ru_TJ/products/

3. Биков В. Ю. Хмарні технології, ІКТ-аутсорсинг і нові функції ІКТ підрозділів освітніх і наукових установ / В. Ю. Биков // Інформаційні технології в освіті. – № 10. – 2011. – С. 8–23.

4. Проскуряков С. Віртуальна реальність може замінити седативні препарати під час операцій – дослідження [Електронний ресурс] / Проскуряков Самуїл // hromadske.ua. – 2019. – Режим доступу до ресурсу: https://hromadske.ua/posts/virtualna-realnist-dozvolila-pozbutisya-sedativnihpreparativ-pid-chas-operacij.

5. Байрамов В.Е., Лобанчикова Н.М., Мельниченко В.В. Аналіз вразливостей хмарних технологій [Електронний ресурс] – Режим доступу до ресурсу: https://conf.ztu.edu.ua/wp-content/uploads/2017/06/51-2.pdf

6. Ориник С. Забезпечення безпеки використання хмарних сховищ для захисту персональних даних / С. Ориник, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.80–83).

УДК 004.056

ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАННИХ В ЕЛЕКТРОННОМУ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

Анна Чурілова, Сергій Прокопов

Дніпропетровський державний університет внутрішніх справ м. Дніпро, Україна

Анотація. *Розглянуто дослідження сутності проблем інформаційної безпеки персональних даних. Показано, що інформаційна безпека користувачів електронних пристроїв грає все більш вагому роль, а питання її забезпечення стають дедалі гострішими. Доведено, що комплексний захист персональних користувачів передбачає використання спеціальних правових, фізичних, організаційних і програмно-апаратних засобів захисту інформації.*

Ключові слова: *інформація, безпека, захист, кібербезпека, соціальні мережі.*

Abstract. *The study of the essence of problems of information security of personal data is considered. It is shown that the information security of users of electronic devices plays an increasingly important role, and the issues of its provision are becoming increasingly acute. It has been proven that the comprehensive protection of personal users involves the use of special legal, physical, organizational and software and hardware means of information protection.*

Keywords: *information, security, protection, cyber security, social networks.*

Технологічний прогрес створив все більше і більше потреб і можливостей збору, обробки персональних даних і самі персональні дані знайшли широке використання в різних сферах бізнесу і політики. Використання персональних даних стало багатогранним, і крім надання допомоги в їх роботі і повсякденному житті, вони можуть для декого служити інструментом порушення прав і свобод певних людей, особливо права на недоторканність приватного життя. У зв'язку з цим розвиток системи захисту персональних даних є одним з найбільш актуальною проблемою.

Захист персональних даних та їх вдосконалення є не тільки національним обов'язком, а й предметом державного регулювання. Крім того, створення ефективної системи захисту персональних даних є міжнародним зобов'язанням України.

Проблеми витоку персональних даних громадян України, державних установ та приватних компаній стали основними причинами злочинної

діяльності. Ситуація стає все більш і більш складною, тому що нові форми злочинів включають в себе не тільки виведення персональних даних з ПК користувачів, а і даних їх банківських карток, що в наступному призводить до втрати власних накопичень (коштів приватних підприємців або державних установ).

На сьогоднішній день національні органи влади зіткнулися з низкою загроз і проблем у сфері кібербезпеки. В Україні існує багато державних реєстрів, які містять конфіденційну інформацію громадян. Більшість з них використовують для авторизації секретні логіни і паролі. Таким чином не можливо ідентифікувати особу, яка намагається увійти в систему, для отримання інформації [1].

У сучасних умовах захист збереженої інформації в реєстрах є гострою проблемою. Більшість ПК якими користуються звичайні користувачі та адміністратори підключені до всесвітньої павутини Інтернет, що значно спрощує роботу кіберзлочинцям при спробах заволодіти персональними даними.

За роки незалежності України було накопичено переважну більшість інформації в цих системах та реєстрах. Приватні компанії тимчасово отримують доступ до інформації, яка містить персональні дані. Тобто ризик отримання конфіденційних даних зростає. На відміну від цього, накопичення більшої кількості інформації, обробки та зберігання вимагає збільшення цифрової інфраструктури.

Збір, обробка та накопичення даних в реєстрах вимагає реалізації принципів прозорості. Будь-яка інформація та обробка персональних даних повинні бути зроблені доступно і зрозуміло. Спеціальна мета обробки конфіденційної інформації їх комплекція завжди повинна бути чітко позначена і легальна. Крім того, період часу для зберігання персональних даних повинен бути зведений до абсолютного мінімуму для досягнення принципу – "дані не повинні зберігатися, якщо вони не потрібні". Чітко визначені терміни зберігання і знищення, забезпечить від витоку інформації.

Національною поліцію встановлено, що на спеціальних форумах та у закритих спільнотах розміщені різні бази даних. Існування цієї інформації створює основу для вчинення протиправних дій у межах кіберпростору, метою яких є отримання прибутку від продажу персональних даних. Злочинці створюють спеціальні сервіси для перевірки інформації або безпосереднього продажу баз даних [2].

Більш широка сфера – шахраї. Вони під приводом продажі інформації, особистих даних здійснюють заволодіння коштами. Широкий спектр розголошення, а також інше привертання уваги, щодо витоку персональних даних активують злодіїв.

Розглянемо ситуацію яка сталась у травні 2020 року. У месенджері Telegram з'явився бот, який поширював особисті дані українців за гроші. А саме поширював інформацію:

1) з банківських рєстрів, таких як "ПриватБанк" до його націоналізації;

2) із соціальної мережі "ВКонтакті" (логіни та паролі);

3) з електронної пошти;

4) з водійських посвідчень. [3]

Національною поліцією було розпочато кримінальне провадження з питання про незаконне втручання у роботу комп'ютерних мереж, автоматизованих систем.

Виникали питання щодо витоку персональних даних із додатка "ДІЯ", який виник відносно недавно і містить у собі електронні версії документів. Саме у цьому додатку знаходяться самі посилання основні документи в цифровому вигляді такі як: паспорт (ID-карта), закордонний паспорт, студентський квиток, водійське посвідчення, сертифікати про вакцинацію. Більше десяти мільйонів українців завантажили додаток і користуються ним. Проте, на офіційному сайті Міністерства і цифрової трансформації України спростовано думку про витік даних із цієї системи.

Зараз, Національною поліцією постійно забезпечено відслідковування активності учасників хакерської спільноти та їх діяльність. Зокрема інформацію про це розміщують на закритих онлайн-платформах "darknet", "tor", закритих скайп-каналах, телеграм-каналах. Дослідники приватної інформаційної безпеки відстежують новини про витоки персональних даних громадян України, державних установ, автоматизованих систем та приватних компаній. Виходячи з наявної інформації, такі витоки відбуваються не рідше одного разу на 2 місяці.

У Національній поліції цей напрямок роботи забезпечується системними заходами індивідуального пошуку, які проводяться найдосвідченішими співробітниками, агенти працюють з членами хакерської спільноти, в тому числі: завдяки активному залученню поліції і інших правоохоронних органів іноземних держав. Крім того, Національна поліція вжила низ-

ку заходів, спрямованих на викриття кримінальних правопорушень при використанні високих інформаційних технологій [4].

При формуванні баз даних, обробці та поширенні відомостей, поширенні інформації без відома власників персональної інформації доволі часто призводить до виникнення глобальних проблем інформаційної безпеки суспільства і держави щодо захисту персональних даних. Для захисту персональних даних користувачів персональних комп’ютерів та гаджетів доцільним є удосконалення їх антивірусного програмного забезпечення, яке необхідно використовувати лише ліцензоване та з перевірених джерел.

Ключовою проблемою витоку персональних даних є відсутність централізованого захисту, адже кожна організація самостійно захищає свій веб-сайт чи портал. Витік особистих даних є переважно проблемою нелокального характеру, тобто це питання стосується не лише національного органу влади, а є цілком глобальним питанням забезпечення інформаційної безпеки національних інтересів України.

Підсумовуючи, можна зробити висновок, що в умовах стрімкого розвитку інформаційних технологій необхідно приділяти особливу увагу розвитку систем захисту персональних даних користувачів, приватних підприємців. Захист персональних даних користувачів, як і комплексний захист інформації передбачає використання спеціальних правових, фізичних, організаційних і програмно-апаратних засобів.

Інформаційні джерела

1. Інтеграція України в Європейське інформаційне суспільство: виклики та завдання / упор. А. В. Пазюк; рец. О. О. Гріненко, О. В. Олійник. Київ: ФОП Клименко, 2014. 221 с.

2. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. Київ: К.І.С, 2015. 220 с.

3. Солонина Є.О. Злив персональних даних українців: що сталося і як захиститися. Радіо Свобода : вебсайт. URL: https://www.radiosvoboda.org/a/zlyv-danyxidiya/30610626.html (дата звернення: 16.11.2022)

4. Захист систем електронних комунікацій: навч. посіб. / В.О. Хорошко,О.В.Криворучко, М.М. Браіловський та ін. Київ: Київ. нац. торг.-екон. ун-т, 2019. 164 с.

Напрям 5

КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.4

ЗАСТОСУВАННЯ СТЕГАНОГРАФІЇ ДЛЯ ЗАХИСТУ ПРОГРАМ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Владислав Антонюк, Марина Сидорова

Дніпровський національний університет імені Олеся Гончара, м. Дніпро, Україна

Анотація. *Захист інтелектуальної власності та інформації набуває пріоритетного значення в сучасному комп'ютерному світі. Метою цієї роботи є дослідження задачі стеганографії та реалізація алгоритму LSB для захисту менеджера макросів у додатку "Draw & GO".*

Ключові слова: *інформаційна безпека, захист персональних даних, стеганографія, шифрування.*

Abstract. *Protection of intellectual property and information is becoming a priority in today's computer world. The purpose of this work is to research the steganography and implement the LSB algorithm to protect the macro manager in the "Draw & GO" application.*

Keywords: *information security, personal data protection, steganography, encryption.*

Сучасні інформація та технології "Know-how" мають підвищений інтерес для конкуруючих компаній, що породжує комп'ютерне піратство.

На сучасному етапі розвитку інформаційного суспільства, коли комп'ютери доступні практично для кожної родини, в умовах комерціалізації інтелектуальної власності актуально створювати програмні продукти, які дозволяють в зручному та безпечному режимі захистити особисті дані користувача при збереженні, передачі та модифікації.

Стеганографія – тайнопис, при якому повідомлення, закодоване таким чином, що не виглядає як повідомлення – на відміну від криптографії. Таким чином непосвячена людина принципово не може розшифрувати по-

відомлення – бо не знає про факт його існування. Якщо криптографія приховує зміст повідомлення, то стеганографія приховує сам факт існування повідомлення. Крім того, актуальність захисту даних підтверджена чинним законодавством: концепція національної системи захисту інтелектуальної власності № 1243-V від 27 червня 2007 р. [1].

Питанню безпеки інформації приділено значну увагу при розробці авторського програмного забезпечення “Draw & GO” [2]. “Draw & GO” – сучасний крос-платформний програмний продукт, який дозволяє полегшити, прискорити та автоматизувати роботу з пристроями. Це можливо завдяки макросам – мікро командам, що виконуються на вимогу користувача. Кожен користувач сам формує та комбінує команди, які потім можна відтворити необмежену кількість разів.

“Draw & GO” складається з наступних частин: Менеджер та Записувач макросів. Для захисту менеджера макросів було реалізовано метод Least Significant Bit (LSB) [3], суть якого полягає в заміні останніх значущих бітів у зображенні на біти приховуваного повідомлення. Проведене дослідження показало, що треба замінювати саме останній біт, а не якийсь інший:

Візьмемо піксель зі значеннями кодованого каналу:

Red = 255; byte R = 255; //11111111

Припустимо нам потрібно замінити один біт цього каналу на біт символу, рівний “0”. Якщо ми замінимо перший біт байту R (відлік йде справа наліво), то отримаємо:

byte R = 127; //11111110

Отримали дуже велику різницю значень. Тепер спробуємо замінити останній біт пікселя:

byte R = 254; //01111111

Тобто відтінок кольору зміниться незначно. Отже, вирішено, що треба змінювати останній біт, аби не була відчутна різниця між звичайним та зашифрованим пікселем.

Були виявлені недоліки методу LSB, а саме, чутливість до розміру зображення. Також при побітовому перегляді зображення видно області зображення, в які приховано інформацію. Попри це, метод запису Least Significant Bit широко використовується завдяки простоті в реалізації.

Приклад зображення до та після шифрування представлено на рисунку 1.

а) б)

Рисунок 1 – Приклад зображення до (а) та після (б) шифрування

Розглянемо алгоритм шифрування, який було реалізовано:

− завантажуємо зображення, у якому буде зашифровано текст;

− визначаємо кількість пікселів, з яких воно складається;

− ділимо отримане значення на розмір 1 символа (8 біт) і отримуємо максимальний розмір текстового повідомлення;

− вводимо текст для шифрування;

− визначаємо розмір тексту і зіставляємо його з максимально допустимим;

− визначаємо крок просування по зображенню;

− організуємо два цикли:

− зовнішній: обхід по символах;

− внутрішній: обхід по бітам символу;

− у циклах замінюємо біти зображення бітами тексту, рухаючись по зображенню з заданим кроком;

− зберігаємо отриманий результат.

Розглянемо алгоритм дешифрування, який було реалізовано:

− завантажуємо зображення, яке містить зашифрований текст;

− встановлюємо ключ шифрування;

− організуємо два цикли:

− зовнішній: обхід по символах;

− внутрішній: обхід по бітам символу;

− у циклах зчитуємо з кроком, зазначеним в ключі, значення останніх бітів пікселів;

− групуємо біти в символи і формуємо з символів текстовий рядок.

Інформаційні джерела

1. Про Рекомендації парламентських слухань “Захист прав інтелектуальної власності в Україні: проблеми законодавчого забезпечення та правозастосування” – [Електронний ресурс] – https://zakon.rada.gov.ua/laws/show/1243-16#Text

2. “Draw & GO” – [Електронний ресурс] – https://drawgo.azurewebsites.net/

3. Langdon, Glen G. (1982). Computer Design. Computeach Press Inc. p. 52. ISBN 0-9607864-0-6.

УДК 004.05+681.5.032

ДОСЛІДЖЕННЯ НАБОРУ СТАТИСТИЧНИХ ТЕСТІВ TESTU01 ДЛЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Михайло Кіх, Марія Шабатура

Національний університет "Львівська політехніка", м. Львів, Україна

Анотація. *В роботі досліджено набір для оцінювання статистичних характеристик генераторів псевдовипадкових послідовностей під назвою TestU01. Набір складається з шести батерей тестів, таких як: Small Crush, Crush, Big Crush, Rabbit, Alphabit і Block Alphabit. Описано принципи роботи програми TestU01 і особливості статистичного аналізу послідовностей, який проходить у два етапи: обчислення та обробка отриманих результатів.*

Ключові слова: *статистичний аналіз послідовностей, статистичні тести, TestU01, генератори псевдовипадкових послідовостей.*

Abstract. *The work analyses a set for evaluating the statistical characteristics of pseudorandom sequence generators, called TestU01. The set consists of six batteries of tests, such as Small Crush, Crush, Big Crush, Rabbit, Alphabit and Block Alphabit. The operating principles of the TestU01 program and the features of the statistical analysis of positions are described, which take place in two stages: calculation and processing of the obtained results.*

Keywords: *statistical analysis of sequences, statistical tests, TestU01, pseudorandom sequences generators.*

Оцінювання якості генераторів випадкових та псевдовипадкових послідовностей вже давно є актуальним питанням, оскільки від цього залежить ступінь випадковості, складність передбачення послідовності та шляхи застосування. На сьогоднішній день створено цілі набори тестів, які дають змогу дослідити статистичні характеристики генераторів. Найбільш популярним вважається стандарт статистичних тестів NIST, проте існують інші набори, такі як DIEHARTER, PractRand, FIPS, TestU01 та інші.

Метою роботи є дослідження набору статистичних тестів TestU01.

TestU01 – це бібліотека програмного забезпечення, реалізована на мові ANSI C і пропонує набір утиліт для емпіричного статистичного тестування уніфікованих генераторів випадкових і псевдовипадкових чисел [2].

Вона надає загальні реалізації класичних статистичних тестів для генераторів випадкових чисел, а також декілька інших, запропонованих у літературі [1, 3], і деякі оригінальні. У TestU01 доступні спеціальні набори тестів для послідовностей уніфікованих випадкових чисел у [0, 1] або послідовностей бітів. Ці тести можна застосувати до генераторів псевдовипадкових послідовностей, попередньо визначених у бібліотеці, а також до генераторів, визначених користувачем.

Пакет TestU01 містить шість основних батарей статистичних тестів [4]: Small Crush, Crush, Big Crush, Rabbit, Alphabit, Block Alphabit..

Small Crush батарея є достатньо швидкою та малою за обсягом, всього 10 тестів. Вона зчитує генератор як файл, що містить числа з крапкою, що плаває в межах [0,1]. Обмеження на файл трохи менше 51,320,000 випадкових чисел. Файл буде переписано на початку кожного тесту. Деякі тести вимагають щоб генератор повертав щонайменше 30 біт рішення, інакше генератор з великою ймовірністю провалить їх. Ця батарея зазвичай використовується для перевірки доцільності проведення тестів більш суворих батарей.

Перелік тестів: smarsa_BirthdaySpacings, smarsa_MatrixRank; sknuth_Collision, sknuth_Gap, sknuth_SimpPoker, sknuth_CouponCollector, sknuth_MaxOft; svaria_WeightDistrib; sstring_HammingIndep; swalk_RandomWalk1. Назви тестів починаються з s, після чого йде префікс, що вказує на походження тесту. Наприклад, “knuth” посилається на тести Дональда Кнута, а “marsa” посилається на Джорджа Марсалію.

Crush складається із 96 тестів. Батарея із суворих статистичних тестів. Включає як класичні тести Кнута, так і безліч інших. Деякі з цих тестів припускають, що генератор повертає щонайменше 30 біт рішення, інакше тести вважатимуться проваленими. Один із тестів вимагає 31 біт даних. Батарея використовує приблизно 235 випадкових чисел.

Big Crush складається із 106 тестів. Батарея найсуворіших статистичних тестів. Так само як і в інших батареях деякі тести вимагають як мінімум 30 біт вхідних даних, інакше тести будуть провалені. Також один із тестів вимагає 31 біт даних. Батарея використовує майже 238 випадкових чисел.

Alphabit і Block Alphabit складаються із 17 тестів кожний. Батарея Alphabit створювалася для тестування апаратних генераторів випадкових чисел. Проводить дев’ять послідовних тестів перед кожним переписуючи вхідні дані.

Rabbit складається із 38 тестів. Батарея більше сфокусована на тестуванні двійкових даних, але деякі тести проходять з фіксованими параметрами, якого б розміру не були вхідні дані. Тому дані, розмір яких перевищує 64 мегабайти, призводять до помилки в одному з тестів і переповнення оперативної пам’яті.

TestU01 приймає лише 32-розрядні вхідні дані та інтерпретує їх як значення в діапазоні [0, 1]. Це призводить до того, що він більш чутливий до недоліків у старших бітах, ніж у найменш значущих бітах. Важливо тестувати генератори загального призначення в біт-інвертованій формі, щоб перевірити їх придатність для програм, які використовують молодші біти.

На комп'ютері для простого генератора час роботи батареї тестів Small Crush займає кілька хвилин, Crush – близько години, Big Crush – близько десятка годин.

Статистичний аналіз послідовностей, як правило, проходить у два етапи.

Перший етап можна назвати підготовчим, він трудомісткий, тут виконується основна маса обчислень.

1.1. За допомогою генератора, що досліджується, формуються випадкові послідовності.

1.2. Для кожної послідовності обчислюється статистика тесту. Якщо працює батарея тестів (проводиться відразу кілька тестів), статистика по послідовності обчислюється кожному за тесту.

1.3. Для кожної послідовності обчислюється ймовірність значущості.

1.4. Отримані статистики та ймовірності значущості зберігаються.

На другому етапі проводиться обробка отриманих результатів.

2.1. За допомогою критеріїв згоди перевіряються гіпотези щодо відповідності розподілів статистик та ймовірностей значущості гіпотетичних розподілів.

2.2. Визначається число послідовностей, що пройшли тест. Будується довірчий інтервал для останньої величини.

2.3. Приймається рішення про те, чи пройдено тест.

2.4. Остаточні висновки.

Отже, було досліджено шість батарей статистичних тестів TestU01. На основі вищеперечисленого можна зробити висновок, що TestU01 чудово підходить як один із основних інструментів для емпіричного статистичного тестування генераторів псевдовипадкових послідовностей.

Інформаційні джерела

1. Pierre L'Ecuyer and Richard Simard. TestU01: A Software Library in ANSI C for Empirical Testing of Random Number Generators. user's guide, Universit´e de Montr´eal, 2013. [Електронний ресурс]. Режим доступу: http://simul.iro.umontreal.ca/testu01/guideshorttestu01.pdf

2. TestU01. [Електронний ресурс]. Режим доступу: http://simul.iro.umontreal.ca/testu01/tu01.html

3. Pierre L'Ecuyer and Richard Simard. A Software Library in ANSI C for Empirical Testing of Random Number Generators. D´epartement d'Informatique et de Recherche Op´erationnelle Universit´e de Montr´eal, 2013, user's guide. http://simul.iro.umontreal.ca/testu01/guideshorttestu01.pdf

4. P. L'Ecuyer and R. Simard, TestU01: A C Library for Empirical Testing of Random Number Generators ACM Transactions on Mathematical Software, Vol. 33, article 22, 2007. ERRATUM: The period of generator Brent-xor4096s in Table I should be 2^4128 and not 2^131072.

УДК 004.056.5

КРИПТОГРАФІЧНІ ТА СТЕНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Катерина Овчинікова[1], Орест Полотай[2], Андрій Лагун[2]

[1]Кафедра безпеки інформаційних технологій Національного університету "Львівська політехніка", м. Львів, Україна
[2]Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Описано загальні особливості криптографічних та стеганографічних засобів захисту інформації.*
Ключові слова: *криптографія, стенографія.*

Abstract. *General features of cryptographic and steganographic means of information* ***protection are described.***
Keywords: *cryptography, stenography.*

Криптографія – це метод захисту інформації та комунікацій за допомогою кодів, щоб лише ті, кому призначена інформація, могли її читати та обробляти. В загальному це наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації. Розвинулась з практичної потреби передавати важливі відомості найнадійнішим чином. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри та теорії ймовірностей.

Криптографія тісно пов'язана з дисциплінами криптології та криптоаналізу. Вона включає такі методи, як мікроточки, об'єднання слів із зображеннями та інші способи приховування інформації під час зберігання чи передачі. Однак у сучасному світі криптографія найчастіше асоціюється з перетворенням відкритого тексту у зашифрований текст, цей процес називається шифруванням, а потім знову у відкритий текст, цей процес відомий як дешифрування.

Шифрування поділяється на симетричне і асиметричне.

1. Симетричне шифрування – це тип шифрування, у якому лише один ключ (секретний ключ) використовується як для шифрування, так і для дешифрування електронних даних. Суб'єкти, які спілкуються за допомогою симетричного шифрування, повинні обмінятися ключем, щоб його можна було використовувати в процесі дешифрування. До симетричного шифрування відносяться алгоритми: AES, DES, IDEA, Blowfish, RC4, RC5, RC6.

2. Асиметричне шифрування – використовує два різні, але пов’язані ключі. Один ключ, відкритий ключ, використовується для шифрування, а інший, закритий ключ, призначений для дешифрування. Як випливає з назви, приватний ключ має бути закритим, щоб лише автентифікований одержувач міг розшифрувати повідомлення. До асиметричних шифрів відносяться: RSA, Діффі-Хеллман, ECC, Ель Гамаль, DSA.

В наш час криптографія дуже важлива, якщо ви хочете, щоб ваші дані були захищеними. Компанії заставляють своїх працівників шифрувати всі дані з якими вони працюють, тому що якщо, навіть, зловмисник і зможе отримати доступ до даних, то він не зможе їх розшифрувати без ключа.

Компанії часто кажуть своїм працівникам встановити спеціальні програми для того, щоб зашифрувати свої дані. Такі програми шифрують обраний диск і додатково просять вводити пароль коли операційна система запускається. До програм, які займаються шифруванням, відносяться:

1. BitLocker – це функція повного шифрування томів, яка входить до складу версій Microsoft Windows, починаючи з Windows Vista. Програма призначений для захисту даних шляхом забезпечення шифрування для цілих томів. За замовчуванням він використовує алгоритм шифрування AES.

2. Cryptocat – настільна програма з відкритим кодом, призначена для зашифрованого онлайн-чату, доступного для Windows, OS X і Linux. Вона використовує наскрізне шифрування для захисту всіх комунікацій з іншими користувачами Cryptocat. Користувачі мають можливість самостійно перевіряти списки пристроїв своїх друзів і отримують сповіщення, коли список пристроїв приятеля змінюється, а всі оновлення перевіряються за допомогою вбудованого завантажувача оновлень.

3. Java Cryptography Extension – це офіційно випущене стандартне розширення для платформи Java та частина Java Cryptography Architecture (JCA). JCE забезпечує структуру та реалізацію алгоритмів шифрування, генерації ключів і узгодження ключів, а також коду автентифікації повідомлень (MAC).

Стеганографія – це техніка приховування секретних даних у звичайному, несекретному файлі чи повідомленні, щоб уникнути виявлення. Потім секретні дані витягуються в місці призначення. Використання стеганографії можна поєднати з шифруванням як додатковий крок для приховування або захисту даних.

Стеганографію можна використовувати для приховування майже будь-якого типу цифрового вмісту, включаючи текст, зображення, відео

чи аудіоконтент. Дані, які потрібно приховати, можуть бути приховані майже в будь-якому іншому типі цифрового вмісту.

Програмне забезпечення стеганографії використовується для виконання різноманітних функцій, щоб приховати дані, включаючи кодування даних, щоб підготувати їх до приховування в іншому файлі, відстеження того, які біти текстового файлу обкладинки містять приховані дані.

OpenStego – програма стеганографії з відкритим кодом; інші програми можна охарактеризувати типами даних, які можна приховати, а також типами файлів, у яких ці дані можуть бути приховані. Деякі онлайн-інструменти стеганографії включають Xiao Steganography, який використовується для приховування секретних файлів у зображеннях BMP або WAV. Також є Crypture – це інструмент командного рядка, який використовується для виконання стеганографії.

Стеганографією займаються ті, хто хоче передати секретне повідомлення або код. Хоча існує багато законних способів використання стеганографії, розробники зловмисного програмного забезпечення також використовують стеганографію для приховування передачі шкідливого коду.

Люди мають бути обережними коли вони скачують картинки, або відео від невідомих осіб. Відкривши, звичайний на вигляд, файл на ваш комп'ютер може потрапити вірус який може вкрасти ваші персональні дані. Зловмисники часто вкладають шкідливе ПЗ в картинки які може скачати люба людина. Тому потрібно бути уважним коли скачуєш картинки з інтернету, якщо зображення надзвичайно велике, це може вказувати на те, що використовувалася стеганографія.

Щоб захиститися компанії від стенографії потрібно зосередити зусилля з виявлення безпосередньо на кінцевих точках, де легше виявити шифрування. Також потрібно проводити тренінги для працівників, щоб підвищити обізнаність.

Інформаційні джерела

1. "Криптографія". Електронний ресурс. Режим доступу з – https://en.wikipedia.org/wiki/Cryptography;

2. Kukharska, N., Lagun, A., Polotai O.I. The steganographic approach to data protection using arnold algorithm and the pixel-value differencing method. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020, 2020, pp. 174–177, 9204108

3. Полотай О.І., Белей О.І., Мальцева Н. Фізичний зміст комп'ютерної стеганографії. Том 23 (2021): Вісник Львівського Державного університету безпеки життєдіяльності. С. 27–32.

Напрям 6

ІНФОРМАЦІЙНІ ВІЙНИ

UDC 004

POSSESSION OF ACCOUNTS OF UKRAINIANS IN MESSAGING SERVICE

Viktoriia Pohorila, Daria Klymenko

National Aviation University, Kyiv, Ukraine

Abstract. *Today, the problem of possession of accounts in messaging service is extremely urgent. This has always happened and still happens in other social networks and countries as well. However, in Ukraine, this has serious and sometimes catastrophic consequences.*

Therefore, it is important to be knowledgeable about this topic. It is important to know what it is, how it happens and how it can be prevented. This is the purpose of these theses. Analyze this topic in detail and also with examples.

The results of this work are: greater awareness of the problem and its understanding. Thanks to this – knowledge of what to do in this or that situation. In addition, there are recommendations on how to prevent these situations.

Keywords: *social media, battleground, hackers, emails, bots, criminals, spy, information, war, account, location, protection against theft, two-factor authentication.*

Анотація. *Сьогодні проблема керування обліковими записами в службі обміну повідомленнями є надзвичайно актуальною. Це завжди відбувалося і досі відбувається в різних соціальних мережах і країнах. Однак в Україні це має серйозні, а часом і катастрофічні наслідки. У роботі наведено низку рекомендацій, щодо коректного поводження з обліковими записами.*

Ключові слова: *соціальні мережі, поле битви, хакери, електронні листи, боти, злочинці, шпигун, інформація, війна, обліковий запис, місцезнаходження, захист від крадіжки, двофакторна аутентифікація.*

In the lead-up to Russia's invasion of Ukraine, and throughout the ongoing conflict, social media has served as a battleground for states and non-state actors to spread competing narratives about the war and portray the ongoing conflict in their own terms. Russia and Ukraine both use social media extensively to portray their versions of the events unfolding, and amplify contrasting narratives about the war, including its causes, consequences, and continuation. Government officials, individual citizens, and state agencies and have all turned to an array of platforms, including Facebook, Twitter, TikTok, YouTube, and Tel-

egram, to upload information. It is difficult to pinpoint the exact amount of content uploaded by these various actors, but the scale of information being uploaded on social media about the war is immense. For instance, in just the first week of the war, videos from a range of sources on TikTok with the tag #Russia and #Ukraine had amassed 37.2 billion and 8.5 billion views, respectively [4].

Since the start of the Russia-Ukraine war, Telegram's use has rapidly increased. In the first three weeks of the war, Telegram users increased by 46 percent and from February to April 2022 it was Russia's most downloaded app with 4.4 million downloads.

Russian hackers are increasingly carrying out cyberattacks against ordinary Ukrainians, and the number of messages and psychological actions targeting Ukrainians in social networks and messengers is increasing [1].

This is reported by the National Agency for Special Communications and Information Protection. The National Agency for Special Communications noted that hackers often speculate on patriotic themes and state payments in phishing emails. Therefore, officials advise not opening letters from unknown recipients, not clicking on links contained in such letters, not entering personal data on linked pages in order to enable two-factor authentication in networks social services and all the services that support these services [1].

Criminals can also send emails to spy on someone and their contacts, the agency warned. In addition, according to the Special State Communications Service, the number of phishing e-mails disguised as information about state assistance to displaced persons and Ukrainians temporarily emigrated abroad is increasing. Criminals who make such mailings carefully follow Ukrainian news and respond quickly to any information about aid [1].

"Do not use links in such messages, leave your card, phone number, etc. You can only get financial assistance from Dia being in another countries. Information about payments in other countries can only be obtained from official agencies of these countries"- added the State Service.

In the early days of the war, many Telegram users complained that the site was created to show their own locations in Moscow, Chircask and other Russian cities. "Telegram website with unauthorized access to accounts, in particular with the possibility of intercepting one-time codes of text messages" – writes the information service of the State Service for Special Communications [2].

All this is the work of the enemy who, through Ukrainian data, is waging an information war with Ukraine. Therefore, check that your Telegram account is not being used by criminals [2] It is easy to do:

In the settings, check which region your device is connected to. If the location of the smartphone or computer matches the real location, then everything is fine. Also cancel any other active sessions. To reduce the risk of your account being hacked, enable two-factor authentication. This will provide additional protection against personal data theft. By the way, this also applies to accounts on social networks [2].

There are various bots in Telegram designed to trick Ukrainians and they are also good at hacking into their accounts. One of Telegram's dangerous bots is @DdosInstruction_bot, which allegedly has "cyber warfare instructions", according to the Ukrainian National Security Council's Counter Disinformation Center [3].

On startup, it will ask you to "Verify your account". Once verified, you will lose your account. In the future, it could be used for criminal purposes.

How to prevent such situations?

− In Telegram, as in other messengers, activate 2-step verification.

− Only use official chatbots!

References

1. Сергій Мельник. – Хакери з Росії стали більше атакувати простих українців – Держспецзв'язку. – 25.05.2022. – URL: https://www.epravda.com.ua/news/2022/04/25/686230/.

2. Сергій Кулеш. – Кібератаки та фейки: якими бувають, як розпізнати і захиститися. – 17.03.2022. – URL: https://itc.ua/ua/novini/kiberataki-ta-fejki-yakimi-buvayut-yak-rozpiznati-i-zahistitisya/.

3. У Telegram з'явився бот, який краде облікові записи користувачів. – 03.04.2022. – URL: https://radiotrek.rv.ua/news/u-telegram-z-yavivsya-bot-yakiy-krade-oblikovi-zapisi-koristuvachiv_284557.html.

4. Christian Perez, Senior Policy & Quantitative Analyst with FP Analytics, and Anjana Nair, Policy Fellow with FP Analytics. – Information Warfare in Russia's War in Ukraine. – URL: https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/.

УДК 327.5:327.8-92:070

ГОЛОВНІ ОСОБИСТОСТІ РОСІЙСЬКОЇ ІНФОРМАЦІЙНОЇ ВІЙНИ ПРОТИ УКРАЇНИ: ДУГІН

Н. Басій, М. Коник

Львівський торговельно-економічний університет, м. Львів, Україна

Анотація. *У публікації репрезентовано загальний огляд створення та функціонування інформаційної війни в Росії та її наслідки для української державності. Представлено діяльність А. Дугіна як одного з головних ідеологів російської інформаційної війни проти України. Здійснено спробу узагальнити основні віхи формування його як провідного російського філософа на прикладі його основних праць.*

Ключові слова: *інформаційна війна, пропаганда, А. Дугін, публіцистика.*

Abstract. *A general overview of the creation and functioning of the information war in Russia and its consequences for Ukrainian statehood is presented. The publication analyzes A. Dugin's activities as one of the main ideologues of the Russian information war against Ukraine. An attempt has been made to summarize the main milestones of his formation as a leading Russian philosopher on the example of his main works.*

Keywords*: information war, propaganda, A. Dugin, journalism.*

Початки введення інформаційної війни в РФ беруть своє коріння ще з часів татаро-монгольської орди, оскільки головною метою для тодішньої верхівки войовничої країни була навмисно спотворена картина відносин з іншими народами. Головна мета таких створених суджень полягала у вихованні власного населення відчуття ненависті, заздрості та посилення войовничого духу. Як бачимо, інформаційна війна РФ ведеться не лише стосовно інших країн, а й з власним народом. Відомо, що їх концепція інформаційної війни була створена ще під час Другої світової війни, зокрема, з початком функціонування у СРСР Військового Інституту закордонних мов, яке спеціалізувалося на поширенні та створенні пропаганди. З приходом В. Путіна до влади, наприкінці 1999 р. Інститут було реорганізовано у відділ закордонної інформації Військового Університету Міністерства оборони РФ. Головним документом механізму інформаційної війни була "Доктрина інформаційної безпеки".

Варто зазначити, що інформаційною війною вважається зумисно організований інформаційний вплив, який спрямований на розв'язання конкретної конфліктної ситуації політичного, економічного, національного характеру між державами, націями, соціальними групами, що безпосередньо загрожує національним інтересам і безпеці. Масштаби інформаційної війни охоплюють психологічну та кібернетичну сферу; на відмінну від військових дій, поле бою інформаційної – людська свідомість. Важливо, що принципи інформаційної війни зосереджені на концепції ведення нелінійної війни.

"І німі солдати, що так марно загинули, Встановлять на троні з льоду двоголовий скелет, Із моховитої могили повстане сяючий Гіммлер. І туманом зірниць обійме Абсолютний світанок" [2]. Рядки, присвячені Г. Гіммлеру (німецький військовий та громадсько-політичний діяч Третього Рейху, очільник нацистських формувань СС, за його керівництва функціонували концтабори, в яких було вбито мільйони євреїв) не належать німецькому солдату часів Третього Рейху, ані сучасному неонацисту із терен Європейського Союзу. Ці слова написав А. Дугін, "сірий кардинал", "Распутін", "мозок" Путіна, ідеолог "руского мира" та "неоєвразійства". Філософ, політолог, соціолог, керівник Міжнародного Євразійського руху (МЄР створений 2001 р., діяльність якого представлена у майже 30 країнах світу. До його створення/популяризації були причетні знані українці Н. Вітренко, Д. Корчинський, А. Арестович) роками послідовно вишліфовував інструменти інформаційної війни. Зброя А. Дугіна виявилася ефективною, оскільки результат ми, українці, сьогодні відчуваємо із кожною запущеною ракетою на наші землі. Ця зброя – виголошені промови, проспівані пісні, написані вірші, опубліковані статті. (До слова, це єдина "зброя" А. Дугіна, оскільки про військову справу йому відомо, мабуть, лише з книжок, бо ж вдалося уникнути військової служби через лікування в психіатричному закладі).

А. Дугін народився у Москві 1962 р. у сім'ї радянського генерала та лікарки українського походження. Навчався в Московському авіаційному інституті, проте його не закінчив. Належав до організацій "Чорний орден СС", Національно-патріотичного фронту "Пам'ять", "Орден східних тамплієрів"; очолював Націонал-більшовицьку партію, політичну партію "Євразія"; пра-

цював у відділі архіву КДБ із секретними матеріалами. З 1991 р. він розпочав публіцистичну діяльність у газетах “День”, “Завтра”. Того ж року світ побачили його пресодруки: “Гіперборець”, “Елементи”, альманах “Милий ангел”.

А. Дугін зумів проштовхнути ідею меншовартості українського народу серед росіян, особливо серед верхівки країни: наша історія, культура, наука, на його думку, не повинна самоіснувати. Адже для прибічника ідеї відродження Євразійської цивілізації, де Росія повинна стати центром, важливо, щоб усі сусідні держави ввійшли до цього складу “імперії” без власної національної ідентичності. Одне з головних завдань наддержави, на його думку, полягатиме у протистоянні вільному та демократичному світу (США). При цьому, формування національної тотожності приєднаних держав не повинна реалізуватися, а кращим методом для цього є, звичайно, руйнація згуртованості та єдності нації підняттям таких питань як: мова, віросповідання, політичний вибір, економічне досягнення окремого регіону та ін. Так, зокрема, 2015 року світ побачила книга А. Дугіна “Україна. Моя війна” (“Украина. Моя война”), в якій автор роздумував про те, що в Україні існують дві нації, тому держава має бути поділена на дві частини відповідно: Лівобережну та Правобережну. До слова, цей поділ формується на вище названих критеріях руйнації ідентичності нації. (Власних суджень не покинув, і у травні 2022 р. він наголосив на тому, що, наприклад, Західна Україна переходить під протекторат Польщі [3]).

Окрім геополітичних, історичних, суспільно-політичних критеріїв А. Дугін акцентував і на релігійному чиннику, згідно з яким усправедливлював військове вторгнення рашистів в Україну. 17 квітня 2022 р. у telegram-каналі “Незигар” писав: “[…] Україна потрібна не нам, росіянам. Вона потрібна Христові. І тому ми там і перебуваємо. І тому ми звідти нікуди не підемо” [1].

Інформаційна війна може стати основою для вже класичного ведення воєнних дій. 1991 р. Росія продовжила проти нашої державності довготривалу руйнівну інформаційну війну започатковану Радянським Союзом, яка у 2022 рр. була реалізована веденням повномасштабних військових дій в Україні. Безсумнівно, десятки книг та сотні опублікованих статей А. Дугіна були одним із чинників провадження “ефективної” інформаційної війни, оскільки у квітні 2022 р. російські ЗМІ цитували А. Дугіна на сторінці інтернет-видання “Камчатский край” (12.04.2022): “Контроль над певною частиною Донбасу чи України – це не перемога Росії. Наші солдати не повернуться додому, допоки не будуть знищені цілі, поставлені по всій країні […]”.

Інформаційні джерела

1 Александр Дугин, лидер международного Евразийского движения, главный редактор портала Катехон, специально для Незыгаря.: URL https://t.me/russica2/45498 (дата звернення: 05.10.2022).

2. Дугин А. Г. : URL http://anticompromat.panchul.com/dugin/duginbio. html (дата звернення: 15.10.2022).

3. Дугин: Россия не должна соглашаться на аннексию Польшей Западной Украины.: URL https://vz.ru/news/2022/5/25/1160183.html (дата звернення: 05.10.2022).

УДК: 004.056:351.749

КІБЕРПОЛІЦІЯ: РОБОТА В УМОВАХ ВОЄННОГО СТАНУ

Валерія Івкова

Управління протидії кіберзлочинам у Львівській області Департаменту кіберполіції Національної поліції України, м. Львів, Україна

Анотація. *Тези присвячено питанню протидії кіберзагрозам та роботі кіберполіції в умовах воєнного стану. Окреслено найбільш нагальні проблеми організаційно-правового забезпечення національної безпеки в інформаційному просторі. Визначено заходи протидії російській агресії в мережі Інтернет.*

Ключові слова: *кібербезпека, кіберполіція, поліція, шахрайство, інформаційна війна, пропаганда, кіберпростір, Інтернет.*

Abstract. *Theses are devoted to the issue of combating cyber threats and the work of cyber police under martial law. The most urgent problems of organizational and legal provision of national security in the information space are outlined. Measures to counter Russian aggression on the Internet have been determined.*

Keywords: *cybersecurity, cyberpolice, police, fraud, information warfare, propaganda, cyberspace, Internet.*

З розвитком високих технологій та подальшим їх впровадженням у повсякденне життя людини спостерігається перехід основної діяльності людини з матеріального світу в світ віртуальний. Але разом з позитивним прогресом, зменшенням затрат часу та ресурсів на обмін інформацією, зміну та прийняття рішень, розвитком бізнесу, виник прогрес негативний: злочинність у традиційному розумінні почала видозмінюватися, інтегруючись у кіберпростір, такі ж зміни обумовили відкриття кіберфронту, на ряду з активними бойовими діями.

У сучасних умовах спостерігається поширення терористичної діяльності радикально налаштованих осіб, груп і організацій, ускладнюється характер їх діянь, зростає тяжкість вчинених терористичних актів. Зазначена тема набуває ще більшої загостреності та актуальності, зважаючи на той факт, що терористична діяльність часто переходить у кіберпростір, з чим дедалі частіше стикаються в своїй практичній діяльності національні та міжнародні правоохоронні органи.

Зокрема, останнім часом стрімко зростає кількість кібератак на об’єкти критичної інфраструктури, приватні та державні установи, масово розповсюджуються повідомлення про замінування об’єктів, поширюються фейки та здійснюються інформаційно-психологічні атаки.

Окремий напрямок роботи кіберполіції – протидія фейкам і пропаганді, що поширюють прокремлівські джерела або поплічники “руского мі-

ра”. Для цього було створено бот у Telegram, куди громадяни надсилають посилання на ворожі канали, групи та профілі у соцмережах та месенджерах. Далі для блокування диверсійних ресурсів використовується канал StopRussiaChannel | MRIYA – тут висвітлюються детальні інструкції, як це зробити.

Так наприклад станом на 10.11.2022 року на каналі https://t.me/stoprussiachannel приймає участь майже 265 тис. людей, які надіслали з початку війни більше 6,3 млн скарг та заблокували (обмежили доступ) до 19 215 ворожих ресурсів, загальна аудиторія яких була близько 230 млн підписників. Крім цього, було отримано інформацію (виявлено) більше 77 тисяч ворожих ресурсів, з них перевірено та відправлено на блокування 38 тисяч.

Також кіберполіція здійснює пошук та ідентифікацію колаборантів і військових-окупантів, запобігає DDoS-атакам на приватний та державний сектори, попереджає атаки проросійських хакерських угруповань, виявляє та фіксує факти злочинної діяльності загарбників. У рамках міжнародної кооперації з представниками правоохоронних органів і біржами криптовалют проводиться комплекс заходів для виявлення та припинення руху криптоактивів, що використовують окупанти для фінансування злочинів.

Одним з основних векторів роботи кіберполіції залишається протидія шахрайству в інтернеті. Щодня правоохоронці виявляють та попереджають спроби зловмисників “заробити” на війні.

Найрозповсюдженішими схемами шахрайства в інтернеті є псевдоблагодійність, пропозиції з оренди неіснуючого житла, фейкові пасажирські перевезення та продаж неіснуючих товарів, зокрема і військової амуніції. Також поширені схеми фішингу або виготовлення фіктивних документів, які нібито дозволять чоловікам призовного віку перетнути державний кордон.

Закликаємо громадян інформувати правоохоронців про ворожі дії, зокрема через бот кіберполіції “Народний месник” – https://t.me/ukraine_avanger_bot. Функціонал бота дозволяє передати інформацію про виявлену техніку або військових-окупантів, випадки мародерства, місця знаходження снарядів, що не розірвалися, мітки, залишені ворогом, поплічників окупантів або надати доступ правоохоронцям до приватних камер зовнішнього відеоспостереження.

Інформаційні джерела

1. Офіційний сайт Департаменту кіберполіції Національної поліції України [Електронний ресурс] /2022/ Режим доступу до ресурсу: https://cyberpolice.gov.ua/

УДК: 32.22/28(477.74)

ІДЕОЛОГІЧНЕ ОБҐРУНТУВАННЯ ЗБРОЙНОЇ СПЕЦОПЕРАЦІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ

Олег Лозинський

Кафедра соціальної роботи, управління та соціальних дисциплін Львівського державного університету безпеки життєдіяльності, Львів, Україна

Ключові слова: *образ "ворога"; московська українофобія; "русский мир" як казко-терапія, менталітет.*

Keywords: *the image of the "enemy"; moscow ukrainophobia; "russian world" as a fairy-tale therapy; mental.*

Одержимість В. Путіна, з якою він впродовж 7 місяців на очах світової громадськості руйнує міста і убиває мирних громадян, намагається окупувати все нові частини української землі, зруйнувати її економіку та культурну спадщину – засвідчує, що в московському світогляді існував і досі існує симптом українофобії, щодо існування незалежної української держави та її культури [6]. За останні 20 років путінського авторитарного правління шовіністичні і людиноненависницькі наміри щодо України вийшли на поверхню і прозвучали "прямим текстом" в неоімперській українофобській ідеології "русского мира" [3, 5].

Московська пропаганда під час правління В.Путіна реанімувала головні неоімперські ідеологеми, зокрема нав'язала громадянам РФ думку, що українська держава – це фікція, її земля – це "исконно русские территории", а українців як окремої нації неіснує. А тому усі, хто заперечує цю фальшиву московську вигадку є "ворогами" або "зрадниками", яких слід винищити, або фізично витіснити з їх території проживання в еміграцію, а більш "лояльних" – підкорити.

Назвемо головні пропагандистські форми, завдяки яким українофобська ідеологія у Москві досягає поставлених цілей.

1. Заперечення української ідентичності. Московська пропаганда не одне сторіччя заперечує існування України як окремої політичної та культурної спільноти. Ця політика заперечення української ідентичності має 400-річну давність, й розпочалась ще до Переяславської угоди. Найбільш відомі Валуєвський Циркуляр 1863 р. та Ємський указ 1876 р. забороняли українське книгодрукування, шкільне навчання, театральні вистави, богослужіння українською мовою, не дозволяли хрестити дітей українськими іменами, санкціонували репресії українців, їх витіснення в еміграцію. У радянський період московська політика докладала неймовірні репресивні засоби винищення усіх можливих форм української культурної та інтелектуальної самобутності – репресувала письменників, науковців, композиторів, театральних та музичних діячів, представників духовенства і ін., –

щоб московська фіктивна ідея про неіснування української самобутності корелювала з дійсністю [1].

2. Применшення статусу. Московська пропаганда постійно знаходить і нав’язує українській спільноті принизливі слова-епітети (малороси, хохли, западенци, окраїна), які формують фальшивий образ українців як придаток до так званих “великоросів” не лише територіально, але також культурно чи соціально. Міф про “братні народи” обов’язково виділяє українцям роль “молодшої сестри”, а не рівноцінну роль. Українській мові також приписують меншовартісність, тому її забороняли використовувати у публічному просторі.

3. Демонізація українських національних символів, структур, персон. Особливу увагу московська пропаганда приділяла і досі приділяє демонізації українських державних чи політичних діячів, які наважувались військово чи ідейно протистояти російській експансії [2]. Прізвища І. Мазепи, С. Петлюри, С. Бандери – перетворено на демонічні ярлики – віроломних, підступних зрадників, заколотників, запроданців-колаборантів, убивць, антисемітів в яких “руки по лікті у крові”. Такими ж демонізованими представляли представників Української Греко-Католицької церкви – “Уніатів-віровідступ-ників”. Радянська репресивна машина жорстко репресувала українців за спроби мати український синьожовтий прапор, співати український гімн, кваліфікуючи ці дії як антрадянську пропаганду, екстремізм, український буржуазний націоналізм. До так званих “класичних” українофобських символів московська пропаганда за останні 30 років додала “новітні” демонізовані символи: партію “Правий сектор”, полк “Азов”, про які висловлюється як про “нацистські”, “терористичні” незаконні збройні формування, а про Українську Православну Церкву як про “розкольницьку”, “неканонічну” і т.п.

Московська ідеологія “русского мира” також реанімувала міф про “ворожий” Захід. Мовляв Росія (СРСР) перемогла нацистську Німеччину у ІІ-й Світовій війні, і в цьому є її історична “місія”. Однак країни Євросоюзу і НАТО сьогодні (в доктрині “русского мира”) стали загрозою для РФ. Тому РФ має “денацифікувати” військовим шляхом не лише Україну, але і країни “ворожого” Заходу.

Названі вище фентезійні символи щоденно поширюються з телеекранів для масової свідомості громадян РФ.

Московська українофобія психологічно проявляється у: страхах, заздрості, ненависті, зверхності щодо українців.

Українофобія як невід’ємний елемент ідеології “русского мира” є своєрідною казко-психотерапією, що збудована на антиісторичних основах, вона підживлює міфологеми про “величие родины”, з метолю усунути психологічний дискомфорт від цивілізаційної “дрімучості” її прихильників.

У корумпованій РФ єдиний засіб емоційно “прив’язати” до себе “население”, легітимізувати свою абсолютну владу – це культивувати образ “зовнішнього ворога”, щоденно з телевізора в стилі Гебельса втовкмачувати фікцію про “враждебный Запад”, “Защиту соотечественников в Крыму и на Донбасе”, “Превентивную спецоперацию с целью предотвращения размещения баз НАТО в Украине”.

Ідеологія “русского мира” – суцільна фальшивка, підтасовка фактів і шулерство. Вона спекулює примітивними міфологами про:

– “втрачений Рай” – міфологема про єдиний словянський народ, який був розділений, і який необхідно відновити в російській державі;

– “заблукалих овець” – духовну єдність “соотечественников”, що змушені проживати в різних пострадянських країнах; і мовляв РФ має законне право втручатись в політику держав, де проживають “соотечественники”;

– “відокремлення козлів від овець” – лояльних хохлів-русофілів залишити (“перевоспитать”), а “бандерівців-западенців” (зрадників) знищити;

– “ідеальну державу” – органіцистську тоталітарну державу, що перебуває у ворожій облозі, в якій особа є гвинтиком соціального організму;

– “Москву як третій Рим” – особливу місію православної Московії і т.п. нісенітниці.

Примітивна ідеологія “русского мира” виявилась прийнятною для малоосвіченого В.Путіна і його корумпованої “верхівки”, котрій була потрібна хоч якась видимість “значущої ідеї” для оправдяння війни.

Висновки. Антиісторична та агресивна доктрина “русского мира” (що оправдовує порушення РФ норм міжнародного права, захоплення інших незалежних держав, пропагує етнічну нерівність, вищість росіян) має бути визнана на міжнародному рівні як людиноненависницька, імперська, шовіністична, а її пропаганда має каратись кримінальною відповідальністю, так як це закріплено стосовно нацистської ідеології.

Інформаційні джерела

1. Лінгвоцид української мови. URL: https://uk.wikipedia.org/wiki/%D0%9B%D1%96%D0%BD%D0%B3%D0%B2%D0%BE%D1%86%D0%B8%D0%B4_%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%BE%D1%97_%D0%BC%D0%BE%D0%B2%D0%B8

2. Келман Герберт, Гамілтон Лі. Санкціоновані винищення. (Переклад з англійської мови Ілони Тижбір). URL: https://zavantag.com/docs/11/index-2155517.html?page=4#550793

3. Путин объяснил, почему Украине необходима денацификация. URL:https://regnum.ru/news/polit/3525659.html

4. Політичні репресії радянської доби. URL: https://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%96%D1%82%D0%B8%D1%87%D0%BD%D1%96_%D1%80%D0%B5%D0%BF%D1%80%D0%B5%D1%81%D1%96%D1%97_%D0%B2_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96_%D1%80%D0%B0%D0%B4%D1%8F%D0%BD%D1%81%D1%8C%D0%BA%D0%BE%D1%97_%D0%B4%D0%BE%D0%B1%D0%B8

5. Таран И. и др. «Принял абсолютно правильное решение»: как на фоне спецоперации на Украине растёт поддержка Путина среди россиян (И.Таран, М.Лобанов, Е.Комарова, А.Заквасин). 27.03.2022. URL:https://russian.rt.com/russia/article/981483-reiting-putin-specoperaciya-doverie

6. Українофобія. URL: https://uk.wikipedia.org/wiki/%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%BE%D1%84%D0%BE%D0%B1%D1%96%D1%8F

УДК: 004.56

ЛАНДШАФТ КІБЕРЗАЗРОЗ ТА ТРЕНДИ 2022 РОКУ

Володимир Любчак, Анастасія Підлісна

Сумський державний університет, м. Суми, Україна

Анотація. *Надається огляд найбільш актуальних для європейського простору кіберзагроз на основі щорічного звіту ENISA, виконується їх аналіз та визначається динаміка розвитку основних загроз.*

Ключові слова*: кібербезпек, ландшафт загроз, ENISA.*

Abstract. *An overview of the most relevant cyber threats for the European space is provided based on the annual ENISA report, their analysis is performed and the dynamics of the development of the main threats is determined.*

Keywords*: cybersecurity, threat landscape, ENISA.*

На початку листопада Агенство Європейського союзу з кібербезпеки (ENISA) опублікувало звіт про ландшафт кіберзагроз, у якому представлено комплексний аналіз вразливостей та загроз, найбільш актуальних для європейського кіберпростору в період з липня 2021 по липень 2022 років [1]. Аналітичні дослідження та створення звіту виконується за методологію CTL щодо ландшафту кібербезпеки [2]. У звіті визначено поточні загрози кібербезпеці, надано розуміння поширеності та серйозність векторів атак у Європі, описуються горизонтальні, тематичні і галузеві ландшафти кіберзагроз. Особлива увага приділяється галузевим "тенденціям", визначаючи суб'єкти загрози, відповідні наступальні методи та окреслюючи заходи щодо зменшення ризиків і реагування на інциденти безпеки.

Ландшафт загроз у 2022 році сформували: програми-вимагачі, шкідливе програмне забезпечення, загрози соціальної інженерії, загрози щодо даних, відмова в обслуговуванні, Інтернет-загрози, дезінформація, атаки на ланцюги поставок. Для кожної з ідентифікованих загроз описуються методи атаки, найбільш суттєві інциденти разом із заходами пом'якшення.

Серед основних загроз кібербезпеці слід окремо відзначити атаки програм-вимагачів. Вони, як і в 2021 році, посідають перше місце в рейтингу. Разом з ними за звітній період високий рейтинг також мають атаки на доступність. Саме розповсюдженню програм-вимагачів, як одних

із найруйнівніших видів атак на кібербезпеку за останнє десятиліття, присвячено окремий звіт ENISA [3].

Геополітика продовжує сильніше впливати на ландшафт загроз: у цьому році значні зміни внесла російсько-українська війна. Цей конфлікт сприяв зростанню кіберінцидентів та появі нових хвиль хактивізму. Він також вплинув на зростання DDos-атак, які стали одним із інструментів кібервійни. Атаки на доступність стають більш масштабними та складнішими у порівнянні з 2021 роком, переходячи до мобільних мереж та Інтернету речей. Активніше й більше стала поширюватись і дезінформація. Це здійснюється через розповсюдження ботів, що моделюють персонажів і можуть порушити ділові процеси, а також взаємодію спільноти, засипаючи державні установи фейковим вмістом і коментарями. Фішинг все ще залишається актуальною загрозою, яка набула в цьому році нових форм, які зосереджені на українсько-російському конфлікті. Окрім цього, продовжує розвиватися ще з 2021 року бізнес-модель “хакер як послуга”.

У порівнянні з минулим роком не змінилися категорії суб’єктів загрози кібербезпеці: Державні суб’єкти, Суб’єкти кіберзлочинності, Суб’єкти-хакери за наймом, Хактивісти. Суб’єкти кіберзагроз є невід’ємною складовою ландшафту загроз. Це суб’єкти, які прагнуть здійснити зловмисну дію, скориставшись наявними вразливими місцями. Розуміння того, як думають і діють суб’єкти загрози, які їхні мотиви та цілі, є важливим кроком до ефективнішого реагування на кіберінциденти. Моніторинг останніх розробок щодо тактики та методів, які використовують суб’єкти загрози для досягнення своїх цілей, має вирішальне значення для ефективного захисту в сучасній екосистемі кібербезпеки.

Незмінним в порівнянні з минулорічним звітом залишається те, що велика кількість інцидентів була націлена на державну адміністрацію, уряд та постачальників цифрових послуг.

Нижче наведена таблиця із порівнянням динаміки розвитку основних загроз протягом звітного періоду 2021 та 2022 років.

2021			**2022**		
	Основні загрози	**Динаміка**		**Основні загрози**	**Динаміка**
1	Програми-вимагачі	Збільшення	1	Програми-вимагачі	Збільшення

2	Шкідливе програмне забезпечення	Збільшення	2	Шкідливе програмне забезпечення	Збільшення
3	Криптоджекінг	Збільшення	3	Соціальна інженерія	Збільшення
4	Загрози, пов'язані з електр. поштою	Стабільно	4	Загрози щодо даних	Збільшення
5	Загрози щодо даних	Стабільно	5	Загрози доступності: відмова в обслуговуванні	Збільшення
6	Загрози доступності та цілісності	Стабільно	6	Загрози доступності: інтернет загрози	Збільшення
7	Дезінформація	Стабільно	7	Дезінформація	Збільшення
8	Нешкідливі загрози	Збільшення	8	Атаки на ланцюги постачання	Стабільно

Слід зазначити, що щорічні звіти з аналізом ландшафту кіберзагроз публікують також інші організації, наприклад Fortinet [4], CrowdStrike [5], Sophos [6], Kroll [7].

Інформаційні джерела

1. ENISA THREAT LANDSCAPE 2022 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (дата звернення: 10.11.2022).

2. ENISA Threat Landscape Methodology https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology

3. Ransomware: Publicly Reported Incidents are only the tip of the iceberg https://www.enisa.europa.eu/news/ransomware-publicly-reported-incidents-are-only-the-tip-of-the-iceberg

4. Global Threat Landscape Report. A Semiannual Report by FortiGuard Labs https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-1h-2022.pdf

5. Global Threat Landscape Report https://www.crowdstrike.com/global-threat-report/

6. Sophos 2022 Threat Report https://www.sophos.com/en-us/content/security-threat-report

7. Q1 2022 Threat Landscape: Threat Actors Target Email for Access and Extortio https://www.kroll.com/-/media/kroll-images/pdfs/q1-2022-threat-landscape-report.pdf

УДК 351.865 (043.2)

РОСІЙСЬКО-УКРАЇНСЬКА КІБЕРВІЙНА: ДОСЛІДЖЕННЯ ДІЯЛЬНОСТІ ІТ ВІЙСЬКА УКРАЇНИ

Алла Пінчук, Р. Одарченко, Владислав Самойленко, Т. Дика

Національний авіаційний університет, м. Київ, Україна

Анотація. *Початок повномасштабного збройного вторгнення РФ став початком першої світової кібервійни. Українські вебресурси потерпали від російських кібератак. Внаслідок чого, міністром цифрової трансформації України М. Федоровим було засноване ІТ військо України (IT Army of Ukraine). Наразі ІТ армія веде активну та успішну роботу на кіберфронті.*

Ключові слова: *російсько-українська кібервійна, IT army of Ukraine, кіберфронт.*

Abstract. *The beginning of the full-scale armed invasion of Russia was the beginning of the first world cyberwar. Ukrainian web resources suffered from Russian cyberattacks. As a result, the Minister of Digital Transformation of Ukraine M. Fedorov founded the IT Army of Ukraine. Currently, the IT Army is actively and successfully working on the cyber front.*

Keywords: *russian-ukrainian cyberwar, IT army of Ukraine, cyber front.*

Повномасштабне вторгнення РФ супроводжувалося масовими кібератаками на всі можливі інформаційні та урядові ресурси України. Внаслідок чого, 26 лютого міністр цифрової трансформації України М. Федоров заявив про створення ІТ армії України – “IT Army of Ukraine” – для боротьби на кіберфронті [1]. Передбачалося, що в цьому кіберволонтерському війську будуть брати участь ІТ-фахівці, однак зараз зробити свій вклад у перемогу в цій війні може кожний бажаючий. ІТ армія України включає в себе як і українських, так і іноземних волонтерів [2]. Проте, окрім офіційної спільноти, є ще й низка “партизанських” спільнот, які були сформовані ініціативними українцями. Ключовою задачею війська є нанесення DDoS-атак на вебресурси Росії.

Для дослідження діяльності ІТ війська України, було зібрано статистичні дані по кількості отриманих завдань (рис. 1). Кількість DDoS-атак (отриманих завдань) була найбільшою в липні. Але зазначимо, що весною було більше різноманіття інформаційних ресурсів ворога, тобто атакували більшу кількість різних сайтів. З часом почали працювати по окремих ресурсах та їх піддоменам. Робота ініціативи IT Army of Ukraine досить ефективна, адже вся спільнота працює злагоджено.

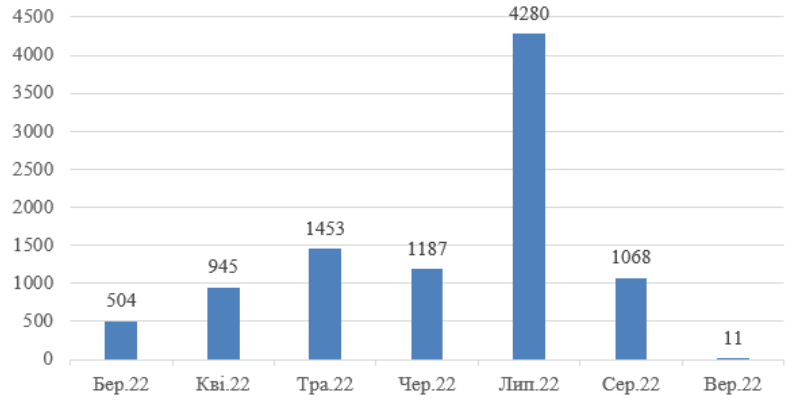


Рисунок 1 – Кількість DDoS-атак на сайти (виконаних завдань)

Таку ефективність роботи ІТ війська України зручно пояснити за допомогою теорії графів. На додачу до офіційних телеграм-каналів, було зібрано низку “партизанських”. Дослідивши наповнення каналів завданнями, можемо змоделювати сам процес поширення завдань. При цьому, розглядаємо дві ситуації: початок повномасштабного вторгнення та сьогодення. У зв’язку з гострою фазою кібервійни, з метою забезпечення безпеки зібраних телеграм-каналів, їхні назви не розкривали, або не полегшувати завдання ворогу. Телеграм-канали пронумеровані в хронологічному порядку. Темнішим кольором зображено офіційні та/або найбільші канали за кількістю учасників. Всього зібрано 13 телеграм-каналів, досліджено їх публікації та виявлено взаємозв’язки між іншими каналами (рис. 2).

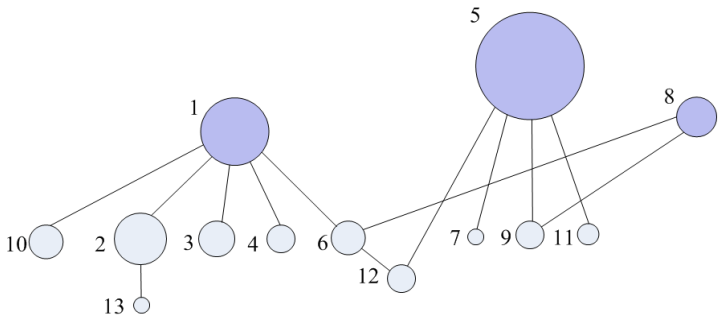


Рисунок 2 – Канали по DoS/DDoS (станом на початок війни)

Отриманий граф показує здебільшого “розсіюваність” атак, вони не є синхронізовані разом з усіма іншими каналами. Саме тому на початку війни було складніше досягнути ефективності атак. Загалом була велика кількість “самостійних” каналів, які самі обирали цілі для атак, та мали відносно невелику аудиторію.

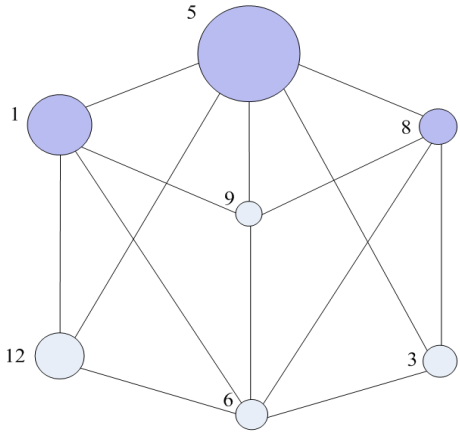


Рисунок 3 – Канали по DoS/DDoS (станом на зараз)

Станом на зараз маємо граф (рис. 3), який відображає синхронність атак. Досліджені телеграм-канали намагаються працювати по однаковим цілям, завдяки чому і досягається ефективність всього кібервійська. При цьому, із 13 каналів зараз працюють тільки 7. Перш за все, це пов’язано з тим, що аудиторія почала переходити до великих каналів, де публікують всі актуальні цілі, інструкції і т.д.

Незважаючи на складну ситуацію, яка склалася в країні, українці не занепали духом, стали на захист всіх фронтів, в тому числі і кіберфронту. Діяльністю ІТ армії України захоплюється весь світ та самі долучаються до боротьби з ворогом всього сучасного світу.

