MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
KYIV NATIONAL UNIVERSITY OF CONSTRUCTION AND ARCHITECTURE

MINISTRY OF EDUCATION OF IRAQ
ALRAFIDAIN UNIVERSITY COLLEGE

UNIVERSITY OF BIELSKO-BIALA
MINISTRY OF EDUCATION AND SCIENCE OF POLAND

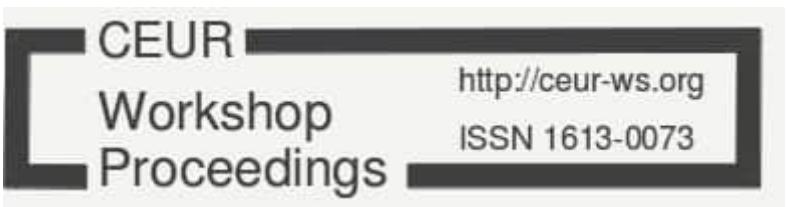
The 1st International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Things

«TTSIIT»

January 19th – 20th 2022

Ukraine-Iraq-Poland

РЕДАКЦІЙНА КОЛЕГІЯ:



СТАТТІ, РЕКОМЕНДОВАНІ ДЛЯ ПУБЛІКАЦІЇ У ВИДАННІ, ЯКЕ ІНДЕКСУЄТЬСЯ У НАУКОМЕТРИЧНІЙ БАЗІ SCOPUS
RECOMMENDED IN SCOPUS

ВСТУПНЕ СЛОВО. INTRODUCTORY WORD

Петро Куліков

Професор, доктор економічних наук,
Ректор Київського національного університету будівництва і архітектури.
Почесний академік Національної академії педагогічних наук України,
Лауреат Державної премії України в галузі науки і техніки.
Заслужений працівник освіти України,
Президент Спілки ректорів закладів вищої освіти України,
Віце-президент Будівельної палати та Академії будівництва України

Шановні учасники конференції!

Між нашими Університетами підписані Меморандуми про співпрацю. І сьогодні ми маємо нагоду прийняти участь у спільному заході – конференції, яка організована ініціативними групами наших університетів.

Наш університет готує фахівців з будівельних та архітектурних спеціальностей, а також зацікавлений у підготовці фахівців з таких перспективних напрямків, які сьогодні будуть обговорюватися на конференції. Тема конференції на сьогоднішній день є дуже актуальною, тому що в будівництві впроваджуються нові технології, такі як “Розумний будинок”, “Розумне місто” та впроваджуються технології Інтернету речей при експлуатації житлових та промислових будівель. КНУБА має тісні партнерські зв’язки з будівельними компаніями та може запропонувати архітектурні та будівельні рішення та проекти житлових та промислових об’єктів.

Сподіваюсь, що робота конференції буде плідною, ми виступимо з доповідями та поділимося результатами своїх наукових досліджень.

Бажаю успіху!

IMAGE DENOISING IMPROVEMENT USING SINY-SOFT WAVELET THRESHOLDING

Ibraheem H. M. Al-Dosari[1], Ibrahim Beram Jasim[2]

[1] *Al-Rafidain University College, computer communications engineering department, Baghdad, Iraq*
[2] *Alqalam University College, electrical and computer engineering department, Kirkuk, Iraq*

Abstract

The problem of image denoising plays an important role in the field of image processing due to the noise foundation in any life medium that will causing image corruption, the goal of the paper is to present a new proposed thresholding technique for image denoising.

The aim of the work is to evaluate the new proposed thresholding method and make a comparison with other denoising methods in the recent literatures using some common performance measure. A wavelet based denoising algorithm is proposed to improve the image quality; different methods are listed for comparative study and evaluation. The procedure for wavelet based denoising method is to calculate the wavelet transformation for the noisy image, then thresholding the coefficients in the wavelet domain with new proposed thresholding and proper selected threshold other parameters. The evaluation process involved of suing PSNR as a performance metric among various introduced denoising methods. The proposed thresholding method has been implemented using Matlab simulation program for denoising image and improves its quality. The obtained results have confirmed the proposed thresholding method operability and permit for recommending the new proposed method for solving the problem of noisy image by improving its quality though the proposed method. The prospects for further research can involve the investigation for proposed method operability with signal and image applications and other life and practical problems.

IMPACT OF NOISE INSIDE SERVER ROOM

Ahmed Alnuaimy[1], Oleksii Shushura[2], Genadiy Zhyrov[3]

[1] *School of Engineering, St. Mary's University, San Antonio, Texas, USA*
[2] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine*
[3] *Taras Shevchenko National University of Kyiv, Kyiv, Ukraine*

Abstract

Hearing loss is a major health issue in the work environment. Exposing humans to excessive sound levels or frequencies can adversely impact the ability of workers to communicate or hear. Noisy environments inside data centers present a unique occupational safety exposure to staff and operators which spend a considerable amount of time in the rooms to perform daily tasks. The specific sound frequency emitted by servers may also have a negative impact on worker performance and well-being which has not been analyzed in the past as this is an emerging technology. Specific opportunities may exist by analyzing the characteristics of the sound signal produced from servers in the server rack partially cancel the sound waves through similarity, time-delay and the correlation for the produced signals.

SIMULATION OF A NEW ALGORITHM TO ENHANCE THE SPECTRAL EFFICIENCY OF 5G FOR IOT APPLICATIONS

Ahmed A. Thabit[1], Jawad H. M.[2], Jawad A. M.[3]

[1] Computer Communications engineering department, Al-Rafidain University College, Baghdad, Iraq
[2] Department of Technical Computer Engineering, Al-Rafidain University College, Iraq
[3] Department of Technical Computer Engineering, Al-Rafidain University College, Iraq

Abstract

The wireless communication systems witness a huge developments in the mobile generations (1G to 5G and recently 6G). These generations is available to satisfy the users need. The basic goal of this paper is to simulate a 5G system in the physical layer for IoT applications.

A proposed model in this paper is a sensing system for various signals schemes at different noisy channels. The model depends on new radio (NR) to work at high frequencies in wireless communication applications and IoT applications. The design of the system was based on using a variety types of modulation most commonly used in communication systems: OFDM, 8PSK and MQAM. Matlab simulation tools is used to implement the proposed system, where signals of various lengths and different types of noise were taken. The noise types such as AWGN, phase noise, frequency offset and Dc offset are applied to check the efficiency of the aimed system.

The proposed 5G system have been implemented in software by matlab simulation tools to evaluate the results through constellation diagram, frequency spectrum and time scope shows a good response

Obtained results from this work shows a good results in terms the frequency spectrum and. constellation diagram. 5G is the attractive newest technology that must to be studied in details, especially for communication engineers.

INTERNET SECURITY IMPACT ON E-BANKING USERS

Mohammed Khodayer Hassan[1], Ali Hassan[2], Aymen Mohammed Khodayer[3], Omer Mohammed Khodayer[4]

[1] Al-Rafidan University, Department of Computer Science, Baghdad, Iraq
[2] Institutes for post graduate studies, Iraqi commission for Computers & Informatics, Baghdad, Iraq
[3] Al-Farhidai University, Head of the Department of Communication Engineering Baghdad, Iraq
[4] Polteckina University of Bucharest, the Department of Telecommunication Engineering, Bucharest, Romaine

Abstract

Information technology has been used widely in different sectors in daily task to fulfill Customers and organization's needs. Banking business is one of the main trends that use information technology in wide range. Customers can deal with banks through Websites which E-banking or using a credit card at an ATM what it is called. One of the most important factors in the success of electronic banking services is security. A strong security system is critical for a safe banking system in order to prevent hacking of the client's banking account and any private information of the customers in the bank system's databases. Any of the tasks can only be performed by legal or authorized personnel. As a result, bank systems must ensure that their transactions run as they should, in a secure manner, and that no activities occur that could result in a loss to the bank organization and its clients or customers. Banking account hacking has resulted in millions of dollars in losses in the wild world due to security system vulnerabilities. That kind of paper discusses the attacks on the banking system, the importance of the robust security system and the security measures that have been taken to prevent a great lost to the financial institution. Recommendations have been made to prevent any intrusion in the future. This paper shows the security trends to word helping customer and banks in their works to get better performance in doing their jobs by using electronic banking system.

ADVANCED SMART ALGORITHM FOR INTEGRATING RFID AND IOT SECURITY

Aseel Khalid Ahmed[1], Ammar Falih Mahdi[1], Dmytro Khlaponin[2]

[1] Al Rafidain University College, College of computer communications Engineering, Hay Al - Mustansiriyah, P. O. Box 46036, Baghdad, Iraq
2 Kyiv National University of Construction and Architecture, Povitriflotskyi Ave., 31, 03037, Kyiv, Ukraine

Abstract

This research is an exploration into developing a system for enabling Radio Frequency Identification (RFID) labels to be connected to the Internet while taking into account their unique impediments. Additionally, this mechanism enables the tag to be extraordinarily distinct and spoken to as a communication material capable of communicating with other participants, which can facilitate and rearrange the use of the "Internet of Things" concept in the not-too-distant future.

To build a mechanism capable of connecting RFID labels to the Internet. The methods taken by various researchers are investigated and dissected, enabling a better understanding of the difficulties and shortcomings associated with RFID labels connected to the Internet. The analysis and examination have resulted in the creation of another system that allows use of TCP/IP. The structure established in this paper is predicated on the capability of RFID labels to be used as procedures (TCP forms) within a host. As a result, each procedure has a procedure ID or port number, which enables various members to identify and communicate with the tag through the process ID. This is accomplished through a built-in interpretation portion that converts the RFID tag's authentic personality (ID) to a new ID that can be recognized as a TCP port number.

The results of this paper show that the system worked effectively for the purpose for which it was designed. The results show that the actualized system enables RFID labels to be linked to the Internet and to be exceptionally distinct. Additionally, it enables labels to send and receive information and guidance outside of the RFID system, through the Internet, and from various members. The framework's success would provide several experts with opportunities to actualize the concept of "Internet of Things".

IOT-BASED PAIN MONITORING AND MANAGEMENT SYSTEM

Fouad Jameel Ibrahim Alazzawi[1], Marwa Azzawi[2], Madiha Fouad Jameel[3], Yurii Khlaponin[4]

[1] Computer Engineering Department, Al-Rafidain University college, Baghdad, Iraq
[2] Biomedical Engineering Department, Al-Nahrain University, Baghdad, Iraq
[3] Department of Dentistry, Al-Rafidain University college, Baghdad, Iraq
[4]Kyiv National University of Construction and Architecture, Povitriflotskyi Ave., 31, 03037, Kyiv, Ukraine

Abstract

Patient suffering from pain is in need for an immediate medical intervention, however in some cases self-pain assessment is not available due to unconsciousness or prone to errors due to observer's biases. Therefore, automated pain assessment and management is needed. The internet of things (IoT) revolution along with biosensor technology could be convenient for pain assessment and management application. Therefore, this paper is a mini-survey of the literatures in this field published in six years (2016-2021) was conducted in three online databases. Hundreds of papers were found, however after title, abstracta and contents screening only 13 papers were included. This paper is aimed to review the papers that suggest a pain assessment model in a IoT philosophy, in order to summarize the present work and propose new suggestions for future work. Research with different pain levels, in a bigger and real patient population with different diseases were suggested in the conclusion for future work.

A NOVEL MINIMIZED ENERGY ROUTING TECHNIQUE FOR IOT ASSISTED WSN

Hazem N. Abdulrazzak[1], Aya A. Hussein[2], Alexander Kuchansky[3]

[1] Al-Rafidain University College, Baghdad, Iraq.
[2] Gilgamesh Ahliya University-GAU Baghdad, Iraq
[3] Kyiv National University of Construction and Architecture, Povitriflotskyi Ave., 31, 03037, Kyiv, Ukraine

Abstract

The problem of routing in WSN (Wireless Sensor Network) is to minimize the energy consumption during data transmission, the IoT (Internet of Things) monitoring system use the horizontal clustering of WSN to achieve this goal. The goal of this work is to create multi clusters with multi cluster head to communicate with sink node, the sink node directly connects to IoT server. A set of clusters has been created by dividing the WSN area in to 5 clusters horizontally, in each cluster the CH (Cluster Head) collects the data from all sensor nodes and communicate with sink node. The energy consumption is calculated based on wireless radio model and proposed clustering algorithm. The total energy consumption, normalized average energy and residual energy of proposed protocol is better than the two existing protocols that compared, the two protocols are PEGASIS (Power-Efficient Gathering in Sensor) and IEEPB (Improved Energy- Efficient PEGASIS- Based protocol). The results show that the H-IEEPB (Horizontal Improved Energy-Efficient PEGASIS- Based protocol) has an improvement in energy consumption and minimize it more than 10% and 25% compared with PEGASIS and IEEPB respectively, the residual energy and the normalized average energy also get good results compared with the others.

A NEW IMPLEMENTATION FOR MAXIMAL ITEMSETS MINER USING ORACLE PL/SQL

Hussein K. Khafaji[1], Mais A. Al-Sharqi[2], Oleksiy Nedashkivskiy[3], Pawel Falat[4]

[1] Al-Rafidain University College, Baghdad, Iraq
[2] University of Information Technology and Communications Baghdad, Iraq
[3] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
[4]University of Bielsko-Biala, 2 Willowa St, 43-309, Bielsko-Biala, Poland

Abstract

The problem of determining how to implement a data mining system as looslly-coupled or tightly-coupled remains a major challenge as it affects the performance of the system and the consumption of memory and computation resources.

The aim of the research is to propose a new approach to data mining design based on aggregating a data mining system with data intended for mining under the umbrella of database management systems. The authors produced a new algorithm to mine maximal itemsets depending on Bees' algorithm named Maximal Itemsets Mining Algorithm Based on Bees' Algorithm, MMIBA. MMIBA was implemented as loosely-coupled miner. This research presents a new implementation for MMIBA using Oracle PL\SQL. The aim of this implementation is to combine the mining system with the data to be mined. This approach excludes many drawbacks associated with other approaches such as the conflict of data environment and mining system environment, data transfer between these different environments, and data format conversion due to the mismatch of the formats that are supported by various environments. This approach dominants the loosely-coupled implementation in considerable amount of execution time and memory consumption. The proposed system was tested using many real and synthetic databases with wide range of properties including size, number of items, database sparseness or its density. Many values for minimum support and conflict were used in these tests to prove the robustness of the designed system. Experiments showed that the techniques of implementing mining algorithms affected their efficiency, and this was demonstrated by increasing the efficiency of MIMBA when it was implemented by collecting data with the miner that uses it in a single software environment.

IMPLEMENTATION AND EVALUATION OF COGNITIVE RADIO BY FPGA FOR IOT APPLICATIONS

Ahmed A. Thabit[1], Mikolaj Karpinski[2]

[1] *Al-Rafidain University College, Baghdad, Iraq*
[2] *Department of Computer Science and Automatics, University of Bielsko-Biala, Poland*

Abstract

The receivers have problems in the detection of signals from noisy signals at high frequencies. The object from this work is to evaluate of implemented cognitive radio to make a difference between signal and noise by FPGA and Arduino.

The basic goal of this paper is the implementation of cognitive radio at high frequency for IoT applications based on FPGA and Arduino. A model that has been proposed is a detection system to distinguish the signal from the noise. The model depends on cognitive radio (CR) to work at high frequencies in wireless communication applications and IoT applications. The design was based on the use of a variety of types of modulation most commonly used in communication systems, namely MFSK, MPSK and MQAM. Different and varied levels up to 256QAM and at high frequencies are used to simulate the existing reality and using the Matlab program for the purpose of simulating the proposed system in the work, where signals of various lengths and different types of noise were taken, such as AWGN and also FADING. After that, the system was trained based on Monte Carlo simulation and the use of neural networks. The practical implementation relied on the use of programmable chips such as FPGA and also ARDUINO, in order to achieve the principle of Internet of Things or device to device communication.

The proposed system have been implemented in software by matlab and practically using programmable digital devices (FPGA and ARDUINO) to evaluate the results. High detection probability are obtained with very low sensing time at low SNR value

The proposed system provide excellent results as shown in the paper that shows higher detection probability at minimum SNR. There is a good compatible of the results between the simulation and the practical results.

INTELLIGENT CLASSIFICATION ENHANCEMENT USING SINY-HARD WAVELET THRESHOLDING

Ibraheem H. M. Al-Dosari[1], Viktor Sykhomlyn[2], Alexander Sieliukov[3]

[1] *Al-Rafidain University College, computer communications engineering department, Baghdad, Iraq*
[2] *Vice-Rector forUkrainian State Employment Service Training Institute (USESTI), Ukraine*
[3]*Kyiv National University of Construction and Architecture, Povitriflotskyi Ave., 31, 03037, Kyiv, Ukraine*

Abstract

Many signal transmission over communications system face an inherent noise attack the transmitted signal and cause the degradation in the signal quality at the receiver end. One of the popular techniques to overcome this noise attack is to make a prepossessing for the noisy signal before transmission over the channel. The aim of the work is to use Wavelet based signal denoising method for noise removal and enhance the intelligent classification results.

In this work a new proposed wavelet thresholding method is formulated and implemented for signal enhancement. The proposed method is compared with classical method using different performance indices such as NMSE (normalized mean square error) and ESNR (enhancement in signal to noise ratio).

The results for new proposed method shows outperforming 10% in ESNR and 5 % in NMSE when using symlet8 wavelet mother function with5 decomposing levels.

The conducted results have confirmed the success for the new proposed wavelet thresholding method in signal denoising, this enhancement in processed signal will improve the signal quality at the receiving end and increasing signal to noise ratio enhancement for the overall communication system.

NEAR FIELD WPT CHARGING A SMART DEVICE BASED ON IOT APPLICATIONS

Aqeel Mahmood Jawad[1], Nameer Hashim Qasim[2], Haider Mahmood Jawad[1], Mahmood Jawad Abu-Alshaeer[1], Rosdiadee Nordin[3], Sadik Kamel Gharghan[4]

[1] Al-Rafidain University College, Iraq, Baghdad, Filastin Street, 10064
[2] Kyiv National University of Construction and Architecture, Kyiv, Ukraine
[3] Universiti Kebangsaan Malaysia, Malaysia, Bangi, Selangor 43600
[4] Middle Technical University, Baghdad, Iraq,

Abstract

Near-field wireless power transfers (WPTs) have seen major developments in recent years due to the increasing popularity and availability of smart devices for the Internet of Things (IoT) applications. To improve the power transfer energy (PTE) and transfer distance for charging smart mobile phones based on MRC by designing a copper wire coil to solve the air gap problem between the transmitter and receiver coils. As an energy-harvesting technique based on magnetic resonator coupling (MRC), WPT can charge batteries in smart devices, especially in mobile IoT devices where changing the batteries can be inconvenient. In this study, the multi-different copper wire coil (MDCWC) cover shield and double-receiver copper wire coil (DRCWC) systems were proposed to deliver power to devices with low-power consumption with a P-P topology using a Royer oscillator in one important scenario. The design scenario was implemented using the MDCWC in the transmitting and receiving circuits. However, three loads were used to test the performance metrics of the system, namely, 20, 50, and 100 Ω for home appliances. To achieve the aim, two near-field WPT techniques a DRCWC and MDCWC were designed and developed. An MDCWC having a covered copper wire coil design improved transfer power to 5.04 W and efficiency to 84% at 20 mm with a 100 Ω loaded systemin alignment condition. The results revealed that the coil geometry contributed to improving the performance metrics in terms of transfer power efficiency and transfer distance. The corresponding transfer power and efficiency values for the MDCWC were 5.04 W and 84% at 20 mm, 4.2 W and 70% at 60 mm, and 3.02 W and 50.37% at 150 mm, respectively, whereas the theoretical result of the transfer efficiency was 96%. However, the theoretical and experimental studies proved that the DRCWC prototype could be used to charge cell phones with a maximum air-gap range of 10 to 300 mm between the transmitter and receiver coils. Lastly, it should be noted that the proposed system can charge one device.

IOT AND E-LEARNING WITH THE IMPACT OF COVID 19 PANDEMIC LOCKDOWN ON THE UNDERGRADUATE UNIVERSITY STUDENT BLOOD PRESSURE LEVELS: EDUCATIONAL PAPER

Talib A. Al-Sharify[1], Zinah A. Alshrefy[2], Hussein Ali Hussein[3], Zainab T. Al-Sharify[4,5], Helen Onyeaka[5], Mushtaq T. Al-Sharify[6], Soumya Ghosh[7]

[1] Al Rafidain University College, College of computer communications Engineering, Hay Al - Mustansiriyah, P. O. Box 46036, Baghdad, Iraq
[2] Quality Assurance and University Performance Department, University Presidency, Northern Technical University, Mosul/Iraq
[3] University of technology, production Engineering and Metallurgy, Baghdad, Iraq
[4] School of Chemical Engineering, University of Birmingham, Edgbaston B15 2TT, UK
[5] Environmental Engineering, College of Engineering, University of Mustansiriyah, Baghdad, Iraq
[6] Radio Engineering and Radio Electronics Systems department, Radio physics, Electronics and Computer Systems Faculty, Taras Shevchenko National University of Kyiv, 03127, Kyiv, Ukraine
[7] Department of Genetics, Faculty Natural and Agricultural Sciences, University of the Free State, Bloemfontein 9301, South Africa
Corresponding author: Z.t.alsharify@uomustansiriyah.edu.iq

Abstract

Since December 2019, Millions of people around the world suffer from the effects of hypertension due to COVID 19 pandemic and all the stressed caused by this new virus. Around 40-50% of people worldwide can be assumed to have some form of hypertension especially after the pandemic lockdown. However, the advancement of using the new technologies, IoT and the E-learning during this lockdown period can support the education performance of the university students and continue their study without spreading the virus due to the direct contact with infected patients. This paper will study and compare the factors that contribute to hypertension which are caused by changes in systolic and diastolic blood pressure during this lockdown period. many students were surveyed and their blood pressures (BP)were monitored using automatic devices. The BP of undergraduate students during the lockdown period were identified as having higher systolic and diastolic readings however the results reflected no direct causation between stress and blood pressure, and rather were representative of the factors which will be studied further in this paper. The readings are compared with the definitions of hypertension according to the American Heart Association (AHA). A thorough understanding of the factors is important in the field of Internet of medical things (IoMT) medicine and therapy to help patients suffering from hypertension and to monitor this situation.

METHOD OF FORMING COMPLEX SERVICES IN NETWORKS USING VIRTUALIZATION TECHNOLOGY OF NETWORK FUNCTIONS

Yurii Khlaponin[1], Muhi-Aldin Hassan Mohamed[2], Alexander Nikitchyn[3]

[1] Kyiv National University of Construction and Architecture, Povitriflotskyi Ave., 31, 03037, Kyiv, Ukraine
[2] Al Iraqia University, hayba Katoon, Street 22, Avenue 308, 7366 Haifaa, Baghdad, Iraq
[3] Taras Shevchenko National University of Kyiv, Volodymyrska St., 60, 01033, Kyiv, Ukraine

Abstract

NFV technology allows you to replace physical network devices with certain functions with their software image as virtual network devices that perform the same functions on public server equipment. In order to cover the whole range of solutions for providing the required quality of service, it is necessary to develop a method for increasing the QoS level, in the absence of services with the required level of quality of service. In order to solve the problem, a mathematical method for the formation of a distributed complex service based on the information on available atomic services in the network is proposed.

The proposed method allow to increase the reliability and performance of the requested services. Applying the method of forming a distributed service and a method to increase the reliability of the service will allow to supplement and improve the mechanism of formation of services with the required quality indicators, increase the number of better services in the network, reduce the load of services with high PCs through the use of services with lower values of parameters QoS.

TECHNOLOGY IN THE INDUSTRIAL REVOLUTIONS AND ITS IMPACT ON THE KEY PERFORMANCE INDICATORS OF ORGANIZATIONS

Oleg Zaritskyi[1], Oleksandr Ponomarenko[2]

[1] National Aviation University, Liubomyra Huzara Ave, 1, Kyiv, 03058, Ukraine
[2] Professional College of Engineering and Management of the National Aviation University, Metrobudivska str., 5a, Kyiv, 03065, Ukraine

Abstract

Context. The article considers topical issues of interconnection of life cycles of business, production, product models of enterprises and key indicators of their activities through the prism of the evolution of information systems, their impact on the pace of development of enterprises and the role that information systems play in industrial revolutions.

Objective. The overall objective of the study is to assess the impact of information systems on the development of enterprises in the process of industrial revolutions by assessing the key performance indicators covering all perspectives (functional areas of enterprise development) of the balanced scorecard as one of the progressive systems of strategic management of organizations.

Method. Formalization of key performance indicators through the mathematical apparatus was carried out using the methodology of strategic management of the enterprise - the balanced scorecard.

Results. The study formalized the types of basic IS and software, their impact on the development processes of enterprises during the industrial revolutions by assessing certain key performance indicators in terms of the balanced scorecard methodology, which was first described using a mathematical apparatus.

Conclusions. The main directions of transformation of modern production are defined by three global technological trends: network integration, intellectualization and flexible automation. The development and widespread implementation of IP has doubled the pace of technological revolutions and, in fact, determines all further enterprise development strategies within these technological trends. The next (fifth) industrial revolution will be defined exclusively by the development of data science and the transition to new system architectures of computing systems or their combinations, for example using neurosynaptic and quantum computers, which will allow using all the possibilities of industrial Internet of Things and Digital twin's concepts in almost real time.

ASSESSMENT OF POSSIBILITY OF MODERNIZATION OF HIERARCHY CODE STRUCTURE OF MULTIDIMENSIONAL SIGNAL TO INCREASE THE EFFICIENCY OF FUNCTIONING OF EDUCATIONAL AND TRAINING TELECOMMUNICATION SYSTEMS

Oleksandr Golubenko[1], Andrii Onysko[2], Andriy Lemeshko[3], Andrii Zelnytskyi[4], Oleg Zabolotnyi[4], Andrii Zakharzhevskyi[4], Oleksandr Turovsky[5]

[1] State University of Telecommunications, 7, Solomenska str., Kyiv, 03110, Ukraine
[2] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37, Prosp. Peremohy, Kyiv, 03056, Ukraine
[3] State University of Telecommunications, 7, Solomenska str., Kyiv, 03110, Ukraine
[4] National Defence University of Ukraine named after Ivan Cherniakhovskyi, Povitroflotskyi ave. 28, Kyiv, 03049, Ukraine
[5] National Aviation University, Lubomyr Husar ave. 1, Kyiv, 03058, Ukraine

Abstract

Context. In order to increase the efficiency of modern functioning of educational and training telecommunication systems, research is currently being conducted to increase the amount of information transmitted, its security and speed of transmission through communication channels. One of the directions of such work is the introduction of the approach to the use of multidimensional signals when using them in continuous information transmission channels of educational and training telecommunication systems. The results of research conducted in recent years show that to ensure high quality information transmission in continuous channels can be a method of joint demodulation and decoding operations in the process of performing a single procedure, which involves creating a code structure of multidimensional signal.

In the given article the questions of an estimation of possibility of modernization of a hierarchical code design of a multidimensional signal by a method of variation of its parameter for increase of efficiency of work of a continuous channel of information transfer in educational and training telecommunication systems are considered. It is established that the hierarchical code construction of a multidimensional signal, when applied, has the potential to increase the speed of information transmission through a continuous channel. This can be done by upgrading the specified code structure of the signal by reducing the signal distance.

The influence of the reduction of the signal distance on the efficiency of the hierarchical code construction is estimated. It was found that by reducing the signal distance of the hierarchical code structure of the signal from 2 or more times, the signal transmission rate can increase and reach up to twenty percent. The implementation of the modulation procedure has no fundamental difficulties, provided that for each code of the code structure known coding procedure using binary codes. The obtained results allow to build a sufficiently accepted procedure for demodulation according to the hierarchical code constructions of the signal with a simultaneous increase in the data rate in the continuous channel that will use such a code construct.

INFORMATION TECHNOLOGY OF INFORMATION SECURITY AUDIT OF OBJECTS OF CRITICAL INFRASTRUCTURE

Igor Kozubtsov[1], Nataliya Lishchyna[2], Lesia Kozubtsova[1], Igor Trush[3], Andrii Yashchuk[2]

[1] Military Institute of Telecommunications and Informatization named after Heroes of Kruty, 45/1 Moscow street, 01011, Kyiv, Ukraine
[2] Lutsk National Technical University, 75 Lvivska Street, 43000, Lutsk, Volyn Region, Ukraine
[3] Legistation Institute of the Verkhovna Rada of Ukraine, 4 Nestorivsky prov., 04053, Kiyiv, Ukraine

Abstract

Context. The scientific and practical task to substantiate the mathematical apparatus on the basis of which the information technology of information security audit of critical infrastructure is developed, which provides verification of compliance of critical infrastructure with the general requirements approved by the Cabinet of Ministers of Ukraine dated 2019-06-19, No.518. A security audit is one of the most effective measures to increase the level of information security of the critical infrastructure. Objective. The purpose of the work is to create information security audit of critical information infrastructure on the basis of separate partial solutions of information technology. Method. On the basis of the general requirements defined by the Resolution of the Cabinet of Ministers of Ukraine dated 2019-06-19, No.18 "On approval of the General requirements for cyber protection of critical infrastructure objects" a set of indicators and evaluation criteria was proposed. The structure of future information technology was offered. In accordance with the structure of information technology, the stages of the methodology of information security audit of critical infrastructure were built. The technique contains a simple mathematical apparatus that simplifies calculations even in Microsoft Excel spreadsheets. In this paper, in contrast to the known methods and techniques, it is proposed to take into account the weight of the importance of information security requirements. As a result, the method has become sensitive to the most critical requirements for cybersecurity of critical infrastructure. Results. Information technology of information security audit of critical information infrastructure objects has been developed. Conclusions. The experiments in Microsoft Excel spreadsheets confirm the efficiency of the proposed method. It is advisable to recommend the development of software that would in practice automate the process of information security audit of critical information infrastructure. The scientific novelty of the obtained result is that for the first time the information technology of information security audit of critical infrastructure facilities was developed, which provides verification of compliance of critical infrastructure facilities with the general requirements approved by the Cabinet of Ministers of Ukraine dated 19 June 2019, No.518. The practical significance of the work lies in the possibility of developing information technology software. Prospects for further research in this area. The presented study does not cover all aspects of this problem. Theoretical and practical results obtained in the process of scientific research are the basis for further study in such areas as the development of information technology software.

ТЕЗИ ДОПОВІДЕЙ
ABSTRACTS OF REPORTS

ENSURING THE SAFE TRANSMISSION OF INFORMATION WHEN USING THE INTERNET OF THINGS

Kondakova A. M. – Postgraduate at the Department of Cyber Security and Computer Engineering, Kyiv National University of Construction and Architecture, Kyiv, Ukraine.

Kondakova S. V. – PhD. Assoc., Professor, Department of Cyber Security and Computer Engineering, Kyiv National University of Construction and Architecture, Kyiv, Ukraine.

Shabala Y. Y. – PhD. Assoc., Professor, Department of Cyber Security and Computer Engineering, Kyiv National University of Construction and Architecture, Kyiv, Ukraine.

АНОТАЦІЯ

Користуючись досягненнями Інтернету речей, мало хто замислюється про те, чи захищені дані, що передаються від датчиків. Розуміючи небезпеку перехоплення та несанкціонованої зміни інформації, у роботі розглядаються основні варіанти несанкціонованого доступу до інформації під час її передачі по кабелю та відкритому Інтернету та шляхи зниження ймовірності перехоплення даних.

КЛЮЧОВІ СЛОВА: Інтернет речей, захист інформації, середовище передачі інформації, класифікація інформації, протоколи тунелювання.

ABSTRACT

When using the achievements of the Internet of Things, few people think about whether the data transmitted from sensors is protected. Understanding the danger of interception and unauthorized changes in information, the paper considers the main options for unauthorized access to information during its transmission by cable and open Internet and ways to reduce the likelihood of data interception.

KEYWORDS: Internet of Things, information protection, information transmission medium, information classification, tunneling protocols.

1. HOW TO MAKE SAFE SIGNAL TRANSMISSION FROM THE SENSOR TO THE ADMINISTRATOR?

In today's world, data protection from a variety of sensors, CCTV cameras, and more plays an important role.

Next, we will consider the problem of protection of information transmitted in digital and analog form by various communication channels on the example of IP camera and temperature sensor.

1.1 ENSURING SECURE DIGITAL DATA TRANSMISSION OVER THE INTERNET

To begin with, consider the principle of operation of the IP camera. The lens focuses the image on the matrix. The matrix converts color into an electrical signal. The signal is fed to the processor for processing color, brightness and more. The video stream arrives at the compressor. The compressor compresses the flow - the data is now ready to be transmitted to the network via an Ethernet controller. It is at this point that there is a need to implement additional measures to protect information.

Each IP camera has its own IP address, which is transmitted with the connection and is used to synchronize the camera with the recorder: using a command or a special program, the recorder uses the IP address of the camera and connects to it. Without an IP address, it is impossible to configure the equipment to work together, access the IP camera from a mobile device.

IP cameras work on the TCP / IP protocol stack. Therefore, for data protection, it is possible to use information security tools, such as IPsec, ssh-protocol that provides data encryption, or an extension of the tcpcrypt protocol itself. And if you use additional secure tunneling with OpenVPN or L2TP / IPsec, the probability of successful unauthorized access to data is quite small.

Another option to ensure an increased level of security of data transmission and information integrity is the use of electronic digital signature.

An electronic digital signature in accordance with ISO 7498-2 is the information obtained by cryptographic conversion of a data block, which allows the recipient to verify the integrity of the block and the authenticity of the source, as well as protection against forgery of the recipient.

This information is a cryptographic hash function, which is usually created with a length of 128 bits or more, which far exceeds the number of messages that will ever exist in the world. Many reliable cryptographic hash features are available for free. MD5 and SHA are widely known. The main mathematical methods used in EDS systems today are asymmetric transformations in rings, Galois fields and a group of points of elliptic curves.

Quite a good hardware and software solution for creating EDS is a complex of users of CSC "IIT User CSC-1".

Ensuring the integrity and irrefutability of the authorship of electronic data and documents circulating in the system is implemented by creating and verifying an electronic digital signature of data and documents, both on the user side of the system and on the server side.

The key certification center (CSC software and hardware complex) is used to organize the key system (key data management) of the complex.

The complex cryptographic algorithms and protocols are used in the complex:

- encryption algorithms according to DSTU GOST 28147: 2009 and TDEA and AES according to ISO / IEC 18033-3: 2010;
- EDS algorithms for DSTU 4145-2002, RSA for PKCS 1 (RFC 3447) and ECDSA for DSTU ISO / IEC 14888-3: 2014;
- hashing algorithms according to GOST 34.311-95 and SHA (SHA-1 and SHA-224/256/384/512) according to DSTU ISO / IEC 10118-3: 2005;
- key distribution protocols according to DSTU ISO / IEC 15946-3 (item 8.2) and RSA according to PKCS 1 (RFC 3447).

Formats of key data and other special information meet the requirements of international standards, recommendations and current regulations:

- formats of certificates and lists of revoked certificates - according to DSTU ISO / IEC 9594-8: 2006 and technical recommendations RFC 5280;
- formats of signed data (data from EP) - according to DSTU ETSI EN 319 122-1: 2016 and DSTU ETSI EN 319 122-2: 2016, technical recommendations RFC 5652 (PKCS 7) and 5126;
- secure data formats (encrypted data) - according to the requirements for cryptographic message formats and technical recommendations RFC 5652 (PKCS 7);
- Certificate status information request formats and Certificate status information response formats (OCSP protocol) - according to RFC 2560 technical recommendations;
- formats of requests for the formation of timestamps and timestamps themselves (TSP protocol) - in accordance with DSTU ETSI EN 319 422: 2016 and technical recommendations RFC 3161;
- private key formats - according to technical recommendations RFC 5958 (PKCS 8) and PKCS 12.

1.2 ENSURING SECURE DATA TRANSMISSION IN DIGITAL FORM BY WIRED COMMUNICATION LINES

In addition to transmitting data over the open Internet, it is possible to send information via wired transmission lines.

Wired connection provides stable and high-speed transmission, but requires the laying of networks limited by the length of the cable type: 100 m - for twisted pair, 500 m - for coaxial, 100 km - for fiber (excluding repeaters or switches). So it makes sense to consider only fiber-optic transmission lines to send data from sensors or cameras to the user.

Connecting to fiber-optic communication lines is quite difficult and expensive, because such a communication channel has no side radiation and requires at least careful removal of insulation. There are now many hardware solutions to combat the illegal interception of information from optical communication cables, from additional protection of the cable to the installation of reflectometers for continuous measurement of optical signal, which makes it impossible to intercept.

1.3 PROVIDING SECURE DATA TRANSMISSION FROM THE SENSOR IN ANALOG FORM OVER THE INTERNET

However, not all sensors transmit information in a digital signal.

If an analog signal coming from the Internet comes from the sensor, it is advisable to use an analog-to-digital converter, but it is necessary to avoid the possibility of error during the conversion. Then the signal is protected as in the previous case.

The scheme will look something like this:

Figure 1 – Information conversion scheme

1.4 ENSURING SECURE DATA TRANSMISSION FROM THE SENSOR IN ANALOG FORM, WIRED COMMUNICATION LINES

However, sometimes it is impractical to use analog-to-digital converters. In this case, the best solution is to transmit the signal over fiber-optic communication lines using amplitude or frequency modulation and the best possible control of the integrity of the communication line.

Although in most cases it is safer and more reliable to transmit information in digital form.

REFERENCES

1. https://trassir.dev.aurocraft.com/product-category/ip-kamery/
2. http://snegovik24.com.ua/articles/2021/videokamery_ip/
3. https://kanrit.com/blog/videosposterezhennya/ip-kamera-shcho-tse-take-yak-pratsyuye-yaki-buvayut-ip-kamery/
4. https://iit.com.ua//index.php?page=itemdetails&p=9&gtype=1&type=1&id=38
5. https://studopedia.su/16_51291_yuridichne-zabezpechennya-elektronnogo-pidpisu.html

CONCEPTUAL MODEL OF THE MOBILE COMMUNICATION NETWORK

Sieliukov A. – Doctor of Technical Sciences, Senior Research Officer, Professor at the Department of Cybersecurity and Computer Engineering, Kyiv National University of Civil Engineering and Architecture, Kyiv. Ukraine.

Qasim N. H. – PhD. Assoc., Department of Cyber Security and Computer Engineering, Kyiv National University of Construction and Architecture, Kyiv, Ukraine.

Khlaponin Y. - Doctor of Technical Sciences, Professor at the Department of Cybersecurity and Computer Engineering, Kyiv National University of Civil Engineering and Architecture, Kyiv. Ukraine.

АНОТАЦІЯ

Під концептуальною моделлю будь-якої системи слід розуміти її абстрактну модель, яка визначає структуру та властивості її елементів, а також враховує вхідні, вихідні параметри, зовнішні фактори та керуючий вплив. Мережа мобільного зв'язку в загальному вигляді є розподіленою в просторі технічною системою з програмно-технічними засобами обробки та обміну інформації (підсистемами). Запропонована концептуальна модель мережі мобільного зв'язку може бути застосована для розробки методології її подальшого розвитку.

КЛЮЧОВІ СЛОВА: структура, передача, термінал, індикатор, ресурс, пакети, мережа LTE.

ABSTRACT

The conceptual model of any system should be understood as its abstract model, which determines the structure and properties of its elements, as well as takes into account input, output parameters, external factors and control effects. The mobile network in general is a technical system distributed in space with software and hardware means of information processing and exchange (subsystems). The proposed conceptual model of the mobile communication network can be used to develop a methodology for its further development.

KEYWORDS: structure, transmission, terminal, indicators, resource, packets, LTE network.

The conceptual model of any system should be understood as its abstract model, which determines the structure and properties of its elements, as well as takes into account input, output parameters, external factors and control effects. Such a model in the most general form is determined by the dependence [1]:

$$Y^k = f\left(X^k(t), \mathrm{W}^k(t), \mathrm{U}^k(t), \mathrm{O}^k(t)\right),$$

де Y^k - initial parameters of the system, which consists of $k$classes of elements;

X^k - input parameters;

W^k - parameters of the internal state;

U^k - parameters of controlled influence;

O^k - parameters of external factors.

All parameters may change over time t.

Any communication system in general is a technically distributed technical system with software and hardware for processing and exchanging information (subsystems). The Mobile Network (MN) is not exclusive. For example, for MNs of the LTE standard at the input of such a system are UE (UserEquipment), the internal state is described by the network core, controlled influence is provided in eNodeB nodes, control the necessary flows and resources, external factors are usually interference, multi-beam reflection and others, the initial parameters of the system will be a significant number of indicators of quality of service.

The MN conceptual model can be built both for the general system and for its individual elements. Thus, [2] proposes an approach to building a conceptual model of a mobile network, which will provide adaptive management of resources and individual information flows to ensure end-to-end service quality in conditions of temporary lack of spectral resources and instability of the radio channel. This model is based on the use of the method of optimal distribution of radio resources. However, it is recognized that the proposed solutions concern only the allocation of resources at the base station level to the so-called channel level in order to rationally use resources to ensure quality of service within the LTE architecture. In fact, the mobile operator cannot guarantee the quality of service from end to end, because the packet data goes beyond the LTE level of the network core, namely the level of external IP-oriented networks does not provide any guarantees of quality of service. information flows in network nodes (routers) is based on certain methods of QoS, to which the mobile operator has no influence.

The vector of input parameters X^k can be set by a set of units, for example [1]:

$$X^k = \left[Q^{\mathrm{k,q}}, \mathrm{y}_{\mathrm{ij}^m}\right],$$

Де $Q^{k,q}$ - the number of terminal systems k-th traffic class q-th type;

y_{ij^m} - call intensity between nodes i and j network.

The vector of internal state parameters W^k can be set by a set of units, for example [3]:

$$W^k = \left[G, Z, H_{h^k}, V_{\mathrm{ij}}, p_{\mathrm{ij}}\right],$$

де G - type of communication network structure;

Z - communication system properties;

H_{h^k} - types of communication protocols;

V_{ij} - baud rate;

p_{ij} - probability of transmission error.

The structure of the communication network G is described by the unit

$$G = [\mathrm{G}^*, \mathrm{U}_s],$$

де $G*$ - many structures of functional subsystems;

U_s - many connections between functional subsystems.

There are [4] seven types of structures $G*$:

$$G*\left[G_d,G_f,G_a,G_m,G_v,G_p,G_g\right],$$

де G_d - structure of actions;

G_f - structure of functions;

G_a - abstract structure;

G_m - morphological structure;

G_v - the structure is variant;

G_p - spatial structure;

G_g - geometric structure.

The properties of the communication system Z are determined by the properties of its structural components Z^i, which can differ significantly from the properties of the communication system as a whole.

The parameters of controlled impact can be indicators of controllability and observability (monitoring). Controlled influence parameters reflect the type of communication system administration system, incl. security management systems:

$$U^k = [A^k,S^{k_h}(M_h)],$$

де A^k characterizes the network management system;

$S^{k_h}(M_h)$ - basic S- security services that are implemented M- protection mechanisms at the level $h$of logical structure [5].

Parameters of external factors O^k are a physical or technological process of internal or external nature, which can disrupt the functioning of network elements: informational influence on the equipment of network nodes, electromagnetic influence on the radio channel, etc. Very often in modern mobile networks, including radio segment there is a situation in which there are short-term channel failures due to temporary deterioration of the signal-to-noise ratio by various external factors, interference, multi-beam reflection, signal attenuation and others, which significantly affects the quality of service.

The initial parameters Y^k of the conceptual model of mobile communication networks, such as the LTE standard, may be the parameters of service quality QoS:

1. Allocated resource type: with guaranteed data rate (GBR) or non-guaranteed baud rate (Non-GBR);

2. Параметри QoS:

– QCI (QoS Class Identifier) - service quality class identifier.

– ARP (Allocation and Retention Priority) - priority of appointment and channel content.

- GBR (Minimum Guaranteed Bit Rate) - guaranteed baud rate.
- MBR (Maximum Bit Rate) - maximum baud rate.
- APN-AMBR (Access Point Name Aggregate Maximum Bit Rate) – total maximum baud rate for one access point.

– UE-AMBR (User Equipment Aggregate Maximum Bit Rate) – total maximum transfer rate for one user equipment.

Let's dwell on these parameters in more detail. Parameters such as QCI and Channel Assignment Priority (ARP) must be defined for each virtual connection. The QCI parameter is very important because it serves as a reference in determining the QoS level for each end-to-end EPS channel. In the case of bandwidth, the GBR and MBR are determined only in EPS streams with guaranteed data rates, while AMBR (APN-AMBR and UE-AMBR) are determined only in EPS streams with non-guaranteed speeds. Below we will explain each of the QoS parameters in the LTE network separately.

GBR resource type (with guaranteed data rate):

The presence of the GBR resource type in the EPS virtual connection means that the bandwidth of the communication channel is guaranteed. Obviously, GBR-type flow

EPS has an associated guaranteed data rate (which will be explained below) as one of the QoS parameters.

Only the selected virtual connection type can be a GBR stream, and the default EPS type cannot be one. The QoS identifier of the EPS stream with a guarantee of data rate can be in the range from 1 to 4.

Non-GBR resource type (with non-guaranteed data rate):

For an EPS virtual connection, the non-GBR type means resource allocation on the principle of "best of the best" (best effort), and bandwidth connection is not guaranteed. There is always a virtual virtual connection a stream with a non-guaranteed baud rate, while a dedicated virtual connection can be both a stream with a guaranteed and a non-guaranteed baud rate. The QoS ID of the EPS stream without a guaranteed data rate can be in the range from 5 to 9.

The QCI parameter, an integer from 1 to 9, indicates 9 different workers QoS characteristics of each IP packet. QCI values are standardized for individual QoS output characteristics, and each QCI contains the following standard performance characteristics (values):

The quality of service guaranteed for end-to-end EPS channel or logical data flow varies depending on the specified QCI values.

The QCI parameter, although an integer, is a specific node parameter that provides details on how the LTE node handles packet forwarding (eg, weighted scheduling parameters, input thresholds, queue thresholds, channel layer protocol configuration, etc.).

Determining in advance the performance of each QCI value and by standardizing them, network operators can ensure that the same the minimum level of QoS required by LTE standards is different services / applications. These services and applications are used in the LTE network, which consists of different nodes. QCI values are likely to be used mainly by eNBs (LTE base stations) to control the priority of packets transmitted over radio channels.

ARP is considered only when deciding whether to create new through channel EPS or not. After creating a new channel and transfer through it ARP packets do not affect the priority of the received packet and thus thus, the network node forwards packets regardless of their ARP values. GBR (UL / DL) This parameter is used for virtual connection type GBR and determines the bandwidth (data rate in bits), guaranteed by the LTE network. It is not used

for non-GBR streams with unguaranteed bandwidth (UL for uplink traffic and DL for downlink).

MBR (UL / DL) MBR is used for a flow type GBR and defines the maximum bit rate of data transfer that is allowed in the LTE network.

Any packets that enter the through channel are discarded after the specified MBR rate becomes exceeded.

Thus, the conceptual model of a mobile network will generally be too cumbersome, so it is better to build such a model to study a specific problem with a limited list of parameters. For example, the model of a mobile network of the 5G standard may be as follows (Fig. 1).

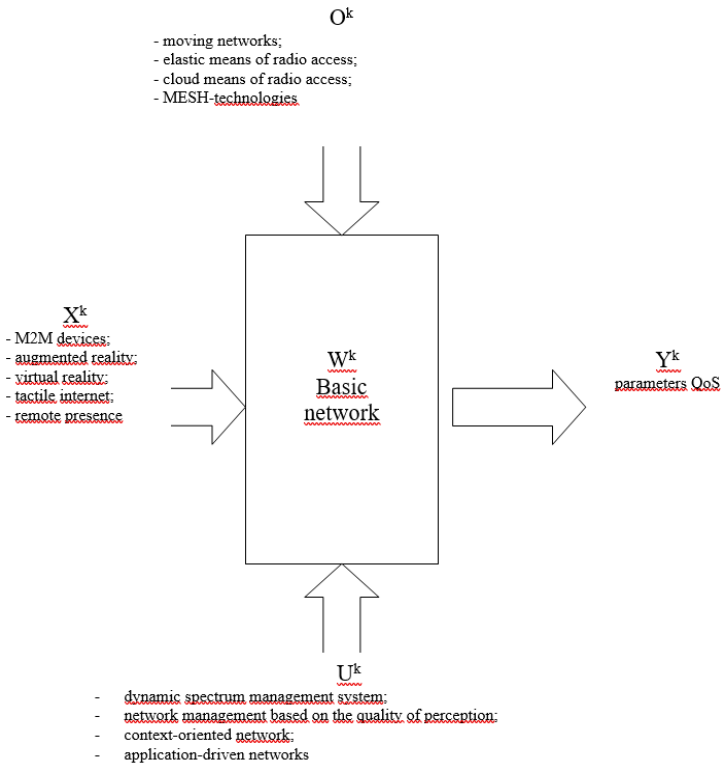


Fig.1. Conceptual model of a 5G mobile network

The proposed conceptual model of the mobile communication network can be used to develop a methodology for its further development.

REFERENCES

1. Пылинский М.В., Мякотин А.В., Кривцов С.П., Байсаитов Г.Н. Концептуальна модель сети связи специального назначения. // Радиотехника и связь. Серия «Естественные и технические науки». - № 11. - 2018. – С.67.
2. Бешлей Г. В. Моделі та метод оптимального розподілу мережних ресурсів в програмно-конфігурованих гетерогенних мережах мобільного зв'язку: дис. … доктора філософії: спец. 172. Львів: НУ «Львівська політехніка». - 2021. - 240 с.
3. Пирогов Ю.А. Методология исследовании систем и сетей военной связи: Учебное пособие. – СПб.: ВАС, 2016. – 164 с.
4. Исаков Е.Е., Мякотин А.В., Губская О.А., Кривцов С.П. Оптимальная цифровизация военных систем связи // Современная наука: актуальные проблемы теории и практики. Серия «Естественные и технические науки». - № 3-4. – 2017. – С.22-26.
5. Исаков Е.Е., Мякотин А.В., Жадан А.П., Кривцов С.П., Басулин Д.В. Оценка необходимых и достаточных значений реальной пропускной способности военных систем передачи информации. Информация и космос. // Радиотехника и связь. Серия «Естественные и технические науки». - 2017. – С.133-136.
6. Хлапонін Ю. І., Касім Н. Х., Симоненко О. А. Застосування технології LTE при впровадженні інтернету речей. Системи і технології зв'язку, інформатизації то кібербезпеки: актуальні питання і тенденції розвитку : Міжнар. науково-техн. конф., м. Київ, 25–26 листоп. 2021 р. Київ, 2021. С. 148–149.