Інформаційні джерела

1. FEDOROV. *Telegram*. Режим доступу: https://t.me/zedigital/1114

2. Ukrinform. В Україні створили потужну 300-тисячну ІТ-армію – Федоров. *Укрінформ – актуальні новини України та світу*. Режим доступу: https://www.ukrinform.ua/rubric-technology/3490947-v-ukraini-stvorili-potuznu-300tisacnu-itarmiu-fedorov.html

УДК 351.865 (043.2)

РОСІЙСЬКО-УКРАЇНСЬКА КІБЕРВІЙНА: ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ ТА ПРОПАГАНДОЮ

Владислав Самойленко, Р. Одарченко, Алла Пінчук, О. Лавриненко

Національний авіаційний університет, м. Київ, Україна

Анотація. *З початком повномасштабного вторгнення Російської Федерації в Україну, крім збройного вторгнення, також була розпочата кібервійна. З-за великої кількості дезінформації та фейків, люди не могли відрізнити правдиву інформацію від бережно сконструйованої неправди. У зв'язку з цим, в Інтернеті розпочалась волонтерська діяльність, направлена на боротьбу з дезінформацією, ворожими ресурсами та захистом істини.*

Ключові слова*: російсько-українська кібервійна, дезінформація, платформа* "*Мрія"*.

Abstract. *With the beginning of the full-scale invasion of the Russian Federation into Ukraine, in addition to the armed invasion, a cyberwar was also launched. Due to the abundance of misinformation and fake news, people could not distinguish between true information and carefully constructed falsehoods. In this regard, volunteer activities aimed at combating disinformation, hostile resources, and protecting the truth have started on the Internet.*

Keywords*: russian-ukrainian cyber war, disinformation,* "*Mriya" platform.*

Волонтерська діяльність, направлена на боротьбу з дезінформацією, ворожими ресурсами та захистом істини може бути класифікована за трьома напрямами: кібератаки на ворожі ресурси, боротьба з російською пропагандою та поширення правдивої інформації.

Один з основних рухів, який займається боротьбою з російською пропагандою, є Платформа "Мрія" – виробник проєктів за підтримки Кіберполіції України та волонтерів. Перший проєкт якого був бот, по блокуванню незаконних телеграм-каналів, але після 24.02.2022 р. бот було переформатовано на опрацювання фейкових та проросійських ресурсів, котрі в подальшому "йдуть" на блокування. Крім цього, з'явилися також інші проєкт: "Mriya Automatic" – автоматизований сервіс для боротьби з російською пропагандою, бот "Народний месник" – офіційний чат-бот України для повідомлення про ворожі дії на території нашої держави та інші, бот "StopRussia | Mriya" – приймає інформацію про фейкові ресурси, котрі

перевіряються модераторами та відправляються на блокування як завдання в головний канал “StopRussia | Mriya”. Для більшої ефективності скарги надсилалися неодноразово на деякі сторінки/канали/пости. Варто зазначити, що дані спільноти є офіційними, створені держорганами України, однак ініціативні українці створили й інші “партизанські” кіберспільноти, які діють за цими ж напрямками [1].

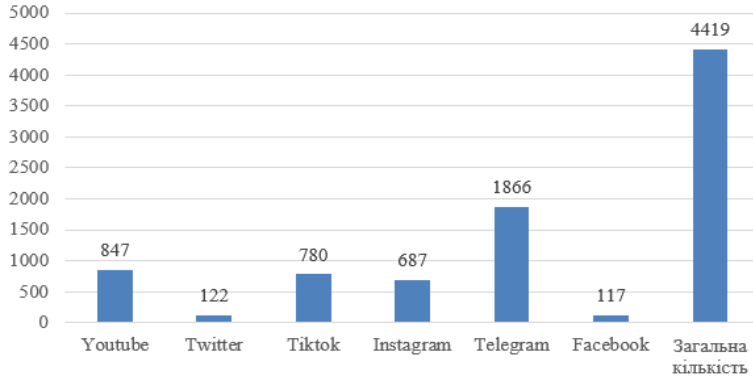


Рисунок 1 – Кількість виданих завдань по блокуванню ворожих ресурсів

Для того, щоб провести аналіз роботи напрямку боротьби з дезінформацією, проводився збір за кількістю виданих завдань в часовому проміжку 05.03 – 09.09.2022 р. Завдання надходили з телеграм-каналів Stop Russia Channel | Mriya, Інтернет Війська України та інших. Статистика за кількістю завдань представлена на рис. 1. Як ми бачимо, найбільша кількість цілей мала місце саме в месенджері Telegram. Головним показником ефективності виконання завдань є кількість заблокованих ворожих інформаційних ресурсів. За допомогою чат-боту “StopRussia | Mriya” в загальному заблоковано 9206 ресурсів (станом на 19.09.2022 р.). Це число з кожним днем росте, що свідчить про ефективність роботи всієї спільноти кіберволонтерів.

Зв’язки між різними джерелами видачі завдань, для блокування ворожих ресурсів, можливо показати графами. Для дослідження зібрано 12 телеграм-каналів. Кількість завдань на цьому напрямку значно більша, також потребує масовості, але здебільшого не така ефективна. Причиною цьому є строгість політик соціальних мереж щодо блокування контенту, на який надсилаються скарги. Тим не менш, завдяки наполегливості кібервійська, також є значні результати.

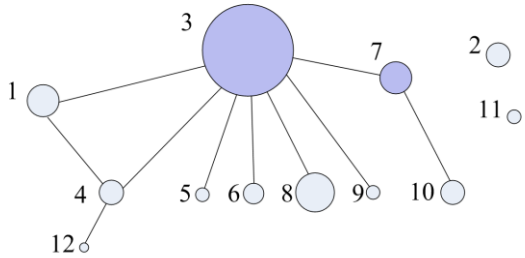


Рисунок 2 – Канали з блокування пропаганди та дезінформації (початок війни)

Деякі канали працювали самостійно, тому на графі вони зображені окремо від всіх інших. Загалом тут не так важливо досягти повної синхронності у часі, але важливо працювати по однаковім завданням, щоб заблокувати ворожий контент.

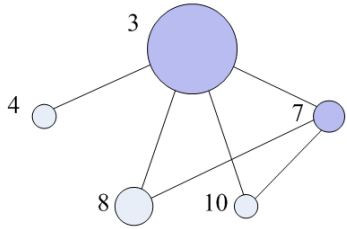


Рисунок 3 – Канали з блокування пропаганди та дезінформації (станом на зараз)

Деякі канали завершили свою роботу. Таким чином, із досліджуваних 12 каналів, лише 5 працюють і сьогодні. Канали, зображені темнішим кольором, є основними з публікації завдань на цьому напрямку, їхні завдання поширюються і по наступним каналам, що забезпечує більш ефективну роботу.

Платформа “Mriya” є лише однією з низки платформ, які ефективно протидіють ворожій пропаганді. Взяти участь в протидії з ворогом може абсолютно кожний, попри місцеперебування та громадянство. А налагоджена та синхронна робота дозволяє отримати максимальні результати за короткий час.

Інформаційні джерела

1. STOP RUSSIA | MRIYA URL: https://mriya.social/

УДК 347.775

АВТОРСЬКЕ ПРАВО ЧЕРЕЗ ПРИЗМУ ВОЄННОГО СТАНУ В УКРАЇНІ

Надія Федорова

Сектор розпорядження авторськими та суміжними правами відділу авторського права і суміжних прав НДІ інтелектуальної власності НАПрН України, м. Київ, Україна

Анотація. *Розглянуто авторське право через призму воєнного стану в Україні. Публікації в Meta всесвіті на воєнну тематику порівнюються з інформаційною війною, яку ведуть більшість українців. Проаналізовано, які фотографії, відео та різноманітні дописи можуть бути правомірно опубліковані, а які – ні. Здійснено коротке порівняння доктрини "fair use" та поняттям вільного використання об'єктів авторського права.*

Ключові слова: *авторське право, інформаційна війна, вільне використання творів, фотографії, відео, автор.*

Abstract. *Copyright is considered through the prism of martial law in Ukraine. Publications in the Meta universe on military topics are compared to the information war waged by the majority of Ukrainians. Analyzed which photos, videos and various posts can be legitimately published and which cannot. A brief comparison of the doctrine of "fair use" and the concept of free use of copyright objects is made.*

Keywords: *copyright, information war, free use of works, photos, video, author.*

Реалії сьогодення такі, що будь хто з нас, нині, може стати автором воєнного контенту. Зокрема, фотографій, відео, різноманітних дописів (статей) у Meta просторі, пісень, каверів, віршів тощо. Зруйновані будинки, понівечені вибухами чи пожежею різноманітні архітектурні споруди, пам'ятники, паркові зони можуть бути зафіксовані за допомогою фотографії. Очевидці документують на відео жахи на окупованих територіях України, відео з Бородянки та Ірпеня й завдяки таким платформам, як Meta, YouTube воно поширюється всією Україною та світом. Подібні публікації є не лише суто інформативними а й можуть бути використаними як докази воєнних злочинів у міжнародних судових інстанціях. Втім, зроблені фото та відео, що фіксують жахливі кадри війни в Україні можуть бути не лише доказами воєнних злочинів а й об'єктами авторського права.

Відповідно, виникає гостра необхідність у детальному розгляді який же воєнний контент може бути опублікованим а який – ні.

Погодьмося, що зараз, як ніколи, потрібно показувати світу об'єктивну, правдиву інформацію щодо подій в Україні. За загальним правилом використання об'єкта авторського права здійснюють лише за згодою його автора та за відповідну плату. Проте реальність така, що твори часто використовують не подбавши про отримання згоди автора. В епоху диджиталізації у світі набула поширення доктрина добросовісного використання ("fair use" – згідно з

якою, кожен може використовувати авторський контент, зокрема, для таких цілей як повідомлення в новинах, коментарі, дослідження. У решті випадків, потрібно зважати на чужі авторські права та використовувати авторський контент лише за згодою автора [2]), яка в багатьох аспектах збігається з принципами та випадками вільного використання об’єктів авторського права, передбаченими ст. 21 Закону України “Про авторське право і суміжні права” [1]. Так, не охороняються авторським правом повідомлення про новини дня або поточні події, що мають характер звичайної прес-інформації. Наприклад, інформаційна колонка про обстріли чи повідомлення про гуманітарні коридори не будуть охоронятися авторським правом, хоча кожен журналіст може висвітлювати це стилістично по-різному.

Випадки добросовісного використання авторських прав без отримання згоди автора також передбачені Законом України “Про авторське право і суміжні права”. Так, маємо вичерпний перелік випадків коли чужий авторський контент може використовуватись іншими без попереднього отримання дозволу. Для прикладу, чужий воєнний контент може використовуватись з метою висвітлення поточних подій засобами фотографії або кінематографії. Тобто, для інформування про події чи їх перебіг можна використати чужу фотографію чи відео. Але при цьому, слід обов’язково зазначити автора чи авторів та використовувати лише в обсязі, виправданому інформаційною метою.

Фото документування різноманітних подій, в тому числі й воєнного контенту відбувається вже не перше століття. На разі це можуть робити не лише професійні фотографи та оператори а й звичайні люди за допомогою телефону стаючи свідками війни.

Так, в кінці жовтня 2022 року, в українських соцмережах стало вірусним фото нібито знеструмленого після обстрілів Києва. Користувачі поширювали його зазвичай без жодних посилань, адже світлина стала символом української стійкості. Однак згодом виявилося, що у фото є конкретний автор – Віталій Рубцов, якого медіа мали би вказати (а фото, наспрвді, було зроблене 10-го травня 2019 року під час заходу сонця. Саме тому вуличне освітлення ще не ввімкнене) (рис. 1).

Рисунок 1 – Автор фортографії – Віталій Рубцов 2019 р.

Однак, це не перший випадок такого стрімкого поширення фото чи відео, де забувають вказати справжнього автора контенту. Звісно, що люди хочуть розповісти світові про злочини російських окупантів та незламність українського народу. Проте, ні воєнний стан, ні інформаційна війна, яку веде більшість українців, не скасовують авторське право навіть у Meta просторі. Й, навіть, якщо фотографія викладена в "безкоштовному" фотобанку потрібно уважно ознайомитися з умовами ліцензії та перевірити, чи дозволяє вона комерційне використання і яке саме. Що ж до умов ліцензії, то вони мають бути чіткими й детальними: вид ліцензії; сфера використання об'єкта права інтелектуальної власності (конкретні права, що надаються за договором, способи використання зазначеного об'єкта, територія та строк, на які надаються права, тощо); розмір, порядок і строки виплати винагороди за використання об'єкта права інтелектуальної власності (ч. 3 ст. 1109 Цивільного Кодексу України); якщо в ліцензійному договорі про видання або інше відтворення твору винагорода визначається у вигляді фіксованої грошової суми, то в договорі має бути встановлений максимальний тираж твору (ч. 8 ст. 1109 Цивільного Кодексу України) [3].

Однак, якщо цих деталей у договорі не буде – це не значитиме, що об'єкт авторського права можна використовувати будь яким чином. Швидше – навпаки, адже за законом усі права та способи використання, прямо не зазначенні у ліцензійному договорі, вважаються такими, ще не надані ліцензіату.

Наприклад, якщо ліцензійна угода передбачає зображення на марках, це жодним чином не дозволяє його друкувати на футболках, світшотах та іншому одязі. На це потрібен прямий дозвіл. Навіть якщо 99 % виручених від продажу коштів будуть передані на допомогу ЗСУ.

Отож, війна не привід для порушень та нехтування авторськими правами. Кожен із нас робить свій внесок. Вдала фотографія чи картина – це актив, часом дуже потужний, що заслуговує на повагу, як і права на нього.

Інформаційні джерела

1. Про авторське право й суміжні права: Закон України від 23 грудня 1993 р.// Відомості Верховної Ради. – 2003. – №40-44. – ст.21

2. Larson, Aaron (February 11, 2018). "Fair Use Doctrine and Copyright Law". ExpertLaw.com. Retrieved April 16, 2018.

3. Цивільний кодекс України: офіц. текст від 16 січня 2003 року. *Відомості Верховної Ради України.* 2003. № 40. – ст. 1109.

УДК 316.101

ІНФОРМАЦІЙНІ ВІЙНИ ТА ЇХ ВПЛИВ НА СУСПІЛЬСТВО

Артем Чупахін, Анастасія Корякіна

Харківський національний університет радіоелектроніки, м. Харків, Україна

Анотація. *Сьогодні рівень розвитку сектору інформаційно-комунікаційних технологій визначає роль держави у світовій економіці та її політичну вагу на міжнародній арені. Тому боротьба за інформацію, досягнення та утримання інформаційної переваги відіграє важливу роль у геополітичній конкуренції країн. Це призводить до поширення загроз інформаційній безпеці та, що ще гірше до інформаційних війн.*

Ключові слова: *інформаційна війна, інформаційна безпека, фейки, інформація, вплив на суспільство.*

Abstract. *Today, the level of development of the information and communication technologies sector determines the role of the state in the world economy and its political weight in the international arena. Therefore, the struggle for information, achieving and maintaining an information advantage plays an important role in the geopolitical competition of countries. This leads to the proliferation of threats to information security and, even worse, to information wars.*

Keywords: *information war, information security, fakes, information, influence on society.*

У сучасному світі інформаційна війна є одним із найнебезпечніших видів зброї. Використання секретної інформації, розповсюдження бруду, поширення неправдивої інформації, спроби ввести в оману інформацією стали сенсом життя для багатьох людей. А все тому що інформація має вплив на маси, тобто якщо вдало маніпулювати свідомістю мас, то можна досягти практично будь-якої мети: знищити опонента чи почати війну.

У журналістів і не тільки, зброя в руках, але не завжди вона використовується за призначенням. Беручи за фон останні події в Україні, можна зрозуміти, що основна боротьба між політичними силами ведеться за допомогою інформації, тобто в країні почалася інформаційна війна Не плутайте її з кібервійною – війною за домінування в кіберпросторі; з психологічною війною – війною за психологічну перевагу; радіоелектронною – боротьба за домінування в радіопросторі; кібервійна – війна за використання мережевих технологій.

Самі засоби масової комунікації є новим “природним ресурсом”, який збільшує суспільне багатство. Тобто конкуренція за кошти, площі збуту тощо відходить за лаштунки, переважно за отримання інформаційних ресурсів та знань, що призводить до війни в інформаційному просторі та за допомогою зброї інформаційного типу. Як ми всі знаємо, історія великомасштабних інформаційних технологій, відомих як “інформаційна війна”, налічує тисячі років. А М. Маклюен висуває цікаву тезу: “Справжня тотальна війна – це війна інформації”.

Інформаційна війна – це подання інформації таким чином, щоб сформувати необхідні думки, громадську думку, розгорнуту систему думок з певних питань, на користь організатора або групи осіб соціальної інформаційної пропаганди. У результаті виникає необхідне усвідомлення маніпулятором тих чи інших фактів чи подій, необхідна перспектива чи життєва позиція з питань, які раніше містили протиріччя чи непорозуміння. За відсутності протиріч і існуючих стійких систем думок завдання інформаційної війни полягає в тому, щоб породжувати сумніви, сіяти протиріччя і домисли в існуючі переконання.

Розвиток людини влаштований таким чином, що людина завжди шукає відповіді на хвилюючі її питання, і ці суперечливі питання є невід’ємною частиною постійного пізнавального процесу. У молодому віці, серед менш освічених верств суспільства, зі слабкою свідомістю, незрілістю і прогалинами в знаннях, завдання інформаційної війни полягає в тому, щоб закрити їх необхідною, легко засвоюваною і на перший погляд логічною інформацією. Безумовно, у міру підвищення обізнаності вразливість зменшується, і в цьому випадку інформаційна війна вимагає більш складних методів для створення підозри, використовуючи різноманітні прийоми, які спотворюють інформацію, наприклад, використання логічних доказів для підтвердження правдивості цих фактів, фальсифікація досліджень і докази припускають, що жертва повинна вірити і приймати їх як свої переконання.

Протиотрута від інформаційної війни – комплекс заходів під загальною назвою інформаційна гігієна, який розкриває механізм боротьби з інформаційною війною, простою мовою пояснює, як запобігти використання неправдивої інформації. Перевірка джерел інформації, виявлення фейкових новин, загальні просвітницькі кампанії, зосередження на можливому спотворенні окремих фактів супротивниками – це все антидоти

інформаційної війни. Деякі способи боротьби з фейковою інформацією зображені на рис. 1.

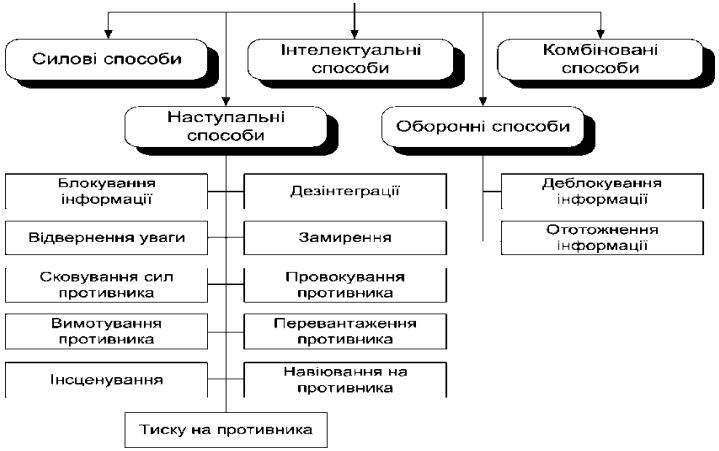


Рисунок 1 – Методи інформаційної боротьби

Російська Федерація веде безперервну інформаційну війну проти України з моменту проголошення Україною незалежності, особливо,з 2013-2014 років. Деякі з ключових завдань цієї інформаційної війни:

1. Знизити моральний дух українського населення.

2. Деморалізувати військовослужбовців і спонукати до зради.

3. У громадян Росії та України формується спотворене "медіабачення" того, що відбувається, а не його реальних причин і наслідків.

Поставлені завдання виконуються практично через повні канали зв'язку, в основному включаючи: традиційні ЗМІ, електронні ЗМІ (телебачення), інтернет ЗМІ, соціальні мережи.

Загалом, світ не стоїть на місці, і технічний прогрес озброює сучасну людину не лише новими вдосконаленими засобами виробництва та комунікації, а й засобами знищення себе та інших. Якщо правильно розуміти важливість інформаційних проблем, то сьогодні слід рухатися до їх подолання, адже інформаційна зброя здатна знищити найголовніше, що є у людини – її свідомість.

Інформаційні джерела

1. Інформаційна війна URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0 (дата звернення 10.11.2022).

2. Інформаційна війна – зброя масового знищення! URL: https://www. pravda.com.ua/rus/articles/2006/04/20/4399050/ (дата звернення 11.11.2022).

3. Поняття інформаційної війни URL: http://politics.ellib.org.ua/pages-8282.html (дата звернення 11.11.2022).

Секція 2

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Напрям 7

ПРИКЛАДНЕ ТА СИСТЕМНЕ ПРОГРАМУВАННЯ

UDC 004.9

DEVELOPMENT OF SOFTWARE FOR COUNTING THE NUMBER OF REPETITIONS OF PHYSICAL EXERCISES WITH VOICE CONTROL

Bohdan Bondarenko, Maryna Sydorova

Oles Honchar Dnipro National University, Dnipro, Ukraine

Анотація. *Прикладне програмне забезпечення є суттєвим помічником у найрізноманітніших сферах людського життя. Спорт та фізична активність не є виключенням. Метою цієї роботи є створення програмного додатку для контролю виконання фізичних вправ, який дозволяє розпізнавати, рахувати та вести статистику виконаних вправ користувача. Для спрощення взаємодії реалізовано голосове керування.*

Ключові слова*: програмний додаток, класифікація зображень, голосове керування.*

Abstract. *Application software is an essential assistant in the most diverse areas of human life. Sports and physical activity are no exception. The purpose of this work is to create a software application for monitoring the performance of physical exercises, which allows recognizing, counting and keeping statistics of the performed exercises of the user. To simplify interaction, voice control is implemented.*

Keywords: *software application, image classification, voice control.*

Movement is life, no one is going to argue with this, but, unfortunately, a huge number of factors, such as a pandemic, economic problems in various parts of the world, war – all of them have greatly changed the approach to life for lots of people. Many lost the opportunity to exercise due to the closure of gyms. Others cannot find enough time to pack their bags, go to some gym that is located far from home and return home after training. And this, in fact, is an enormous problem. Of course, you can question yourself – why go to the gym, if you can exercise right at your place? In fact, everything is not as simple as it seems. Gym sessions with friends are very different from exercising at home on your own. The biggest problem was, is, and always will be – motivation. Simple agreement with several friends to be in the gym at seven o'clock in the evening, makes it much more difficult to find a reason not to go there. Alone, a person can rarely find enough motivation and interest for such individual trainings, and even if this person can, it is, more likely, an exception to the rule than the rule itself. Fortunately, there is a fairly simple way to gain enough motivation to go to the gym or just to

exercise at home – music. It has been scientifically proven that music has the ability to provide significant positive effects for those engaged in sports and athletes, in particular, in the field of enhancing affective reactions and improving physical performance, as well as in terms of reducing perceived stress and more efficient use of oxygen [1]. What is more, it seems that the problem should be solved, but in fact – not yet, not so simple. There is one huge downside to training with music – it is impossible to properly count the number of repetitions of exercises when there is disco party in your ears. Loud and active music helps to concentrate on the correct execution of the exercise, but, as you can guess, interferes with counting the number of repetitions. Because of this, it was decided to develop an application that would count the number of repetitions of different exercises and help to fully concentrate on the correctness of physical exercise.

Voice-controlled software for image classification that would help monitor the performance of physical exercises, with possible expansion of functionality, had to be developed. Why exercises and image classification? How are those topics related? The thing is, a huge number of exercises consists of two states. The beginning of the exercise, conventionally, the lowest position, and the moment when we can say that the exercise was performed once, conventionally – the highest point. For example, for pull-ups: the first class – when a person hangs on straight arms, the second class – when a person is at the top point, that is, when you can say that the exercise has been completed one time, for dumbbell bicep curls, the first class, the beginning of the exercise is when the arm is almost completely relaxed, the dumbbell is at the lowest position, the second class – hand is contracted, and the dumbbell is at the highest position. Of course, not all exercises can be counted using this method. For example, isometric exercises such as the plank – globally consist of one class – the highest point, the body is tense and fixed. In the future, it is possible to develop a special features for static exercises, in which only the time of correct execution of the exercise will be calculated.

Globally, the main task was to separate the images into two classes, the images at the beginning of the exercise and the images of a certain peak point of the exercise. Various methods, algorithms and approaches for image classification were researched and considered solving the given problem. After that, based on the results of scientific research [2], it was decided to use several methods as Support Vector Machine (SVM), k-Nearest Neighbors (k-NN) and Random Forest. These methods proved to be the best during the initial tests of the application. Other methods, such as AdaBoost and Multi-layer Perception classifier, did not learn as fast and did not work as stable, that is why they were not included in the application.

The Python programming language was chosen to create the application. The GUI part was created using the Tkinter framework. The scikit-learn library was used as a source of classifiers, and the SpeechRecognition library was used to perform speech recognition. With the help of these tools, an application was developed. Using a built-in or external webcam, the application takes, works with and saves a certain number of photos for the first and second classes. After that, the application

trains the model and when counting function is enabled – counts the number of repetitions of the physical exercise. All the functions can be used with voice control.

The implementation of the ability to control the application with the help of voice brought a huge benefit and convenience when using the application. The most important part of the adequate operation of the classifier and the whole application is a sufficient number of high-quality photos, which could easily be divided into two classes. Therefore, the more photos are used to train the model, the better the classifier. It will positively influence determination of the current picture from the webcam and answer whether this picture belongs to a certain class. At the first stage of the development of the program, taking photos in the application took place only using a button in the interface. Each time the button was pressed, the application saved one photo. The problem was that for almost any physical exercise, this method was quite inconvenient. Even the usual dumbbell bicep curls required a fixed position, in which it was not very convenient to reach for a computer mouse or for a laptop and press the button to save the photo for one or another class. In addition, not all exercises can be performed while sitting in front of a webcam. For example – push-ups, pull-ups, squats, exercises with barbell, etc. All these problems are easily solved by voice recognition. The recognition itself takes place using the Google API Client. It can recognize multiple languages, but this software uses default settings, so it recognizes English language. A list of words is defined inside the application, and each time recognized text matches the defined word – various functions are activated, such as "take 50 photos", "train model", "start counting" and others. Basically, this allows the user to do things that have not been possible until now. Use case can be as simple as it seems. User activates voice recognition, move away from the webcam, take a comfortable starting position for physical exercise, then user says something like "first class", after which the application will take the selected number of photos. Next steps are "second class", "train model", "count" or "start counting".

Quite helpful feature that has been implemented, added an ability to save trained model or load previously created one. This saves the user a huge amount of time, since it is not necessary to take photos for both classes and train the model each time the user wants to exercise.

During the implementation of the application, the problem of software with similar functionality was identified and resolved. Due to the constant display of the main interface and the image from the webcam, any third-party process, like speech recognition or model training, led to a complete freeze of the interface along with the image from the webcam. In order to solve this – the async module was used.

References

1. Terry P. C., Karageorghis C. I., Curran M. L., Martin O. V., & Parsons-Smith R. L. (2019, December 5). Effects of Music in Exercise and Sport: A Meta-Analytic Review. Psychological Bulletin

2. Laura Morán-Fernández Verónica Bólon-Canedo Amparo Alonso-Betanzos How important is data quality? Best classifiers vs best features. Neurocomputing. 2022. Vol. 470, P.365-375. URL: https://www.sciencedirect.com/ science/article/pii/ S0925231221011127

УДК 004.85

"TEMPERATURKA BOT": A CHAT-BOT IS LAUNCHED THAT HELPS MONITOR YOUR HEALTH

Nazar Hembara

Chef Executive Officer of Chatbot development company BotsCrew
548 Market St #39969, San Francisco, California 94104, USA

Abstract. *In order to decide which chatbot we want to create, we need to find out what types they are and what their functional differences are. A chatbot is similar to a regular messaging app, but the difference is when one of the recipients of the messages is a bot. In other words, to describe a situation like when a person communicates with a robot (computer). Conversation messages can be sent using several means, such as voice commands, test chats, graphical interfaces, or graphical widgets. Today, chatbots are a popular system that, by themselves, can help a person in performing many tasks. In particular, a developed chatbot for detecting the symptoms of the coronavirus is presented.*

Keywords: *chat bot, program, messenger, robot, widget.*

Анотація. *Для того, щоб вирішити який чат-бот ми хочемо створити, потрібно визначити яких актуальних типів вони бувають і яка різниця їх функціоналів. Чат-бот схожий на звичайну програму для обміну повідомленнями, але відмінність полягає в тому, що одним із одержувачів повідомлень є робот. Іншими словами, щоб описати ситуацію, як коли людина спілкується з роботом (комп'ютером). Повідомлення розмови можна надсилати за допомогою кількох засобів, таких як голосові команди, тестові чати, графічні інтерфейси або графічні віджети. На сьогодні чат-боти є популярною системою, яка, власноруч, може допомогти людині у виконанні багатьох завдань. Зокрема представлений розроблений чат-бот для виявлення симптомів коронавірусу.*

Ключові слова:*чат-бот, програма, месенжер, робот, віджет.*

The first information about the bot can be considered an experiment – namely, the Turing test, published in 1950, which boils down to the fact that artificial intelligence can be recognized as a program capable of conducting a similar conversation to a person In 1966, MIT professor Joseph Weitzenbaum wrote the ELIZA program. She imitated the speech of the stereotypical psychotherapist, constantly answering the lines of the human interlocutor with counter questions. Although communication was an illusion, and a primitive one at that, Weisenbaum was amazed by how much people were interested in the conversation [1].

By 1990, the tree-based rule sets underlying ELIZA and other similar programs had become so elaborate and complex that the test Turing turned from a philosophical concept into a real test. The annual AI Loebner Award was established. Then the very concept of "chat-bot" appeared. It is customary to associate it with Julia – electronic assistant, designed by Michael moldings in 1994. Julia was much better at simulating communication than her predecessors, but still used key words to select appropriate cues. It was a year later featured bot A.L.I.C.E. (Artificial Linguistic Internet Computer Entity), which formulates appropriate phrases using heuristic pattern analysis. Communication with A.L.I.C.E. already resembled a full-fledged dialogue. The program never passed the Turing test, but it was recognized three times (in 2000, 2001, 2004) as the best chatbot of the AI Loebner competition. Beat this record succeeded Mitsuku, developed by the British Steve Worswick, only in 2018. In 2006, the IBM company began the development of the supercomputer Watson, which has encyclopedic knowledge and could provide answers to questions, asked aloud Four years later, similar solutions became available to the general public. Apple introduced the voice assistant Siri (Speech 12 Interpretation and Recognition Interface), and then appeared Google Now, Alexa from Amazon, Microsoft Cortana and Yandex Alice [1]. At the same time, the principles and technologies of machine learning that underlie voice assistants have ceased to be the prerogative of corporations. With their help, classic chatbots have become much smarter, have become reliable enough for commercial use and became popular with users.

Today, bots are becoming the de facto interface standard for interacting with software services. This is due to the widespread use of messaging platforms (for example, Facebook Messenger for users of the social network and Slack for developers), and thanks in part to advances in natural language understanding tools, which are supported by many bots. Another driving force is the massive use of big data and machine learning algorithms: bots are convenient as a user interface 13 for interacting with systems that provide answers based on the results of the analysis of huge volumes of information. Large software companies recognize the convenience of bots for the integration of services, communication channels and user association. Facebook, for example, wants to gradually replace bots on the exchange platform all programs with Messenger messages, and Microsoft claims that the operating system of the future is "a dialogue as a platform".

Lviv IT Cluster together with the BotsCrew company presented the "Bot Temperature" project in Lviv. This is a special chatbot that will help you monitor your health on a daily basis. Lviv Mayor Andriy Sadovy invited

everyone to actively use the chatbot, and young people to teach their parents, grandparents [2]. Now it's even easier to monitor your health. Lviv IT Cluster together with the company BotsCrew developed TemperaturkaBot.

The app asks the user about their health and symptoms of COVID-19 via FaceBook Messenger. If signs of the disease are detected, the application recommends staying at home or contacting a doctor. In this way, we can understand what the average temperature is in Lviv. It is very useful and convenient. You can join here – https://bit.ly/2BWnp1O

Take care! "Andriy Sadovy noted". This is a chatbot in FaceBook Messenger that allows you to collect information about a person's state of health and give him recommendations, whether he has symptoms of the coronavirus or not. There is a link to a FaceBook page and you can message him just like you communicate with your colleagues and friends. He asks what is your temperature, and then – the most popular symptoms – whether there is shortness of breath, whether there were contacts with confirmed infected people, there are questions about travel, etc. "I will definitely use it and recommend it to my friends. Young people are responsible for their health and the health of their relatives. It is necessary to teach grandparents and parents how to use this chatbot, to do everything possible to make it a daily use", said Andriy Sadovy, the mayor of the city.

The chatbot works on the basis of the Facebook Messenger platform. Every day, the bot sends an automatic reminder for the user to update their stats and share information about themselves. This happens in a fairly easy and playful way. Therefore, the project will allow monitoring the dynamics of indicators of people's well-being and body temperature.

In addition, on the basis of the results received from the users of the project, a depersonalized analysis of the symptoms of the users will take place. Therefore, it will become an additional source of information for assessing the epidemiological situation. The project is implemented with the support of Lviv IT Cluster as part of the United for Health initiative [2].

References

1. Tvoroshenko I., and Gorokhovatskyi V. (2022) The Application of Hybrid Intelligence Systems for Dynamic Data Analysis, International Journal of Engineering and Information Systems, 6(2), pp. 40–48.

2. Lviv City Council: https://city-adm.lviv.ua/news/science-and-health/medicine/279960-temperaturka-bot-u-lvovi-zapratsiuvav-chat-bot-iakyi-dopomahaie-kontroliuvaty-stan-svoho-zdorovia.

УДК 004.09

RESEARCH OF THE PROBLEM AND CREATION OF A WEB-BASED DECISION SUPPORT APPLICATION BASED ON EXPERT EVALUATION

Serhii Vakulchyk, Maryna Sydorova

Oles Honchar Dnipro National University, Dnipro, Ukraine

Abstract. *Almost any sphere of human activity is associated with the need to make decisions. The aim of this work is to develop a web application for expert evaluation and decision support based on collective choice methods, which will allow to quickly and efficiently generate recommendations to a person, based on expert assessments and collective choice methods.*

Keywords: *expert evaluation, decision making methods, Saaty method, web application, Angular 14, ASP.NET Core.*

Анотація. *Майже будь-яка сфера діяльності людини пов'язана з необхідністю прийняття рішень. Метою цієї роботи є розроблення вебдодатку для експертного оцінювання та підтримки прийняття рішень на основі методів колективного вибору, що дозволить швидко та якісно сформувати рекомендації особі, на основі експертних оцінок та методів колективного вибору.*

Ключові слова: *експертне оцінювання, методи прийняття рішень, метод Саати, вебдодаток, Angular 14, ASP.NET Core.*

Almost any field of human activity is inextricably linked to decision-making processes. People have always made decisions based on their own experience, intuition and common sense. In this case, as a rule, the author himself is not able to describe the exact path that led to the choice of the decision, although there is every reason to believe that he somehow took into account and weighed all aspects of the decision. The ability to make decisions that give the best results in various difficult situations has always been considered an art.

Decision theory studies the process of how people choose to solve complex problems. Under decision making we will understand a special process of human activity aimed at choosing the best course of action.

Aristotle formulated a basic concept describing the decision-making approach. During the Second World War, based on military needs, a formal mathematical approach was fully implemented within the theory of operations research. The science of choosing the best decision option as an independent discipline – decision theory – was developed quite recently, in the early 1960s. At the same time, the main goal of this theory was formulated – to rationalize the decision-making process.

In general, the decision-making problem consists in ranking alternatives by quantitative estimates of their expected efficiency.

Decision theory methods are designed to support decision making in the study of complex systems (environmental, economic, technical). Examples of tasks can be any elections (presidential, parliamentary), the process of choosing the purchase of equipment (mobile phone, TV, washing machine), choosing the direction of potential investment, evaluation of job offers.

The decision-making problem arises when there is a certain number of given alternatives (choices) in order to achieve a certain result. In this case, the best alternative in a certain sense is chosen.

The most important role in decision making is played by a person who is called a decision maker. As a rule, this is a competent person in his/her field, who has some experience and relevant authority. There is also a problem owner – a person who has to solve the problem and take responsibility for it. Very often the decision maker and the problem owner are different people. Often, professionals, experts in a particular field are involved in the decision-making process to solve the problem.

Automation of the expert evaluation process and processing of results for aggregation of preferences is a relevant area of research. Therefore, the aim of this work is to create a web application for expert evaluation and decision support based on collective choice methods, which will allow you to quickly and efficiently generate recommendations to a person based on expert assessments and collective choice methods.

In order to make a certain decision, a goal must be formulated – the goal that one wants to achieve by making a decision.

In the decision-making process, there are always several options for achieving a certain goal, i.e. decision options. They are called alternatives. Alternatives can be independent and dependent. Independent alternatives are such alternatives, any action with which does not affect the quality of other alternatives.

Each alternative has a certain number of properties that influence the potential choice of one of the alternatives. Each property is a certain degree of influence of alternatives on achieving a given result. This property is called a criterion – some category that reflects an important property of the alternative. There are quantitative and qualitative criteria.

Quantitative criterion – reflects a property of an alternative that can be measured on some common scale, such as weight, cost, distance.

Qualitative criterion – reflects the property of the alternative that cannot be naturally expressed in numbers, for example, the quality of comfort, the level of motivation of employees.

The analytical hierarchy approach is appropriate when we have a rather small number of options for solving the problem, i.e. alternatives. The approach can be divided into several stages:

− structuring the problem in the form with several levels: goal, criteria, alternatives;

− carrying out pairwise comparisons of the elements of each level. The results of comparisons are converting into numbers;

− calculation of importance coefficients for the elements of each level;

− calculate the quality weight of each alternative and determine the best one.

At the lower level of the hierarchical scheme, the given alternatives are compared for each criterion separately.

The main advantage of the analytical hierarchy method is its focus on comparing realistically given alternatives. Also this method can be applied even when experts cannot accurately assess the given criteria.

However, there is also a rather significant disadvantage of the analytical hierarchy method – the addition of a new alternative can lead to a change in the preferences of the previously given two alternatives.

As a result of the work, a web application was developed to solve the problem of decision-making using analytical hierarchy methods. The following tasks were implemented:

− the main structure of main application was created, the backend and frontend parts were configured;

− developed the functionality of user registration and authorization;

− the file format for reading is selected, it structure is developed;

− parsing data from a file is implemented;

− the algorithm of analytical hierarchy is implemented;

− an algorithm was applied based on the created files;

− the quality of the obtained results was assessed and conclusions were drawn for further research on the theory of analytical hierarchy methods.

The author of the expertise has the opportunity to involve experts, the scores are stored in the database and used as input for collective decision-making methods. The software also makes it possible to assess the competence and consistency of experts, which is quite important in the methods of aggregation of preferences. The system consists of two modules, the first module is designed to ensure the functioning of the site, and the second is the computational part, which implements the computational schemes of the methods.

To create the application, the programming language C# and the platform for developing web applications ASP.NET Core were chosen – for backend development, the frontend part was developed using the Angular 14 Framework.

During the development, the Saaty analytical hierarchy method was used to solve the decision-making problem. Various experiments were conducted with different data sets (different number and order of criteria, adding new alternatives).

References

1. Ємел'яненко Т.Г. Основи теорії прийняття рішень: навч. посіб. / Т.Г. Ємел'яненко. – Д.: РВВ ДНУ, 2010. – 60с.

2. Опорний коспект лекцій з дисципліни "Теорія прийняття рішень"| [Електроний ресурс] URL : https:// http://dspace.wunu.edu.ua/retrieve/52501/lek.pdf

УДК 004.056

ДОСЛІДЖЕННЯ СУЧАСНИХ АСПЕКТІВ КЛАСИФІКАЦІЇ ДОДАТКІВ

Олеся Головата, Сергій Попитак, Марія Навитка

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україні

Анотація. *В роботі проведено аналіз систематизації додатків. Призначення, область використання, інтерфейс, область використання та уніфікованість залишаються головними критеріями в класифікації додатків.*

Ключові слова*: додаток, застосунок, програмне забезпечення, Web-додатки, мобільні застосунки, Desktop-застосунки.*

Abstract. *The paper analyzes the systematization of applications. Purpose, field of use, interface, field of use and uniformity remain the main criteria in the classification of applications.*

Keywords: *application, application, software, Web applications, mobile applications, Desktop applications.*

Технології стрімко розвиваються, багатозадачні застосунки стають неактуальними, адже швидкість та продуктивність таких застосунків є дуже низькою. Така низька швидкість пов'язана із вічним "діалогом" користувача із сервером, адже на кожну дію користувача з сервера запитується нова сторінка і відбувається повне перезавантаження застосунку, навіть якщо зміни були незначними. На зміну їм прийшли швидкі, динамічні, інтерактивні, нелегкі в проєктуванні і розробленні невеликі застосунки, але завдяки великій кількості логіки як на клієнтській, так і на серверній частинах їх можна називати повноцінними Додатками. Додаток – це набір інструкцій у вигляді слів, цифр, кодів, схем, символів, або у будь-якому вигляді, що в подальшому виражається в такій формі, яка придатна для зчитування комп'ютером та керують роботою комп'ютера для досягнення бажаного результату. Саме в цей момент перед розробниками постало питання підвищення швидкості і продуктивності Додатків, адже користувачі стають все більш не терплячими та вимогливими, тому неправильно обрані методи та інструменти розроблення Додатка можуть призвести до провального проєкту, який залишиться поза увагою клієнтів.

За призначенням додатки можна поділити на:

− Прикладні – ті які вирішують прикладні (буденні), однотипні задачі, наприклад та дають конкретний результат. Наприклад: редактори тексту, електронні таблиці, графічні редактори.

− Пакети прикладних програм – це комплекс взаємопов’язаних між собою прикладних програм. Наприклад пакет Microsoft Office до якого входить Word, Excel, PowerPoint, Teams і тд.

− Системні – ті які взаємодіють з операційною системою, або залізом комп’ютера. В основному вони призначені для забезпечення працездатності ПК, його налагодження і тд. До цих додатків відносяться наприклад операційні системи, або драйвери.

− Інструментальні – призначені для написання програм. Прикладами таких додатків є інтегровані середовища розробки, такі як Eclipse, PyCharm, CLion, Visual Studio Code і тд.

− Системи управління базами даних – комплекс програм і мовних засобів, призначених для створення, ведення і використання баз даних.

Відносно області використання:

− Вертикальне програмне забезпечення – розроблене за індивідуальним замовленням для конкретного завдання

− Горизонтальне програмне забезпечення – призначене для масового використання, та вирішення широкого кола задач

За інтерфейсом:

− Web-додатки – ті додатки, взаємодія з якими відбувається у браузері, а логіка самої програми виконується на віддаленому сервері.

− Desktop-застосунки – такі додатки, які відкриваються в робочому вікні комп’ютера.

− Мобільні застосунки, ті що працюють на смартфонах під керуванням операційної системи Android, або IOS.

За ступенем уніфікованості:

− Платформозалежні застосунки – це ті, що працюють на одному типі пристрою або операційній системі.

− Кросплатформові застосунки – здатні працювати незалежно від різновиду пристрою, архітектури його процесора або операційної системи.

Розробка додатків – це комплексний процес, який передбачає залучення широкого спектру спеціалістів та технологій. У ході реалізації мають бути передбачені конкретно визначені рамки обов’язків всіх учасників розробки, а також інструкції та порядок залучення спеціалістів.

Інформаційні джерела

1. Онищенко С. В. WEB-технології: навч.-метод. комплекс. Бердянськ: “БДПУ”, 2016. 500 с.

2. Алексенко О. В. Технології програмування та створення програмних продуктів: конспект лекцій. – Суми : Сумський державний університет, 2013. – 133 с.

3. Створення додатків за допомогою Eclipse. Eclipse: веб-сайт. URL: https://www.eclipse.org/articles/Article-EclipseDbWebapps/article.html

4. Android Studio – це офіційне інтегроване середовище розробки. Android Studio: веб-сайт. URL: https ://developer.android.com/studio/intro.

УДК 004.056

АНАЛІЗ ВЕРТИКАЛІ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Даніїл Гриченко, Олександр Синиця, Марія Навитка

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *З метою стандартизації та удосконалення процесу розробки, запроваджено стандарт ISO/IEC 12207:2008 "System and software engineering – Software life cycle processes" В даній статті проведено аналіз робіт на кожному етапі розробки програмного забезпечення згідно стандарт ISO/IEC 12207:2008 :розгляд предметної області, проєктування структури програми та дизайну інтерфейсу, реалізації в коді, тестування та впровадження програми, підтримка ПЗ та рішення про цілковиту відмову від використання програми.*

Ключові слова: *програмне забезпечення, предметна область.*

Abstract. *In order to standardize and improve the development process, the ISO/IEC 12207:2008 standard "System and software engineering – Software life cycle processes" was introduced. This article analyzes the work at each stage of software development according to the ISO/IEC 12207:2008 standard: review of the subject of the field, design of the program structure and interface design, implementation in the code, testing and implementation of the program, software support and the decision to completely abandon the use of the program.*

Keywords: *software, subject area.*

Розробка програмного забезпечення це не лише написання програми та отримання оплати за роботу. Це набагато ширше поняття, яке включає в себе підтримку, виправлення помилок, системний аналіз не лише особливостей систем моделювання і розробки, але й предметної області. Розробка додатку починається з потреби в самому додатку. Якщо на ринку ще не існує рішень, які б змогли її задовольнити, єдиним виходом залишається розробити, самостійно, або із залученням спеціалістів, цей додаток.

Зазвичай для масштабних проєктів, великі фірми звертаються до аутсорсингових компаній, які і розроблятимуть для них цей продукт, використовуючи певний стандарт.

Після встановлення потреби, визначаються вимоги до майбутнього програмного забезпечення. Тут замовник, разом з бізнес аналітиками IT компанії опрацьовує чіткий план того що повинен вміти майбутній застосунок. В результаті чого складається технічне завдання. Також на цьому етапі дуже важливою компонентою є словник термінів, що будуть використані в проєкті. Потрібен він тому що програмісти не є інженерами широкого профілю і якщо програмне забезпечення призначене для, наприклад, медичної сфери, то очевидно в інтерфейсі цієї програми будуть вживатися

певні медичні терміни які невідомі програмістам. Тому для коректного написання програми він потрібен.

Коли по завершенню першого етапу є готове технічне завдання і словник, переходять до наступного – проєктування. До роботи беруться архітектори і дизайнери. Архітектори створюють віртуальну модель застосунку. Вона може бути не остаточна та може змінюватись в процесі написання, проте зараз від неї все буде відштовхуватись. Що стосується дизайнерів, то вони створюють прототип інтерфейсу.

Маючи прототип інтерфейсу і дизайн, розробники створюють саму програму. В результаті цього буде отримано програмний код – те що працює, і програмну документацію – те що пояснює як працює код.

Після написання коду, обов'язково наступає фаза тестування. Якщо зануритись в історію розвитку IT, то років 10-15 тому, тестерів як таких не було і програмісти самі тестували свій код. Проте поєднувати ці дві роботи було занадто довго, важко і в підсумку неякісно. Тому ці два завдання розділили і з'явилася така професія як тестувальник. Тестувальник програмного забезпечення потрібен для того щоб перевіряти код написаний програмістами. В залежності від того яку помилку буде виявлено тестувальниками, роботу буде повернено на відповідний етап на доопрацювання. Якщо програма не працює – її повертають розробникам. Якщо специфікація не є задоволена, тобто програма робить не те чого хотів замовник, її повертають на стадію проєктування. Якщо взагалі виявиться що реалізація тих речей які хоче замовник є неможлива, її буде повернено на стадію визначення вимог, а всі етапи доведеться проходити повторно.

Коли програма вже є відтестованою – її видають замовнику, починається етап експлуатації. Також разом із програмою замовник отримує так званий комплект поставки, який може включати в себе як інструкцію з використання, так і повноцінні навчання персоналу. Під час використання програми збираються відгуки, показники експлуатації, виправляються проблеми а також за потреби дописується новий функціонал, згідно вищеописаного плану. Завершується все в момент коли програмне забезпечення стає неактуальним для використання.

Отже, успішна розробка програмних застосунків потребує компетенцій великої кількості спеціалістів і фахівців різних областей знань. Від дизайнерів, аналітиків і бізнесменів, до програмістів, електротехніків та інженерів, а також чіткого дотримання встановленого порядку дій.

Інформаційні джерела

1. Systems and software engineering – Software Life Cycle Processes. ISO 12207:2008. – [Чинний від 2008-02-01] – II, 122 с.– (Міжнародний стандарт).

2. Алексенко О. В. Технології програмування та створення програмних продуктів: конспект лекцій. – Суми : Сумський державний університет, 2013. – 133 с.

УДК 004.9

ПРОГРАМНИЙ МОДУЛЬ НЕПРЯМИХ МЕТОДІВ ПОБУДОВИ ФУНКЦІЙ НАЛЕЖНОСТІ

Артем Гречка, Наталія Науменко

ДВНЗ "Український державний хіміко-технологічний університет", м. Дніпро, Україна

Анотація. *У роботі пропонується формалізувати дані з використанням апарату теорії нечітких множин. Розглядається прикладна задача інформаційної оцінки поточних конкурентних можливостей підприємства, яка використовує дані опитування експертів. Отримані експертні оцінки у роботі пропонується формалізувати у вигляді побудови функцій належності при використанні непрямих методів. Згідно експертних оцінок формуються терми нечітких множин по кожній лінгвістичній змінній.*

Ключові слова: *теорія нечітких множин, непрямі методи побудови функцій належності, функції належності, експертні оцінки.*

Abstract. *The paper proposes to formalize the data using the apparatus of fuzzy set theory. The applied problem of information assessment of the current competitive capabilities of the enterprise, which uses the data of the survey of experts, is considered. It is proposed to formalize the obtained expert evaluations by constructing membership functions using indirect methods. According to expert assessment, terms of fuzzy sets are formed for each linguistic variable.*

Keywords: *theory of fuzzy sets, indirect methods of construction of membership functions, membership functions, expert evaluations.*

З різними видами тієї чи іншої нечіткості та розмитості даних доводиться стикатися у різних предметних областях. При застосуванні детермінованих підходів відбувається втрата деякої інформації та зміст таких даних. Досить часто формалізація їх є непростим та складним процесом, але при успішному вирішенні такого питання надає широкі можливості використання нечіткого підходу [1, 2].

Прийняття рішень в умовах невизначеності набуває особового значення та верифікація результатів потребує особливої уваги. Як відомо, математичний апарат теорії нечіткості виявився достатньо корисним та затребуваним у самих різних прикладних предметних областях, у тому числі: в хімічній технології та медицині; в теорії надійності та при контролі якості продукції; при автоматизованому управлінні рухом; при нечіткому оцінюванні земель; при проєктуванні складних механічних систем та в економіці [3–5].

Інформація, яку отримано з використанням знань експертів у даній предметній області, потребує додаткового опрацювання, а саме: відповіді угруповують в блоки за визначеною методологією [6]. Ділиться банк питань відповідним чином, наприклад, за критеріями можливостей та конкурентоспроможності. Після виділення основного блоку питань можна розглядати кожну таку змінну як складну (агреговану) лінгвістичну змінну. Кожна змінна є складною тому, що вона містить об'єднання питань окремого блоку.

Як відомо, від проєктувальника нечіткої системи залежить вибір термів, причому їх кількість не повинна бути завеликою або замалою. У роботі пропонується кількість термів рівною п'яти: велике ("В"), вище середнього ("ВС"), середнє ("С"), нижче середнього ("НС"), низьке ("Н"). Відповіді на кожне питання можуть містить вказані п'ять значень термів лінгвістичної змінної.

У роботі для формалізації нечіткої інформації реалізовано два непрямих методи побудови функцій належності: метод статистичних даних та метод попарних порівнянь, які реалізовано у відповідному програмному забезпеченні на мові програмування Python.

Для реалізації методу побудови функцій належності на основі методу статистичних даних було реалізовано наступний алгоритм:

1 крок. Задається лінгвістична змінна X.

2 крок. Визначити універсальну множину, на якому задається змінна X.

3 крок. Задати сукупність нечітких термів $\{S_1, S_2, \ldots, S_n\}$, які використовуються для оцінки змінної X.

4 крок. Для кожного терму формується матриця підказок відповідним чином $S = \|s_{ij}\|$.

5 крок. Обчислити значення функції належності для кожного терму. Виконати нормування шляхом ділення на найбільші степені належності.

Алгоритм було доповнено тим, що результати опитування є неструктурованими даними, тому завдяки їх формалізації (у вигляді функцій належності) можна виконувати впорядкування даних. Зокрема, завдяки функціям належності можна впорядкувати питання і в середині кожного блоку, звісно, якщо виникає така необхідність.

Альтернативою методу статистичних даних є у роботі алгоритм попарних порівнянь, який використовується приблизно таким же самим чином. Переваги та недоліки запропонованих непрямих методів є відомими та не потребують додаткових пояснень. Звісно, що використання кожного з них залежить від вхідних даних та переваг користувача. Запропонований у роботі підхід для систематизації даних з використанням непрямих методів

побудови дозволяє не тільки ці дані структурувати, але й за рахунок візуалізації процесу, надає можливість користувачеві змінювати кількість термів, наприклад, у сторону їх зменшення.

Створене програмне забезпечення містить наступні модулі: формалізації даних двома непрямими методами (алгоритм статистичних даних та попарних порівнянь), інформаційні блоки, упорядкування та систематизації даних, візуалізації процесу структурування результатів опитування. Формалізований кількісний аналіз має свої межі [6], за якими можуть бути втрачені якість, глибина і повнота осмислення дійсності. Тому в гуманітарних дослідженнях необхідно використовувати м'які методи, одним з яких і є нечітка логіка.

Фактично можна вважати, що такі впорядковані дані можуть бути використані як підґрунтя для побудови нечіткої бази знань, яка може слугувати основою нечіткої системи. Звісно, що структура отриманої бази знань потребуватиме деякого опрацювання, але це не є розглядом даної роботи. Автор хоче лише зазначити про можливість подальшого застосування отриманих у роботі результатів. Як відомо, процес формалізації нечіткої інформації потребує подальшого використання, наприклад, при застосування побудованої повної бази знань та використання алгоритмів нечіткого логічного виведення.

Інформаційні джерела

1. Zadeh Lotfi A., Chuen-Chien Lee Fuzzy Logic in Control Systems: Fuzzy Logic Controller. *IEEE Transactions on systems, man, and cybernetics*. 1990. Part II, Vol. 20, № 2. P. 404-418. 2. Sosnin K., Tkachev V., Us S., Taradaichenko M. Multiobjective identification of convective drying of grain based on fuzzy sets. *19th International Drying Symposium*, Lyon, France, 2014. August 24–27.

3. Korotka L. I. The use of fuzzy clustering in solving problem in predicting the durability of corrosive structures. *Mathematical modeling.* 2020. №2(43). P. 44–54.

4. Harmider L. D., Taranenko I. V., Korotka L. I., Begma P. O. Methodological approach to labor potential assessment based on the use of fuzzy sets theory. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2019. № 6. P. 144–149.

5. Ovcharenko O., Korotka L., Smiesova V., Kuchkova O., Karpenko R. Economic security of regions: A methodological approach to assessment, management, and legal regulation. *Region: The journal of ERSA*. 2022. Vol. 9, Nu. 1, pp. 83–100.

6. Нефедова О.Г. Формування конкурентоспроможного адаптаційного потенціалу підприємства в умовах нестабільності ринку: дис. канд. ек. наук: 08.00.04. Національний університет "Одеська політехніка", м. Одеса, 2021. 217 с.

УДК 005.8

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРОЄКТАХ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ ПРИ РОЗРАХУНКУ ЧАСУ ЕВАКУАЦІЇ ЛЮДЕЙ

Андрій Івануса, Тарас Репетило, Даниїл Кашуба

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Проведено інформаційний аналіз предметної області використання сучасних інформаційних продуктів у проєктах забезпечення безпеки на об'єктах масового перебування людей. Розроблено концептуальну модель забезпечення людей на об'єктах їх масового перебування. Використовуючи існуючий математичний апарат, що описує рух потоків людей по споруді, а також топологічне моделювання, розроблено прикладне програмне забезпечення, що дозволяє проводити автоматизацію розрахунку часу евакуації людей із споруд у безпечну зону.*

Ключові слова: *інформаційні технології, евакуаціє людей, об'єкт масового перебування людей.*

Abstract. *An information analysis of the subject area of the use of modern information products in projects to ensure security at objects of mass presence of people was carried out. A conceptual model of providing for people at the objects of their mass stay has been developed. Using the existing mathematical apparatus, which describes the movement of people's flows through the building, as well as topological modeling, application software has been developed that allows you to automate the calculation of the time of evacuation of people from buildings to a safe zone.*

Keywords: *information technologies, evacuation of people, object of mass stay of people.*

Підвищення ефективності реалізації програми створення та розвитку системи безпеки на об'єктах масового перебування людей потребує використання методів та моделей, що побудовані на основі використання інформаційних технологій, системного підходу та проєктно-орієнтованого управління [1].

Для побудови моделей руху людських потоків, на основі аналізу причинно-наслідкових зв'язків і використання японської системи знань P2M, початково побудована концептуальна модель управління проєктами безпечної експлуатації (УПБЕ) об'єктів масового перебування людей (ОМПЛ), яка враховує: стан турбулентного середовища споруди, рівень проведення спортивних та культурно-масових заходів, ключові фактори успіху реалізації проєктів, нормативно-правову базу України, психофізіо-

логічний стан людей, стратегічні цілі, показники результативності. Схема реалізації такої моделі представлена на рис. 1.

Рисунок 1 – Концептуальна модель управління проєктами безпечної експлуатації об'єктів масового перебування людей

У створеній моделі закладено, що результатом успішної реалізації проєктів безпечної експлуатації ОМПЛ є збережене життя та здоров'я людей під час перебування на споруді, які виступають в ролі зацікавлених сторін проєкту. Моделі управління зацікавленими сторонами відображають евакуаційні маршрути руху потоків людей із споруди в безпечну зону, а також параметри, що вливають на рух людей на окремих евакуаційних ділянках, які потрібно враховувати при проведенні розрахунку часу їх евакуації.

Враховуючи, що процес руху зацікавлених сторін проєктів БЕ СВС характеризується такими динамічними параметрами, як щільність "*D*", швидкість "*V*", кількість користувачів "*N*", геометричні параметри сходів "*M*", напрямки руху "*S*", архітектуру споруди "*A*", довжина евакуаційного маршруту "*L*", психологічний стан користувачів "E" та інформаційне забезпечення користувачів "*I*" тощо, цільову функцію потоку зацікавлених сторін проєктів при евакуації із СВС у безпечну зону можна показати у вигляді кортежу:

$$F(x) = \langle D, V, N, M, S, A, L, E, I, O, P, HC \rangle, \quad (1)$$

де: *O* – природні умови, *P* – рівень проведення спортивних змагань (територіальний, державний, міжнародний), *HC* – тип надзвичайної ситуації.

Використовуючи методику наведену в [2] та моделі розроблені в працях [3, 4], що описують рух потоків людей на спорудах масового їх пере-

бування було створено програмний продукт (рис. 2), який забезпечить автоматизацію проведення необхідних розрахунків. Результати розрахунків покажуть спроможність евакуаційної системи забезпечити своєчасну евакуацію людей із споруди в межах регламентованого часу та необхідність проведення оптимізації руху потоків зацікавлених сторін проєктів.

Рисунок 2 – Виведення результатів проведеного розрахунку часу евакуації людей у програмі “ТОПАЛ-ЕВАКАС 1.0”

За допомогою програми було проведено почерговий розрахунок часу евакуації людей із спортивно-видовищної споруди “Арена Львів”. Працювати з комп’ютерною програмою “ТОПАЛ-ЕВАКАС 1.0” можна на будь-якому персональному комп’ютері, який відповідає зазначеним мінімальним вимогам.

Інформаційні джерела

1. Зачко О.Б., Івануса А.І., Кобилкін Д.С. Управління проектами: теорія, практика, інформаційні технології [навчальний посібник]. – Львів: ЛДУ БЖД, 2019. – 173 с.

2. ДСТУ 8828:2019. Пожежна безпека. Загальні положення. [Чинний від 2020-01-01]. Вид. офіц. Київ, 2018. 163 с.

3. Ivanusa A. Project of forming culture and safety of the airport // MATEC Web of Conferences, V. 247, 00045 (2018) https://doi.org/10.1051/matecconf/ 20182470004

4. Івануса А. І., Яковчук Р. С., Ємельяненко С. О., Івануса З. З. Управлінські та інформаційні особливості проекту безпечної експлуатації спортивно-видовищних споруд. Науковий вісник НЛТУ України. 2019, т. 29, № 8. С. 134–141.

5. Івануса А.І. Методи та моделі безпеко-орієнтованого управління зацікавленими сторонами проектів у системі цивільного захисту / А.І. Івануса, С.О. Ємельяненко, Є.В. Морщ // Вісник Львівського державного університету безпеки життєдіяльності: зб. наук. праць. – Львів, 2019. – С. 36–43.

УДК 004.056

НАЙВАЖЛИВІШІ ПЕРЕВАГИ СУЧАСНИХ ФРЕЙМВОРКІВ ДЛЯ ПОБУДОВИ WEB-ДОДАТКІВ

Марія Навитка, Катерина Стецик, Андрій Івануса

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Фреймворки визначають правила розробки архітектури програми: вони мають скелетну структуру, яка розширюється та змінюється відповідно до вимог. Розробникам не потрібно починати проєкти з нуля, оскільки вони вже мають основу для впровадження інших функцій, що стосуються конкретного проєкту. Ринок frontend розробки досить динамічний і мінливий. Незважаючи на те, що React, Angular і Vue.js все ще є лідерами серед інтерфейсних фреймворків, нові фреймворки та бібліотеки активно розробляються та набирають обертів.*

В даній статті проведено аналіз сучасних фреймворків. Наведено перелік інтерфейсних фреймворків та представлено переваги використання фронтенд-фреймворків.

Ключові слова: *фреймворк, React.js, Angular, Vue.js, Svelte, Ember.js, Backbone.js та Preact.*

Abstract. *Frameworks define the rules for developing the architecture of an application: they have a skeletal structure that expands and changes according to requirements. Developers don't need to start projects from scratch because they already have the foundation to implement other project-specific features. The frontend development market is quite dynamic and changing. While React, Angular, and Vue.js are still the front-end framework leaders, new frameworks and libraries are being developed and gaining momentum.*

This article analyzes modern frameworks. The list of interface frameworks is given and the advantages of using front-end frameworks are presented.

Keywords: *framework, React.js, Angular, Vue.js, Svelte, Ember.js, Backbone.js and Preact.*

Веб-розробка Frontend – це процес перетворення даних у графічний інтерфейс. Інтерфейси спрощують процес розробки та полегшують створення веб-сайту чи програми. Вони надають різноманітні шаблони для взаємодії з компонентами браузера, включаючи підготовлений код, який програмісти можуть використовувати для вирішення типових завдань програмування.

Фреймворки сумісні з різними бібліотеками, які підвищують продуктивність, зменшуючи кількість необхідного коду. Вони поділяють код на багато будівельних блоків або модулів, які є автономними та можуть використовуватися повторно. Це також запобігає неправильним практикам, таким як дублювання коду, і спрощує модульне тестування.

Найважливіші переваги використання фронтенд-фреймворків.

− Швидший час розробки.

Багаторазові компоненти та шаблони скорочують час розробки, дозволяють оновлювати окремі частини сторінок, не змінюючи весь дизайн, і дозволяють швидше запускати програми.

Фреймворки дозволяють розробникам використовувати перевірені та вільні від помилок бібліотеки, не витрачаючи багато часу на пошук та виправлення помилок.

− Зменшена довжина коду.

Frameworks забезпечують компонентний підхід, розділяючи код на модулі, що дозволяє розробникам заощадити багато часу та зусиль, повторно використовуючи колись розроблені компоненти будь-де в проєкті.

− Ремонтопридатність.

Фреймворки розбивають програму на багаторазово використовувані та автономні компоненти, що спрощує внесення швидких змін, які не впливають на решту програми. Використання подібних шаблонів дизайну дозволяє новим розробникам легше створювати та підтримувати додаток.

− Двостороння прив'язка даних.

Деякі зовнішні фреймворки, наприклад Angular, підтримують двостороннє зв'язування даних із коробки, що дозволяє зв'язувати дані та перегляд. Будь-які зміни, пов'язані з даними, що впливають на модель, поширюються на відповідне представлення, а будь-які зміни, внесені в представлення, відображаються в основній моделі без необхідності самостійного повторного оновлення DOM.

Основні інтерфейсні фреймворки: React.js, Angular, Vue.js, Svelte, Ember.js, Backbone.js та Preact. Ринок frontend розробки досить динамічний і мінливий. Незважаючи на те, що React, Angular і Vue.js все ще є лідерами серед інтерфейсних фреймворків, нові фреймворки та бібліотеки активно розробляються та набирають обертів.

Найкращий інтерфейсний фреймворк має забезпечувати гнучкість для подальшого використання, а кінцевий користувач має отримувати відмінний UX та UI. З точки зору розробника, фреймворк повинен бути стабільним, гнучким, багатим на функціональність і мати хорошу підтримку спільноти.

Технології розробки не стоять на місці, вони постійно розвиваються та вдосконалюються. На зміну колись популярним фреймворкам приходять нові, що дає ще більше можливостей розробникам. Прагнення спростити процес розробки, зробити його менш ресурсномістким і прибутковим як для клієнтів, так і для постачальників послуг, залишається незмінним.

Отже, перш ніж почати веб-розробку, потрібно ознайомитися з доступними функціями фреймворка. Розглянути CLI, бібліотеки та плагіни, які підтримує фреймворк, і переконатися, що їх можна застосувати до майбутніх проєктів. Кращим вибором буде фреймворк з достатньою, але не надмірною функціональністю, який підходить для конкретного проєкту.

Інформаційні джерела

1. https://en.wikipedia.org/wiki/Comparison_of_JavaScript-based_web_ frameworks
2. https://geekflare.com/best-javascript-frameworks/

Напрям 8

МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.75

СУЧАСНІ ПІДХОДИ ВИРІШЕННЯ ПРОБЛЕМ ПЕРЕВАНТАЖЕННЯ СЕРВЕРІВ

Віталій Бойко, Назарій Бурак

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Сучасні умови життя та використання засобів інформаційних технологій сприяють росту популярності використання хмарних рішень для організації роботи систем обробки та зберігання даних. Однак, для забезпечення стабільного показника швидкодії опрацювання запитів користувачів такі архітектури систем потребують механізмів якісного управління ресурсами. Забезпечення якісної роботи таких систем можливе за умови використання зрівноважувачів навантаження.*

Ключові слова: *Load Balancer, хмарні рішення, мережа, користувач, ресурси.*

Modern living conditions and the use of information technologies contribute to the growing popularity of the use of cloud solutions for organizing the operation of data processing and storage systems. However, in order to ensure a stable rate of processing of user requests, such system architectures require high-quality resource management mechanisms. Ensuring high-quality operation of such systems is possible under the condition of using load balancers.

Keywords: *Load Balancer, cloud solutions, network, user, resources.*

Останні події в країні та сучасні умови розвитку інформаційних технологій призвели до росту популярності використання хмарних рішень для організації роботи систем обробки та зберігання даних, які потребують механізмів якісного управління ресурсами та забезпечення стабільного показника швидкодії опрацювання запитів користувачів. Актуальність таких систем в Україні стрімко зросла від початку повномасштабних військових дій, особливо в умовах перенесення основних ресурсів систем оповіщення, безпеки і збереження життєдіяльності населення на хмарні середовища. Однак, під час використання таких рішень потрібно пам’ятати про проблеми, які можуть виникнути.

У якості наочного прикладу можна привести ситуацію, яка виникла після початку обстрілів критичної інфраструктури, які призвели проблем із електроенергією. Перебої у живлення відобразились на роботі серверів, на яких розміщений офіційний ресурс компанії-надавача відповідних послуг. Результатом стала ситуація, яка призвела до збільшення кількості одночасних звернень користувачів до ресурсів і, як наслідок, перевантаження серверів та призупинення надання послуг.

Проблема з перевантаженням системи виникає тоді, коли кількість запитів, які може обробити один комп’ютер(система, сервер, процесор тощо) у момент часу перевищує допустимі значення. У такій ситуації відбувається стрімке зменшення продуктивності роботи системи та мережі. Вирішення цієї проблеми можливе двома шляхами – масштабуванням архітектури системи або удосконаленням системи управління.

Перший варіант передбачає збільшення фізичних параметрів системи – пам’яті (диска) або обчислювальної потужності (RAM, CPU) до наявних машини або їх кількості. Однак такий підхід завжди має обмеження, оскільки є границі такого масштабування. Додавання додаткових серверів вирішить проблему трафіку, але ефективне використання ресурсів стає наступною проблемою.

Другий варіант передбачає використання сучасних готових рішення, які забезпечують ефективне управління навантаженням серверів шляхом розподілу усіх запитів рівномірно на усі доступні сервери (рис. 1).

Зрівноважувачі навантаження – це керовані служби, які розподіляють трафік між кількома екземплярами програми. Ці сервіси забезпечують керування обчислювальними ресурсами, що зменшує ризик виникнення стану нефункціональної, повільної або перевантаженої роботи сервера.

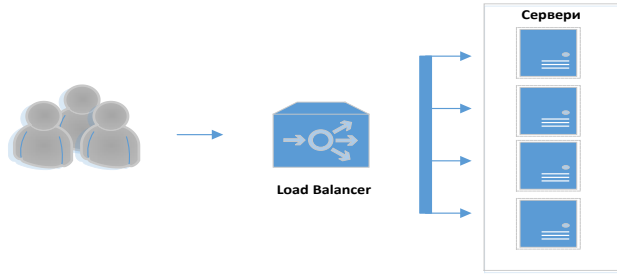


Рисунок 1 – Архітектура системи розподілу навантаження серверів

Основними перевагами використання систем розподілу навантаження є:

1. Запобігання перевантаженню мережевого сервера. Завдяки використанню хмарних зрівноважувачів навантаження можливо розподілити робоче навантаження між кількома серверами, мережевими одиницями, центрами обробки даних і хмарними провайдерами. Це дозволяє ефективно запобігати перевантаженню мережевого сервера під час стрибків трафіку.

2. Доступність системи в надзвичайних ситуаціях. У сучасних умовах, часто виникають ситуації, коли доступ до системи та ресурсів зникає при виході з ладу одного із компонентів самої системи чи будь-якого із допоміжних засобів. Використання зрівноважувачів навантаження забезпечує резервну можливість оперативно та автоматично перенаправляти запити до справних вузлів у випадку та підтримувати загальний доступ та працездатність системи.

3. Висока якість використання ресурсів. Однією із функцій зрівноважувачів навантаження є ефективне управління усіма ресурсами, які забезпечують роботу системи: центри обробки даних, зовнішні диски, сервери, кластери, комп'ютери тощо. Правильний та оперативний розподіл навантаження на основі даних про використання ресурсів максимізує пропускну здатність, оптимізує використання доступних ресурсів, уникає перевантаження будь-якого окремого з них та мінімізує час відповіді сервера і, як результат, – ефективність роботи системи зростає.

4. Попередження загального збою в роботі системи. Сучасні технології розподілу навантаження можуть виявляти несправні вузли у кластері за допомогою різних алгоритмів і методів перевірки працездатності. У разі збою навантаження активується режим перенаправлення на інший вузол, яке є не вплине на доступ до ресурсів чи роботу користувачів. Такий підхід дає змогу швидко вирішення проблеми на етапі її виникнення.

Одним із таких є продукт компанії Google – це Load Balancer, який доступний на платформі Google Cloud Platform. Load Balancer має різні типи роботи, які забезпечують різні рівні розподілу навантаження:

− Глобальне врівноваження навантаження (Global Load Balancing);
− Регіональне врівноваження навантаження(Regional Load Balancing);
− Внутрішнє врівноваження навантаження (Internal Load Balancing);
− Зовнішнє врівноваження навантаження (External Load Balancing);
− Врівноваження навантаження TCP/SSL (TCP/SSL Load Balancing);
− Врівноваження навантаження TCP-проксі (TCP Proxy Load Balancing).

Таким чином, ефективним вирішення проблем забезпечення високої швидкодіє роботи систем, які використовують хмарні рішення є використання сучасних засобів розподілу навантаження серверів, зокрема Load Balancer. Такий підхід дозволить оперативно управляти та підтримувати повноцінну стабільну роботу систем за будь-яких надзвичайних ситуацій.

Інформаційні джерела

1. S. Rajagopalan "An Overview of Server Load Balancing" Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, Volume-7 | Issue-2, April 2020, [Електронний ресурс]. – Доступний з http://www.ijtrd.com/papers/IJTRD22061.pdf

2. Load Balancer: what is it and what is its importance? [Електронний ресурс]. – Доступний з https://senhasegura.com/load-balancer/

УДК 004.71

АНАЛІЗ ФУНКЦІОНАЛЬНИХ ОСОБЛИВОСТЕЙ КОМУТАТОРІВ LAYER 2 ТА LAYER 3

Олексій Герговський, Назарій Бурак

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Сучасні комп'ютерні мережі забезпечують реалізацію моделі OSI, яка визначає сім "рівнів" мережі, кожен з яких реалізується різними пристроями. Проведено дослідження підходів до організації побудови мереж за допомогою комутаторів другого та третього рівнів. Виконано аналіз переваг та недоліків їх використання.*

Ключові слова: *комп'ютерна мережі, протоколи, рівні, маршрутизація, VLAN.*

Abstract. *Modern computer networks implement the OSI model, which defines seven "levels" of the network, each of which is provided by different devices. A study of approaches to the organization of building networks using Layer 2 and Layer 3 switches was conducted. An analysis of the advantages and disadvantages of their use was performed.*

Keywords: *computer networks, protocols, levels, routing, VLAN.*

Модель OSI визначає сім "рівнів" мережі, кожен з яких відповідає за певний тип обміну інформацією та використовує відповідні протоколи. Кожен рівень обслуговує свою частину процесу взаємодії. Завдяки такій структурі спільна робота мережевого обладнання й програмного забезпечення стає набагато простішою, прозорішою та зрозумілішою.

Організація процесу обміну даним відбувається на другому(канальному) та третьому(мережевому) рівнях моделі OSI. На канальному рівні для обмін інформацією використовується протокол Ethernet, який ідентифікує пристрої за допомогою їх MAC-адреси (Media Access Control), яка присвоюється пристрою заводом-виробником та є унікальною і незмінною. Для об'єднання хості у єдину мережу застосовуються комутатори – фундаментальні складові будь-якої мережі, які забезпечують якісний обмін та контроль трафіку, що є необхідною умовою для правильного функціонування мережі.

На наступному рівні (рівень 3, мережевий рівень) для організації міжмережної взаємодії застосовується протокол IP(Internet Protocol). Пристрої в IP-мережі ідентифікуються за їх відповідною IP-адресою, яку можна задати двома шляхами – статично та динамічно. Мережевим пристроєм, який найчастіше застосовується для побудови мереж третього рівня є маршрутизатор, який дозволяє підключати пристрої до різних IP-мереж.

Розвиток інформаційних технологій у сфері комп'ютерних мереж сьогодні дозволяє будувати мережі із використанням також і комутаторів, які можуть ефективно управляти трафіком як на другому, так і на третьому рівнях. Вони дозволяють з'єднувати декілька пристроїв у локальній мережі та

зменшувати область колізій за допомогою комутації пакетів. Перевіряючи вміст заголовків пакетів, комутатор створює таблицю MAC-адрес і відповідних їм фізичних портів на комутаторі, щоб ефективно приймати рішення щодо направлення майбутніх пакетів. Коли пакет даних надходить на пристрій, він перевіряє його заголовок, щоб визначити адресата, перевіряє таблицю MAC-адрес із відповідними фізичними портами та приймає рішення, на який фізичний порт відправляти дані.

Сучасні комутатори можуть реалізовувати і більш складніші топології мереж, використовуючи віртуальні локальні мережі – VLAN. Даний тип мереж дозволяє розділяти інтерфейси одного фізичного пристрою на різні підмережі, поділяючи одну мережу фізично підключених пристроїв на кілька логічних мереж, які не можуть безпосередньо взаємодіяти одна з одною, реалізовуючи принцип сегментації мережі.

Щоб два пристрої могли взаємодіяти в типовій корпоративній або домашній мережі, вони повинні мати як IP-адресу, пов'язану з рівнем 3 (рівень IP), так і MAC-адресу, пов'язану з рівнем 2 (рівень Ethernet). У застарілих мережах, створених до появи інтелектуальних комутаторів, здатних підтримувати VLAN, єдиним способом для взаємодії двох пристроїв в окремих мережах Ethernet рівня 2 було використання маршрутизація між цими двома мережами, яка здійснювалася за допомогою маршрутизатора (рис. 1). З розвитком мережевих технологій і появою VLAN, керовані комутатори отримали можливість з'єднувати два пристрої в окремих мережах Ethernet. Однак, такий підхід усе ще потребував зв'язку через маршрутизатором.

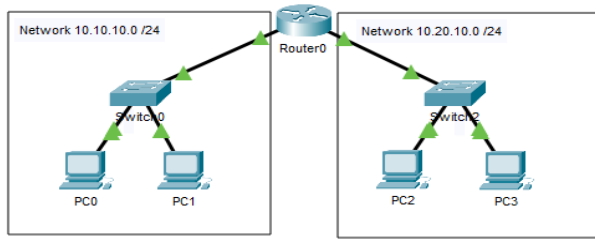


Рисунок 1 – Побудова мережі за допомогою комутатора Layer

Із появою комутаторів, які працюють як на рівні 2, так і на рівні 3, відбулися зміни в принципах побудови мереж, адже ці пристрої дозволяли хостам, підключеним до різних мереж VLAN, спілкуватися один з одним без використання спеціального маршрутизатора (рис. 2). У таких мережах маршрутизація виконується комутатором, а не виділеним маршрутизатором. У мережі, яка побудована на основі комутаторів 3 рівня, під час перевірки заголовка пакета, відбувається визначення мережі його отримання і якщо цей пакет призначено для іншої VLAN, комутатор рівня 3 "підносить" пакет до рівня маршрутизації. Після цього, на рівні маршрутизації (рівень 3) приймається рішення про те, куди надсилати пакет – комутатор звертається до таблиці пересилання MAC-адрес, щоб вирішити, на який порт надсилати вихідний пакет.

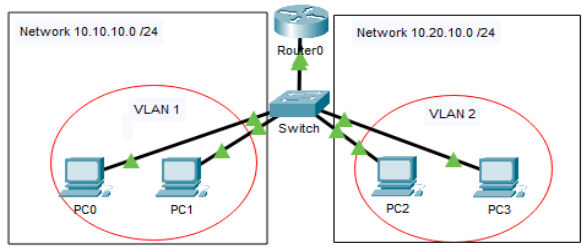


Рисунок 2 – Побудова мережі за допомогою комутатора Layer 3

Аналізуючи технології побудови мережі та принципи функціонування комутаторів Layer 3 можна виділити наступні переваги та недоліки їх використання.

Переваги: підтримує маршрутизацію між VLAN; забезпечує легкість управління безпекою; дозволяє зменшити обсяг трансляційного трафіку; полегшить процес налаштування для VLAN, оскільки окремий маршрутизатор не потрібен між кожною VLAN; використовує окремі таблиці маршрутизації та, як наслідок, кращий розподіл трафіку; контролює потоки та забезпечує високу швидкість масштабування; менша затримка мережі, оскільки пакет не робить додаткових стрибків, щоб пройти через маршрутизатор.

Недоліки: вартість значно вища в порівнянні з комутатором рівня 2; не підтримує функції WAN; при відносно невеликих розмірах мережі, може збільшити складність, не забезпечуючи додаткових переваг; не пропонує жодних функцій для складних топологій.

Таким чином, на основі дослідження особливостей сучасних комутаторів, можна зробити висновок, що комутатор рівня 3 виконує функції маршрутизації на додаток до комутації та визначає шляхи на основі логічної адресації. Комутатори 2 рівня виконують функцію комутації для перевпорядкування кадрів даних від джерела до мережі призначення та допомагають пересилати пакети на основі унікальних MAC-адрес, однак не дозволяють реалізувати будь-який інтелект під час пересилання пакетів. Загалом, комутатори рівня 2 використовуються для зменшення трафіку в локальній мережі, тоді як комутатори рівня 3 переважно використовуються для реалізації VLAN. Рішення про використання одних чи інших – залишається за особою, яка проєктує мережу. При цьому слід враховувати усі особливості майбутньої мережі та зважити переваги і недоліки кожного з видів комутаторів.

Інформаційні джерела

1. Xiaowei, Ji & Zhimin, Li & Wenlong,. (2019). Application of Routing Communication Between VLANs in A Layer 3 Switch. IOP Conference Series: Materials Science and Engineering. 569. 032030. 10.1088/1757-899X/569/3/032030.

2. Layer 2 Switch vs Layer 3 Switch? [Електронний ресурс]. – Доступний з https://www.guru99.com/layer-3-layer-2-switch.html

3. Routing Between VLANs & Layer 3 Switches. [Електронний ресурс]. – Доступний з https://www.practicalnetworking.net/stand-alone/routing-between-vlans/

УДК 004.056

КІБЕРФІЗИЧНА СИСТЕМА “РОЗУМНИЙ ДІМ”: СТРУКТУРА – ЗАГРОЗИ – БЕЗПЕКА

Валентин Дудикевич, Галина Микитин, Максим Галунець, Роман Кутень

Кафедра безпеки інформаційних технологій Національного університету “Львівська політехніка”, м. Львів, Україна

Анотація. *В роботі розглянуто структуру багаторівневої кіберфізичної системи (КФС) “Розумний дім” в просторі “інтелектуалізація – кібербезпека”. Проаналізовано функціональність: фізичного простіру (ФП), комунікаційного середовища (КС) кібернетичного простіру (КП) кіберфізичної системи. Розгорнута зовнішня та внутрішня безпека багаторівневої структури КФС на рівні цілеспрямованих і випадкових загроз.*

Abstract. *The paper examines the structure of the multi-level cyber-physical system (CFS) “Smart Home” in the space of “intellectualization - cyber security”. The functionality of: physical space (FP), communication environment (CS), cyber space (CP) of the cyber-physical system was analyzed. I will expand the external and internal security of the multi-level structure of the KFS at the level of targeted and random threats.*

Вступ. В Україні розгортаються процеси безпечної інтелектуалізації інфраструктури суспільства в просторі Концепції Індустрії 4.0 та Стратегії кібербезпеки [1]. Ефективними технологіями підтримки безпечного функціонування інтелектуальних обєктів є багаторівневі кіберфізичні системи. Актуальним питанням залишається комплексна система безпеки КФС за впливу випадкових і цілеспрямованих загроз.

Кіберфізична система “Розумний дім”: багаторівнева структура – загрози – безпека. Багаторівнева кіберфізична система “Розумний дім” функціонує у взаємозвязку “фізичний простір – комунікаційне середовище – кібернетичний простір” (рис. 1).

Рисунок 1 – Структура багаторівневої кіберфізичної системи “Розумний дім”

Фізичний простір КФС "Розумний дім" представляють давачі, що забезпечують:

– параметри обладнання (водопостачання, електроживлення т. і);

– комфорт (освітленість, якість повітря і води, вологість, температуру т. і);

– безпеку (системи відео нагляду, біометричні системи т. і).

Комунікаційне середовище КФС – системи безпровідного звязку – LTE, Wi-Fi. Кібернетичний простір КФС – інформаційні ресурси (централізована структурована обєктно-реляційна база даних); інформаційна система (комп'ютеризована система обробки, аналізу та прийняття рішення на управління станом об'єкта); інформаційні процеси (фази, операції, обробка).

Випадкові та цілеспрямовані загрози безпеці КФС на зовнішньому і внутрішньому рівнях представлені в табл. 1.

Таблиця 1

Цілеспрямовані і випадкові загрози безпеці КФС "Розумний дім"

Зовнішні цілеспрямовані загрози	*Захист*
Виведення з ладу пристроїв відеоспостереження	*КП*: розмежування доступу до серверу налаштування та зберігання даних в хмарному середовищі *КС:* покращення захисту Wi-Fi-мережі *ФП*: маскування місць встановлення камер; подвійне охоплення спектру відеоспостереження
Порушення функціонування каналів енергоживлення та інтернет-зв'язку	*КП:* автоматизоване виявлення несправностей каналів електроживлення інтернет-зв'язку *КС*: створення резервних каналів забезпечення енергоживлення та інтернет-зв'язку (сонячні батареї, генератор, 4G/5G модем, Starlink); резервне кабельне забезпечення зв'язку між компонентами КФС *ФП:* спорудження зовнішньої захисної конструкції
Підміна санкціонованого користувача	*КП*: ідентифікація та авторизація користувачів, обладнання та даних КС: шифрування даних в мережі.
"Сніфінг" даних у каналі зв'язку	*КС:* покращення захисту WiFi-мережі (стійкі паролі, використання найновіших стандартів безпеки); шифрування даних у мережі
Зовнішні випадкові загрози	*Захист*
Заглушення корисного сигналу сто-	*КС:* завадостійке кодування; використання ретрансляторів/Mesh-систем; створення резервних каналів

ронніми передавачами (ПЕМВ)	зв'язку; використання багаточастотних Wi-Fi-роутерів; екранування приміщень
Порушення функціонування систем хмарного провайдера	*КП:* використання практик "high availability" для налаштування віддаленого сервера; створення резервних копій даних та конфігурацій систем; шифрування даних "at rest"; КС: шифрування даних "in transit"
Внутрішні цілеспрямовані загрози	*Захист*
Нехтування безпекою пристроїв під час встановлення та/або транспортування підрядником з монтажу	*ФП*: Вибір елементів системи з нерозбірним корпусом та хорошим ступенем захисту від зовнішнього впливу *КС:* Перевірка компонентів перед встановленням *КП:* Перевірка показників з номінальними таблицями від виробника та іншим пристроєм
Втрата даних через вихід з ладу жорсткого диску	*ФП*: Моніторинг роботоздатності компонентів зберігання інформації *КС:* З'єднання з додатковим сховищем даних по технології RAID1 (дзеркалювання даних) *КП:* Дублювання даних та конфігурацій налаштувань систем на незалежні носії
Потрапляння шкідливого програмного забезпечення через оновлення елементів системи	*КС*: Дублювання інформації у системі з правами "виключно читання" *КП:* Оновлення програмного забезпечення на сталі та перевірені версії
Внутрішні випадкові загрози	*Захист*
Передача некоректних даних через "зашумлення" каналів зв'язку	*ФП:* Вибір компонентів "розумного дому" з можливістю безпровідного та провідного звязку *КС*: Використання алгоритмів з надлишковістю *КП*: Моніторинг отриманих даних з можливістю підтвердження (повторного отримання) даних
Помилки синхронізації пристроїв через різні типи елементів з'єднання з мережею	*ФП:* Вибір елементів з під'єднанням до інтранет-мереж *КС*: Розроблення архітектури системи перед закупівлею елементів та їх встановленням *КП:* Вибір елементів з можливістю програмного вибору кодування та шифрування інформації

Інформаційні джерела

1. Стратегія кібербезпеки України – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text

УДК 614.8-084:615.91

ПЕРЕВАГИ ТА НЕДОЛІКИ НОВОЇ СИСТЕМИ ОПОВІЩЕННЯ ПРО НАДЗВИЧАЙНІ СИТУАЦІЇ

Ян Карлінський, Андрій Гаврись

Кафедра цивільного захиту Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація: *На сьогоднішній день ефективне оповіщення населення щодо небезпечних подій стало надзвичайно актуальним та необхідним завданням. Тому, Державна служба України з надзвичайних ситуацій впроваджує та тестує нову систему оповіщення, що працює на технології Cell Broadcast. Автори проаналізували позитивні та негативні сторони її впровадження.*

Ключові слова: *цивільний захист, системи оповіщення, технологія Cell Broadcast.*

Abstract. *Today, effective notification of the population about dangerous events has become an extremely relevant and necessary task. Therefore, the State Emergency Service of Ukraine is implementing and testing a new notification system based on Cell Broadcast technology. The authors analyzed the positive and negative aspects of its implementation.*

Keywords: *civil protection, alarm systems, Cell Broadcast technology.*

На сьогоднішній день в Україні одним із головних заходів захисту населення від надзвичайних ситуацій (НС) є його своєчасне оповіщення про небезпеку, обстановку, яка склалася внаслідок її реалізації, а також інформування про порядок і правила поведінки в умовах НС, що на мою думку є правильним, адже населення має знати про загрозу а не так як було при вибуху Чорнобильської АЕС(людей евакуйовували не сказавши про аварію яка сталась). Також, з цивільним населення має проводитись навчання, щоб у разі виникнення надзвичайної ситуації вони знали свої дії [1].

Локальна система оповіщення – це програмно-технічний комплекс, що створюється і функціонує на об'єкті підвищеної небезпеки та призначений для оповіщення у разі загрози виникнення та під час виникнення надзвичайних ситуацій, в результаті яких у зону можливого негативного впливу потрапляє населення, територія інших підприємств, установ і організацій [2].

Під кінець вересня в Україні завершилось тестування нової системи оперативного інформування населення про надзвичайні ситуації за допомогою операторів мобільного зв'язку Київстар, Vodafone та lifecell. Вона працює в 17 областях та місті Києві [3], як зазначили в Державній службі України з надзвичайних ситуацій. Нова система оперативного інформування працює завдяки технології Cell Broadcast. Вона має значні переваги над SMS-інформуванням. Сповіщення стосуватимуться абсолютно різних загроз: від метеорологічних явищ (буревії, лісові пожежі) до хімічних загроз, якщо поруч є хімічні підприємства, на яких сталися викиди. Це можуть бути загрози радіаційних викидів, зокрема для населення, яке проживає в 30-кілометровій зоні спостереження навколо атомних станцій. Це може бути термінова евакуація на деяких територіях.

До складу цих систем входять пристрої для звуко- і відеовідтворення інформації та інші технічні засоби, у тому числі абонентські радіоточки, вуличні гучномовні пристрої (сигнально-гучномовні пристрої), пристрої для запуску електросирен і електросирени, системи автоматизованого виклику [2]. Проте, якщо для працівників об'єкту гучномовні пристрої та електросирени будуть ефективним способом оповіщення, то для населення, яке проживає поблизу об'єкта сигнали оповіщення від цих пристроїв можуть бути нечутні [1].

Нова система оперативного інформування працюватиме завдяки технології Cell Broadcast. Cell Broadcast- функція мережі GSM, що дозволяє мобільному оператору передавати різноманітну інформацію, що може бути відображена на дисплеї мобільного телефону. На відміну від служби коротких повідомлень від точки до точки (SMS-PP), Cell Broadcast – це служба обміну повідомленнями з геотаргетингом і геозоною "один до багатьох". Тобто повідомлення надходять набагато швидше, повідомлення надходять абонентам мобільних операторів, які перебувають у радіусі дії обраних базових станцій мобільного зв'язку. Людям надсилатимуть повідомлення з назвою загрози та інструкцією дій. Отож ДСНС може відправляти інформацію жителям конкретного населеного пункту, області або по всій Україні, в залежності від ситуації. Звуковий сигнал про надходження повідомлення буде навіть у тому випадку, якщо звук на телефоні вимкнений, щоб на сповіщення обов'язково звернули увагу та реагували відповідно до інструкцій та порад щодо дій у різних загрозах.

Проте в даній системі є ряд недоліків. Приймати повідомлення від системи Cell Broadcast можуть переважно мобільні телефони (смартфони), які вироблено починаючи з 2019 року, та які мають операційну систему Android версії 11 та вище або iOS від версії 14.5. Також вона інколи дає збій та може надіслати сповіщення про загрозу в іншу область чи район в якій нічого не відбувається.

Водночас, старі моделі телефонів (до 2019 року випуску) з великою ймовірністю не зможуть приймати оповіщення Cell Broadcast. У майбутньому планують розширювати перелік моделей смартфонів, які зможуть отримувати такі повідомлення.

Також не потрібно забувати про оповіщення сільського району,там воно розвинене гірше. Частина із них взагалі не має зв'язку. Не всі люди мають мобільний телефон або смартфони тому вони змушені отримувати сповіщення через радіо або телебачення. Все це обмежує можливості щодо використання існуючої апаратури управління і засобів оповіщення, що потребує залучення значних фінансових і матеріальних ресурсів.

Також не потрібно забувати про людей з вадами слуху. Опитавши їх з'ясувалось що на час воєнного стану в країні вони тримають всі потрібні речі біля себе включаючи телефон тому якраз оповіщення від системи Cell Broadcast добре їх інформує про небезпеку та вказує інструкцію щодо дій при певній надзвичайній ситуації.

Отже, можна зазначити шо нова система оповіщень про надзвичайні ситуації має значні переваги над SMS-повідомлення : швидше отримання сповіщень, звуковий сигнал навіть при вимкненому смартфоні. Але є ще над чим попрацювати наприклад: не всі люди мають смартфони, не у всіх населених пунктах такі як села є зв'язок, тому потрібно ще працювати над цими нюансами.

Інформаційні джерела

1. Гаврись А. П. (2018). Проблеми влаштування систем оповіщення населення в сільській місцевості.

2. Гаврись А. (2019). СМС-повідомлення, як спосіб оповіщення населення про надзвичайні ситуації в сільській місцевості.

3. Офіційний сайт Державної служби України з надзвичайних ситуацій. Режим доступу – https://dsns.gov.ua/

УДК 004.7

СТВОРЕННЯ СИСТЕМИ АНАЛІЗУ МЕРЕЖЕВИХ АТАК НА БАЗІ МАШИННОГО НАВЧАННЯ

Аліна Павлишин, Орест Полотай

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Описано застосування машинного навчання в системах аналізу мережевих атак, Визначення та класифікація мережевих атак, Методи виявлення мережевих атак, Методи машинного навчання, Моделі, що застосовуються під час машинного навчання, Сфери застосування машинного навчання та Вибір програмного забезпечення для створення системи аналізу атак на основі машинного навчання.*

Ключові слова: *розроблення програмного забезпечення на базі машинного навчання, безпека програмного забезпечення, системи аналізу атак.*

Abstract. *It describes the application of machine learning to network attack analysis systems, Definition and classification of network attacks, Methods for detecting network attacks, Machine learning methods, Models used during machine learning, Applications of machine learning and Selection of software for creating a machine learning based attack analysis system.*

Keywords: *Machine learning software development, software security, attack analysis systems.*

В даний час засоби та системи комунікації розвиваються стрімкими темпами, різко збільшилися обсяг та швидкість передачі даних. Інформація безпосередньо впливає на життя людей, функціонування та регулювання організацій та держав у цілому, саме тому інформацію прийнято вважати одним із ключових ресурсів. Важливість інформації у суспільстві зростає з кожним днем.

У зв'язку з цим гостро постає проблема забезпечення безпеки інформація, яка безпосередньо залежить від зростання обсягу та значущості інформації. Випадки порушення інформаційної безпеки, різні мережеві атаки вже не є чимось дивовижним та несподіваним. Люди стикаються з ними щодня.

Мережевою атакою називають навмисні дії третіх осіб (зловмисників), спрямовані на отримання контролю над локальним або віддаленим комп'ютером для подальшого порушення роботи мережі, зміни прав користувачів, отримання персональних даних або реалізації будь-яких деструктивних дій над інформацію. Для реалізації мережевої атаки можуть застосовуватися як програмні, і технічні засоби.

Мережеві атаки мають таку класифікацію:

1. За характером впливу.
2. За метою впливу.
3. За наявності зворотного зв'язку з об'єктом, що атакується.
4. За умовою початку здійснення дії.
5. За розташуванням суб'єкта атаки щодо об'єкта, що атакується.
6. За рівнем моделі OSI, на якому здійснюється дія.

Мережеві атаки можуть бути проведені на будь-якому рівні моделі OSI, починаючи з мережевого рівня. До високорівневих атак відносяться ті які реалізуються на сеансовому та прикладному рівні, а до низькорівневих – на мережевому та транспортних рівнях.

Прикладами мережевих атак можуть бути:

1. Mailbombing.
2. Застосування спеціалізованих додатків.
3. Переповнення буфера.
4. Мережна розвідка (збір відомостей за допомогою додатків, що знаходяться у вільному доступі).
5. IP-спуфінг (зловмисник видає себе за авторизованого користувача).
6. Man-in-the-Middle (впровадження з метою отримання пакетів, що передаються всередині системи).
7. Фішинг (шахрайство шляхом надсилання повідомлень з елементами соціальної інженерії).
8. DDOS-атака (перевантаження системи чи її елементів із єдиною метою повного чи часткового виведення її з ладу).
9. XSS-атака (ПК клієнта зазнають атаки через уразливості на сервері).
10. Brute Force (отримання несанкціонованого доступу до індивідуальних облікових записів, систем та мереж шляхом підбору.
11. Sql Injection (використання шкідливого коду SQL для управління базою даних та доступу до конфіденційної інформації).

Тож для захисту інформаційних систем від проведення на них вищезгаданих атак розробляються системи виявлення мережевих атак.

Виявленням мережевих атак називається процес розпізнавання аномальної чи підозрілої діяльності. Алгоритм виявлення аномалій мережі може бути описаний наступним чином. Даними для аналізу є мережевий трафік у вигляді мережевих пакетів. Ці дані збираються без обробки, після чого можуть бути нормалізовані для завдання ознакових атрибутів загального виду. Такі дані використовуються для створення активного профілю. Далі профіль порівнюється з нормальною діяльністю об'єкта, і при виявленні розбіжностей параметрів профілю фіксується аномалія. Даний алгоритм має кілька варіантів подальшої реалізації: процедура порівняння з граничною величиною (при перевищенні граничної величини фіксується аномалія), ідентифікація несанкціонованих дій шляхом порівняння мере-

жевого трафіку з шаблоном атак, методи інтелектуального аналізу даних (методи обчислювального інтелекту, машинного навчання).

Метод інтелектуального аналізу успішно застосовується при розробці сучасних систем виявлення атак і є перспективним напрямом розвитку даної галузі.

Одним із класів методу інтелектуального аналізу є машинне навчання.

Машинне навчання (англ. machine learning, ML) – галузь штучного інтелекту, характерною рисою яких є не пряме рішення задачі, а навчання, засноване на використанні даних та алгоритмів для імітації навчання людини. Вирішуючи схожі завдання, поступово підвищується точність рішень. Для побудови таких методів використовуються засоби математичної статистики, чисельних методів, математичного аналізу, методів оптимізації, теорії ймовірностей, теорії графів, різних технік роботи з даними в цифровій формі.

Способи навчання поділяють на:

1. Навчання із вчителем (supervised learning).
2. Навчання без вчителя (unsupervised learning).
3. Навчання з підкріпленням (reinforcement learning).

Усі перелічені алгоритми навчання підходять на вирішення завдання виявлення аномалій. Для реалізації методу навчання з вчителем потрібен набір даних, записи в якому спочатку розділені на класи “нормальні” та “аномальні”. При розробці системи виявлення мережевих атак ці класи позначені як “немає атаки” і “є атака” відповідно.

Виконання машинного навчання включає створення певної моделі, яка навчається на вхідних навчальних даних, а потім може обробляти інші дані, для прогнозування. Для систем машинного навчання використовуються різні типи моделей, наприклад:

1. Дерево прийняття рішень.
2. Випадковий ліс.
3. Лінійна регресія.
4. Наївний Байєс.

Машинне навчання зачіпає практично всі сфери діяльності людства: від харчової промисловості та сільського господарства до економіки та науки.

Прикладами конкретних систем, розроблених з урахуванням машинного навчання, можуть служити:

1. Image to Recipe – перетворює зображення страви на рецепт приготування.

2. Diseases – ідентифікація шкідників та хвороб сільськогосподарських культур та за зображеннями.

3. Auctions – оптимальні аукціони з використанням глибокого навчання.

4. Variant calling – визначення відхилень від еталонного геному в ДНК людини.

5. Manufacturing Anomalies – інтелектуальне виявлення аномалій для виробничої лінії на підприємстві.

6. SMAC – система захисту від шахрайства в Move-To-Earn грі STEPN.

У навчанні нейронної мережі, що розробляється, для системи виявлення мережевих атак в більшості випадків буде використаний метод "з вчителем". Вхідним буде набір даних CSE-CIC-IDS2018 – Спільний проєкт Установи безпеки зв'язку (CSE) та Канадського інституту кібербезпеки (CIC).

Набір даних містить інформацію, отриману за допомогою програмного забезпечення – аналізатора мережевого трафіку CICFlowMeter V3. Набір даних представлений як файл з розширенням .csv.

Модулі системи виявлення мережевих атак розроблялися мовою програмування Python.

Python – це інтерпретована об'єктно-орієнтована мова програмування високого рівня, з гарною читальністю коду, динамічною строгою типізацією та автоматичним керуванням пам'яттю.

Таким чином маючи цікавість та деякі знання у сфері програмування можна розробити, навчити та запустити роботу своєї унікальної системи виявлення атак яка буде допомагати вам та вашій компанії захищатись від сторонніх атак та несподіваній втраті ваших дорогоцінних даних.

Інформаційні джерела

1. IDS 2018 Canadian Institute for Cybersecurity. https://www.unb.ca/cic/datasets/ids-2018.html

2. Anomaly Detection in Networks Using Machine Learning. https://www.researchgate.net/publication/328512658_Anomaly_Detection_in_Networks_Using_Machine_Learning

3. Transfer learning – Wikipedia. https://en.wikipedia.org/wiki/Transfer_learning

4. Network Attacks and Their Detection Mechanisms: A Review http://lib.itsec.ru/articles2/Oborandteh/ tselenapravlennye-ataki-pryamaya-i yavnayaugroza

5. Polotai O., Kukharska N., Lagun A. The steganographic approach to data protection using arnold algorithm and the pixel-value differencing method. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020. 2020. Article ID 9204108. P. 174–177.

6. Полотай О.І., Деменко В. Особливості оцінки ризиків загроз інформаційної безпеки. Зб. наук. праць XI Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів "Проблеми та перспективи забезпечення безпеки життєдіяльності" (м. Львів, 24 березня 2016 р.). Львів : ЛДУБЖД, 2016. С. 204–205.

УДК 004.42:[656.2: 004.732]

ОРГАНІЗАЦІЯ МАРШРУТИЗАЦІЇ В MPLS ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ З ВИКОРИСТАННЯМ НЕЙРОМЕРЕЖНИХ ТЕХНОЛОГІЙ

Вікторія Пахомова

Кафедра електронних обчислювальних машин,
Український державний університет науки і технологій,
м. Дніпро, Україна

Анотація. *Запропонована методика визначення оптимального маршруту в MPLS інформаційно-телекомунікаційної системи залізничного транспорту з використанням нейромережних технологій, яка складається з наступних етапів: визначення поточної завантаженості тунелів домену MPLS; кластеризації потоків трафіку за умови параметру QoS на основі SOM та визначення тунелів домену MPLS на основі MLP; розподіл потоків трафіку за тунелями домену MPLS.*

Ключові слова: *залізничний транспорт, MPLS, імітаційна модель, маршрутизація, параметр QoS, трафік, SOM, домен, MLP.*

Abstract. *The proposed method of determining the optimal route in the MPLS information and telecommunication system of railway transport using neural network technology, which consists of the following stages: determination of the current load of MPLS domain tunnels; clustering of traffic flows under the condition of QoS parameter based on SOM and definition of MPLS domain tunnels based on MLP; distribution of traffic flows by MPLS domain tunnels.*

Keywords: *railway transport, MPLS, simulation model, routing, QoS parameter, traffic, SOM, domain, MLP.*

Постановка проблеми. На сучасному етапі організація маршрутизації у комп'ютерних мережах, що складають основу інформаційно-телекомунікаційної системи залізничного транспорту (ІТС), вирішується за допомогою протоколу OSPF. Але такий протокол маршрутизації не в стані працювати в умовах зміни конфігурації мережі та інтенсивності потоків трафіку, а також при урахуванні декількох метрик при визначенні оптимального шляху. Це потребує проведення досліджень інших підходів щодо маршрутизації в комп'ютерних мережах ІТС залізничного транспорту.

Аналіз останніх досліджень. Рішення поставленої проблеми можливо при використанні нових транспортних технологій в ІТС залізничного транспорту, зокрема технології багатопротокольної комутації за допомогою меток (Multiprotocol Label Switching, MPLS) з одного боку та використання нейромережних технологій з іншого боку

[1]. У загалі дослідженням характеристик MPLS [2–6] на основі аналітичних та імітаційних моделей займалися такі науковці: Будилдіна Н. В., Гольдштейн А. Б., Зайченко О. Ю, Зайцев Д. А., Олифер В. Г., Романов О. І., Руккас К. М., Шарадка А. М. та ін. Проведені дослідження показали, що застосування технології MPLS дозволяє забезпечити збільшення трафіку в середньому в 1,7 разів.

Відомо, що розв'язок задачі маршрутизації в комп'ютерних мережах можливо знайти на основі наступних нейронних мереж (НМ): мережі Хопфілда; багатошарового персептрону; мережі RBF; нейронечіткої мережі, а також з використанням мультиагентних методів інтелектуальної оптимізації. Однак, слід зауважити, що на сучасному етапі існує дуже обмежена кількість наукових джерел з відповідними дослідженнями щодо організації маршрутизації в мережі MPLS, зокрема ІТС залізничного транспорту з використанням нейромережних технологій. Також відомо, що донедавна робота залізничного транспорту України являла собою взаємодію шести залізниць: Донецької; Львівської; Одеської; Придніпровської; Східної; Харківської, на кожній з яких впроваджена відповідна ІТС [1], що потребує проведення додаткових досліджень відповідного домену MPLS.

Метою роботи є розробка методики визначення оптимального маршруту в MPLS ІТС залізничного транспорту з використанням нейромережних технологій.

Основна частина

Запропонована загальна структура системи маршрутизації в MPLS ІТС залізничного транспорту, основу якої складає використання наступних НМ: SOM (Self Organizing Maps) для кластеризації потоків трафіку та MLP (Multi Layer Perceptron) для визначення тунелів домену MPLS. Класи обслуговування потоків трафіку CoS (Class of Service) призначені відповідно до обраного параметру QoS (Quality of Service).

У [7] виконано дослідження залежності якості вирішення задачі інжинірингу трафіка від послідовності призначення потоків мережі MPLS. На підготовчому етапі передбачалося використання імітаційних моделей мережі MPLS різних фрагментів ІТС залізничного транспорту, що створювалися в системі Opnet Modeler [8]. Отримані результати на імітаційних моделях, що працюють за різними сценаріями (IP, MPLS і MPLS TE), свідчать про ефективність використання MPLS TE.

Крім того, створений MLP для визначення тунелів домену MPLS. Вибірки для MLP формулювалися на основі даних, що отримані на імітаційній моделі мережі MPLS в системі Opnet Modeler. Так, наприклад, на створеній в Python за допомогою фреймворку Keras програмній моделі "CoSThDist" проведено дослідження оптимальних параметрів НМ для розглянутого фрагменту ІТС залізничного транспорту [9].

Висновки. Запропонована методика, що складається з наступних етапів: визначення поточної завантаженості тунелів домену MPLS; кластеризація потоків трафіку з урахуванням параметру QoS на основі SOM та визначення тунелів домену MPLS на основі MLP; розподіл потоків трафіку за тунелями домену MPLS на основі створеного програмного комплексу та організації досліджень.

У подальшому планується створити SOM для кластеризації потоків трафіку за умови урахування параметрів QoS: Maximum Packet Transfer Delay (maxPTD) від 50 до 100 мс; Packet Delay Variation (PDV) від 1,5 до 5 мс, та провести відповідний аналіз.

Інформаційні джерела

1. Пахомова В. М. Дослідження інформаційно-телекомунікаційної системи залізничного транспорту з використанням штучного інтелекту: монографія. Дніпро: Вид-во ПФ “Стандарт-Сервіс”, 2018. 220 с.

2. Гольдштейн А. Б. Модель управления туннелирования в сети MPLS. Информатизация и связь. 2015. № 1. С. 10–14.

3. Романов О. І., Пасько С. П. Оцінка часу затримки в мережах IP і MPLS при обслуговуванні повідомлень у складних багатотранзитних напрямках зв’язку. Наукові вісті Національного технічного університету України “КПІ”. 2011. № 5. С. 11–20.

4. Akinsipe O., Goodarzi F., M. Li. Comparison of IP, MPLS and MPLS RSVP-TE Networks using OPNET. International Journal of Computer Applications. 2012. URL: https://pdfs.semanticscholar.org/bef6fe5e.pdf

5. Herguner K., Kalan R. S., Cetinkaya C., Sayit M. Towards QoS-aware routing for DASH utilizing MPTCP over SDN. IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) (6–8 Nov. 2017). Berlin, Germany, 2017. pp. 1–6. DOI: 10.1109/nfv-sdn.2017.8169844.

6. Ємець Н. І., Голь В. Д., Бердников О. М. Аналіз можливостей мережі IP/MPLS для застосування механізмів QoS. Системи управління, навігації та зв’язку. Полтава: ПНТУ, 2021. Т. 4(66). С. 94–98. DOI: 10.26906/SUNZ.2021.4.94.

7. Пахомова В. М. Дослідження інжинірингу трафіка в комп’ютерній мережі УЗ за технологією MPLS TE. Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту. 2015. № 1 (55). С. 154–157.

8. Introduction to Using OPNET Modeler. OPNETWORK2002. Simulation and modeling. SYSC 4005/5001.

9. Zhukovyts’kyy I., Pakhomova V., Domanskay H., Nechaiev A. Distribution of information flows in the advanced network of MPLS of railway transport by means of a neural model. MATEC294 (EOT-2019). 04007(2019). 7 p. URL: https://doi.org/10.1051/matecconf/201929404007.

УДК [004.942+005.5]: 614.84

МОДЕЛЮВАННЯ СИСТЕМИ МАРШРУТИЗАЦІЇ ОПЕРАТИВНОЇ ІНФОРМАЦІЇ З МІСЦЯ НАДЗВИЧАЙНОЇ ПОДІЇ

Олександр Придатко, Юрій Борзов, Валентин Придатко, Сергій Дідушок

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *В роботі представлені окремі елементи процесу моделювання системи маршрутизації оперативної інформації між рятувальними підрозділами. Робота орієнтована на висвітлення процесу визначення кількості та місць розташування ретрансляційного обладнання на основі математичного апарату теорії графів.*

Ключові слова: *маршрутизація інформації, оперативне інформування.*

Abstract. *The work presents separate elements of the modeling process of the operational information routing system between rescue units. The work is focused on highlighting the process of determining the number and locations of relay equipment based on the mathematical apparatus of graph theory.*

Keywords: *information routing, operational information.*

Основною метою роботи є розробка рекомендацій щодо визначення необхідної кількості технічних засобів для забезпечення обміну оперативної інформації між рятувальними підрозділами в ході ліквідації надзвичайної події (НП). Визначення необхідної кількості та різновидів засобів маршрутизації оперативної інформації є однією із основних складових процесу моделювання означеної системи. Для налагодження роботи системи необхідно розгортати мережу ретрансляційного обладнання, а відтак визначати необхідну кількість та місця їх розташування.

Задля визначення оптимальної чисельності та місць розташування ретрансляційного обладнання запропоновано використання понятійного апарату теорії графів із урахуванням характеристик ретрансляційного обладнання та потужностей автомобільних радіостанцій, які є основним засобом маршрутизації оперативної інформації з місця ліквідації НП.

Алгоритм запровадження моделі маршрутизації оперативної інформації визначає один із ключових кроків – це визначення кількості та місць розташування ретрансляційного обладнання за умови дотримання граничних віддалей передачі радіосигналу. При визначенні місця розташування ретрансляційного обладнання ключовим показником є наявність стаціонарних веж із підведенням відповідних мереж (живлення, інтернет).

Ймовірні місця розташування ретрансляційного обладнання наносяться у вигляді графу на карту регіону. Приклад побудови графу системи представлено на рисунку 1.

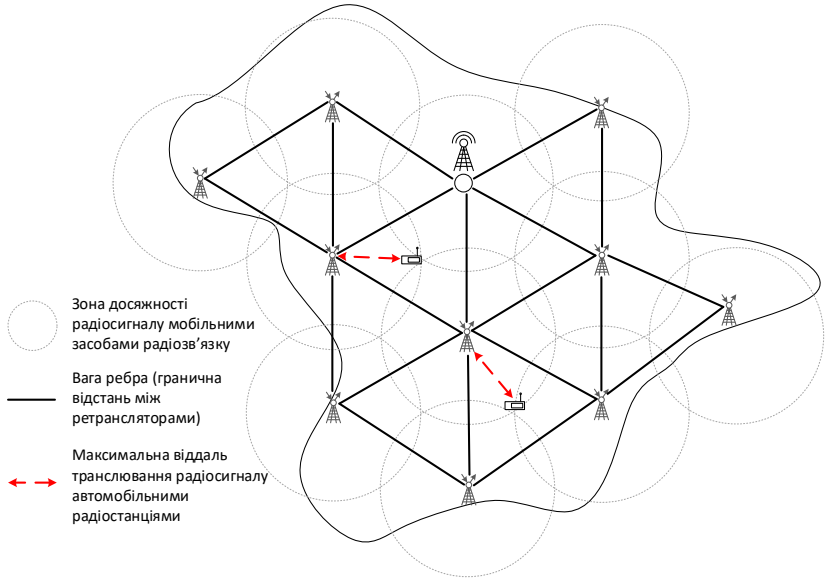


Рисунок 1 – Мережа ймовірних місць розташування ретрансляторів

Граф системи описаний ребрами та вершинами. В якості вершин виступають місця розташування ретрансляторів, а ребра описують відстані між ретрансляційним обладнанням.

Пошук ваги ребер *Ri-j* (відстані між ретрансляторами) визначається картографічним методом із використанням доступних геоінформаціних систем. З метою кращого розуміння, отриману вагу ребер можна представити у вигляді матриці віддалей між вершинами графа:

$$R = \begin{array}{c|ccccccc} & a_0 & a_1 & a_2 & a_3 & \dots & a_n \\ a_0 & 0 & R_{0-1} & R_{0-2} & R_{0-3} & \dots & R_{0-n} \\ a_1 & R_{1-0} & 0 & R_{1-2} & R_{1-3} & \dots & R_{1-n} \\ a_2 & R_{2-0} & R_{2-1} & 0 & R_{2-3} & \dots & R_{2-n} \\ a_3 & R_{3-0} & R_{3-1} & R_{3-2} & 0 & \dots & R_{3-n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_m & R_{m-0} & R_{m-1} & R_{m-2} & R_{m-3} & \dots & R_{m-n} \end{array}, \quad (1)$$

де $R_{i\text{-}j}$ – відстань між суміжним ретрансляційним обладнанням; a_n – маркування ретранслятора.

Зважаючи на потужність автомобільних радіостанцій, які дозволяють транслювати сигнал на відстань L, виборі веж для розміщення ретрансляційного обладнанням (вибір місць розташування) має враховуватись дотримання граничних віддалей між ними (максимально-допустима вага ребра), що визначається із виразу:

$$L_{гр} = k \cdot L, \tag{2}$$

де L – відстань транслювання радіосигналу автомобільними радіостанціями; k – коефіцієнт, що враховує накладання зон досяжності радіосигналу (запобігання утворення "мертвих" зон), приймається в межах 1,7 – 1,75.

Отримавши фактичні значення ваги ребер графа (1) та граничну віддаль між розташуванням ретрансляційного обладнання (2), необхідно провести порівняння означених величин. Якщо справджується нерівність $R_{i\text{-}j} \leq L_{гр}$, то визначена кількість та обрані місця розташування ретрансляторів у повній мірі забезпечуватимуть покриття досліджуваного регіону необхідним рівнем зв'язку. В противному випадку, необхідно зменшувати вагу ребер шляхом передислокації ймовірного місця розташування ретранслятора або збільшення їх загальної кількості та проводиться повторний перерахунок. При виборі місць розташування ретрансляційного обладнання слід враховувати особливості рельєфу місцевості.

За результатами аналітичних досліджень та з використанням понятійного апарату теорії графів розроблено рекомендації щодо визначення необхідних технічних засобів для забезпечення обміну оперативною інформацією в ході ліквідації надзвичайної події, що орієнтовано на налагодження стабільного зв'язку між підрозділами ДСНС на регіональному рівні.

Інформаційні джерела

1. Informational System of Project Management in the Areas of Regional Security Systems' Development / O. Prydatko, O. Smotr, Yu. Borzov, I. Solotvinskyi, O. Didyk // 2018 IEEE Second Conference on Data Stream Mining & Processing. – 2018. – №2. – С. 187–192.

2. Shcherbachenko O. Organizational and technological backgrounds of project configuration management for firefighting / O. Shcherbachenko // TEKA an international quarterly journal on motorization, vehicle operation, energy efficiency and mechanical engineering. – 2017. – №3(17). – С. 49–53.

3. System approach to the investigation of the projects of the fire-fighting systems' functioning and development of the united territorial communities / A. Tryguba, R. Ratushny, O. Shcherbachenko, O. Bashynsky // TEKA an international quarterly journal on motorization, vehicle operation, energy efficiency and mechanical engineering. – 2018. – Vol.18, №1. – С. 5–12.

4. Придатко О. В. Модель портфельного управління проектами розвитку регіональних систем безпеки життєдіяльності / О. В. Придатко, І. В. Солотвінський, І. Я. Кокотко, М. Б. Івановський // Управління розвитком складних систем : Зб. наук. праць. К. : КНУБА, 2018. – №36. – С.42-51.

Напрям 9

3D МОДЕЛЮВАННЯ ТА 3D ДРУК

УДК 514.18

3D ЛАЗЕРНЕ СКАНУВАННЯ В МОДЕЛЮВАННІ ОБ'ЄКТІВ БУДІВНИЦТВА

Олена Гумен, Ірина Селіна, Дмитро Глеба

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", м. Київ, Україна

Анотація. *Сфера використання лазерів у сучасному інформатизованому суспільстві майже безмежна. У даній роботі розглядається питання лазерного сканування різного роду поверхонь об'єктів, доцільність використання такої технології в будівництві. Дана робота має оглядовий характер, матеріал окреслює перспективи майбутніх досліджень.*

Ключові слова: *лазерне сканування, будівництво, моделі об'єктів, 3D сканування.*

Abstract. *The scope of use of lasers in today's information society is almost limitless. The paper examines the issue of laser scanning for various surfaces of objects, the feasibility of using such technology in construction. This work has a review character, the material outlines the prospects for future research.*

Keywords: *laser scanning, construction, object models, 3D scanning.*

Технологія лазерного сканування дозволяє дистанційно досліджувати і за отриманими даними створювати кресленики, перерізи, плани та тривимірні цифрові моделі об'єктів складної геометричної форми [1, 2]. Даний метод є найбільш раціональним та точним і реалізується через лазерні сканери (рис. 1).

Рисунок 1 – Сучасний наземний лазерний сканер

Суть технології лазерного сканування полягає у визначенні просторових координат точок поверхні

об’єкта. Кількість точок визначається регулярною сіткою (кількість рядків і кількість стовпчиків задаються користувачем) – так звана, матриця сканування [1]. Чим більша щільність матриці сканування, тим більша щільність точок на поверхні об’єкта. Результатом роботи являється множина точок з відомими тривимірними координатами. Такі набори точок прийнято називати хмарами точок або сканами. Кількість точок в одному скані може варіюватись від декількох десятків тисяч до десятків і сотень мільйонів [3].

Робота по скануванню (рис. 2) найчастіше відбувається в декілька сеансів через форму об’єкта, коли всі поверхні не видно з однієї точки (наприклад, чотири стіни будівлі). Отримані з різних точок стояння скани суміщаються за допомогою спеціального програмного модуля в єдиний простір – хмару точок всього об’єкта. Хмара точок всього об’єкта несе максимум інформації про нього. В подальшому по цій хмарі точок можна вирішувати найрізноманітніші задачі, такі як: отримання тривимірної моделі об’єкта; отримання креслеників, у тому числі, перерізів, планів, фасадів; виявлення дефектів конструкцій шляхом порівняння з проєктною моделлю; визначення і оцінка значень деформації шляхом порівняння з раніше проведеними вимірами; отримання топографічних планів методом віртуальної зйомки; розрахунок об’ємів між поверхнями та ін.

Рисунок 2 – Процес створення 3D моделі

Суттєве зменшення термінів польових робіт; точність, як у традиційних геодезичних методів; легка інтеграція у виробництво; сумісність з традиційними геодезичними методами**;** отримання максимально повної

інформації про об’єкт; можливість повторного використання результатів зйомки; отримання точних і наочних результатів вже на попередньому етапі робіт є перевагами технології лазерного сканування.

Основні переваги застосування 3D сканування у будівництві – це зручне створення просторових моделей (рис. 3); можливість коригування проєкту в процесі будівництва; оптимальне планування і контроль переміщення, установки і видалення великих частин споруд або обладнання; монтажні роботи; моніторинг стану об’єкта при експлуатації; відновлення втрачених креслеників.

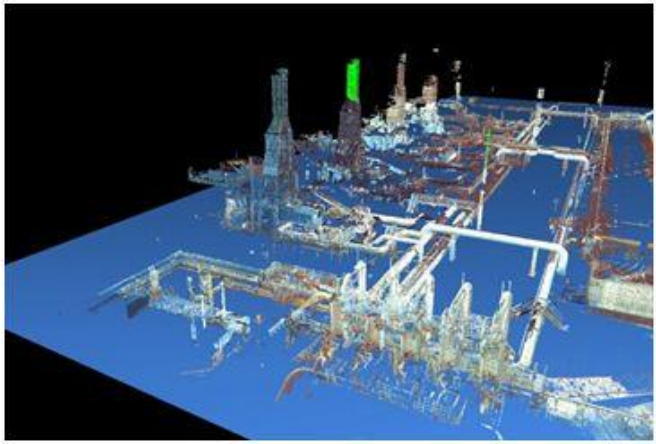


Рисунок 2 – Результат 3D моделювання

Загалом вказані вище переваги 3D лазерних технологій дуже вагомі. Подальший їх розвиток відкриє нові напрямки та можливості застосування. Дані технології мають найбільш високу точність зчитування матеріальних точок різного роду об’єктів. Також слід відмітити високу автоматичність процесу, порівняну дешевизну та простоту в використанні.

Інформаційні джерела

1. Лазерне сканування / методичний посібник. – К.: ЗАТ Науково-виробниче підприємство НАВГЕОКОМ, 2006.

2. Прилади зчитування компанії Faro [Електронний ресурс] – Режим доступу: http://faro.in.ua/focus3d.html.

3. Лазерное сканирование [Електронний ресурс] – Режим доступу: http://ukrgeo.com.ua/ua/473/678.

УДК 004.8 + 614.8

ЗГОРТКОВА НЕЙРОННА МЕРЕЖА ДЛЯ ВИЗНАЧЕННЯ ГРУП МОБІЛЬНОСТІ УЧАСНИКІВ ЗА ДАНИМИ КАМЕР ВІДЕОСПОСТЕРЕЖЕННЯ

Олександр Хлевной, Діана Райта

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Наведено концептуальну модель для визначення параметрів руху евакуаційних потоків за даними камер відеоспостереження із застосуванням штучної нейронної мережі та алгоритму SORT. Запропоновано архітектуру згорткової нейронної мережі для вирішення задачі класифікації учасників евакуації за групами мобільності, представлену 2 згортковими шарами, 2 шарами субдискретизації, двома прихованими повнозв'язними шарами та вихідним класифікаційним шаром нейронів.*

Ключові слова: *машинне навчання, згорткові нейронні мережі, евакуація при пожежі, швидкість руху, група мобільності.*

Abstract. *A conceptual model for determining the movement parameters of evacuation flows based on the data of video surveillance cameras using an artificial neural network and the SORT algorithm is presented. A convolutional neural network architecture is proposed for solving the problem of evacuation participants classification by mobility groups. It is represented by 2 convolutional layers, 2 Max Pooling layers, two hidden fully connected layers and an output classification layer.*

Keywords: *machine learning, convolutional neural networks, fire evacuation, mobility group.*

При дослідженні параметрів руху евакуаційних потоків вихідні дані визначають на основі опрацювання записів відеокамер без застосування програмних засобів аналізу відеопотоку, що займає багато часу і є трудоємким процесом. В той же час на основі аналізу ряду досліджень можна зробити висновок, що засоби аналізу та класифікації зображень, а також виявлення та класифікації рухомих об'єктів у відеопотоці дають змогу отримати якісні результати. Підвищити швидкість та точність процесу отримання емпіричних даних можливо за рахунок нейромережевого аналізу евакуаційних потоків.

На першому етапі необхідно розподілити учасників евакуації за групами мобільності (М1, М2, М3, М4). Для цього необхідно вирішити задачу класифікації. Для розпізнавання на кадрах учасників евакуації найбільш доцільно використати згорткову нейромережу. Для забезпе-

чення класифікації учасників евакуації вихідні дані, отримані згортковими та субдискретизаційними шарами, слід подати на кілька шарів повнозв'язних нейронів. Ми пропонуємо використати 2 приховані шари із функцією активації ReLu (512 і 128 нейронів відповідно), а також вихідний класифікаційний повнозв'язний шар із 4 нейронів з функцією активації Softmax. Також у якості основних параметрів моделі в процесі навчання пропонуємо застосувати градієнтну нормалізацію на кожному шарі, алгоритм оптимізації – метод стохастичного градієнта та функцію втрат Negative Log Likelihood (рис. 1).

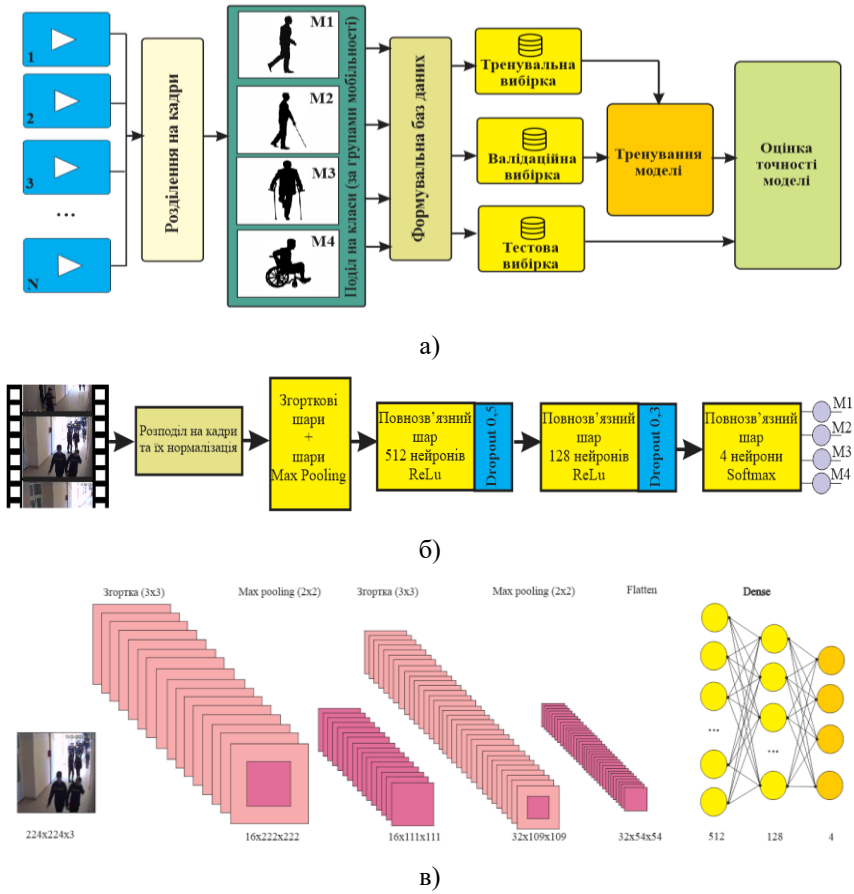


Рисунок 1 – Концептуальна модель розпізнавання учасників евакуації та класифікації їх за групами мобільності: а) принципова схема навчання нейромережі; б) загальна архітектура мережі; в) структура шарів нейронної мережі

Для навчання нейромережі найбільш доцільно застосовувати тензорні процесори на хмарній платформі для машинного навчання Google Colaboratory. В якості тренувальної та тестової вибірок для навчання необхідно використати результати замірів, отримані в процесі попередніх досліджень [1], під час яких бази емпіричних даних формувалися шляхом опрацювання відеозаписів авторами із використанням методів, описаних на початку статті.

Застосування алгоритму SORT [2] у поєднанні із запропонованою моделлю для конверсії швидкості дає змогу отримувати значення миттєвої швидкості руху учасників евакуації, що дозволить суттєво пришвидшити процес формування баз емпіричних даних параметрів евакуації для змішаних потоків та матиме важливе практичне значення для подальших наукових досліджень.

Інформаційні джерела

1. Хлевной О.В. Нормування вимог пожежної безпеки до евакуаційних шляхів і виходів у закладах середньої освіти з інклюзивним навчанням: дис.... канд. техн. наук: 21.06.02 / Львів, 2021. – 188 с.

2. Bewley, A., 2020. Simple online and realtime tracking. Available at: https://github.com/abewley/sort

Напрям 10

МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ СИСТЕМ

УДК 004.94

THE MODEL OF AUTOMATED WAREHOUSE DESIGN SYSTEM

Oleksandr Muliarevych

Lviv Polytechnic National University, Lviv, Ukraine

Анотація. *В роботі представлено короткий огляд моделі проєктування складу. Розроблена система допомагає розрахувати динамічну частину складу – зону прийому та вигрузки, зони збору та поповнення. Розглянута система включає в себе наступні рішення: модель прогнозування та технології безсерверного обчислення. В підсумку, такі підходи зменшують час пошуку результуючої оптимальної параметричної комбінації та дозволяє автоматизувати процедуру проєктування складу.*

Ключові слова: *проєктування складу, безсерверні обчислення, зона прийому та вигрузки.*

Abstract. *In this work short model overview of warehouse design system is represented. Developed system helps to calculate dynamic part of warehouse – acceptance and shipping zones, picking and replenishment zones. The described system includes next solutions: prediction model and serverless computing technologies. In summary, such approaches decrease time for optimal parameters combination result search and automate warehouse design procedure.*

Keywords: *warehouse design, serverless computing, acceptance and shipping zones.*

Warehouse operation is one of the main problems that appears for different industries and business models that are not conducted with building and design new warehouse buildings [1]. This fact causes a high popularity of such called "logistics outsourcing" or when between 2 typical participants in a goods flow: supplier and customer appear the third, who helps with goods storage, distribution, and transfer, it is called also "third-party logistic"

provider (3PL) [2]. Third-party logistics provider – is usually a firm which provides multiple logistics services for use by customers related to facilitate the movement of parts and materials from suppliers to manufacturers and finished products from manufacturers to distributors and retailers. Goods transportation, warehousing, cross-docking, inventory management, packaging and freight forwarding are provided together as a package of services by the 3PL provider [3]. The estimation of space should be done as fast as possible by professional logistics engineers [4], but a lot of manual calculation has several disadvantages:

1) human failure probability on some step that is hard to detect;

2) in the case of huge portions of input order data and big list of constraints from a customer, it could increase calculation complexity and time for final result definition till the month or even more [2];

3) set of options that would be checked by professionals doesn't guarantee that the best optimal by cost design option wouldn't be missed, because full combinatorial analysis is impossible task for manual execution.

That's why developing software and computer systems for logistics, especially automated warehouse design, is so popular nowadays [3] and Deopware.com platform that includes methodology and approaches described in this article isn't an exclusion. Firstly, let's overview what type of zones warehouse consists of and what list of parameters, constraints and input order data used for evaluation. The processing areas for the goods flow are next [4]:

1) unloading and acceptance zone;

2) storage and collection zone;

3) control and picking zone;

4) transport expedition zone;

5) shipping zone.

The model of a system at the top level is demonstrated in Fig. 1. Input data is uploaded to a sub-system of data and limits processing. As a result, we receive calculated statistics about input data and potential pattern [5], that could be used in the optimal result prediction sub-system [6] for searching for similar evaluated already warehouse design tasks to find out potential optimal combinations of parameters. The most sensitive sub-system to performance is the search for an optimal combination task executor, which should use prepared and processed input data and constraints with a list of parameter combinations. The aim is to run an evaluation of each combination – find its summary labor cost value, then define which combination has the lowest cost.

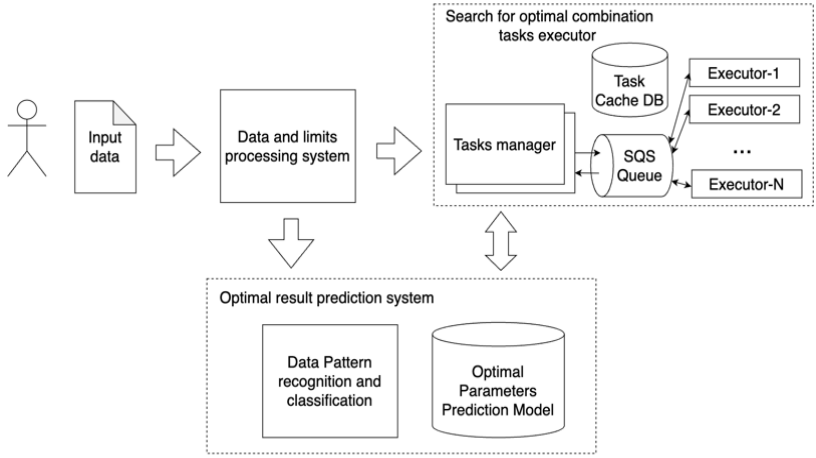


Fig. 1. Model of automated developed warehouse design system

For that purpose, the task manager caches processed input data and constraints in-memory task cache DB and creates tasks for execution in SQS queue (Amazon Simple Queue Service) [7]. The N executors triggers execution when events are fired via queue, so the number of light-weighted functions with cached context that evaluate separate combination correlates with the number of task complexity. Time results for differet set of tasks with mentioned number of combinations and number of available executors is represented in Fig. 2.