NETWORK SYSTEM STRUCTURE DESIGN FOR DATA CENTERS

Shestak Y. V. – PhD, Department of Cyber Security and Information Security, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.

Tolupa S. V. – Dr. Sci., Professor, Department of Cyber Security and Computer Engineering, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.

Torchylo A. P. – Student, Department of Cyber Security and Information Security, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.

АНОТАЦІЯ

Контекст. Центри обробки даних є основними об'єктами, які підтримують високопродуктивні обчислення та великомасштабну обробку даних. Щоб гарантувати, що центр обробки даних може забезпечувати чудові властивості розширення та маршрутизації, мережа взаємозв'язку центру обробки даних має бути розроблена ретельно.

Мета. Метою роботи є аналіз методів структурування даних в ЦОД для побудови безпечної та ефективної системи ЦОД.

Метод. У цій статті описані основні моделі структурування даних в дата-центрах. Дослідження зосереджено на дослідженні основних напрямків застосування технології Big Data та визначенні взаємозв'язку між рівнем ефективності системи кібербезпеки та прибутковістю підприємств.

Результати. Досліджено основні методи, проаналізовані в даній роботі, для вирішення проблем зберігання та обробки даних в ЦОД.

Висновки. Проведене дослідження скоригував основні проблеми при використанні ЦОД та підтвердив шляхи вирішення деяких з них. Це дослідження допомагає зрозуміти найбільш ефективні способи структурування даних, а перспективи подальших досліджень можуть включати створення паралельних методів для проектування структури ЦОД.

КЛЮЧОВІ СЛОВА: кібербезпека, CRM, ERP, великі дані, дизайн бази даних, специфікація даних, методи структурування даних.

ABSTRACT

Context. Data centers are fundamental facilities that support high-performance computing and large-scale data processing. To guarantee that a data center can provide excellent properties of expanding and routing, the interconnection network of a data center should be designed elaborately.

Objective. The goal of the work is the analysis of methods for Data Structuring in Data Centers to build a secure and efficient Data Center system.

Method. This article is describing the main models of data structuring in data centers. The study is focused on the investigation of the main areas of Big Data technology application and determining the relationship between the level of efficiency of the cybersecurity system and the profitability of enterprises.

Results. The main methods analyzed in this work have been investigated for solving the problems of data storage and data processing in Data Centers.

Conclusions. The conducted research has adjusted the main problems when using Data Centers and confirmed the ways to solve some of them. This study helps to understand the most efficient ways for data structuring and the prospects for further research may include the creation of parallel methods for the structure design of Data Centers.

KEYWORDS: Cybersecurity, CRM, ERP, Big Data, Database Design, Data Specification, Data Structuring Methods.

ABBREVIATIONS

DC is a Data Center;
DS is a data structuring;
OS is an operating system.

INTRODUCTION

The world's data is growing faster than ever. Every two years, the amount of information is becoming double more [2]. The phenomenon of information explosion, i.e., a constant tremendous increase in the volume and speed of publication of information on a global scale, when the amount of information in the world grows more than 30% annually [1], confidentiality, integrity and availability of information and protection of data from cyberattacks is becoming more and more urgent task than ever. Therefore, the organization of data centers (DC) is a modern and effective tool focused on solving these problems.

Consequently, data consolidation is the main way to reduce or minimize the complexity of information processing by reducing the number of devices controlled directly by people, maximum formalization and automation of data processing, attracting combined hardware and software resources to implement large-scale standardized software tasks from various information sources.

The object of study is the process of structuring the data in DCs.

The subject of study is the sampling methods for DS to perform efficient and secure environment to store the vulnerable data.

The purpose of the work is to highlight the main problems of structuring the data in DCs and find the most efficient way to make secure DS design.

1 PROBLEM STATEMENT

The freedom to develop systems and programs within a distributed computing architecture has significantly accelerated the speed of development and implementation of software products, which has become a significant competitive advantage in today's business environment. At the same time, as new programs solve more and more critical tasks and require more and more computing resources, high-quality data processing and protection systems, the number of servers in DCs is growing, which complicates the management of software environment and databases.

2 REVIEW OF THE LITERATURE

The creation and dynamic development of DC in recent decades is associated in the work of leading scientists primarily with the need to ensure consolidation processes at various levels of information management, software and hardware components, engineering systems, as well as organizational procedures, IT resources and information security [3;4;5].

According to Webster College's dictionary, consolidation is the act of merging individual parts into one whole [6]. At the same time, the term "consolidation" can have several meanings. In a broad sense, consolidation can be understood as the process of searching, selecting, analyzing, structuring, transforming, storing, registering (cataloging) and providing the consumer with necessary information.

In the process of strengthening the consolidation of data, equipment, operations, software and other components within the DC, the unit costs of DC maintenance for specific consumers are reduced, which is primarily important for an increase in efficiency, involvement and development of the DC as a whole.

In the late 1990s, while acknowledging the importance and potential impact of IT consolidation, researchers and practitioners were focused on the problems of consolidating servers and applications. Mainly, they aimed creating new opportunities to run additional apps in a single instance of the operating system (OS). Nowadays, the amount of information is enormous on a global scale, as a result, the problem of data processing is constantly expanding, and consequently, almost all components in IT environments at this time are potential targets for consolidation, including server, computers, applications, storage systems, networks and processes.

In the early 1990s, there was a crisis in the mainframe market, due to the active transition of users from centralized to distributed information processing (using personal computers connected by a two-tier client-server architecture). Thus, with the creation and dissemination of the client-server architecture, companies have the opportunity to provide a stable high-speed Internet connection and continuous operation of equipment. At the same time, since the mid-1990s, interest in mainframes has resumed, due to the fact that, as practice has shown, centralized processing based on mainframes solves most of the problems of building enterprise-scale information systems more efficiently, faster and cheaper than distributed ones.

3 MATERIALS AND METHODS

The main methods used in the study were: bibliographic analysis of literary scientific sources, analysis and synthesis, grouping and systematization.

4 DISCUSSION

Tthe genesis of DC in the context of development and the complexity of consolidation processes characterizes the presence and constant updating of the use of DC as an important tool for data consolidation, technical and software solutions and IT-technologies.

At the same time, the activities of modern DCs are associated with the need for continuous improvement due to the rapid growth of information that needs to be stored and remain confidential. This requires constant improvement of software and hardware solutions for information processing and protection.

The DC is a queuing system, as it is a set of hardware, software and information resources and many requests that come at random times and compete for the right to access these resources. All resources are limited and the number of requests is a random variable, so, on the one hand, there may be blockages, queues and losses or delays in requests, including important and urgent, and on the other hand, there may be unused resources from time to time [9].

The process of functioning of the DC is that under the influence of external requests in the process of processing the information stored in databases is corrected, resources are interrogated, activated or released. According to the task, the necessary resources are provided or not provided to users.

The components of the DC infrastructure are divided into two main parts [8;10]:

1) the management subsystem, which is a set of means of delivery, processing and storage of information designed to monitor, control and coordinate the operation of facilities, which provide information services to users;

2) the executive subsystem, which contains the resources used by the management subsystem to provide services.

The basis of the DC is the engineering infrastructure that ensures the continuous operation of both management and executive subsystems, physical data security and the technological foundation for the construction of IT infrastructure. Complex engineering infrastructure of DC is a large room or even a separate building, which contains the necessary equipment for remote access to computing resources: uninterruptible power supply, ventilation, fire extinguishing, etc.

One of the most important problems in the functioning of the DC infrastructure is to ensure its reliability and efficiency under the influence of cyberattacks. This is a task of both technical and technological terms. As a result, creation of information security systems often lags behind the development of technologies for transmission and processing of information. It is a consequence, a response

to potential threats, rather than a systematic process of constantly preventing cyberattacks, even at the stage of designing and planning the construction of systems.

Characterizing the basic concepts related to the issue of cybersecurity of data centers, it is necessary to define some concepts: system disability - a state when the system does not perform its functions; does not operate according to the specified protocol; system error – is a part of the state of the system, as a result of which an accident may occur (e.g. error of broadcast data); vulnerability - the cause of the error, control of vulnerabilities is carried out by preventing, removing and waiting; system failure - visible inability to perform the function of the system, which is a consequence of an error due to the presence of vulnerabilities [11;12].

A cyberattack is an attack on a DC security system carried out for profitable purposes using external or internal vulnerabilities, hardware and software, and data networks.

As we can see, the protection of cyberspace is currently one of the main strategic objectives in the field of DC security. Offensive action in cyberspace has become an effective weapon in the hands of cybercriminals, used for a purpose determined by political and financial interests or ideology. Only proactive action and significant financial costs for cybersecurity will allow to respond effectively to a cyberattack. Thus, the ability to control and anticipate potential threats and attacks is very important, because on the one hand, changes in technology make work easier and faster, and on the other hand, they cause additional risks and create opportunities for cyberattacks.

The proliferation of instant e-mail, messaging, and voice over IP [13], as well as the huge growth of data on the World Wide Web [14], established the role of the Internet as a main area for communication and dissemination in the late twentieth century. Undoubtedly, the activities of online stores and online shopping platforms, platforms for streaming music and video and online entertainment became significantly popular. In the last decade, social networks have become especially important in public life, which in some way have changed the way people communicate with friends and relatives. Another strong trend has spread to entire industries due to the rapid proliferation of smartphones and mobile computing devices. These new services and technical capabilities require a combination of large-scale computing, huge storage volumes, and a high-speed, high-bandwidth communications network.

Currently, many scientists and experts in economics, marketing, IT-technologies are talking about the exacerbation of the problem of Big data. Every now and then huge amounts of content are generated by such sources as social networks, information sites, file sharers - and this is only a small part of the providers. Digital technologies are present in all spheres of human life, the amount of data recorded in the world's repositories is growing every moment [15].

Big data technology can be divided into three main areas:

- storage and translation of information received in gigabytes, terabytes and zettabytes for their processing and practical application;
- structuring disparate content: texts, photos, videos, audio and all other types of data;
- analysis of Big data and the introduction of various methods of processing unstructured information, its structuring, the creation of various analytical reports.

The purpose of this technology is the maximum efficiency, introduction of new products and growth of competitiveness [16, 17]. Thanks to the introduction of data structuring technology using Big Data technology, it is possible to receive necessary information in time and in a good quality [16].

With increasing size and speed of network and distributed system, the amount of output data increases significantly. As a result, it is often difficult to find the information users need quickly and fully. Data collection, processing and selection in such systems is a problem that remains common to many DCs, which vary greatly not only in scale but in perception modality, depending on what type of data is collected and what model of processing these information is applied. Some sensor networks, for example, control only simple physical phenomena, such as temperature and humidity. In other networks, data sources may be different, require more speed, and have a complex structure that produce for the purchase some additional information.

For the purposes of data structuring in modern practices that widely use intellectual data analysis, based on Data Mining or Knowledge Discovery in Databases. These systems implement a general methods of classification, prediction and modeling, generally using the methods of artificial intelligence: neural measurements, fuzzy logic and more. Such methods are intended for use in large databases and encourage the rejection of the use of hidden patterns in them.

Strengthening of consolidation processes stipulate the further development of modern data centers, the possibility of using their infrastructure and software, features of data protection due to the fact that confidential data, reduced information stored in business applications, or through joining to the introduction of malicious code in the systems of enterprises that are in the company of 400 billion people who arrived in the United States. For example, 97% of the corporate Fortune 500 has suffered from IT security breaches at least once. The global average loss for medium-sized companies (from 100 million to 1 billion of annual income) reaches $3 million. For large companies (more than $1 billion), losses have already exceeded $10 million [20].

The amount of damage, as well as the scale of the risk associated with a possible cybersecurity breach, suggests that this problem has long ceased to be a problem that only affects IT departments and is discussed at operational meetings of companies. Statistics show that 70% of executives at the highest level make decisions related to IT security, realizing that they cannot avoid responsibility for the security of their company.

According to statistics, every business will suffer from a cyberattack or malfunction caused by a cybersecurity breach eventually. Full data center protection is not possible. The idea of an effective cybersecurity system is to be prepared for an attack when it is carried out and to be able to minimize the losses caused by the incident. This can be achieved primarily through the preparation and implementation of action plans in the event of cyber threats. Actions of this kind can be implemented by the internal security department of the data center, or by specialized providers.

Due to the great diversity in scale and modality in data centers, there is no common set of components and protocols that can serve as a model for all DCs, in particular with regard to data protection and cybersecurity systems. However, some characteristics that are common to most data processing systems may form the basis of the data-structuring model within the data center, which is the basic model of data array processing and the formation of a user-adapted model of DC-user interaction. Therefore, the problem of fast and correct structuring of large amounts of information, ensuring the confidentiality and security of information in modern data centers, comes to the fore.

CONCLUSIONS

Therefore, implementing the latest technological structures and data protection in DCs, functions, OLAP-systems and cloud solutions, solutions based on artificial neural measurements (models initiated by the principle of organization and functioning of biological neural measurements), methods of preliminary analysis, statistics and Natural Language Processing (areas of artificial intelligence and mathematical linguistics that study the problems of computer analysis and synthesis of natural languages) and others, can solve the main problem of big data, which still remains relevant - the response to processing speed, structuring, speed data analysis and confidentiality. it is obtained and increasing its volume.

The conducted research has adjusted the main problems when using Data Centers and confirmed the ways to solve some of them. This study helps to understand the most efficient ways for data structuring and the prospects for further research may include the creation of parallel methods for the structure design of Data Centers.

REFERENCES

1. T. Sommestad, “A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour”, T. Sommestad, H. Karlzén, J. Hallberg, International Journal of Information Security and Privacy. – 2015. – Vol. 9, Issue 1. – P. 26– 46. DOI: 10.4018/ijisp.2015010102.
2. Creating trust in the digital world EY’s Global Information Security Survey 2015 [Electronic resource]. Available at: http:// www.ey.com/Publication/vwLUAssets/ey-global-information- security-survey-2015/$FILE/ey-global-information-security- survey-2015.pdf
3. Oleynik M. A., Pevtsov G.V., Fastovsky E.G, "Analysis of methods of information consolidation and features of its application", Bulletin of the National Technical University Kharkiv Polytechnic Institute. Series: Informatics and modeling. № 39/2007, pp.145.
4. Zimmermann O., “Elements of service-oriented analysis and design. Interdisciplinary approach to modeling in SOA construction projects” [Electronic resource]. Available at: http://www.ibm.com/developerworks/ webservices/library/ws- soad1/
5. Shashi Kiran, “About the new perspectives of data center infrastructure”. [Electronic resource]. Available at: http://www.iksmedia.ru/blogs/post/5004485-O-novyx- perspektivax-infrastruktury.htm
6. Merriam-Webster Dictionary [Electronic resource]. Available at: https://www.merriam-webster.com/dictionary
7. Dovgy S. A., “New technologies in telecommunications: the choice of technological architecture. Modern development trends”, S. A. Dovgiy, O. V. Kopeyka, S. P. Polenok. - K.: Ukrtelecom, 2001. – pp. 281. 2021 IEEE International Conference on Problems of Infocommunications. Science and Technology PIC S&T'2021
8. Kopiyka, O.V., “Design of IT infrastructure management services in modern data centers”, O.V. Kopiyka, Communication, № 5(105), pp.23-31, 2013.
9. Yaremko, I.M., “Models of queuing in the data center”, I.M. Yaremko, B.B. Turupalov, Information and control systems for railway transport, №6, pp. 23-26, 2011.
10. Turupalov, V.V., "Analysis of the principles of building a model of the data center of the telecommunications network.", "Machinery in agricultural production, industrial engineering, automation", №25, vol.2, 2012.
11. Tsimbal, A.A., “Technologies for creating distributed systems. For professionals”, A.A. Tsimbal, M.L. Anshina, Peter, pp.576, 2003.
12. Pleskach, V.A., “Information technologies and systems”, V.A. Pleskach, Yu.V. Rogushina, N.P. Kustova; Kyiv National University trade and economy, Book, pp.519, 2004.
13. Varshney U., Snow A., McGivern M., and C. Howard, “Voice over IP”. Commun. ACM, 45(1):89–96, Jan. 2002.
14. World Wide Web Consortium (W3C). [Electronic resource]. Available at: http://www.w3.org/
15. What is Big data in marketing: problems, algorithms, methods of analysis. [Electronic resource]. Available at: http://lpgenerator.ru
16. Shevchenko M.V., Kos'yanova E.A., “Big Data: Problem, management and economics of enterprises”, Belgorod, pp.31-35,2016.
17. Bryantseva T.A., Shevchenko M.V., “Organization of the system of internal control of innovation activity”, Bulletin of the Belgorod State Technological University of V.G. Shukhov, № 7, pp. 175–181, 2016.

18. Cisco Visual Networking Index: Forecast and Methodology, 2011–2016. [Electronic resource]. Available at: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf.
19. Cisco Global Cloud Index: Forecast and Methodology, 2011–2016. [Electronic resource]. Available at: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.pdf.
20. PricewaterhouseCoopers, 2020. [Electronic resource]. Available at: https://www.pwc.com

NATIONAL CYBER SECURITY SYSTEM: ANALYSIS OF CURRENT CHALLENGES IN THE FIELD OF NATIONAL SECURITY AND STATE DEFENSE

Shypovskyi V. V. – Adjunct of the Department of Information Technology and Information Security the National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine.

АНОТАЦІЯ

Сучасні виклики у кіберпросторі змусили визнати кібербезпеку одним із пріоритетів у системі національної безпеки України. Кіберпростір, поряд з іншими фізичними просторами, вже визнаний одним із можливих театрів воєнних дій. Для забезпечення обороноздатності держави у кіберпросторі виникає потреба у створенні кібервійськ, у завдання яких входитимуть не лише захист критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних дій у кіберпросторі, у тому числі зняття з експлуатації критичної інфраструктури противника шляхом знищення. інформаційні системи, які керують такими об'єктами.

КЛЮЧОВІ СЛОВА: кібербезпека, кіберзагроза, кібератака, Національна система кібербезпеки.

ABSTRACT

Current challenges in cyberspace have forced the recognition of cyber security as one of the priorities in the national security system of Ukraine. Cyberspace, along with other physical spaces, has already been recognized as one of the possible theaters of war. To ensure the state's defense capabilities in cyberspace, there is a need to create cyber troops, whose tasks will include not only protecting critical information infrastructure from cyber attacks, but also conducting preventive offensive operations in cyberspace, including the decommissioning of critical enemy infrastructure by destroying information systems that manage such facilities.

KEYWORDS: cyber security, cyber threat, cyber attack, National Cybersecurity System.

The Russian Federation remains one of the main sources of threats to national and international cybersecurity, actively implementing the concept of information confrontation, based on a combination of destructive actions in cyberspace, the mechanisms of which are actively used in the hybrid war against Ukraine. The number of states that are trying to form their own cyber intelligence, master modern technologies of intelligence and subversive activities in cyberspace, and strengthen state control over national segments of the Internet is actively increasing. At the same time, the number of information technologies is growing, which involves the accumulation of large amounts of information on human behavior, social groups and the use of modern advances in artificial intelligence [1].

In the modern information space, the technical level of implementation of cyber threats is growing, new tools and mechanisms of cyber attacks are constantly being improved and developed. The tendency to use cyber attacks as a tool for special information operations by Special Forces is growing. Timely response to challenges in cyberspace is provided by the National Cyber Security System, which is a set of cybersecurity actors and interrelated measures of political, scientific, technical, informational, educational, organizational, legal, operational and investigative, intelligence, counterintelligence, defense, engineering -technical measures, as well as measures of cryptographic and technical protection of national information resources, cyber protection of critical information infrastructure. The main subjects of the National Cybersecurity System are the State Service for Special Communications and Information Protection of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine, intelligence agencies, the National Bank of Ukraine [2]. The following is necessary for the further development of the national cybersecurity system:

strengthening the capacity of the national cybersecurity system to prevent armed aggression against Ukraine in cyberspace or with its use, neutralization of intelligence and subversive activities, minimization of threats of cybercrime and cyber terrorism;

gaining the ability to quickly adapt to internal and external threats in cyberspace, to maintain and restore the sustainable functioning of the national information infrastructure, especially critical information infrastructure (cyber resilience);

ensuring the development of communication, coordination and partnership between cybersecurity actors at the national level, development of strategic cybersecurity relations with key foreign partners, primarily with the European Union, the United States and other NATO member states, cooperation in this field with

other countries and international organizations based on the national interests of Ukraine (interaction) [1].

According to the new Strategy, the main threats to Ukraine's cybersecurity are:

hybrid aggression of the Russian Federation against Ukraine in cyberspace. The aggressor state is constantly increasing the arsenal of cyber weapons for offensive purposes, the use of which can cause irreparable, irreversible destructive consequences. Cyberattacks of the Russian Federation are aimed primarily at information and communication systems of state bodies of Ukraine and critical information infrastructure in order to disable them (cyber diversion), gain covert access and control, intelligence and intelligence activities. Cyber attacks are also actively used by the aggressor state as an element of special information operations aimed at manipulating the population, interfering in electoral processes and discrediting Ukrainian statehood;

cybercrime, which harms information resources, social processes, personally citizens, reduces public confidence in information technology and leads to significant material losses. The use of cyberspace to commit crimes against the foundations of national security of Ukraine, as well as criminal offenses related to money laundering, trafficking in human beings, illicit handling of weapons, ammunition or explosives, illicit trafficking in narcotic drugs, psychotropic substances is becoming widespread., their analogues or precursors and other objects and substances that threaten human life and health, etc. [1];

organized and sponsored by governments of other states cyber attacks related to the theft for political, economic or military purposes of sensitive information (cyber espionage) and the implementation of intelligence and subversive activities. Features of such cyber attacks are their duration, complexity and hidden nature, which complicates their prevention, detection and neutralization;

using of cyberspace by terrorist organizations to commit acts of cyber terrorism, financial and other support for terrorist activities [1].

Thus, the spread of cyber threats to all spheres of life and improving the tools for their implementation necessitates a change in strategy and tactics to combat them. It is important to quickly identify vulnerabilities and cyberattacks, respond and disseminate information about them to minimize possible damage. Every day, Ukraine acquires the capabilities of effective cyber defense and improves the level of cyber resilience of the state.

REFERENCES

1. Стратегія кібербезпеки України / URL: https://www.president.gov.ua/documents/4472021-40013 28/12/2021
2. Закон України “Про основні засади забезпечення кібербезпеки України” /URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text1 30/12/2021

ANALYSIS OF TECHNOLOGIES FOR ORGANIZING THE PROTECTION OF CORPORATE INFORMATION SYSTEM

Delembovskyi M. M. – Ph.D., Associate Professor of the Department of Cybersecurity and Computer Engineering, Kyiv National University of Construction and Architecture, Ukraine.

Terentiev O. O. – Doctor of Technical Sciences, Professor, Head of the Department of Information Technologies of Design and Applied Mathematics, Kyiv National University of Construction and Architecture, Ukraine.

Hamera L. – MSc, Department of Computer Science and Automatics, University of Bielsko-Biala, Bielsko-Biala, Poland.

АНОТАЦІЯ

З метою забезпечення ефективної роботи та організації повного захисту інформаційних активів, систем і засобів існує нагальна потреба у структуруванні різних підходів до вирішення цієї проблеми. Основною ідеєю роботи є аналіз на основі визначення та оптимального вибору складних систем захисту корпоративної мережі в умовах сучасних викликів і загроз.

КЛЮЧОВІ СЛОВА: кібербезпека, корпоративна мережа, автоматизована система, конфіденційність, надійність.

ANNOTATION

In order to ensure the effective operation and organization of full protection of information assets, systems and facilities, there is an urgent need to structure different approaches to solving this problem. The main idea of the work is the analysis based on the definition and optimal selection of complex systems of corporate network protection in the conditions of modern challenges and threats.

KEY WORDS: cybersecurity, corporate network, automated system, privacy, reliability.

INTRODUCTION

In the conditions of rapid development of the information environment there is an urgent need to organize the protection of large amounts of conference and private information. Private and confidential information today essentially forms an information asset that has a huge impact on the functioning of the organization. Corporate network security in Ukraine requires the use of

new reliable and modern solutions and an equally important component is the availability of highly qualified specialists.

Due to the latest developments in the world of information environment, various software packages are constantly being developed and implemented, which can receive information about the state of the network and report critical changes.

The problem of protection facing modern business is the task of considering the full range of existing solutions and choosing the right combination. Today, many technologies and means of protection are offered. The difficulty in implementing network security is not the lack of appropriate security technology, but the choice of many solutions that are best suited to your particular network and the requirements of your business, and where the cost of supporting and maintaining the security offered by the provider is minimal.

The aim of the study is to find and optimal choice of solutions for the protection of a small corporate network.

Along with the continuous development of information systems, new ways of unauthorized intrusion are emerging. Existing traditional security mechanisms implemented in firewalls, authentication servers, access control systems, etc. are essentially anti-attack tools. Building a secure network requires tools that not only detect and block attacks, but also prevent them. Based on the requirements for a secure computer system, this paper will consider the existing methods of protection of the COP and propose a new approach to protection - adaptive protection.

1 ANALYSIS OF LITERARY DATA AND STATEMENT OF THE PROBLEM

An analysis of modern publications on this topic indicates a fairly large number of publications [1-6] and a huge number of organizations that organize and ensure the protection of computer systems. In order to ensure reliable protection of the corporate information network, it is necessary to provide a fully functional systematic integrated approach [7-8]. The use of an integrated approach makes it possible to achieve the availability, integrity and confidentiality of information assets. This approach involves the implementation of protection at the legislative level, administrative and software and hardware levels.

2 TECHNOLOGIES TO PROTECT THE CORPORATE SYSTEM

When creating an information infrastructure of an automated system (AS) based on modern computer networks, a number of issues arise in organizing the protection of this infrastructure from threats that threaten the security of information. In accordance with this, a number of questions are formulated, namely:

- to what extent the security mechanisms, correctly implemented in the AU, are adapted to the existing risks;
- can this system be trusted to process, store and transfer confidential information;
- are there any errors in the current configuration that allow potential intruders to bypass access control mechanisms;
- does the software installed in the AS contain vulnerabilities that can be used by attackers to bypass the access control mechanism;
- how to assess the level of safety of the AU and how to determine whether it is sufficient in a given environment;
- what countermeasures will actually increase the safety level of the AU?
- what safety assessment criteria should be observed and what safety indicators should be used?

These questions sooner or later are asked by all specialists of IT departments, information security departments and other departments responsible for the functioning and maintenance of the AS [1-5]. The answers to these questions are far from obvious. Analysis of AS security from information security threats is not a simple task [1]. The ability to assess and manage risks, knowledge of typical threats and vulnerabilities, criteria and approaches to security analysis, knowledge of analysis methods and special tools, knowledge of various software and hardware platforms used in the latest computer networks - this is not a complete list of professional qualities that must be possessed specialists working on NPP safety analysis. Safety analysis is the main component of such types of work as certification, audit and safety inspection of nuclear power plants.

Along with such reliability indicators as fault tolerance (non-failure operation), performance, etc., security is one of the most important indicators of the efficiency of the AS. AS protection is the degree of timely response of the implemented mechanisms in it to threats that threaten information security. Information security threats are usually understood as the possibility of violation of information properties (SIA triad), such as confidentiality, availability and integrity.

In practice, it is difficult to obtain the exact values of these characteristics, since the concept of threat is difficult to formulate. For example, the assessment of damage caused by unauthorized access to political and military information cannot be accurately determined at all, and the determination of the probability of a threat cannot be based on statistical analysis. The assessment of the degree of reliability of protective mechanisms is always subjective.

Currently, there are no standardized methods for analyzing the safety of AS. Therefore, the algorithms of actions in certain situations can differ significantly. However, it is possible to offer a typical method for analyzing the security of a corporate network [3]. And although this technique does not claim to be universal, its effectiveness has been repeatedly tested in practice.

Thus, taking into account the above, the technique involves the use of the following methods of analysis [5], namely:

study of the initial data of the AU;

assess the risks associated with the implementation of threats to the security of NPP resources;

analysis of security mechanisms at the organizational level, the organization's security policy and organizational and administrative documentation in order to ensure the information protection regime and assess whether they meet the requirements of current regulations and whether they are resistant to existing risks;

manual analysis of configuration files of routers, MEs and proxy servers that control internetworking of mail and DNS servers and other important elements of the network infrastructure;

scanning external network addresses of the local network from the Internet;

scanning internal resources of the local network; configuration analysis of local network servers and workstations using special software.

These research methods include both active and passive testing of the protection system. The active test of the protection system includes imitation of the actions of a potential attacker to overcome the defense mechanisms. In passive testing, the configuration of the operating system and applications are analyzed by patterns using checklists [6]. Testing can be done manually or using special software.

3 CONCLUSIONS

Therefore, in practice, there are still a large number of ways that are not subject to an accurate assessment of the possible means of implementing security threats to NPP resources. Ideally, each threat path to AS resources should be blocked by an appropriate protection mechanism. This condition is the first factor determining the safety of the AS. The second factor is the strength of existing defense mechanisms, which is characterized by the degree of resistance of these mechanisms to their attempts to circumvent or overcome. The third factor is the amount of damage that will be caused to the owner of the AS if the threat successfully overcomes the path to the system resources.

REFERENCES

1. Делембовський, М., Терентьєв, О., & Шабала, Є. (2020). Технологія впровадження середовища Matlab в досліджені моделі загроз інформаційної безпеки. ΛΌГОΣ. ОНЛАЙН. https://doi.org/10.36074/2663-4139.15.08
2. Скопа, О. О., & Казакова, Н. Ф. (2009). Аналіз розвитку сучасних напрямів інформаційної безпеки автоматизованих систем. Системи обробки інформації, (7), 48-53.
3. Гужва, В. М. (2001). Інформаційні системи і технології на підприємствах. К.: КНЕУ.
4. Павленко, П. М., Філоненко, С. Ф., Бабіч, К. С., Гавриленко, О. В., & Логачов, Є. Г. (2013). Інформаційні системи і технології.
5. Гавловський, В. (2000). Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект).
6. Корнієнко, С. К., & Корниенко, С. К. (2015). Проектування інформаційного забезпечення автоматизованих систем.
7. Коробейнікова Т. І. Комплексна система моніторингу корпоративної мережі / Коробейнікова Т. І., Каневський М. В. Зимові наукові підсумки 2018: XII Міжн. наук.-практич. конференція: тези доповідей, Дніпро, 25 грудня 2018 р. –Ч. 1. –Дніпро: НБК, 2018, с. 79-84.
8. Коробейнікова Т. І. Комплексний метод організації IP-телефонії в структурі захищеної корпоративної мережі підприємства / Коробейнікова Т. І., Ткачук В. Ю. Зимові наукові підсумки 2018: XII Міжнародна наук.-практич. конференція: тези доповідей, Дніпро, 25 грудня 2018 р. –Ч. 1. –Дніпро: НБК, 2018, с. 105-111.
9. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. –К.: КУБГ, 2019. –218 с

MATHEMATICAL MODEL OF THE SYSTEM FOR PROVIDING SPTA COMPLEX TECHNICAL OBJECTS

Zhyrov G. – PhD, Associate professor of department of the Radio Engineering and Radioelectronic Systems, Taras Shevchenko National University of Kyiv.

Lenkov E.S. – candidate of Technical Sciences, senior researcher at the Scientific Center of Military Institute of Telecommunications and Informatization.

АНОТАЦІЯ

Система забезпечення запасними елементами, інструментом та приладами (ЗІП) входить в загальну структуру системи технічного обслуговування і ремонту. Для її якісної роботи необхідний математичні та програмні інструменти для визначення оптимальних параметрів цих систем. В роботі запропонована математична модель системи забезпечення ЗІП, яка використовується для розрахунку оптимальних параметрів цієї системи та входить в загальну імітаційну статистичну модель.

КЛЮЧОВІ СЛОВА: Система забезпечення ЗІП, імітаційна статистична модель.

ABSTRACT

Spare parts, tools and accessories (SPTA) system is part of the overall structure of the maintenance and repair system. For its quality work requires mathematical and software tools to determine the optimal parameters of these systems. The paper proposes a mathematical model of the support system SPTA, which is used to calculate the optimal parameters of this system and is included in the general simulation statistical model.

KEYWORDS: Supply systems SPTA, simulation statistical model.

For quality maintenance and repair of complex radio-electronic equipment, it is necessary to create and maintain at the necessary level the system of providing SPTA. The concept of SPTA refers to many spare elements, parts, component modules, etc., which are designed to restore the operability of objects, in case of their failure.

There are different types of SPTA, which territorially can be located at a considerable distance from each other. In this paper, only three varieties of SPTA sets are considered: SPTA -0 - the set of the object itself, which is used for current repairs and contains the least reliable elements. SPTA -1 - the set assigned to a group of objects is designed to store elements that may be missing in SPTA -0. SPTA -2 will be considered a non-exhaustible source of supply (NSP), which is used for periodic replenishment of SPTA -0 and SPTA -1.

Thus, the SPTA supply system can be described by the following generalized parameter:

$$P_{\text{зип}} = \begin{Bmatrix} \vec{X}_{\text{SPTA}k}, T_{\text{SPTA}k}, \tau_{d\text{SPTA}k}, \\ C_{d\text{SPTA}k}; k = \overline{0,2} \end{Bmatrix}, \quad (1)$$

where: $\vec{X}_{\text{SPTA}k} = \{x_i\}$- a vector defining the composition of the k-th level of SPTA, in which x_i - the number of elements of the i-th type available in this SPTA $(k = 0,1)$;$T_{\text{SPTA}k}$ - the periodicity of replenishment of the k-th level of SPTA; $\tau_{\text{SPTA}k}$- the average time of delivery of elements from the k-th level of SPTA $(k = 0,1,2)$;$C_{d\text{SPTA}k}$- the cost of delivery of elements from the k-th level of SPTA.

To describe the object of technology itself, we can use such a generalized parameter [1,2]:

$$P_{\text{ob}} = \left\{ E_{\text{o}}, \left\{ \begin{matrix} T_{M\text{TTF}i}, \nu_i, \tau_{\text{MTFF}i}, \\ \tau_{M\text{TRE}i}, C_{0i}, C_{\text{ORi}}; i = \overline{1, |E_{\text{o}}|} \end{matrix} \right\} \right\}, \quad (2)$$

where: E_{o} - is the set of failing elements of the object; $T_{M\text{TTF}i}$ and ν_i- indicators of reliability of the i-th element (mean time to failure and coefficient of variation of time to failure); $\tau_{\text{MTFF}i}$ and $\tau_{M\text{TRE}i}$ - indicators of maintainability of the i-th element (mean time to find a fault and mean time to replace an element); C_{0i} and C_{ORi} - the cost of the element and the cost of the operation to replace it.

The following indicators can be used as criteria for the quality of technical operation of equipment objects:

T_0 - mean time between failures of an object;

T_{NO} - average non-operational time;

c_{e} - unit cost of operating the object.

However, the value of the generalized parameter P_{SPTA}affects only T_{NO} and c_{e}, so only they will be taken as criteria.

Based on this assumption, the formalized task of optimizing the parameters of the SPTA support system can be represented by the following expression [1,3-5]:

$$\begin{gathered} \mathrm{T_{NO}}(\mathrm{P_{ob}}, \mathrm{P^*_{SPTA}}) \le \mathrm{T^{re}_{NO}}; \\ \mathrm{c_e}(\mathrm{P_{ob}}, \mathrm{P^*_{SPTA}}) = \min_{\mathrm{P_{SPTA}}} \mathrm{c_e}(\mathrm{P_{ob}}, \mathrm{P_{SPTA}}), \end{gathered} \quad (3)$$

where: $T^{\text{re}}_{\text{NO}}$ - the required value of the allowable idle time; P_{SPTA} - the sought-after optimal values of the parameters of the supply system SPTA.

To solve the optimization problem, we need a mathematical model of the supply system SPTA. Thus, it is necessary to derive mathematical dependences of criterion values T_{NO} and c_e from parameters of the support system (1) and object parameters (2).

The average non-operational time T_{NO}can be represented by two components:

$$T_{\text{NO}}(P_{\text{ob}}, P_{\text{SPTA}}) = T_{\text{MTTR}}(P_{\text{ob}}) + T_{w\text{SPTA}}(P_{\text{ob}}, P_{\text{SPTA}}), \quad (4)$$

where:$T_{\text{MTTR}}(P_{\text{ob}})$ - mean reversion time of the object; $T_{w\text{SPTA}}(P_{\text{ob}}, P_{\text{SPTA}})$ - mean time of waiting for delivery of a serviceable element from SPTA.

In turn: $T_{\text{MTTR}}(P_{\text{ob}}) = \sum_{\forall i \in E_{\text{o}}}(\tau_{\text{MTFF}i} + \tau_{\text{MTRE}i})\bar{\omega}_i / \sum_{\forall i \in E_{\text{o}}} \bar{\omega}_i$, where: $\bar{\omega}_i$ - is the mean value of the failure flow parameter of the i-th element.

The value of $T_{w\text{SPTA}}(P_{\text{ob}}, P_{\text{SPTA}})$ is determined by the expression: $T_{w\text{SPTA}}(P_{\text{ob}}, P_{\text{SPTA}}) = K_{\text{SPTA0}}\tau_{\text{SPTA0}} + (1 - K_{\text{SPTA0}})[K_{\text{SPTA1}}\tau_{\text{SPTA1}} + (1 - K_{\text{SPTA1}})\tau_{\text{SPTA2}}]$, where: $K_{\text{SPTA}k}$ - availability rate SPTA.

The availability rate SPTA can be obtained by averaging the value of the probability of SPTA sufficiency, but it is much easier to determine it implicitly, using a statistical simulation.

Substituting these formulas into (4), we determine the average idle time in the inoperative state:

$$\begin{gathered} T_{\text{NO}}(P_{\text{ob}}, P_{\text{SPTA}}) = \\ \frac{\sum_{\forall i \in E_{\text{o}}}(\tau_{\text{MTFFi}} + \tau_{\text{MTREi}})\bar{\omega}_i}{\sum_{\forall i \in E_{\text{o}}} \bar{\omega}_i} + \\ + K_{\text{SPTA0}}\tau_{\text{SPTA0}} \\ + (1 - K_{\text{SPTA0}}) \\ \left[\begin{matrix} K_{\text{SPTA1}}\tau_{\text{SPTA1}} + \\ (1 - K_{\text{SPTA1}})\tau_{\text{SPTA2}} \end{matrix} \right], \end{gathered} \quad (5)$$

The unit cost of operating the object c_e, can also be represented by two components [1,2]:

$$c_e(P_{\text{ob}}, P_{\text{SPTA}}) = c_{\text{cr}}(P_{\text{ob}}) + \text{c}_{\text{SPTA}}(P_{\text{ob}}, P_{\text{SPTA}}), \quad (6)$$

where: $c_{\text{cr}}(P_{\text{ob}})$ - the costs of current repairs of the facility; $\text{c}_{\text{SPTA}}(P_{\text{ob}}, P_{\text{SPTA}})$ - costs of the collateral system SPTA.

The value $c_{\text{cr}}(P_{\text{ob}})$ can be calculated as follows: $c_{\text{cr}}(P_{\text{ob}}) = \left(\sum_{\forall i \in E_{\text{o}}}(C_{0i} + C_{\text{ORi}})\bar{n}_{fi}\right)/T_e$, where: - $\bar{n}_{fi}$ - the average number of faults of the i-th element during the considered period of operation T_e.

The value of $\text{c}_{\text{SPTA}}(P_{\text{ob}}, P_{\text{SPTA}})$is determined by the expression: $\text{c}_{\text{SPTA}}(P_{\text{ob}}, P_{\text{SPTA}}) = c_{t\text{SPTA}}(P_{\text{ob}}, P_{\text{SPTA}}) + c_{r\text{SPTA}}(P_{\text{ob}}, P_{\text{SPTA}})$, where: $c_{t\text{SPTA}}(P_{\text{ob}}, P_{\text{SPTA}})$ - unit cost of transporting spare parts from SPTA; $c_{r\text{SPTA}}(P_{\text{ob}}, P_{\text{SPTA}})$ - specific costs for replenishment kits SPTA.

In turn:

$$c_{t\text{SPTA}}(P_{\text{ob}}, P_{\text{SPTA}}) = \frac{\bar{n}_{f\Sigma}\left[K_{\text{SPTA0}}\text{C}_{s\text{SPTA0}} + (1 - K_{\text{SPTA0}})\left(\begin{matrix}K_{\text{SPTA1}}\text{C}_{t\text{SPTA1}} + \\ (1 - K_{\text{SPTA1}})\end{matrix}\right)\text{C}_{t\text{SPTA2}}\right]}{T_e},$$

where: $\bar{n}_{f\Sigma}$ - the average total number of object failures over time T_e, $\text{C}_{t\text{SPTA}k}$ - the cost per transport of SPTA of the k-th level ($k = 0,1,2$).

The second component is defined by the expression:

$$c_{r\text{SPTA}}(P_{\text{ob}}, P_{\text{SPTA}}) = \frac{1}{T_e}\sum_{k=0}^{k=1}\left[\begin{matrix}n_{r\text{SPTA}k} \\ \sum_{\forall i \in E_{\text{o}}} x_i C_{0i} - \\ \sum_{\forall i \in E_{\text{o}}}[x_i - a_i(T_{\text{SPTA}k})]C_{0i} + C_{\text{ov}}\end{matrix}\right],$$

where: $n_{r\text{SPTA}k}$ - the number of replenishments SPTA of the k-th species over time T_e; $a_i(T_{\text{SPTA}k})$ - average flow rate of elements of the i-th type in the replenishment interval $T_{\text{SPTA}k}$; C_{ov} - overhead cost.

Substituting these components in (6), we obtain that the unit operating cost of the object is determined by the expression:

$$c_e(P_{\text{ob}}, P_{\text{SPTA}}) = \frac{\sum_{\forall i \in E_{\text{o}}}(C_{0i} + C_{\text{ORi}})\bar{n}_{fi}}{T_e} + \frac{\bar{n}_{f\Sigma}\left[\begin{matrix}K_{\text{SPTA0}}\text{C}_{s\text{SPTA0}} + \\ (1 - K_{\text{SPTA0}})\end{matrix}\left(\begin{matrix}K_{\text{SPTA1}}\text{C}_{t\text{SPTA1}} + \\ (1 - K_{\text{SPTA1}})\text{C}_{t\text{SPTA2}}\end{matrix}\right)\right]}{T_e} + \frac{\sum_{k=0}^{k=1}\left[\begin{matrix}n_{r\ \text{SPTAk}} \\ \sum_{\forall i \in E_{\text{o}}} x_i C_{0i} \\ -\sum_{\forall i \in E_{\text{o}}}[x_i - a_i(T_{\text{SPTAk}})]C_{0i} + C_{\text{ov}}\end{matrix}\right]}{T_e}. \quad (7)$$

Expressions (5) and (7), are a mathematical model of the system of providing spare parts and spare parts for complex technical objects.

The developed mathematical model is used in the simulation statistical model of determining the optimal parameters of the maintenance and repair system in terms of quality provision of spare parts and spare parts both of the objects themselves and of the repair bodies.

REFERENCES

1. Forecasting reliability of complex technology objects. Parameters optimization of their technical exploitation: [monograph] in English / Sergey Lenkov, Igor Tolok, Vadim Tsitsarev, Genadiy Zhyrov, Evgen Lenkov, Yurii Khlaponin, Bohdan Borowik; under edition S.V. Lenkov. – Poland, Bielsko-Biala: Publishing house «BEL », 2018. – 253 p.
2. Lenkov S., Zhyrov G., Zaitsev D., Tolok I., Lenkov E., Bondarenko T., Gunchenko Y., Zagrebnyuk V., Antonenko O. Features of modeling failures ofrecoverable complex technical objects with a hierarchical constructive structure. Eastern-European Journal of Enterprise Technologies, 2017, № 4/4 (88), pp.34–42.
3. Bandi B. Metody optimizatsii. Vvodnyi kurs : per s angl. M. : Radio i sviaz', 1988, 128 p.
4. Shup T. Reshenie inzhenernyh zadach na EVM: prakticheskoe rukovodstvo, M.: Mir, 1982, 238 p.
5. Duc-Hanh Dinh, Phuc Do, Benoit Iung. Maintenance optimisation for multi-component system with structural dependence: Application to machine tool sub-system", CIRP Annals, 2020, Article in pres. https://doi.org/10.1016/j.cirp.2020.04.004

MATLAB SIMULINK MODEL TESTING BASED ON ISO 26262-6

Humennyi D. – Ph.D., Associate Professor at Sikorsky Kyiv Polytechnic Institute, Project Manager at N-iX Ukraine.

Veselska O. – Msc, Department of Computer Science and Automatics University of Bielsko-Biala 2 Willowa St, Bielsko-Biala, 43-309 Poland.

INTRODUCTION

To minimize the probability of error in the program code, according to the ISO 26262 should use automatic code generation. Automatic code generation performs the tasks of interpreting the model into the program code and compiling the object file.

In the automotive and medical industries, the automatic generation of software code from models is recommendatory. The decision on implementation is made by the Product Over in the development organization of the product. This decision is based on the need to enter the market of certain regions or countries that may require a

certificate of compliance with a particular ISO. Often such requirements classify not only the requirements for the software product as a whole but also for the development technology.

The automotive industry is one such industry. A detailed description of the document available here ISO 26262 (ISO.org). A detailed description of the best practices for providing security functionality designed in the MISRA GMG (MISRA c / o HORIBA MIRA Ltd #) and other documents.

Using MATLAB Simulink as a tool for algorithm formation and C / C ++ code generation, give the possibility to minimize errors in the program code (comparable to the manual programming conception). The generated code does not require verification and can be loaded into the target hardware using third-party software. However, at the stage of developing the algorithm, mistakes can be made. Consequently, the identification of errors at the stage of the development of the algorithm blocks, the functioning of the algorithm, and the correspondence of the code with the algorithm is an important stage of development and should be carried out in parallel with the development of the algorithm.

For testing MATLAB Simulink models, there are applications such as Simulink Test, MES, and others. These applications are effective tools for performing typical test cases, in particular:

- Unit Test,
- Functional Test,
- Composition test

based on MIL, SIL, and HIL based on the type and completeness of test coverage.

The listed software products can be used to test software products with QM, ASIL A, B, C, and D marks according to ISO 26262 (ISO.org #). both Simulink Test and MES are available for a fee.

Since the standalone testing QM systems is possible. It means that QM can be tested without ASIL systems. It is important to note the possibility of conducting such testing with non-certified software, which can be provided free of charge.

AUTOMOTIVE TEST PROCESS

It is important to note that the development and testing of models, algorithms, and code in the automotive industry are characterized by a class of threat to life and health. Threat classification is assessed on the QM, ASIL [A, B, C, D] scale and is detailed in ISO 26262. It is also worth noting that testing non-ASIL subsystems (ISO26262-08, page 21) does not require the use of validated software. product (can be carried out using the custom toolset).
According to ISO 26262, a safe development concept for automotive must comply with the V Model as shown in Figure 1.

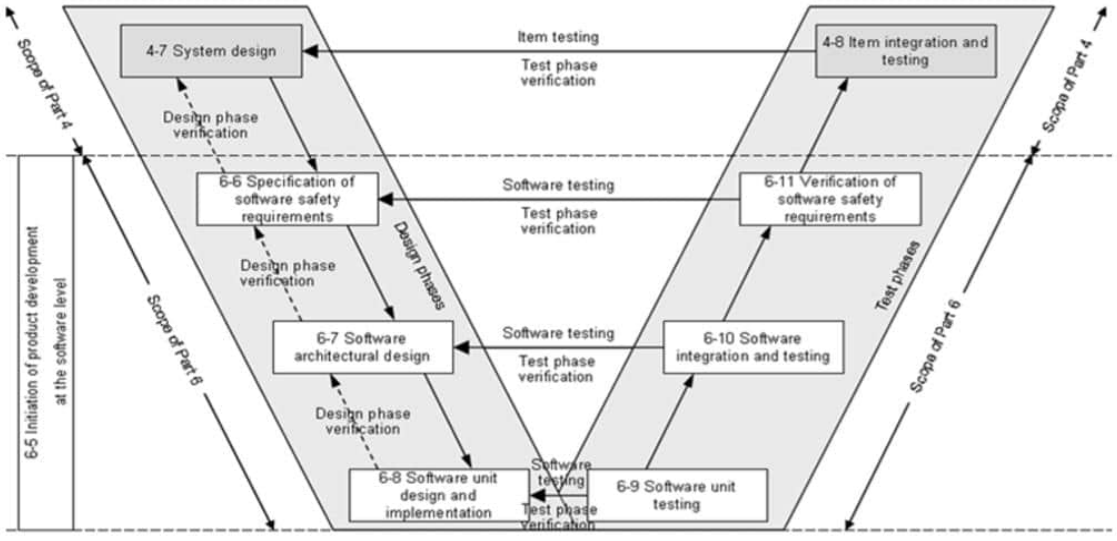


Figure 1. The V Model.

The figure was copied from the ISO 26262-6

From Figure 1 it can be seen that the testing process is carried out in a closed cycle with the process of developing. The Test process and Development process are classified by levels.

From the practice of testing models, it is worth noting that you need to start the testing process with the analysis and review of requirements. In this case, the test group should have the right to influence the text of the requirements. The review should be finished before the test group will start any new test activities.

After completing the work with the requirements, it is worth starting the Software unit test (6-9, Figure 1). It is at stage 6-9 that the status of requirements should be changed (from Work to Release of the software product).

Based on the unit test results, the test group recommends the development team to introduce certain changes in the models. This approach is important because there are rarely projects in which the requirements are sufficient for testing.

It is also rare that there is sufficient Design Document to develop a Test Harness before the implementation of the model is complete. Therefore, repeating, it is important to note that working on requirements and models is a process in which both teams, both developers and testers, are involved. Returning to the topic. When the Software unit

test for all subsystems is complete, the test team can proceed to functional testing (6-10 Picture 1, Software integration and testing).

So, according to ISO 26262, testing models for automotive includes the following stages of testing:

- verification of software safety requirements;
- software unit test;
- software integration and testing.

With practical experience, it is recommended to include as test criteria, the criteria specified in the MISRA AC GMG. In particular, checking data types, names of inputs and outputs, number of interfaces.