Task Name / Type	100-executors	500-executors	1000-executors
Task1 (3128 combinations)	2146 s	486 s	299 s
Task2 (5980 combinations)	4144 s	949 s	572 s
Task3 (6130 combinations)	4506 s	993 s	587 s
Task4 (7005 combinations)	4805 s	1123 s	644 s
Task5 (7761 combinations)	5704 s	1220 s	764 s
Task6 (8608 combinations)	5724 s	1394 s	808 s
Task7 (8890 combinations)	6659 s	1469 s	875 s
Task8 (10219 combinations)	7225 s	1589 s	940 s
Task9 (21010 combinations)	15148 s	3404 s	1933 s

Fig. 2. Demonstration of waregouse design task calculations

In the list of commercial tasks, per each of them are demonstrated execution times required for full combination evaluation solved on different scaling of serverless computing: 100, 500 and 1000 executors. The range of combinations in tasks approximately from 3000 till 21000. The applied serverless computing in developed system brings next benefits:

1) saving of resources – we don't use any resources in case we have no active tasks;

2) maximum efficiency of used resources – the required number of executors used at max ratio of cpu and RAM load exactly for task execution.

Moreover, using scaling up from 100 to 1000 executors pool boost system performance in 7 times and more. The developed system for automated warehouse design using serverless computing and prediction model enables reducing time for search of parameter's combination that will help to achieve optimal labor cost value in acceptable time comparing to manual evaluation of several selected potentially good combinations, that highly speed up the performance of 3PL provider companies.

References

1. S. S. Heragu, Facilities Design. CRC Press, 2018, pp. 261–314.

2. A. Ekeskar, Exploring Third-Party Logistics and Partnering in Construction: A Supply. Linköping University Electronic Press, 2016.

3. K. Grzybowska, A. Awasthi, R. Sawhney, Sustainable Logistics and Production in Industry 4.0: New Opportunities and Challenges. Springer Nature, 2019, pp. 31–57.

4. M. P. Stephens, Manufacturing Facilities Design & Material Handling, 6-th ed. Purdue University Press, 2019, pp. 287–301.

5. G. Bonaccorso, Machine Learning Algorithms, 1st ed.. Packt Publishing, 2017, pp. 476–507.

6. C. M. Bishop, Pattern Recognition and Machine Learning. Springer New York, 2016, pp. 179–196.

7. D. Poccia, AWS Lambda in Action: Event-driven serverless applications. Simon and Schuster, 2016, pp. 287–334.

УДК 621.372.083.92

МАТЕМАТИЧНІ МЕТОДИ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ВІЗУАЛІЗАЦІЇ ФАЗОВО-ЧАСТОТНИХ ХАРАКТЕРИСТИК АКУСТИЧНИХ СИГНАЛІВ

Тарас Гембара

Кафедра прикладної математики і механіки Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Дослідження акустичних характеристик приміщень представляє великий інтерес з наукової точи зору, з метою забезпечення їх акустичної безпеки. В роботі розробляються основи системи вимірювання і аналізу акустичних характеристик приміщень, наприклад з використанням поширених акустичних систем і мікрофонів на базі комп'ютера зі звуковою картою і програмним забезпеченням MATLAB та Mathcad, досліджені можливості такої системи по вимірюванню імпульсної реакції приміщення, його амплітудно – частотних і фазово – частотних характеристик.*

Ключові слова: *акустичний сигнал, статистичний розподіл, імпульсна реакція, фаза, частота.*

Abstract. *The study of acoustic characteristics of premises is of great interest from a scientific point of view, in order to ensure their acoustic safety. In the work, the basics of the system for measuring and analyzing the acoustic characteristics of rooms are developed, for example, using common acoustic systems and microphones based on a computer with a sound card and MATLAB and Mathcad software, the possibilities of such a system for measuring the impulse response of a room, its amplitude – frequency and phase – frequency characteristics.*

Keywords: *acoustic signal, statistical distribution, impulse response, phase, frequency.*

Дослідження акустичних характеристик приміщень, є складною задачею, далекою від остаточного і однозначного вирішення, але в той же час представляє великий інтерес з наукової точи зору, з метою забезпечення їх акустичної безпеки. Важливим є аналіз можливості по вимірюванню імпульсної реакції приміщення, встановлення його амплітудно-частоних характеристик (АЧХ) та фазово частотних характеристик (ФЧХ).

При моделюванні сигнал задається у вигляді функції одного або декількох аргументів, причому функції поділяються на два типи: вбудовані функції; функції, визначені користувачем. Застосування функцій обох типів в розрахунках абсолютно однакове, з тим винятком, що будь-яку вбудовану функцію можна використовувати відразу в будь-якому місці доку-

мента, а для користувача функцію необхідно попередньо визначити в документі до моменту обчислення її значення. Функції в пакеті Mathcad записуються в звичайній математичній формі : *f (x, ...)* – ім’я функції; *x, ...*– список змінних.Функції в пакеті MATLAB – мають спеціальні імена об’єктів, виконують певні перетворення над своїми аргументами і при цьому повертають результати цих перетворень.При цьому результат обчислення функції з одним змінним параметром підставляється на місце її виклику, що дозволяє використовувати функції в математичних виразах. Наприклад: 2xsin (pi / 2). Функції, в загальному випадку, мають список аргументів (параметрів), укладені в круглі дужки. Якщо функція повертає кілька значень, то вона записується в вигляді: [Y1,Y2, ...]=func (X1,X2, ...), де Y1, Y2, ... – список вихідних аргументів і X1, X2,... – список вхідних аргументів (параметрів), func – ім’я функції.

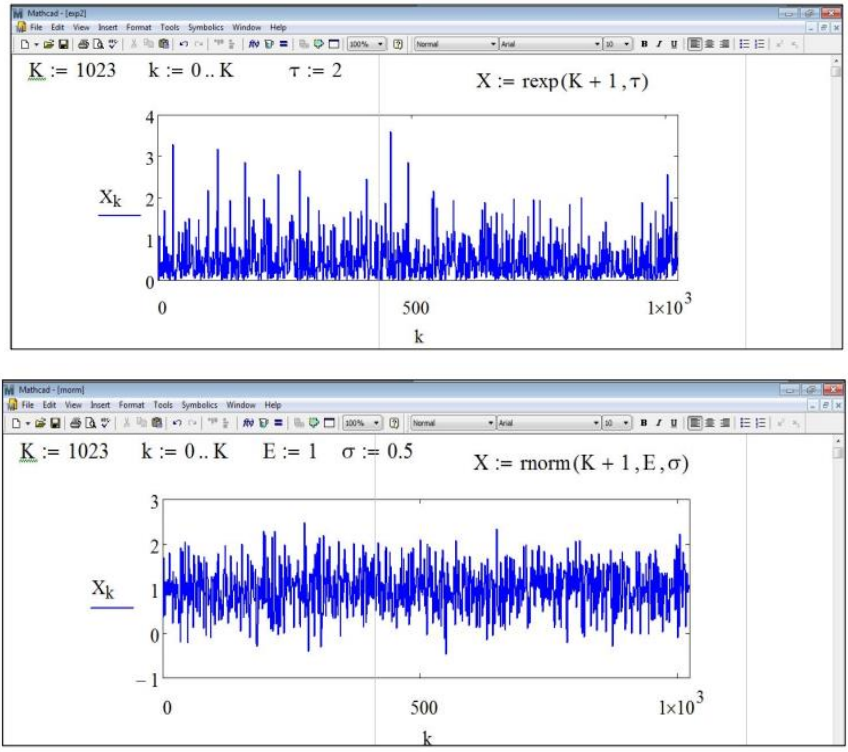


Рисунок 1 – Задання випадкового сигналу з нормальним (верхній лістинг) і експоненціальним (нижній лістинг) розподілом ймовірностей

У сучасних методах математичної обробки акустичних сигналів для дослідження характеристик електроакустичних систем і приміщень знаходять широке застосування ЛЧМ сигнали і псевдовипадкові послідовності MLS. При впливі випромінюваного ЛЧМ сигналу, прийнятий акустичний відгук обробляють синхронно побудованим смуговим фільтром. Швидкість зміни частоти повинна бути такою, щоб у смугу фільтра встигли потрапити всі сигнали системи. Тому час вимірювання методом ЛЧМ має бути набагато більше тривалості відгуку системи.

При застосуванні методу MLS за допомогою регістра зсуву генерується періодична псевдовипадкова послідовність значень 1 і -1. Період такого сигналу дорівнює 2^N-1, где N – порядок послідовності, кореляційна функція близька до дельта-функції, а спектр близький до білого шуму. У середовищі MATLAB створені програми, які генерують ці випробувальні сигнали із заданими параметрами і можуть їх відтворювати через звукову карту. За допомогою розробленого програмного забезпечення в системі MATLAB формується тестовий сигнал ЛЧМ або MLS, який відтворюється досліджуваною активною програмною акустичною системою через звукову карту. Для задання випадкових сигналів в Mathcad є вбудована функція, що задає найпоширеніші в математичній статистиці закони розподілу, наприклад r*(K,par) -створює вектор K незалежних випадкових чисел, кожне з яких має відповідні розподіл, де * – частина імені функції, яка задає закон розподілу; par – список параметрів розподілу. Наведемо приклади задання випадкових сигналів за допомогою вбудованих функцій. Для їх введення зручно скористатися діалоговим вікном InsertFunction. У списку FunctionCategory потрібно вибрати Random Numbers (випадкові числа) – для вставки функції генерації випадкових чисел. У списку Function Name вибираємо функцію, в залежності від потрібного закону розподілу.

Порівнюючи графіки відгуків приміщення, можна авважати, що за зовнішнім виглядом відгуку на ЛЧМ сигнал вже можна зробити висновок про нерівномірність АЧХ системи. З відгуку системи на MLS сигнал таких певних висновків зробити не можна. Розрахунок імпульсної характеристики системи, а також АЧХ і ФЧХ проводився за допомогою математичної операції згортки системного відгуку з опорним сигналом. Операція згортки здійснювалася в спектральній області шляхом перемноження спектра прийнятого сигналу на комплексно спряжений спектр опорного сигналу.

Інформаційні джерела

1. Цифрова обробка аудіо- та відеоінформації у мультимедійних системах: Навчальний посібник / Коваль В.В., Розорінов Г.М., Сукач Г.О. – К.: Наукова думка.

УДК 614.841.2

МАТЕМАТИЧНА МОДЕЛЬ ТЕМПЕРАТУРНОГО ПОЛЯ РУХОМОГО ОБ'ЄКТА

Оксана Карабин, Мирослава Кусій, Роман Яницький

Кафедра прикладної математики і механіки Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Створено математичну модель температури займання рухомого об'єкта від нерухомої поверхні випромінювання. Наявність функції залежності температури від часу дозволяє за допомогою програмних математичних пакетів моделювати різні ситуації залежно від висоти польоту r, кута α між вектором швидкості і віссю Ox, розмірів пожежі. На основі складеного алгоритму реалізовано розрахунок температури.*

Ключові слова: *конвективний теплообмін, температура спалаху, полум'я рухомої низової пожежі, коефіцієнт опромінення.*

Abstract. *A mathematical model of the ignition temperature of a moving object from a stationary radiation surface is created. The presence of the function of temperature dependence on time allows using mathematical software packages to simulate different situations depending on the height of flight r, the angle α between the velocity vector and the axis Ox, the size of the fire. Based on the compiled algorithm, the temperature calculation is implemented.*

Keywords: *convective heat transfer, flash point, flame of a moving ground fire, radiation coefficient.*

Людина є причиною виникнення пожеж, але і в силах людини запобігти цьому великому лиху. В науковій періодиці зустрічаємо тисячі публікацій, пов'язаних з цією проблематикою. Кожна з цих публікацій вносить свою частку в запобіганні цьому лиху. Експериментальні моделі процесів теплообміну на відкритій території є необхідними, але багатовартісними. Математичні і ком'ютерні моделі цих процесів дозволяють прогнозувати і моделювати процеси теплообміну з врахуванням різноманітних вхідних параметрів і умов не затрачаючи при цьому матеріальних ресурсів для постановки експерименту.

Багато робіт присвячено комп'ютерному моделюванню контурів пожеж та поширенню пожеж [1−3]. Окремої уваги заслуговують роботи, присвячені математичному моделюванню процесів теплообміну та тепломасопереносу під час лісових пожеж [4, 5]. Зокрема, в роботі [5] отримана математична модель процесу нагрівання хвоїнки внаслідок радіаційного теплового випромінювання з поверхні у формі прямокутника, за якою можна встановити час її нагрівання до температури самозаймання.

Метою роботи є створення математичної моделі температури займання рухомого об'єкта від нерухомої поверхні випромінювання. Рухомим об'єктом ми вважаємо літальний апарат, який здійснює моніторинг території, на якій відбувається пожежа. Вирішення поставленої задачі здійснювалось методом безпосереднього інтегрування.

Нехай ділянка, що опромінюється рухається вздовж діагоналі прямокутника зі сталою швидкістю v (рис. 1). Положення ділянки визначається $x = vt\cos\alpha$, $y = vt\sin\alpha$, де α – кут між вектором швидкості і віссю Ox.

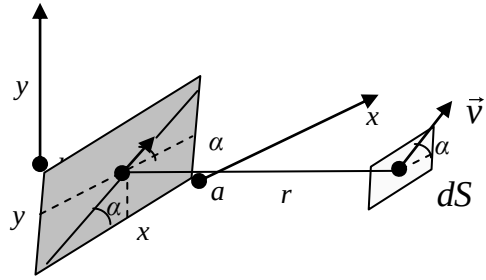


Рисунок 1 – Рухома ділянка опромінення

Диференціальне рівняння, яке описує процес нагрівання поверхні до температури $T = T(t)$ за час t має вигляд:

$$cmdT = \sigma\varepsilon\left(T_1^4 - T^4\right)\psi(t)Sdt \qquad (1)$$

Початкова умова

$$T(0) = T_0$$

де, m – маса поверхні, кг, σ – стала Стефана-Больцмана, ε – випромінювальна здатність, ψ – кутовий коефіцієнт опромінення (відповідно до закону Ламберта).

Визначено методом безпосереднього інтегрування кутовий коефіцієнт опромінення ψ(t). Підстановка коефіцієнта опромінення в рівняння (1) та почленне інтегрування цього рівняння дає нам функцію залежності температури від часу в неявному вигляді. Наявність функції залежності температури від часу дозволяє за допомогою програмних математичних пакетів, таких як Maple, MathCad та інші моделювати різні ситуації залежно від висоти польоту r, кута α між вектором швидкості і віссю Ox, розмірів пожежі.

На основі складеного алгоритму реалізовано розрахунок температури

Алгоритм

− Ініціалізація:

− *обчислити*: сталу інтегрування C; коефіцієнт опромінення ψ_k(t);

− сформувати масив температур T;

– *вхідні дані*: лічильник ітерацій *r*-висота польоту літального апарата;
– крок ітерацій лічильника *r step* 1=4;
– лічильник ітерацій *k*, крок ітерацій лічильника *k step* 2=16
– розмір ділянки пожежі *a, d*; кут нахилу α до осі *Ox*;
– швидкість руху *v*; питома теплоємність *c*;
– температура навколишнього середовища T_0, температура полум'я T_1;
– маса літального апарата *m*;
– випромінювальна здатність ε; стала Стефана-Больцмана σ;
– *a, d, α, v*, T_0, – вхідні дані, які може змінювати користувач залежно від умов пожежі

while $r \le r_{\max}$ do
  обчислення сталих інтегрування C
  while $k \le t_{\max}$ do
    обчислення коефіцієнта опромінення $\psi_k(t)$
    обчислення температури $T_k(t)$
    k=k+step 2
  end
  r=r+step 2
end
Return масив температур *T*

Інформаційні джерела

1. Karabyn, O., Smotr, O., Kuzyk, A., Malets, I., Karabyn, V. (2023). Mathematical and Computer Model of the Tree Crown Ignition Process from a Mobile Grassroots Fire. In: Babichev, S., Lytvynenko, V. (eds) Lecture Notes in Data Engineering, Computational Intelligence, and Decision Making. ISDMCI 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 149. Springer, Cham. https://doi.org/10.1007/978-3-031-16203-9_9.

2. О.О. Смотр, Ю.І. Грицюк Моделювання контурів лісових пожеж. Пожежна безпека. Збірник наукових праць №20, 2012, 170-180 с.

3. Кононов Михайло Володимирович / Судаков Олександр Олександрович Особливості моделювання лісових пожеж на кластерах в Grid Вісник Київського національного університету імені Тараса Шевченка. Фізико-математичні науки Том 2., 2011, 185–193

4. Зеленський К. Х. Математичне моделювання аеродинаміки верхових лісових пожеж / К. Х. Зеленський, В. О. Ліщина // Наукові нотатки. – 2010. – Вип. 27. – С. 110–115. – Режим доступу: http://nbuv.gov.ua/UJRN/Nn_2010_27_23.

5. Кузик А. Д. Математичне моделювання процесів кондуктивного і радіаційного теплообміну під час пожежі в соснових лісах / А. Д. Кузик, В. І. Товарянський // Пожежна безпека. – 2017. – № 30. – С. 105–113. – Режим доступу: http://nbuv.gov.ua/UJRN/Pb_2017_30_14

УДК 614.8

КОМП'ТЕРНЕ МОДЕЛЮВАННЯ МЕТОДУ БАГАТОКАНАЛЬНИХ ВИМІРЮВАНЬ ДЛЯ СИСТЕМ КОНТРОЛЮ ТА ПОПЕРЕДЖЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Сергій Рудаков, Ігор Рудаков

Національний університет цивільного захисту України м. Харків, Національний технічний університет "Харківський політехнічний університет, м. Харків, Україна

Анотація. *Досліджено та обгрунтовано застосування модифікованого методу залежності розрахунку при багатоканальних вимірюваннях частотних імпульсних сигналів. Отримані результати можуть бути використані при розробці, проєктуванні та виготовленні багатоканальних вимірювачів частотних імпульсних сигналів для систем централізованого контролю та попередження надзвичайних ситуацій.*

Ключеві слова: *багатократні вимірювання, частотні імпульсні сигнали, системи централізованого контролю, попередження надзвичайних ситуацій.*

Abstract. *In article it is investigated and soundly application of the modified method of dependent calculation at multichannel measurements of frequency pulse signals. The received results can be used by working out, designing and manufacturing of multichannel measuring instruments of frequency pulse signals for systems of the centralized control and the prevention of emergency situations.*

Keywords: *multichannel measurements, frequency pulse signals, systems of the centralized control, the prevention of emergency situations.*

Модифікований метод залежного рахунку полягає:

– у використанні єдиної шкали часу для всіх вимірюваних сигналів;

– у виконанні непрямих вимірювань за допомогою вимірювання інтервалу часу, рівного цілому числу періодів вимірюваного сигналу, з подальшим визначенням вимірюваної частоти;

– у конвеєрній паралельній організації вимірювань і передачі результатів вимірювань в ЕОМ.

Розглянемо реалізацію такого методу вимірювань n-канального модуля введення (МВ) частотних імпульсних сигналів в ЕОМ. На входи n-канального МВ поступають імпульсні послідовності $S_1(t)$, ..., $S_n(t)$ частоти слідування імпульсів, які підлягають вимірюванню.

До складу МВ входять n ідентичних вимірювальних каналів ВК1, ..., *ВКj, ..., ВКn* та мікроконтролер МК з п'ятьма портами введення-виводу: ПСС – портом сигналів статусу $\{c_{ji}\}$; ПВвД– портом вводу даних $\{d_{ji}\}$; ПУ– портом управляючих сигналів $\{u_{ji}\}$; ЛВС – процесором зовнішніх подій, який приймає сигнали $\{z_{ji}\}$ та формує команди $\{k_{ji}\}$; ППВ – портом послідовного вводу-виводу, який дозволяє проводити обмін командами та результатами вимірювань з центральною ЕОМ (ЦЕОМ), де *j* й *i* означають, відповідно, номери вимірювального каналу та вимірювання, що проводиться, при цьому $j = \overline{1,n}$.

Склад довільного вимірювального каналу МВ представлений на рисунку 1. По аналогових лініях зв'язку з виходів частотних датчиків або інших джерел сигналів на входи МВ поступають вимірювані імпульсні сигнали $S_1(t)$, ..., $S_n(t)$. У промислових умовах експлуатації вони піддаються дії перешкод $n(t)$ загального і нормального вигляду.

На вході вимірювального каналу розташований тригер Шмітта ТШ, який поновлює прямокутну форму імпульсів, що поступають по лініях зв'язку, і перешкод нормального вигляду, що знижують дію. Вихідний сигнал ТШ поступає на вхід пристрою гальванічної розв'язки ПГР, що здійснює гальванічну розв'язку входу і центральної частини МВС і зниження рівня перешкод загального вигляду. З виходу ПГР імпульси через цифровий ключ ЦК1 поступають на вхід двійкового лічильника імпульсів ЛІ, що здійснює рахунок цілого числа періодів вимірюваного сигналу. Виходи ЛІ підключені до входів порту ПВвД мікроконтролера.

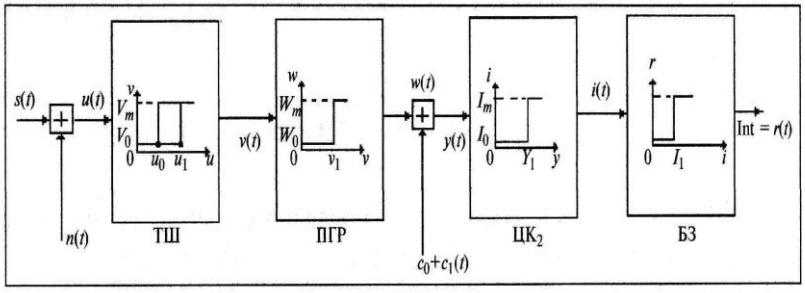


Рисунок 1 – Схема вимірювального каналу модуля вводу даних

Мікроконтролер виробляє команду початку і-го вимірювання. З приходом першого імпульсу z_{ji} мікроконтролер за допомогою внутрішнього таймера фіксує момент його появи і генерує команду k_{ji}, яка блокує вхід блоку захвата *БЗj* процесора зовнішніх подій на мінімальний час вимірювання $T_{в\,min}$.

Після інтервалу часу, рівного часу вимірювання $T_{в\,min}$, розблокується вхід блоку захоплення БЗj процесора зовнішніх подій, мікроконтролер переходить в режим очікування приходу першого наступного імпульсу z_{ji} з виходу ПГР. За допомогою таймера фіксується момент приходу імпульсу z_{ji} і знову блокується захоплення по j-му входу процесора зовнішніх подій.

Час обробки $\tau_{01\,j}$ включає часи захоплення імпульсу $I_{п\,j}$, фіксації моменту його появи $t_{п\,j}$, розрахунку моменту часу $t_{в\,j} = t_{п\,j} + T_{в\,min}$, блокування блоку *БЗj* та ініціалізації блоку *БПj* на якийсь час $T_{в\,min}$. Час $\tau_{пер}$ передачі результатів вимірювань в ЦЕОМ визначається довжиною повідомлення та швидкістю його передачі по каналу зв'язку в ЦЕОМ. Застосування інтерфейсу RS-485 забезпечує високу швидкість передачі повідомлень.

Таким чином, комп'ютерне моделювання запропонованого методу дозволяє модулю вводу даних забезпечити широкий динамічний діапазон вимірювань, який збільшується з ростом амплітуди імпульсів, що вимірюються; високу точність вимірювань. Похибки вимірювань суттєво залежать від параметрів імпульсів, що вимірюються, час вимірювання любого вихідного сигналу приблизно дорівнює двом періодам імпульсної послідовності.

Відмітимо, що запропоновані структура та модифікований для багатоканальних вимірювань метод залежного підрахунку забезпечує рішення задачі розробки універсальних високоточних швидкодіючих модулів вводу частотних імпульсних сигналів в ЦЕОМ для вимірювальних і телевимірювальних систем, програмованих контролерів автоматичного управління, контролю та попередження надзвичайних ситуацій.

УДК 004.94:514.18

ІНФОРМАЦІЙНІ МОДЕЛІ СПІВРОЗМІРНОСТІ ПОВЕРХОНЬ ТЕНТОВИХ КОНСТРУКЦІЙ

Ганна Смаковська

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", м. Київ, Україна

Анотація. *Публікація актуалізує питання комп'ютерного моделювання, а також деякі фізичні властивості модельованих об'єктів. Також в роботі розглядаються питання щодо мембранних тентових конструкцій, що є актуальним у наш час. Аналізуються вимоги до засобів проєктування та вирішення задачі пошуку оптимального розкрою конструкційних матеріалів для виготовлення технічних об'єктів.*

Ключові слова: *комп'ютерне моделювання, тентова конструкція, поверхня, просторові мембрани.*

Abstract. *The publication updates the issues of computer modeling, as well as some physical properties of modeled objects. Also, the paper considers issues related to membrane awning structures, which is relevant nowadays. The requirements for design tools and solving the problem of finding the optimal cutting of structural materials for the production of technical objects are analyzed.*

Keywords: *computer modeling, tent construction, surface, spatial membranes.*

Сьогодні існує багато різних методів комп'ютерного моделювання в залежності від обсягу, мети дослідження та складу використовуваних моделей. Усі вони є потужними аналітичними інструментами, які увібрали весь арсенал новітніх інформаційних технологій, включаючи графічні оболонки для моделювання та інтерпретації початкових результатів моделювання, об'єктно-орієнтоване програмування, інтернет-рішення тощо [1].

Аналіз останніх досліджень і публікацій вітчизняних і зарубіжних вчених показав, що технічні засоби ускладнюються, а будівельні матеріали залишаються стандартними. Це зумовлює нові вимоги до засобів проєктування, які повинні вирішувати завдання пошуку оптимального розкрою конструкційних матеріалів для виготовлення технічних об'єктів.

Так як тентові конструкції в сучасних соціально-економічних умовах набирають сьогодні все більшої популярності завдяки своїм широким властивостям, виникає потреба у швидкому будівництві маловитратних будівель для подолання дефіциту мобільного житла та споруд іншого призна-

чення. Виникає необхідність застосування спеціальних методів, які основані на використанні рівноважного стану мембран, що застосовуються у будівництві.

Для поверхонь, що не розгортаються, вимога “збереження певної геометричної властивості якомога точніше” реалізується у вигляді мінімізації спотворень. Проте, незважаючи на наявність великої кількості наукових праць з даної проблеми ця категорія є недостатньо вивченою.

Геометричне моделювання розглядається як напрямок математичного моделювання, що включає опис геометричних образів і виконання над ними певних операцій у двовимірному, тривимірному або багатовимірному просторі [2]. Теоретичною основою геометричного моделювання є диференціальна та аналітична геометрія, топологія та розділи обчислювальної математики, вивчаються методи побудови кривих ліній, поверхонь, тіл та методи виконання над ними різних операцій і методи керування числовими моделями [3, 4].

Останнім часом все більшого поширення та популярності набувають легкі економічно ефективні тентові конструкції. Вони відносяться до класу м’яких оболонок. Такі конструктивні системи являють собою просторові мембрани з нульовою згинальною жорсткістю, які складаються зі складних поверхонь двоякої кривизни. Ці покриття можуть чинити опір тільки щодо розтягу. Тому їхня перспективність є очевидною внаслідок наявності у них цілого набору позитивних властивостей, що вигідно відрізняє тентові конструкції від традиційних, таких як металічні, залізобетонні та ін. До таких властивостей можна віднести: мобільність, поліфункціональність, легкість, короткий термін побудови (зведення) та демонтажу, а також виразний, привабливий та сучасний зовнішній вигляд.

Для вибору проєктних рішень, важливим фактором є термін служби тентових конструкцій, а також їх вартість. Термін використання залежить від вибору тканини для оболонки. Сама тканина має різну міцність та еластичність у всіх напрямках прикладання навантаження. Тому для напружених конструкцій кращими будуть матеріали, що мають малу повзучість, бо попереднє напруження може бути втрачене, якщо тканина буде розтягуватись чи деформуватись.

Процеси геометричного моделювання та інженерного аналізу подібних споруд мають свою специфіку [5]. На відміну від традиційних конструкцій при заданих крайових умовах, форма натягнутої тканинної поверхні від’ємної кривини Гауса є невідомою на самому початку, а може бути обчислена тільки з використанням відповідних методів [6]. Ще однією відмінністю є те, що в силу своєї специфіки, поверхні двоякої кривини

на відміну від лінійчатих поверхонь, відображуються на плоску область тільки приближено [7]. Це ускладнює побудову їх карт розкрою. Тентова поверхня має ряд небажаних властивостей, таких як наявність “мертвих” зон, нерівномірність розподілу навантаження, концентрація напруги в окремих точках тощо [8].

Таким чином, фактори, які забезпечують велике розмаїття позитивних властивостей м’яких оболонок, одночасно є причинами, котрі суттєво ускладнюють процес аналізу і проєктування тентових конструкцій. Тому, щоб вирішити теоретичні задачі розрахунку якісної тентової конструкції, необхідне застосування спеціальних методів, що основані на використанні рівноважного стану мембран. Не менш актуальною є проблема створення адекватних карт розкрою м’яких оболонок, що тісно зв’язана з коректним рішенням основних задач.

Інформаційні джерела

1. Панкова Л.А. Способи створення універсального інструментарію для комп’ютерного моделювання / Л.А. Панкова, В.А. Проніна // Проблеми управління. – 2006. – № 6. – С. 2–5.

2. Бойко В.А. Щодо змістовної характеристики поняття комп’ютерного геометричного моделювання / В.А. Бойко // Науковий часопис Національного педагогічного університету імені М.П. Драгоманова. Серія 5: Педадогічні науки: реалії та перспективи: [збірник наукових праць] Міністерство освіти і науки України, Нац. Пед. Ун-т ім. М.П. Драгоманова. – К.: Видавництво НПУ ім. М.П. Драгоманова, 2015. – Вип. 51. – С. 26–32.

3. Райковська Г. Геометричне моделювання – основа конструкторськотехнологічних здібностей / Г. Райковська, В. Головня // Нова пед. думка: науково-методичний журнал – 2013. – № 1 Ч. 2. – С. 68–70.

4. Пилюгин В.В. Модель як ключове поняття геометро-графічної підготовки / В.В. Пилюгин, Л. Н. Сумароков // Математичне моделювання, 6: 5, 1994. – С. 21–36.

5. Хейфец А.Л. О реорганизации курса начертательной геометрии на основе 3d компьютерного геометрического моделирования / А.Л. Хейфец // Весник ЮУрГУ. Серия: Образование. Педагогические науки. – 2012. – №14 (273). – С. 96–100.

6. Антоненко І.В. Особливості формування внутрішнього простору будівель і споруд за допомогою тентових конструкцій. Матеріали XI Всеукраїнської практично-пізнавальної конференції “Наукова думка сучасності і майбутнього”, 2017.

7. Gale S., Lewis W. J. Patterning of tensile fabric structures with a discrete element model using dynamic relaxation [Text] / Gale S., W. J. Lewis // Comp’s and Structures. – V. 169. – 2016. – P. 112–121.

8. Высоцкая И.И. Технические развертки изделий из листового материала / И.И. Высоцкая, А.М. Иерусалимский, Р.А. Невельсон, В.А. Федоренко // “Машиностроение”, 1968, 272 с.

Напрям 11

ОРГАНІЗАЦІЯ БАЗ ДАНИХ І ЗНАНЬ

UDC 004:001.102:929

THE BIRTH OF THE INFORMATION AGE: PAUL OTLET

Yaroslav Melnyk[1], Lyudmila Pet'ko[2]

[1]Faculty of Mathematics, Informatics and Physics
Dragomanov National Pedagogical University, sity Kyiv,Ukraine
[2]Department of Foreign languages
Dragomanov National Pedagogical University, sity Kyiv, Ukraine

Annotation. *Described the activity by Paul Otlet, who formulated the concept of universal understanding the concept* "*document*" *and the general principles of the theory of documentation and became the founder of informatics as a science that comprehensively considers the issues of the theory of information and communication, as well as the organization of the processes of collecting, storing and information searching.Given Paul Otlet's achievements and inventions: The Universal Bibliographic Repertory, The Universal Decimal Classification (UDC), Mundaneum.*

Keywords: *Paul Otlet, document, bibliography, 'Treaties on Documentation', International Federation for Information and Documentation, Mundaneum.*

Анотація. *Описано діяльність Поля Отле́, який сформулював концепцію універсального розуміння поняття* "*документ" та загальні засади теорії документації і став фундатором інформатики як науки, що всебічно розглядає питання теорії інформації і комунікації, а також організації процесів збору, збереження і пошуку інформації. Згадано винаходи Поля Отле́: Універсальний бібліографічний каталог, Універсальна десяткова класифікація (УДК), Mundaneum.*

Ключові слова: *Поль Отле́, документ, бібліографія,* "*Трактат про документацію", Міжнародна федерація з інформації та документації, інформаційне сховище* "*Mundaneum".*

Paul Otlet, in full Paul-Marie-Ghislain Otlet, (born August 23, 1868, Brussels, Belgium – died December 10, 1944, Brussels). Paul was the oldest child in the family. His mother, Marie, died at the age of 24. He didn't go to school till the age of 11, his father hired tutors instead before entering secondary school at age 12. Father believed that classrooms were a stifling environment. Paul Otlet was educated at the Catholic University of Leuven and at the Université

Libre de Bruxelles, where he earned a law degree on 15 July 1890 [15] (Fig. 1, 2, 3), see the video [17].

Fig. 1. Paul Otlet, 1888

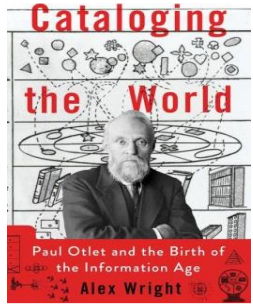


Fig. 2. Book by Alex Wright

Fig. 3. A collection

In 1891 he met the lawyer and future Nobel Peace Prize winner Henry La Fontaine (1913 in recognition of his contribution towards the peace movement) (Fig. 4), marking the beginning of a long-standing collaboration. In 1895 Otlet and La Fontaine established the International Institute of Bibliography and announced plans to create a Universal Bibliographic Repertory that would serve as a global clearinghouse for bibliographical data. Despite considerable resistance from other European librarians, they pressed forward with their plans, creating a headquarters for the institute and obtaining recognition and a small subsidy from the Belgian government [16].

Fig. 4. Henry La of index cards. Fontaine, 1916

They wrote to the creators of the classification and asked for permission to modify his system. And soon they began to work and created the Universal Decimal Classification. The same year they created a headquarters for the institute and obtaining recognition and a small subsidy from the Belgian government [3, 15, 27]. In 1895 Otlet and La Fontaine began the creation of a collection of index cards, meant to catalog facts (Fig. 3), that came to be known as the Universal Bibliographic Repertory. Soon this collection had more than 15 million entries [16, 15].

In the late 1800s and early 1900s Otlet pioneered the field of what we today call information science, but what he called documentation. A hundred years before the development of the Internet, Otlet used terms like web of knowledge, link, and knowledge network to describe his vision for a central repository of all human knowledge. It is fabulous introduction to pre-digital information classification. We can use this video in students' groups in the con-

ditions of university. It will give the students a visual appreciation of pre-digital classification and organization of information (Fig. 3) (see the video [1]).

In 1904, Otlet and La Fountaine began to publish their Universal Decimal Classification [19] (see the video [21]).

In 1906, Otlet and the chemist Robert Goldschmidt, had proposed "micro-fiche" as a standard format for a "micro-photographic book". Later on, they proposed a portable library of "micro-photographic books" [19].

In 1907, his father died, and family struggled to maintain all parts of the business. They created a company "Otlet Brothers", Paul became the president of the company [7].

In 1910 Otlet and La Fontaine established the Union of International Associations, a federation of 132 international organizations that would play an important role in the formation of the League of Nations [19, 27].

The same year they created plans about the "city of knowledge", which Otlet originally named the "Palais Mondial" ("World Palace"), that would serve as a central repository for the world's information [19, 27], (Fig. 5, 6).

Fig. 5. Otlet with his Mundaneum team

Fig. 6. Paul Otlet, Henri La Fontaine(left) and Mathilde Lhoest (his wife) outside the gates of Palais Mondial, in Cinquantenaire (Brussel), 1930

In 1913, La Fontaine won the Nobel Peace Prize (Fig. 4), and invested his winnings into Otlet and La Fontaine's bibliographic works, because they were suffering from lack of funding [16] (see the video [17]).

During World War I, Paul spent a lot of time trying to bring about piece. In 1914, he published a book, "La Fin de la Guerre" ("The End of War") that defined a "World Charter of Human Rights" as the basis for an international federation…

After the end of World War I, they asked the Belgian government to sponsor the project in hopes that it would form the intellectual bulwark of a new "World City" that would bolster Belgium's case for making Brussels the headquarters of the nascent League of Nations. The Belgian government granted space for the installation – which Otlet eventually began referring to as the Mundaneum [33, p. 59], see the video [14].

After failing in its bid for the League of Nations headquarters, the politically unstable Belgian government began to lose interest in the project, eventually closing it in 1934 [15, 16, 19].

Paul Otlet wrote about his theories of organizing information on a grand scale. His two major books were the Traité de documentation ("Treatise on Documentation") in 1934 (Fig. 7) and Monde: essai d'universalisme ("World: Essay on Universalism") in 1935, in which Otlet described his vision for a worldwide information network that in many ways presaged the creation of the World Wide Web more than 50 years later [19, 27] (Fig. 8). Otlet's primarily female staff answered information requests by hand. Without the digital luxury of keyword searches, a single query could take painstaking hours, even days, of sifting through the elaborate index card catalog (Fig. 9), see the video [13].

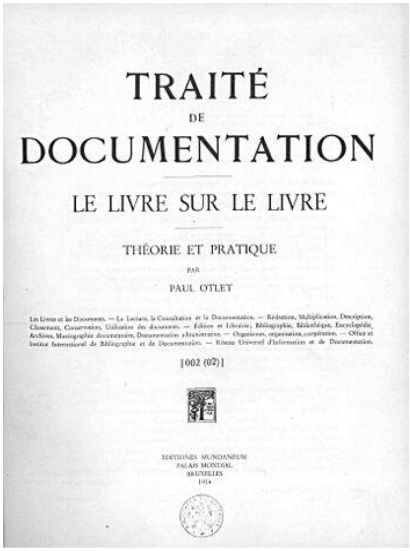


Fig. 7. Traité de documentation, 1934

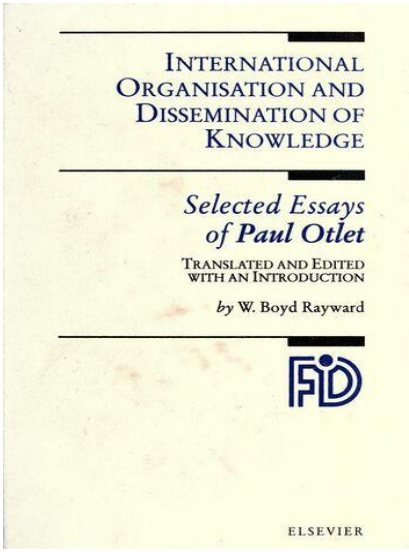


Fig. 8. Selected Essays by P. Otlet, 1990

Fig. 9. Otlet's primarily female staff

The library catalog card is one form of the popular 3×5 index card that served as a filing system for a multitude of purposes for over two hundred years (Fig. 10). The original purpose of the index card and its subsequent development represented the early stages of information theory and practice. Additionally, as becomes clear below, without the index card as the first functional system for organizing complex categories, subcategories and cross-references, studies in the natural sciences would have never gotten off the ground [5].

Fig. 10. Printed library catalog card

The index card became the indispensable tool for both organizing and comprehending the expansion of human knowledge at every level (Fig. 10). Along with several important intermediary steps, the ideas that began with index cards eventually led to relational databases, document management systems, hyperlinks and the World Wide Web.

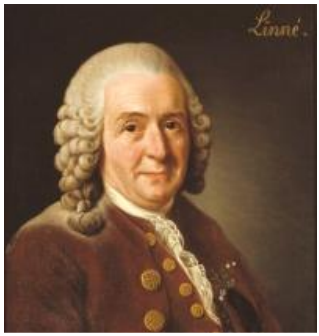


Fig. 11. Carl Linnaeus

The Swedish naturalist and physician Carl Linnaeus (1707–1778) is recognized as the creator of the index card (Fig. 11). Linnaeus used the cards to develop his system of organizing and naming the species of all living things. Linnaean taxonomy is based on a hierarchy (kingdom, phylum, class, order, family, genus, species) and binomial species naming (homo erectus, tyrannosaurus rex, etc.). He published the first edition of his universal conventions in a small pamphlet

called "The System of Nature" in 1735 [5] (Fig. 12).

Fig. 12. Linnaeus' "*The System of Nature*"

While index cards continued to be used in Europe, an important step forward in information management was made in the US by Melvil Dewey (1851–1931), the creator of the well-known Dewey Decimal System (or Dewey Decimal Classification, DDC). Used by libraries for the cataloging of books since 1876, the DDC was based on index cards and introduced the concepts of "relative location" and "relative index" to bibliography [5] (Fig. 13, 14).

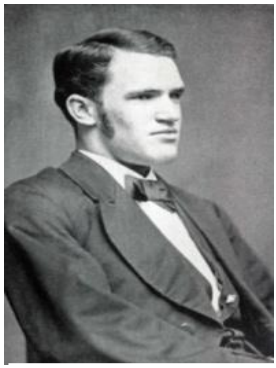


Fig. 13. Melvil Dewey

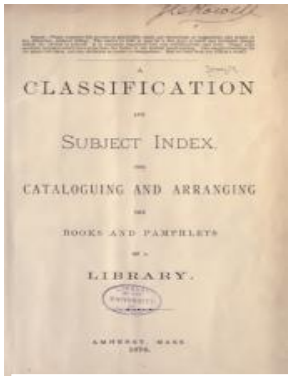


Fig. 14. The 1st edition

By the end of the nineteenth century the Dewey classification system and his 3×5 card catalog were being used in nearly every school and public library in the US. The basic concept was that any member of society could walk into a library anywhere in the country, go to the card catalog and be able to locate the information they were looking for [35].

While Dewey's classification system became the standard in US libraries, others were working on bibliographic cataloging ideas, especially in Europe. In 1895, the Belgians Paul Otlet (1868–1944) and Henri La Fontaine founded the International Institute of Bibliography (IIB) and began working on something they called the Universal Bibliographic Repertory (UBR), based on index cards. Funded by the Belgian government, the UBR involved the collection of books, articles, photographs and other documents in order to create a one-of-a-kind international index.

Otlet and La Fontaine made an important conceptual breakthrough over Dewey's approach. In particular, they conceived of a complex multidimensional indexing system that would allow for more deeply defined subject categories and cross-referencing of related topics: the content of bibliographic collections needed to be separated from their form and that a "universal" classification system needed to be created that included new media and information sources (magazines, photographs, scientific papers, audio recordings, etc.) and moved away from the exclusive focus on the location of books on library shelves (Fig. 15), see the video [18].

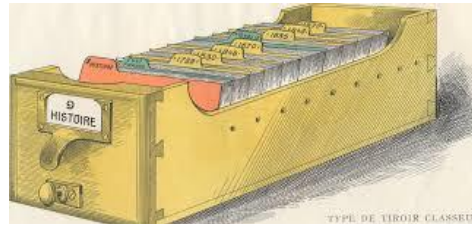


Fig. 15. Otlet's ingenious index card system

The UDC (the Universal Decimal Classification) by Otlet and La Fontaine extended Dewey's cataloging expressions to include symbols (equal sign, plus sign, colon, quotation marks and parenthesis) for the purpose of establishing "links" between multiple topics. This was a very significant breakthrough that reflected the enormous growth of information taking place at the end of the nineteenth century. By 1900, the UBR had more than 3 million entries on index cards and was supported by more than 300 IIB members from dozens of countries [5, 31] (Fig. 16, 17).

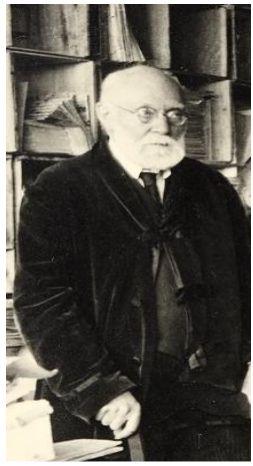


Fig. 16. P. Otlet. of Dewey's bibliographic classification system

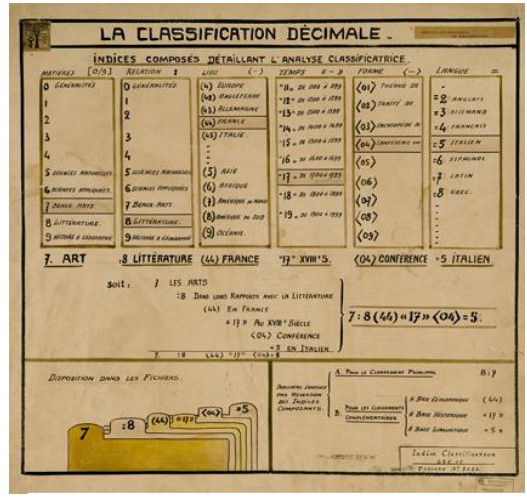


Fig. 17. An explanatory schema of the UDC index formation in French, 1920

Fig. 18. is an illustration of the path of information from a book (A), via the Universal Bibliographic Repertory (RBU) (B), and from there to classification in individual libraries catalogues (C) and shelves (D). At the centre of it is an index card, carrying the important information, plus decimal code [29].

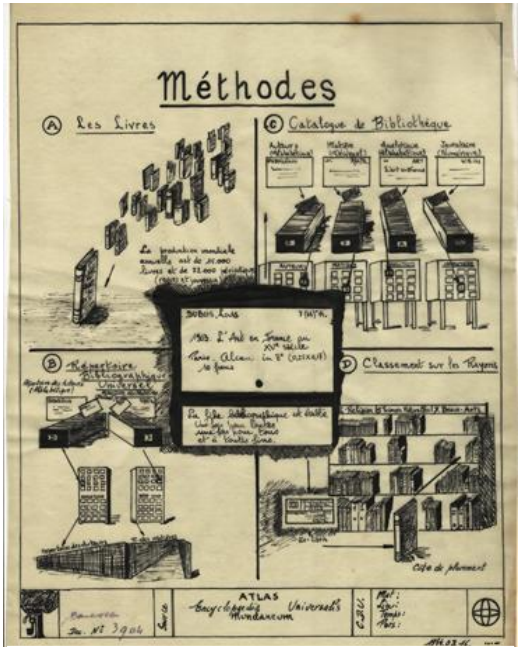


Fig. 18. Method

Within a year's time, the two men and a team of volunteers had gathered 400,000 entries recording books, speeches, sheet music, medical journals, museum pieces, even newspaper and poster advertisements. By 1896, Otlet opened the doors on a mail-in research service: users would pay a small fee to request information on any number of topics, while staff would copy relevant note-cards, and send them back by delivery service. In essence, Otlet and Fontaine were on their way to turning their bibliography into a steampunk version of Wikipedia [34], see the video [20].

Over the next decade, as their bibliography swelled to millions of entries, simply organizing data into broad categories was not enough. Otlet sought to create a classification system and subsequent search mechanism that could intersect several subjects, and in 1904 he published a more polished version of his Universal Decimal Classification system (Fig. 15, 18), see the video [6]. Basically it was a hierarchical card catalog system, sort of like the Dewey Decimal System on 'roids'. To handle retrieval, Otlet devised an algebraic algorithm based on category and subcategory identification numbers, complete with a set of relational operators. He had created his own analog search engine almost 90 years before Archie was developed… The jewel of Otlet's vision for the new "global village" would be the Mundaneum, a vast repository open to the public,

that would house the now 12 million 3×5 index cards and accompanying filing system [34] (Fig. 19, 20), see the video [45].

Fig. 19. A Mundaneum media room

Fig. 20. A reproduction of Otlet's original Mondotheque desk

In 1910, Otlet and La Fontaine shifted their attention to the establishment of the Mundaneum in Mons, Belgium. Again with government support, the aim of this institution was to bring together all of the world's knowledge in a single UDC index and by 1924, the Mundaneum contained 18 million index cards housed in 15,000 catalog drawers (Fig. 9). But during the Depression and lead up to World War II, Paul Otlet realized that further management of the card catalog had become impractical. He began to consider more advanced technologies – such as photomechanical recording systems and even ideas for electronic information sharing – to fulfill his vision [35], see the video [2].

A massive center for documentation and communication, the Mundaneum aimed at hosting all human knowledge and facilitating worldwide sharing through the connection of universities, governmental institutions, and individuals. It was also meant to embody the idea of promoting peace among nations. The information would have been classified on indexing cards under the Universal Decimal Classification, developed by Otlet, and the institutions would have merged shelves

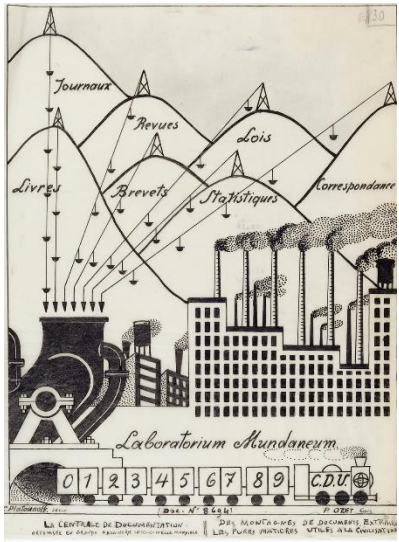


Fig. 21. Plan of the Mundaneum

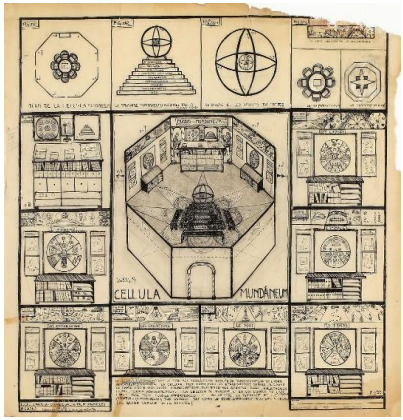


Fig. 22. The center of the Mundaneum (1935)

and printed documentation with screens and telephones allowing users from all over the world to ask questions (see the video [28]). A first version of the project was indeed realized and hosted in 150 rooms of the Palais du Cinquantenaire in Mons, a location offered by the Belgian government [4, 30], see the video [12], (Fig. 23–25).

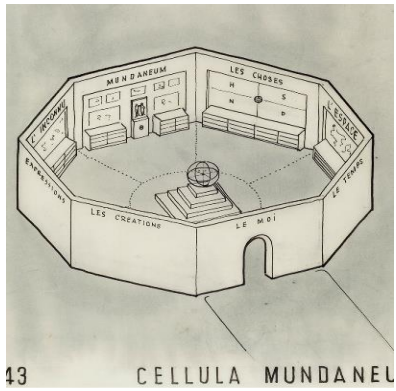


Fig. 23. Laboratorium Mundaneum: Powerhouse of Documentation. C. Platounoff on commission of Otlet (28 Dec 1937)

Below we present a Video game: *Mundaneum Web 1895 in the Mundaneum Museum* (Fig. 26, 27) located in Mons in a magnificent Art Deco building (Belgium) [30]. The trilingual game Mundaneum Web 1895 on tablet provides a journey through the museum: our very founder, Paul Otlet, rediscovers a new youthfulness and guides visitors Upon finding each featured location or object in the museum, little games are unlocked at geolocated landmarks. These fun and instructive challenges allow to learn a little more about the founders of the Mundaneum, Paul Otlet and Henri La Fontaine, and their project: to gather together all of the world's

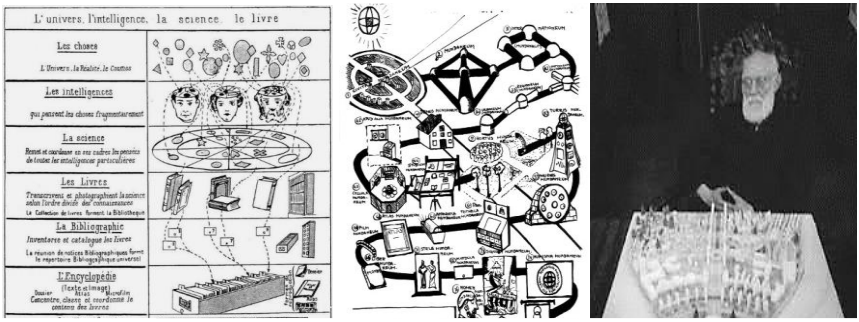


Fig. 24. Paul Otlet: Universe, Intelligence, Science, Book. Species Mundaneum, 16 Jan 1937

Fig. 26. Photograph of Otlet sitting behind a scale model of the Cité Mondiale designed by the Belgian modernist architect Stanislas Jasinski in 1941

knowledge. The various purposes of the game:

– To discover the museum space of the Mundaneum.

– To learn who its founders are and how their inventions worked (sheet, archive, ...).

– To get the best score possible [32].

The Mundaneum consists of a ground floor overlooked by two modular floors on demand, a glass conference room overlooking a brand new courtyard at the back of the museum and a terrace. The Mundaneum is today a center of private archives and a museum space recognized by the Wallonia Federation. In the basement of the building are 6 kilometers of archives which are made available to researchers around the world. The museum space hosts a permanent exhibition and major temporary exhibitions all year round recognized internationally by the UNESCO World Memory Program and the European Heritage Label [9].

Fig. 27. The Mundaneum Museum in Mons (Belgium)

In brief. Otlet's monumental collection was predicated not on ownership but on access and sharing – while amassing it, he kept devising increasingly ambitious schemes for enabling universal access, fostering peaceful relations between nations, and democratizing human knowledge through a global information network he called the "Mundaneum" – a concept partway between Voltaire's Republic of Letters, Marshall McLuhan's "global village", and the übermind of the future [26].

Otlet was more than a bibliographer, encyclopaedist, and founding father of the discipline of "documentation". He was also a sociologist, an internationalist, and an untiring promoter of his conception of "universalism" or "mondial-

isme", of the Mundaneum and the Cité Mondiale [33, p. 58] (Fig. 28), see the video [10].

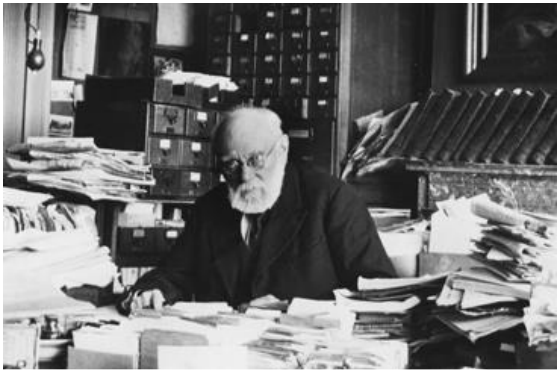


Fig. 28. Paul Otlet in his office in the 1930 s

While Otlet did not by any stretch of the imagination "invent" the Internet – working as he did in an age before digital computers, magnetic storage, or packet-switching networks – nonetheless his vision looks nothing short of prophetic. In Otlet's day, microfilm may have qualified as the most advanced information storage technology, and the closest thing anyone had ever seen to a database was a drawer full of index cards. Yet despite these analog limitations, he envisioned a global network of interconnected institutions that would alter the flow of information around the world, and in the process lead to profound social, cultural, and political transformations [26].

And while he might well have been flummoxed by the anything-goes ethos of present-day social networking sites like Facebook or Twitter, he also imagined a system that allowed groups of individuals to take part in collaborative experiences like lectures, opera performances, or scholarly meetings, where they might "applaud" or "give ovations" [26].

In summary. *First dimension* in Otlet's work that may be called visionary is the way he approached "information" as consisting of "morselized", quantifiable, and coded units or pieces of information. Otlet's idea to record information in separate chunks or units according to the "monographic principle" foreshadowed, in a certain sense, the present tendency to conceive of information as detachable and manipulable units or atoms of content, whose retrieveability has become more important than the information itself [33, p. 61].

A second level on which Otlet's utopia still resonates with our present times is the similarity between his vision of a collective, mechanical brain, on the one hand, and the emergence of a global brain that some theoreticians and philosophers observe to be emerging today. From the "collective, mechanical brain" of Otlet, the "superorganism" of Herbert Spencer (1820–1903), the "world brain" of H. G. Wells (1866–1946), the "noosphere" of the French philosopher and Jesuit priest Pierre Teilhard de Chardin (1881–1955), different scholars have tried to conceptualize in terms of evolutionary, humanist, and organicist models what seems to be an emergent cognitive [33, p. 61].

Thirdly, Otlet's ideas about the Cité Mondiale (Fig. 26) (see the video [8]) resonate with some of the trends that characterize current European planning politics. Otlet's idealist activism for the location of international organization in one world capital seems outdated in that the capital of Europe is today in fact a superposition of the three official capitals (Luxembourg, Strasbourg and Brussels), a network of cities hosting European Agencies, and a rotating European Capital of Culture. Yet, even within this new paradigm of a polycentric capital, the process of centre formation within the European Union continues, as well as the competition for that matter between political, cultural, and economic centres [33, p. 61].

Otlet's idea of collective intelligence working toward a common good presaged modern concepts like crowdsourcing and "cognitive surplus" as well as initiatives like Singularity University [26].

References

1. Biography of Paul Otlet. Documentary in English and French. Produced for Dutch television in 1998. URL: https://www.youtube.com/watch?v=KLX2OGw31Oo

2. Boyd Rayward talks about the Mundaneum and Paul Otlet. URL: https://www.youtube.com/watch?v=jIFiubSPC2Q *in English*

3. Buckland Michael. Paul Otlet, Pioneer of Information Management, biography of Paul Otlet for the School of Information at UC Berkeley, n.d. URL: https://people.ischool.berkeley.edu/~buckland/otlet.html

4. Fabrizi Mariabruna. The Shape of Knowledge: The Mundaneum by Paul Otlet and Henri La Fontaine. SOCKS. May 5, 2019. URL: https://socks-studio.com/2019/05/05/the-shape-of-knowledge-the-mundaneum-by-paul-otlet-and-henri-la-fontaine/

5. How the index card launched the information age. Multimediaman. September 30, 2016. URL: https://multimediaman.blog/2016/09/30/how-the-index-card-launched-the-information-age/

6. Internet – Paul Otlet. URL: https://www.youtube.com/watch?v=qwRN5m64I7Y&t=3s

7. Mundaneum. URL: https://en.wikipedia.org/wiki/Mundaneum

8. Mundaneum. URL: https://www.youtube.com/watch?v=sQGccmVsEkU

9. Mundaneum. Archives Center of Wallonia-Brussels Federation and Museum Space. URL: http://lieu.mundaneum.org/en/today

10. Mundaneum & Google. URL: https://www.youtube.com/watch?v=DvLKr8Go3i A&t=2s

11. Mundaneum – L'archive à l'ère du numérique. Access mode: https://www.youtube.com/watch?v=SoAVVkj-xk8

12. Mundaneum loop.URL: https://www.youtube.com/watch?v=Ywz5tB2QUww *in English*

13. Mundaneum – Petite histoire d'une grande idée: Contexte FR. URL: https://www.youtube.com/watch?v=sWv7FSirk14 *in French*

14. Mundaneum – Small history of a big idea. Context EN. URL: https://www.youtube.com/watch?v=flBcebZ7MCo&t=22s

15. Paul Otlet. URL: https://en.wikipedia.org/wiki/Paul_Otlet

16. Paul Otlet. URL: https://www.britannica.com/biography/Paul-Otlet

17. Paul Otlet. URL: https://www.youtube.com/watch?v=r6IMRtAYbHQ

18. Paul Otlet at the London Science Museum (Information age gallery). URL: https://www.youtube.com/watch?v=mVOxcZn08kA *in English*

19. Paul Otlet biograghy, history and inventions. URL: https://history-computer.com/paul-otlet-biography-history-and-inventions/

20. Paul Otlet, co-fondateur du Mundaneum, l'inventeur d'internet ?.URL: https://www.youtube.com/watch?v=N_oLH0B9Sac *With English subtitles*

21. Paul Otlet et le Traité de documentation.URL: https://www.youtube.com/watch?v=S4grwR6BDgQ

22. Pet'ko Lyudmila. Developing students' creativity in conditions of university // Research: tendencies and prospects: Collection of scientific articles. – Editorial Arane, S.A. de C.V., Mexico City, Mexico, 2017. P. 272–276.

23. Pet'ko L. Multicultural upbringing of students and the formation of professionally oriented foreign language teaching environment // Perspectives of research and development: Collection of scientific articles. – SAUL Publishing Ltd, Dublin, Ireland, 2017. P. 164–170.

24. Pet'ko L. V. Teaching methods and the formation of professionally oriented foreign language learning environment in conditions of university. *Intellectual Archive.* Toronto: Shiny Word Corp., Canada.2016. Vol. 5. No. 4 (July/August). Pp. 73–87.

25. Pet'ko L. V. Unity of teaching and upbringing in the formation of professionally oriented foreign language teaching environment / L.V.Pet'ko // Science and practice: Collection of scientific articles. – Thorpe Bowker. Melbourne, Australia, 2016. P. 303–307. URL: http://enpuir.npu.edu.ua/handle/123456789/11892

26. Popova M. The Birth of the Information Age: How Paul Otlet's Vision for Cataloging and Connecting Humanity Shaped Our World. *Themarginalian*. URL: https://www.themarginalian.org/2014/06/09/paul-otlet-alex-wright/

27. Rayward W. B. The case of Paul Otlet, pioneer of information science, internationalist, visionary: reflections on biography. *Journal of Librarianship and Information Science*, Vol. 23. Issue 3, pp. 135–145. URL: https://doi.org/10.1177/096100069102300303

28. The Man Who Wanted to Classify the World. Documentary, 2002. Directed by Francoise Levie. URL: https://letterboxd.com/film/the-man-who-wanted-to-classify-the-world/

29. The Noble History of The Index Card: Universal Decimal Classification. URL: https://www.inventingeurope.eu/knowledge/the-noble-history-of-the-index-card-universal-decimal-classification

30. Towards the information age. URL: https://artsandculture.google.com/story/awXRg4ha0wAA8A

31. Universal Decimal Classification. URL: https://en.wikipedia.org/wiki/ Universal_Decimal_Classification

32. Video game: Mundaneum Web 1895. url: https://www.visitmons.co.uk/see-do/top-sights/10-top-reasons-to-fall-in-love-with-mons/unesco/mundaneum/video-game-mundaneum-web-1895

33. Wouter van Acker. Hubris or Utopia? Megalomania and Imagination in the work of Paul Otlet. *Cahiers de la documentation – Bladen voor documentatie*. 2012. No. 2. Pp. 58–66. URL: https://www.abd-bvd.be/wp-content/uploads/2012-2_Van_Acker.pdf

34. The first internet hero was paul otlet and his steampunk wikipedia. url: https://www.inverse.com/article/7549-the-first-internet-hero-was-paul-otlet-and-his-steampunk-wikipedia

УДК 004

ЗАСТОСУВАННЯ АДАПТИВНИХ СЕМАНТИЧНИХ АНАЛІЗАТОРІВ ПРИ ДИНАМІЧНІЙ ОБРОБЦІ ВЕЛИКИХ ОБСЯГІВ ТЕКСТОВОЇ ІНФОРМАЦІЇ

Руслан Аль Хадж

Національний університет "Одеська політехніка" м. Одеса, Україна

Анотація. *Розглянуто сучасний метод аналізу тексту для автоматичного визначення авторства який заснований на синтаксичної інформації та на використанні визначника меж речень і абзаців Sentence and Chunk Boundaries Detector – SCBD у вихідному тексті для отримання стильових маркерів меж слів і пропозицій.*

Ключові слова: *аналіз тексту, інтелектуальна система, метод SCBD.*

Abstract. *A modern method of text analysis for automatic determination of authorship is considered, which is based on syntactic information and the use of the Sentence and Chunk Boundaries Detector – SCBD in the source text to obtain stylistic markers of word and sentence boundaries.*

Keywords: *text analysis, intelligent system, SCBD method.*

Комп'ютерний аналіз текстів – перспектива, яка швидко розвивається в області штучного інтелекту. Одна з ключових задач комп'ютерного аналізу полягає в побудові такого структурованого подання тексту, до якого можна застосовувати методи й алгоритми рішення прикладних задач.

Існує значна кількість різновидів методів як синтаксичного, так і семантичного аналізу, які засновані на різних моделях синтаксичної структури пропозиції та різному розумінні семантики. Існуючі системи аналізу та моделювання текстів, до яких належать інформаційно-пошукові та інформаційно-аналітичні системи різного спрямування, які включають розгляд і вирішення таких завдань як класифікація документів за тематичними категоріями, ідентифікація авторства, виявлення некоректних запозичень, плагіату, моделювання уявлень знань про предметної області та змісту текстів, класифікація і фільтрація документів за заданими запитами і багато інших.

Розвиток моделей та методів аналізу та обробки текстових даних тісним чином пов'язано з розвитком інформаційних технологій, що робить можливим використання таких методів у побудові інтелектуальних інформаційних систем, експертних систем і баз знань.

Інтелектуальну систему можна визначити як біологічну, штучну або формальну систему, яка виявляє здатність до цілеспрямованої поведінки. Останнє включає властивості спілкування, накопичення знань, прийняття рішень, навчання, адаптації тощо. Однією зі сфер застосування автоматизованих аналітичних алгоритмів, може бути рішення класів завдань, які

або не можуть бути вирішені людиною за реальний час, або ж їх рішення вимагає автоматизованої підтримки, або ж їх рішення дає результати, порівнянні по інформативності з рішеннями людини.

Метод автоматичного визначення авторства на основі синтаксичної інформації заснований на використанні визначника меж речень і абзаців (Sentence and Chunk Boundaries Detector – SCBD) у вихідному тексті для отримання стильових маркерів меж слів і пропозицій – є найбільш актуальним методом для інтеграції до сучасного програмного рішення.

SCBD поділяє текст на речення, а потім визначає межі внутрішніх речових виразів, таких як іменники, прийменники та інші (рис. 1). На основі результатів програмної обробки обчислюються наступні оцінки:

− на рівні символів: кількість речень, кількість слів, число знаків пунктуації;

− на рівні виразів: число іменників, прийменників, тощо.