Tasks related to the verification of software safety requirements are to document (Jama, CarWeaver, SystemWeaver). At this stage, the requirements are refined through a review process by the Software architecture and QA engineer.

Tasks related to software unit test and software integration and testing include working with the model in MATLAB Simulink and requirements.

So, a software unit test provides for the creation of such a model testing scenario in which a set of combinations of signals at the inputs will be sufficient to obtain complete coverage of the model by tests according to the selected criteria (Condition, Decision, Execution, MCDC **, Complexity **). In this case, the test scenario (Test Sequences) and the expected model responses should be based strictly on the requirements text.

The Test Harness should be constructed in such a way that any actions of the QA Engineer do not lead to changes in the Design Model. Also, Test Harness must be one-way synchronized with the Design Model to enable Continuous Integration in Test Process. A software unit test involves testing a small part of the model, in which the completeness of a certain part of the algorithm is observed. In this case, the test is completed if the number of requirements is sufficient to obtain full coverage, and the model is performing as expected.

With practical experience, it is convenient to conduct a software unit test based on MIL technology. This thesis is not contested by ISO 26262 and MISRA GMG

As for software integration and testing, this stage provides for verification of the correctness of the generation of program code for the selected Hardware Target architecture. This stage is also carried out in order to test the conformity of the functioning of the function (Software Component) as a whole.

With practical experience, software integration and testing are convenient to carry out based on MIL, SIL, and HIL and technology. For obvious reasons, HIL is the most compelling and most challenging of these testing options. On the other hand, MIL and SIL have an advantage over HIL in terms of the ability to iterate over a much larger set of states of input signals to the Software Component, which when using Virtual Target (for example, Car Maker) allows you to implement test methods that are rarely used in HIL testing, for example, such as error injection.

CONCLUSION

The automation industry is one of the most sought after branches of engineering today. Development in which involves the constant injection of new methods. The implementation of these methods involves raising funds for software and specialists. The development of new methods for covering the model with tests will not only reduce the cost of introducing expensive software packages but also provide the ability to inject new methods that are not provided for by the developers of large software systems for software testing.

Describing test software development methods will be the purpose of future publications.

REFERENCES

1. ISO 26262 Software Compliance: Achieving Functional Safety in the Automotive Industry International Standardization Organization.
2. MISRA AC GMG: Generic modelling design and style guidelines, ISBN 978-906400-06-4 (PDF), May 2009.
3. Humennyi D., Parkhomey I., Tkach M. (2019) Structural Model of Robot-Manipulator for the Capture of Non-cooperative Client Spacecraft. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education. ICCSEEA 2018. Advances in Intelligent Systems and Computing, vol 754. Springer, Cham. https://doi.org/10.1007/978-3-319-91008-6_4

ANALYSIS OF FACTORS AFFECTING THE CYBERSECURITY STATUS OF THE INFORMATION AND TELECOMMUNICATIONS SYSTEM OF CRITICAL INFRASTRUCTURE OBJECTS

Katsalap V. – Doctor of Technical Sciences, docent, Department of Information Technologies Employment and Information Security, the National Defence University of Ukraine named after Ivan Cherniakhovskyi. Kyiv, Ukraine.

Pribyliev Y. – Candidate of Military Sciences, docent, Department of Information Technologies Employment and Information Security, the National Defence University of Ukraine named after Ivan Cherniakhovskyi. Kyiv, Ukraine.

Tsurko Y.

АНОТАЦІЯ

Кібератаки, що призводять до порушення функціонування об'єктів критичної інфраструктури держави, є причиною надзвичайних ситуацій. Кіберзахист об'єктів критичної інфраструктури держави стає ключовим напрямком, який спроможний забезпечити інформаційну безпеку держави. Проаналізовано основні фактори, які впливають на стан кібербезпеки інформаційно-телекомунікаційної системи об'єктів критичної інфраструктури держави.

КЛЮЧОВІ СЛОВА: Кібербезпека, кіберзахист, кіберзагроза, кібератака, інформаційно-телекомунікаційна система, об'єкт критичної інфраструктури.

ABSTRACT

Cyberattacks that disrupt the state critical infrastructure objects' functionality are the cause of emergencies. Cybersecurity of the state critical infrastructure objects becomes a key area that can ensure the state's information security. The main factors influencing the status of cybersecurity of the information and telecommunication system of the state critical infrastructure objects are analyzed.

KEYWORDS: Cybersecurity, cyberprotection, cyberthreat, cyberattack, information and telecommunication system, critical infrastructure object.

Protection of vital interests of human being and citizen, society and the state during the use of cyberspace is ensured by implementing a set of organizational, legal and technical measures for cyber protection of the state's critical infrastructure objects. Cyberattacks in modern society, become more frequent and increasingly affect the economy of the state. Therefore, reliable protection of the state critical infrastructure objects from cyberattacks is a condition of economic, political, social, defense and other components of national security [1]. Disruption of the state critical infrastructure objects functionality can lead to emergencies, environmental disasters, causing critical material, financial, economic damage or large-scale disruptions of cities and communities vital activities. The Decree of the President of Ukraine implemented urgent measures to form in the system of the Ministry of Defense of Ukraine the cyber forces to protect the sovereignty of the state, ensure its defense ability, prevent armed conflict and repel armed aggression in cyberspace [2].

The report analyzes existing information protection systems in information and telecommunication systems and defines the main components of cyber protection systems of information and telecommunication systems of the state critical infrastructure objects. Regulatory, organizational and technical components of cyber protection system directly affect the status of cybersecurity of information and telecommunication systems of the state critical infrastructure objects.

Information and telecommunication system of the state critical infrastructure objects is the complex organizational - technical system that includes mutually related elements: service staff, technical means, mathematical, software and information support. Sources of cyberattacks against information and telecommunications systems of critical infrastructure objects can be located both from the outside (external intruder) and from the inside. Features of construction and vulnerability of information and telecommunication systems of the Armed Forces of Ukraine, sources of information leakage, and the possibility of access to confidential information of cybercriminals are considered.

The analysis of the following factors impacts on the status of cybersecurity of information and telecommunication systems of the state critical infrastructure objects of has conducted, namely:

the status of the regulatory and legal documental base for cybersecurity of information and telecommunication systems of the critical infrastructure objects;

the sources of cyber threats, their capabilities, types, aspects, purpose, motives for cyberattacks;

the vulnerabilities in cyber protection systems that can be used for cyberattacks;

the existence or absence of favorable conditions for the cyber threats realization;

the attractiveness of the assets targeted by cyberattacks;

the consequences of the possible cyber threats realization;

the level of professional skills of personnel responsible for cybersecurity of objects and training organization for cybersecurity specialists.

Thus, it is found that cybersecurity of information and telecommunication systems of critical infrastructure is an integral part of information security of the state and depends on the factors considered in the briefing.

REFERENCES

1. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 року.
2. Указ Президента України №446/2021 від 26.08.2021 "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави".

АДАПТИВНІ ТЕХНОЛОГІЇ ЗАХИСТУ КІНЦЕВОЇ ТОЧКИ

Vlasenko M. M. – інженер кафедри кібербезпеки та комп'ютерної інженерії, Київський національний університет будівництва і архітектури, Київ, Україна.

Kajstura K. – PhD, Department of Computer Science and Automatics, University of Bielsko-Biala, Bielsko-Biala, Poland.

ABSTRACT

In today's world, during human-led attacks, thieves use predictable methods to infiltrate the device. Most suppliers put customers in a difficult and expensive position because they are too dependent on detection rather than prevention. Solutions are considered, most of which focus on prevention in order to stop threats as soon as possible. Detection is then used as another level to find the most challenging of the advanced threats. Without this balance, SOCs are full of incidents and warnings, and attackers eventually succeed. In fact, the vast majority of alerts seem to have created a crisis in an industry that is destroying SOCs and preventing them from focusing on the critical incidents for which critical incident detection products were actually created. In short, it is important to find violations. But it is better to prevent them - for efficiency and to focus SOC.

KEY WORDS: information security, cybersecurity, adaptive security, endpoint security.

АНОТАЦІЯ

В сучасному світі під час атак, керованих людьми, зловмисники використовують передбачувані методи для проникнення на пристрій. Більшість постачальників ставлять клієнтів у важке та дороге становище, оскільки вони занадто залежать від виявлення, а не від запобігання. Розглянуті рішення котрі в більшості зосереджуються на запобіганні, щоб якнайшвидше зупинити загрози. Потім використовується виявлення як інший рівень, щоб знайти найскладніші з передових загроз. Без цього балансу SOC переповнюються інцидентами та попередженнями, і зловмисники в кінцевому підсумку досягають успіху. Насправді, переважна кількість сповіщень, здається, створила кризу в галузі, яка руйнує SOC і не дозволяє їм зосередитися на критичних інцидентах, для яких насправді були створені продукти для виявлення критичних інцидентів. Коротше кажучи, важливо знайти порушення. Але краще запобігти їм – для ефективності та для концентрації уваги SOC.

КЛЮЧОВІ СЛОВА: захист інформації, кібербезпека, адаптивний захист, безпека кінцевої точки.

ВСТУП

Підприємства по всьому світу вкладають значні кошти в безпеку кінцевих точок, щоб захистити свої кінцеві точки. Незважаючи на витрачений час і гроші, сьогодні відбувається більше порушень, ніж будь-коли раніше. Зловмисники знайшли сліпі зони і щогодини експлуатують їх. Щоб вирішити цю проблему, командам безпеки потрібно зробити більше, ніж закрити кілька дір. Їм необхідно розглянути інноваційний підхід для підвищення рівня захисту кінцевих точок і максимального забезпечення безпеки в цілому. Цей підхід називається адаптивним захистом.

Кінцева мета кібербезпеки в адаптивності. Це означає, що кіберінцидент повинен бути вирішений і система має повернутися до нормальної роботи за максимально короткий час. Кожне середовище клієнта унікальне, але сьогодні більшість технологій безпеки постачаються «приглушеними», щоб запобігти та уникнути помилкових спрацьовувань. Крім того, щоб отримати максимальний захист, багато виробників надають складні налаштування та параметри конфігурації. Їх налаштування лягає на плечі замовника, і якщо зроблено неправильно, негативний результат часто є катастрофічним. Крім того, покладатися лише на виявлення призводить до зменшення віддачі – і до великої кількості потенційних порушень. [1]

ЩО ТАКЕ ENDPOINT SECURITY?

Безпека кінцевої точки або захист кінцевої точки — це підхід кібербезпеки до захисту кінцевих точок, таких як настільні комп'ютери, ноутбуки та мобільні пристрої, від зловмисної діяльності.

За словами Gartner, платформа захисту кінцевих точок (EPP) — це рішення, яке використовується для «запобігання атак зловмисного програмного забезпечення на основі файлів, виявлення зловмисної активності та забезпечення можливостей розслідування та усунення, необхідні для реагування на динамічні інциденти безпеки та попередження».

Кінцева точка — це будь-який пристрій, який підключається до корпоративної мережі поза межами свого брандмауера.

Стратегія безпеки кінцевої точки є важливою, оскільки кожна віддалена кінцева точка може бути точкою входу для атаки , а кількість кінцевих точок лише збільшується зі швидким переходом на віддалену роботу, пов'язаним із пандемією. Згідно з опитуванням Gallup , більшість працівників США були віддалені в 2020 році, а 51% все ще були віддалені в квітні 2021 року. Ризики, пов'язані з кінцевими точками та їхніми конфіденційними даними, є проблемою, яка не зникає.

Кожне злом даних коштує в середньому 3,86 мільйона доларів США по всьому світу, а США в середньому становлять 8,65 мільйона доларів за злом даних згідно зі звітом Ponemon «Cost of a Data Breach Report 2020» (за замовленням IMB). Дослідження виявило, що найбільшим фінансовим впливом порушення був «втрачений бізнес», що становить майже 40% середніх витрат на порушення даних.

Захист від атак на кінцеві точки є складним завданням, оскільки кінцеві точки існують там, де перетинаються люди та машини . Підприємства намагаються захистити свої системи, не втручаючись у законну діяльність своїх співробітників. І хоча технологічні рішення можуть бути високоефективними, ймовірність того, що працівник піддасться атаці соціальної інженерії, можна пом'якшити, але ніколи не запобігти повністю.

Рішення захисту кінцевих точок працюють шляхом перевірки файлів, процесів і системної активності на наявність підозрілих або шкідливих індикаторів .

Рішення для захисту кінцевих точок пропонують централізовану консоль керування, з якої адміністратори можуть підключатися до своєї корпоративної мережі для моніторингу, захисту, розслідування та реагування на інциденти. Це досягається шляхом використання локального, гібридного або хмарного підходу.

Програмне забезпечення безпеки кінцевих точок захищає кінцеві точки від злому — незалежно від того, фізичні вони чи віртуальні, локальні чи поза ним, у центрах обробки даних чи в хмарі. Він встановлюється на ноутбуки, настільні комп'ютери, сервери, віртуальні машини, а також самі віддалені кінцеві точки. [2]

РІШЕННЯ

Корпоративні технології безпеки кінцевих точок для компаній середнього розміру намагаються здивувати нас чимось абсолютно новим. Вони забезпечують надійний захист від зловмисного програмного забезпечення, а в поєднанні з відповідними політиками, регулярними оновленнями та кібергігієною співробітників вони можуть захистити бізнес від більшості кіберризиків.

Насправді, у стратегіях кібербезпеки більшості середніх компаній, навіть із рішенням кінцевої точки, імовірно, все ще залишаться прогалини, які можна і потрібно закрити.

Багато компанії пропонують найновіші рішення безпеки – адаптивні рішення.

Symantec зосереджується на захисті, який є превентивним, гнучким і автоматичним. Ключовим компонентом є машинне навчання, створене на основі десятиліть досвіду Symantec з великими організаціями, які працюють над автоматизацією конфігурації параметрів захисту та забезпеченням найвищого рівня індивідуального захисту з нульовим впливом на продуктивність. Посилений захист також робить виявлення більш ефективним, дозволяючи SOC (Security Operations Center, Операційний центр безпеки — це об'єкт, де корпоративні інформаційні системи (вебсайти, додатки, бази даних, центри обробки даних, сервери, активне мережеве обладнання, комп'ютери та інше кінцеве обладнання) контролюється, оцінюється та захищається.) зосередитися лише на обмеженому наборі загроз і не мати справу з попередженнями та проблемами, які захист міг би зупинити.

Адаптивний захист автоматично/безперервно зменшує поверхню атаки кінцевої точки. Зловмисники більше не можуть створити єдину атаку, яка працює скрізь. Адаптивний захист індивідуальний для кожного підприємства та адаптується у міру змін у вашій організації. У вас унікальний захист. Це змушує просунутих зловмисників або адаптуватися - за величезну ціну для них, або просто відмовитися від вашої організації. Навіщо витрачати час, коли погані хлопці можуть легше зламати іншу організацію, яка має «універсальне» рішення безпеки кінцевої точки? Кіберзлочинці воліють писати один раз – і заразити щоразу – використовуючи свою мерзенну економію від масштабу.[1]

CrowdStrike пропонує новий підхід до безпеки кінцевих точок. На відміну від традиційних рішень безпеки або мережевої безпеки, рішення CrowdStrike для безпеки кінцевих точок об'єднує технології, необхідні для успішного припинення злому, включаючи справжні антивіруси наступного покоління та виявлення та реагування на кінцеві точки (EDR), керований пошук загроз та автоматизацію аналізу загроз , що надаються через єдиний легкий агент. Falcon Enterprise включає в себе такі модулі:

- Рішення NGAV від CrowdStrike, Falcon Prevent™ , має 100-відсотковий рейтинг для виявлення як відомих, так і невідомих зразків зловмисного програмного забезпечення з показником хибнопозитивних результатів нуль відсотків.
- Falcon Insight™ EDR збирає та перевіряє інформацію про події в режимі реального часу для запобігання та виявлення атак на кінцеві точки.
- Команда CrowdStrike Falcon Overwatch™ підносить виявлення за межі автоматизації. Завдяки одній з найдосвідченіших команд у галузі та CrowdStrike Threat Graph ™ , базі даних, яка обробляє понад 6 трильйонів подій на тиждень, Falcon Overwatch виявляє та зупиняє понад 30 000 спроб злому на рік.

Коли загроза буде виявлена, команда Overwatch може вжити заходів за лічені секунди.

- Платформа Falcon X від CrowdStrike робить реальністю предикативну безпеку, інтегруючи розвідку загроз і захист кінцевих точок. Підходить для підприємств будь-якого розміру, організації нарешті мають можливість випередити дії супротивника і залишатися попереду. [2]

Panda Adaptive Defence — це додатковий рівень захисту для вашого поточного корпоративного рішення інформаційної безпеки.

Panda Adaptive Defence здатне точно класифікувати кожен активний додаток у вашій компанії, дозволяючи запуск тільки легітимним.

Робота рішення заснована на трьох принципах:

- безперервний моніторинг додатків на комп'ютерах і серверах компанії;
- автоматична класифікація з використанням технік машинного навчання на хмарній платформі Big Data;
- робота технічних експертів Threat Hunting, що аналізують додатки, щоб точно знати поведінку всіх програм, запущених у корпоративних системах. [3]

Адаптивний захист *Google Cloud Armor* допомагає захистити ваші програми, веб-сайти та служби Google Cloud від атак розподіленої відмови в обслуговуванні (DDoS) рівня L7, таких як HTTP flood та іншої високочастотної зловмисної активності рівня 7 (на рівні програми). Adaptive Protection створює моделі машинного навчання, які виконують такі дії:

- Виявляти й повідомляти про аномальну активність
- Створіть підпис, що описує потенційну атаку
- Створіть спеціальне правило Google Cloud Armor WAF, щоб заблокувати підпис

Ви вмикаєте або вимикаєте адаптивний захист на основі політики безпеки.

Сповіщення про аномальний трафік (потенційні атаки), які включають сигнатури атак, з’являються на інформаційній панелі подій Adaptive Protection з журналами подій, які надсилаються в Cloud Logging, де їх можна безпосередньо аналізувати або пересилати в подальший журнал або робочий процес моніторингу подій безпеки. Попередження про потенційні атаки також генеруються як висновки в Центрі управління безпекою .

Adaptive Protection створює кілька моделей для виявлення потенційних атак і визначення їхніх сигнатур. Сигнали, які використовуються цими моделями, щоб визначити, чи триває атака, походять із спостережуваних метаданих вхідного трафіку запитів із ваших проектів. Такі метадані включають: IP-адресу джерела, географію джерела та значення деяких заголовків запитів HTTP.

Фактичні характеристики, використані моделями, є похідними статистичними властивостями вищезгаданих сигналів. Тобто навчальні дані для моделей не включають фактичні значення будь-яких метаданих, таких як IP-адреси та/або значення заголовка запиту.

Загальний набір моделей виявлення, навчених лише зі штучними даними, використовується всіма клієнтами, щоб визначити, чи має місце атака, коли вперше ввімкнено адаптивний захист. Після того, як ви повідомляєте про будь-яку помилкову подію атаки, і моделі оновлюються за допомогою сигналів світлофора, характерних для ваших проектів, ці моделі є локальними для ваших проектів і не використовуються для інших клієнтів.

Після того, як адаптивний захист визначить, що відбувається потенційна атака, він генерує сигнатуру атаки, яка ефективна, щоб допомогти цілі швидко пом’якшити атаку. Щоб досягти зазначеного вище, після ввімкнення адаптивного захисту в політиці безпеки метрики трафіку та метадані запиту до серверної служби (пов’язані з політикою безпеки) постійно записуються, щоб дізнатися базові характеристики трафіку.

Оскільки Adaptive Protection потрібно дізнатися про базовий трафік, Adaptive Protection може знадобитися до однієї години перед створенням правил для пом’якшення потенційних атак. [4]

ВИСНОВКИ

На сьогоднішній день кіберзахист є одним із головних завдань, вирішення яких покладено на фахівців з інформаційної безпеки. Завдяки адаптивному захисту для кінцевої точки може регулювати атаки у режимі реального часу відповідно до стану пристрою, виділяє центрам безпеки більше часу, коли трапляються інциденти, і потенційно зупиняє ланцюжок атак із самого початку. Додавання нових технологій доводить, що розширення технологій запобігання та виявлення є життєво важливим для перемоги у битві проти зловмисників.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. K. Haley, "How Symantec Adaptive Protection Marks a New Chapter in Security Defense," 3 JUN 2021. [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/how-symantec-adaptive-protection-marks-new-chapter-security-defense.
2. A. Aarness, "WHAT IS ENDPOINT SECURITY? HOW ENDPOINT PROTECTION WORKS," 15 November 2021. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/endpoint-security/.
3. PANDA, "PANDA ADAPTIVE DEFENCE," [Online]. Available: https://iitd.com.ua/en/panda/adaptive-defence/. [Accessed 11 January 2022].
4. Google Cloud, «Google Cloud Armor Adaptive Protection overview,» 3 January 2022. [В Интернете]. Available: https://cloud.google.com/armor/docs/adaptive-protection-overview.

МЕХАНІЗМИ ДЕРЖАВНОГО УПРАВЛІННЯ ВИРОБНИЦТВОМ ПРИ ВПРОВАДЖЕННІ ІНДУСТРІЇ 4.0

Хлапонін Д. Ю. – кандидат наук з державного управління, доцент кафедри політичних наук і права, Київський національний університет будівництва і архітектури, Київ, Україна.

ABSTRACT

Industry 4.0 increases operational visibility, reduces costs, speeds up production time, and provides exceptional customer support. Operational sustainability is becoming a key corporate goal. The tendency of transition from "automated" to "autonomous" operations is analyzed. The directions of the state policy of Ukraine on stimulating the development of Industry 4.0 are outlined.

KEYWORDS: Industry 4.0, cyberphysical systems, Internet of Things, manufacturing, operational stability, governance mechanisms, Industry 4.0 standards.

АНОТАЦІЯ

Індустрія 4.0 підвищує оперативну видимість, знижує витрати, прискорює час виробництва, забезпечує виняткову підтримку клієнтів. Операційна стійкість стає ключовою корпоративною метою. Проаналізовано тенденцію переходу від «автоматизованих» до «автономних» операцій. Окреслено напрями державної політики України щодо стимулювання розвитку Індустрії 4.0.

КЛЮЧОВІ СЛОВА: Індустрія 4.0, кіберфізичні системи, Інтернет речей, виробництво, операційна стійкість, механізми державного управління, стандарти Індустрії 4.0.

1. ЗНАЧЕННЯ ТА ПЕРЕВАГИ ІНДУСТРІЇ 4.0

Визначення Industrie 4.0, запропоноване в 2011 році, було досить довгим. У статті під назвою «Індустрія 4.0 – розумне виробництво для майбутнього» GTAI (Germany Trade and Invest) розглянув питання, що таке розумна промисловість (синонім Індустрії 4.0) і що означає Індустрія 4.0.

Витяг: «Розумна промисловість» або «INDUSTRIE 4.0» відноситься до технологічної еволюції від вбудованих систем до кіберфізичних систем… INDUSTRIE 4.0 представляє майбутню четверту промислову революцію на шляху до Інтернету речей, даних і послуг. Децентралізований інтелект допомагає створювати інтелектуальні об'єктні мережі та незалежне управління процесами із взаємодією реального та віртуального світів, які представляють новий вирішальний аспект виробничого процесу».

1.1. ТЕХНОЛОГІЯ ІНТЕРНЕТУ РЕЧЕЙ ЯК НЕВІД'ЄМНА СКЛАДОВА ІНДУСТРІЇ 4.0

Інтернет речей, який передбачає взаємозв'язок унікальних пристроїв в рамках існуючої інфраструктури Інтернету, надав виробникам можливість приймати обґрунтовані стратегічні рішення, використовуючи дані в режимі реального часу, і досягати широкого спектру цілей, включаючи зниження витрат, підвищення ефективності, підвищення безпеки, інноваційні продукти, і більше. Згідно з дослідженням MPI Group, майже третина (31%) виробничих процесів зараз включає розумні пристрої та вбудований інтелект. Крім того, 34% виробників планують впровадити технологію IoT у свої процеси, а 32% планують впровадити технологію IoT у свої продукти.

Таким чином, можна зробити висновок, що Інтернет речей (IoT) є однією зі значущих технологій, яка впроваджується у виробничі процеси в різних галузях і є визначальною для функціонування виробничих ліній на основі зниження витрат, підвищення ефективності, підвищення безпеки, інновацій продукту.

COVID-19 знову викликав інтерес до технології IoT завдяки її віддаленому моніторингу та можливостям прогнозного обслуговування. З точки зору громадської безпеки, непрактично, а то й неможливо, щоб технічні працівники польових служб з'являлися на робочих місцях миттєво; кожен робочий порядок повинен бути ретельно спланований заздалегідь. Пристрої з підтримкою IoT дозволяють виробникам безпечно контролювати роботу обладнання на відстані та виявляти потенційні проблеми ще до того, як виникне несправність; вони також дають можливість технічним працівникам отримати повне уявлення про проблему та знайти потенційні рішення до того, як вони прибудуть на робоче місце, щоб вони могли увійти в курс справи та вийти із рішенням проблеми набагато швидше.