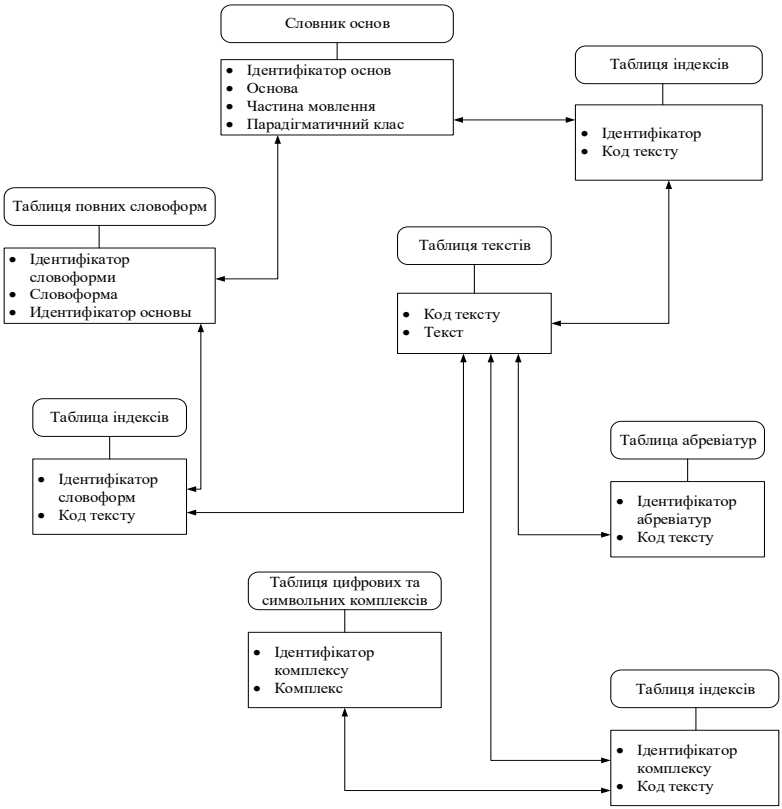


Рисунок 1 – Схема розподілу складових компонентів тексту

Крім того, використовуються такі параметри, що оцінюють процес обробки тексту програмою: кількість слів, що залишилися неаналізованою після кожного проходу, число ключових слів, кількість невідповідних для класифікації слів.

Метод на основі SCBD виробляє множинні проходи по тексту. Кожен прохід аналізує частину пропозицій в залежності від результатів попереднього проходу. Решта зберігається для подальшого аналізу. Складність розбору збільшується при кожному проході.

Відсоток слів, які залишилися непроаналізованими після кожного проходу, є важливим стилістичним фактором, який відображає семантичну складність тексту.

Інформаційні джерела

1. Литвиненко О. Є. Інженерно-лінгвістичні принципи аналізу текстів / О. Є. Литвиненко, Д. А. Бурко // Наукоємні технології. – 2009. – Том 3, № 3. – С. 60–62. – DOI : 10.18372/2310-5461.3.5130

2. Заболеева-Зотова А. В. Латентный семантический анализ: новые решения в Internet / А. В. Заболеева-Зотова, А. Ю. Пастухов, П. В. Сердюков, Н. А. Козлова, С. А. Чернов // Информационные технологии. – 2001. – № 6. – С. 67–82.

УДК 004.67

ОБРОБКА ВЕЛИКИХ ДАНИХ ДЛЯ ПРОГНОЗУВАННЯ ОБСЯГУ АКЦІЙ ЗА ДОПОМОГОЮ ІНСТРУМЕНТІВ DEEP LEARNING

Є. Медяник

Національний Університет “Одеська Політехніка”, м. Одеса,Україна

Анотація*. У епоху великих даних глибоке навчання для прогнозування обсягу кількості акцій, що торгуються в межах певної акції, індексу чи іншої інвестиції за певний проміжок часу. цін та тенденцій фондового ринку стало ще більш популярним, ніж раніше. Для наведення прикладу обробки даних за допомогою технологій Deep Learning було обрано дані фондового ринку 2021 року акції компанії Tesla.Пропоноване рішення обробки та візуалізації даних є комплексним, оскільки включає в себе попередню обробку фондового ринку набору даних, Після проведення всеобічної оцінки використовуваних моделей машинного навчання можна дійти висновку, що запропоноване рішення може бути використано при обробці інших наборів даних за умови їх попередньої класифікаці параметрів.*

Ключові слова*: Deep Learning,Stock market forecasting, Keras, Tensorflow, візуалізація даних.*

Abstract*. In the age of Big Data, Deep Learning is used to predict the volume of the number of stocks traded in a particular stock, index, or other investment over a given period of time. prices and stock market trends have become even more popular than before. To give an example of data processing using Deep Learning technologies, we selected data from the 2021 stock market of Tesla shares.The proposed solution for data processing and visualization is complex, since it involves preprocessing the stock market data set, after conducting a comprehensive assessment of the machine learning models used, it can be concluded that the proposed solution can be used for processing other data sets, provided that their parameters are pre-classified.*

Keywords*: Deep Learning,Stock market forecasting, Keras, Tensorflow,data visualisation.*

Фондовий ринок – одна з основних областей, якою займаються інвестори, тому прогнозування цінового тренду на фондовому ринку завжди є цікавою темою для дослідників як з фінансової, так і з технічних областей. У цьому дослідженні мета полягає в тому, щоб побудувати сучасну модель прогнозування цінового тренда, яка фокусується на короткостроковому прогнозуванні обсягу цінового тренда. Після значного розвитку методів штучного інтелекту в останні роки багато запропонованих рішень було опробовано для того щоб об'єданти Машинне навчання і методи глибокого навчання, засновані на попередніх підходах, а потім пропонували нові метрики, які служать функціями навчання, Цей тип попередніх робіт відноситься до області розробки об'єктів і може розглядатися як джерело натхнення для ідей розширення функцій у нашому дослідженні. Одним із таких підходів є імплементування згорткової нейронної мережі(CNN), а також модель на основі нейронної мережі з тривалою короткочасною пам'яттю (LSTM) для аналізу різних кількісних стратегій на фондових ринках. CNN зокрема служить для стратегії вибору акцій, автоматично витягує характеристики на основі кількісних даних, потім слід LSTM, щоб зберегти характеристики часових рядів для підвищення прибутку. Проте для початку аналізу набору історичних даних необхідно дослідити як кожен з параметрів, що впливає на обсяг цінових акцій тієї чи іншої фірми для цього використовуючи мову програмування Python та засобу візуалізації бібліотеки matplotlib виконаємо аналіз змін кожного з параметрів з плином часу для подальшого аналізу та чистки даних які можуть вплинути на прогнозування цільового параметру при проєктуванні нейронної мережі.

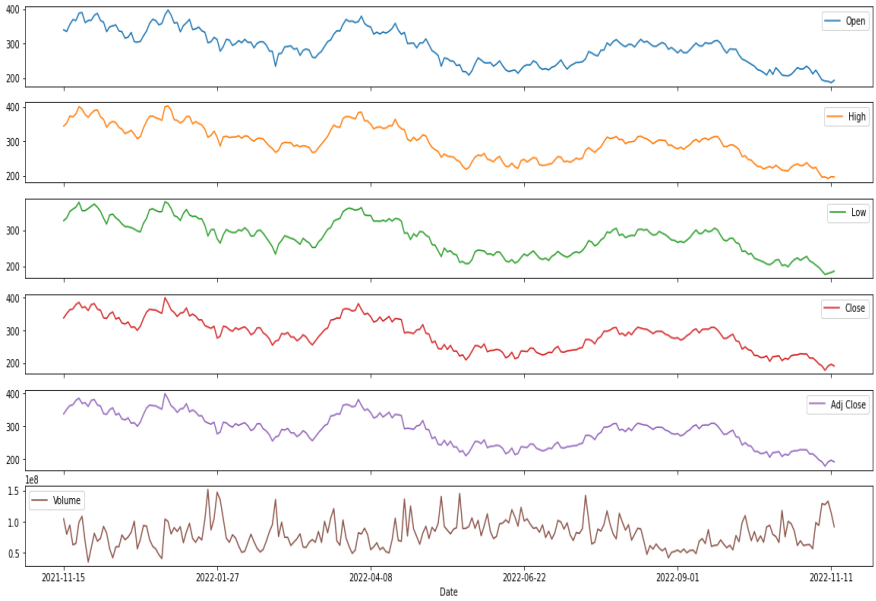


Рисунок 1 – Зміни параметрів набору даних з плином часу

Під час обчислень було використано розподілення на навчальні, валідаційні та тестові набори відповідно на 70%, 20% та 10%. Необхідно зазначити, що дані не перемішуються випадковим чином перед поділом їх на тестові та навчальні набори даниї. Це відбувається з двох причин: це гарантує, що розподіл даних на вікна послідовних зразків все ще можливий, а також це гарантує, що результати валідації або тестування будуть більш реалістичними, оскільки оцінюються на основі даних, зібраних після навчання моделі. Важливо масштабувати об'єкти перед навчанням нейронної мережі. Нормалізація-поширений спосіб виконання такого масштабування, воно полягає у тому щоб відняти середнє значення і розділити на стандартне відхилення кожної ознаки.Середнє значення та стандартне відхилення слід обчислювати лише за допомогою навчальних даних, щоб моделі не мали доступу до значень у наборах перевірки та тестів. Можна також стверджувати, що модель не повинна мати доступу до майбутніх значень у навчальному наборі під час навчання, і що ця нормалізація повинна виконуватися за допомогою середніх значень. Моделі для нейронної мережі цього рішення будуть збирати набір прогнозів на основі вікна послідовних зразків з даних. Основними

функціями вікон введення є : Ширина (кількість тимчасових кроків) вікон введення і написів та часовий зсув між ними. Які об’єкти використовуються як вхідні дані, мітки або обидва. Виконавши всі зазначені вимоги можна побачити результати роботи моделі навчання побудованної нейронною мережою:

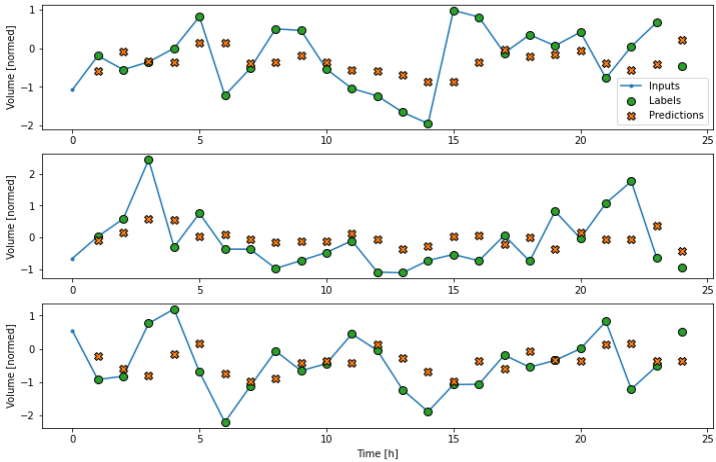


Рисунок 2 – Побудова графіку передбачуваного обсягу акцій компанії у майбутньому

Висновки. У результаті проведення аналізу даних та їхньої обробки за допомогою технологій машиного,глибокого навчання і подальшої побудови графіків можна дійти висновку, що запропонована техніка обробки даних може бути використана у обробці та подальшому прогнозуванні цін та обсягів акції на фондовому ринку у майбутньому.

Інформаційні джерела

1. Shen J, Shafq MO. Deep learning convolutional neural networks with dropout–a parallel approach. ICMLA. 2018;2018:572–7.

2. Shen J, Shafq MO. Learning mobile application usage–a deep learning approach. ICMLA. 2019;2019:287–92.

3. Shih D. A study of early warning system in volume burst risk assessment of stock with Big Data platform. In: 2019 IEEE 4th international conference on cloud computing and big data analysis (ICCCBDA). 2019. pp. 244–8.

4. Sirignano J, Cont R. Universal features of price formation in fnancial markets: perspectives from deep learning. Ssrn. 2018. https://doi.org/10.2139/ ssrn. 3141294.

УДК 004.65

ДОСЛІДЖЕННЯ ПРОБЛЕМ ОБРОБКИ НЕСТРУКТУРОВАНИХ ДАНИХ

Олег Стасьо, Назарій Бурак

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Розвиток інформаційних технологій та інтеграція у щоденне життя суспільства призвів до стрімкої генерації великої кількості даних. Аналіз останніх років демонструє радикальні зміни у принципах розуміння даних та можливостей їх використання. Виникнення стану* "*інформаційного вибуху*" *призвело до появи перевантаження інформаційно-комунікаційних мереж потоками даних (великих даних), що, своєю чергою, ускладнило процес обробки та аналізу.*

Ключові слова: *дані, технологія, модель, Big Data, якість.*

Abstract. *The development of information technology and its integration into the daily life of society has led to the rapid generation of a large amount of data. The analysis of recent years demonstrates radical changes in the principles of data understanding and the possibilities of its use. The* "*information explosion*" *state led to the appearance of overloading of information and communication networks with data flows (big data), which, in turn, complicated the process of processing and analysis.*

Keywords: *data, technology, model, Big Data, quality.*

Еволюція технологій відбувається швидкими темпами. Така ситуація формує стан, коли усе та усі навкруги свідомо чи несвідомо генерують дані тим чи іншим способом. Різні сфери виробляють дані з безпрецедентною швидкістю, зокрема це стосується сфер охорони здоров'я, дані соціальних медіа, дані датчиків, телефонів, серверних журналів, фондовий ринок, і т. д. Ці процеси призводить до формування великого обсягу, високої швидкості та різноманітності даних, що призвело до появи терміну "великі дані".

В аналітиці великих даних існує два типи даних: структуровані та неструктуровані дані. У той час як структуровані дані стосуються впорядкованої інформації в базі даних, неструктуровані дані навпаки, це необроблені дані, які нелегко класифікувати в існуючих базах даних, і вони доступні в різних форматах. Її часто називають інформацією довільної форми, оскільки вона доступна в різних форматах.

Більшість традиційних методів аналізу демонструють високу ефективність за умови, що усі вхідні дані складаються з єдиного набору атрибутів і збиралися за єдиною схемою вимірювання, тобто мають єдину структуру. Натомість великі дані наповнені різнорідними, неузгодженими, нев-

порядкованими та неструктурованими даними, оскільки інформація щодо певного випадку може отримуватись з різних джерел. Саме тому виникає потреба у розробленні засобів та методів видобування знань із тих даних, що генеруються в процесі діяльності людства та можуть бути корисними для подальшого використання.

Актуальність проблеми також загострюється через стрімке поширення великих даних у сфері безпеки життєдіяльності, зокрема в системі захисту населення від надзвичайних ситуацій. У діяльності оперативно-рятувальних служб щоденно відбувається обробка великих обсягів інформаційних ресурсів різного походження та, із наперед не відомими моделями даних, оскільки дані про події надходять з різних джерел. Необхідність аналітики таких даних визначається потребою у прискореному зборі і накопиченні великих масивів емпіричних даних з різноманітних джерел, видобуванні цінного та корисного за змістом і зручного за формою контенту та формуванні знань і ресурсів для прийняття оперативних управлінських рішень при прогнозуванні, попередженні чи ліквідації надзвичайних ситуацій. Така неструктурованість та різнорідність даних створює певні проблеми для їх обробки та формування знань, що формує потребу в нових, більш ефективних методах аналізу та засобах, які забезпечуватимуть автоматизований процес збору, обробки та видобування цінної інформації з потоків великих даних.

Бурхливий розвиток Big Data генерує велику кількість актуального неструктурованого контенту, а його обробка звичними методами не забезпечує необхідної якості та швидкості. Саме тому, постає питання розробки сучасних систем автоматичної обробки та класифікації великих об'ємів даних.

Процес структуризації неструктурованих даних пов'язаний із величезною кількістю проблем. З поміж усіх, виділяють наступні:

1. Відсутність можливості аналізу за допомогою звичайних систем

Неструктуровані дані не можна аналізувати за допомогою поточних баз даних, оскільки більшість аналітичних баз даних призначені для структурованих даних і не обладнані для неструктурованих даних. Тому, актуальним залишається питання розробки нові методи пошуку, вилучення, організації, аналізу та зберігання даних.

2. Високі темпи масштабованості неструктурованих даних

Рівень росту великих даних здійснюється за експоненційною залежністю. Згідно існуючих досліджень, у 2053 році неструктуровані дані становитимуть понад 93% від усіх даних, які перебуватимуть в обробці. Такий великий обсяг інформації може призвести до неспроможності існуючих методів обробки забезпечити якісний аналізу такого типу даних, оскільки чим більший набір даних, тим складніше їх зберігати та опрацьовувати у спосіб, який є своєчасним та ефективним. Для вирішення цією проблеми

необхідно розробити системи, які “розумітимуть” та “вмітимуть” ефективно обробляти великі обсяги даних.

3. Актуальність

Переконатися, що дані релевантні, – одна з найбільших проблем, коли справа доходить до аналізу неструктурованих даних. Моделі аналізу даних не можуть розрізняти причинно-наслідковий зв’язок і кореляцію. Якщо моделі аналітики даних бачать частий зв’язок між двома різними змінними, вони нададуть цьому зв’язку значну вагу, навіть якщо дані, які містяться в ньому не є цінними. Такий підхід має великий вплив на достовірність і точність висновків.

4. Не всі неструктуровані дані мають високу якість

Загальна якість неструктурованих даних є значною мірою неоднорідна. Відсутність послідовності в якості виникає через не точність даних. Велика частина даних, яка отримана від суспільства може бути недостовірною, або частково достовірною, оскільки людям притаманно перебільшувати, спотворювати або бути нечесними щодо своєї інформації. Якщо організації внесе цю інформацію у свої аналітичні системи для подальшого опрацювання, вони не отримають точних висновків, що може зашкодити та знизити якість прийнятих рішень.

Таким чином, актуальності набуває науково-прикладна задача побудови багаторівневої високоорганізованої інформаційної технології підтримки прийняття рішень на основі розроблених моделей та методів аналізу неструктурованих даних.

Інформаційні джерела

1. Cetera, W., Gogołek, W., Żołnierski, A. et al. Potential for the use of large unstructured data resources by public innovation support institutions. J Big Data 9, 46 (2022). [Електронний ресурс]. – Доступний з https://doi.org/10.1186/s40537-022-00610-6

2. Grimes S. Unstructured Data and the 80 Percent Rule, 2008, Clarabridge, Bridgepoints. [Електронний ресурс]. – Доступний з http://breakthroughanalysis.com /2008/08/01/unstructured-data-and-the80-percent-rule/

3. Khlevnoi O., Burak N., Borzov Y., Raita D. (2023). Neural Network Analysis of Evacuation Flows According to Video Surveillance Cameras. In: Babichev, S., Lytvynenko, V. (eds) Lecture Notes in Data Engineering, Computational Intelligence, and Decision Making. ISDMCI 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 149. Springer, Cham. https://doi.org/10.1007/978-3-031-16203-9_35

4. The challenges of analysing unstructured data, [Електронний ресурс]. – Доступний з https://seleritysas.com/blog/2019/08/27/the-challenges-of-analysing-unstructured-data/

5. Рогушина Ю. В. Засоби та методи аналізу неструктурованих даних. Проблеми програмування. 2019. № 1. С. 57–77. [Електронний ресурс]. – Доступний з http://pp.isofts.kiev.ua/ojs1/article/view/348/3 46

Напрям 12

ТЕХНОЛОГІЇ ВІЗУАЛІЗАЦІЇ ДАНИХ

УДК 004.9:378

ВІЗУАЛІЗАЦІЯ ДАНИХ

Анжеліка Дам-Васильєва Чанг, Владислав Ріпний

Харківський національний університет радіоелектроніки, м. Харків, Україна

Анотація. *Ми живемо в епоху даних, а щоб не бути приголомшеними кількістю контенту, ми маємо правильно його сприймати. Для цього необхідно подавати інформацію цікаво та зрозуміло. Використовуючи елементи візуалізації, такі як діаграми, карти, графіки тощо, ми забезпечуємо користувача кращим розумінням даних. Мета статті – вивчення важливості використання інструментів візуалізації даних.*

Ключові слова: *візуалізація даних, інформація, контент, графіки, дані.*

Abstract. *We live in the era of data, and in order not to be overwhelmed by the amount of content, we have to perceive it correctly. For this, it is necessary to present information in an interesting and understandable way. By using visualization elements such as charts, maps, graphs, etc., we provide the user with a better understanding of the data. The purpose of the article is to study the importance of using data visualization tools.*

Keywords: *data visualization, information, content, graphs, data.*

Сфера візуалізації інформації є результатом досліджень взаємодії людини з комп'ютером, інформатики, графіки, дизайну, психології та методів бізнесу. Сама візуалізація – це процес представлення деяких даних у вигляді зображень для максимального полегшення розуміння. Людський мозок сприймає інформацію за допомогою 5 органів чуття: зору, слуху, дотику, смаку та нюху. Проте 80–90% інформації людина сприймає візуально. Взагалі візуалізація заснована на принципі наочності: проілюструвати, продемонструвати предмет і дію, а також процес, явище. За допомогою цих речей ми можемо подати інформацію в більш цікавий і зрозумілий спосіб.

Також візуалізація даних допомагає сприймати та запам'ятовувати інформацію. Наш мозок створений для сприйняття візуальних зображень краще, ніж текст, числа чи табличний вміст. Тому ми часто ігноруємо важливу інформацію у великих обсягах тексту. Візуалізація покликана донести до користувача те, що він зазвичай не бачить.

Веб-дизайнери та інші творці контенту можуть скористатися цією природною людською властивістю, щоб передати їм більше даних. А продумана візуалізація, особливо персоналізована, здатна не тільки передати інформацію, але й закарбуватися в пам'яті. Бо візуалізація даних не тільки допомагає в обробці великих обсягів інформації, але й навіть переконує користувачів.

Коли дизайнер оформляє інформацію у візуальному форматі, він використовує абстрактні дані та робить їх реальними, надаючи їм форми та об'єму загальній картині. Якщо додати до свого матеріалу схеми, діаграми тощо, то зміст миттєво стає переконливішим.

Це можна успішно використовувати в Інтернеті, щоб змусити користувачів думати, вірити та змінювати свої емоції. Така інформація "в реальному часі" з більшою ймовірністю вплине на користувача, оскільки створює в його свідомості образи, які апелюють до його почуттів і починають говорити з ним на емоційному рівні. Тому довіра до нього набагато більша, ніж довіра до тексту.

Візуалізація даних допомагає викликати інтерес. В Інтернеті користувачі рідко мають час і сили цілеспрямовано читати аналітичні матеріали. Як наслідок, сучасні ЗМІ активно займаються візуалізацією даних. Його використовують, щоб цікаво подати (доповнити) масштабний матеріал, адже візуалізація здатна перетворювати складні речі на прості для розуміння.

Вчені встановили, що людина може дізнатися лише 70% інформації з сайту, якщо на ньому є лише текст. А якщо додати картинки або інші методи візуалізації, які вказані на рис. 1, то людина здатна вже запам'ятати 95%.

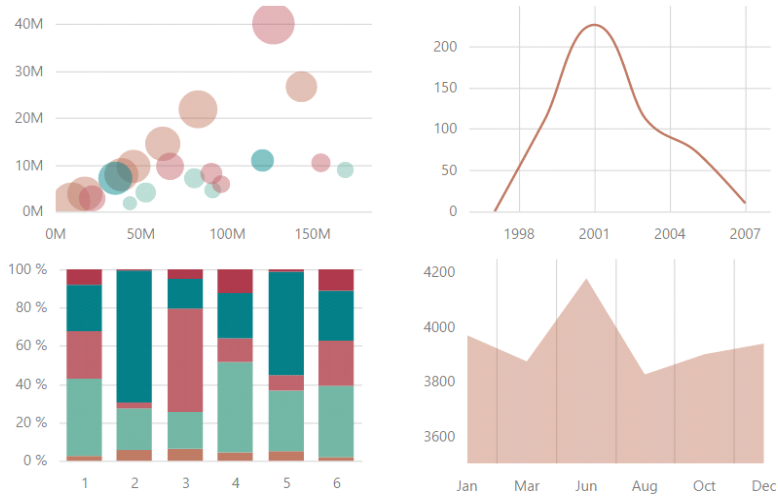


Рисунок 1 – Деякі методи візуалізації даних

А успіх візуалізації безпосередньо залежить від правильності її застосування, тобто вибору графічного типу, правильного використання та оформлення. Як вказано на рис. 2, 60% успіху візуалізації залежить від вибору типу діаграми, 30% від правильного використання та 10% від правильного дизайну.

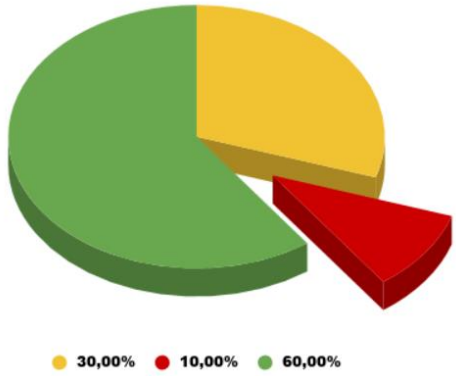


Рисунок 2 – Структура візуалізації даних

Отже, візуалізація – це потужний інструмент для донесення ідей до користувачів, помічник для сприйняття та аналізу даних. Це одна з важливих навичок для маркетологів і веб-аналітиків й не тільки тому, що за допомогою візуалізації даних вони можуть пояснити майже всі дії та результати. Але, як і всі інструменти, візуалізацію потрібно використовувати в потрібний час і в потрібному місці. В іншому випадку інформація може сприйматися повільно або навіть помилково.

Інформаційні джерела

1. Візуалізація даних, як і навіщо її використовувати URL: https://bizautomation.com.ua/vizualizacziya-danikh-yak-i-navishho-yiyi-vikoristovuvati/ (дата звернення 12.11.2022).

2. Як і для чого використовувати візуалізацію даних? URL: http://eidos.org.ua/novyny/yak-i-dlya-choho-vykorystovuvaty-vizualizatsiyu-danyh/ (дата звернення 13.11.2022).

3. Навіщо візуалізація даних в сучасному інтернет-просторі? URL: http://yellowarrow.design/index.php/ua/blog-article/98-data-visualisation-web (дата звернення 13.11.2022).

УДК 004.03

АНАЛІЗ ЗАСОБІВ ТА СИСТЕМ ОПТИЧНОГО ДОСЛІДЖЕННЯ ПРОСТОРУ

Остап Кузик, Олександр Придатко, Назарій Бурак

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *Для оптичного дослідження простору застосовують різноманітні пристрої (камери сенсори), які дають змогу отримати різні аспекти навколишніх об'єктів. Інформація отримується з матриці або за допомогою сканування простору. Більш детальну інформацію для розрізняння об'єктів можна отримати, застосовуючи алгоритми обробки інформації, отриманої з різних пристроїв.*

Ключові слова: *оптичне дослідження простору, алгоритм, камера, лідар.*

Abstract. *Various devices (cameras and sensors) are used for optical exploration of space, which make it possible to obtain various aspects of surrounding objects. The information is obtained from the matrix or by scanning the space. More detailed information for distinguishing objects can be obtained by applying algorithms for processing information received from various devices.*

Keywords: *optical space exploration, algorithm, camera, lidar.*

Простір навколо нас часто вимагає цифрового дослідження для можливості виявлення його структури та реагування на різноманітні зміни. В залежності від умов середовища та завдань, які ставляться перед дослідником, використовують різноманітні діапазони електромагнітних хвиль: видиме світло, інфрачервоні промені, ультрафіолетові промені.

Основними методами дослідження простору є отримання, подальша обробка та аналіз відповідно до завдань статичних або динамічних зображень, а також виявлення змін за допомогою зміни стану оптичних сенсорів. Основними пристроями, які отримують інформацію про навколишній простір, є різноманітні камери, які працюють у відповідних оптичних діапазонах, мульти- та гіперспектральні камери, а також оптичні сенсори. Інформація з камер для її використання може потребувати подальшої цифрової обробки за відповідними алгоритмами, наприклад, значення температури пікселя, отримане за допомогою інфрачервоної камери, перетворюється у відповідний колір, зображення з видимої камери отримує зміну контрастності, яскравості та ін. Після обробки інформація може аналізуватися на наявність динамічних змін різноманітними методами та алгоритмами. Оптичні сенсори для вивчення простору використовуються у поєднанні зі скануванням простору, а після отримання інформації передають її для подальшої обробки за відповідними алгоритмами.

У багатьох практичних задачах дослідження простору на теперішній час набули поширення сенсори класу лідар (з англ. Light Detection and Ranging) [1]. Попереднім аналогом лідару є сенсор типу ToF [2]. ToF використовує один імпульс світла для оцінки всього простору, а лідар використовує сканер який з кількох точок світла отримує ці дані частіше та з більшою точністю.

Розглянемо детальніше LiDAR, та принцип його роботи. Сенсор за допомогою лазера випромінює світлові промені в навколишнє середовище. Пульсуючі промені відбиваються від об'єктів та повертаються до сенсора. Сенсор передає інформацію про час, за який відбитий промінь повертається до сенсора, щоб визначити відстань до об'єкта. Повторення цього процесу багато разів у процесі сканування простору дає можливість створити 3D карту навколишнього середовища.

Кожен із методів та пристроїв дослідження простору має свою сферу застосування, яка визначається практичними завданнями. Для працівників окремих спеціальностей (поліція, військові, інженери електричних мереж, працівники ДСНС та ін.) може бути потрібною специфічна інформація про об'єкти у навколишньому просторі та їх властивості. У цьому випадку розробляють відповідні алгоритми, які після процесу обробки виводять інформацію у зручному вигляді. Проте інформації, отриманої лише з одного сенсора чи камери, може бути недостатньо для оцінювання властивостей об'єктів. Тоді за допомогою спеціальних алгоритмів, які аналізують інформацію, отриману одночасно з різних пристроїв, отримують додаткові дані про об'єкти (наприклад, не лише їх зображення, а температуру, геометричні розміри, тощо). В умовах недостатньої видимості, наприклад задимлення, звичайна камера не дає чіткого зображення, яке дозволяє розгледіти окремі предмети. Тоді може допомогти застосування інших пристроїв, які працюють в інших оптичних діапазонах, або на окремих частотах, а також підсвічування об'єктів відповідним кольором.

Отже, для дослідження простору можуть бути застосовані різноманітні пристрої, які працюють в різних оптичних діапазонах. Для отримання більш повної інформації про об'єкти актуальним завданням є розробка алгоритмів, які обробляють інформацію, отриману з різних пристроїв у сукупності.

Інформаційні джерела

1. Tessema L.S., Jaeger R., Stilla U. (2019). A mathematical sensor model for indoor use of a multi-beam rotating 3D LIDAR. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XLII-2/W16, 2019 PIA19+MRSS19 – Photogrammetric Image Analysis & Munich Remote Sensing Symposium, 18–20 September 2019, Munich, Germany, 227-234.

2. Foix S., Alenya G., Torras G. (2011). Lock-in Time-of-Flight (ToF) Cameras: A Survey. IEEE sensors journal, 11(3), 1–11.

УДК 378.147

ВІЗУАЛІЗАЦІЯ ГЕОГРАФІЧНИХ ДАНИХ ДЛЯ ПОТРЕБ НАСЕЛЕННЯ

Інна Мельникова, Денис Бойко

Відокремлений структурний підрозділ
"Машинобудівний фаховий коледж Сумського державного університету"
м. Суми, Україна

Анотація. *У статті представлено короткий аналіз технологій візуалізації географічних знань комп'ютерними науками для створення корисних програмних продуктів різної тематики, що є розвитком професійних компетентностей майбутніх фахівців.*

Ключові слова: *візуалізація, географія, комп'ютерні науки.*

Abstract. *The article provides a brief analysis of technologies for visualization of geographic knowledge using informatics to create useful software products of various topics according to the needs of the population.*

Keywords: *visualization, geography, computer science.*

Географія, є однією із наук, що дає фундамент для подальшого удосконалення досліджень у галузі господарства, демографії чи сфер послуг. Удосконалення досліджень відбувається через застосування обчислювальної техніки, електронних багатофункціональних джерел інформації, тощо. Відповідно різні комп'ютерні науки дають можливість здійснювати таку роботу з якісним результатом, який максимально простий для розуміння населенням, часто не потребує встановлення необхідного програмного забезпечення, мають на меті допомогти людині у вирішенні різних повсякденних питань, наприклад, знайти необхідний об'єкт на місцевості одним нажаттям клафіші гаджета.

Сучасне інформаційне суспільство потребує чіткої і зрозумілої картини світу з мінімальною кількістю зайвих текстових пояснень, що мають другорядне значення до об'єкта уваги. Наприклад, чи то прогноз погоди із синоптичною картою (рис. 1), чи то карта повітряних тривог, або ж карта вулиць міста з інфраструктурою, містять чітку візуалізацію хвилюючого питання. Такий спосіб збереження й подачі географічної інформації є прикладом взаємозв'язку різних комп'ютерних наук та географії, що нале-

жить до електронних картографічних матеріалів, наприклад, у вигляді програмних додатків.

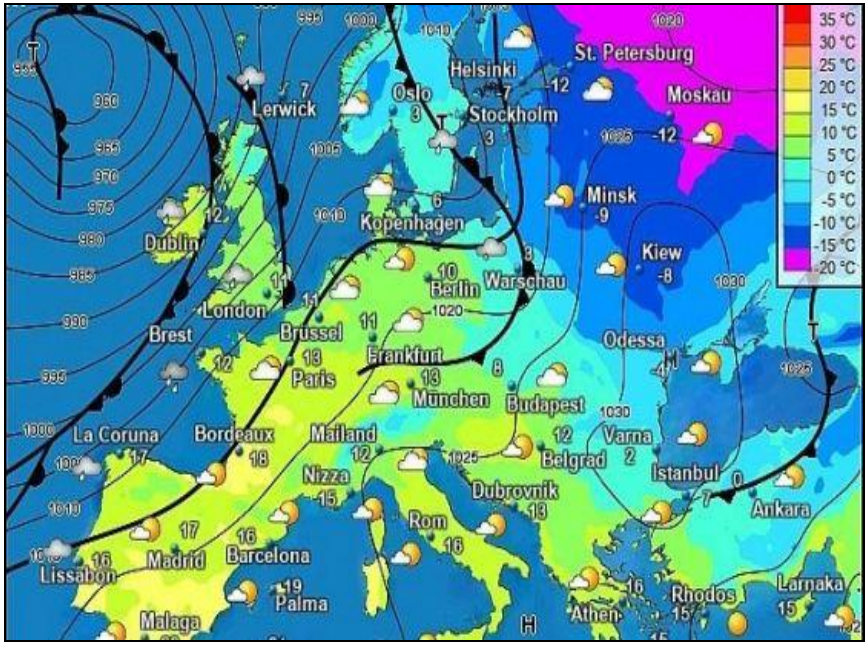


Рисунок 1 – Зразок синоптичної карти

Обробкою і аналізом географічних даних займаються геоінформаційні системи, які населення зараз використовує у вигляді програмних додатків своїх гаджетів. Комп'ютерна візуалізація географічних даних набула активного поширення ще в середині 60-х років XX століття, її "батьком" вважають канадця Роджера Томлінсона, який вперше у світі розробив працюючий пакет системи обробки географічних даних [1, с. 10].

Електронні карти та глобуси – це цифрові картографічні моделі, аналоги звичайних географічних карт або навігаційних систем. Електронне збирання, накопичення й зберігання географічної інформації створює передумови для її постійного використання в різних формах [3]. Наявність автоматизованих комп'ютерних системи, призначених для збирання, зберігання, обробки (рис. 2), аналізу та візуалізації (подання) інформації у вигляді тексту, карт, таблиць, графіків тощо є якраз результативним доказом корисної взаємодії комп'ютерних наук та географії.

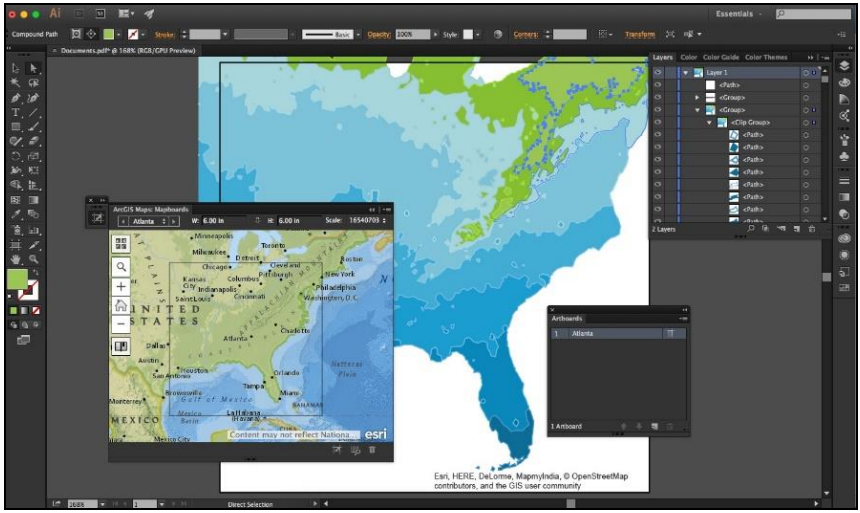


Рисунок 2 – Використання графічного редактора для обробки й візуалізації географічних даних

Інформація в таких базах накопичується швидко й надходить з усього світу від різних джерел: дані стаціонарних та експедиційних досліджень нашої планети, космічний моніторинг Землі (рис. 3), матеріали статистичних довідників, навчальних підручників і посібників, географічні карти, плани й картосхеми, дані аерофотозйомки тощо [3].

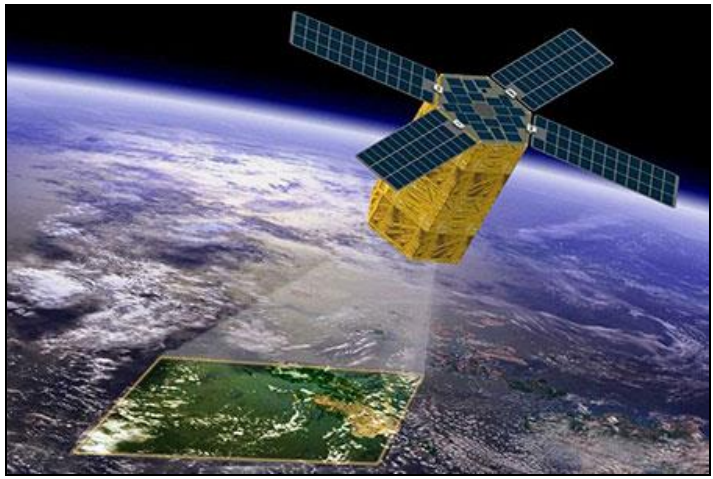


Рисунок 3 – Космічний моніторинг Землі

В основі будь-якої електронної карти є географічна основа, що складається із даних про процеси, які відбуваються на території та їх динаміка. Електронні картографічні продукти можуть бути як безкоштовними, так і комерційними. До переваг таких джерел знань можна віднести, наприклад, не вибагливість до будь-якої операційної системи; достатньо зрозумілий інтерфейс без додаткового вивчення термінології що стосується тематики програмного картографічного продукту; повнота інформації на картах змінюється в залежності від масштабу відображення; система пошуку дозволяє знаходити об'єкти за назвами чи іншими характеристиками та відображати їх на картах; для кожної карти надається легенда та описова інформація [3].

Збирання, накопичення і зберігання географічної інформації в електронному вигляді дає змогу використовувати її в найрізноманітніших формах. Однією з найпоширеніших є виведення географічних карт різного змісту на екран технічного пристрою, а також на принтер для отримання їх паперових варіантів [1, с. 11].

Висновки. Таким чином, сьогодні результати візуалізації географічних даних, а це карти, атласи, аеро- й космічні знімки викладені в мережі Інтернет і є загальнодоступними. Зростає й кількість супутників Землі, які постійно сканують її поверхню, цю інформацію також розміщують у вільному доступі. Тому, сучасні потреби суспільства спрямовані на отримання інформації з використанням всіх технічних можливостей сьогодення. Якраз такі можливості пришвидшують збір, обробку необхідної інформації та візуалізують об'єкт дослідження. Наука географія як і інші не є виключенням у взаємозв'язку з різними комп'ютерними галузями діяльності, використовуючи їх аспекти роботи для удосконалення традиційних картографічних продуктів, що розширює можливості застосування та вільного доступу до них усіх бажаючих.

Інформаційні джерела

1. Лаврик О. Д. Геоінформаційні технології в географії : навчальний посібник / О. Д. Лаврик. – Умань : ФОП Жовтий О. О., 2014. – 120 с.

2. Лаврук М. М. Методика навчання географії: практична і самостійна робота студентів : навчально-методичний посібник / М. М. Лаврук. – Львів : ЛНУ імені Івана Франка, 2015. – 136 с.

3. Електронні карти та глобуси [Електронний ресурс] – Режим доступу: https://uahistory.co/pidruchniki/dovgan-geography-10-class-2018-profilelevel/php

4. Національний атлас України [Електронний ресурс] – Режим доступу: https://atlas.igu.org.ua/maps_elektron.html

УДК 004

ВИКОРИСТАННЯ ВЕБ-ЗАСТОСУВАННЯ ДЛЯ ВІЗУАЛІЗАЦІЇ ОБРОБЛЕНИХ ДАНИХ ДЛЯ ВІРУСНИХ ЗАХВОРЮВАНЬ НА ПРИКЛАДІ COVID-19

М. Плотніков, М. Рудніченко, Н. Шибаєва

Національний університет "Одеська політехніка", м. Одеса, Україна

Анотація. *У даній роботі розглядається застосування візуалізації оброблених даних вірусних захворювань через веб-ресурс. Для аналізу даних використовуються різні методи та нейронні мережі.*

Ключові слова: *аналіз даних, вірусні інфекції, COVID-19, Дерево рішень.*

Annotation. *This article considers the application of visualization of processed data of viral diseases through a web resource. Different methods and neural networks are used for data analysis.*

Keywords: *Data analysis, viral infections, COVID-19, Decision tree.*

Вступ. У сучасному світі важко уявити галузь, у якій не застосовувалися цифрові технології. Цифрові технології дозволяють прискорити процес збору, обробки та використання даних із різних джерел. Також можна оптимізувати та прискорити різні процеси з виробництва ресурсів та інше. Так, на сьогоднішній день велику популярність набирає використання різних методологій аналізу даних та їхньої візуалізації для зручного збирання інформації. А проблематика різних вірусних захворювань також потребує постійної обробки та пошуку різних залежностей.

Мета роботи. Мета роботи розглянути візуальне застосування моделі аналізу даних на наборі вхідних значень для COVID-19 та виявити основні симптоми при хворобі.

Основна частина роботи. Тематика COVID-19 починає втрачати свою актуальність і з кожним роком про неї забувають все частіше і частіше, але це не означає, що не з'явиться у світі новий вірус або поточна мутація. Виявлення різних симптомів та інших залежностей все одно залишається актуальним на сьогоднішній день [1].

Завдяки машинному навчання та іншим методам аналізу даних можна з легкістю розглянути те чи інше джерело даних. Також можна з легкістю зробити прогноз можливого зростання захворювань або взагалі визначити джерело захворювання.

Так, на сьогоднішній день штучний інтелект дозволяє діагностувати COVID-19. Нейронна система дозволяє провести оцінку ступеня ураження легень у пацієнтів. Алгоритм досліджує аналіз крові, рівень сатурації, ре-

зультати КТ. Висновки таких методів допомагають правильно підібрати лікування та полегшує роботу співробітників у подальших процесах.

Можна знайти безліч наборів даних в Інтернеті. Їх можна проаналізувати та знайти певні залежності. Але порахувати математично із заданими параметрами це правильний спосіб, але дати користувачеві інструмент з доступними візуальним інтерфейсом набагато важливіше. Візуальні дані простіше надати і для виявлення залежностей вони ще кращі.

Для демонстрації роботи виберемо невеликий датасет джерела kaggle [2] містить інформацію про пацієнтів, які здали тест на COVID-19. Всього 5434 рядки та 21 стовпець. Кожен рядок відповідає симптомам пацієнта, а кожен стовпець симптому. Перетворивши дані, можна розпочати аналізу.

Продемонструємо невеликий приклад від джерела kaggle [2] містить інформацію про пацієнтів, які здали тест на COVID-19. Всього 5434 рядки та 21 стовпець. Кожен рядок відповідає симптомам пацієнта, а кожен стовпець симптому. Перетворивши дані, можна застосувати різні методи аналізу даних. Наприклад, для даного набору можна скористатися наївним класифікатором деревом ухвалення рішень.

Дерево рішень – це представлення завдання у вигляді діаграми, що відображає варіанти дій, які можуть бути здійснені в кожній конкретній ситуації, а також можливі результати (результати) кожної дії. Такий підхід особливо корисний, коли необхідно прийняти ряд послідовних рішень та коли на кожному етапі процесу прийняття рішення можуть виникати численні результати [3]. Скориставшись цим класифікатором, ми можемо отримати змінені дані та за допомогою візуальних засобів вивести її (рис 1).

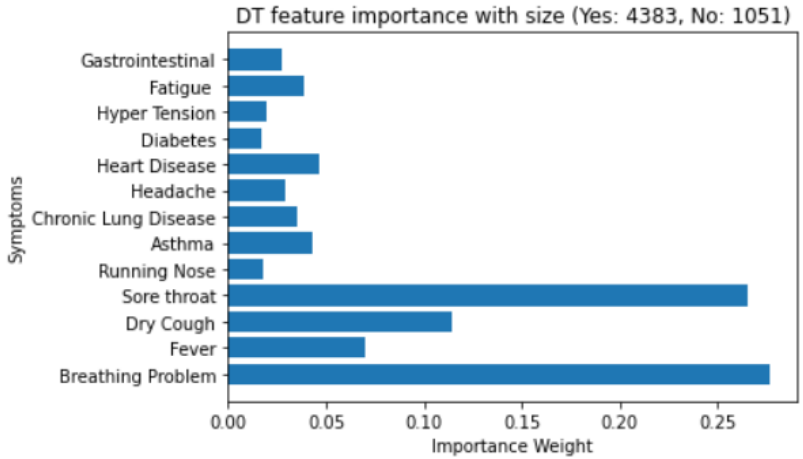


Рисунок 1 – Демонстрація роботи дерева ухвалення рішень

Як бачимо, модель виділяє такі основні три симптоми: сухий кашель, хворе горло, проблеми з диханням. Так можна побачити з графіка, що два критерії однаково йдуть: хворе горло та проблеми з диханням. Зупинившись на цих даних можна зробити хибний висновок, але якщо користувач продовжить тестування, і проведе аналіз з використанням інших моделей, він отримає, що проблеми з диханням не мають такого повноцінного впливу, як видно з малюнка. Це з тим що дані подаються з урахуванням 1 до 4 малюнку. Але якщо подати 1 до 2, то графік одразу стабілізується і залишиться тільки хворе горло.

Завдяки візуалізації даних можна побачити як відображаються вплив тих чи інших параметрів. А якщо задати невеликий веб-ресурс, у якому користувачі змогли б вводити свої дані, змінювати їх та переглядати, то можна надати конструктор для подальшого аналізу як і існуючих моделей, а також прогнозування та визначення симптомів з вірусології.

Висновок. На сьогоднішній день аналіз даних здатний прискорити процес збирання результатів та полегшити цей процес. У роботі я продемонстрував роботу моделі на невеликому наборі даних на прикладі інформації про симптоми у осіб, які хворіють на COVID-19 і визначив, що основними симптомами хвороби є сухий кашель, хворе горло і проблеми з диханням. Для цього застосував просту модель GNB, яка не дає високого результату, в чому переконався в кінцевому результаті. Для детальної роботи з даними бажано використовувати моделі за рівнем складності вище.

Інформаційні джерела

1. COVID-19 Pandemic: Insights from RAND [Електронний ресурс] / Objective analysis. effective solutions. – Режим доступу: https://www.rand.org/latest/covid-19.html – Назва з екрану.

2. Symptoms and COVID Presence (May 2020 data) [Електронний ресурс] / Kaggle – Режим доступу: https://www.kaggle.com/datasets/hemanthhari/symptoms-and-covid-presence – Назва з екрану.

3. Decision Tree Classification in Python Tutorial [Електронний ресурс] / Datacamp. – Режим доступу: https://www.datacamp.com/tutorial/decision-tree-classification-python – Назва з екрану.

УДК 004.738.52

РОЗРОБКА ОДНОСТОРІНКОВОГО ВЕБЗАСТОСУНКУ З ЕЛЕМЕНТАМИ ВЕБСКРАПІНГУ ТА ВІЗУАЛІЗАЦІЇ ГЕОПРОСТОРОВИХ ДАНИХ ЗАСОБАМИ PYTHON

Ірина Семчук

Львівський національний університет імені Івана Франка, м. Львів, Україна

Анотація. *У роботі розглядається вебзастосунок, який використовує вебскрапінг як інструмент збору інформації про послуги онлайнових книгарень та здійснює подальший аналіз цієї інформації з метою формування замовлення за найкращою ціною. Застосунок забезпечує візуалізацію даних (відображення бібліотек і книжкових магазинів поблизу певного місця). Описано його функціонал та інструменти для розробки.*

Ключові слова: *вебзастосунок, пошук інформації, вебскрапінг, візуалізація даних, Python.*

Abstract. *The paper discusses a web-application that uses web-scraping as a tool for collecting information about online bookstore services and further analysis of this information to form the best-priced order. Additionally, data visualization is present to display libraries and bookstores near a given location. Its functionality and tools for development are described.*

Keywords: *web-application, information retrieving, web-scraping, data visualization, Python.*

Вступ. У сучасному світі кількість інформації загалом та в мережі Інтернет зокрема збільшується постійно. Це, у свою чергу, вимагає постійного удосконалення методів та інструментів пошуку і структурування інформації. Усе частіше постає питання автоматизованого збирання та аналізу інформації, "розкиданої" по різних вебресурсах. Без користування спеціалізованими сервісами людині самотужки неможливо охопити та проаналізувати великі обсяги слабоструктурованої інформації [1]. На допомогу в таких випадках приходять програмні розробки у сфері автоматизованих агентів, які полегшують пошук інформації в мережі Інтернет.

На сьогоднішній день існує велика кількість як високотехнологічних пошукових систем відомих розробників, так і власноруч розроблених компаніями чи пересічними програмістами вузькоспеціалізованих пошукових роботів, функціональність яких ґрунтується на вебскрапінгу – технологічних інструментах для виймання та структуризації даних з Інтернет з метою подальшого їх аналізу [2].

В даній роботі береться до уваги візуалізація даних, адже часто для того, щоб зрозуміти певну інформацію, написане потрібно прочитати декілька разів, тоді як з картинки чи з карти може одразу стати все зрозумілим. Є велика кількість технологій візуалізації даних для представлення великих обсягів інформації. Інформація постійно збільшується і найкращим рішення, щоб зрозуміти несчисленні рядки даних є візуалізація [3].

Передумовою виконання цієї роботи стало те, що існує не так багато сервісів та вебзастосунків для оптимізації онлайнових замовлень книг. Більшість з них надають посилання на потрібну книжку з вказуванням її ціни або порівнюють ціни на конкретну книгу в різних онлайнових книгарнях, що робить їх корисними для користувача. Але вони не досконалі, оскільки часто не надають інформації про вартість доставки, а також не повідомляють про діючі знижки. У них зазвичай немає можливості цінового аналізу набору книг, формування замовлення з декількох книгарень з мінімальністю сумарною вартістю, у якій враховані загальна сума доставки, діючі знижки тощо. Недоліком окремих застосунків є відсутність візуалізації геопросторових даних, які могли б допомогти користувачеві краще зрозуміти, де саме йому здійснити купівлю книг чи забрати замовлення. Максимальний функціонал більшості таких застосунків – це отримання інформації про загальну вартість замовлення в межах однієї книгарні. Таким чином, користувача позбавляють можливості купити книжки за вигідними для нього умовами. З огляду на сучасні тренди, найкращим вирішенням цих проблем є створення вебзастосунка, який би враховував всі ці недоліки.

Мета. Використовуючи технології Python, створити вебзастосунок з можливістю формування замовлення в декількох книгарнях та з елементами візуалізації геопросторових даних.

Використані технології. Розробка вебзастосунку була проведена за допомогою мови програмування Python, з використанням фреймворка Streamlit. Для отримання інформації з різних сервісів та вебресурсів використано бібліотеку BeautifulSoup. За допомогою бібліотеки Folium створено геопросторову карту.

Програмна реалізація. В межах цієї роботи було розроблено користувацький інтерфейс для вебзастосунку, який шукає книги за вигідними цінами. Щоб знайти оптимальне замовлення, користувач має заповнити три поля: “Прізвище автора”, “Назва книги” і “Кількість примірників” (рис 1). Після натискання на кнопку “Пошук замовлення” здійснюється пошук корисної релевантної інформації по онлайнових книгарнях за допомогою вебскрапінгу, отримана інформація аналізується на основі гра-

фових алгоритмів і виводиться пропозиція замовлення з мінімально можливою вартістю та супровідною інформацією (логотипи книгарень bookclub.ua, yakaboo.ua та їх назви, вартості книг, доставок, загальна сума замовлення). Користувач може скористатися картою та за своїм місцем розташуванням побачити книгарні в околі заданого радіусу. Є можливість змінити тип карти та скористатися спливаючим вікном над маркером, щоб дізнатися, які саме книги йому купити відносно сформованого замовлення.

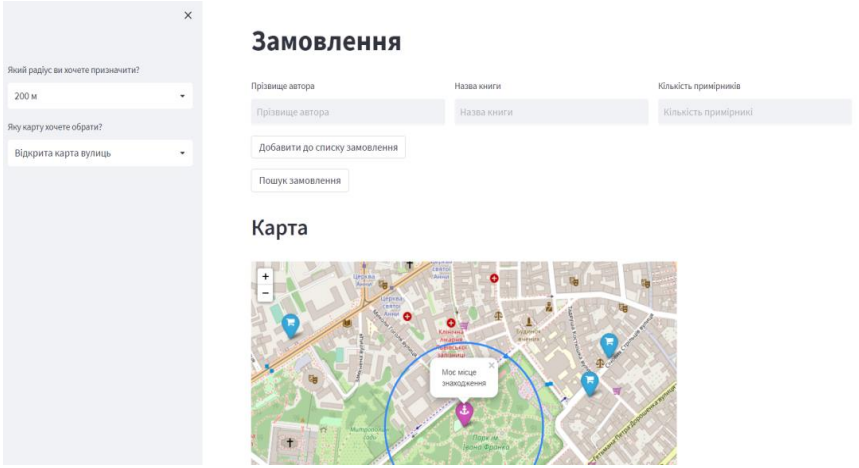


Рисунок 1 – Головна сторінка вебзастосунку

Висновки. Запропонований вебзастосунок у порівнянні з існуючими програмними продуктами має розширений функціонал, оскільки дає змогу сформувати замовлення з кількох книг у кількох книгарнях за вигідною загальною вартістю та надає можливість дізнатися місця книгарень для здійснення самовивозу. Вебзастосунок реалізовано за допомогою сучасних інструментів розробки.

Інформаційні джерела

1. Manning C. Introduction to Information Retrieval / C. Manning, P. Raghavan, H. Schütze., 2008. – 482 p.

2. Krotov V. Scraping Financial Data from the Web Using R Language / V. Krotov, M. Tennyson // Journal of Emerging Technologies in Accounting, 2018, vol. 15, no. 1, pp. 169–181.

3. Панченко Ю. Візуалізація даних: що це таке і для чого вона потрібна (26 березня 2017) [Електронний ресурс]. – https://gurt.org.ua/articles/37609/

Напрям 13

ОПЕРАЦІЙНІ СИСТЕМИ

UDC 004:347.191.11(73)

AMERICAN COMPANY "THE MICROSOFT CORPORATION"

Katerina Makeyeva[1], Lyudmila Pet'ko[2]

[1]Department of Information System
Faculty of Engineering and Pedagogy
Dragomanov National Pedagogical University, sity Kyiv,Ukraine
[2]Department of Foreign languages
Dragomanov National Pedagogical University, sity Kyiv, Ukraine

Annotation. *Described history of Microsoft Corporation, its development and identified features of its activities. BASIC for computer systems on the 8086 microprocessor as the first high-level resident language to appear for 16-bit machines. Investigated its products and given some examples of company activities: Microsoft software, personal computer, Windows operating systems.*

Keywords: *Microsoft Corporation, Bill Gates, Paul Allen, Internet Business, Microsoft Windows, Microsoft Office, Microsoft Servers, Microsoft Visual Studio, Microsoft Mobile.*

Аннотація. *Описано історію корпорації Microsoft, її розвиток та визначено особливості її діяльності. BASIC для комп'ютерних систем на мікропроцесорі 8086 як перша резидентна мова високого рівня, що з'явилася для 16-бітних машин. Досліджено її продукцію та наведено приклади діяльності компанії: програмне забезпечення, персональний комп'ютер, операційні системи Windows.*

Ключові слова: *корпорація Microsoft, індустрія програмного забезпечення, Білл Гейтс, Пол Аллен, інтернет-бізнес, Microsoft Windows, Microsoft Office, Microsoft Servers, Microsoft Visual Studio, Microsoft Mobile.*

The company Microsoft Corporation (Fig. 1) began its history in 1975, when Harvard student friends Bill Gates [2] and Paul Allen (Fig. 2), having read an article published on January 1, 1975 in Popular Electronics magazine about the new Altair 8800 personal computer, developed a Basic language interpreter for it- a popular mainframe computer programming language, for use on an early personal computer (PC), the Altair. A month later, on February 1, a license agreement was signed with Micro Instrumentation and Telemetry Systems (MITS), the manufacturer of this PC, to use Basic as a part of Altair

Fig. 1. Logotype of Microsoft Corporation

few years, they refined BASIC and developed other programming languages [14], (see the video [16]).

In 1980 International Business Machines Corporation (IBM) asked Microsoft to produce the essential software, or operating system, for its first personal computer (Fig. 3), the IBM PC. Note that MS-DOS (Microsoft Disk Operating System) was released with the IBM PC in 1981. Thereafter, most manufacturers of personal computers licensed MS-DOS as their operating system and by the early 1990s Microsoft had sold more than 100 million copies of the program and defeated rival operating systems such as CP/M, which it displaced in the early 1980s, and later IBM OS/2 [1, 14] (Fig. 4).

Fig. 3. Personal Computer

By 1993, Windows 3.0 and its subsequent versions were selling at a rate of one million copies per month, and nearly 90 percent of the world's PCs ran on a Microsoft operating system. In 1995 the company released Windows 95, which for the first time fully integrated MS-DOS with Windows and effectively matched in ease-of-use Apple Computer's Mac OS. Microsoft also became the leader in productivity software such as word-software. They thought of calling their company Allen & Gates, but felt it would be more appropriate for a law firm, so Paul suggested Micro-Soft, from microcomputer and software. Shortly afterward, Gates and Allen founded Microsoft, deriving the name from the words microcomputer and software. During the next

Fig. 2. Bill Gates and Paul Allen

Fig. 4. IBM OS/2

processing and spreadsheet programs, outdistancing longtime rivals Lotus and WordPerfect in the process [9].

Fig. 5. Encyclopedia, Encarta

Microsoft dramatically expanded its electronic publishing division, created in 1985 and already notable for the success of its multimedia encyclopedia, Encarta (1993–2009) (Fig. 5). It also entered the information services and entertainment industries with a wide range of products and services, most notably the Microsoft Network and MSNBC (a joint venture with the National Broadcasting Company, a major American television network, which began in 1995 and ended in 2012) [8].

As a result, by the mid-1990s Microsoft (Fig. 1), which became a publicly owned corporation in 1986, had become one of the most powerful and profitable companies in American history. It consistently earned profits of 25 cents on every sales dollar, an astonishing record [5].

Below we will describe it below **Microsoft software** (Microsoft office). Microsoft Office comes in several editions, the differences between which are in the package and price. The most complete edition contains:

Fig. 6. Microsoft Word

Microsoft Word (Fig. 6) is a word processor. Available on Windows and macOS. Allows we to prepare documents of varying complexity. The product occupies a leading position in the market of word processors [9].

Microsoft Excel (Fig. 7) – spreadsheet. Supports all the necessary features to create spreadsheets of any complexity. Occupies a leading position in the market. The latest version uses OOXML format with ".xlsx" extension, previous versions used binary format with ".xls" extension. Available on Windows and Apple Mac OS [9].

Fig. 7. Microsoft Excel

Fig. 8. Microsoft Outlook

Microsoft Outlook (Fig. 8) is a personal communicator. Outlook includes: calendar, task scheduler, notes, e-mail manager, address book. Joint networking is sup-

ported. The main competitors of the email client are Mozilla Thunderbird / SeaMonkey, Eudora Mail, The Bat! [9].

Microsoft PowerPoint (Fig. 9) is an application for preparing presentations for Microsoft Windows and Apple Mac OS X [9].

Fig. 9. Microsoft PowerPoint

Fig. 10. Microsoft Access

Microsoft Access (Fig. 10) – database management.

Microsoft InfoPath (Fig. 11) a data collection and management application, simplifies the information collection process.

Fig. 11. Microsoft InfoPath

Microsoft Office Communicator (Fig. 12) – designed to organize comprehensive communication between people. Microsoft Office Communicator 2007 provides the ability to communicate easily with instant messaging, as well as voice and video chat. This application is part of the Microsoft Office software package and is closely integrated with it, which allows it to work with any program in the Microsoft Office family.

Fig. 12. Microsoft Office Communicator

Microsoft Publisher (Fig 13) – an application for preparing publications.

Fig. 13. Microsoft Publisher

Microsoft Visio (Fig. 14) **–** an application for working with business charts and technical charts, lets you turn concepts and ordinary business data into charts.

Fig. 14. Microsoft Visio

Microsoft Project (Fig. 15) **–** project management.

Microsoft Query – view and select information from databases [9].

Fig. 15. Microsoft Project

Microsoft OneNote (Fig. 16) is an application for recording and managing notes.

Fig. 16. Microsoft OneNote

***Microsoft Office Groove* 2007** (Fig. 17) is a collaboration support application.

Microsoft Office Picture Manager – work with pictures.

Microsoft Office Diagnostics – diagnose and repair damaged Microsoft Office applications.

Microsoft Office SharePoint Designer is a tool for building applications on the Microsoft SharePoint platform and adapting SharePoint sites [9].

Fig. 17. Microsoft Office Groove 2007

The beginning of 1983 was marked by the release of Apple's Lisa personal computer (Fig. 18) which – though not very successfully – used a graphical interface. The instability and high price of the Lisa determined its failure among users, but the Macintosh computer, created in 1984 based on the work of the Lisa project, sold more than 100,000 copies in its first year of sales. Apple immediately benefited from Microsoft's success – its first GUI products, Word and Excel, were designed specifically for the Macintosh. Adherents of Dos simply laughed at the Lisa and PC graphics shell, calling it the WIMP interface (window, Icons, Mice, Pointers, wimp in translation "boring"). Folders and long file names, which are now an integral part of Windows, also come from Apple computers, which only in 1990 guessed Microsoft to sue for "plagiarism". In 1983 Microsoft has developed a hand-held, low-cost Microsoft Mouse computer (Fig. 19) **(**September 23 1983) [7].

Fig. 18. Apple Lisa personal computer

Fig. 19. Microsoft Mouse computer

Microsoft is a leading manufacturer of software for Apple Macintosh computers. Apple announces the use of BASIC (Fig. 20) and Multiplan for its computers at the Macintosh PC presentation in 1984.

Fig. 20. Applesoft BASIC

Microsoft is creating a new division, Hardware and Peripherals, to expand sales in the computer market, which uses Microsoft software products (April 1984). Windows development tools are being transferred to computer manufacturers and independent software vendors. This month, Microsoft is also launching Project Software, a program for hosting and allocating resources (May 1984) [9].

The number of MS-DOS installations continues to grow, with 200 computer manufacturers already licensed. August. IBM releases the latest version of IBM PC AT with Microsoft system software – MS-DOS 3.0, MS-DOS 3.1 and XE-

NIX. Microsoft announces sales of the Chart business graphics program. Microsoft creates and starts selling File and Word programs for Macintosh PCs. Windows 1.0 users are finally able to work with multiple programs at once and switch freely between them. However, overlapping windows is not allowed, which dramatically reduces the comfort of the environment. In addition, quite a few programs are written for Windows 1.0 (Fig. 21, see the video [4]), as a result, it did not become widespread in the market [8].

Fig. 21. Windows 1.0.

Microsoft and IBM announce an agreement to develop an OS / 2 operating system (1987). The first Microsoft application on CD is Bookshelf (September 8, 1987). The corporation announces a new version of Excel for Windows (October 6, 1987) [9], (see the video [15].

Thus, today, the corporation's success rests on operating systems of the Windows family, including Windows Phone mobile operating systems, as well as on Microsoft Office programs. Microsoft began planning a major replacement for all of its operating systems in 2001. The project, code-named Longhorn (Fig. 22), encountered numerous delays, in part because of efforts to address the public's growing concern with computer security and consumers' desire for PCs to have greater integration with a full range of entertainment equipment within the modern electronic home [9] (see the video [4]).

Fig. 22. Development of Windows Vista

The company started over, and the new operating system, renamed Vista, was released to other software developers late in 2006 and to the general public in 2007. Like most new operating systems, Vista met with initial problems involving incompatibilities with older computer peripherals. More problematic for the new operating system was its "bloated" structure, which required a very fast microprocessor and large amounts of dedicated computer memory for proper functioning. Its high threshold for adequate system resources deterred many companies and individuals from upgrading systems from earlier, and perfectly serviceable, systems such as Windows XP (Fig. 23) (derived from the term Windows Experience). In addition,

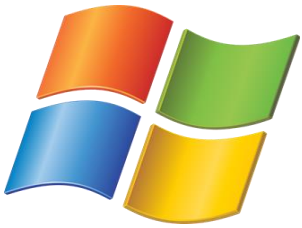


Fig. 23. Windows XP

consumers were baffled by the numerous Vista options – Home (Basic or Premium), Ultimate, Business, and others – while business users (Microsoft's core market) balked at its major change to the user interface and were unwilling to port their internal applications to the new system [6].

Fig. 24. Microsoft Skype

In May 2011, the corporation announced the purchase of Internet telephony company Skype Limited for $ 8.5 billion. After the takeover, the Microsoft Skype Division (Fig. 24) was created on the basis of Skype Limited, with Skype director Tony Bates remaining its head [9].

Fig. 25. Windows 8

In October 2012, Microsoft introduced the new Windows 8 (Fig. 25) operating system. At the beginning of September, 2013 Microsoft announced purchase from Finnish Nokia (Fig. 26) of its division on production and service of mobile phones Devices & Services for 5.44 billion euros. According to analysts, in a similar way, Microsoft, by combining the development of mobile devices and software stuffing for them, will try to compete with Apple. On November 19, 2013, Nokia's shareholder meeting approved this deal. The deal was closed on April 25, 2014 [9].

Fig. 26. Finnish Nokia

In September 2014, Microsoft acquired the Swedish company Mojang AB, the developer of Minecraft. In January 2018, Microsoft announced the acquisition of PlayFab (Fig. 27), a backend service provider for creating and launching cloud-based games. On January 16, 2018, Microsoft closes free updates for Windows 8.1 with the transition to Windows 10. Now Windows 8.1 will not receive any significant improvements and bug fixes – only patches against vulnerabilities, which will be released for another five years, until 2023 [9].

Fig. 27. Microsoft and GitHub

In conclusion, the slogan "hugs, keep and go" often describes Microsoft's strategy of entering the market with extensive use of different standards, continuing to use them with their own improvements.