1.2. КОНВЕРГЕНЦІЯ ТЕХНОЛОГІЙ

Зближення інформаційних технологій та операційних технологій (конвергенція IT/OT) швидко прогресує, оскільки виробники усвідомлюють, що це є ключем до успішної цифрової трансформації. Пов'язаність та/або конвергенція між OT та IT є важливими для бізнесу, щоб конкурувати зі зростаючим попитом на більш тісну інтеграцію та більше інформації, яка використовує промисловий Інтернет речей, індустрію 4.0, 5G, хмару, периферію (edge), адитивне виробництво, розширену аналітику, цифровий близнюк, AR/ VR, AI, ML та інші новітні технології.

1.3. ДЕРЖАВНА ПОЛІТИКА УКРАЇНИ ЩОДО ВПРОВАДЖЕННЯ ТА РЕГУЛЮВАННЯ ІНДУСТРІЇ 4.0

Україна, як і інші розвинені країни, також впроваджує в свою економіку концепцію Індустрія 4.0.

З метою регулювання «Індустрії 4.0» в Україні Кабінет Міністрів України видав розпорядження від 17 січня 2018 року «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації». Це розпорядження є досі чинним.

Це розпорядження закріплює, що Індустрія 4.0 - оновлена концепція "розумного виробництва", що ототожнюється з "четвертою промисловою революцією" та появою кіберфізичних систем. Індустрія 4.0 - наступний етап цифровізації виробництв та промисловості, на якому головну роль відіграють такі технології та концепти, як Інтернет речей, "великі дані" (big data), "предиктивна аналітика", хмарні та туманні обчислення, "машинне навчання", машинна взаємодія, штучний інтелект, робототехніка, 3D-друк, доповнена реальність.

Інтеграція цифрових технологій у процеси виробництва, або цифровізація промисловості, є пріоритетом державної промислової політики. Державна політика стимулювання розвитку Індустрії 4.0 має три напрями:

створення інфраструктури Індустрії 4.0 - індустріальних парків, галузевих центрів технологій тощо;

доступ до капіталу для створення нових інноваційних виробництв;

розвиток цифрових навичок для підготовки персоналу, здатного працювати з технологіями Індустрії 4.0.

Іншими важливими завданнями є офіційне визнання міжнародних стандартів, які становлять загальновизнану основу Індустрії 4.0 (близько 100 стандартів), державна підтримка діяльності технічних комітетів, які беруть участь у роботі над стандартами, що стосуються Індустрії 4.0; створення механізмів трансферу технологій.

На підставі вищевикладеного випливає, що найбільш ефективними державними механізмами впровадження Індустрії 4.0 в Україні є створення індустріальних парків, галузевих центрів технологій, створення та розвиток інженерних кластерів, офіційне визнання міжнародних стандартів, які є загальновизнаною основою Індустрії 4.0.

Цих рішень вимагає поточна глобальна економічна ситуація, вплив пандемії COVID-19, прогрес у цифровізації та конвергенції інформаційних технологій та операційних технологій (конвергенція IT/OT), потреба в стійкій роботі виробничих заводів та інших підприємств. Тому ці рішення можуть бути прийняті до уваги іншими країнами для ефективного впровадження і управління Індустрією 4.0 у різних галузях економіки.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Industry 4.0 and the fourth industrial revolution explained: https://www.i-scoop.eu/industry-4-0/, 01.10.2021.
2. Industry 4.0. Preparing for the 4th Industrial Revolution. 15 June 2017. World Summit on the Information Society: https://www.unido.org/sites/default/files/2017-06/WSIS_Event_Flyer_v5_0.pdf, 01.10.2021.
3. 11 Trends That Will Dominate Manufacturing in 2021: https://global.hitachi-solutions.com/blog/top-manufacturing-trends, 01.10.2021.
4. Urquhart K.: Top Trends in 2021. Manufacturing Automation, February 2021, Vol. 36, No. 1, 12-13.
5. Framework for Cyber-Physical Systems Release 1.0 May 2016 Cyber Physical Systems Public Working Group: www.nist.gov, 01.10.2021.
6. Order of the Cabinet of ministers of Ukraine dated 17 January 2018 "On the approval of the concept of digital economy and society development in 2018-2020 years and the plan for its realization": https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text, 01.10.2021.

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПО ВСТАНОВЛЕННЮ ЦІННОСТІ ІНФОРМАЦІЙНОГО АКТИВУ

Ізмайлова О. В. – канд.техн. наук, доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури, Київ, Україна.

Красовська Г. В. – канд.техн. наук, доцент, доцент кафедри інтелектуальних технологій Київського національного університету імені Тараса Шевченка, Київ, Україна.

Красовська К. К. – докт. філософії (PhD), бізнес-аналітик компанії SoftServe, Київ, Україна.

ABSTRACT

The object of research of this work is decision-making processes to determine the value of information assets (IA) in information security systems, the subject of research are the principles and methodological foundations of information technology for assessment of IA, which is operating on the basis of the model base management subsystem of the decision support system (DSS). Methods of alternative and scenario modeling, forecasting, multifactor analysis and evaluation of decisions, expert evaluation, analysis of hierarchies are used in building the database of models.

KEY WORDS: information systems security, information asset value, decision support system, expert evaluation, model base, alternative and scenario modeling.

АНОТАЦІЯ

Об'єктом дослідження цієї роботи є процеси прийняття рішень по встановленню цінності інформаційного активу (ІА) в системах інформаційної безпеки, предметом дослідження – принципи та методологічні основи побудови інформаційної технології оцінювання ІА, що функціонує на основі підсистеми управління базою моделей системи підтримки прийняття рішень (СППР). При побудові бази моделей застосовані методи альтернативного та сценарного моделювання, прогнозування, багатофакторного аналізу та оцінки рішень, експертного оцінювання, аналізу ієрархій.

КЛЮЧОВІ СЛОВА: безпека інформаційних систем, цінність інформаційного активу, система підтримки прийняття рішень, експертне оцінювання, база моделей, альтернативне та сценарне моделювання.

ВСТУП

В умовах стрімкого розвитку цифрових технологій та в нових реаліях функціонування бізнес-структур з використанням «всесвітньої павутини» інформація стає не тільки найважливішим вирішальним ресурсом компанії, частиною її інтелектуального капіталу, а і вирішальною проблемою її різноаспектної безпеки. Як об'єкт забезпечення інформаційної безпеки визначається інформаційний актив компанії, який розглядається як сукупність відомостей (інформації), що представляє цінність для організації та (або) його клієнтів, ділових партнерів і працівників. Правильно враховані та оцінені активи дозволяють при управлінні компанією визначити міри критичності порушення інформаційної безпеки ІА та встановити вимоги до їх системного захисту, ефективно управляти вже наявними вигодами володіння цінною інформацією.

Метою дослідження є пошук та оптимізація шляхів розв'язання задачі встановлення цінності ІА з поширенням міри систематизації та формалізації процесів оцінювання. Основою формалізації процесів є математико-логічного інструментарій оцінювання, що враховує реальні ситуаційні фактори функціонування компанії, слабко структуровані умови прийняття рішень та концептуальну невизначеність даних.

1 АНАЛІЗ ЛІТЕРАТУРНИХ ДАНИХ ТА ПОСТАНОВКА ПРОБЛЕМИ

В сучасних наукових публікаціях та практичних розробках цінність ІА представляється як якісний і (або) кількісний показник, що визначає міри критичності для компанії порушення їх інформаційної безпеки, ступінь тяжкості наслідків від втрати значущих властивостей ІА, встановлює їх рейтинг як об'єкту захисту та прогнозує розмір можливих збитків при реалізації на цьому активі загроз інформаційній безпеці [1-5]. Достовірність встановлення цінності активу є гарантом обґрунтованого визначення вразливих точок інформаційних небезпек та орієнтує розробника на ефективний вибір засобів захисту. Існуючі розробки, як правило, базуються на застосуванні методів експертного оцінювання [1-8]. Спираючись на проведений аналіз літературних джерел, був зроблений висновок, що існує проблема недостатньої досконалості системи оцінювання ІА, що потребує рішення як з точки зору забезпечення міри достовірності та своєчасності результатів, так і з точки зору підвищення досконалості, доступності та зручності для користувача існуючого інструментарію оцінювання. Ефективним важелем розв'язання цієї проблеми є застосування сучасних можливостей СППР, побудова якої базується на стандартизованій інформаційній людино-машинної технології (протоколі) оцінювання. Остання структурує процеси прийняття рішень, забезпечує їх альтернативність, визначає послідовність, виконавців, моделі та методи оцінювання; удосконалює інтерактивний інструментарій оцінювання з наданням експерту та особі, що приймає рішення (ОПР), можливості врахування різних властивостей інформаційної

безпеки ІА (конфіденційність, цілісність, доступність).

2 ПРИНЦИПИ ТА МЕТОДОЛОГІЧНІ ОСНОВИ ПОБУДОВИ СППР

У відповідності до встановленої мети дослідження були проаналізовані і закладені наступні принципи та методологічні основи побудови СППР по встановленню цінності ІА:

- побудова людино-машинної технології експертного оцінювання на основі бази моделей СППР і правил керування цими моделями;
- реалізація ідеї системної узгодженості апарату формалізації, математичного забезпечення та правил отримання якісної інформації від ОПР та експертів;
- використання методів якісного аналізу з їх інтерпретацію в кількісному вимірюванні цінності ІА на основі встановленої шкали оцінювання;
- врахування при побудові шкал оцінювання здатність людини розпізнавати та формувати свої оцінки в рамках рекомендованих обмежень числа Міллєра) [1,6];
- встановлення правила управління моделями, що гарантує користувачеві можливість у відповідності з існуючими ситуаційними умовами створювати альтернативні сценарії оцінки ІА;
- прийняття рішень має базуватись на професійності, інформованості, інтуїції, інтелекті ОПР та експертів;
- застосування методу індивідуального опитування зі встановленими правилами доступу;
- забезпечення при узгодженні та угрупуванні кінцевих результатів реального компромісу з урахуванням думок і рівня компетентності кожного експерта;
- прийняття остаточного рішення є прерогативою людини – колективу спеціалістів, відповідальних за політику компанії та її інформаційну безпеку.

Ключовим аспектом побудови СППР є підсистема управління моделями, що має два компоненти: наповнення бази моделей та система управління базою моделей (СУБМ). При наповненні бази моделей застосований апарат побудови відкритої бази моделей, що включає дві складові: перша – створення процесової альтернативної моделі інформаційної технології (ПАМІТ) прийняття рішень по встановленню цінності ІА, друга – формування бази моделей по її реалізації. При формуванні бази моделей застосовуються основи реляційного моделювання. При цьому ідентифікується тип моделі, її зміст, структура вхідної та вихідної інформації, виконується прив'язка кожної моделі до процесів ПАМІТ. Кожен процес ПАМІТ на основі моделі «сутність - зв'язок» асоційований з базою моделей. Цей зв'язок визначає, модель (або моделі) якого типу застосовуються для реалізації процесу. Таким чином ПАМІТ є логічним та обчислювальним середовищем для складання, подання і маніпулювання множиною моделей і є основою програмної реалізації СУБМ.

3 ВИСНОВКИ

В роботі проаналізовані принципи та методологічні основи побудови СППР встановлення цінності ІА компанії.

Цінність ІА розглядається як якісно-кількісний показник, визначений в межах структурованої шкали оцінювання. Він визначає міру критичності порушення їх інформаційної безпеки для компанії, ступінь тяжкості наслідків від втрати значущих властивостей ІА, встановлює рейтинг ІА як об'єкту захисту.

Визначальним фактором підвищення ефективності встановлення цінності ІА є те, що СППР будується як «комфортний» для людини інструментарій оцінювання у вигляді інформаційної людино-машинної технології, в якій системно пов'язані математичні моделі та методи експертного оцінювання. Для реалізації цього пропонується апарат побудови відкритої бази моделей та системи управління цією базою з метою налаштування технології на конкретні умови прийняття рішень.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Izmailova O. Assessing the Variety of Expected Losses upon the Materialisation of Threats to Banking Information /O.Izmailova, H. Krasovska, K. Krasovska ,V. Zaslavskyi// Information & Security: An International Journal , vol. 45 (2020): 89-118 https://doi.org/10.11610/isij.450
2. Yurii Kozhedub, "Implementation of a process approach to information security risk management in documents NIST P-ISSN 2411-1031," Information Technology and Security, no.2(9) (2017): 76–89
3. Oleksii Barybin, "Methodology of testing for the penetration of the website of higher education institute," Standartyzatsiia, sertyfikatsiia, yakist. Systemy upravlinnia, no.4(116) (2019): 12–18
4. Пискунов И. Оценка стоимости информационніх активов, https://www.anti-malware.ru/analytics /Technology_Analysis/informational_assessment
5. Поляничко М.А. Методика оценки совокупной ценности информационных активов при оценке рисков от инсайдерских угроз информационной безопасности Bush // Информатика, вычислительная техника и управление, серия: Естественные и технические науки, 2019 , -№8. - с.107-110
6. Khlaponin Y. Management risks of dependence on key employees: Identification of personnel /Khlaponin Y.,Izmailova, O., Qasim, N.H., Krasovska, H., Krasovska, K.//CEUR Workshop Proceedings, 2021, 2923, - P.295–308
7. Красовска Г.В., Ізмайлова О.В. Підхід до побудови відкритої бази моделей СППР по оцінці інвестиційних проектів техногенної безпеки, Київ //

Управління розвитком складних систем.-2018.- вип. №33.- с. 118-124

8. Гожий А. П. Системные технологии генерации и анализа сценариев / А. П. Гожий, И. И. Коваленко // Автоматика. Автоматизація. Електротехнічні комплекси та системи . - 2005. - № 2. - С. 89-96.

МУЛЬТИАГЕНТНИЙ ПІДХІД ПРИ ПОБУДОВІ СЦЕНАРІЮ ОЦІНКИ ОЧІКУВАНИХ ЗБИТКІВ ПРИ РЕАЛІЗАЦІЇ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ

Красовська К. К. – докт. філософії (PhD), бізнес-аналітик компанії SoftServe, Київ, Україна.

Ізмайлова О. В. – к.т.н., доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури, Київ, Україна.

Красовська Г. В. – к.т.н., доцент, доцент кафедри інтелектуальних технологій Київського національного університету імені Тараса Шевченка, Київ, Україна.

ABSTRACT

The object of the study is the scenario of estimating the expected losses in the implementation of information security threats to the bank's information systems, the subject of the study is to optimize the scenario of forecasting losses based on the use of multi-agent technologies.

KEYWORDS: information security, risk assessment, multi-agent system, expected loss, information asset, intelligent agent.

АНОТАЦІЯ

Об'єктом дослідження є сценарій оцінки очікуваних збитків при реалізації загроз інформаційної безпеки інформаційних систем банку, предметом дослідження є оптимізація сценарію прогнозування збитків на основі застосування мультиагентних технологій.

КЛЮЧОВІ СЛОВА: інформаційна безпека, оцінка ризиків, мультиагентна система, очікуваний збиток, інформаційний актив, інтелектуальний агент.

ВСТУП

Основою стабільного функціонування програмних комплексів, які забезпечують роботу банків та проходження їх бізнес-процесів, є вирішення проблем забезпечення інформаційної безпеки установ в умовах постійного розвитку інформаційних технологій та діджиталізації суспільства.

Широке використання інформаційних технологій для підтримки конкурентної спроможності банків та фінансових установ, що, в свою чергу, викликає появу нових видів шахрайства та способів порушення інформаційної безпеки, унеможливлює повне уникнення втрат при функціонуванні інформаційних систем (ІС) банків. Тому актуальною стає проблема результативної оцінки ризиків та можливих втрат при реалізації загроз інформаційної безпеки ІС банку. Достовірна оцінка прогнозованих втрат надає можливості по знаходженню раціонального компромісу щодо прийняття, зниження або використання на користь банку того чи іншого рівня ризику.

Метою дослідження є оптимізація сценарію оцінки очікуваних збитків при реалізації загроз ІС банку шляхом використання мережі інтелектуальних агентів[6,8,9].

1 АНАЛІЗ ЛІТЕРАТУРНИХ ДЖЕРЕЛ ТА ПОСТАНОВКА ПРОБЛЕМИ

Існує багато досліджень щодо аналізу та управління ризиками в банках та фінансових установах. Серед наукових розробок представлено результати пошуку рішень ефективного ризик-менеджменту, а також протидії загрозам що виникають в процесі банківської діяльності [1–3]. Крім того представлена велика кількість наукових робіт, присвячених застосуванню сценарного підходу, експертної оцінки, багатокритеріального оцінювання та побудові систем підтримки прийняття рішень (СППР) для управління ризиками та оцінки очікуваних збитків при реалізації загроз ІС банку [4–7].

Аргументація ефективності застосування багатокритеріального оцінювання групою где усилия разных агентов направлены на решение общей проблемыекспертів різних факторів впливу незалежно вид їхньої природи (кількісної або якісної) доведено у роботі [4], а також побудовано сценарій проведення оцінки очікуваних збитків при реалізації загроз ІС банку. Важливо зауважити, що основу даного сценарію складає проведення прогнозування можливих збитків по інформаційних активах (ІА), що складають ІС банку, в даній роботі ІА – це інформація або ресурс (інформаційний, технічний, програмний), що підлягає захисту у банку, його інформаційних мережах та

системах, наприклад: дані про клієнтів банку, системне та прикладне програмне забезпечення (ПЗ), фізичне комп'ютерне устаткування тощо.

З огляду на те, що оцінювання можливих втрат проводиться людиною-експертом, постає проблема виникнення так званого людського фактору: можливість помилок при проведенні оцінювання. Крім того постає питання необхідності та складності резервування експертів як вузькопрофільних спеціалістів (наприклад, у випадку відпустки, лікарняного, звільнення тощо). Таким чином, з метою розв'язання цих питань, пропонується проведення оптимізації розробленого людино-машинного інструментарію, шляхом використання мережі інтелектуальних агентів. Пропонована оптимізація, окрім забезпечення формалізації оцінювання, розширює можливості розробленого сценарію, дозволяючи проводити різносторонню оцінку можливих втрат через співпрацю експертів та інтелектуальних агентів.

2 ОПТИМІЗАЦІЯ СЦЕНАРІЮ ПРОВЕДЕННЯ ОЦІНКИ ОЧІКУВАНИХ ЗБИТКІВ БАНКУ

З огляду на складність та динамічність банківської діяльності та середовища, в якому функціонують банки, було виявлено наступні вимоги до оптимізації сценарію проведення оцінки очікуваних збитків при реалізації загроз ІС банку:

- з метою якісного проведення прогнозування збитків при реалізації загроз необхідно впровадження гнучкої експертної системи, що здатна до автономних дій;
- необхідна розробка програмного інтерфейсу для забезпечення співпраці користувача та мережі інтелектуальних агентів, що використовуються для оптимізації;
- необхідна підтримка дистрибуції та контролю даних, що розподіляються між агентами;
- оскільки у банках досить часто існують застарілі ІС та різнотипні програмні платформи, тому необхідна підтримка можливості взаємодії з такими ІС.

Для реалізації поставлених вимог пропонується розробка мультиагентної системи. Використання мультиагентної системи забезпечує організацію складних взаємодій та кооперацію багатьох систем з підтримкою обміну даними, цілісність існуючої організаційної структури та автономію її компонентів [8, 9].

Вищезгаданий сценарій проведення багатокритеріальної оцінки очікуваних збитків при реалізації загроз ІС банку складається з декількох кроків [4]. На першому кроці необхідно провести оцінку ймовірності відбуття можливих рівнів збитку по кожному критерію при реалізації певного класу загрози по інформаційному активу ІС банку. На другому кроці проводиться згортка оцінок по кожному експерту, на третьому кроці відбувається обчислення загального показника очікуваного збитку при реалізації загрози по інформаційному активу ІС банку.

Тому для побудови мультиагентної системи для реалізації даного сценарію необхідно:

- визначити ролі та типи взаємозв'язків між агентами, що замінюють експертів;
- визначити та провести до єдиної структури дані – інформацію про випадки реалізації загроз, якими оперують агенти в системі;
- забезпечити можливість кластеризації та класифікації інформації про випадки реалізації загроз для забезпечення проведення прогнозування можливих збитків агентами.

Розроблені моделі, методи та алгоритми впровадження мультиагентної системи для проведення оцінки очікуваних збитків при реалізації загроз ІС банку буде покладено в основу інформаційно-аналітичної системи (ІАС), що може використовуватись для підвищення ефективності ризик-менеджменту банку.

3 ВИСНОВКИ

В роботі запропоновано оптимізацію сценарію проведення оцінки очікуваних збитків при реалізації загроз ІС банку [4] шляхом використання мультиагентних технологій, проаналізовані вимоги та принципи проведення оптимізації. Автоматизація процесу оцінювання та прогнозування очікуваних збитків дозволить підвищити ефективність розробленого логіко-математичного апарату проведення експертного оцінювання побудови та в подальшому провести розробку ІАС підтримки прийняття рішень, що реалізує розроблені моделі методи та алгоритми.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. В.Заславський Оптимизация кредитного риска коммерческого банка / В.Заславський, Э.Ненахов, А.Стрижак // Теория оптимальных решений. – 2005. – №4. – с.120-126.
2. А.Б. Камінський Концептуальні підходи до вимірювання фінансових ризиків / А.Б. Камінський // Фінанси України. – 2006. – № 5. – С. 78–85.
3. В. А. Кравченко Функціональний та інтегральний підходи до управління підприємницькими ризиками / В.А. Кравченко // Проблеми системного підходу в економіці. – 2008. – Т.1. – №6. http://jrnl.nau.edu.ua/index.php/EPSAE/article/view/4012.
4. Izmailova O. Assessing the Variety of Expected Losses upon the Materialisation of Threats to Banking Information /O.Izmailova, H. Krasovska, K. Krasovska ,V. Zaslavskyi// Information & Security: An International Journal. – 2020. – vol. 45. – P. 89-118. https://doi.org/10.11610/isij.450
5. М. З. Згуровський Сценарний аналіз як системна методологія передбачення / М.З. Згуровський // Системні дослідження та інформаційні технології. – 2002. – №1. – с. 7-38.
6. H.V. Krasovska Prototyping of intellectual decision support system for organizational and technological

trainings in construction./ Krasovska H.V., Izmailova O.V.,Krasovska K.K. // Materials of the XII International scientific and practical conference, "Areas of scientific thought", - 2015/2016. Volume 16. Mathematics. Physics. Modern Information technologies.
http://journals.uran.ua/eejet/article/view/3881/3557
7. О. В. Ізмайлова Підхід до побудови інформаційної основи системи підтримки прийняття рішень (СППР) по комплексній оцінці інноваційних проектів техногенної безпеки в будівництві / О. В. Ізмайлова, Г. В. Красовська та К. К. Красовська // Шляхи підвищення ефективності будівництва в умовах формування ринкових відносин: Зб. наукових праць. – 2012. – №28. – с. 222-229.
8. M. Wooldridge, An Introduction to MultiAgent Systems. New Jersey, USA: Wiley, 2002.
9. C. che Huang Using intelligent agents to manage fuzzy business processes / C. che Huang // 2001 IEEE Transactions on Systems Man and Cybernetics - Part A Systems and Humans 31(6), pp. 508 – 523.

ОБҐРУНТУВАННЯ ДОЦІЛЬНОСТІ РОЗРОБКИ МЕТОДИК ПРОВЕДЕННЯ АУДИТУ КІБЕРБЕЗПЕКИ

Штонда Р. М. – начальник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна.
Артемчук М. В. – старший науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна.
Черниш Ю. О. – старший науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна.

ABSTRACT

The need for regular audit of cybersecurity is the need to periodically assess the real state of security of information and communication systems.

KEY WORDS: audit of cybersecurity, information and communication systems.

АНОТАЦІЯ

Необхідність проведення регулярного аудиту кібербезпеки (АК) полягає в потребі періодично здійснювати оцінку реального стану захищеності інформаційно-комунікаційних систем (ІКС).

КЛЮЧОВІ СЛОВА: аудит кібербезпеки, інформаційно-комунікаційні системи.

ВСТУП

На даний час забезпечення кібербезпеки є одним із пріоритетів національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі [1]. Одним із способів перевірки досягнення зазначеного пріоритету стануть результати проведення АК в ІКС.

Метою дослідження є огляд ключової перспективи доцільності розробки методик проведення АК в ІКС.

1 АНАЛІЗ ЛІТЕРАТУРНИХ ДАНИХ ТА ПОСТАНОВКА ПРОБЛЕМИ

Заслуговує уваги наукова праця, в якій розглядається поняття аудиту інформаційної безпеки в організації, наведено його види та основні етапи [2]. Також в даному напрямку заслуговує уваги наукова праця, в якій запропоновано методику проведення незалежного аудиту інформаційної безпеки в установі щодо ефективності забезпечення захисту інформації – одного з найбільш результативних на сьогоднішній день інструментів для отримання незалежної та об'єктивної оцінки поточного рівня захисту інформації, приведення та підвищення стану захищеності систем [3].

Однак, невелика кількість публікацій та досліджень розглядають систематизований підхід до проведення АК в ІКС.

2 РЕЗУЛЬТАТ ДОСЛІДЖЕННЯ

АК в ІКС – це систематизований, незалежний і документований процес отримання оцінки стану кібербезпеки в ІКС та його відповідності вимогам, процедурам та методикам, що базуються на вимогах національних стандартів та рекомендаціях міжнародних стандартів з питань кібербезпеки.

Необхідність проведення регулярного АК полягає в потребі періодично здійснювати оцінку реального стану захищеності ІКС щодо можливості протистояти зовнішнім і внутрішнім кіберзагрозам, які постійно змінюються та адаптуються.

Проблеми забезпечення належного рівня кібербезпеки вимагають систематизованого підходу до аналізу стану захисту інформації та кібербезпеки, який базувався би на реальних показниках, отриманих під час АК, тому для досягнення даного пріоритету є необхідним розроблення методик проведення АК в ІКС.

3 ВИСНОВКИ

Таким чином, проведення АК є обов'язковим для всіх органів державної власності. Чітке виконання розроблених методик дозволить визначити ефективність забезпечення кібербезпеки в ІКС.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Указ Президента України від 26.08.2021 року №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". URL:https://zakon.rada.gov.ua/laws/show/447/2021.
2. Рой Я.В., Мазур Н.П., Складанний П.М. Аудит інформаційної безпеки – основа ефективного захисту підприємства // Кібербезпека: освіта, наука, техніка №1(1), Київ, Київський університет імені Бориса Грінченка, 2018. С. 86-93.
3. Артемчук М.В. Штонда Р.М., Нещерет І.Г., Терещенко Т.П., Цимбал І.В., Придатченко В.О. Методика проведення незалежного аудиту інформаційної безпеки установи щодо ефективності забезпечення захисту інформації // Вісник ВІТІ. Комунікаційні та інформаційні системи №2(2), Київ, Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2021. С. 4-17.

БОЙОВИЙ ІОТ ЯК НОВІТНІЙ ТРЕНД ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ: ПЕРСПЕКТИВИ ТА НОВІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Козубцов І. М. – доктор пед. наук, канд. техн. наук, старший науковий співробітник, провідний науковий співробітник науково-дослідного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна.

Козубцова Л. М. – канд.техн. наук, доцент кафедри математики та фізики Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна.

Кіт Г. В. – канд.техн. наук, доцент, завідувач кафедри інформаційних технологій та програмування Івано-франківська філія університету "Україна".

Ліщина В. О. – канд.техн. наук, доцент, завідувач кафедри комп'ютерних наук Луцького національного технічного університету.

Артемчук М. В. – старший науковий співробітник науково-дослідного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна.

ABSTRACT

The last decade is characterized by a technological trend towards using the concept of Internet of Things, IoT. It was further developed in the Armed Forces as the Internet of Battle Things (IOBT). The main prospects and problems affecting the state of cybersecurity of the Armed Forces are analyzed.

KEY WORDS: IoBT, Technology, Internet of things, prospects, problems, cybersecurity.

АНОТАЦІЯ

Останнє десятиліття характеризується технологічним трендом до використання концепції Internet of Things, IoT. Вона набуло подальшого розвитку в Збройних силах як бойовий інтернет речей (Internet of Battle Things, IoBT). Проаналізовано основні перспективи та проблеми, які впливають на стан кібербезпеки Збройних сил.

КЛЮЧОВІ СЛОВА: IoBT, технологія, інтернет речей, перспективи, проблеми, кібербезпека.

ВСТУП

За прогнозами [1] на полях битв майбутнього буде безліч "розумних" речей, які будуть обмінюватися інформацією, взаємодіючи один з одним і з людьми, але щоб це стало реальністю необхідно вирішити безліч проблем. Одним із способів вирішення цієї проблеми стало застосування рішень на основі Інтернету речей. Нове рішення отримало назву Інтернет бойових речей (Internet of Battle Things, IoBT).

Метою дослідження є огляд ключової перспективи та проблем забезпечення кібербезпеки новітньої технології бойового інтернету речей.

1 АНАЛІЗ ЛІТЕРАТУРНИХ ДАНИХ ТА ПОСТАНОВКА ПРОБЛЕМИ

В сучасних наукових публікаціях предметом огляду є перспективність використання концепції Internet of Things, IoT в Збройних силах розвинених країн світу стало технологічним трендом останнього десятиліття. Це яскравий показник їх сучасності та інноваційності. У міру появи нових технологій, спектр завдань і можливостей військових "розумних пристроїв" розширюється стрімкими темпами. IoT став проникати в усі можливі аспекти військової справи, починаючи від вирішення найскладніших завдань високоточного виявлення і знищення противника, закінчуючи моніторингом фізичного стану

конкретного військовослужбовця [2].

Стрімка поява Інтернету речей обумовлено логікою двох непереборних технологічних аргументів: машинного інтелекту і мережевих комунікацій [3].

Зважаючи на безумовну перспективність у застосуванні в Збройних силах, проте недослідженим є питання забезпечення кібербезпеки IoBT.

2 РЕЗУЛЬТАТ ДОСЛІДЖЕННЯ

Наступне десятиліття прогнозується кардинальними змінами у військовій сфері щодо підходів ведення бойових дій і всього, що їх супроводжує, починаючи від військової логістики та закінчуючи безпосередньо нанесенням удару по противнику. Театр військових дій буде щільно наповнений різними пристроями, що виконують величезний спектр основних і допоміжних бойових завдань. Це прилади, датчики, мобільні пристрої, "розумна" зброя, транспорт, роботи тощо (рис. 1). Всі вони будуть пов'язані між собою і солдатами, кожен у міру своєї "інтелектуальності" буде діяти як джерела інформації, яка підлягає аналізу для вироблення правильного рішення та видачі команди чинним підрозділам або техніці [3].

Відзначимо, що мілітаризація IoT розпочалось з розробки теорій "сетецентричної війни" (Network-centric warfare) і "багатодоменної битви" (Multi-Domain Battle) [4]. Вони передбачають абсолютно новий спосіб проведення військових операцій, при якому всі учасники (техніка, жива сила, штаби тощо) пов'язані єдиною інформаційною мережею [5].

Переваги IoBT, що привертають увагу військових є сусідами з низкою вразливістю, яку належить подолати розробникам. Одним з факторів точкового застосування IoBT у військовій справі є необхідність створення спеціальних пристроїв володіють підвищеним ступенем захисту, часто на базі "цивільних" моделей. Сьогодні бойові операції стають все складніше, в тому числі і технічно, але також зростають вимоги до безпеки і збереження життів солдатів. Тому будь-який мобільний або мережевий додаток, що забезпечує роботу IoBT-пристроїв, як і самі вони, повинні бути максимально захищені від стороннього втручання.

Рис. 1 Наочність широкого спектру взаємодіючих систем на полі бою в із застосуванням IoBT

Уразливість окремих елементів системи може бути спровокована різними доступними противнику або хакерам способами: фізичний і мережевий злом, прослуховування, РЕБ тощо.

Тому перед військовими науковцями стоїть складне наукове завдання: забезпечити, щоб при прийнятті на озброєння IoBT-пристроїв не залишалося можливостей маніпуляції ними або мережею, крадіжки, порушення потоку даних або фізичного знищення. Зробити це зараз непросто, враховуючи відносини багатьох виробників "розумних" пристроїв до забезпечення їх безпеки, а також тісне переплетення комерційних стаціонарних, мобільних і супутникових мереж, що сприяє наявності маси точок входу і незахищених місць. Незважаючи на це військовим відомствам рано чи пізно, але доведеться працювати з постачальниками і виробниками IoBT-пристроїв з метою примусу їх до введення більш надійних стандартів безпеки.

Безумовно використання у військовій сфері "розумних" пристроїв вже незворотний процес. Однак, на відміну від "цивільних", IoBT-пристрої

схильні до більш серйозних ризиків через участь в протиборстві між воюючими сторонами. Використовуючи їх уразливості, можна завдавати відчутної шкоди противнику.

3 ВИСНОВКИ

Зважаючи на перелічені переваги варто замислитися доки не пізно про негативні можливі наслідки [6]. Адже широкомасштабне використання IoBT-пристроїв несе великий ризик до створення передумов щодо порушення функціонування автоматизованих систем управління військами (функціональний збій і несанкціоноване керування військами та озброєнням). І хоча на перший погляд це виглядає фантастично, проте перебіг подій у науково-фантастичному фільмі “Terminator”, де штучний інтелект мережі “SkyNet” отримавши доступ до керування системою протиракетної оборони та ядерним озброєнням Збройних сил США, створив умови для знищення людства може стати реальністю. Так сьогоднішні “кібервійни” та “кіберпростір” з науково-фантастичного роману У. Гібсона “Нейромант” (1982) перекочували в сучасну дійсність [7].

Перспективи подальших досліджень у даному напрямку. Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні результати, що одержані в процесі наукового пошуку, становлять підґрунтя для подальшого вивчення проблеми кібербезпеки IoBT.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Слипченко В.И. Войны шестого поколения оружие и военное искусство будущего. М.: Вече, 2002. 382 с.
2. IoBT: empowering readiness to meet commander intent. URL: https://iobt.illinois.edu/
3. Kott A., Ananthram S., West B. The Internet of Battle Things.Computer 49.12 (2016): 70-75.
4. Буренок В.М., Кравченко А.Ю., Смирнов С.С. Курс на сетецентричесекую систему вооружений. Военно-космическая оборона. 2009. №5. URL: http://www.vko.ru/koncepcii/kurs-na-setecentricheskuyu-sistemu-vooruzheniya.
5. George I. Seffers. Defense Department Awakens to Internet of Things. January 1, 2015. URL: https://www.afcea.org/content/?q=defense-department-awakens-internet-things.
6. Козубцов І.М., Козубцова Л.М. Прогноз можливих наслідків настання “колапсу інформаційних систем спеціального призначення”. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). Київ: НА СБУ, 2021. С. 50-53.
7. Гибсон У. Нейромант: Фантаст.роман / Пер. с англ. Е. Летова, М. Пчелинцева. М.: Аст; СПб.: Terra Fantastica, 2000. 317с.

ПРИНЦИПИ ПОБУДОВИ СИСТЕМ IoT ЗАХИЩЕНИХ ВІД КІБЕРАТАК

Вишняков В. М. – канд. техн. наук, доцент, доцент кафедри кібербезпеки та комп’ютерної інженерії Київського національного університету будівництва і архітектури, Київ, Україна.

Комарницький О. О. - канд.техн. наук, заступник начальника відділу стратегічного планування Департаменту транспортної інфраструктури виконавчого органу Київської міської ради, Київ, Україна.

ABSTRACT

Building IoT systems without taking into account the possibility of security threats to information resources poses a danger not only to your system, but also provides the conditions for cyber attacks on any other Internet site. Therefore, it is important when using IoT systems to use secure technologies that would prevent unauthorized intrusion into resources that can be used by attackers, as to create threats of various kinds. The principles of construction of IoT systems, described in this paper, provide perfect protection of information resources of the system itself, as well as prevent their use by attackers to carry out cyber attacks on other network objects.

KEY WORDS: IoT system, security of Internet systems, secure data exchange, protection of IoT system resources from malicious use.

АНОТАЦІЯ

Побудова систем IoT без врахування можливості виникнення загроз безпеці інформаційним ресурсам утворює небезпеку не тільки для своєї системи, але і надає умови для реалізації кібератак на будь-які інші об’єкти мережі Інтернет. Тому важливо під час розробки систем IoT використовувати безпечні технології, які б не дозволяли несанкціонованому проникненню до ресурсів, які можуть бути використані зловмисниками, як для утворення загроз різного характеру. Принципи побудови систем IoT, що описані у цій роботі, забезпечують досконалий захист інформаційних ресурсів самої системи, а також унеможливлюють їх використання зловмисниками для реалізації кібератак на інші об’єкти мережі.

КЛЮЧОВІ СЛОВА: система IoT, безпека систем у мережі Інтернет, безпечний обмін даними, захист ресурсів систем IoT від зловмисного використання.

1 ПРОБЛЕМИ БЕЗПЕКИ СИСТЕМ IoT

Як показують опубліковані дані дослідників [1], у 2020 році кількість підключених пристроїв до IoT перевищила 30 млрд., а їх щорічний приріст збільшувався від 3 млрд. у 2017 році до 5 млрд. у 2020 році. У прогнозах до 2025 року передбачається, що цей приріст не знижуватиметься, а має тенденцію до збільшення. Це свідчить про швидке зростання потреб в управлінні віддаленими об'єктами і широкими можливостями для їх реалізації з використанням існуючих засобів і технологій. Однак швидке зростання потреб і широкі можливості реалізації IoT в короткі терміни часто призводить до недостатньо глибоко продуманих рішень з точки зору безпеки, що описано в роботі [1], де до найбільшої проблеми віднесено забезпечення безпеки на рівні мережі. Через недостатній захист систем IoT зловмисники можуть використовувати їх для реалізації DDoS-атак, число та потужність яких зростає зі збільшенням кількості користувачів IoT. Переважна більшість користувачів IoT вважають, що мають бути розроблені на державному чи міждержавному рівні загальні правила безпеки для IoT. Однак через розрізнення вимог, що висуваються до безпеки залежно від галузі використання IoT, розробка єдиних рекомендацій або стандартів є складною.

Результати опитування користувачів IoT, виконані компанією Gemalto, показали, що 90% із них не впевнені у забезпеченні безпеки. Таким чином, аналіз систем IoT з метою забезпечення безпечного обміну даними по каналах мережі Інтернет, а також технічні рішення в цій галузі, що наведені в даній роботі, є актуальними.

2 АНАЛІЗ ВАРІАНТІВ ОБМІНУ ДАНИХ У СИСТЕМАХ IoT

Для підключення пристроїв IoT до мережі Інтернет може використовуватися одна з двох схем, що представлені на рис.1 та рис. 2 відповідно.

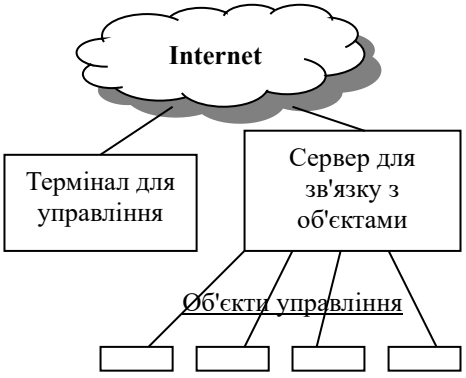


Рис. 1. Пряме управління об'єктами через мережу загального доступу

Схема, що представлена на рис.1, є найпростішою і може з успіхом використовуватися у внутрішніх комп'ютерних мережах, але в умовах мережі Інтернет, таке рішення має цілу низку недоліків:

1. підключення сервера безпосередньо до Інтернету сприяє втручанню непередбачуваних зовнішніх загроз у процеси управління;
2. через таке рішення для зловмисників підвищується можливість встановлення своїх ботнетів (шкідливих програм) на вашому сервері для реалізації DoS та DDoS атак;
3. для сервера потрібна виділена IP-адреса в Інтернеті, що пов'язано з матеріальними витратами;
4. для забезпечення безпеки сервера потрібно кваліфіковане обслуговування.

Перелічені недоліки відсутні у схемі, що представлена на рис. 2.

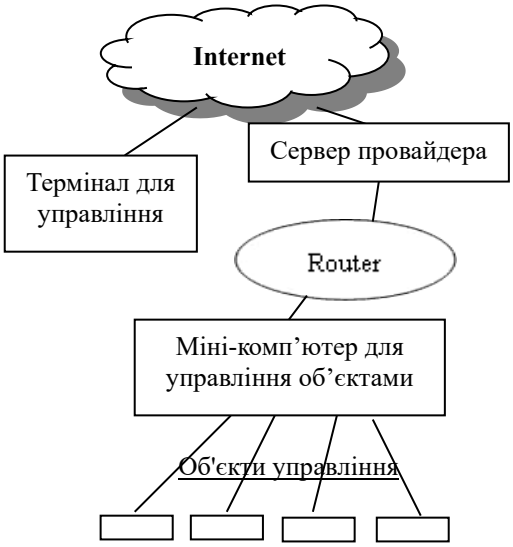


Рис. 2. Управління об'єктами з використанням сервера-посередника

У цій схемі потоки даних між терміналом та об'єктами управління фільтруються сервером посередником. Цей сервер може одночасно обслуговувати безліч користувачів, захищаючи потоки даних від атак. Встановлювати такі сервери можуть провайдери Інтернет-послуг, надаючи замовникам доступ до ресурсів з використанням хмарних технологій. Однак у разі високих вимог щодо безпеки інформації користувач може встановити власний або корпоративний сервер посередник. У випадках, коли сервер посередник буде вражений загрозою, інформація про об'єкти збережеться в цілісності.

3 ТЕХНІЧНІ РІШЕННЯ БЕЗПЕЧНОЇ СИСТЕМИ IoT

Управління об'єктами через Інтернет не вимагає передачі великих обсягів даних та високої швидкодії обміну повідомленнями. Це дозволяє використовувати найдосконаліші методи захисту даних. Слід зазначити, що для абсолютного захисту не потрібні дорогі технічні рішення. Такий захист реалізується програмно. Математично доведено, що абсолютний захист інформації забезпечує шифр Вернама [2]. Використання цього шифру вимагає генерування випадкових (не псевдовипадкових) бітів. Метод генерування таких бітів на будь-якому комп'ютері запропоновано у роботі [3], а у роботі [4] обґрунтовано вибір параметрів алгоритму Діффі-Хеллмана. З метою запобігання розкриття даних для криптографічних перетворень обрано алгебраїчну

групу у вигляді поля Галуа з характеристикою 2 і ступенем, який є безпечним простим числом з ряду 503, 563, 587, 719.Оскільки для таких полів невідомо розв'язання задачі дискретного логарифмування, то в сучасних умовах цей захист зламати неможливо [5].

4 НАТУРНА МОДЕЛЬ СИСТЕМИ IoT

Головним елементом системи, що слід захистити, від зловмисників, які можуть створювати загрози типу DDoS-атак, є міні-комп'ютер (див. рис. 2), у якості якого обрано Raspberry Pi 3. Він має 40 контактний інтерфейс GPIO для підключення об'єктів управління. Операційна система Linux версії Ubuntu 20.10, а як засіб програмування обрано Node.js версії v12.18.2 з пакетом onoff.

Для демонстрації процесу управління є посилання http://91.198.50.144:8000/CONPIN.html

5 ВИСНОВКИ

Описано причини виникнення проблеми безпеки у системах IoT. Визначено можливі загрози безеці як для самої IoT, так і для реалізації зловмисниками атак на інші об'єкти мережі Інтернет. Обрано схему безпечного обміну даними в системах IoT Розглянуто технічні рішення, які дозволяють убезпечити обмін даними в системах IoT за рахунок побудови ідеально захищеного каналу обміну даними. Показано на прикладі діючої моделі системи IoT можливість усунення проблем з аварійними ситуаціями в системах IoT, що виникають з різних причин, включаючи тимчасове відключення живлення та спроби несанкціонованого проникнення в систему. Наведено посилання на ресурс в Інтернеті для демонстрації процесу управління об'єктами. Запропоновані у цій роботі технічні рішення дозволяє повною мірою убезпечити системи IoT від інформаційних загроз.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Орлов С. (2020) Почему проблему безопасности интернета вещей оказалось так трудно решить? https://safe.cnews.ru/articles/2020-05-21_pochemu_problemu_bezopasnosti_interneta
2. Shannon C. Communication Theory of Secrecy Systems. *Bell System Technical Journal.* 1949. 28 (4). Pp. 656–715.
3. Чуприн В.М. Генерування випадкових чисел штатними засобами хостів мережі Інтернет./ В.М. Чуприн, В.М.Вишняков, М.П. Пригара // *Захист інформації*. – 2016. – Т. 18, №4. – С. 323-335.
4. Чуприн В.М., Вишняков В.М., Пригара М.П. Метод протидії незаконному впливу на виборців у системі Інтернет голосування. *Безпека інформації*. – 2017. – Том 23, №1. – С. 7–14.
5. Вышняков В.М., Комарницкий О.А. Транспарентные системы электронной демократии. Accent Graphics Communications & Publishing, Оттава, Канада, 2019, 98 с. http://doi.org/10.29013/VyshnyakovVM.KomarnickiyOA.TSED.2019.228

ІНТЕГРО-ДИФЕРЕНЦІАЛЬНА МОДЕЛЬ ЗАХИЩЕНОСТІ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ ЗМІШАНОГО ТИПУ

Страх О. П. – кандидат фіз.-мат. наук, старший викладач кафедри кібербезпеки, Сумський державний університет, Україна.

Мартинова Н. С. – кандидат технічних наук, доцент, доцент кафедри математичного аналізу і методів оптимізації, Сумський державний університет, Україна.

ABSTRACT

Wireless sensor networks (WSN) are undoubtedly one of the important places in the development of IT technologies, in particular the Internet of Things (IoT). But, given the peculiarities of their operation, these networks need reliable protection. First of all, it applies to hybrid network, which is characterized by high power mobile users, for example, with Wi-Fi extensions. In this work, we proposed a mathematical model of security management of this network, which is based on Fredholm integro-differential system.

KEYWORD: hybrid wireless sensor networks (WSN), integro-differential equation, theory of Moore–Penrose pseudo-inverse matrixes.

АНОТАЦІЯ

Бездротові сенсорні мережі безсумнівно займають одне з важливих місць у розвитку IT-технологій, зокрема інтернету речей. Але, враховуючи особливості їх функціонування, ці мережі потребують надійного захисту. Перш за все це стосується мереж змішаного типу, які характеризуються високою щільністю мобільних користувачів, наприклад з пристроями Wi-Fi. У даній роботі запропонована математична модель керування захищеністю такої мережі, яка ґрунтується на інтегро-диференціальній системі фредгольмового типу.

КЛЮЧОВІ СЛОВА: бездротові сенсорні мережі змішаного типу, інтегро-диференціальні рівняння, теорія псевдо-обернених матриць.

Функціонування новітніх бездротових сенсорних мереж (БСМ) з інтегрованими в них модульними мобільними вузлами, здатними використовувати різні датчики відповідно до потреб користувача, перетворює їх в мережі змішаного типу (БСМЗТ) з відповідними характеристиками гнучкості. Оскільки інтеграція зазначених модулів досягається без необхідності багатоступінчастої маршрутизації,а бази даних містять інформацію, отриману як мобільними, так і статичними вузлами [1], то виникає необхідність забезпечення належного захисту мережі в режимі реального часу. Запропонуємо нову модель захисту БСМЗТ від шкідливого програмного забезпечення, засновану на системі інтегро-диференціальних рівнянь фредгольмового типу.

Нехай бездротова сенсорна мережа складається з $x_1(t)$ статичних та $x_2(t)$ мобільних вузлів, які одночасно є справними (не піддалися зараженню шкідливим програмним забезпеченням) у кожний момент часу t. Тоді, враховуючи особливості взаємодії цих вузлів, а також їх відповідні характеристики, пов'язані зокрема з їх вразливістю до впливу шкідливих програм, а також спроможністю передачі шкідливого ПЗ на інші вузли мережі за певний проміжок часу $[a,b]$, режим функціонування цієї мережі можна описати за допомогою такої системи інтегро-диференціальних рівнянь:

$$\frac{d}{dt}x(t) - \Phi(t)\int_a^b\left(A(s)x(s) + B(s)\frac{d}{ds}x(s)\right)ds = f(t), \quad (1)$$

де $x(t) = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}(t) \in D_2^2\left([a,b]\right)$ — абсолютно-неперервна на відрізку $[a,b]$ 2-вимірна вектор-функція, похідна якої є інтегровною з квадратом на $[a,b]$: $\left(\frac{d}{dt}x(t)\right) \in L_2\left([a,b]\right)$, $\Phi(t)$ — $(2\times m)$-вимірна, $f(t)$ – (2×1)-вимірна, $A(t), B(t)$ — $(m\times 2)$-вимірні матриці, елементи яких належать простору $L_2\left([a,b]\right)$, крім того $\operatorname{rank}\Phi(t) = m$.

Тоді, аналогічно результату роботи [2], використовуючи теорію псевдообернених матриць Мура–Пенроуза, можна знайти необхідні та достатні умови розв'язності системи (1), а також побудувати відповідний вигляд загального її розв'язку.

Теорема. *Нехай для сталої* $\left(m\times(m+2)\right)$*-вимірної матриці*

$$D = \left(I_m - \int_a^b\left(A(s)\Psi(s) + B(s)\Phi(s)\right)ds, -\int_a^b A(s)ds\right),$$

де $\Psi(t) = \int_a^t \Phi(s)ds$, $\operatorname{rank} D = n_1$. *Відповідна однорідна для системи* (1) *інтегро-диференціальна система* ($f = 0$) *має* r_1*-параметричну* ($r_1 = m+2-n_1$) *сім'ю розв'язків виду*

$$x(t, c_{r_1}) = \Psi_0(t)P_{D_{r_1}}c_{r_1}, \quad c_{r_1} \in \mathbb{R}^{r_1},$$

де $\Psi_0(t) := \left(\Psi(t), I_2\right)$ — $(2\times(m+2))$*-вимірна матриця*, а $P_{D_{r_1}}$ — $((m+2)\times r_1)$*-вимірна матриця, що складається з* r_1 *лінійно незалежних стовпців* $((m+2)\times(m+2))$*-вимірної матриці-проектора* $P_D := I_{m+2} - D^+D$, $P_D: \mathbb{R}^{m+2} \to N(D)$, D^+ — *єдина* $((m+2)\times m)$ *-вимірна псевдо-обернена за Муром-Пенроузом до* D *матриця. Неоднорідна система* (1) *буде розв'язною тоді й тільки тоді, коли неоднорідність* $f(t) \in L_2([a,b])$ *задовольнятиме* $d_1 = m - n_1$ *лінійно незалежні умови*:

$$P_{Q_d^*}\tilde{b} = 0, \quad (2)$$

де $P_{Q_d^*}$ — $(d_1\times m)$*-вимірна матриця, що складається з* d_1 *лінійно незалежних рядків* $(m\times m)$*-вимірної матриці* $P_{D^*} := I_m - DD^+$, *яка є ортопроектором* $P_{D^*}: \mathbb{R}^m \to N(D^*)$, D^* — *транспонована до* D *матриця,* $\tilde{b} = \int_a^b\left(A(s)\int_a^s f(\tau)d\tau + B(s)f(s)\right)ds$.