References

1. A Short History of Microsoft. URL: https://www.thoughtco.com/microsoft-history-of-a-computing-giant-1991140

2. Bill Gates: A Timeline, BBC News Online, BBC (June 15, 2006). URL: http://news.bbc.co.uk/2/hi/business/5085630.stm

3. Global Research Identifier Database, 2015. URL: https://en.wikipedia.org/wiki/Global_Research_Identifier_Database

4 History of Microsoft Windows (Windows 1.0–10). URL: https://www.youtube.com/watch?v=4oE6nEt3uRM

5. Microsoft Corporation. URL: https://hozir.org/microsoft-corporation.html

6. Microsoft corporation form 10-K For the Fiscal Year. URL: https://www.sec.gov/Archives/edgar/data/0000789019/000156459020034944/msft-10k_20200630.htm

7. Microsoft Corporation. URL: https://www.britannica.com/topic/Microsoft-Corporation#ref288469

8. Microsoft electronic publishing division. URL: https://www.coursehero.com/file/100150996/Microsoft-dramatically-expanded-its-electronic-publishing-divisiondocx/

9. Microsoft. URL: https://en.wikipedia.org/wiki/Microsoft

10. Pet'ko Lyudmila. Developing students' creativity in conditions of university // Research: tendencies and prospects: Collection of scientific articles. – Editorial Arane, S.A. de C.V., Mexico City, Mexico, 2017. P. 272−276.

11. Pet'ko L. Multicultural upbringing of students and the formation of professionally oriented foreign language teaching environment // Perspectives of research and development: Collection of scientific articles. – SAUL Publishing Ltd, Dublin, Ireland, 2017. P. 164−170.

12. Pet'ko L. V. Teaching of students' professionally oriented foreign language writing in the formation of professionally oriented foreign language learning environment // Economics, management, law: innovation strategy: Collection of scientific articles. Henan Science and Technology Press, Zhengzhou, China, 2016. P. 356−359.

13. Pet'ko L. V. Teaching methods and the formation of professionally oriented foreign language learning environment in conditions of university. *Intellectual Archive*. 2016. Vol. 5. No. 4 (July/August). Toronto: Shiny Word Corp., Canada. Pp. 73–87.

14. Roy A. Allan (2001). A History of the Personal Computer. A History of the Personal Computer: The People and the Technology 1st Edition. Publisher: Allan Publishing, 2001. 528 p.

15 The History of Microsoft (1975–2001). URL: https://www.youtube.com/watch?v=JmtPWvT1vp8.

16. The Story of Microsoft - How a Computer Club Took Over The World URL: https://www.youtube.com/watch?v=Xjq0kljBZnY

УДК 004.45

ОСОБЛИВОСТІ ПОТРЕБ У ЗАХИСТІ ОПЕРАЦІЙНИХ СИСТЕМ

Валерія Балацька, Тарас Брич, Орест Полотай

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Описано потреби у необхідності захисту операційних систем. Наведено основні завдання захисту операційних систем.*

Ключові слова: *операційна система, захист операційних систем.*

Abstract. *Describes the need for protection of operating systems. The main tasks of protection of operating systems are presented.*

Keywords: *operating system, protection of operating systems.*

Операційна система (ОС) – це набір програм, призначений для забезпечення взаємодії всіх пристроїв комп'ютера і виконання користувачем різних дій.

Захист особливо важливий у багатокористувацькому середовищі, коли кілька користувачів використовують такі ресурси комп'ютера, як процесор, пам'ять тощо. ОСзобов'язана запропонувати механізм, який захищає кожен процес від інших процесів. У багатокористувацькому середовищі всі активи, які потребують захисту, класифікуються як об'єкти, а ті, хто хоче отримати доступ до цих об'єктів, називаються суб'єктами. ОС надає різні "права доступу" різним суб'єктам.

Механізм, який контролює доступ програм, процесів або користувачів до ресурсів, визначених комп'ютерною системою, називається захистом. Захист можна використовувати як інструмент для мультипрограмних операційних систем, дозволяючи кільком користувачам безпечно спільно використовувати загальний логічний простір імен, включаючи каталог або файли.

Користувачам ОС потрібен захист комп'ютерних ресурсів, таких як програмне забезпечення, пам'ять, процесор тощо. Користувачі повинні вживати заходів захисту, щоб допомогти багатопрограмній ОС, щоб кілька користувачів могли безпечно використовувати загальний логічний простір імен, як-от каталог або дані. Захист може бути досягнутий шляхом збереження конфіденційності, чесності та доступності в ОС. Важливо захистити пристрій від несанкціонованого доступу, вірусів, черв'яків та інших шкідливих програм.

В чому все ж таки полягає необхідність захисту в операційній системі?

Різні потреби захисту в операційній системі такі:

− існують ризики безпеки, такі як неавторизоване читання, запис, модифікація або перешкоджання ефективній роботі системи для авторизованих користувачів;

− захист допомагає забезпечити безпеку даних, процесів і програм від несанкціонованого доступу користувачів або програм;

− важливо переконатися, що немає порушень прав доступу, вірусів і несанкціонованого доступу до наявних даних;

− мета захисту полягає в тому, щоб забезпечити доступ до програм, ресурсів і даних лише системних політик.

Також необхідно враховувати цілі захисту в ОС. Вони формуються відповідно до політик безпеки ОС. Політики безпеки визначають, які процеси отримують доступ до ресурсів комп'ютерної системи, таких як центральний процесор, пам'ять, програмне забезпечення та навіть операційна система. Це обов'язок як розробника операційної системи, так і програміста програми. Хоча ці політики змінюються в будь-який час.

Захист ОС – це техніка захисту даних і процесів від шкідливого або навмисного проникнення. Він містить політики захисту, створені ним самим, установлювані керівництвом або накладені індивідуально програмістами, щоб гарантувати, що їхні програми захищені якнайбільшою мірою.

Основними завданнями захищених ОС є:

− забезпечення захисту свого власного середовища від несанкціонованого доступу, підміни компонент та даних;

− захист інформації, що обробляється, накопичується та зберігається в середовищі захищеної ОС, від несанкціонованого доступу.

Він також забезпечує багатопрограмну ОС із безпекою, яку очікують її користувачі, коли спільно використовують спільний простір, наприклад файли чи каталоги.

Роль захисту в операційній системі полягає в забезпеченні механізму реалізації політик, які визначають використання ресурсів у комп'ютерній системі. Деякі правила встановлюються під час проєктування системи, тоді як інші визначаються системними адміністраторами для захисту своїх файлів і програм.

Кожна програма має окремі політики щодо використання ресурсів, і ці політики можуть змінюватися з часом. Таким чином, безпека системи не є відповідальністю розробника системи, і програміст також повинен розробити техніку захисту, щоб захистити свою систему від проникнення.

Отже, якою б сучасною та бездоганною, з першого погляду, системою захисту не була б оснащена ОС та інформаційно-телекомунікаційна система, завжди знайдеться спосіб для несанкціонованого доступу до інформації.

Але при правильному підході до реалізації та експлуатації системи, її компонент – можливо максимально зменшити ризик втрати чи витоку інформації, яка оброблюється та зберігається в системі, забезпечити максимальну працездатність системи навіть за критичних обставин.

ОС можна вважати захищеною, якщо вона забезпечує збереженість інформації та цілісність даних власними засобами, без використання допоміжного програмного забезпечення.

Інформаційні джерела

1. Belej O., Nestor N., Panchak S., Polotai O.I. Developing a Model of Cloud Computing Protection System for the Internet of Things. 2020 IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 – Proceedings, 2020, pp. 53–58.
2. Belej O., Nestor N., Sadeckii J., Polotai O.I. Features of Application of Data Transmission Protocols in Wireless Networks of Sensors. 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019. Proceedings. 2019. Article ID 8847878. P. 317–322.
3. Kukharska N., Lagun A., Polotai O.I. The steganographic approach to data protection using arnold algorithm and the pixel-value differencing method. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020. 2020. Article ID 9204108. P. 174–177.
4. Зерко А., Оксіюк О. Аналіз питань захисту інформації в операційних системах на прикладах захищених операційних систем. Геометричне моделювання та інформаційні технології, № 1 (3), квітень 2017.

УДК 004.45

АВТЕНТИФІКАЦІЯ, ЯК ОДИН З МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОПЕРАЦІЙНИХ СИСТЕМ

Валерія Балацька[1], Орест Полотай[1], Андрій Пузир[2]

[1]Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна
[2]Кафедра безпеки інформаційних технологій Національного університету "Львівська політехніка", м. Львів, Україна

Анотація. *Описано механізм автентифікації, як одного з механізмів забезпечення безпеки операційних систем.*

Ключові слова: *операційна система, автентифікація.*

Abstract. *The authentication mechanism is described as one of the mechanisms for ensuring the security of operating systems.*

Keywords: *operating system, authentication.*

Операційна система (ОС) – це базовий комплекс програмного забезпечення, що виконує управління апаратним забезпеченням комп'ютера або віртуальної машини, забезпечує керування обчислювальним процесом і організовує взаємодію з користувачем. Поняття ОС передбачає комплекс взаємопов'язаних системних програм, призначенням яких є забезпечення взаємодії користувача з комп'ютером та функціонування інших програм.

ОС забезпечує взаємодію між апаратним забезпеченням комп’ютера, прикладними програмами і користувачем.

У сучасних ОС розробниками реалізовано певний перелік механізмів забезпечення безпеки – алгоритми шифрування інформації, автентифікації при доступі до інформації, захисту від несанкціонованого доступу тощо. Комбінація цих механізмів, їх можливості цілком залежать від фантазії розробника ОС або програмного забезпечення.

Механізми забезпечення безпеки більш сильно реалізовані в операційних системах серверного застосування – Linux, BSD. Це пов’язано з галуззю призначення даного типу ОС – серверне застосування в середовищі відкритих систем – Інтернет.

В той же час в операційній системі Windows більш повно реалізовано механізми забезпечення безпеки для використання програмного забезпечення користувачів.

Одним з основних механізмів забезпечення безпеки ОС є автентифікація.

Автентифікація – використовується для підтвердження доступу до інформації, що прив’язана або надається за унікальним ідентифікатором. Зазвичай автентифікація відбувається способом надання:

− унікального предмету або атрибуту (електронний ключ, стартка карта, криптографічний сертифікат тощо);

− паролю (найбільш розповсюджений вид автентифікації);

− біометричних даних (голос, відбитки пальців, підпис, форма долоні тощо).

Найкращі методи автентифікації включають комбінацію імені користувача та пароля, сканування сітківки ока, відбиток пальця або навіть картки користувача для доступу до системи.

Одноразові паролі, зашифровані паролі та криптографія використовуються для створення надійного пароля та потужного джерела автентифікації.

1. Одноразовий пароль

Це унікальний спосіб для кожного входу користувача. Це комбінація двох паролів, які дозволяють користувачеві отримати доступ. Система створює випадкове число, а користувач надає відповідне. Алгоритм генерує випадкове число для системи та користувача, а результат зіставляється за допомогою загальної функції.

2. Зашифровані паролі

Це також дуже ефективна техніка автентифікації доступу. Зашифровані дані передаються через мережу, яка передає та перевіряє паролі, що дозволяє передавати дані без перерв або перехоплення.

3. Криптографія

Це ще один спосіб гарантувати, що неавторизовані користувачі не зможуть отримати доступ до даних, переданих через мережу. Це допомагає безпечно передавати дані. Він представляє концепцію ключа для захисту даних. У цій ситуації ключ має вирішальне значення. Коли користувач надсилає дані, він кодує їх за допомогою комп'ютера, який має ключ, а одержувач повинен декодувати дані за допомогою того самого ключа. У результаті, навіть якщо дані буде вкрадено в середині процесу, існує велика ймовірність того, що неавторизований користувач не зможе отримати до них доступ.

4. Двохфакторна аутентифікація – це додатковий рівень безпеки, окрім вашого пароля або PIN-коду. Якщо після входу в обліковий запис за допомогою пароля вас просили ввести цифровий код, надісланий на мобільний пристрій для підтвердження вашої особи, ви вже знаєте, що таке 2FA.

Двофакторна аутентифікація в поєднанні з традиційною системою паролів забезпечує більш надійний захист, ніж використання тільки облікових даних для входу. Саме завдяки наявності двофакторної аутентифікації багатьох атак за останні місяці можна було б запобігти.

Рішення потрібне для компаній будь-якого розміру, оскільки щоденно співробітники здійснюють вхід на декілька платформ. В першу чергу двофакторну аутентифікацію необхідно забезпечити для облікових записів з правами адміністратора та тих, хто має доступ до конфіденційної інформації. Це є потужним кроком до запобігання крадіжці даних і можливим фінансовим втратам.

Інформаційні джерела

1. Belej O., Nestor N., Sadeckii J., Polotai O.I. Features of Application of Data Transmission Protocols in Wireless Networks of Sensors. 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019. Proceedings. 2019. Article ID 8847878. P. 317–322.

2. Kukharska N., Lagun A., Polotai O.I. The steganographic approach to data protection using arnold algorithm and the pixel-value differencing method. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020. 2020. Article ID 9204108. P. 174–177.

3. Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/index.

4. Зерко А., Оксіюк О. Аналіз питань захисту інформації в операційних системах на прикладах захищених операційних систем. Геометричне моделювання та інформаційні технології, № 1 (3), квітень 2017

5. Поняття операційної системи та її складові. [Електронний ресурс]. – Режим доступу: https://sites.google.com/site/sunlight3555/ponatta-operacijnoie-sistemi-ta-ieie-skladovi

УДК 004.9:378

ВИДИ ОПЕРАЦІЙНИХ СИСТЕМ

Павло Проценко, Ілля Гавриленко

Харківський національний університет радіоелектроніки, м. Харків, Україна

Анотація. *Важко назвати галузь, яка розвивається так стрімко, як інформатизація та комп'ютеризація. У сучасних реаліях вміння користуватися інформаційними технологіями стало актуальним для більшості людей. Оскільки комп'ютер пронизує всі сфери життя, люди вважають, що культура спілкування з комп'ютером важлива. Метою цієї статті є розуміння поняття операційних систем та їх типів.*

Ключові слова: *операційні системи, комп'ютери, інформаційні технології, Windows, Microsoft, MacOS.*

Abstract. *It is difficult to name an industry that develops as rapidly as informatization and computerization. In modern realities, the ability to use information technologies has become relevant for most people. Since the computer permeates all areas of life, people believe that the culture of communication with the computer is important. The purpose of this article is to understand the concept of operating systems and their types.*

Keywords: *operating systems, computers, information technologies, Windows, Microsoft, MacOS.*

Коли комп'ютер вмикається, операційна система завантажується в пам'ять раніше інших програм, а потім служить платформою та середовищем, на якому вони працюють. Неможливо уявити роботу з комп'ютером без операційної системи. А знання операційних систем необхідні для успішного використання сучасних комп'ютерів.

Операційна система – це складна сукупність багатоцільових і багатофункціональних програм, яка є невід'ємною частиною майже всіх сучасних комп'ютерних систем.

Утиліти, такі як завантажувачі та бібліотеки загальновживаних процедур, які почали розроблятися з появою першого покоління комп'ютерів загального призначення (кінець 1940-х років), слід вважати попередниками операційних систем. Утиліти мінімізують фізичні маніпуляції оператора з пристроєм, а бібліотеки дозволяють уникнути багаторазового програмування одних і тих самих дій (реалізація операцій введення-виведення, обчислення математичних функцій тощо).

Операційна система (ОС) займає більш важливе місце в сукупності сучасних системних програмних засобів, що складають програмне забезпечення електронно-обчислювальної машини. До функцій операційної системи входить також забезпечення високої продуктивності двох найважливі-

ших характеристик комп'ютерної системи: ефективності та надійності. Підвищення ефективності – це підвищення ефективності використання апаратних засобів; зниження системних витрат; підвищення продуктивності праці користувача; підвищення зручності використання комп'ютерної техніки.

Яка операційна система найпопулярніша серед користувачів? Список виглядає так:

– Windows;
– MacOS;
– Android;
– Ubuntu;
– Linux тощо.

Якщо розбити операційні системи, встановлені на комп'ютерах, то тут лідирує Windows – на неї припадає 76,58% всіх комп'ютерів. OS X – 18.93 і Linux – 1.62%. Це можна побачити на рис. 1.

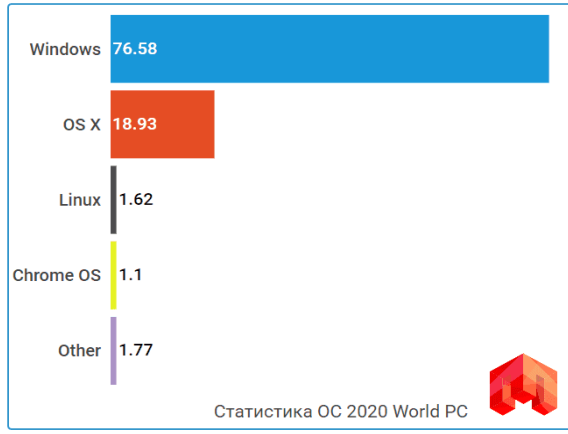


Рисунок 1 – Найпопулярніші ОС на 2020 рік

Отже, давайте детальніше розглянемо три найпопулярніші операційні системи.

Microsoft Windows – це загальний термін для операційних систем смартфонів, планшетів, ноутбуків і персональних комп'ютерів, розроблених корпорацією Microsoft у Сполучених Штатах.

Основні переваги улюбленої багатьма "Вінди" полягають в наступних факторах:

– Зручний інтерфейс;
– Велика кількість якісного програмного забезпечення, яке можна встановити безкоштовно;
– Легко встановити та налаштувати.

Але є й мінуси. Більшість версій Windows є платними операційними системами. Також висока вартість програмного забезпечення – головний недолік Windows.

MacOS – це операційна система, розроблена Apple для комп'ютерів, які вона виробляє. Ця ОС відома як продукт преміум-класу, створена для користувачів – вона відома своїм гарним дизайном, зручним інтерфейсом і чудовими мультимедійними можливостями. Але це рішення далеко не кожному по кишені, оскільки і сам комп'ютер, і операційна система Apple дуже дорогі в порівнянні з іншими комп'ютерами. Отже, операційна система має менший відсоток користувачів.

Linux – це сімейство операційних систем з відкритим кодом. Це означає, що їх може модифікувати (змінювати) і розповсюджувати будь-хто в будь-якій точці світу. Це робить цю операційну систему дуже відмінною від інших операційних систем, таких як Windows, які може змінювати та розповсюджувати лише власник (Microsoft). Linux названо на честь Лінуса Торвальдса, який заклав основу Linux у 1991 році.

Його перевага в тому, що він безкоштовний і є багато різних версій на вибір. Кожна версія має свій власний зовнішній вигляд, найпопулярнішими є Ubuntu, Mint і Fedora.

Однак, незважаючи на всі ці переваги, Linux вимагає високих навичок користувача. Тому Linux найчастіше встановлюють програмісти, мережеві інженери та інші фахівці.

Отже, кожна операційна система має свої переваги і недоліки, тому кожен вибирає відповідно до своїх побажань і сфери діяльності.

Інформаційні джерела

1. Операційні системи URL: https://ukrreferat.com/chapters/komputerny-nauki/operatsijni-sistemi-referat.html (дата звернення 14.11.2022).

2. Сучасні операційні системи, архітектура, відмінні характеристики, функціональність, виробництво і перспективи розвитку URL: https://xreferat.com/33/2118-1-suchasn-operac-iyn-sistemi-arh-tektura-v-dm-nn-harakteristiki-funkc-onal-n-st-virobnictvo-perspektivi-rozvitku.html (дата звернення 14.11.2022).

3. Операційні системи: призначення, різновиди URL: https://crashbox.ru/ installing-multiple-os/computer-operating-systems-operating-system-purpose-varieties/ (дата звернення 14.11.2022).

4. Операційна система URL: https://uk.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0 (дата звернення 14.11.2022).

Напрям 14

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ ПРОЄКТАМИ

УДК: 658.004

CYBER SECURITY IN BUSINESS PROCESSES

Roman Panovyk[1], Ardon Carol Rocio[2]

[1]Master's student of Ukrainian Academy of Printing, Ukraine
[2]IT Security & Compliance Specialist at Nestle, Switzerland

Abstract. *The paper considers the problem of cyber security and its impact on business in the modern world. Global cyber security trends from a business perspective, how global companies are interested in cyber security. An overview of the most common threats, methods of cyber-attacks, consequences, and measures to avoid or mitigate them.*

Keywords: *cyber security, cyberattacks, global business, protection, social engineering, information.*

Анотація. *У статті розглядається проблема кібербезпека та її вплив на бізнес у сучасному світі. Глобальні тенденції кібербезпеки з точки зору бізнесу та наскільки глобальні компанії зацікавлені в кібербезпеці. Огляд на найпоширеніші загрози, методи кібератак, наслідки та заходи їх уникнення або пом'якшення.*

Ключові слова: *кібербезпека, кібератаки, глобальний бізнес, захист, соціальна інженерія, інформайція.*

Cyber security has become a necessity for businesses of all sizes as their systems and networks containing sensitive and valuable data have come under siege by malicious actors. It is designed to protect all categories of data from theft and damage. Without a cyber security strategy, your business cannot defend itself from cyber threats leaving it vulnerable to malicious actors, who will identify your business as an easy target. Along with the way technology has evolved over the years, there has been a steady increase in inherent and residual risks. Businesses have adopted more convenient methods of carrying out their operations, for example, data can now be stored on the cloud, i.e. many businesses use cloud services like Amazon Web Services, to store their valuable data. Although convenient, businesses rarely secure their information adequately while using these cloud services, paired with an increase in attacker sophistication, this has led to a heightened level of risk that your business may succumb to a successful cyber-attack or data breach. Cyber-attacks are increasingly getting more sophisticated as criminals are having an easier time evading traditional security controls, through the adoption of new methods of attack that imple-

ment AI and social engineering. Businesses as they adopt newer technology need to also enhance their cyber security efforts to match it.

A strong cybersecurity strategy consists of different layers of protection to defend your business against all kinds of cybercrime, including attacks that are designed to access, change or destroy data, extort money from your employees or business, or aim to disrupt your day-to-day business operations.

Cyber strategies should take into account: infrastructure security, network security, application security, information security, cloud security, employee security training and awareness, disaster recovery, or business continuity.

We are only becoming more reliant on technology, sensitive information like client and customer information is being stored online on cloud storage solutions like Dropbox or Google Drive. Businesses have become more reliant on computer systems, and this has only been boosted by the COVID-19 pandemic, with the majority of businesses having to adopt work-from-home solutions. This reliance along with the adoption of cloud services, smartphones, the Internet of Things, and AI has led to various new security vulnerabilities that didn't exist a few years ago.

Governments have also increased their regulation when it comes to cybercrime, for example, the General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. With the GDPR, Europe is signaling its firm stance on data privacy and security at a time when more people are entrusting their personal data with cloud services and breaches are a daily occurrence. Therefore, with the increase in regulation by government bodies on cybercrime, there has been an increase in importance and attention given to cybersecurity. Standard boards like the National Institute of Standards and Technology (NIST), have released a framework to help businesses understand their information security risks, and improve their own cybersecurity measures in the hopes of defending against cyber-attacks and data breaches [1].

Criminals are increasingly targeting the information stored by businesses, with information theft being the most expensive and fastest-growing segment of cybercrime. This is supported by the increase in businesses storing identifiable information via cloud services, thus increasing its exposure. However, it is important to note that theft is not the only possible goal, with some criminals choosing to either change or destroy information, with the hope of building distrust in an organization or government.

Social engineering continues to be the easiest form of cyber-attack with ransomware and phishing attacks being common attack methods to gain entry into a business's critical systems or networks. Third-party risk is also increasing, as criminals choose to target third or fourth-party vendors, such as IT providers to gain access to businesses they partner with. All of the above trends have only helped heighten the need for and importance of cybersecurity to be taken seriously by businesses. Cyber-attacks can influence every organization regardless of size, in many ways including financial losses, dip in productivity, damage to reputation, legal liability, and business continuity problems. Accord-

ing to The U.N. disarmament chief, cybercrime is up 600% because of the COVID-19 pandemic. All signs point to cyberattacks only increasing from here on out, therefore, businesses need to prioritize the implementation of a robust cybersecurity program or strategy [2].

To protect your business from cybercriminals, we offer a few simple steps:

− Educate employees. Cybersecurity training is a strategy implemented by the IT and Security professionals in an organization to prevent and mitigate risk when it comes to compromising an organization's information security. These training programs are specifically designed to provide employees with clarity regarding their roles and responsibilities when it comes to upholding information security. A successful security awareness program helps employees understand proper cyber etiquette, and the security risks associated with their actions and to identify cyberattacks they may encounter during their day-to-day operations.

− Implement privileged access. Privileged Access Management refers to the strategies and technologies organizations utilize to manage privileged access and permissions for users, accounts, processes, and systems across an IT environment. By strategically assigning employees the correct level of access depending on their role and responsibilities in the organization, the overall risk of suffering extensive damage from a cyber-attack is effectively mitigated, irrespective of whether it is from an external actor or due to internal errors.

− Monitoring, Detection & Response. Businesses need to monitor their systems and networks on a 24/7 basis to ensure that there is no suspicious activity that may point to an attack or breach. If cybersecurity monitoring is not in place this could lead to a delay in detecting that an attack is underway, and your business may not be able to respond in time to prevent it or reduce its impact.

− Manage Third-Party Risk. Third-Party Risk refers to the potential threat presented to a business's employees and customer data, financial information, and operations, from third-party vendors e.g. suppliers and other outside parties that provide products and services and have access to your systems. It is important for businesses to do their due diligence when collaborating with a vendor e.g. ensuring that they have adequate information security policies in place and continue to monitor that these standards are upheld when handling their valuable data.

Conclusions. The steps described above are reducing cyber-attack-related issues in our day-to-day work, increasing our cybersecurity, and reducing the chance of falling prey to a cyber-attack or data breach. This is one of the most important parts of the process that ensures the continuation of all business activities.

References

1. Steve Morgan. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine, Nov. 13, 2020. Available at: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

2. Accenture/Ponemon Institute: The Cost of Cybercrime. Report Analysis. Network Security Vol. 2019, No. 3. Published Online: https://doi.org/10.1016/S1353-4858(19)30032-7

УДК 004.45

ІНФОРМАЦІЙНА СИСТЕМА ДИСТАНЦІЙНОГО МОНІТОРИНГУ КЛІМАТИЧНИХ УМОВ

Анна Антіпенко, Тарас Басюк

Національний університет "Львівська політехніка" м. Львів, Україна

Анотація. *Створено веб-додаток з необхідним функціоналом. Програмні модулі є документованими. Програмний код виконаний відповідно до правил "гарного стилю" і максимально оптимізований. Практичним застосуванням роботи є створення веб-застосунку з прогнозом погоди на основі дистанційного моніторингу кліматичних умов. Створена інформаційна система дає можливість зручно і швидко дізнатись детальні показники пронозу погоди в будь-якій точці світу.*

Ключові слова: *інформаційна система, веб-додаток, моніторинг, кліматичні умови.*

Abstract. *A web application with the necessary functionality has been created. The software modules are documented. The program code is made in accordance with the rules of "good style" and is optimized as much as possible. The practical application of the work is the creation of a web application with a weather forecast based on remote monitoring of climatic conditions. The created information system makes it possible to conveniently and quickly find out detailed indicators of the weather forecast in any part of the world.*

Keywords: *information system, web application, monitoring, climatic conditions.*

Для реалізації даного проєкту використовували бібліотеку React. React – JavaScript-бібліотека є для створення користувацьких інтерфейсів. Вона допомагає спростити створення інтерактивних інтерфейсів. Нам потрібно лише описати, як різні частини інтерфейсу виглядають у кожному стані додатку і React ефективно оновить лише потрібні компоненти, коли дані зміняться [1, 2].

Для створення React-додатку відкриваємо термінали за допомогою команди npxcreate-react-app створюємо проєкт з ім'ям weather-app. Після того, як каталог з проєктом створився, видаляємо весь вміст файлів App.js та App.css у каталозі src – він нам більше не знадобиться.

Встановлюємо наступні пакети, які будуть потрібні в процесі розробки:

− react-icons (для роботи з іконками);

− google-map-react (для роботи з картами);

− react-alert та react-alert-template-basic (для роботи з повідомленнями);

− recharts (для роботи з графіками).

У програмі будуть дві основні сторінки – сторінка для вводу міста, в якому ми хочемо дізнатися інформацію про погоду (сторінка CityForm.js),

та сторінка де безпосередньо виводиться інформація про погоду (сторінка WeatherData.js). У каталозі src створюємо каталог pages, у якому створюємо файли CityForm.js та WeatherData.js – в них буде описана розмітка сторінок і логіка, а також CityForm.css та WeatherData.css, де будуть описані стилі цих сторінок.

Інформацію про погоду отримуватимемо використовуючи api сайту openweathermap. Для цього необхідно зареєструватися на даному ресурсі і у персональному кабінеті отримати api-ключ. Також необхідно отримати api-ключ для роботи з google-картами. Це необхідно зробити у персональному кабінеті на сайті console.cloud.google.com.

У файлі App.js описуємо функцію getData() для отримання погоди у будь-якому місті світу. Логіка даної функції наступна: виконується GET-запит за посиланням http://api.openweathermap.org і api-ключа, який ми попередньо отримали, після чого отримаємо JSON-відповідь, яку заносимо у властивість data. Також паралельно виконуємо обробку помилок, використовуючи методи з бібліотеки react-alert для відображання їх на екрані.

У файлі CityForm.js, використовуючи розмітку jsx, створюємо форму з текстовим полем і однією кнопкою, при натисканні на яку викликатиметься функція getData(). У файлі WeatherData.js створюємо jsx розмітку сторінки, на якій відображатиметься інформація про погоду: атмосферний тиск, вологість повітря, поточна температура, мінімальна та максимальна температура за годину та за день,стан погоди (наприклад – дощ, туман, сонце), час сходу та заходу сонця, прогноз погоди на 5 днів вперед, а також створюємо функцію getWeatherForecast() для отримання прогнозу погоди. Дана функція працює аналогічно до функції getData(), тільки отримує і зберігає дані про прогноз погоди. У кожному з блоків на екрані, в яких відображаються дані, відбувається парсинг даних зі змінної data. Усі стилі зберігаються у файлі WeatherData.css.

У блоці з даними про температуру відбувається їх перетворення у градуси Цельсія (у JSON-об'єкті вони вказані у Фаренгейтах), у блоці з часом сходу та заходу сонця перетворюємо мілісекунди у години та хвилини, а у блоці зі значенням тиску переводимо значення Паскаль у значення в міліметрах ртутного стовпця.

Відображення прогнозу погоди відбувається наступним чином. Після того як отримаємо дані про погоду, зберігаємо значення температури у масив forecast, а значення конкретного часу, коли буде та чи інша температура – у масив categories. Дані масиви передаються у властивості лінійного графіка з бібліотеки recharts, де відображаються за обраним індексом дня (від 0 до 5, що відповідає кількості днів). Вибір індекса відбувається нижче графіка – за допомогою методу map() відбувається рендеринг усіх можливих значень часу, коли можна переглянути погоду. Для створення

блоку з google-картою використаємо компонент GoogleMapReact з бібліотеки google-map-react, в параметри якого передаємо попередньо отриманий арі-ключ, значення приближення карти, а також координати (довготу та широту), які отримали, виконавши GET-запит на сайт openweathermap.org. На даному етапі створення web-додатка завершено.

Для прикладу вводимо у текстовому полі будь-яке місто (наприклад Львів), натискаємо кнопку “Getinfo”, на наступній сторінці отримаємо інформацію про погоду у даному місті (рис. 1).

Рисунок 1 – Візуалізація даних

На цій сторінці відображається інформація про погоду: атмосферний тиск, вологість повітря, поточна температура, мінімальна та максимальна температура за годину та за день, стан погоди (дощ, туман, сонце), час сходу та заходу сонця, прогноз погоди на 5 днів (можемо обрати потрібний нам день), а також є можливість переглянути google-карту, де вказано розташування міста.

Таким чином, практичним застосуванням роботи є створення вебзастосунку з прогнозом погоди на основі дистанційного моніторингу кліматичних умов. Створена інформаційна система підходить для використання як окремій особі для своїх потреб, так і для аналізу метеоданих вузькоспеціалізованими підприємствами або науковими установами. Вона дає можливість зручно і швидко дізнатись детальні показники пронозу погоди в будь-якій точці світу.

Інформаційні джерела

1. Литвин В.В. Проектування інформаційних систем /Н. Б. Шаховська, В. В. Литвин. Львів: “Магнолія-2006”. 380 с.

2. Боггс У. UML и Rational Rose / У.Боггс, М.Боггс. М.: ЛОРИ, 2000. 582 с.

УДК 614.842, 681.5

БЕЗПІЛОТНІ ЛІТАЛЬНІ АПАРАТИ ДЛЯ ПІДВИЩЕННЯ ФУНКЦІОНУВАННЯ КРИЗОВОГО ЦЕНТРУ ЦИВІЛЬНОГО ЗАХИСТУ

Даниїл Беген, Сергій Ємельяненко

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *Кризовий центр цивільного захисту відіграє важливу роль у прийнятті управлінських рішень при надзвичайних ситуаціях на основі моніторингу та аналізу отриманої інформації. Він також слугує для налагодження та для координування взаємодії всіх органів держаної влади та оперативно-рятувальних підрозділів міста, та області у разі виникнення надзвичайної ситуації. Для ефективного та безпечного проведення розвідувальних задач є доцільним застосування БПЛА на відкритому просторі, що дозволяє покращити діяльність Кризового центру цивільного захисту.*

Ключові слова: *кризовий центр, надзвичайна ситуація, цивільний захист, БПЛА, кризове управління.*

Abstract. *The Crisis Center of Civil Protection Crisis Center plays a vital role in making emergency management decisions based on monitoring and analysis of the received information. It also serves to establish and coordinate the interaction of all state authorities and operational rescue units of the city and region in case of emergency. For the effective and safe performance of reconnaissance tasks, it is advisable to use UAVs in open spaces, which allows for to improvement of the activities of the Crisis Center of Civil Protection.*

Keywords: *crisis centre, emergency, civil defence, UAVs, crisis management.*

Стихійні лиха, катастрофи на нашій планеті щороку забирають людські життя, руйнують населенні пункти й різні об’єкти, приносячи великі збитки державі та населенню. Тільки за 2021 рік Україна втратила від надзвичайних ситуацій збитків на суму понад 24,4 млн доларів [1], а лише за вісім місяців від повномасштабної війни, збитки України сягають понад 127 млрд доларів [2].

Як наслідок Державна служба України із надзвичайних ситуацій ініціює та впроваджує сучасні технології та новітні методи для вирішення проблем з ліквідації наслідків військових дій. Вона створює та/або запозичує у закордонних партнерів нові та сучасні способи у боротьбі із надзвичайними ситуаціями (військового характеру). Одним із хороших прикладів освоєння та імплементування закордонного досвіду та європейських стандартів, є створення на базі навчальних установ цивільного захисту та підрозділів центрального підпорядкуванню апарату ДСНС України Кризових центрів.

Метою Кризового центру цивільного захисту – підвищення рівня компетентностей та навиків у відпрацюванні взаємодії всіх органів державної влади та оперативно-рятувальних підрозділів міста та області у разі виникнення надзвичайної ситуації. Налагодження взаємодії та порядку залучення відповідних органів управління в умовах виникнення НС, зокрема з практичними працівниками, які безпосередньо входять до складу комісій ТЕБтаНС міста та області, штабу з ліквідації НС [3].

Одним із основних завдань Кризового центру є моніторинг і аналіз отриманої інформації та здійснення своєчасних та правильних управлінських рішень. А для цього надважливо провести якісну розвідку місця виникнення НС. Метою проведення розвідки вважається отримання даних, що будуть використані для визначення ступеню загрози людям, правильної оцінки обстановки на місцевості та прийняття відповідного рішення щодо ліквідації даної події. Ефективність розвідувальних заходів буде залежати від виконання низки вимог, таких як оперативність, безперервність, активність, достовірність і цілеспрямованість [4], тому застосування безпілотної техніки для виконання розвідувальних задач на відкритому просторі є найбільш ефективним та безпечним. Безпілотні літальні апарати, які також в простонародді називають "безпілотниками" і/або "дронами", широко застосовують як у військових справах, так і у цивільному житті.

В Україні БПЛА широко використовують для проведення розвідувальних операцій під час воєнних дій, а для потреб цивільного захисту його популяризація тільки набирає обертів, але вже зараз їх використання показує досить хороші результати. Їх застосовують для гарантування роботи гуманітарних коридорів, для евакуації та для супроводу розмінування. Також безпілотники здійснюють розвідки пожеж та огляд зон надзвичайних ситуацій.

Спектр застосувань БПЛА з кожним роком росте і розвивається, а його популяризація все краще і швидше дозволяє отримувати аналітичну інформацію, більше того воно здешевлює дану задачу. До прикладу [5–7], можна виділити такі сфери застосування БПЛА, які використовуються закордоном: військова розвідка; виконання завдань моніторингу потенційно небезпечних зон, виявлення радіаційної, хімічної та біологічної небезпек чи загроз, ідентифікації отруйних речовин, ідентифікації біологічних засобів, попередження та визначення місця розташування небезпек і загроз; необхідність картографування та створення 3D карт; при оцінці ступеню пошкодження будівлі і ризику проведені аварійно-рятувальних робіт; використання БПЛА для доставки гуманітарних речей першої допомоги; використання БПЛА при виникненні надзвичайної ситуації природного характеру (повені, землетрусах); використання БПЛА при проведені пошуково-рятувальних робіт на воді, в горах, чи при розбиранні

конструкцій; використання БПЛА проведення профілактичної діяльності у будівельній галузі для допомоги інспекції у перевірці будівель і майданчиків для забезпечення безпеки та контролю; використання БПЛА для створити загальної картини надзвичайної ситуації під час або після події, для сформування справжньої картини масштабу та її впливу; для сформування оптимальної логістичної розв'язки та правильного розподілу ресурсів після стихійного лиха; спостереження за подіями та масовими зібраннями в реальному часі, які охоплюють великі території, такі як марафони, спортивні заходи та фестивалі, які створюють багато проблем для бригад швидкої допомоги.(медицина катастроф); швидше реагування на виклики у сільській місцевості (розроблення прототипів пасажирських повітряних транспортних засобів для доставлення пацієнтів до лікарень); контроль за станом лісових масивів, сільськогосподарських посівів, стеження за якістю та своєчасністю вжиття різних заходів на цих територіях.

Отже, Використання БПЛА для потреб Кризового центру відіграє важливу роль для прийняття управлінських рішень під час НС, а особливо під час військового стану.

Інформаційні джерела

1. Звітні матеріали Державної служби України з надзвичайних ситуацій. Режим доступу: https://dsns.gov.ua/uk/diyalnist-sluzhbi/zvitni-materiali-derzhavnoyi-sluzhbi-ukrayini-z-nadzvichaynih-situaciy (Last accessed: 05.09.2022).

2. Збитки України від війни перевищили $127 мільярдів у вересні – KSE. Режим доступу: https://www.epravda.com.ua/news/2022/10/21/692884/

3. Кузик А. Д., Ємельяненко С. О., Безнос Н., Кушпа С. Кризовий центр цивільного захисту. Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської наук.-практ. конф. молодих учених, студентів і курсантів: Львів, 2021. С. 146–148. URL: https://sci.ldubgd.edu.ua/jspui/handle/123456789/9467

4. СТАТУТ дій органів управління та підрозділів Оперативно-рятувальної служби цивільного захисту під час гасіння пожеж: Наказ Міністерства внутрішніх справ України 26 квітня 2018 року № 340. URL: https://zakon.rada.gov.ua/laws/show/z0802-18#Text (дата звернення: 07.09.2022).

5. Ways Drones are Being Used for Disaster Relief. URL: https:// safetymanagement.eku.edu/blog/5-ways-drones-are-being-usedfor-disaster-relief/ (Last accessed: 04.09.2022).

6. Oliver F. Six ways drones are helping in emergency response. URL: https://www.soarizon.io/news/six-ways-drones-are-helpingin-emergency-response (Last accessed: 04.09.2022).

7. The Future of Emergency Response: 4 Ways Drones Can Help Save Lives. URL: https://www.skygrid.com/blogs/emergencyresponse-how-drones-can-help-save-lives/ (Last accessed: 04.09.2022).

УДК 004.942

АНАЛІЗ МЕТОДИК ТА ПРИСТРОЇВ СКАНУВАННЯ РАЙДУЖНОЇ ОБОЛОНКИ ОКА ДЛЯ ВИКОРИСТАННЯ В ГАЛУЗІ ПАСАЖИРСЬКИХ ПЕРЕВЕЗЕНЬ

Валентин Гончар[1], Ганна Мартинюк[2]

[1]Національний авіаційний університет, м. Київ, Україна
[2]Маріупольський державний університет, м. Київ, Україна

Анотація*. У доповіді наведено основні методики сканування райдужної оболонки ока. Надано порівняльну характеристику методів біометричної ідентифікації. Наведено та проаналізовано пристрої, які можна використовувати в галузі пасажирських перевезень.*

Ключові слова: *райдужна оболонка ока, біометрична ідентифікація, методи сканування, пасажирські перевезення.*

Abstract. *The report describes the basic methods of scanning the iris. A comparative description of biometric identification methods is provided. Devices that can be used in the field of passenger transportation are given and analyzed.*

Keywords*: iris, biometric identification, scanning methods, passenger transportation.*

Розпізнавання райдужної оболонки ока – це біометричний метод, який набирає популярності в усьому світі. Його точність і безконтактний метод ідентифікації осіб роблять його ідеальним біометричним рішенням для багатьох напрямків людської діяльності.

Як і у випадку з усіма біометричними рішеннями, одним із факторів, який перешкоджає зростанню, є турбота про конфіденційність і незручності, що виникають для кінцевого користувача. Однак у міру того, як рішення стають безпечнішими та зручнішими для користувачів, ці проблеми вирішуються, і галузь продовжує стрімко розвиватися [3].

Сканування райдужної оболонки вимірює унікальні візерунки в райдужній оболонці, кольорові кола в очах людей. Біометричні сканери для розпізнавання райдужної оболонки ока працюють шляхом освітлення райдужної оболонки ока невидимим інфрачервоним світлом для виявлення унікальних візерунків, які не видно неозброєним оком. Сканери райдужної оболонки виявляють і виключають вії, повіки та дзеркальні відблиски, які зазвичай блокують частини райдужної оболонки. Кінцевим результатом є набір пікселів, що містить лише райдужну оболонку. Далі візерунок ліній і кольорів ока аналізується, щоб виділити бітовий візерунок, який кодує інформацію в райдужній оболонці. Цей бітовий шаблон оцифровується та

порівнюється із збереженими шаблонами в базі даних для перевірки (зіставлення шаблонів один до одного) або ідентифікації (зіставлення шаблонів один до багатьох) [2].

Прикладом використання цього біометричного методу в галузі пасажирських перевезень є транспортна служба, яка обслуговує чотири округи Каліфорнії, США. Вона тестує сканери райдужної оболонки ока, щоб переконатися, що студентів випадково не залишили в автобусі, але дані випробування викликає занепокоєння щодо конфіденційності деяких експертів.

Експеримент у Каліфорнії стався в той момент, коли школи все частіше впроваджують технології для контролю за учнями задля їхньої безпеки. Сканери райдужної оболонки ока рідше зустрічаються в школах, але в багатьох штатах їх використовували як заміну студентських карток.

В аеропортах світу технологія розпізнавання райдужною оболонкою ока все ширше використовується для підвищення безпеки, зручності пасажирів і поліпшення ефективності роботи персоналу [1].

Порівняно новий додаток розпізнавання райдужної оболонки призначений не для пасажирів, що прибувають в аеропорт, а для тих, хто відбуває. Воно дозволяє для “Надійних пасажирів” (Trusted Travellers) прискорити проходження реєстрації та інших процедур, пов’язаних із безпекою польоту.

Унікальний додаток розпізнавання райдужної оболонки включає ретельну перевірку на наявність того чи іншого пасажира в контрольному списку WatchList, що містить інформацію про підозрілих, розшукуваних або висланих з країни осіб. Найбільша на сьогоднішній день інсталяція цієї програми розпізнавання райдужної оболонки, що використовує розподілену архітектуру під назвою IrisFarm [4].

Отже, розпізнавання райдужної оболонки ока – це автоматизований метод біометричної ідентифікації, який бере унікальні візерунки в кільцеподібній області навколо зіниці кожного ока. Це надзвичайно надійний і точний метод ідентифікації з дуже низьким рівнем помилкових збігів, порівняно з іншими системами біометричної ідентифікації. Оскільки підтвердження особистості пасажира за результатами сканування райдужки, вимагає параметру – точність визначення. Помилки можуть траплятися з вірогідністю 1 до 2 мільйонів, в той час як сканування відбитку пальця – лише до 100 000. Тобто під час використання даної системи в галузі пасажирських перевезень, проблеми з помилковою ідентифікацією будуть виникати не так часто, порівняно з іншими біометричними методами ідентифікації пасажирів.

Також метод ідентифікації пасажира за райдужною оболонкою ока, дозволяє зчитувати оболонку з відстані до 150 см, та не потребує прямої

взаємодії з особою, яку перевіряють. До того ж, наявність інфрачервоного підсвітлення дозволяє зчитувати біометричні дані з оболонки ока, при одягнутих людиною сонцезахисних або оптичних окулярів, а також лінз, що в свою чергу, не створює для осіб необхідності додаткових маніпуляцій для здійснення зчитування оболонки ока. Розглянемо систему ідентифікацій особи за допомогою пристрою EyeLock. Швидкість зчитування такого сканера становить 50 осіб за хвилину, що становить 72000 осіб на добу [5]. Така висока швидкість розпізнавання є необхідною для більшості аеропортів, з великим потоком пасажирів. І наразі це найкраще рішення, враховуючи швидкість пропускання пасажирів та коефіцієнт помилок. Наразі технологія використовуються в аеропорту Дубаї в Об'єднаних Арабських Еміратах 6].

Висновки. Системи ідентифікації особи за райдужною оболонкою ока для пасажирського транспорту, збільшать швидкість обслуговування пасажирів, оскільки зникне необхідність реєстрації на рейс. Також призведе до запобігання можливим терактам або іншим правопорушення, що в свою чергу призведе до поліпшення транспортної безпеки. Наявні методики та пристрої сканування райдужної оболонки ока для використання в галузі пасажирських перевезень, дозволяють втілити в життя проєкт з впровадження системи ідентифікації особи за райдужною оболонкою ока в містах, де це наразі не впроваджено, без створень великих труднощів для пасажирів.

Інформаційні джерела

1. California school bus service eyes biometric technology for pupils: веб-сайт. URL: https: // www. eff. org / pages / iris-recognition (дата звернення: 04.11.2022).

2. Iris recognition systems for access control and identity management gain popularity: веб-сайт. URL: https: // www. eff. org / pages / iris-recognition (дата звернення: 04.11.2022).

3. Iris Recognition: веб-сайт. URL: https: // www. eff. org / pages / iris-recognition (дата звернення: 04.11.2022).

4. Methods for improving airport security and travel experience with iris recognition: веб-сайт. URL: https: // www. securityinfowatch. com / critical-infrastructure / article / 21281973 / methods-for-improving-airport-security-and-travel-experience-with-iris-recognition (дата звернення: 05.11.2022).

5. Биометрические системы распознавания радужной оболочки глаза EyeLock (4). URL:http://www.ualock.com/eyelock-usa.html(дата звернення: 4.11.2022).

Проходження контролю в аеропорту Дабаї. URL: https://www.dubaiairports.ae/ (дата звернення: 4.11.2022).

УДК 004.67

ОБГРУНТУВАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ ЩОДО МАТЕРІАЛЬНОГО ЗАБЕЗПЕЧЕННЯ СПЕЦІАЛІЗОВАНИХ ФОРМУВАНЬ

Богдан Кокотко[1], Олександр Придатко[2], Роман Головатий[2]

[1]IT-компанія Scanmarket, м. Копенгаген, Данія
[2]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *Мова йде про створення системи підтримки прийняття рішень на основі отримання і агрегації даних для оптимізації процесів оперативного управління ресурсного забезпечення спеціалізованих формувань.*

Ключові слова: *спеціалізовані формування, управління процесами, пейперлес, хмарні технології, агрегація даних, прийняття рішень.*

Abstract. *We are talking about the creation of a decision-making support system based on the acquisition and aggregation of data to optimize the processes of operational management of food resources of specialized formations.*

Keywords: *specialized formations, process management, paperless, cloud technologies, data aggregation, decision-making.*

Сучасні умови логістичного та ресурсного управління спеціалізованими формуваннями потребують постійної роботи із великими об'ємами даних. Нажаль, процедура обробки даних, зазвичай, здійснюється вручну, а максимальний прогрес щодо автоматизації цих процесів досягнув лише рівня використання пакетів офісних прикладних програм. Ручне або напівавтоматичне оброблення великого обсягу даних може зумовлювати до виникнення помилок, створює низку проблем пов'язаних з неточністю опрацювання даних, зумовлює повторні перерахунки тощо. Якщо розглядати сектор ресурсного забезпечення оперативних формувань, то додатковою характеристикою таких даних – динамічність. До прикладу складське приміщення служби продовольчого забезпечення протягом доби має надходження низки нових даних – нові надходження, облік використаного, терміни зберігання, накладні витрати та багато іншого.

Актуальним прикладом потреби у автоматизації процесів обробки великих масивів даних є потреба у підготовці тижневих або щомісячних звітів стосовно використання ресурсів, їх кількості, цінності чи витрат на

прикладі продовольчих товарів. Власне обробка та отримання таких даних за умови великої кількості вхідних параметрів буває вкрай ускладненою. Підтримка подібних процесів у традиційному форматі є вкрай громіздкою та повільною, що може спричинити до втрати актуальності отриманого результату.

У світлі поставлених проблем варто розглянути впровадження системи прийняття рішень (надалі СПР) з побудовою зручного людинно-машинного інтерфейсу який дозволить здійснювати керування відповідними процесами матеріального забезпечення. СПР не мають загальноприйнятого визначення так як їх конструкція залежить від поставлених задач. Використання СПР, в першу чергу, дозволить автоматизувати низку процесів, а інші радикально спростити – ввід, підтримка та моніторинг даних і формування відповідних звітів.

На першому етапі розробки планується реалізація прототипу системи підтримки прийняття рішень щодо організації продовольчого забезпечення на базі Львівського державного університету безпеки життєдіяльності. За умови ефективної реалізації системи, буде можливе її подальше масштабування на інші спеціалізовані формування України шляхом агрегації унікальних даних в межах одного сервісу. Звичайно, що масштабування системи потребуватиме розробки додаткових модулів залежно від специфіки функціонування підрозділу.

Важливо відмітити, що розробка таких систем стає не лише актуальною, а й доступною через популяризацію IT технологій та все більш активного їх поширення. На даний час існує великий стек технологій із необмеженим доступом, що дозволяє їх використання з метою реалізації прикладних завдань аналітики великого обсягу даних. Здебільшого розробка подібних систем підтримки прийняття рішень не потребує великих фінансових затрат, лише розробки архітектури системи та її імплементації.

На початковому етапі програмної реалізації системи достатньо залучення невеликої команди розробників у кількості 2 – 3 особи. Таким чином без затрат додаткових ресурсів, на початкових етапах розробки можна буде активно використовувати філософію підходу до розробки програмних систем “fail fast, move/learn faster”. Така система може бути реалізована за клієнт-серверною архітектурою із використанням однієї мови програмування (до прикладу Javascript). Оптимізація роботи системи можлива за рахунок використання низки поширених фреймворків на різних рівнях представлення даних, а також існуючих прикладних програмних інтерфейсів (API) та прикладних інтерфейсів користувача та хмарних серверах.

В кінцевому випадку користувачі системи матимуть доступ на різних пристроях у будь який час. В систему також пропонується інтеграція процесів синхронізації клієнтських операцій з серверною частиною після тимчасової втрати з'єднання (до прикладу після відключення електропостачання). За умови відновлення з'єднання клієнтської частини із серверною, відбудеться автоматична синхронізація даних та звітів без додаткових маніпуляцій користувача.

Однією з основних задач при реалізації системи буде формування належної архітектури даних для їх зручного отримання, оновлення та оброблення. Дані мають володіти варіативністю та зручною конфігурацію. Код на стороні клієнта (інтерфейс користувача) має будуватись таким чином, щоб бути незалежним від програмної реалізації на серверній чи хмарній частині із можливістю його майбутньої міграції на інші сервіси. В свою чергу при відповідній підтримці таких систем в режимі реального часу можна володіти актуальними даними для прийняття ефективних рішень і оптимізації управлінських процесів.

Наукова актуальність розробленої системи полягатиме у розробці нових методів отримання та документування управлінських рішень та побудові на їх основі ефективних алгоритмів аналітики великих даних і підтримки прийняття рішень. Наприклад в розробленій системі буде вирішена проблема щодо виведення великих обсягів даних для їх порівняння в межах єдиної сторінки, на прикладі таблиці, з десятками тисяч комірок без значної втрати швидкодії (мова йде про клієнтську сторону, а не big query чи big data).

Інформаційні джерела

1. Martyn Ye. Software for Shelter's Fire Safety and Comfort Levels Evaluation / Martyn Ye., Smotr O., Burak N., Prydatko O., Malets I. // Communications in Computer and Information Science, Springer, Cham. – Vol. 1158, 2020. pp. 457-469 https://doi.org/10.1007/978-3-030-61656-4_31 (Scopus)

2. Kordunova, Y., Prydatko, O., Smotr, O., Golovatyi, R. Expert Decision Support System Modeling in Lifecycle Management of Specialized Software. Lecture Notes on Data Engineering and Communications Technologies, Springer, Switzerland. Vol. 149, 2022, pp. 367–383, https://doi.org/10.1007/978-3-031-16203-9_22 (Scopus)

3. Шопський О.М., Придатко О.В., Малець І.О. Аналітика великих масивів даних для прогнозування ризикових ситуацій. Проблеми використання інформаційних технологій в освіті, науці та промисловості : матеріали 16 Міжнародної конференції 15.12.2021. – Дніпро, НУ "ДП", 2021. – С. 212–214.

УДК 004.42

ВЕБ-РОЗРОБКА "BUSINESS INTELLIGENCE" ЗАСОБІВ

Олександр Мантуленко[1], Ольга Бабаджанова[2]

[1]Львівський національний університет імені Івана Франка, м. Львів, Україна
[2]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *Веб-додаток (BI-застосунок) створено з використанням бібліотеки React.js та ряду певних модулів (встановлені за допомогою node package manager безпосередньо під час розробки додатку), за допомогою яких можна розширити функціонал програми певними готовими рішеннями (наприклад, додати можливість використання різних видів графіків до додатку, або стилізовані компоненти select та інші).*

Ключові слова: *веб-додаток, BI-застосунок, бібліотека React.js.*

Abstract. *Web application (BI-tool) was created using library React.js and list of modules (they were installed using node package manager during of development of app), for the help of which it is possible to expand the functionality of the program with ready-made solutions (for example, to add the possibility to display different types of graphics or styled components select, etc).*

Keywords: *Web application, BI-tool, library React.js.*

Терміни "Business Intelligence" (BI) та "бізнес-аналітика" найчастіше використовуються як синоніми, але між ними є різниця. Бізнес-аналітика (у вузькому розумінні), на відміну від BI, має справу з уже очищеними, підготовленими для аналізу даними, використовує статистичні та кількісні інструменти для оцінки поточної ситуації та прогнозування, тому її все частіше називають "поглиблена аналітика".

Business Intelligence спочатку займається очищенням, консолідацією даних, перетворенням їх у зручний для аналізу формат, її завдання − інтерпретувати велику кількість даних, загострюючи увагу лише на ключових факторах, які впливають на ефективність, моделювати результат різних варіантів дій, відстежувати результати прийняття рішень. Основне призначення BI − це саме прийняття рішень для бізнесу.

BI підтримує прийняття безлічі бізнес-рішень − від операційних до стратегічних. Основні операційні рішення включають в себе позиціонування продукції або цін на неї. Стратегічні бізнес-рішення включають в себе пріоритети, цілі і напрямки. BI-система найбільш ефективна, коли

вона об'єднує дані, отримані з ринку, на якому працює підприємство (зовнішні дані), з даними з джерел на підприємстві, такими як фінансові та виробничі (внутрішні дані). У поєднанні зовнішні і внутрішні дані дають повнішу картину бізнесу, тобто аналітику, яку не можна отримати в результаті аналізу даних тільки від одного з цих джерел [1].

BI-системи розвиваються за чотирма основними напрямками:

− Збереження даних. Дані в сховищі BI-системи (data warehouse, DW) структуруються спеціальним чином для більш ефективного аналізу і обробки запитів (на відміну від звичайних баз даних, де інформація організована таким чином, щоб оптимізувати час обробки поточних транзакцій).

− Інтеграція даних. Для формування і підтримки сховищ даних використовуються ETL-засоби − інструменти, які забезпечують отримання даних (extract), їх перетворення (transform), тобто приведення до необхідного формату, і завантаження (load) даних в сховище або в іншу базу.

− Аналіз даних. Для всебічного аналізу даних використовуються OLAP-інструменти (on-line analytical processing). Вони дозволяють розглядати різні зрізи даних, виявляти тренди і залежності (за регіонами, продуктами, клієнтами тощо).

− Представлення даних. Для представлення даних використовуються різні графічні засоби − звіти, графіки, діаграми. Загальноприйнятим засобом візуалізації даних є інформаційні панелі (dashboards), на яких результати відображаються у вигляді індикаторів і шкал, що дозволяють контролювати поточні значення вибраних показників, порівнювати їх з мінімально/максимально допустимими і таким чином виявляти потенційні загрози для бізнесу.

Для реалізації власного BI-застосунку обрали бібліотеку React.js (використовувалися мова розмітки html, стилі css, мова javascript), яка є досить популярною та зручною для створення веб-додатків [2]. В основному дана бібліотека використовується у поєднанні з іншими технологіями, наприклад – node.js (використовується для написання серверної частини додатка), але в даному випадку вистачило лише одного React-у.

React – JavaScript-бібліотека є для створення користувацьких інтерфейсів. React спрощує створення інтерактивних інтерфейсів. Декларативні інтерфейси роблять код більш передбачуваним і його набагато легше налагоджувати. За допомогою React.js ми можемо створювати інкапсульовані компоненти, які керують власним станом, а з них можемо побудувати складні інтерфейси. Оскільки логіка компонентів написана на JavaScript,

замість шаблонів з легкістю можна передавати складні дані у додатку і зберігати стан окремо від DOM.

Однією з особливостей React є віртуальний DOM. Він дозволяє бібліотеці визначити, які частини DOM змінилися, порівняно зі збереженою версією віртуального DOM, і таким чином визначити, як найефективніше оновити DOM браузера. Таким чином програміст працює зі сторінкою, вважаючи що вона оновлюється вся, але бібліотека самостійно вирішує які компоненти сторінки треба оновити.

Було створено три різні сторінки, на яких є можливість переглянути усі дані з обраного файлу формату csv, а також побудувати графіки різних типів (barplot, line plot, areaplot) на основі цих даних. Графік будується за допомогою компоненти <Chart>, яку ми створили власноруч. Дана компонента знаходиться у каталозі componentsy файлі Chart.js. Для побудови графіків нам знадобиться модуль Recharts [3].

Для того щоб знайти основні характеристики даних, такі як мода, медіана, кореляція, квартилі та інші, реалізували ряд функцій в окремому файлі (у даному файлі реалізована одна функція – Reacthook, всередині якої і описані усі наші функції). Усі ці характеристики помістили у таблицю, в якій можна переглянути результати (дана таблиця є аналогом результату методу description бібліотеки pandas у мові python). За допомогою графіків можна обрати потрібні нам дані, і після цього подати їх у зручному для сприймання вигляді, обравши відповідний тип графіка.

Один з мінусів цього веб-застосунка – для того, щоб завантажити файли з великою кількістю даних (файли розміром більші за 10 Мб) може знадобитися деякий проміжок часу, і під час переходів між сторінками додатку можуть бути зависання на декілька секунд. Для того, щоб посортувати дані великих об'ємів за певним стовпцем, знадобиться деякий час. Найкраще дана програма справляється з файлами невеликих розмірів.

За допомогою barplot можна побудувати досить інформативні графіки з декількома колонками, які йдуть по осі Y (наприклад, мінімальна та максимальна ціна долара за місяць).

Інформаційні джерела

1. BI – бізнес-аналітика. Retrieved from: https://www.it.ua/knowledge-base/technology-innovation/ business-intelligence-bi

2. Офіційна документація бібліотеки React. Retrieved from: https://ru.reactjs.org/

3. Використання модуля Recharts. Retrieved from: http://recharts.org/en-US/api

УДК 004.42

ЧАТ-БОТИ ЯК ЗАСОБИ СПІЛКУВАННЯ ІЗ КОРИСТУВАЧЕМ

М. Недільська, О. Суринович

Луцький національний технічний університет, м. Луцьк, Україна

Анотація. *В статті проаналізовано чат-боти як засоби спілкування із користувачем. Розглянуто значення чат-бота, виділено їх основні види (за алгоритмом роботи, за форматом взаємодії, за цілями застосування). Зазначено основні переваги чат-ботів. Розглянуто принцип роботи чат-бота.*

Ключові слова: *чат-бот, види чат-ботів, комунікація, Telegram, API месенджери.*

Abstract. *The article analyzes chat bots as a means of communication with the user. The meaning of a chat bot is considered, their main types are highlighted (by the algorithm of work, by the format of interaction, by the purposes of application). The main advantages of chat bots are indicated. The principle of operation of the chat bot is considered.*

Keywords: *chat bot, types of chat bots, communication, Telegram, API messengers.*

Постановка проблеми. Сучасний Інтернет є універсальним середовищем для спілкування, розваг та навчання. Спілкування через мережу стало невід'ємною частиною життя для багатьох людей. В даний час у світі існує безліч засобів, форм і способів спілкування, і чимала частина з них пов'язана з сучасними технічними можливостями, які, зокрема, представлені використанням глобальної комп'ютерної мережі.

Аналіз останніх досліджень і публікацій. Наукових досліджень, присвячених чат-ботам, існує незначна кількість. Вивчення процесу розробки чат-ботів та розмовних інтерфейсів здійснюється на основі матеріальної бази Сріні Джанарсанам. Тематика розробки чат-ботів у популярних месенджерах розкривається у книзі Сергія Гераськова "Доступний чат-бот. Як залучити та утримати клієнтів за допомогою WhatsApp".

Формулювання цілей дослідження. Метою роботи є створення класифікації чат-ботів за функціоальними особливостями. Завданнями роботи є: 1) проаналізувати значення та актуальність чат-ботів; 2) виявити основні види чат-ботів та їх особливості; 3) зазначити переваги чат-ботів; 4) визначити принцип роботи чат-бота.

Виклад основного матеріалу дослідження.

На сьогоднішній день чат-боти як сучасні інструменти комунікацій стали широко використовуватися в багатьох сферах життєдіяльності людини з метою встановлення контакту з користувачами мережі Інтернет. Найбільшу популярність чат-боти отримали, коли почалося їх використання в месенджерах і соціальних мережах (наприклад, в Telegram, Viber, Facebook).

Створювати чат-боти за допомогою API-месенджерів настільки просто, що це може зробити будь-який програміст-початківець. Для їх розробки використовують готові протоколи. У свою чергу, месенджери підтримують працездатність ботів за допомогою власних серверних потужностей.

У контексті нашого дослідження важливим є визначення поняття “чат-бот”. Під чат-ботом в загальному сенсі зазвичай розуміють спеціальну програму, яка здійснює інтернет-спілкування з одним чи з декількома користувачами, використовуючи штучний інтелект. Бот, скорочено від робот, – комп’ютерна програма, яка автоматично чи за певною заданою схемою виконує дії через ті ж інтерфейси, що й звичайний користувач.

Розробник та науковець В. Голіков називає чат-боти віртуальними співрозмовниками, які з’єднують користувача із сервером і розуміють набір команд чи мову людини [1].

Отже, аналізуючи зазначене, пропонуємо під поняттям “чат-бот” розуміти програму-помічник, що дозволяє комунікувати з користувачем за заздалегідь прописаним сценарієм.

Боти можуть виконувати практично будь-які завдання, які може робити кожен користувач акаунту Telegram з онлайн-сервісами. Роботи можуть вчити, розважати, шукати, транслювати, нагадувати, з’єднувати та підключатися до інтернету речей. По суті, боти – це такий собі зручний для людини інтерфейс роботи з різноманітними веб-службами [2].

Чат-боти можна класифікувати за наступними ознаками: алгоритм роботи, формат взаємодії та цілі застосування [3].

Залежно від алгоритму роботи чат-боти бувають обмежені та саморозвиваючі. Обмежені боти відповідають на конкретні запити користувачів за заздалегідь розробленим скрипту. Вони мають обмежену кількість відповідей.

Саморозвиваючі чат-боти – різновид ботів, які розробляються на основі штучного інтелекту (ШІ) і здатні розуміти суть бесіди та можуть вести “живу” розмову з користувачем. Даний вид боту з часом навчається і дає більш релевантні відповіді на запити користувача [3].

За форматом взаємодії з користувачем чат-боти поділяють на кнопкові, текстові і вбудовані (inline). Особливість кнопкових чат-ботів – спілкування з користувачем через кнопки з варіантами дій. Бот реагує на них, як на команди, і пропонує користувачеві уточнюючі кнопки або дає відповідь на поставлене запитання (рис. 1а). Даний тип чат-боту часто застосовують в месенджерах.

Найбільш функціональним видом віртуального співрозмовника вважають текстовий чат-бот. Комунікація з ним близька до людської, оскільки бот розпізнає запит, аналізує інформацію і підбирає для користувача необхідну відповідь (рис. 1б).

Вбудований (inline) чат-бот з’являється усередині діалогу в месенджері після виклику @нік бота і пропонує варіанти дій (рис. 1в). Inline bots використовують для пошуку локацій, замовлення їжі тощо [3].

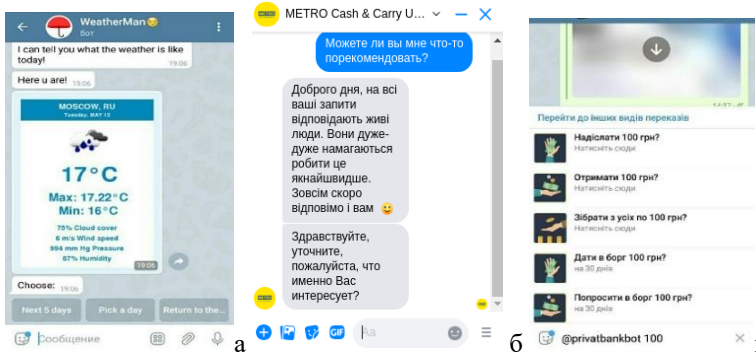


Рисунок 1 – Види чат-ботів: а – кнопкові, б – текстові, в – вбудовані

В залежності від цілей застосування chat bots бувають двох видів: комунікаційні та функціональні.

Комунікаційні боти забезпечують спілкування компанії з клієнтами. Серед основних функцій комунікативного чат-бота є:

– відповідь на запитання, які найчастіше задають користувачі;

– сповіщення та надсилання інформації про знижки, акції, спеціальні пропозиції;

– здійснення консультацій щодо надання сервісів та послуг;

– забезпечення зворотнього зв'язку.

Функціональний чат-бот є заміною повноцінного мобільного додатку. Віртуальний помічник надає можливість користувачам здійснювати пошук, резерв, замовлення товарів; бронювання авіа та залізничних квитків, житла, столиків в ресторані тощо; банківські операції [5].

Чат-боти мають низку переваг, зокрема ефективна взаємодія з користувачами, легкість у користуванні, простий і зручний доступ до інформації, кросплатформність, можливість автоматизувати рутинні дії, експериментувати з подачею матеріалу тощо [3].

Чат-боти можуть використовуватися для спілкування між користувачами, а також в розважальних, інформаційних цілях (чат-боти можуть повідомляти користувачу прогноз погоди, курс валют, записувати клієнта на прийом, здійснювати реєстрацію дзвінків) і в службах підтримки.

Більшість людей хоч раз зіштовхувалися з ботами та намагалися з ними поспілкуватися. Принцип роботи будь-якого чат-бота полягає в отриманні та виконанні команд (рис. 2). Скрипт, прописаний у боті, йде за певним циклом. Якщо користувач йде по закладеному скрипту, жодних проблем не виникає. Робот відпрацьовує запит та відповідає на запитання. Коли він не може знайти відповідь, в діалог вступає менеджер чи чат-бот пропонує користувачу залишити свій номер телефону.

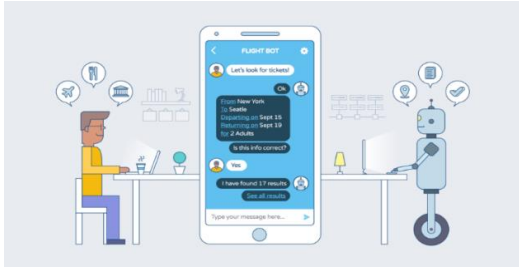


Рисунок 2 – Принцип роботи чат-бота

Сьогодні в Telegram працюють десятки роботів. Серед популярних Telegram-ботів є наступні:

– @ytranslatebot – перекладає ваші повідомлення на будь-яку мову світу. Працює як в особистих чатах, так і в групових.

– @ImageBot – відправте цьому боту ключове слово, і він знайде відповідне зображення.

– @HotOrBot – шукає нових знайомих у стилі програми для знайомств Tinder, у якій треба виставляти людям “подобається” або “не подобається”.

– @glavburgerbot – бот, який бере ваші координати та шукає найближчий заклад, де можна з’їсти бургер.

– @telerobot – виводить погоду, новини та цитати із сайту bash.im.

– @paypbbot – дозволяє клієнтам “Приватбанку” переказувати один одному кошти в месенджері Telegram [1].

Висновки. Використання чат-боту в наш час є досить ефективним та економічно вигідним у будь-якій сфері діяльності. На сьогоднішній день вони є різноманітними. Чат-боти можна класифікувати за наступними ознаками: алгоритм роботи, формат взаємодії та цілі застосування.

Інформаційні джерела

1. Чат-боти як інструмент для популяризації матеріалів ЗМІ. URL:https://science.lpnu.ua/sites/default/files/journalpaper/2021/may/23703/12.pdf

2. Що таке боти в сервісі Telegram та як ними користуватися. URL: https://techtoday.in.ua/news/shho-take-boti-v-servisi-telegram-ta-yak-nimi-koristuvatisya-64222.html

3. Все про чат-боти: типи і приклади, якому бізнесу підійде, список конструкторів для створення. URL: https://web-promo.ua/ua/blog/vse-o-chat-botah-tipy-i-primery-kakomu-biznesu-podojdet-spisok-konstruktorov-dlya-sozdaniya/

4. Чат-боти: хайп або ефективний бізнес-інструмент. URL: https://jam.in.ua/ua/blog/chat-boty-khajp-abo-efektyvnyj-biznes-instrument/

5. Яким чином використання чат-ботів впливає на ефективність введення бізнесу. URL: https://armedsoft.com/ua/blog/yakym-chynom-vykorystannya-chat-botiv-vplyvaye-na-efektyvnist-vedennya-biznesu

УДК 004.056.5

КОГНІТИВНІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ В УМОВАХ РИЗИКУ

Olena Pavliuk[1], Наталія Лиса[2], Богдана Федина[3]

[1]Department of Distributed Systemsand Informatic Devices Silesia University of Technology Gliwice, Poland
[2]Національного університету "Львівська політехніка", м. Львів, Україна
[3]Української академії друкарства, м. Львів, Україна

Анотація. *Сучасний етап розвитку технологій управління слабо структурованими ієрархічними системами, виробничими процесами, фінансовими та ресурсними потоками ґрунтується на концепції оперативно-командного діалогу з різними рівнями пріоритетів при формуванні та прийнятті рішень.*

В умовах дії загроз і збурюючих факторів (як на технологічні процеси та і управляючі процеси), різко зростає важливість проблеми інформаційного та системного забезпечення прийняття рішень при формуванні стратегії координаційного управління в ієрархічній структурі.

Ключові слова: *інтелект, нейроструктура, оперативна діяльність, сенсор, ризик, надзвичайні ситуації, техногенні структури, прийняття рішень, управління, дані, інформація, когнітивна модель.*

Abstract. *The current stage of development of management technologies for loosely structured hierarchical systems, production processes, financial and resource flows is based on the concept of operational-command dialogue with different levels of priorities when forming and making decisions.*

In the conditions of threats and disturbing factors (both on technological processes and management processes), the importance of the problem of information and system support for decision-making in the formation of a coordination management strategy in a hierarchical structure is sharply increasing.

Keywords: *intelligence, neurostructure, operational activity, sensor, risk, emergency situations, man-made structures, decision-making, management, data, information, cognitive model.*

Актуальність. Сучасне виробництво – це складні інтегровані людино-машинні керовані системи. Стратегії управління для досягнення мети функціонування входять як в структуру автоматизованої системи управління (АСУ), так і в базу знань і нормативів професійних навиків оператора. В ієрархії забезпечення надійного функціонування системи АСУ перед оператором стоять задачі, які необхідно розв'язати на циклах поточного і термінального часу:

− контроль динамічного стану енергоактивних об'єктів АСУ-ТП;

− оцінка режимної ситуації енергогенеруючих об'єктів;

− формування координуючих дій для підтримки цільового функціонування системи (як в ручному так і автоматичному режимі) при відхилені від цільової траєкторії режиму функціонування;

− управління і регулювання технологічними процесами в нормальних режимах і надзвичайних ситуаціях (згідно нормативних вимог і цільового завдання зменшення шкідливих викидів).

Основні аспекти проблеми управління енергоактивними системами розглянуті у працях [1–5] щодо компонент інтелектуальної і операторської діяльності. Функції та роль когнітивної структури у процесі діяльності управлінського персоналу при прийнятті рішень у повній мірі не досліджені і проблема не розв'язана. Це робить цей напрям досліджень у подальшому актуальним.

Важливою є проблема обґрунтування можливості зменшення ризику (при дії збурень, інформаційних та ресурсних атак) прийняття неправильних цільових рішень оперативним персоналом в автоматизованих системах управління які функціонують в граничних режимах і в структуру яких входять енергоактивні об'єкти.

Метою досліджень є розроблення ефективної системи підтримки прийняття оперативних рішень в автоматизованих система управління в умовах ризику.

В умовах дій активних факторів впливу на структур енергоактивного об'єкта, потоки ресурсів які впливають на стан об'єкта, та інформаційних атак на процеси управління, оператор без відповідної спеціальної підготовки не може приймати адекватні рішення у стресових ситуаціях, так як необхідно виконати комплекс операцій інтелектуальної обробки даних про стан об'єкта.

При прийнятті оператором рішень в екстремальних умовах необхідно виконати наступні операції для розв'язання проблеми (оцінка ситуацій) вироблення цілі, декомпозиція задач, які мають інформаційний та когнітивний характер в умовах прийняття рішень

На основі проведеного аналізу, обґрунтовано вибір управлінських інтелектуальних та інформаційних операцій обробки потоків даних про стан об'єкта. Розроблено операційну модель виконання цілеорієнтованих управлінських рішень та реалізації дій (які виводять техногенну систему в цільову область режиму функціонування в умовах дії збурень і атак).

Вищезгадана проблема є комплексною. Вона включає системний, ресурсний, інформаційний та управлінський рівні. В проблему також входять задачі цілеорієнтованої поведінки персоналу (на психофізичному і когнітивному рівні аналізу ситуацій і прийняття рішень) в екстремальних умовах, ризиках, конфліктах. В комплексі ця проблема не розв'язана і тому є актуальною.

На структуру енергоактивного об'єкта та потоки ресурсів впливають дії активних факторів впливу та інформаційні атаки на процеси управління. Оператор без відповідної спеціальної підготовки не може приймати адекватні рішення у стресових ситуаціях, оскільки необхідно виконати комплекс операцій інтелектуальної обробки даних про стан об'єкта (рис. 1). [4].

При прийнятті оператором рішень в екстремальних умовах необхідно виконати наступні операції для розв'язання проблеми оцінки ситуації, ви-

роблення цілі, декомпозиції задач (які мають інформаційний та когнітивний характер в умовах прийняття рішень) (рис. 1):

1) *KVd* – відбір, обробка і оцінювання даних про стан об'єктів у структурі АСУ-ТП;

2) *KId* – інтерпретування даних, виділення їх змісту (на основі процедури класифікації у цільовому просторі системи згідно множини ознак режиму функціонування об'єктів);

3) *KRs* – визначення ступеня відхилення стану системи від цільового стану (і на основі визначених стратегій побудувати процедуру приймання управляючих рішень, тактик і планів командних дій);

4) $strat(U/Ci)$ – сформувати тактики плану командних дій (відповідно до стратегій управління для реалізації цільових задач);

5) обґрунтувати спосіб формування динамічних таблиць прийняття рішень (для планування послідовності командних цільових дій);

6) оцінити ризики управління в умовах дії загроз.

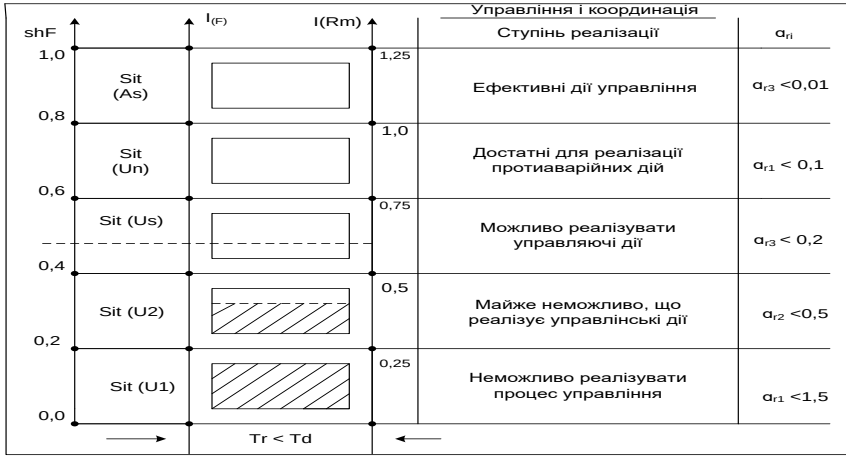


Рисунок 1 – Можливі стани та реалізації управлінських дій при дії активних факторів як при нечітких даних приводять до ризику – аварійної ситуації

Аналіз рівня системних і когнітивних ризиків при прийнятті рішень в складній техногенній системі в умовах дії активних факторів загроз та інформаційних атак.

Відповідно до структурно-функціональної схеми інформаційної технології формування управлінських рішень виділимо класи управлінських дій:

1. Інформаційні операції (процедури і методи обробки даних, статистики, формування образів ситуацій, методи оцінювання параметрів траєкторії, класифікації, змісту даних) та методи оцінки часових характеристик зміни траєкторій відносно цільової області;

2. Когнітивні операції (планування схеми процесу розв'язання цілеорієнтованих задач, інтерпретація та прогноз розвитку ситуацій відносно цілі формування управляючих дій, що виконуються на основі динамічних таблиць згідно стратегій і планів управління на термінальному циклі).

Для оцінки ризику формуємо:

– множину альтернативних рішень $A = \{A(U_{ij})\}$;

– множину траєкторій стану $M(Trak(X_i))$;

– лінії допустимих режимів $L(L_m, L_g, L_n)$;

– лінію аварійного режиму – L_A,

– множину інтелектуальних факторів впливу $M[I_K F_V]$;

– множину інформаційних факторів загроз $M[IF_{a,Z}]$;

– множину критеріїв для оцінки ризиків $M[K_i]$ та альтернативне розбиття простору допустимих станів.

Залежність ступеня реалізації управлінських і координаційних дій від факторів наведено на рис. 1.

Висновки. В роботі розглянута інформаційно-функціональна структура процедур вибору та планування дій управління в екстремальних ситуаціях.

Виконано:

1. Аналіз процесу виникнення кризових і конфліктних ситуацій;

2. Обґрунтовано постановка проблеми прийняття рішень і наведена структурна схема;

3. Обґрунтована схема ситуаційного управління;

4. Проаналізована причини виникнення загроз і кризових ситуацій;

5. Сформовано вимоги до процедур управлінських дій на основі системи моделі динамічного реагування;

6. Побудована схема динамічних шкал навантаження.

Інформаційні джерела

1. Зайцев В.С. Системный анализ операторской деятельности / В.С. Зайцев – М.: Радио и связь, – 1990. – 120 с.

2. Завалишина Д.Н. Психологічний аналіз оперативного мислення / Д.Н. Завалишина. – М.: Наука, – 1985. – 220 с.

3. Лурия А.Ф. Основы нейропсихологии / А.Ф. Лургия. – М.: Академия, – 2002. – 384 с.

4. Сікора Л.С. Когнітивні моделі та логіка оперативного управління в ієрархічних інтегрованих системах в умовах ризику / Л.С. Сікора. – Львів: ЦСД "ЕБТЕС", 2009. – 432 с.: схеми, табл.

5. Ткачук Р.Л. Логіко-когнітивні моделі формування управлінських рішень інтегрованими системами в екстремальних умовах: [посібник] / Р.Л. Ткачук, Л.С. Сікора. – Львів: Ліга-Прес, 2010. – 404 с.: схеми, табл., іл.

УДК 004.4: 338.48

СУЧАСНІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ТУРИЗМІ

Наталія Погуда

Харківський національний економічний університет ім. С. Кузнеця, м. Харків, Україна

Анотація. *Сучасні інформаційно-комунікаційні технології (ІКТ) відіграють вагому роль у сучасній цифровій економіці. ІКТ стають факторами конкурентоспроможності та сприяють покращенню ефективності підприємницької діяльності у туризмі. Такі ІКТ як VR, AR, Big Data, SaaS, хмарні технології забезпечують кращу комунікацію між усіма стейкхолдерами та сприяють виходу з локальних на глобальні туристичні ринки.*

Ключова слова: *інформаційно-комунікаційні технології, туризм, діджиталізація.*

Abstract. *Modern information and communication technologies (ICT) play an important role in the modern digital economy. ICTs become factors of competitiveness and contribute to improving the efficiency of business activities in tourism. Such ICT as VR, AR, Big Data, SaaS, Cloud technologies provide better communication between all stakeholders and contribute to the exit from local to global tourism markets.*

Keywords: *information and communication technologies, tourism, digitalization.*

Сучасний бізнес став активним учасником діджиталізації, тобто цифрових трансформацій, що викликані переходом від індустріалізації до епохи знань та сучасних технологій, в основі яких знаходяться інформаційно-комунікаційні та цифрові технології. Даний процес охоплює суспільство та економіку вже понад 50 років, однак саме події 2019 року стали, відповідно до Діаманту Портера, “випадком”, який хоч і досить негативно вплинув на усі сфери діяльності, у той же час, став поштовхом до активного використання сучасних ІКТ.

У більшості випадків щодо туристичної сфери, то дослідження процесів та наслідків діджиталізації зосереджені на питаннях інформаційно-комунікаційних технологій [1–3], їх недоліках та можливих ризиках [4]. Великий блок досліджень присвячений зв’язку діджиталізації та економічного розвитку країни, економічним моделям, що досліджують даний зв’язок, наприклад, TSAs and CGE моделі. Тобто актуальність дослідження не викликає сумніву, оскільки цифрові зміни відбуваються на всіх етапах роботи підприємств туристичної сфери та впливають на ефективну взаємодію усіх зацікавлених сторін.

Високотехнологічні галузі є дуже важливими для економіки, зокрема і економік країн Європейського Союзу. Тому велика увага приділяється підприємствам, що належать до таких галузей, так як вони є двигунами економічного розвитку такої країни, тим самим, забезпечуючи високу додану вартість та оплату працівників, зайнятих у таких сферах економіки. Відповідно до офіційних даних Євростату, майже 50 тис. підприємств, починаючи з 2014 року, працюють як високотехнологічному виробництві та навіть більше у високотехнологічному наукомісткому секторі послуг [6].

Цифрові трансформації відбуваються у всіх країнах світу, щоправда одні стають лідерами та новаторами, інші – обіймають за окремими позиціями кращі місця, а частина – країни, що в силу певних обставин, не можуть досягти позитивних результатів. Цифрові зміни демонструють тенденцію бізнесу використовувати сучасні ІКТ для підвищення ефективності підприємницької діяльності та досвіду роботи з клієнтом. Відповідно, використання таких технологій вже має певні наслідки [7]:

− У 2021 році на цифрову трансформацію було витрачено понад 1,5 трильйона доларів;

− До 2023 року прогнозується збільшення глобальних витрат до 6,8 трлн доларів на цифрові зміни;

− За допомогою впровадження цифрових технологій відбувається підвищення ефективності роботи (40%), прискорюється процес виходу на ринок (36%) та сприяє задоволенню очікувань клієнтів (35%);

− Галузі, які найімовірніше успішно адаптуються до цифрової трансформації, це послуги (95%), фінансові послуги (93%) та охорона здоров'я (92%);

− Очікується, що витрати на ринку цифрової трансформації зростуть на 19,1% протягом наступних п'яти років.

У розрізі розмірів підприємств, то також існують відмінності у використанні сучасних ІКТ. Зокрема, великі підприємства частіше впроваджують нові технології у порівнянні з малими та середніми (МСП). Наприклад, програмне забезпечення для планування ресурсів підприємства (ERP) у великих підприємствах становить 81%, у малих і середніх – 37%. Робота з соціальними мережами більш притаманна великим підприємствам (61%), МСП – 28%. Продаж онлайн здійснюють майже 40% великих підприємств, у той же час, МСП продають лише 18% [8].

Використання сучасних ІКТ перетворює ринки з локальних на глобальні. Розвиток ІКТ впливає на зростання індустрії подорожей і туризму в усіх напрямах бізнесу. По-перше, мультимедіа, як спосіб просування туристичної індустрії, наприклад Instagram, Facebook, ТікТок. По-друге, ІКТ можуть створювати фото, графічні проєкти (наприклад, 3D-тур), які є не-

обхідними туристичним постачальникам для реклами своїх продуктів. По-третє, використання GPS, за допомогою якого туристи знаходять місце призначення (наприклад, Google Maps), а також відстеження (для туристичних підприємств) різноманітних дій туристів за допомогою GPS і смартфону (з обов'язковим ознайомленням туриста про такі дії) [9].

Технології доповненої та віртуальної реальності за останні кілька років стали все більш доступними та широко використовуваними про, що свідчать наступні дані. Очікується, що до 2027 року глобальний ринок віртуальної реальності досягне 26,9 мільярдів доларів, а станом на 2022 рік обсяг ринку становить 7,72 мільярда доларів. Кількість VR користувачів лише у США налічує 57,4 мільйона користувачів, а AR – майже 91 мільйонів користувачів [7].

Віртуальна та доповнена реальність, технології великих даних, персоналізація, інтернет речей, програмне забезпечення як послуга (SaaS), онлайн-платформи, безконтактні та хмарні технології – це ті технології, за якими вважається буде розвиток майбутнього, у тому числі і туризмі.

Інформаційні джерела

1. BUHALIS, D. Strategic Use of Information Technologies in the Tourism Industry. Tourism Management.1998. № 19(3). 409–423.

2. O'Connor, P., & Murphy. J. Research on information technology in the hospitality industry. *International Journal of Hospitality Management*. 2004. № 23(5). 473–484.

3. Aramendia Muneta, M. E., & Ollo López, A. ICT Impact on tourism industry. *International Journal of Management Cases*. 2013. № 15 (2). 87–98.

4. Bayrakcı, S., & Özcan, C. C. Relationship Between ICT and Tourism: The Case of Mediterranean Countries. *ICT as Innovator Between Tourism and Culture*. 2022. 17 P.

5. Dwyer L., P. Forsyth, and R. Spurr. Evaluating Tourism's Economic Effects: New and Old Approaches. *Tourism Management*. 2004. Volume 25. 307–317.

6. Eurostat: official site. URL: https://ec.europa.eu/eurostat (дата звернення: 16.11.2022).

7. 37 Incredible Digital Transformation Statistics [2022]: Need-To-Know Facts On The Future Of Business. URL: https://www.zippia.com/advice/digital-transformation-statistics/ (дата звернення: 16.11.2022).

8. Digital Economy and Society Index (DESI) 2022. URL: https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022 (дата звернення: 16.11.2022).

9. How does ICT Impact in Tourism Industry? URL: https://www.waca.associates/en/growthhacking/kit-how-does-ict-impact-in-tourism-industry/(дата звернення: 16.11.2022).

Напрям 15

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

UDC 378.147:811.111:004.38:929

ALAN TURING: A FOUNDING FATHER OF COMPUTER SCIENCE, ARTIFICIAL INTELLIGENCE AND MODERN COGNITIVE SCIENCE

Roman Vlasiuk[1], Lyudmila Pet'ko[2]

[1]Department of Software engineering
Faculty of Mathematics, Informatics and Physics
Dragomanov National Pedagogical University, sity Kyiv,Ukraine
[2]Department of Foreign languages
Dragomanov National Pedagogical University, sity Kyiv, Ukraine

Annotation. *This paper is devoted to British mathematician and logician Alan Turing, who created and worked in the field of computer science. Described how was created a new field of computer science (artificial intelligence), especially Turing's achievements, what steps needed to be taken to do so, and how it affected our world. Turing's design for the Automatic Computing Engine (ACE) was the first complete specification of an electronic stored-program all-purpose digital computer.*

Keywords: *Alan Turing, probability theory, artificial intelligence, letters from Turing to Churchill, The Imitation Game (USA, United Kingdom, 2014).*

Анотація. *Стаття присвячена британському математику і логіку Алану Тюрінгу, який творив і працював у галузі інформатики. Описано як було створено нову галузь інформатики (штучний інтелект), наукові досягнення Тюрінга та як це вплинуло на наш світ. Наголошено, що проєкт Тюрінга для автоматичного обчислювального двигуна (ACE) був першою повною специфікацією універсального цифрового комп'ютера із збереженими електронними програмами.*

Ключові слова: *Алан Тюрінг, теорія ймовірностей, штучний інтелект, листи Тюрінга Черчілю, фільм "Гра в імітацію" (США, Великобританія, 2014).*

When a true genius appears in the world, you may know him by this sign:
that all the dunces are in confederacy against him
Jonathan Swift

Allan Turing was a founding father of artificial intelligence and of modern cognitive science, and he was a leading early exponent of the hypothesis that the human brain is in large part a digital computing machine. He theorized that

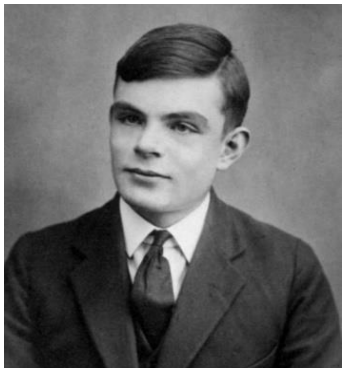


Fig. 1. Alan Turing, age 16 (1928)

the cortex at birth is an "unorganised machine" that through "training" becomes organized "into a universal machine or something like it". Turing proposed what subsequently became known as the Turing test as a criterion for whether an artificial computer is thinking (1950) [11] (Fig. 1), see the videos [4; 37].

Alan Turing, in full Alan Mathison Turing, (born June 23, 1912, London, England – died

June 7, 1954, Wilmslow, Cheshire), British mathematician and logician who made major contributions to mathematics, cryptanalysis, logic, philosophy, and mathematical biology and also to the new areas later named computer science, cognitive science, artificial intelligence, and artificial life. The son of a civil servant, Turing was educated at private Sherborne school (Fig. 2). He entered the University of Cambridge to study mathematics in 1931 (Fig. 3). After graduating in 1934, he was elected to a fellowship at King's College (his college since 1931) in recognition of his research in probability theory [11], see the video [2].

Fig. 2. Sherborne school (2022)

Fig. 3. University of Cambridge

Alan Turing was one of the most influential thinkers of the 20th century. In 1935, aged 22, he developed the mathematical theory upon which all subsequent stored-program digital computers are modeled [29], (see the video [5]).

In 1936 Turing's seminal

Fig. 4. Alonzo Church

paper "On Computable Numbers, with an Application to the Entscheidungsproblem (Decision Problem)" was recommended for publication by the American mathematical logician Alonzo Church (Fig. 4) [11]. In this paper, Turing reformulated Kurt Gödel's 1931 results (Fig. 5) on the limits of proof and computation, replacing Gödel's universal arithmetic-based formal language with the formal and simple hypothetical devices that became known as Turing machine [3, 38] (Fig. 6).

Fig. 5. Kurt Gödel (1926)

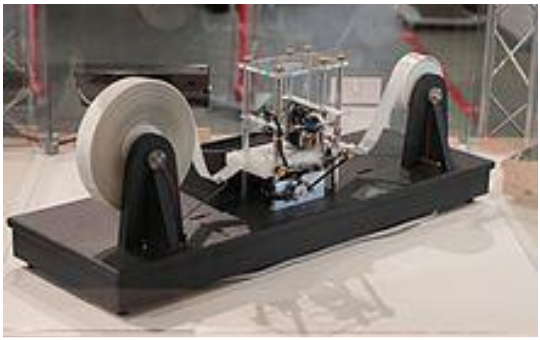


Fig. 6. The Turing machine [2]

The Entscheidungsproblem (German, "decision problem") is a famous problem in mathematics. David Hilbert (Fig. 7) formulated the problem in 1928: Is there an algorithm that will take a formal language, and a logical statement in that language, and that will output "True" or "False", depending on the truth value of the statement? The algorithm does not tell how it reaches the answer, nor prove if the answer is always correct [13].

Fig. 7. David Hilbert

Alonzo Church had himself just published a paper that reached the same conclusion as Turing's, although by a different method. Turing's method had profound significance for

the emerging science of computing. Later that year Turing moved to Princeton University to study for a Ph. D. in mathematical logic under Church's direction (completed in 1938) [11]

Turing Machine (Fig. 6) is extensively studied in *the Theory Of Automata* and was invented by Alan Turing in 1936, who called it an "a-machine" (automatic machine). It was Turing's Doctoral advisor, Alonzo Church later coined the term "Turing machine". Turing gave a brilliant demonstration that everything that can be reasonably said to be computed by a human computer using a fixed procedure can be computed by such a machine. Turing machines are similar to finite automata/finite state machines but have the advantage of unlimited memory. They are capable of simulating common computers; a problem that a common computer can solve (given enough memory) will also be solvable using a Turing machine, and vice versa. The Church-Turing thesis claims that any computable problem can be computed by a Turing machine [41].

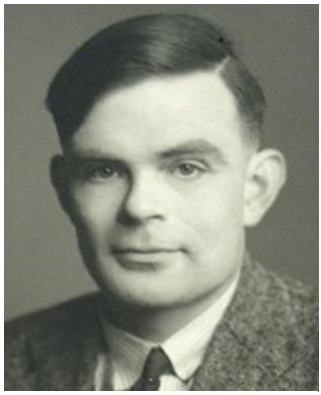


Fig. 8. Alan Turing

Alan Turing (Fig. 8) proved that his "universal computing machine" would be capable of performing any conceivable mathematical computation if it were representable as an algorithm. He went on to prove that there was no solution to the decision problem by first showing that the halting problem for Turing machines is undecidable: it is not possible to decide algorithmically whether a Turing machine will ever halt. John von Neumann (1903–1957) (Fig. 9) acknowledged that the central concept of the modern computer was due to Turing's paper. To this day, Turing machines are a central object of study in theory of computation [3].

Fig. 9. John von Neumann

After graduating from Cambridge and getting his PhD in mathematics from Princeton, Turing worked part-time for the Government Code and Cypher School, helping to decipher encrypted messages [42].

At the outbreak of hostilities with Germany in September 1939, Turing joined the

Fig. 10. Alan Turing reported to Bletchley Park, where he and a team of the best British scientists would work on breaking Enigma

Government Codebreaking team at Bletchley Park (Fig. 10), Buckinghamshire and played a crucial role in deciphering Enigma (Fig. 11), the code used by the German armed forces to protect their radio communications. Turing's work on the version of Enigma used by the German navy was vital to the battle for supremacy in the North Atlantic (the Enigma machine was used by Germans to code their military communications during World War II. British mathematician Alan Turing helped break the Enigma code), see the video [32].

Fig. 11. The Enigma machine

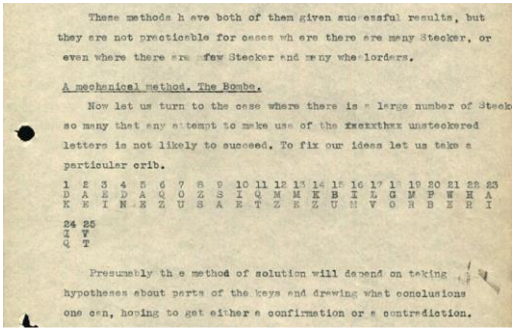
Fig. 12. Peter Twinn

In November 1939, Turing and his colleagues Peter Twinn (1916–2004) (Fig. 12), Gordon Welchman (1906–1985) (Fig. 13) and John Jeffreys (1916–1944) were convinced that the only way to decipher Enigma naval messages

would be “the machine now being made at Letchworth, resembling, but far larg er than, the Bombe of the Poles (superbombe machine)” (HW 14/2) (Fig. 15). Luftwaffe messages were not as intricately enciphered and would only require a normal bombe Many documents connected to Turing’s work during the Second World War were destroyed for the purposes of national security, and some, such as his two papers on statistical theory, “Statistics of Repetitions” and “The Applications of Probability to Cryptography” were only released in 2012 (!). Still, The National Archives holds important documents relating to Turing, from which much can be learnt [14].

Fig. 13. Gordon Welchman

Turing also contributed to the attack on the cyphers known as “Fish”, which were used by the German High Command for the encryption of signals during the latter part of the war. His contribution helped to shorten the war in Europe by an estimated two years (see the video [5]). After the war, his theoretical work led to the development of Britain’s first computers at the National Physical Laboratory and the Royal Society Computing Machine Laboratory at Manchester University. Turing was also a founding father of modern cognitive science, theorizing that the cortex at birth is an “unorganized machine” which through “training” becomes organized “into a universal machine or something like it”. He went on to develop the use of computers to model biological growth, launching



These methods h ave both of them given suc cessful results, but they are not practicable for cases wh ere there are many Stecker, or even where there are few Stecker and many wheelorders.

A mechanical method. The Bombe.

Now let us turn to the case where there is a large number of Steck so many that any attempt to make use of the xxxxthxx unsteckered letters is not likely to succeed. To fix our ideas let us take a particular crib.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
D A E D A Q O Z S I Q M M K B I L G M P W H A
K W I N Z U S A E T Z K Z U H V O H B E R I

24 25
I V
Q T

Presumably th e method of solution will depend on taking hypotheses about parts of the keys and drawing what conclusions one can, hoping to get either a confirmation or a contradiction.

Fig. 14. A crib in Turing’s Mathematical theory of ENIGMA

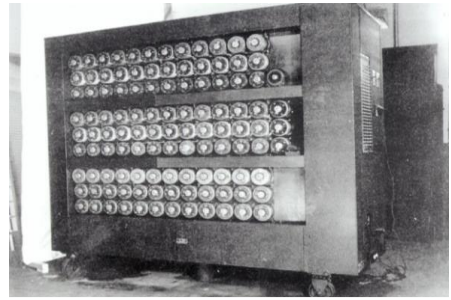


Fig. 15. The Bombe at Bletchley Park

the discipline now referred to as Artificial Life [29].

The Polish cryptologic bomb, designed by mathematician Marian Rejewski in 1938, had been built to mechanize the deciphering of German enigma-encoded messages. In 1939, the Poles had turned everything over to Britain and France, and it is their work that Turing and Welchman used to develop their own version of the machine [14] (Fig. 15), (see the video [28]).

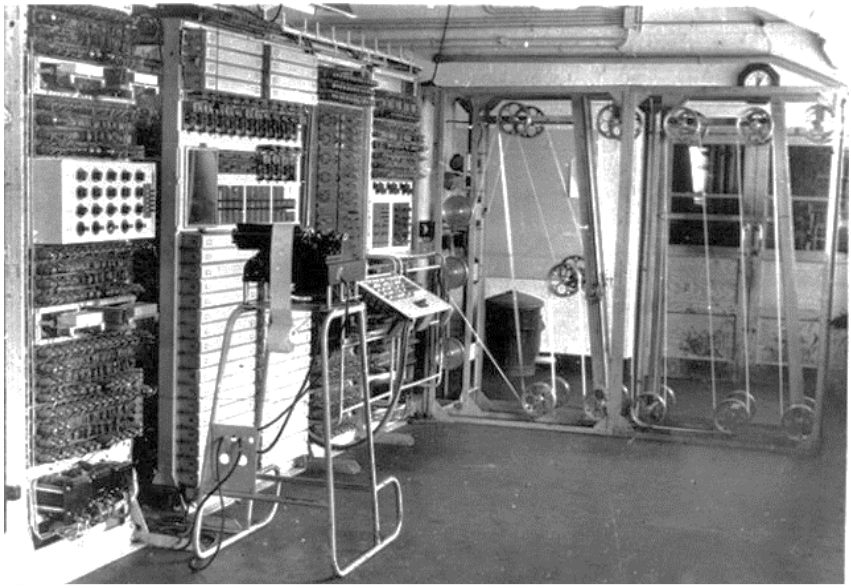


Fig. 16. The Colossus

Below an example of a crib in Turing's Mathematical theory of ENIGMA machine (Fig. 14).

Documents held at The National Archives also tell of other aspects of Turing's war. While he didn't design the Colossus (Fig. 16), the very first programmable digital computer, used to break to Lorenz cipher (codename: Tunny), his work on probability in cryptanalysis proved invaluable in the building of the machine [14], see the video [9, 16].

In July 1942, Turing developed a complex code-breaking technique he named "Turingery". This method fed into work by others at Bletchley in understanding the "Lorenz" cipher machine. Lorenz enciphered German strategic messages of high importance: the ability of Bletchley to read these contributed greatly to the Allied war effort.

Turing travelled to the United States in December 1942, to advise US military intelligence in the use of Bombe machines and to share his knowledge of Enigma. Whilst there, he also saw the latest American progress on a top secret speech enciphering system. Turing also spent some time designing codes as well as breaking them, and worked at Hanslope Park on "Delilah", a portable device that could encipher a voice message. Turing returned to Bletchley in March 1943, where he continued his work in cryptanalysis. Later in the war, he developed a speech scrambling device which he named "Delilah" [15] (Fig. 17).

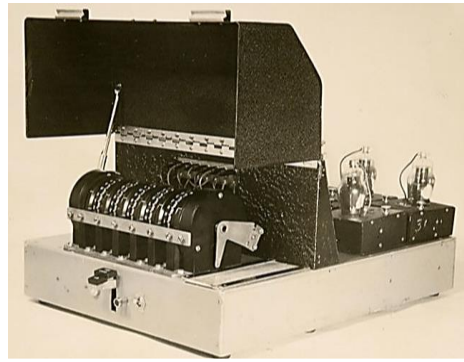
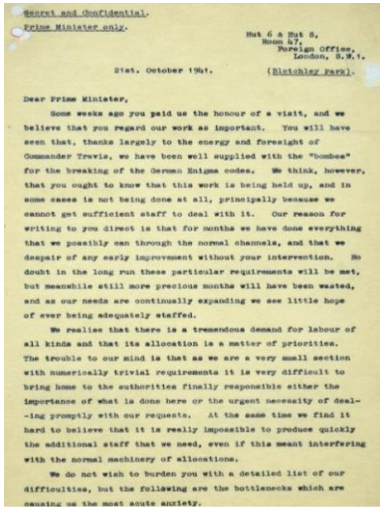


Fig. 17. Delilah code machine, 1946

In 1945, Turing was awarded an OBE for his wartime work.

Turing was a mathematical genius but, like the rest of us, he sometimes had to face more mundane problems. During 1941, codebreaking at Bletchley Park was hindered by shortages of typists and unskilled staff. These shortages could have been easily rectified, but the codebreakers urgent requests were ignored by officials in Whitehall. Going over the heads of those in command at GC & CS, Turing and his colleague Gordon Welchman (the head of Hut 6, responsible for breaking army and air force Enigma messages (Fig. 13) wrote directly to Prime Minister Winston Churchill: "*Work is being held up, and in some cases is not being done at all principally because we cannot get sufficient staff to deal with it.*" (Fig. 18).



Secret and Confidential.
Prime Minister only.

Hut 6 & Hut 8,
Room 47,
Foreign Office,
London, S.W.1.

21st. October 1941. (Bletchley Park).

Dear Prime Minister,

Some weeks ago you paid us the honour of a visit, and we believe that you regard our work as important. You will have seen that, thanks largely to the energy and foresight of Commander Travis, we have been well supplied with the "bombes" for the breaking of the German Enigma codes. We think, however, that you ought to know that this work is being held up, and in some cases is not being done at all, principally because we cannot get sufficient staff to deal with it. Our reason for writing to you direct is that for months we have done everything that we possibly can through the normal channels, and that we despair of any early improvement without your intervention. No doubt in the long run these particular requirements will be met, but meanwhile still more precious months will have been wasted, and as our needs are continually expanding we see little hope of ever being adequately staffed.

We realise that there is a tremendous demand for labour of all kinds and that its allocation is a matter of priorities. The trouble to our mind is that as we are a very small section with numerically trivial requirements it is very difficult to bring home to the authorities finally responsible either the importance of what is done here or the urgent necessity of dealing promptly with our requests. At the same time we find it hard to believe that it is really impossible to produce quickly the additional staff that we need, even if this meant interfering with the normal machinery of allocations.

We do not wish to burden you with a detailed list of our difficulties, but the following are the bottlenecks which are causing us the most acute anxiety.

Fig. 18. First page of the letter to Churchill, 21 October 1941

On receiving the letter Churchill minuted his Chief of Staff, General Ismay: "action this day Make sure they have all they want on extreme priority and

report to me that this had been done." It fell to Stuart Milner-Barry of Hut 6 to deliver the letter by hand to 10 Downing Street.

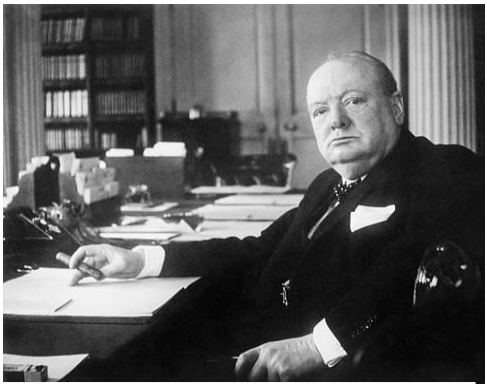


Fig. 19. Winston Churchill at his desk working at Number 10 Downing Street, 1941

Churchill's response was swift. He noted: "*Make sure they have everything they want on extreme priority and report to me that this has been done*". (Fig. 19, 20).

In 1986, Milner-Barry recalled his trip to Whitehall: "Why I was deputed to carry the letter to No. 10 I do not remember – at a guess, because I was the most readily expendable from the scene of action. What I do recall is arriving at Euston Station, hailing a taxi, and with a sense of total incredulity (can this really be happening?) inviting the driver to take me to 10 Downing Street. The taxi-driver never blinked an eyelid: without comment he directed himself to Whitehall. Arrived at the entrance to Downing Street, I was again surprised at the lack of formality: there was just a wooden barrier across the road, and one uniformed policeman who waved my driver on. At the door to No. 10 I paid off the taxi, rang the bell, was courteously ushered in, explained that I had an urgent letter which I was anxious to deliver to the Prime Minister personally, and was invited to wait. Of course I did not see the Prime Minister himself; but very shortly there appeared a dapper dark-suited figure of shortish stature whom I subsequently identified as Brigadier Harvie-Watt, Mr. Churchill's PPS from 1941 to 1945. To him I again explained my errand; and while obviously and understandably puzzled as to who I might be and what this was all about, he

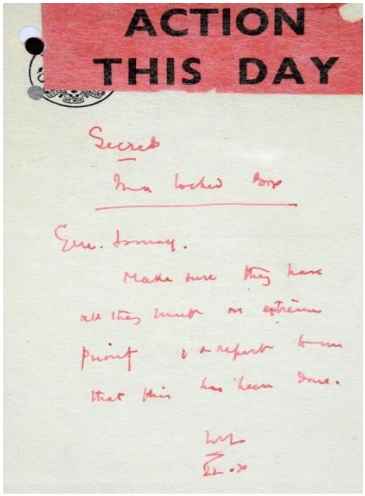


Fig. 20. Churchill's note, 22 October 1941

took me sufficiently seriously to promise that he would without fail deliver the letter to the Prime Minister and stress its urgency" [12]. (Fig. 21, 22).

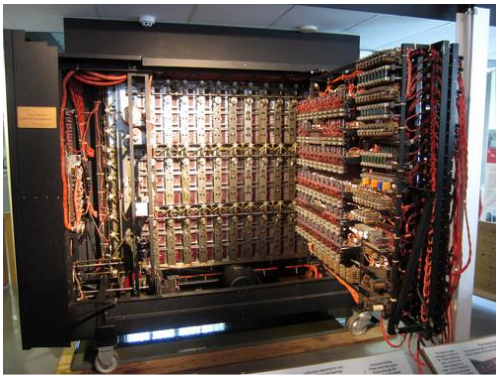


Fig. 21. The Turing machine at Bletchley Park

Let us remember the Oscar-buzzed movie "The Imitation Game" (2014) (see the film [30]) that tells the story of Alan Turing, the British cryptanalyst, who helped a great deal to solve the Enigma code used by the Germans during World War II (Fig. 22, 23, 26).

This movie is full of compelling scenes that demonstrate Turing's capacity to think on a higher level and his single-minded determination to crack the Enigma code, qualities that led to him be named the father of modern computer science. The film's message, repeated by its two main characters, is uplifting: Benedict Cumberbatch as Alan Turing.

Fig 22. The Imitation Game (2014). The Bombe

"Sometimes it is the people no one imagines anything of who do the things that no one can imagine" [14], see the video [43].

Alan Turing, who is the subject of "The Imitation Game", based on Andrew Hodges's excellent biography, "Alan Turing: The Enigma" (1983) [24].

Fig. 23. Decoded scene. Turing's team [32]

As his character points out in the film [30], it is often people's differences and peculiarities that lead them to make new discoveries, and this can be recreated with computers that "think" in a slightly different way. The movie is noteworthy for Benedict Cumberbatch's performance as Turing, which may not be completely true to life but is certainly moving, and realistically captures both the pressures of his role at

Bletchley Park and the personal pain felt because of his oppression [14] (Fig. 24, 25, 26, 27).

Turing's appearance on the big screen does give us an opportunity to discuss his extraordinary scientific and mathematical legacy, on which the movie is built (see the video [35]).

The term "imitation game" comes from a paper Turing written in 1960 called "Computing Machinery and Intelligence", where he asks "Are there imaginable digital computers which would do well in the imitation game?" Turing then goes on to describe a game that is really a test to determine if computers can actually think [40].

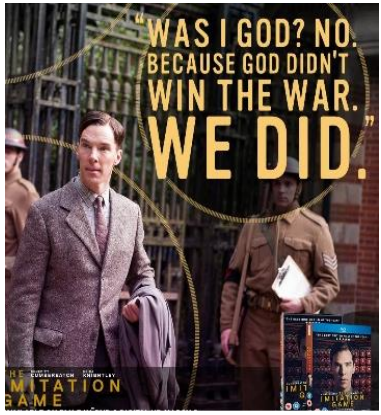


Fig. 24. Quotes from the movie

Fig. 25. Turing Turing was an atheist

On a literal level, the film's title relates to some of Turing's most important work, but it's at best peripheral to the film's plot. The term "imitation game" comes from a paper Turing wrote in 1960 called "Computing Machinery and Intelligence", where he asks "Are there imaginable digital computers which would do well in the imitation game?" Turing then goes on to describe a game that is really a test to determine if computers can actually think.

Fig. 26. The Bombe. "*The Imitation Game*" *(2014)*

Turing describes it as a simple party game involving three players. Player A is a man, player B is a woman and player C (who plays the role of the interrogator) is of either sex. Player C is unable to see either player A or player B, and can communicate with them only through written notes. By asking questions of

player A and player B, player C tries to determine which of the two is the man and which is the woman. Player A's role is to trick the interrogator into making the wrong decision, while player B attempts to assist the interrogator in making the right one.

A. Turing then argues that the game can prove the presence of (artificial) intelligence if a computer could take the role of Player A and make player C guess wrongly just as many times when an actual human being is sitting in for Player A. (Fig. 27, 28).

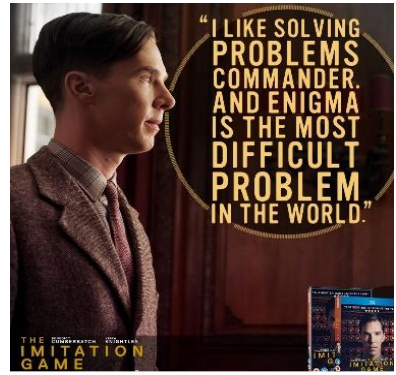


Fig. 27. Turing's motto in "The Imitation Game" (2014). in "The Imitation Game" (2014)

Fig. 28. Keira Knightley as Joan Clark

Examined more closely, one also could interpret the title as a metaphor for Turing's inability to truly understand and relate well to others. Perplexed by the tangled web of social interactions, intimations and subtext, Turing often discusses his difficulty with human interactions [40].

But in real life, the machine that cracked Enigma was called the Bombe (Fig. 15, 21, 29, 30), see the videos [7, 19]), and the first operating version of it was named Victory. The digital computer Turing invented was known as the Universal Turing Machine. Colossus (Fig. 16), the first programmable digital electronic computer, was built at Bletchley Park by engineer Tommy Flowers (see the video [16]), incorporating Turing's ideas [27].

Fig. 29. The bombe at Bletchley Park

Fig. 30. Bombe decryption machine

Manchester University's Computer Machine Laboratory.

The Manchester Mark I (Fig. 31) was built at Manchester University in 1946 under the supervision of Professor Max Newman. Alan Turing had previously been involved with the construction of the ACE (Automatic Computing Engine) at the National Physical Laboratory, and with the construction of "Colossus", the world's first electronic programmable computer, built at Bletchley Park, Buckinghamshire, during WW II.

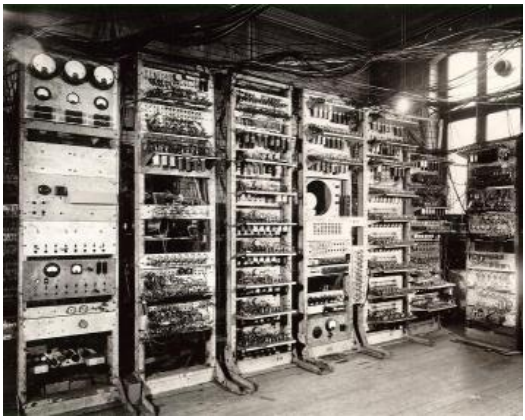


Fig. 31. The Manchester Mark 1 at working on the Ferranti Mark I Computer, 1951

After the War, Alan worked first at the National Physical Laboratory and then at Manchester University on the development of the computer from his first ideas in the early 1930s for a "Turing machine". And although the war work might have delayed Turing's academic work, it greatly accelerated progress in electronics, so that in 1945 he returned to his first love, creating a complete design for what he expected to be the world's first fully programmable computer, the National Physical Laboratory's ACE – the Automatic Computing Engine and then at Manchester University on the development of the computer from his first ideas in the early 1930s for a "Turing machine". Turing joined the Manchester team (Fig. 32), and again with remarkable prescience

Fig. 32. Alan M Turing and colleagues

started work on artificial intelligence, wondering whether electronic machines could be programmed not just to do Maths, but to think in the way human minds do – a hot topic of debate even now [37, 38].

Turing was elected a Fellow of the Royal Society in 1951. In the early 1950s he was developing a theory of morphogenesis, a mathematical theory of organic growth. The work was left incomplete when he died, on 8 June 1954, at his house in Wilmslow, Cheshire. His death at a time when official secrecy still hid his code-breaking work [17, 25], see the video [1].

Alan Turing (Fig. 33) has been identified not just as the father of computer science but as the father of the modern computer. This argument is strengthened by the fact that Turing was involved with the construction of an important computing device (the Bombe) used for decrypting the German Enigma code during World War II at Bletchley Park [18].

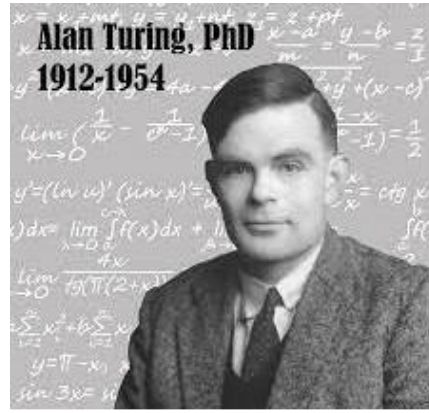


Fig. 33. Alan Turing: the man who changed history

The British genius also made key contributions to the British effort, during the Second World War, to crack the German Army's seemingly unbreakable *Enigma code*, an achievement that integrated mathematics, engineering, and a nascent effort in computer science, and which ultimately played a crucial role in shortening the war [26], see the video [34].

At last, we suggest you look the video where professor Jack Copeland discusses Alan Turing's impact on information technology. Turing is often considered to be one of the greatest minds in the 20th century, and Copeland looks at how many of Turing's ideas lie behind some of information technology's most fundamental theories [39].

Alan Turing is often remembered as the founding father of artificial intelligence. The A.M. Turing Award was created to honor his great work and is frequently referred to as the computer science equivalent of the Nobel Prize.

References

1. Alan Turing. A Genius With A Complex Personal Life. URL: https://www.youtube.com/watch?v=MidJR581irA

2. Alan Turing – Celebrating the life of a genius. URL: https://www.youtube.com/watch?v=gtRLmL70TH0

3. Alan Turing. Math & Physics Club. June 23, 2020. URL: https://mnp-club.github.io/blog/turing/

4. Alan Turing Test – artificial intelligence. URL: https://www.youtube.com/watch?v=HZ7SYI7woJc

5. Alan Turing: The Scientist Who Saved The Allies. URL: https://www.youtube.com/watch?v=XGqbieVcjPU

6. Bell Mark. The Applications of Probability to Cryptography (Part 1). *The National Archive*. Friday 24 April 2020. URL: https://blog.nationalarchives.gov.uk/the-applications-of-probability-to-cryptography-part-1/

7. Bombe Demonstration at Bletchley Park. URL: https://www.youtube.com/watch?v=Dr1U7Bva6Sw

8. Codebreaker: Newburyport's Gordon Welchman at Bletchley Park. URL: https://www.youtube.com/watch?v=SS7w6kvsgP4

9. Colossus – The Greatest Secret in the History of Computing. URL: https://www.youtube.com/watch?v=g2tMcMQqSbA

10. Copiland B. J. Alan Turing 1912–1954. URL: https://academic.oup.com/book/42030/chapter-abstract/355741855?redirectedFrom=fulltext

11. Copiland B. J. Alan Turing. British mathematician and logician. URL: https://www.britannica.com/biography/Alan-Turing/Computer-designer

12. Copiland B. J. Letter to Winston Churchill (1941). URL: https://academic.oup.com/book/42030/chapter-abstract/355745477?redirectedFrom=fulltext

13. Entscheidungsproblem. URL: https://simple.wikipedia.org/wiki/ Entscheidungsproblem

14. Fulton Liz, Desplat Juliette. The Archivists' Guide to Film: The Imitation Game. *The National Archive*. Wednesday 20 May 2020. URL: https://blog. nationalarchives.gov.uk/the-archivists-guide-to-film-the-imitation-game/

15. How Alan Turing Cracked The Enigma Code. URL: https://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code

16. IEEE Computer: Alan Turing at Bletchley Park. URL: https://www.youtube.com/watch?v=5nK_ft0Lf1s

17. Legacy Of Alan Turing – Episode TW. BBC. *Sounds.* Released on: 25 Jun 2012. URL: https://www.bbc.co.uk/sounds/play/p00tgvl9 Text: https://www.bbc.com/news/science-environment-18561092

18. On This Day… *Roal Signals Museum*. November. URL: https://www.royalsignalsmuseum.co.uk/on-this-day-12th-november/

19. Output: how Bletchley Park's Bombes worked to break Enigma. URL: https://www.youtube.com/watch?v=LH2H7v4HTJ4

20. Pet'ko Lyudmila. Developing students' creativity in conditions of university // Research: tendencies and prospects: Collection of scientific articles. – Editorial Arane, S.A. de C.V., Mexico City, Mexico, 2017. P. 272−276.

21. Pet'ko L. Multicultural upbringing of students and the formation of professionally oriented foreign language teaching environment // Perspectives of research and development: Collection of scientific articles. – SAUL Publishing Ltd, Dublin, Ireland, 2017. P. 164−170.

22. Pet'ko L. V. Teaching methods and the formation of professionally oriented foreign language learning environment in conditions of university. *Intellectual Archive.* Toronto: Shiny Word Corp., Canada.2016. Vol. 5. No. 4 (July/August). Pp. 73–87.

23. Pet'ko L. V. Unity of teaching and upbringing in the formation of professionally oriented foreign language teaching environment / L.V.Pet'ko // Science and practice: Collection of scientific articles. – Thorpe Bowker. Melbourne, Australia, 2016. P. 303–307. URL: http://enpuir.npu.edu.ua/handle/123456789/11892

24. Pet'ko L., Dryha I. The higher education in the focus of modern educational technologies // World scientific extent: Collection of scientific articles. – Agenda Publishing House, Coventry, United Kingdom, 2017. P. 415–419

25. Pease Roland. Alan Turing: Inquest's suicide verdict 'not supportable'. *News.* 26 June 2012. URL: https://www.bbc.com/news/science-environment-18561092 sound: https://www.bbc.com/news/science-environment-18561092

26. Rockmore Dan. What's Missing from "The Imitation Game". *The New Yorker*. Novemver 6, 2014. URL: https://www.newyorker.com/tech/annals-of-technology/ imitation- game-alan-turing

27. Tanzelmann Alex. The Imitation Game: inventing a new slander to insult Alan Turing. *The Guardian.* November 20, 2014. URL: https://www.theguardian. com/film/ 2014/nov/20/the-imitation-game-invents-new-slander-to-insult-alan-turing-reel-history

28. The Enigma of WWII codebreaker Alan Turing. URL: https://www.youtube. com/ watch?v= nEomYB94TTI

29. The Essential Turing / Ed. by Copiland B. J. Oxford University Press, 2004. URL: https://academic.oup.com/book/42030#login-purchase

30. *The Imitation Game* (USA, United Kingdom, 2014, Historical drama film directed by Morten Tyldum). URL: https://www.youtube.com/watch?v=8oMDSthscZQ *in English, with English subtitles*

31. *The Imitation Game* (USA, United Kingdom, 2014, Historical drama film directed by Morten Tyldum). URL: https://eneyida.tv/1949-gra-v-imitaciyu.html *in Ukrainian*

32. *The Imitation Game:* Alan Turing Cracked the Enigma Code. URL: https:// www.youtube.com/watch?v=mwFWMM9APLs

33. *The Imitation Game* (2014). Clip – Crossword Winner. URL: https://www. youtube.com/watch?v=QEvPL19I-Ds&t=35s

34. The Life and Death of Alan Turing. URL: https://www.youtube.com/watch?v= nCGF7QZvyTI

35. The Making of the Imitation Game. URL: https://www.youtube.com/watch?v=- WXVyjwuIok

36. The Turing Digital Archive. Kings College at Cambridge University. URL: https://turingarchive.kings.cam.ac.uk/about-alan-turing

37. The Turing test: Can a computer pass for a human? – Alex Gendler. URL: https://www.youtube.com/watch?v=3wLqsRLvV-c

38. Turing Mashine. URL: https://en.wikipedia.org/wiki/Turing_machine

39. Turing: Pioneer of the Information Age. URL: https://www.youtube.com/ watch?v=p7Lv9GxigYU

40. What Is The Significance Of The Film's Title& What Is "The Imitation Game". URL: https://the-take.com/read/what-is-the-significance-of-the-films-title-what-is-the-imitation-game

41. What are Turing Machines? Tech Radicals. July 20, 2020. URL: https://techradicals.wordpress.com/2020/07/20/what-are-turing-machines/

42. Göke Niklas. The Man Who Changed History Twice in a Single Moment. Meet Alan Turing. URL: https://medium.com/personal-growth/alan-turing-how-to-change-history-twice-in-a-single-moment-5cfdb47b8e8d

43. The Making of the Imitation Game. URL: https://www.youtube.com/watch?v=- WXVyjwuIok

УДК 378.14: 004.087

СУЧАСНІ ТЕНДЕНЦІЇ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ ПІДГОТОВЦІ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

Ірина Гелешко, Валентина Ящук

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *У роботі розглянуто теоретичні та науково-методичні напрями використання інформаційних технологій при підготовці спеціалістів з кібербезпеки. Окреслено інструментарій та визначено сучасні підходи до комплексу соціально-педагогічних перетворень, пов'язаних з насиченням освітніх систем інформаційною продукцією. Наведено методичні підходи до формування концепції та структури використання новітніх знань та технологій, що динамічно розвиваються у відповідності до потреб та вимог часу.*

Ключові слова: *інформаційні технології, фреймворк, технологія Django, ручне тестування, автоматизоване тестування, бізнес-аналіз.*

Abstract. *The theoretical and scientific-methodical directions of the use of information technologies in the training of cyber security specialists are considered. The toolkit is outlined and modern approaches to the complex of socio-pedagogical transformations associated with the saturation of educational systems with information products are defined. Methodical approaches to the formation of the concept and structure of the use of the latest knowledge and technologies, which are dynamically developing in accordance with the needs and requirements of the time, are given.*

Keywords: *information technology, framework, Django technology, manual testing, automated testing, business analysis.*

Інформатизація освіти являє собою в широкому розумінні комплекс соціально-педагогічних перетворень, пов'язаних з насиченням освітніх систем інформаційною продукцією, засобами й технологією, у вузькому – впровадження в заклади системи освіти інформаційних засобів, що ґрунтуються на мікропроцесорній техніці, а також інформаційної продукції і педагогічних технологій, що базуються на цих засобах. У науково-педагогічній літературі сутність інформатизації визначають, як створення сприятливих умов для викладачів і студентів щодо вільного доступу до значних об'ємів культурної, навчальної й наукової інформації у базах даних, електронних архівах, довідниках, енциклопедіях.

Навчальний процес сучасного навчального закладу має постійно вдосконалюватись, і це вдосконалення може відбуватися через активне використання інформаційних технологій. Аналіз досліджень українських учених з питань інформатизації освіти та підвищення ефективності навчально-виховного процесу дозволяє стверджувати, що ця проблема завжди

буде актуальною і потребуватиме вдосконалення у зв'язку зі стрімким розвитком інформаційних технологій.

Сьогодні не можна уявити освіту без використання інформаційних технологій. Сучасна освіта повинна бути повністю цифровою. Студенти та викладачі повинні вміти використовувати різні програми для навчання та роботи. Важливим особистісним аспектом якості освіти є формування навичок самостійності й креативності. Формування такої особистості є обов'язковою передумовою демократичного розвитку будь-якого суспільства та успішності сучасної економіки, що потребує відповідальності й активності. Для того щоб здобувачі вищої освіти могли ще в процесі навчання визначити, який саме вид діялфьності буде переважати в подальшому, потрібно під час навчання опанувати якомога більше різноманітних технологій.

Розглянемо деякі застосування, програми та методи, які, на нашу думку, повинні бути присутніми у навчальному процесі. Перший з них це фреймворк – Flutter, розроблений Google з відкритим програмним кодом, який дозволяє просто і швидко створювати мобільні додатки для iOS і Android. При цьому в роботі Flutter не використовує нативні компоненти зовсім. Замість цього всі UI-елементи у фреймворку створюються за допомогою власного графічного движка. Flutter дозволяє створювати всі елементи призначеного для користувача інтерфейсу додатку з готових віджетів.

Порівняльна характеристика використання фреймворків для розроблення мобільних додатків наведена в табл. 1

Таблиця 1

Порівняльна характеристика використання фреймворків

Порівняльна ознака	Flutter	React Native
Бібліотека віджетів	Порівняно незалежний від сторонніх бібліотек-елементів.	Має більшу власну бібліотеку UI-елементів.
Сумісність з конкретними платформами	Більш універсальний і широко застосовується.	Виявляється несумісним з деякими платформами.
Продуктивність	Перевершує по продуктивності, використовуючи повністю відмінний підхід до рендерингу. Створює власні віджети і використовує графічний процесор для рендеринга.	Не запозичує нативні компоненти з інших платформ.
Роззосередженість	Надає можливість зосередити зусилля розробника і всі фінансові ресурси виключно на функціональності самого мобільного додатка.	Роззосереджує зусилля розробника на інші другорядні процеси.

Далі опишемо технологію використання Django. Це відкрита програма для веб-розробок високого рівня, яка написана на Python. Це вільна рамка, яка допомагає працювати і створювати веб-сайт швидше і краще порівняно з іншими рамками, такими як Flask. Для створення веб-сайту потрібно інтегрувати безліч компонентів, потрібно обробляти автентифікацію користувача, наприклад, вхід та вихід з різними формами, панелями та завантаження локальних файлів тощо. Це надає набір готових компонентів у рамки. Ця рамка економить час та енергію від перезапису коду для кожного компонента з нуля та надає вбудовані функції. Додатковим стимулом до включення в освітні програми вивчення технології Django є той факт, що чимало популярних програм, а саме: Instagram, Spotify, YouTube, Mozilla FireFox, використовують Django Framework.

Після проходження курсу по тестуванню, студент матиме можливість ознайомитись з базою тестування, яка потрібна для підтвердження якості продукту, який він розробляє. Не менш важливим є те, що студент навчиться бути більш-уважним та спостережливим, навчиться аналізувати продукт і вносити свої ідеї у проєкт.

Ще одним методом, який, на нашу думку, повинен бути присутнім і навчальному процесі при підготовці фахівців з кібербезпеки є бізнес-аналіз – це набір методів, які допомагають зрозуміти структуру, особливості компанії клієнта, визначити її потреби і запропонувати варіанти рішення задачі. В процесі бізнес-аналізу вибирають оптимальне рішення, готують до нього вимоги, оцінюють, яка функціональність найбільш важлива для замовника, укладають та погоджують документацію для розробників. В IT бізнес-аналітики працюють з інформаційними системами – сайтами та додатками.

Наведемо задачі, які виконують бізнес-аналітики: ознайомлення з бізнесом замовника; виявлення потреб бізнесу; участь у розробленні вимог до системи; підготовка документації та її узгодження; сформулювати задачі для розробників; участь в здачі продукту.

В умовах формування інформаційного суспільства інформація освіти, запровадження нових інформаційних технологій – це лише перший крок у системі перебудови суспільства. Сучасній особистості потрібно прищепити прагнення не тільки навчатись, але й вміло використовувати новітні знання та технології, динамічно розвиватись у відповідності до потреб та вимог часу, що стосується як студентів, так і педагогів. Відтак, ґрунтуючись на нових інформаційних технологіях, освіта повинна набувати випереджальний характер.

Інформаційні джерела

1. Ящук В.І. Методологія наукового пізнання та онтологія наукових досліджень в процесі професійної підготовки фахівців з кібербезпеки // В. Ящук, М. Навитка / матеріали VI Міжнародної науково-практичної конференції "Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи".

УДК 004.9:378

ІНФОРМАТИЗАЦІЯ ОСВІТИ

Данило Гончаров, Дмитро Мєшков

Харківський національний університет радіоелектроніки, м. Харків, Україна

Анотація. *Швидкі темпи інформатизації суспільства призвели до значних змін у повсякденному житті та професійній діяльності людей. Інформатизація освіти є ключовою умовою для формування спеціалістів, здатних працювати в нових умовах праці, дедалі більш автоматизованих. Метою даної роботи є дослідження сутності, стратегій, тенденцій та наслідків застосування технологій у навчальному процесі.*

Ключові слова: *інформаційні технології, освіта, стратегія, тенденції розвитку.*

Abstract. *The rapid pace of the informatization of society has led to significant changes in everyday life and professional activity. Informatization of education is a key condition for training specialists capable of working in radically new, increasingly automated working conditions. The purpose of the article is to study the essence of information technologies, strategies, trends, and consequences of their application in the educational process.*

Keywords: *information technologies, education, strategy, development trends.*

В освіті інформатизація відкриває доступ до глобальних інформаційних ресурсів, зменшує залежність викладання і навчання від місця розташування учасників процесу, прискорює глобалізацію, сприяє вдосконаленню форми і змісту навчального процесу, підвищує ефективність засвоєння матеріалу. Загалом, інформаційні технології – це інтегрована сукупність методів, виробничих процесів і програмно-технічних засобів для збору, обробки, зберігання, розповсюдження, відображення та використання інформації на користь користувачів [1].

Під освітньою інформаційною технологією розуміють модель навчального процесу, цілі якої досягаються насамперед за рахунок можливості повноцінного використання комп'ютерів і програмного забезпечення. Міжнародні експерти та вчені підтвердили важливість і необхідність впровадження інформаційних технологій в освіту. ІТ впливають на всі сфери людської діяльності, але чи не найсильніше вони впливають на освіту, оскільки дають можливість запровадити абсолютно нові підходи до викладання та навчання. Оскільки інтерактивність і мультимедійна наочність сприяють кращому представленню, а отже, кращому засвоєнню інформації.

Головна мета нових інформаційних технологій – зробити так, щоб учні почувалися комфортно в інформаційному суспільстві. Нові інформаційні технології включають в себе формування інформаційної свідомості студентів та підготовку фахівців в галузі комп'ютерних наук.

Інформаційні технології дозволяють студентам отримати доступ до нетрадиційних джерел інформації та підвищити ефективність самостійної роботи. Використання комп'ютера вимагає розуміння того, як комп'ютери працюють і що вони роблять. Технологія використання комп'ютера для проведення уроків дозволяє тренувати і активізувати пам'ять, спостережливість, кмітливість, концентрувати увагу учнів і змушувати їх по-різному оцінювати інформацію, що надається. Комп'ютери значно розширюють можливості подання навчальної інформації. Використання кольорової, графічної, звукової, сучасної відеотехніки дозволяє моделювати різноманітні ситуації та середовища. Це може підвищити ентузіазм учнів до навчання.

Крім того, використання комп'ютерів в навчанні може усунути одну з найважливіших причин негативного ставлення до навчання – неуспішність. Працюючи за комп'ютером, учні мають можливість довести розв'язання задачі до кінця, спираючись на необхідну допомогу.

Розвиток суспільства, науки й техніки поставив освітні системи на випередження потреби використання нових засобів навчання. Одним із таких засобів навчання є комп'ютери та комп'ютерні інформаційні технології, які активно увійшли в наше життя останні 10–15 років. Бо сьогодні комп'ютер – найпотужніший засіб отримання та обробки інформації, можливості комп'ютерної та мережевої техніки, його швидкість вражають. Тому абсолютно закономірним є впровадження цих засобів у сучасний навчальний процес.

По-перше, тому що впровадження інформаційних технологій у сучасну освіту значно прискорило передачу знань і технологічного та соціального досвіду, накопиченого людьми, не лише від покоління до покоління, але й від однієї людини до іншої.

По-друге, сучасні ІТ підвищили якість навчання та освіти, дозволивши людям успішніше та швидше адаптуватися до екологічних та соціальних змін. Це дає можливість кожному студенту отримати необхідні знання в сучасному та постіндустріальному суспільстві.

По-третє, активне та ефективне впровадження цих технологій в освіту є важливим фактором у процесі створення нової системи освіти, що відповідає вимогам інформаційних систем, та модернізації традиційної системи освіти [2].

На разі, сучасний студент повинен бути комунікабельним; вміти самостійно здобувати знання та застосовувати їх на практиці; творчо мис-

лити, генерувати ідеї; грамотно працювати з інформацією (брати необхідні для вирішення певної проблеми факти, аналізувати їх, робити необхідні узагальнення) і т.д. Як ви можете замітити, у цьому переліку є згадка про володіння інформацією. Знову показуючи нам те, що знання технологій, вміння ними користуватися – це дуже важливі фактори у сучасному суспільстві.

Проте труднощів на цьому шляху вистачає, в основному відсутність або нульове фінансування їх розвитку в школах. Крім того, потрібні висококваліфіковані викладачі та постійні підвищення кваліфікації. Розвиток глобального процесу інформатизації, що вже почався в розвинутих країнах, ставить перед системою освіти нову глобальну проблему, а саме підготовку людини до життя і діяльності в абсолютно нових умовах – в інформаційному суспільстві [3].

Це потребує нового підходу до принципового вирішення проблеми інформатизації у сфері освіти. Сьогодні загальновизнано, що інформаційна складова має домінувати в освітній системі майбутнього. Бо освітні системи мають не лише надати учням необхідні знання про нове інформаційне середовище суспільства та практичні навички використання його можливостей, а й виробити в ньому новий світогляд, який має ґрунтуватися на розумінні вирішальної ролі інформації.

На порозі XXI століття ми повинні визнати, що люди вступають у нову еру – інформаційну. Від того, наскільки ефективно ми будемо використовувати інформацію як стратегічний чинник розвитку цивілізації, значною мірою залежить не лише добробут і стабільність нашого суспільства, а й можливість подолання глобальних криз.

Тому інформатизація суспільного життя та широке розповсюдження пов'язаних з нею комп'ютерних технологій суттєво вплинули би на зміст освіти, забезпечили учасників навчального процесу новими технічними засобами викладання та навчання, надихнули на створення автоматизованих інформаційних систем для вирішення можливих проблем.

Інформаційні джерела

1. Інформаційні технології в освіті URL: https://allreferat.com.ua/uk/pedagogika_metoduka_vukladanny/kontrolnaya/5888 (дата звернення 13.11.2022).

2. Інформаційні технології навчання URL: https://sites.google.com/site/ informacijninavcanna/ (дата звернення 13.11.2022).

3. Сучасні інформаційні технології у школах URL: https://osvita.ua/school/ method/34855/ (дата звернення 13.11.2022).

УДК 337.02.004

ЦИФРОВІЗАЦІЇ ОСВІТНЬОЇ ДІЯЛЬНОСТІ ЗАКЛАДІВ ПРОФЕСІЙНОЇ ОСВІТИ

Ірина Гончарова

Білоцерківський інститут неперервної професійної освіти ДЗВО "Університет менеджменту освіти" НАПН України
м. Біла Церква, Київська область, Україна

Анотація. *В роботі розглядаються поняття цифрової трансформації освіти, викладені актуальні проблеми цифровізації освітнього процесу в закладах професійної освіти. Акцентовано увагу на необхідності розвитку інформаційної компетентності педагогів закладів професійної (професійно-технічної) освіти як важливої умови забезпечення ефективності підготовки кадрів для цифрового суспільства і цифрової економіки.*

Ключові слова: *цифровізація, цифрова освіта, інформаційно-комунікаційні технології, цифрова компетентність.*

Annotation. *The concept of digital transformation of education is considered in the work, the current problems of digitalization of the educational process in vocational education institutions are outlined. Attention is focused on the need to develop the information competence of teachers of professional education institutions as an important condition for ensuring the effectiveness of personnel training for the digital society and digital economy.*

Keywords: *digitization, digital education, information and communication technologies, digital competence.*

Сьогодні ми живемо в епоху четвертої промислової революції, в якій Україна обрала стратегічний курс на новітній індустріальний розвиток і одна з умов цього розвитку України – масова та швидка цифровізація промислових секторів. Звичайно не стоїть осторонь і освіта. Цифрові технології є "інструментом" розвитку сучасного інформаційного суспільства та реформування сучасної системи професійної освіти в Україні.

Клаус Шваб, засновник і головний президент Всемірного форуму в Давосе, написав керівництво, яке допомагає нам зорієнтуватися в минулих змінах і дуже влучно описує саме те, що відбувається в нашому цифровому суспільстві зараз: "Характер змін, що відбуваються, настільки фундаментальний, що світова історія ще не знала подібної епохи – часу як великих можливостей, так і потенційних небезпек" [1].

Одним із найважливіших показників інноваційного та технологічного потенціалу кожної країни є рівень розвитку технологій, здатність економіки країни розвиватися в умовах цифрових трансформацій. Portulans Institute та World Information Technology and Services Alliancещорічно щорічно випускають звіт, в якому аналізують індекс мережевої готовності (Networked

Readiness Index) – комплексний показник, що характеризує рівень розвитку інформаційних технологій країн світу. Експерти розраховують індекс мережевої готовності на підставі 62 різних показників, які можна об'єднати у 4 групи: technology (технологічна складова), people (людський фактор), governance (управлінський навик), impact (вплив). На даний час вже опубліковані дослідження рейтингу за 2022 рік, відповідно до якого Україна посідає 50 місце (2019 рік – 67 місце, 2020 – 64, 2021 – 53) [2].

У березні 2021 року Кабінет Міністрів України схвалює Концепцію розвитку цифрових компетентностей та затвердження плану заходів з її реалізації, в якій визначає пріоритетні напрямки і основні завдання з питань розвитку цифрових навичок та цифрових компетентностей, підвищення рівня цифрової грамотності населення в умовах розвитку цифрової економіки та цифрового суспільства [3].

Створення загальноєвропейського освітнього простору, розширення економічних, політичних і культурних контактів, удосконалення системи професійної (професійно-технічної) освіти на сучасному етапі вимагає нових підходів до організації освітньої діяльності здобувачів освіти ЗП(ПТ)О, спрямованих на розвиток особистості майбутнього працівника, формування його професійної мобільності. На сьогодні все гостріше відчувається проблема готовності педагогів, до роботи зі здобувачами освіти, представниками "покоління Z", серед яскравих особливостей яких – цифрова обізнаність. Теорія поколінь Хоува-Штрауса стверджує, що формує та визначає покоління не тільки і не стільки вік, скільки цінності людей, які формуються під впливом суспільних, політичних, економічних, соціальних, технологічних подій та виховання у сім'ї [4].

Використання цифрових засобів у навчальному процесі викликає потребу розроблення нових методик і технологій професійної освіти і навчання.

Під час роботи в одному з закладів професійної освіти м. Дніпра будувати систему методичного супроводу ми розпочали з визначення пріоритетних напрямів формування цифрової компетентності педагога. Нами були виділені наступні пріоритети:

− знання про технології, їх можливості та обмеження для вирішення педагогічних завдань, що засновані на професійно-особистісних можливостях та обмеженнях в галузі застосування цифрових технологій;

− уміння комплексно використовувати цифрові технології у педагогічній діяльності, що засновані на безперервному вдосконаленні та розвитку професійної діяльності;

− досвід подання в педагогічному співтоваристві нових моделей педагогічної діяльності, що засновані на самостійному і ініціативному застосуванні цифрових технологій;

− ціннісне ставлення до використання цифрових технологій у своїй діяльності, що ґрунтується на рефлексії свого і чужого досвіду в галузі ІКТ.

На першому етапі створення моделі методичного супроводу в умовах цифровізації на основі аналізу були виявлені наступні проблеми: недостатній рівень володіння викладачами цифровими технологіями, наявність “психологічних бар’єрів”; відсутність мотивації до освоєння нового виду діяльності; відсутність методик, які б дозволяли здійснювати викладання предметів з використанням сучасних цифрових технологій.

Для самоаналізу стану цифровізації та ефективності використання цифрових технологій у закладі освіти ми скористалися онлайн-інструментом SELFIE (проєкт Європейської комісії), який допоміг оцінити ефективність впровадження інноваційних цифрових технологій в освітньому процесі, з’ясувати, на якому етапі цифрового розвитку знаходиться заклад освіти, оцінити ступінь володіння цифровими технологіями педагогів. Самоаналіз показав, що лише 5% педагогів є новаторами, які одні з перших використовують нові засоби навчання, 47% педагогічного складу починають використовувати новітні цифрові технології, коли пройшли певне навчання, 16% використовують нові ІТ-технології лише тоді, коли бачать в цьому певні переваги.

Цифровізація освіти має достатньо реальних проблем: значна частина здобувачів освіти не має необхідних для онлайн-навчання гаджетів і якісного інтернет-з’єднання; викладачам і здобувачам освіти без достатнього досвіду використання цифрових ресурсів важко навчатися онлайн; найчастіше під виглядом цифрової трансформації викладачі оцифровують цілком традиційні підходи – і це не є цифровізацією.

Освітня діяльність з використанням цифрових технологій мотивує здобувачів освіти до процесу навчання, стимулює до формування особистості, поглиблює професійну спрямованість, оволодіння сучасними технологіями, безпосередньо пов’язаними з майбутньою професійною діяльністю. Тому кожен педагог має зробити свій внесок у формування цифрової компетентності випускників закладів професійної освіти.

Інформаційні джерела

1. Шваб К.Четверта промислова революція / К. Шваб – Книжковий Клуб “Клуб Сімейного Дозвілля”, 2019, с. 176

2. Network Readiness Index 2022. Benchmarking the Future of the Network Economy URL: https://networkreadinessindex.org/countries/ (дата звернення 18.11.2022).

3. Розпорядження КМУ від 3 березня 2021 р. № 167-р Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації – URL: https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text (дата звернення 11.10.2022).

4. Цифрові компетенції в Україні та Європі URL: https://web.kpi.kharkov.ua /si/tsifrovi-kompetentsiyi-v-ukrayini-ta-yevropi/ (дата звернення 18.11.2022).

УДК 371:004

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ ЗВО ДСНС УКРАЇНИ

Ігор Коваль

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *У статті висвітлено теоретико-методологічні основи застосування інформаційних технологій в освіті. Визначено роль і місце інформаційних технологій в освітньому процесі, обґрунтовано напрями інформаційного розвитку та принципи професійної освіти в умовах впровадження інформаційних технологій у закладах вищої освіти галузі безпеки людини.*

Ключові слова: *інформаційні технології, професійна підготовка, майбутні фахівці, галузь безпеки людини.*

Abstract. *The article highlights the theoretical and methodological foundations of the use of information technologies in education. The role and place of information technologies in the educational process is determined, the directions of information development and the principles of professional education in the conditions of the introduction of information technologies in institutions of higher education in the field of human security are substantiated.*

Keywords: *information technologies, professional training, future specialists, the field of human security.*

Світ трансформується як у глобальному, так і локальному вимірах, що вимагає нових підходів підготовки людини до життєдіяльності, зокрема освітніми засобами. Традиційна освіта зберігає консервативний зміст, поступаючись потребам та перспективам сьогодення. Відповідно, постає проблема в активному впровадженні інформаційних технологій та їх інтеграції з іншими науковими галузями, оскільки якість освітнього процесу залежить від використання інформаційних технологій у поєднанні з інтернетом, що сприяє якіснішій подачі навчального матеріалу та зацікавленості молоді у його вивченні.

Впродовж останніх десятиліть спостерігається зацікавленість у вивченні інформаційних технологій, зокрема й в освіті. Цей напрямок висвітлено у працях вітчизняних науковців, таких як В. Биков, О. Бондаренко, Р. Гуревич, М. Коваль, М. Козяр, О. Міщенко, Т. Рак. Ідея “комп’ютерних навчальних середовищ”, яка є підґрунтям більшості сучасних навчальних комп’ютерних програм належить американському дослідникові С. Пейперту. Проблеми дидактики та перспективи використання інформаційних технологій в освіті висвітлено І. Роберт, психологічні основи комп’ютерного навчання виокремив Ю. Машбіц, систему підготовки фахівців до викорис-

тання інформаційної технології в навчальному процесі запропонував і детально обґрунтував М. Жалдак. Аналіз науково-педагогічної літератури, показує, що для співрозмірності часу, освіті потрібно мати інноваційний вектор, який сприятиме функціональності суспільства [2].

Ми погоджуємось з думкою М. Кусій, котра обґрунтувала напрями інноваційного розвитку професійної освіти в умовах впровадження інформаційних технологій у закладах вищої освіти Державної служби України з надзвичайних ситуацій (ЗВО ДСНС України). До таких напрямів вчена відносить [4, с. 30]:

− науково-педагогічні підходи до реалізації вимог модернізації освітнього процесу;

− інноваційні технології навчання для підвищення професіоналізму майбутніх фахівців пожежно-рятувальної служби;

− підвищення якості професійної освіти у ЗВО ДСНС України;

− особистісно-орієнтований підхід до організації професійної освіти;

− методичне супроводження і забезпечення професійної підготовки;

− компетенції у професійній освіті; організація науково-дослідної роботи курсантів; інформаційні технології в управлінні ЗВО ДСНС України, автоматизація роботи бібліотек;

− інновації у підготовці і підвищенні кваліфікації викладачів;

− взаємовідносини між навчальними закладами.

Важливим є й те, що кожен освітній процес повинен опиратись на методологію, зокрема дидактичні принципи. У цьому контексті М. Козяр вказав, що для функціонування освітнього середовища з використанням інформаційних технологій, потрібно враховувати такі три принципи:

− *цілісності* (визначає першочерговість вибору підходів до формування інформаційного середовища закладу освіти як цілісного явища, підпорядкованого завданням повноцінного сприймання майбутніми фахівцями дійсності, зокрема навколишнього світу);

− *комплексного підходу до проблеми інформатизації освіти* (реалізується через науково обґрунтоване визначення первинного вхідного стану процесу інформатизації, застосування програмно-цільового підходу до розвитку й управління цим процесом, кооперацію суб’єктів, зацікавлених у інформатизації освіти, зміну традиційних поглядів на процес інформатизації освіти);

− *системної побудови інформаційного середовища* (вимагає розробку й створення нових структур, що забезпечують організацію та функціонування технологій, реалізацію відкритості цієї системи на всіх рівнях, наявності обмінів інформацією в сфері професійної життєдіяльності) [3, с. 6].

З огляду на це, можемо стверджувати, що всі, без винятку, педагогічні технології є інформаційними технологіями, оскільки основу освітнього

технологічного процесу складає отримання, зберігання і перетворення інформації [1]. Загалом впровадження інформаційних технологій у ЗВО ДСНС України прискорює передачу знань і накопиченого досвіду у галузі безпеки людини не тільки в межах однієї країни, а й по всьому світу. Сучасні інформаційні технології, підвищують якість професійної підготовки, сприяючи успішній адаптації майбутніх фахівців до навколишнього середовища, до умов служби, ще дає можливість кожному з них отримати необхідні знання як сьогодні (формальна освіта), так і в майбутньому (неформальна освіта). Також, активне впровадження цих технологій в освіту є важливим чинником створення нової системи освіти, що відповідає вимогам самого суспільства, й процесу модернізації застарілої, консервативної системи освіти.

Викладене, дає підстави для висновку про те, що впровадження інформаційних технологій є загальним орієнтиром розвитку всіх сфер життєдіяльності ЗВО ДСНС України, а також одним із пріоритетних напрямів розвитку освіти. Інформаційні технології позитивно впливають на процес навчання і виховання майбутніх фахівців насамперед тому, що трансформують застарілі схеми й методи професійної підготовки. Цілеспрямоване впровадження інформаційних технологій у систему освіти в умовах сьогодення ґрунтується на застосуванні комп'ютеризованої техніки, спеціального устаткування, програмних і апаратних засобів, систем обробки інформації тощо.

Подальшими перспективами є виокремлення закономірностей впровадження інформаційних технологій у ЗВО ДСНС України, що сприятиме саморозвитку майбутніх рятувальників у галузі безпеки людини.

Інформаційні джерела

1. Коваль І. С. Використання інноваційних технологій у професійній діяльності психологів закладів вищої освіти Державної служби України з надзвичайних ситуацій. "Актуальні питання психологічного забезпечення діяльності ЗВО МВС України та Національної поліції України". Київ. 2011. С. 44–45.

2. Коваль М. С., Коваль І. С. Загальнодидактичні принципи формування професійної готовності майбутніх рятувальників до діяльності в екстремальних умовах. Young. 2018. Т. 64. Вип. 12. С. 95–99.

3. Козяр М. М. Модернізація навчально-виховного процесу на основі використання єдиного інформаційно-освітнього середовища. Теорія і практика управління соціальними системами. Харків : НТУ "ХПІ". 2011. № 1. С. 3–8.

4. Кусій М. І. Підготовка майбутніх фахівців пожежно-рятувальної служби до професійної діяльності : дис. канд. пед. наук 13.00.04.Львів : ЛДУБЖД. 2011, 267 с.

УДК 004.7

ОРГАНІЗАЦІЯ НАВЧАННЯ СТУДЕНТІВ ЗА ЗМІШАНИМ ФОРМАТОМ З УРАХУВАННЯМ ДОСВІДУ УНІВЕРСИТЕТУ З НІМЕЧЧИНИ

Володимир Любчак, Наталія Мартинова

Сумський державний університет, м. Суми, Україна

Анотація. *Розглядаються питання організації навчального процесу для спеціальності кібербезпека в умовах воєнного стану із застосуванням технологій електронного навчання. Комбінація очних та дистанційних форм навчання, синхронної та асинхронної взаємодії із студентами дозволяє забезпечити безперервність підготовки, але потребує нестандартних рішень. Досвід університету Маннгайм з впровадження гібрідного формату навчання буде корисним в наших умовах.*

Ключові слова*: гібрідне навчання, кібербезпека, платформа електронного навчання.*

Abstract. *Issues of organization of the educational process for the specialty of cyber security in the conditions of martial law with the use of electronic learning technologies are considered. The combination of face-to-face and remote forms of education, synchronous and asynchronous interaction with students allows for continuity of training, but requires non-standard solutions. Mannheim University's experience in implementing a hybrid education format will be useful in our conditions.*

Keywords: *hybrid teaching, cybersecurity, e-learning platform.*

З огляду на воєнний стан в Україні в Сумському державному університеті (СумДУ) організацію навчального процесу визначено за змішаним форматом. В основному заняття проводяться в режимі відеоконференцій, за потребою практичного відпрацювання та можливістю безпеки учасників – очно в аудиторіях. Університет був готовий організаційно, технічно і методично до онлайн режиму навчання, у тому числі для підготовки студентів спеціальності кібербезпека. Функціонує платформа електронного навчання, що інтегрує навчальний контент онлайн курсів з системою менеджменту (LMS) та підтримкою комунікацій учасників [1].

Але виклики та нестабільні умови сьогодення потребують корекції організації навчального процесу. Для впровадження життєздатних та більш ефективних рішень корисним буде досвід університету Маннгайм (Німеччина) організації онлайн навчання, відпрацьований під час пандемії COVID19.

Онлайн-навчання забезпечує безперервність навчального процесу в умовах катастроф, можливість участі у цьому процесі як викладачів і студентів, незалежно від місцезнаходження та того, який розвиток має ситу-

ація навколо. Очевидно, що якість онлайн-навчання залежить здебільшого від дисциплінованості та вмотивованості студентів.

Саме питанню мотивації значну увагу приділяють в університеті Маннгайм. Проєктування навчального курсу, використання інструментів, комунікація із студентами виконуються з урахуванням вимог взаємодії в онлайн курсі, мотивації до навчання, мережевого етикету.

Допомогу викладачам з цих питань, а також навчання з дидактики, методики, використання технічних засобів для створення онлайн курсу та організації ефективного навчання надає Центр викладання та навчання [2]. Підготовлено методичні рекомендації та проводяться тренінги з тематики цифрового навчання, організації онлайн занять та використання платформи електронного навчання ILIAS. Створено базу онлайн курсів ддя освітніх програм університету Маннгайм [3].

В СумДУ також створено свою бібліотеку онлайн курсів, у тому числі з математичних дисциплін [4]. Контент більшості з них є класичним – текстовий матеріал, тренажери, тести, завдання, іллюстративні матеріали. Ця традиційна модель передачі знань "викладач-студент" в дистанційних умовах навчання не дуже ефективна. Студенти краще сприймають інформацію у форматі відеозапису. Саме у вигляді відеозапису лекцій викладача підготовлені більшість курсів для онлайн навчання в університеті Маннгайм. Доцільно в наших умовах теж забезпечити технічні засоби та освоювати нові підходи викладання для створення навчального відеоконтенту.

Незважаючи на сучасні можливості технологій онлайн навчання, для спеціальностей інженерно-технічного профілю більш доречним для оволодіння практичних навичок є оффлайн формат. Також для спеціальності кібербезпека потрібно дати студентам реальний досвід кібербезпеки з практичною складовою та надати навички, щоб вони могли стати успішними професіоналами. Для вирішення цих завдань на кафедрі кібербезпеки Сумського державного університету (СумДУ) відбувається розбудова кіберполігону з метою відпрацювання студентами тактик відбиття кібератак, а також симуляція кібератак з одночасним напрацюванням методик кібернападів. Передбачається підтримка онлайн-навчання з кібербезпеки, можливість віртуалізації класів.

Для набуття практичних навичок з обладнанням кіберполігону за можливості студенти навчаються офлайн і у військовий час. Викладачі поєднують очні заняття та онлайн-навчання. Використовується. гібридний формат – це освітній підхід, коли одні студенти відвідують заняття особисто, а інші беруть участь віртуально. Гібридне навчання потребує більшої гнучкості від викладача, необхідності навчати обидві групи студентів одночасно. Перенесення звичних практик викладання з аудиторних занять в онлайн-формат не працює, потрібно комбінувати "живе" спілкування з

онлайн. Для цього також можуть бути задіяні асинхронні елементи навчання, такі як онлайн курс та попередньо записані відео.

Корисним є досвід університету Маннгайм з впровадження гібрідного формату навчання.

Підготовлені ними методичні рекомендації з планування гібридних занять, спілкування аудиторії та віртуального класу, поєднання синхронних та асинхронних методів взаємодії дозволять налагодити гібрідний формат в наших умовах.

Таким чином, комбінація очних та дистанційних форм навчання, синхронної та асинхронної взаїмодії дозволяє забезпечити безперервність фахової підготовки в умовах військового часу.

Інформаційні джерела

1. Навчальні ресурси СумДУ – URL: https://elearning.sumdu.edu.ua/ (дата звернення: 09.11.2022)

2. The Teaching and Learning Center (ZLL) – URL: https://www.uni-mannheim.de/en/teaching-and-learning-center-zll/ (дата звернення: 09.11.2022)

3. Каталог курсів URL: https://portal2.uni-mannheim.de/ (дата звернення: 09.11.2022)

4. Білоус О.А. Впровадження моделі змішаного навчання при вивченні математичних дисциплін / Інженерні та освітні технології. 2020. –Т. 8. № 1. – С. 8–18. doi: https://doi.org/10.30929/2307-9770.2020.08.01.01.

УДК 378.147:004.4

ДОСЛІДЖЕННЯ ПРОБЛЕМАТИКИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ГЕЙМІФІКАЦІЇ У СИСТЕМУ ОСВІТИ

Христина Мечус[1], Ольга Смотр[1], Наталія Вовчаста[2], Марія Рашкевич[2]

[1]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

[2]Національний університет "Львівська політехніка", м. Львів, Україна

Анотація. *Робота присвячена дослідженню проблеми впровадження технологій гейміфікації у систему освіти. На підставі проведеного аналізу зроблені рекомендації щодо систематизації досліджено в цій царині, з використанням підходів машинного навчання та інструментарію інтелектуального аналізу даних.*

Ключові слова: *гейміфікація освіти, інструментарій гейміфікації, машинне навчання.*

Abstract. *The paper is devoted to the study of the problem of introducing gamification technologies into the education system. Based on the analysis, recommendations were made for the systematization of research in this area, using machine learning approaches and tools intelligent data analysis.*

Keywords: *gamification of education, gamification tools, machine learning*.

Гейміфіка́ція (ігровізація, геймізація, англ. gamification) – використання ігрових практик та механізмів у неігровому контексті з метою залучення кінцевих користувачів до розв'язання проблеми [1, 2]. Цей термін з'явився у 80-х роках XX сторіччя та був введений завдяки шаленій популярності багатокористувацької відеогри MUD1, що поєднувала елементи рольової гри, hack and slash, інтерактивної літератури та надавала змогу у режимі реального часу одночасно взаємодіяти декільком гравцям і спілкуватися при цьому у чаті. З початку 2010-х років ідея гейміфікації стала одним із ключових трендів мотивації персоналу у багатьох бізнес-структурах. Джейн Мак-Гонал у своїй книзі "Reality Is Broken: Why Games Make us Better and How they Can Change the World" спрогнозував, що до 2015 року ринок гейміфікації досягне $15 млрд, й вона проникне в усі сфери людської діяльності, у тому числі й в освіту [3].

Можемо з певністю стверджувати, що прогноз Джейна Мак-Гонала справдився. Поступово процес гейміфікації (ігровізації) набув поширення в усіх сферах нашої життєдіяльності і, звісно ж, сфера сучасної освіти не стала винятком. У 2020 році експерти компанії Growth Engineering засвідчили, що гейміфікацію використовують понад 70% компаній зі списку компаній Global 2000 та в подальшому прогнозують, що глобальний ринок гейміфікації зросте до 30,7 мільярда доларів США до 2025 року при середньорічному темпі зростання (CAGR) у 27,4%. [4]. При цьому, на сьогоднішній день найбільше використовує гейміфіковані рішення роздрібна торгівля, займаючи 28,6% ринку, освіта ж слідує за нею як наступний за популярністю сектор [4].

Очевидно, що проблеми, впровадження елементів гейміфікації в освітній процес, не оминули зацікавленості вітчизняних та зарубіжних учених. Для прикладу, у своїх роботах Лі Шелдон (Lee Sheldon) досліджував використання прототипів багатокористувацької гри для створення навчальних курсів закладів освіти [5]; вплив ефекту ігор на мотивацію в навчанні, у своїх роботах розглядали Дональд Кларк (Donald Clark), Ничкало Н., Матяш Н., Смотр О. [6–9]; гейміфікацію як сучасний напрям вітчизняної освіти досліджували Переяславська С, Смагіна О. [10] та інші.

Проте, не зважаючи на значну кількість публікацій у цій царині, можемо стверджувати, що знання про те, як гейміфікувати діяльність відповідно до специфіки освітнього контексту, все ще обмежені. Інколи складається враження, що стрімкий процес впровадження гейміфікації у найрізноманітніших її проявах в освітній процес, випередив дослідників у розумінні її механізмів і методів. Адже різноманіття форм гейміфікації, реалізованих на сьогодні в освітньому процесі дійсно вражає. Для прикладу, наведемо лише частину найбільш популярних з них:

− гра, як інструмент психологічного впливу;
− гра, як інструмент отримання знання з окремих галузей;
− гра, як інструмент оволодіння практичними навичками;
− гра, як інструмент командної роботи
− гра, як інструмент для створення інновації;
− гра, як симуляція;
− гра як засіб дискусії;
− гра, як інструмент для досліджень тощо.

Однак, на сьогодні все ж не вистачає систематизованих та обґрунтованих досліджень щодо того, які елементи гри, у яких її проявах та для якого контингенту, можуть бути найбільш прийнятними, та за яких обставин стимулюватимуть бажану поведінку.

На нашу думку, одним з найперспективніших напрямків проведення таких досліджень є використання підходів машинного навчання та інструментарію інтелектуального аналізу даних. Для прикладу, на рис. 1 відображено, частину результатів багатокласової класифікації за допомогою AutoML (Pycaret) рівня адаптивності груп, до онлайн-гри, як симуляції.

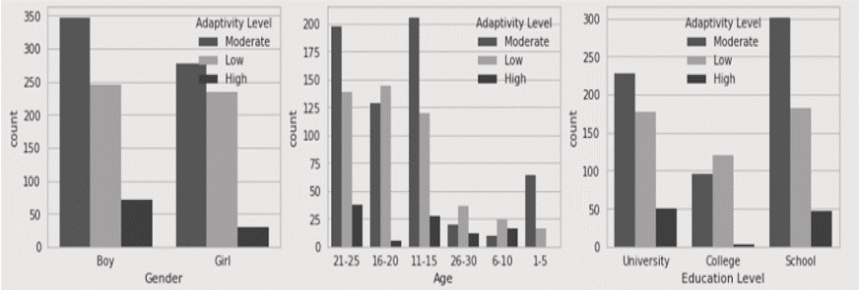


Рисунок 1. – Частина результатів Multiclass Classification AutoML

З наведеного рисунка видно, що найкращий рівень адаптивності у школярів, вікова категорія – 11-15 років, стать – чоловіча.

Інформаційні джерела

1. Huotari, K., & Hamari, J. (2012). Defining Gamification – A Service Marketing Perspective. Proceedings of the 16th International Academic MindTrek Conference 2012, Tampere, Finland, October 3–5.

2. Zichermann, Gabe; Cunningham, Christopher (August 2011). Introduction. Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps (вид. 1st). Sebastopol, California: O'Reilly Media. с. xiv. ISBN 1449315399.

3. Gartner Says By 2015, More Than 50 Percent of Organizations That Manage Innovation Processes Will Gamify Those Processes / Egham, UK, April 12, 2011. – [Електронний ресурс]. – Режим доступу : http://www.gartner.com/newsroom/id/1629214

4. 19 GAMIFICATION TRENDS FOR 2022-2025: TOP STATS, FACTS & EXAMPLES. [Електронний ресурс]. – Режим доступу: http://www.british-legends.com/CMS/index.php/about-mud1-bl/history

5. Sheldon, L. The Multiplayer Classroom: Designing Coursework as a Game / Sheldon, L., – 1 изд. – Boston: Course Technology, 2011. – 284 p.

6. Donald Clark. Learning Experience Design: How to Create Effective Learning that Works – Kindle... Edition. 1st. Publisher. Kogan Page. Publication date. November 3, 2021, 320 p.

7. Смотр О.О. Використання інструментарію інформаційних технологій для підвищення мотивації студента до навчання у форматі змішаної освіти / О. Смотр, М. Рашкевич, Р. Головатий, Х. Мечус // Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи : Збірник наукових праць. Випуск 6. / За ред. М. С. Коваля, Н. Г. Ничкало. – Львів : ЛДУ БЖД, 2021. – С.214–217.

8. Купчак М.І. Тенденції та проблеми впровадження інформаційних технологій в управління університетом / М.І. Купчак, О.О. Смотр, М.Я. Купчак // Вісник Львівського державного університету безпеки життєдіяльності : зб. наук. праць. – Львів : Вид-во ЛДУ БЖД. – 2013. – № 7. – С. 28–32

9. Жолубак Л.В. Гейміфікація як інструмент підвищення мотивації студента донавчання / Л.В. Жолубак, Х.В. Мечус, О.О. Смотр // збірник матеріалів Десятої Міжнародної наукової конференції студентів та молодих вчених "Сучасні інформаційні технології – 2020" "Modern Information Technology – 2020" (14–15 травня 2020 р., м.Одеса) / МОН України; Одес. Нац. політех. ун-т ; Ін-т комп'ют. систем. Одеса : Наука і техніка, 2020. –с. 220–221.

10. Переяславська С. Гейміфікація як сучасний напрям вітчизняної освіти / С. Переяславська, О. Смагіна // Відкрите освітнє е-середовище сучасного університету. – 2019. – Вип. спецвип.. – С. 250–260.

УДК 004.9:378

РОЗВИТОК ТЕХНОЛОГІЙ ОСВІТИ

Дмитро Мєшков, Данило Гончаров

Харківський Національний університет радіоелектроніки
м. Харків, Україна

Annotation. *Currently, there is an increasing understanding that the traditional scheme of obtaining education in the first half of life is obsolete and needs to be replaced by lifelong education and training throughout life. New learning theories must be developed that focus on learning without temporal and spatial boundaries.*

Keywords: *education, teachers, network technologies, information environment.*

Анотація. *В даний час зростає розуміння того, що традиційна схема здобуття освіти в першій половині життя застаріла і потребує заміни безперервною освітою та навчанням протягом усього життя. Необхідно розробити нові теорії освіти, які зосереджуються на навчанні без часових і просторових кордонів.*

Ключові слова: *освіта, викладачі, мережеві технології, інформаційне середовище.*

Today, one of the characteristic features of the educational environment is the ability of students and teachers to access structured educational and methodological materials that teach multimedia complexes of the entire university at any time and any point in space. The UNESCO Report on the main directions of activity in the field of education and informatics after the First International Congress "Computer Science and Education" states that it is not the technology itself that is important, but its interaction with learning and its role in the context of the education system as a whole. The developers of distance education concretize the individualization of educational behavior in the following way, believing that in distance learning the features of a student-centered way of learning are most clearly manifested: flexibility, modularity, accessibility, profitability, mobility, manufacturability, social equality, internationality [1]. Information technologies bring the possibility and necessity of changing the very model of the educational process: the transition from reproductive learning – the "transfer" of knowledge from one head to another, from a teacher to students – to a creative model (when a life situation is modeled in the classroom with the help of new technological and technical support or a process where students, under the guidance of a teacher, must apply their knowledge, show creativity to analyze a simulated situation and develop solutions to the tasks set).

Globalization requires deep and radical changes in the structure, methods of teaching, and research, as well as the training of managerial and teaching staff [2].

According to W. Hasson and E. Waterman, "any discussion of the quality of distance education will inevitably affect the selection, retraining, and support of teaching staff participating in a technical training program. In the traditional academic environment, teachers are carefully selected according to very strict criteria, which are mainly academic in nature, taking into account related factors, the availability of research papers and publications, etc. The criteria for selecting teachers for distance learning programs should be primarily academic" [3]. The development and expansion of the use of educational information technologies are directly related to the problem of changing the effectiveness of education. Determining the effectiveness of any method, training technology includes – measuring the result achieved, the cost of material resources, and the time to achieve it. In this case, groups of students who used and did not use computer learning support are usually compared. Can traditional quality criteria be applied to key aspects of distance education in a technological learning environment? The application of this approach to the assessment of information technology in training implies that the latter does not bring anything new to the goals and objectives of education. The introduction of information technology affects the quality and content of education. There is an approach that involves the use of traditional criteria of quality and efficiency in technological higher education. Key aspects are considered to be: qualified teaching staff; pedagogical skill; development of a course with the addition of elements due to the use of technological teaching aids; work of student services. For example, Regis University, a Jesuit liberal arts university located in Denver, Colorado (USA), is currently developing quality standards in the following areas: the process of selecting teachers and preparing them for online teaching; constant retraining and support of teachers; development of a technological learning environment; technical and academic support for students studying online; technology policies to ensure continuous monitoring and improvement; organization of student services for distance learning [4]. An important and effective condition for the progress of any society has been and is the creation and expansion of a single interactive information space. The common information spaces have historically largely contributed to the acceleration of the development of all mankind as a whole, and have been a decisive factor in the improvement of civilization in all areas. Therefore, the creation of a single interactive information space can be considered a strategic goal of introducing modern and promising information technologies into all spheres of human activity. This can be achieved thanks to modern information and technical equipment for the main types of activities in

education: educational, pedagogical, research, organizational and managerial, expert, etc.

Building a single information space in education will achieve: improving the efficiency and quality of the learning process; intensify the process of scientific research in educational institutions; reduction of time and improvement of conditions for additional education and adult education; increasing the efficiency and effectiveness of managing individual educational institutions and the education system as a whole; integration of national information educational systems into the global network, which will greatly facilitate access to international information resources in the field of education, science, culture, and other areas. Uneven investment and interest in participating in e-learning will have a marked impact on the state of affairs in higher education. Apart from the elite universities, which have a fairly strong political influence (due to rich graduates and solid funds), other institutions of higher education will be in a very vulnerable position. Only those universities that systematically invest in e-learning, constantly create programs, and enter into partnerships will successfully survive this decade [5]. A promising education system should take into account the main challenges of the 21st century and the most important human problems associated with them in the modern and upcoming information society. The most important areas of transition to a new educational concept, which will become the basis of a promising education system necessary for the conditions of the 21st century, include, in particular, the fundamentalization of education at all its levels; implementation of the concept of advanced education; widespread use of innovative and developmental education methods based on the use of advanced information technologies; increasing the availability of quality education through the development of a distance learning system and means of information support for the educational process using modern information and telecommunication technologies.

Інформаційні джерела

1. E.F. Fedorov. Systemic representation of distance education.

2. Kelly M. Francis. Political implications of e-learning // Higher education in Europe. Volume XXVII, №3, 2002.

3. Husson W., Waterman E. Criteria for the quality of distance education // Higher education in Europe. Том XXVII, №3, 2002

4. Husson W., Waterman E. Criteria for the quality of distance education // Higher education in Europe. Том XXVII, №3, 2002

5. M. Francis Kelly. Political implications of e-learning // Higher education in Europe. Volume XXVII, №3, 2002.

УДК. 348.147

СУТЬ ТА ПРАКТИЧНЕ ЗНАЧЕННЯ ЗАПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТНІЙ ПРОЦЕС ВИЩИХ ВІЙСЬКОВИХ НАВЧАЛЬНИХ ЗАКЛАДІВ В СУЧАСНИХ УМОВАХ ВІЙСЬКОВОГО СТАНУ

Вадим Рижиков, Анатолій Юрков

Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ, Україна

Анотація. *Запровадження інформаційних технологій в освітній процес вищих військових навчальних закладів в сучасних умовах участі України у повномасштабній війні на тлі агресії росії сприятиме розв'язанню нагальної потреби сьогодення прискореної підготовки висококваліфікованих офіцерських кадрів, тому що вони максимально наближають освітній процес реальної бойової діяльності.*

Ключові слова*. інформаційні технологій, військова освіта сьогодення, реальна бойова діяльність, офіцери Збройних Сил України.*

Abstract. *The introduction of information technologies into the educational process of higher military educational institutions in the modern conditions of Ukraine is participation in a full-scale war against the background of Russian aggression will contribute to solving today's urgent need for accelerated training of highly qualified officer personnel, because they bring the educational process as close as possible to real combat activity.*

Keywords. *information technology, military education today, real combat activity, officers of the Armed Forces of Ukraine.*

Інформаційна революція, що відбувається протягом останніх десятиріч, зумовлює кардинальні зміни в суспільстві: зароджуються нові культурні та економічні тенденції, нове виробництво (продукування інформації як самостійного товару), нові види соціальних комунікацій. Така сфера життя суспільства, як безпека та оборона, не могла залишитися поза впливом інформаційного фактора у Збройних Силах України. Збройні Сили України (ЗСУ) пройшли випробовування на міцність в умовах боротьби із сучасною зовнішньою агресією, підтвердили свою боєздатність та ефективність використання інформаційних технологій у сучасній війні з росією.

Як свідчать наукові дослідження [2; 3; 4] і показує практика при формуванні готовності військовослужбовців до реальної бойової діяльності в процесі професійної підготовки офіцерів ЗСУ можна забезпечити шляхом реалізації наступних інноваційних напрямів: створення мультимедійних навчальних комплексів за практичною тематикою; створення комп'ютерних навчальних систем; впровадження інформаційних і кейс – технологій у систему підготовки військових фахівців; розроблення муль-

тимедійних віртуальних тренажерів(симуляторів); моделювання навчальних ігор; розроблення системи автоматизованої оцінки знань; розроблення інформаційно-дистанційно-тренажерної системи навчання.

Якщо звертатися до джерел поняття “технологія”, то ми повинні зафіксувати, що воно походить із двох грецьких слів – мистецтво, майстерність і слово, навчання. Таким чином, технологію можна визначити як усвідомлене практичне мистецтво, усвідомлена майстерність.

Запровадження інформаційних технологій у військовій освіті сьогодення передбачає розвиток таких важливих педагогічних технологій які впливають досить позитивно на таку специфічну підготовку, як підготовка офіцерів ЗСУ, а саме: ефективність, відтворюваність, візуалізація. Вище зазначені педагогічні технології в найкоротший час освітнього процесу ВВНЗ чи ВНП (ЗВО) максимально сприяють формування практичної складової максимально наближеної до реальної бойової діяльності військовослужбовця [1].

Надамо коротку характеристику цих педагогічних технологій. Ефективність, це коли сучасні педагогічні технології існують в конкурентних умовах і повинні бути ефективними за результатами й оптимальними за витратами, гарантувати досягнення певного стандарту освіти.

Відтворюваність. Можливість використання (повторення, відтворення) педагогічної технології в специфічних освітніх закладах, таких як військові, іншими суб’єктами [3].

Візуалізація – передбачає використання аудіовізуальної та електронно-обчислювавальної техніки, а також конструювання та застосування різноманітних дидактичних матеріалів і оригінальних наочних посібників.

Запровадження у сучасний освітній процес вищих військових навчальних закладів інформаційних технологій сприятиме широкому використання інтерактивних і комп’ютерних технологій навчання, яких не було в традиційній системі підготовки офіцерів ЗСУ [4]. Це так звані моделі змішаного навчання, мережне співробітництво. Одним із найефективніших факторів в даному випадку є ділові рольові ігри, які виводять освітній процес на новий рівень. Їхня особливість – в урахуванні військово-практичної спрямованості підготовки курсантів та переважанні творчого стилю поведінки учасників занять. Приймаючи безпосередню участь у ділових іграх курсанти опиняються в ситуаціях, максимально наближених до реальної майбутньої професійної діяльності на офіцерських посадах. Під час таких занять в аудиторії моделюють бойову обстановку, в “екстремальних умовах” якої у майбутніх офіцерів, фахівців тактичного рівня, формується готовність виконувати обов’язки з максимальною адаптацією одразу після випуску з ВВНЗ та ВНП(ЗВО) і отримання офіцерського звання. Для цього використовують різноманітні методи і засоби: сучасні програмне забезпечення й навчально-методичні посібники, хмарні технології.

Інформаційні джерела

1. Інноваційні педагогічні технології та методики в освітньому процесі військових навчальних закладів провідних країн-членів НАТО і України/ Колективна моногр./ за заг. ред. проф. В.С. Рижикова; Військовий інститут Київського національного університету імені Тараса Шевченка. – К.: НДЦ ВІКНУ, 2018.– 320 с.
2. Рижиков В. С. Значення професійних якостей в цільовій моделі навчально-виховного процесу підготовки військових. Вісник Київського національного університету імені Тараса Шевченка: соціальна робота. 2017. № 2, С. 61–64.
3. Bakhov I. Leadership abilities of a Military Manager, Professionalism of a Commander as the Guarantee of the Practice of Efective Activity of a Miliatry Organization / I. Bakhov, V. Ryzhykov, O. Kolisnyk. // International Journal of Engineering and Technology. – 2018. – №7. – С. 45–49.
4. Horiacheva K., Ryzhykov V. The oreticales sence and practice of implementation of the system approach in formation of professional reliability of future officersin the armed forces of Ukraine. Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. № 2 (42), Київ, 2019. С. 57–60.

УДК 378+37.004

ВІРТУАЛЬНЕ НАВЧАННЯ В УМОВАХ СЬОГОДЕННЯ: АНАЛІЗ, ТЕНДЕНЦІЇ, ПЕРСПЕКТИВИ

Оксана Трусевич

Кафедра прикладної математики і механіки Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Реальність сьогодення спонукає різні сфери нашого життя пристосовуватися та бути гнучкими. Виникнення віртуальної освіти, віртуального навчання, створення віртуального середовища на основі інформаційно комунікаційних технологій – це результат нашої реальності. Аналіз, тенденції та перспективи процесу віртуального навчання, як основний меседж даної публікації.*

Ключові слова: *віртуальне навчання, віртуальна освіта, інформаційно комунікаційні технології, віртуальне навчальне середовище.*

Abstract. *Today's reality forces various areas of our lives to adapt and be flexible. The emergence of virtual education, virtual training, creation of a virtual environment based on information and communication technologies is the result of our reality. Analysis, trends and perspectives of the virtual learning process, as the main message of this publication.*

Keywords: *virtual learning, virtual education, information and communication technologies, virtual educational environment.*

Реальність сьогодення в Україні підтвердило правильність створення віртуального середовища декілька років тому, як головного вектора нової інформаційно – навчальної епохи розвитку країни. Війна в Україні доводить необхідність створення віртуального середовища не лише для на-

вчання у вищих навчальних закладах, але і у школах, професійно – технічних училищах, коледжах, технікумах тощо. Адже віртуальне навчання забезпечує процес неперервності навчання, що є одним із основних завдань сучасної освіти. Очевидно, що віртуальне навчання – це процес та результат комунікації в умовах віртуального освітнього середовища.

Застосування технологій віртуальної реальності в освіті призвело, власне, до появи віртуального освітнього середовища, в рамках якого можлива безперервна самореалізація і саморозвиток особистості за умов організації та функціонуванні освітніх систем на базі технологій віртуальної реальності. Важливими складниками віртуального навчання є забезпечення, власне, самого навчання, визначивши пріоритет навчання, як домінантний перед викладанням; домінування діяльнісного типу навчання; організації самостійної навчальної діяльності; спонукання до підвищення рівня емоційного сприйняття інформації та формування умінь реалізовувати різні форми самостійної діяльності щодо обробки інформації.

Вищі навчальні заклади використовують віртуальне навчання із метою: економії часу педагогічного складу; надання інструкцій у гнучкий спосіб студентам, не лімітуючи їх у часі та місці навчання; надання інструкцій у спосіб, звичний для сучасного веборієнтованого покоління студентів; сприяння співробітництву та поширенню інформації; надання можливості обміну матеріалами між різними курсами; забезпечення автоматичної інтеграції результатів навчання студентів.

Віртуальне освітнє середовище – це відкрита система, в рамках якої на основі застосування технологій віртуальної реальності забезпечується ефективне інтерактивне самонавчання в освітньому процесі. Зрозуміло, віртуальне освітнє середовище є соціальним результатом реальної дійсності, але його дидактичний потенціал залишається недостатньо розкритим, оскільки наявні протиріччя між потребами освітньої практики в ефективному освітньому середовищі і станом наукового знання про них. Важливою проблемою є розробка моделі віртуального освітнього середовища та визначення шляхів найбільш оптимального застосування технологій віртуальної реальності в освіті.

Віртуальне освітнє середовище є, звичайно, творчим середовищем, навчання в якому можливе за наявності внутрішньої мотивації студентів, їх емоційному підйомі та позитивному, оптимістичному настрої. Необхідною умовою навчання у віртуальному освітньому середовищі є реалізація особистісноорієнтованої особистості. Довіра викладачів до ініціатив студентів в такій системі вища, ніж в традиційній системі освіти. При цьому активність студентів залишається високою, оскільки технології продуктивної творчої діяльності на базі інформаційно комунікаційних технологій надають немалі можливості для самореалізації студента.

Упровадження інформаційно комунікаційних технологій з використанням мультимедійних технологій та віддаленого доступу до інформаційно-освітніх ресурсів сприяють забезпеченню неперервності віртуально-

го навчання, а можливість вибору плану та методики навчання сприяють розкриттю та виявленню індивідуальних творчих здібностей студентів. Реалізація форм та методів навчання, особливо при організації самостійної навчальної діяльності у віртуальному освітньому середовищі, є суттєвим фактором підвищення мотивації до навчально-пізнавальної діяльності, підвищення рівня емоційного сприйняття нового матеріалу. У віртуальному освітньому середовищі реалізується сукупність умов, що сприяють процесу активної взаємодії між викладачами і студентами завдяки орієнтації на виконання різних видів самостійної роботи на основі інформаційних освітніх технологій.

Віртуальна реальність із застосуванням інформаційно комунікаційних технологій в освіті сприяє створенню інтерактивного освітнього віртуального середовища із використанням сукупності засобів, методів створення та реалізації віртуальних образів з метою взаємодії з ними або всередині них, відповідно з високим рівнем достовірності. Віртуальне освітнє середовище, стихійний та водночас цілеспрямований розвиток якого чітко простежується на сучасному етапі, є відкритою системою, що представляє взаємозв'язок засобів нових інформаційно комунікаційних технологій і комунікаційних можливостей для забезпечення ефективного навчання за наявності інтерактивної взаємодії всіх суб'єктів освітнього процесу.

Віртуальне освітнє середовище є типовим творчим середовищем саморозвитку вільної та активної особистості, якій властива активність, висока самооцінка, відкритість, а також свобода міркувань. Домінуючим у віртуальному освітньому середовищі виступає метод самонавчання із постійною взаємодією (співпрацею) суб'єктів викладання та суб'єктів навчання за умови наявності безперервних зворотних зв'язків між ними. В умовах віртуалізації та інформатизації суспільства моделювання віртуального освітнього середовища є основою для виявлення потенціалу сучасного освітнього середовища та можливостей його практичного втілення в навчальному процесі.

Інформаційні джерела

1. Кузик А.Д., Карабин О.О., Трусевич О.М. Вища математика. Частина 1. Навчальний посібник. – Львів: ЛДУ БЖД, 2014. – 400 с.

2. Кузик А.Д., Карабин О.О., Трусевич О.М. Вища математика. Частина 2. Навчальний посібник. – Львів: ЛДУ БЖД, 2014. – 250 с.

3. Огаренко В. Зміна парадигми державного управління та моделі управління вищою освітою// Держава та регіони. – 2004. – №1. – С. 75–80.

4. Степко М., Болюбаш Я., Шинкарук В., Грубінко В., Бабин І. Вища освіта України і Болонський процес: Навчальний посібник. – Тернопіль: Навчальна книга – Богдан, 2004. – 384 с.

5. Топчій Т. Інституціоналізація безперервної освіти в Україні: факторна обумовленість. Автореф. дис. на здоб. наук. ст. канд. соціологічних наук. – Харків: 2006. – 20 с.

6. Тацій Р.М., Стасюк М. Ф., Трусевич О.М. Інтегральне числення. Навчальний посібник. – Львів: ЛДУ БЖД, 2019. – 135 с.

УДК 354.404+614.84

ОСОБЛИВОСТІ ПІДГОТОВКИ ОПЕРАТОРІВ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

Вікторія Філіппова, Андрій Гаврись

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *З кожним роком інноваційні технології вносять зміни в наше життя. Все частіше над головою можна почути та побачити дрони, квадрокоптери, безпілотні літальні апарати чи безпілотні літальні комплекси як в аматорських так і в професійних цілях. Ця техніка стає в пригоді широкому колу професій та спеціальностей на всіх рівнях, тому актуальність осягнення професії оператора безпілотного літального апарата постає нагальною потребою.*

Ключові слова: *цивільний захист, безпілотні літальні апарати, навчання, оператор.*

Annotation. *Every year, innovative technologies bring changes to our lives. Drones, quadcopters, unmanned aerial vehicles or unmanned aerial systems can be heard and seen more and more overhead, both for amateur and professional purposes. These technologies are useful for a wide range of professions and specialties at all levels. Therefore, the urgency of mastering the profession of an unmanned aerial vehicle pilot is an urgent need.*

Keywords: *civil protection, unmanned aerial vehicles, training, operator.*

Забезпечення безпеки суспільно значущої діяльності є комплексним питанням, яке вимагає залучення різноманітних технічних засобів. На сьогоднішній день розроблено низку методів раннього короткострокового прогнозування надзвичайних ситуацій та їх можливих наслідків, наприклад, завчасні обстеження територій чи об'єктів; відомі характеристики об'єктів у їх природному стані; ідентифіковані фактори та явища, які можуть внести зміни до даних, отриманих з карт, описів, довідників та спеціальної літератури. Але протягом останнього десятиліття стрімко розвиваються методи оперативного прогнозування для попередження надзвичайних ситуацій, пошуку та рятування із залученням пілотованих і безпілотних літальних апаратів з використанням геоінформаційних технологій і моніторингу, сигнальних датчиків і сенсорних мереж [1, 2].

Однак можливість використання пілотованої авіації не завжди ефективна через тривалий час реагування, великі фінансові витрати та сувору

залежність від погодних умов. Одним із найперспективніших напрямів вирішення цієї проблеми є використання безпілотних літальних апаратів з корисним навантаженням до 50 кг, із станціями наземного управління та різноманітних засобів моніторингу, виявлення та розвідки надзвичайних ситуацій, що дозволяє скоротити час організації здійснення профілактичних заходів або пошуково-рятувальних (аварійно-рятувальних) заходів [3].

Безпілотні літальні апарати – апарати, які можуть злітати, здійснювати політ та сідати без фізичної присутності пілота чи пасажира на його борту. Керування польотом здійснюється дистанційним керуванням оператором, чи відповідною програмою, або за допомогою спеціальної станції керування, що знаходиться поза повітряним судном. Безпілотні літальні апарати здатні вести повітряну розвідку і спостереження, передавати фото і відеоінформацію в режимі реального часу, бути носіями і мішенями, діяти в екстремальних умовах [4].

Використання безпілотної літальної техніки характеризується великою різноманітністю літальних апаратів, як за зовнішніми характеристиками, так і за способами застосування. Безпілотні літальні апарати, які також називають “безпілотниками” і “дронами”, широко вживають як у військових, так і в мирних цілях.

Невійськові дрони застосовуються для розв’язання усестороннього кола завдань, використання яких пілотованими літальними апаратами може бути небезпечне чи недоцільне.

Вагомого значення безпілотні літальні апарати набули в Держаній службі України з надзвичайних ситуацій. Завдяки роботі з безпілотними літальними апаратами стало значно легше проводити розвідку пожеж у екосистемах з повітря, нетехнічне обстеження територій та акваторій на наявність вибухонебезпечних предметів, здійснювати пошук людей, які заблукали у лісі або яких віднесло у відкрите море [2].

Залучення безпілотного літального апарата здійснюється за рішенням керівників з ліквідації надзвичайної ситуації, гасіння пожежі, пошуково-, аварійно-рятувальних та піротехнічних робіт на території яких виникла надзвичайна ситуація, пожежа чи некласифікована подія.

Керування безпілотним літальним апаратом повинне здійснюватись компетентною особою, яка пройшла курс навчання та має необхідні знання і навички в цій галузі.

Для навчального процесу на приведення у відповідність вимогам професійної кваліфікації підготовки фахівців, що будуть залучатися до моніторингу та ліквідації надзвичайних ситуацій і формування мотивації

до постійного самовдосконалення професійної компетенції створені курси навчання керування безпілотними літальними апаратами. В програмі курсу передбачені теоретичні та практичні відпрацювання. Вона розрахована на фахівців будь-якої галузі чи спеціальності.

Безпілотний літальний апарат вартісний прилад, тому для отримання практичних навичок доцільно було б використовувати симулятор. Це програма, яка встановлюється на персональний комп’ютер і шляхом приєднання пульта керування до персонального комп’ютера дає можливість віртуально керувати безпілотним літальним апаратом.

Використання такої програми дозволить в значно короткий термін, набути необхідні знання та оволодіти практичними навичками керування безпілотним літальним апаратом, а також зменшить можливість механічного ушкодження літальних апаратів та збереження матеріально-технічної бази.

Також це дозволить збільшити кількість підготовлених фахівців в цій галузі, які необхідні кожній державній пожежно-рятувальній частині,яка здійснює виїзд на місце надзвичайної ситуації і використовує безпілотний літальний апарат для отримання певної інформації про надзвичайну подію.

При терміновій необхідності спеціалістів з керування безпілотними літальними апаратами та в умовах пандемії чи війни актуальним було б розробити навчання в онлайн форматі із практичним відпрацюванням на комп’ютерному симуляторі, що дасть можливість пройти курси безпосередньо з місця праці.

Використання отриманих знань та навичок під час навчання дозволить проводити рятувальні операції у надскладних умовах та важкодоступних місцях і допоможе врятувати не одне людське життя.

Інформаційні джерела

1. Malets, I., Popovych, V., Prydatko, O., & Dominik, A. (2018, August). Interactive computer simulators in rescuer training and research of their optimal use indicator. In 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP) (pp. 558–562). IEEE.

2. Лаврівський, М. З., & Гаврись, А. П. (2017). Розвиток безпілотних літальних апаратів в Україні та світі для виконання завдань цивільного захисту. Науковий вісник НЛТУ України, 27(1), 151–153.

3. Havrys, A. P., Tarnavsky, A. B., Lavrivskiy, M. Z., & Veselivsky, R. B. (2017). Rationale use of unmanned aircraft technology as a means of detecting accidents and emergencies situations.

4. ПКМУ від 06.12.2017 року № 954 “Про затвердження Положення про використання повітряного простору України”.

УДК 377.014

ЦИФРОВА КОНТЕНТНА ТВОРЧІСТЬ ЯК ВАЖЛИВА СКЛАДОВА ДИДЖИТАЛІЗАЦІЇ ОСВІТИ

Олена Юденкова

Білоцерківський інститут неперервної професійної освіти ДЗВО "Університет менеджменту освіти" НАПН України, м. Біла Церква, Україна

Анотація*. Формування інформаційно-цифрової компетентності молоді під час освітнього процесу є ключовим у системах освіти як економічно розвинених країн, так і в професійній освіті України. Цифрова контентна творчість є одним з критеріїв вимірювання рівня навичок інформаційно-цифрової компетентності здобувачів освіти і відповідно до цього актуалізується її вагомість як важливої складової диджиталізації освіти в цілому. Висвітлено досвід щодо застосування відеохостингу YouTube для створення освітнього цифрового контенту.*

Ключові слова*: діджиталізація, технології, освітнє телебачення, цифровий контент.*

Abstract. *The formation of information and digital competence of young people during the educational process is key in the education systems of both economically developed countries and in the professional education of Ukraine. Digital content creativity is one of the criteria for measuring the level of information and digital competence skills of education seekers and, accordingly, its importance as an important component of digitalization of education as a whole is actualized. The experience of using YouTube video hosting to create author's educational digital content is highlighted.*

Keywords: *digitization, technologies, educational television, digital content.*

Сучасний етап розвитку освіти пов'язаний з широким використанням сучасних інформаційно-комунікаційних технологій (ІКТ) і можливостей, що надаються глобальною мережею Інтернет. Інформаційні технології значно розширюють можливості подання навчальної інформації. Диджиталізація в освіті є фундаментальним чинником економічного зростання в сучасних умовах. Розвиток Digital Agenda for Europe передбачається за такими напрямами: цифрове суспільство; розумне життя; комунальні послуги; кібербезпека і конфіденційність; Інтернет довіра; дослідження та інновації; доступ та комунікації; цифрова освіта (стартап Європи; дані; хмарні технології; майбутнє Інтернету; консультанти тощо) [1; с. 2].

У зв'язку з цим вирішального значення набувають віддалений доступ до освітніх ресурсів, опублікованими в Мережі, і можливість оперативного спілкування всіх учасників освітнього процесу. Наразі, вже всі розумі-

ють, що Інтернет має колосальні інформаційні можливості і не менш вражаючі послуги. Поширенню диджиталізації в освіті сприяє запровадження 3G-зв’язку, за допомогою якого розповсюджуються цифрові технології. В Україні поступ диджиталізації успішно відбувається у напрямах електронного навчання (elearning), ІТ (інформаційних технологій), ТКП (телекомунікаційні послуги) тощо [2; с. 3].

Однак, якими б властивостями не володів той чи інший засіб навчання, інформаційно-предметне середовище, первинні дидактичні завдання, особливості пізнавальної діяльності учнів, зумовлені певними цілями освіти. Інтернет з усіма своїми можливостями і ресурсами – лише засіб реалізації цих цілей і завдань.

Мета освітніх програм (цифрового контенту) – розширювати кругозір, допомагати сприймати красу світу, просвіщати. Відбувається це в різних формах через відеохостинг YouTube: випуски освітніх новин, ток-шоу, документальних кінофільмів, розважальних передач, спектаклів, кінофільмів, телевізійних лекцій, ігрових навчальних шоу. Основним багатофункціональним завданням освітнього телебачення вважається поширення навчально-культурної інформації, сприяння в навчанні та сприйнятті нових знань різних значень і типів (освітнє завдання).

Так, наприклад в Китаї освітнє телебачення стало “ареною” освітньої реформи. Телебачення постійно пропагує інноваційні освітні концепції, сприяє просуванню реформ, виконуючи свою організаційну функцію. Японське освітнє телебачення відоме якісними передачами про культуру, своїми документальними фільмами. Освітнє телебачення в Південній Кореї вважається головним інструментом виховання людей протягом усього їхнього життя. Особлива увага приділяється позаурочному вихованню. Зміст програм безкоштовного освітнього телебачення США включає дитячі передачі, телевізійні уроки по університетським науковим дисциплінам. Англійське публічне телебачення являє собою цілий спектр високоякісних освітніх послуг, що охоплює всі рівні підготовки аудиторії.

Освітнього телебачення в Україні в даний час в чистому вигляді не існує. Функції освітнього телебачення частково перейшли до дистанційного виховання з застосування новітніх телевізійних технологій та Інтернету.

Цифрові продукти можемо розглядати як проєкти, які створюються власноруч здобувачами закладів професійної освіти під керівництвом педагогічного працівника для подальшого розміщення на відеохостингу YouTube. Телеканали об’єднують у спільноту не тільки здобувачів освіти, але й їх однолітків-друзів, батьків.

Завдання, які можна виконувати за допомогою власного Інтернет-телебачення: включення матеріалів мережі в зміст уроку (інтегрування їх в

програму навчання); самостійний пошук інформації учнями в рамках роботи над проєктом; поглиблене самостійне вивчення іноземної мови, ліквідація прогалин в знаннях, уміннях, навичках; самостійна підготовка до складання кваліфікаційного іспиту чи ЗНО; систематичне вивчення певного аспекту іноземної мови дистанційно під керівництвом викладача; підвищення мотивації і створення потреби в вивчення іноземної мови за допомогою живого спілкування; формування і розвитку умінь і навичок читання, безпосередньо використовуючи матеріали мережі різного рівня складності; формування і розвитку умінь і навичок аудіювання на основі автентичних звукових текстів мережі Інтернет, також відповідно підготовлених викладачем.

Викладачі також мають наразі технічні можливості для запису своїх лекцій на відео і викладення їх в Інтернет. Для "перевернутого навчання" характерно використання водкастів (vodcast), подкастів (podcast) і преводкастингу (pre-vodcasting). Подкаст (Podcast) – це звуковий файл (аудіолекція), який його творець розсилає по підписці через інтернет. Одержувачі можуть завантажувати підкасти на свої пристрої (стаціонарні і мобільні) або слухати лекції в режимі онлайн.

Водкаст (Vodcast) – це відеофайл (відеолекція).

Преводкастінг (Pre-Vodcasting) – це метод навчання, при використанні якого викладач створює водкаст зі своєю лекцією, щоб здобувачі освіти отримали уявлення про тему ще до заняття, на якому ця тема буде розглянута.

Таким чином, застосування цифрового контенту в освітньому процесі є відповіддю на виклики візуального повороту, що характеризує сучасне суспільство і дозволяє вирішити задачу індивідуалізації освітнього простору, що є однією з головних тенденцій освіти XXI століття.

За наслідками аналізу педагогічної практики в закладах професійної освіти можемо зробити висновок, що цифровий освітній контент на Інтернет-каналах має великий потенціал для розвитку процесів диджиталізації освіти. В цілому, освітнє Інтернет-телебачення на даний момент не здатне замінити класичної освіти, але воно може бути хорошим доповненням до базової освіти та до саморозвитку молодої людини.

Інформаційні джерела

1. Digital Agenda for Europe. URL : http://ec.europa.eu/digitalagenda (дата звернення : 01.12.2017).

2. The Global Information Technology Report. Growth and Jobs in a Hyperconnected World. URL : www.weforum.org/gitr_version.pdf (дата звернення: 27.02.2018).

З М І С Т

СЕКЦІЯ 1

КІБЕРБЕЗПЕКА

НАПРЯМ 1. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Секція 2

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

НАПРЯМ 7.
ПРИКЛАДНЕ ТА СИСТЕМНЕ ПРОГРАМУВАННЯ

НАПРЯМ 8.
МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

НАПРЯМ 11.
ОРГАНІЗАЦІЯ БАЗ ДАНИХ І ЗНАНЬ

НАПРЯМ 12.
ТЕХНОЛОГІЇ ВІЗУАЛІЗАЦІЇ ДАНИХ

НАПРЯМ 13.
ОПЕРАЦІЙНІ СИСТЕМИ

НАПРЯМ 14.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ ПРОЄКТАМИ

НАПРЯМ 15.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції
ІБІТ 2022

Відповідальні за випуск **Ростислав ТКАЧУК**
Олександр ПРИДАТКО

Оригінал-макет **Ростислав ТКАЧУК,**
Андрій ІВАНУСА

Видано в авторській редакції

Підписано до друку 30.11.2022 р.
Формат 60×84/16. Папір офсетний. Друк цифровий.
Умовн. друк. арк. 22,09. Обл.-вид. арк. 20,55.
Наклад 100 прим.

Видавець і виготовлювач: ТОВ "Растр-7"
79005, м. Львів, вул. Кн. Романа, 9/1.
Тел./факс: (032) 235 72 13. E-mail: rastr.sim@gmail.com
www.rastr-7.com.ua
Свідоцтво суб'єкта видавничої справи
ЛВ № 22 від 19.11.2002 р.

IV International Scientific and Practical Conference
CYBERSECURITY AND INFORMATION TECHNOLOGY
CIT 2022

November 30 - 2022 Lviv - Ukraine

РАСТР·7

ISBN 978-617-8134-79-2