При виконанні цих умов (2) *система* (1) *має* r_1*-параметричну сім'ю розв'язків виду*:

$$x(t, c_{r_1}) = \Psi_0(t)P_{D_{r_1}}c_{r_1} + F(t), \quad c_{r_1} \in \mathbb{R}^{r_1}.$$

Тут $F(t) = \tilde{f}(t) + \Psi_0(t)D^+\tilde{b}$.

Таким чином, за певних умов можна отримати достовірні дані щодо кількості справних вузлів БСМЗТ. Але залишається питання по налагодженню надійного захисту цієї мережі, який визначає основний компонент режиму її функціонування – $f(t)$. Очевидно, що умови (2) можуть бути виконані не для кожної такої неоднорідності. Розглянемо тоді систему інтегро-динамічних рівнянь з керуванням:

$$\frac{d}{dt}x(t) - \Phi(t)\int_a^b\left(A(s)x(s) + B(s)\frac{d}{ds}x(s)\right)ds = f(t) + +J(t)u, \quad (3)$$

усі відповідні компоненти якої задовольняють ті ж умови, що й у системі (1), $J(t)$ – задана $(2\times k)$-вимірна матриця з компонентами із простору $L_2\left([a,b]\right)$, а $u \in \mathbb{R}^k$ – вектор керування.

Тоді, скориставшись умовами розв'язності (2) системи один, отримуємо такі умови розв'язності розглядуваної системи (3).

$$P_{D_{d_1}^*}\left(\int_a^b\left[A(s)\int_a^s\left(f(\tau) + J(\tau)u\right)d\tau + B(s)\left(f(s) + J(s)u\right)\right]ds\right) = 0.$$

Ці умови можна також розглядати як деяку алгебраїчну систему відносно невідомого вектора $u \in \mathbb{R}^k$:

$$P_{D_{d_1}^*}\left\{\int_a^b\left[A(s)\int_a^s J(\tau)d\tau + B(s)J(s)\right]ds\right\}u = -P_{D_{d_1}^*}\tilde{b}.$$

Позначаючи для зручності $\mathrm{F} := -P_{D_{d_1}^*}\tilde{b}$ і $\mathrm{W} := P_{D_{d_1}^*}\left\{\int_a^b\left[A(s)\int_a^s J(\tau)d\tau + B(s)J(s)\right]ds\right\}$, отримаємо систему алгебраїчних рівнянь

$$\mathrm{W}u = \mathrm{F}:, \quad (4)$$

де W — $(d_1 \times k)$-вимірна матриця, а F — d_1 вимірна вектор-функція. Аналогічно позначаючи $m_1 := \operatorname{rank}\mathrm{W}$ та визначаючи $(k\times k)$-вимірну матрицю-проектор $(d_1 \times d_1)$-вимірну матрицю-проектор $P_{\mathrm{W}^*} := I_{d_1} - \mathrm{W}\mathrm{W}^+$, $P_{\mathcal{W}}: \mathbb{R}^{d_1} \to N(\mathcal{W}^*)$, де $\mathrm{W}^*, \mathrm{W}^+$ — $(k \times d_1)$-вимірні відповідно транспонована та псевдо-обернена за Муром-Пенроузом матриці до матриці W, отримуємо умови розв'язності системи (4):

$$P_{\mathrm{W}_d^*}\mathrm{F} = 0, \quad (5)$$

де $P_{\mathrm{W}_d^*}$ — $(d \times d_1)$-вимірна матриця, яка складається з $d := d_1 - m_1$ лінійно незалежних рядків матриці P_{W^*}.

Якщо вектор функція F, а відтак і матриця $J(t)$, є такою, що умови (5) виконуються, то система (4) є розв'язною, а початкова система (1) є керованою. Більш того, вектор керування системи буде визначатися таким r-параметричним ($r = d_1 + d_2 - n_1 - m_1$) загальним розв'язком системи (4):

$$u = P_{\mathcal{W}_r}c_r + \mathcal{W}^+\mathcal{F},\ c_r \in \mathbb{R}^r$$

де P_{W_r} — $(k \times r)$-вимірна матриця, яка складається з r лінійно-незалежних стовпців $(k \times k)$-вимірної матриці-проектора $P_{\mathrm{W}} := I_k - \mathrm{W}^+\mathrm{W}$.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Bertiz C., Lozano J.,Gomez-Ruiz J., García-Cerezo A. Integration of a mobile node into a hybrid wireless sensor network for urban environments // Sensors (Basel). 2019 Jan; 19(1): 215. doi: 10.3390/s19010215.
2. Самойленко А. М., Бойчук О. А., *Кривошея С. А.* Крайові задачі для систем лінійних інтегро-диференціальних рівнянь з виродженим ядром // Укр. мат. журн., – 1996. – т.48, №11 – С. 1576 – 1579.

АНАЛІЗ УМОВ ОРГАНІЗАЦІЇ ЕКСПЕРИМЕНТАЛЬНОГО ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ПРИКЛАДНОГО ОБЧИСЛЮВАЛЬНОГО ПРОЦЕСУ

Баканов В. С. – старший викладач кафедри кібербезпеки Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна.

Хусаінов П. В. – доцент кафедри кібербезпеки Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна.

Штаненко С. С. – докторант науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна.

ABSTRACT

The need to ensure the effective operation of entities of the National Cyber Security System stipulate the urgency of developing a scientific and methodological apparatus for rapid response to cyber incidents (cyberattacks). The fundamental impossibility of achieving algorithmic and information completeness of cyber defense equipment anticipates the implementation of a process to support the decision-making of the operational staff of cybersecurity. The report is dedicated to the presentation of the results of the analysis of conditions that must be taken into account when organizing an experimental assessment of the possibility of influence on the applied computational process.

KEY WORDS: cyberattack, vulnerability, experiment.

АНОТАЦІЯ

Необхідність забезпечення ефективної діяльності суб'єктів Національної системи кібербезпеки обумовлює актуальність розроблення науково-методичного апарату оперативного реагування на кіберінциденти (кібератаки). Принципова неможливість досягнення алгоритмічної та інформаційної повноти технічних засобів кіберзахисту передбачає впровадження процесу підтримки прийняття відповідних рішень оперативним персоналом органів кібербезпеки. Інший фактор невизначеності рішень полягає у відсутності апріорних даних для ідентифікації величини шкоди від наслідків кіберінциденту. Доповідь присвячена викладенню результатів аналізу умов, які необхідно врахувати при організації експериментального оцінювання захищеності прикладного обчислювального процесу.

КЛЮЧОВІ СЛОВА: кібератака, вразливість, випробування.

ВСТУП

Реагуючи на світові тенденції та виклики сьогодення з 2017 року у інформаційно-правовому просторі нашої держави з'явилася низка законодавчих положень, які визначають 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 [1].

Так, згідно [1] кібербезпека досягається та забезпечується якісним виконанням сукупності заходів кіберзахисту, які спрямовані на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування об'єктів кіберзахисту. На сучасному етапі основний підхід до забезпечення безпеки інформації в автоматизованих системах полягає в організації розмежування доступу, який базується на відповідній концепції диспетчера доступу повноваження на доступ обчислювального процесу до об'єктів інформаційного домену визначаються засобами операційної системи за результатами успішної авторизації користувача автоматизованої системи [2]. Найбільш суттєвим недоліком концепції диспетчера доступу є принципове припущення про сталість правильного функціонування прикладних обчислювальних процесів на всьому часовому інтервалі експлуатації автоматизованої системи тобто неможливість виконання ними непередбачених розробником дій у будь-який момент часу.

1 АНАЛІЗ ЛІТЕРАТУРНИХ ДАНИХ ТА ПОСТАНОВКА ПРОБЛЕМИ

Непривілейований авторизований користувач автоматизованої системи об'єкта кіберзахисту немає можливості розширити (змінити) свої повноваження, але у будь-який момент часу він може ініціювати цілеспрямовану зловмисну діяльність інсайдера (від англ. insider – внутрішній порушник). При цьому, на теперішній час, відомо чимало прикладів організації такої інформаційної взаємодії між прикладними обчислювальними процесами при посередництві системних об'єктів операційної системи (у межах відповідних їм інформаційних доменів (доступу), що перетинаються), яка може призвести до нав'язування непередбаченого виконання алгоритму виконання [3-5].

Отже можна констатувати, що розроблення науково-методичного оперативного реагування на кіберінциденти (кібератаки) тісно взаємопов'язаний з обґрунтуванням визначення ймовірності захищеності прикладних обчислювальних процесів у складі об'єкта кіберзахисту від нав'язування непередбаченого виконання на основі даних відповідних випробувань. На підставі викладеного, метою доповіді є аналіз умов для організації експериментального оцінювання захищеності прикладного обчислювального процесу від нав'язування непередбаченого розробником виконання на основі модифікації його алгоритму.

2 РЕЗУЛЬТАТ ДОСЛІДЖЕННЯ

Модифікація алгоритму роботи цільового обчислювального процесу шляхом руйнівного впливу на зміст її оперативної пам'яті досягається за рахунок нав'язування непередбачених значень тим чи іншим критичним даним. Критичними даними цільового обчислювального процесу будемо називати будь-які розташовані в його оперативній пам'яті дані, нав'язування непередбачених значень яким дозволяє інсайдеру вигідним для себе чином модифікувати (спотворити) алгоритм роботи. В цьому смислі можна говорити, що критичні дані визначають алгоритм. Серед критичних даних цільової програми будемо розрізняти управляючі та інші критичні дані.

Управляючими даними цільового обчислювального процесу будемо називати дані, що прямо або опосередковано визначають потік передачі управління, точніше, значення, яке на певному етапі виконання цільової програми потрапить у лічильних команд процесора. До таких даних можна віднести, наприклад, адреси повернення з функцій та покажчики на них (збережені значення покажчика стекового кадру), покажчики на функції та покажчики на покажчики. Нав'язування непередбачених значень управляючим даним призводить до непередбаченої модифікації (спотворення) потоку передачі управління у цільовому обчислювальному процесі. В результаті управління може (непередбачено) передаватись введеному в адресний простір цільового процесу сторонньому коду або, наприклад, деякому привілейованому фрагменту коду або функції, що дозволяє запускати довільні зовнішні програми. Завдяки цьому може (непередбачено) запускатись як одна із штатних програм, так і попередньо введена в цільову систему стороння програма (в залежності від можливостей та інтересів інсайдера). Нав'язування непередбачених значень управляючим даним дозволяє, в принципі, нав'язати їй довільний напрямок (адресу) передачі управління.

До інших критичних даних цільового обчислювального процесу будемо відносити будь-які її критичні дані, що не впливають на потік передачі управління в ній (або, якщо впливають, то не настільки, щоб шляхом їх непередбаченої модифікації можна було б нав'язати довільний напрямок передачі управління, як у випадку критичних даних, що виступають операндами умовних конструкцій).

Для того, щоб модифікувати алгоритм роботи цільового обчислювального процесу, треба непередбачено модифікувати ті чи інші з її критичних даних, причому, протягом проміжків часу, які обмежуються, з одного боку, моментом ініціалізації або модифікації цих критичних даних, з другого боку – моментом їх використання.

Критичні дані також варто поділити на такі, що прямо (безпосередньо) і непрямо (опосередковано) визначають алгоритм роботи цільового обчислювального процесу. Будемо вважати, що критичні дані прямо (безпосередньо) визначають алгоритм роботи, коли вони не є покажчиками на інші

критичні дані; такі критичні дані будемо називати також кінцевими критичними даними. Відповідно, критичні дані, що є покажчиками на інші критичні дані, будемо вважати такими, що непрямо (опосередковано) визначають алгоритм роботи цільового обчислювального процесу.

Модифікація алгоритму роботи цільового обчислювального процесу (шляхом руйнівного впливу на зміст її оперативної пам'яті) завжди здійснюється на основі фальсифікації тих чи інших критичних даних, які прямо (безпосередньо) визначають алгоритм її роботи, тобто на основі фальсифікації тих чи інших кінцевих критичних даних цієї програми. Фальсифікація критичних даних може виконуватись прямо (безпосередньо) і непрямо (опосередковано). Пряма (безпосередня) фальсифікація критичних даних полягає в нав'язуванні цим даним непередбачених значень, наприклад, шляхом їх ініціалізації такими значеннями або їх непередбаченої модифікації.

Для кібератак, які здійснюються методом нав'язування коду (injection-based attacks) – передбачають нав'язування цільовому обчислювальному процесу певного активного контенту з подальшою його активізацією у відповідному інформаційному домені доступу – передбачено застосування наступних понять (важливі для розуміння механізму реалізації): вектор атаки (injection vector); активний контент ("корисне навантаження"; payload); зона активізації контенту (activation zone); типовий результат активізації контенту (payload activation impact).

Умови реалізації кібератак даного класу:

програмна реалізація завантажувального модуля цільового обчислювального процесу має вразливість до руйнівного впливу на зміст її оперативної пам'яті;

інсайдер (суб'єкт атаки) має можливість спровокувати активізацію цієї вразливості, тобто передати цільовому обчислювальному процесу дані для активізації цієї вразливості.

До типових вразливостей програмної реалізації завантажувального модуля цільового обчислювального процесу, що створюють можливість атак даного класу відносяться: переповнення буфера (в стеку, в статичному або динамічному сегменті даних); переповнення розрядної сітки цілочисельних змінних; нав'язування форматних рядків.

Форми (способи виконання) переповнення розрядної сітки цілочисельних змінних (вони ж – види руйнівного впливу на значення цілочисельних змінних):

переповнення розрядної сітки цілочисельної змінної зверху;

переповнення розрядної сітки цілочисельної змінної знизу.

Руйнівний вплив на зміст оперативної пам'яті цільової програми досягається нав'язуванням вразливій функції форматованого виведення непередбачених специфікаторів формату, тобто форматного рядка, який містить непередбачені специфікатори формату. Функції форматованого виведення мають наступні спільні риси:

приймають змінну кількість аргументів;

приймають один чи більше фіксованих (обов'язкових) аргументів, останнім серед яких є так званий форматний рядок, який і повідомляє їм повну кількість аргументів;

обробляють всі аргументи, що йдуть після форматного рядка, згідно зі специфікаторами формату, що містяться в форматному рядку (як правило, виводять ці аргументи або зміст буферів, на які вони вказують).

Форматний рядок представляє собою суміш зі звичайних символів і так званих специфікаторів формату, які виступають замінниками для наступних аргументів. Відповідно, кожному специфікатору формату відповідає один із наступних аргументів, і при правильному застосуванні форматних рядків кількість специфікаторів формату в них повинна дорівнювати кількості переданих разом із ними функції форматованого виведення додаткових аргументів.

Загальні причини вразливості цільового обчислювального процесу до руйнівного впливу на зміст оперативної пам'яті:

відсутність в них або недостатність процедур забезпечення коректності вхідних даних;,

некоректна реалізація процедур оброблення вхідних даних.

Часто вразливості даного класу є наслідком покладання їх розробників на (невірні) припущення щодо того, що певні вхідні дані не можуть бути некоректними. Типові вектори атак даного класу тобто способи введення в оперативну пам'ять цільового обчислювального процесу руйнівних даних (узагальнено): (через) файли з даними, призначеними для оброблення; аргументи командного рядка; (через) змінні оточення; (через) конфігураційні файли; (через) файли з додатковими даними; (через) відповіді на запити на введення додаткових даних; (через) повідомлення, що надходять через канали комункації.

При цьому контрольований інсайдером обчислювальний процес може бути розташований як локально (в одному обчислювальному середовищі з цільовим обчислювальним процесом), так і віддалено по відношенню до нього (в одному обчислювальному середовищі іншого елементу об'єкта кіберзахисту).

3 ВИСНОВКИ

Основним елементом організації експериментального оцінювання захищеності цільового обчислювального процесу від нав'язування непередбаченого виконання алгоритму є вибір вектора атаки. В якості останнього пропонується використання мережевого інтерфейсу, а конкретніше, певне поле повідомлення, що на певному етапі, згідно комунікаційного протоколу, за яким здійснюється віддалена взаємодія, надається цільовому обчислювальному процесу. Активним контентом буде

включений у це повідомлення і призначений для нав'язування байт-код відкриття сеансу роботи через мережу з інтерфейсом командного рядка, а зоною активізації контенту – момент виходу потоку виконання цільового обчислювального процесу з уразливої функції (команда повернення з цієї функції).

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2010 року № 2163-VIII // Відомості Верховної Ради України. – 2017 . – № 45. – Ст. 403.
2. Автоматизовані системи. Терміни та визначення: ДСТУ 2226-93. – [Чинний від 1994-07-01]. – 94 с.
3. Антонюк А.О. Теоретичні основи моделювання та аналізу систем захисту інформації: [монографія]. – Ірпінь: Національний університет ДПС України, 2010. – 310 с.
4. Хусаінов П. В., Субач І. Ю., Сілко О. В., Любарський С. В. Основи побудови операційних систем, комплексів та засобів автоматизації управління військами: Навчальний посібник. – К.: ВІТІ, 2016. – 220 с.
5. CommonVulnerability Enumeration // – Режим доступу: http://cve.mitre.org.

СИСТЕМНА МЕТОДОЛОГІЯ ПРОГНОЗУВАННЯ КІБЕРБЕЗПЕКИ

Нещерет І. Г. – провідний науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна.

Зінченко І. А. – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна.

Терещенко Т. П. – старший науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна.

ABSTRACT

In today's environment, there is a growing prospect and need to choose the most effective management decisions, which, in particular, should take into account and reflect the likely paths and behaviors of the object of management in the future.

KEY WORDS: management, information, forecasting, research.

АНОТАЦІЯ

У сучасних умовах зростає перспектива та необхідність у виборі найбільш ефективних управлінських рішень забезпечення кібербезпеки, які, зокрема, мають враховувати і відображати ймовірні шляхи та варіанти поведінки об'єкта управління в майбутньому.

КЛЮЧОВІ СЛОВА: управління, кібербезпека, кіберзахист, інформація, прогнозування, дослідження.

ВСТУП

Вибір рішення, визначення діагнозу стосовно об'єкта управління мають обґрунтовуватись на інформації, що вагомо випереджувала у часі існуючі процеси розвитку цього об'єкта. Використання прогнозної інформації, що дорівнює як мінімум тривалості реалізаційного циклу кіберзахисту, є однією з головних умов ефективного управління. Зрозуміло, що чим далі зазирнути в майбутнє, тим управління буде більш ефективним.

Величина мінімального випередження інформації є достатньою умовою ефективного управління лише при відсутності затримки в переробці інформації безпосередньо в керуючій підсистемі. Як нам відомо, такої ідеальної ситуації в практиці фактично не існує. Тому період випередження інформації повинен збільшуватися на час, що витрачається на перетворення даних в керуючій підсистемі.

Таке випередження інформації може бути досягнуте лише на основі наукового прогнозування, яке покликане істотно сприяти вирішенню таких завдань: обґрунтування альтернативних цілей розвитку, відшукання оптимальних шляхів, засобів та ресурсів для досягнення цілей, виявлення обмежуючих чинників розвитку об'єкта [1].

Метою дослідження є огляд найбільш ефективних принципів прийняття рішень управління.

1 АНАЛІЗ ЛІТЕРАТУРНИХ ДАНИХ ТА ПОСТАНОВКА ПРОБЛЕМИ

Аналіз літературних джерел стосовно системної методології прогнозувань показав, що прогнозування надає змогу вирішувати велику кількості специфічних завдань в процесі управління, зокрема:

1. визначення пріоритетів цілей, які можна буде вирішити впродовж періоду прогнозування;
2. виявлення об'єктивних тенденцій розвитку (еволюції) об'єкта управління;
3. визначення трудових, матеріальних, природних ресурсів для досягнення цілей управління в майбутньому;
4. виявлення виробничих та соціальних потреб (запиту) стосовно конкретного об'єкта управління [2].

2 РЕЗУЛЬТАТ ДОСЛІДЖЕННЯ

Метою традиційних прогнозів кібербезпеки є переважно окремі, часткові аспекти досліджуваного об'єкта. Методи їх розробки виправдовують себе, як правило, лише стосовно простих об'єктів, тому відбувається вимушене спрощення опису складних об'єктів до такого рівня, при якому достатньо ефективно працює конкретний метод прогнозування кібербезпеки. В міру ускладнення завдань, що вирішуються прогнозними дослідженнями, порівняльна ефективність окремих методів відходить на другий план стосовно цілей зведення цих методів у системи. В таких системах прогнозування кібербезпеки, що призначені для розробки прогнозів складних об'єктів, використовується певним чином взаємопов'язана та взаємоузгоджена сукупність методів, засобів і процедур. Система прогнозування кібербезпеки покликана виконати принаймні дві задачі: по-перше, виявити множину варіантів розвитку об'єкта управління; по-друге, порівняння і вибір альтернатив розвитку [3].

Об'єднання результатів вирішення даних завдань є синтезом системи прогнозування кібербезпеки, який вирішує комплексну (системну) проблему передбачення розвитку об'єкта управління. При цьому реалізуються такі системні принципи прогнозування:

1. взаємоузгодженість та підпорядкованість прогнозів різних рівнів структури об'єкта;
2. узгодженість наукових і нормативних прогнозів;
3. безперервність прогнозування, що вимагає коригування прогнозів.

Тобто система прогнозування кібербезпеки є по суті динамічною системою управління зі зворотніми зв'язками. Система прогнозування кібербезпеки, як і будь-яка інша, включає в себе підсистеми, які поділяються за принципом локалізації функцій. Вона містить шість підсистем: формування задач розвитку об'єкта; формування функцій, що забезпечують вирішення задач; обґрунтування засобів виконання заданих функцій; оцінка неоднорідності складових засобів; формування комплексних критеріїв вибору альтернатив; синтез сукупності альтернатив розвитку об'єкта. [4].

3 ВИСНОВКИ

Як висновок доцільно зауважити, що, по-перше, категорія "управління" невіддільна від категорії "система", бо тільки стосовно системно організованих об'єктів можливий процес управління; по-друге, і суб'єкт, і об'єкт управління є відносно автономними підсистемами, що функціонують за системними законами; по-третє, сам процес управління є системно організованою цілісністю взаємопов'язаних стадій.

Перспективи подальших досліджень у даному напрямку. Таким чином, можна стверджувати, що використання такого підходу до вибору управлінських рішень значно зможуть забезпечити комплексний розвиток технологій і технічних засобів у галузі кібербезпеки та кіберзахисту держави.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Роль прогнозування і планування в системі управління. URL: http://bukvar.su/menedzhment/112864-Rol-prognozirovaniya-i-planirovaniya-v-sisteme-upravleniya.html.
2. Аналіз управління внутрішнім середовищем підприємства готельного бізнесу. URL: https://www.webkursovik.ru/kartgotrab.asp?id=-58766.
3. Сутність конфлікту та його характерні риси. URL: https://www.afcea.org/content/?q=defense-department-awakens-internet-things.
4. Прогнозування соціально-економічних процесів. URL: http://lib.pnu.edu.ua:8080/bitstream/123456789/6572/1.

ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ ВІДСУТНОСТІ ВИХІДНИХ ДАНИХ ПРО ВИЗНАЧАЛЬНІ ВИПАДКОВІ ВЕЛИЧИНИ

Березовська Ю. – доктор філософії, доцент кафедри комп'ютерних наук Державного університету телекомунікацій, Навчально-наукового інституту інформаційних технологій, Київ, Україна.

Василенко В. – к.т.н., доцент кафедри комп'ютерних наук Державного університету телекомунікацій, Навчально-наукового інституту інформаційних технологій, Київ, Україна.

ABSTRACT

Government organizations, medium and small businesses (companies) use information systems that are in constant interaction with external influences. These impacts lead to the destruction of resources, disruption of staffing processes, and as a consequence, disruption of work functions. To prevent such situations, at the stage of design and experimental development of information systems there is a need to ensure the functional stability of information systems in the absence of initial data on the determinants of random variables. Such actions will reveal individual patterns and properties of information systems and improve the performance of both system components and information systems in general.

KEYWORDS: information system, network, functional stability, reliability, limited a priori information, determining random values, time reserve.

АНОТАЦІЯ

Державні організації, середній і малий бізнес (компанії) використовують для роботи інформаційні системи, які знаходяться в постійній взаємодії із зовнішніми впливами. Ці впливи призводять до руйнування ресурсів, порушення штатних процесів, і як наслідок, зриву виконання робочих функцій. Щоб запобігти таким ситуаціям, на стадії проектування й експериментального відпрацювання інформаційних систем постає необхідність у забезпеченні функціональної стійкості інформаційних систем в умовах відсутності вихідних даних про визначальні випадкові величини. Такі дії дозволять виявити окремі закономірності та властивості інформаційних систем і покращать роботу як компонентів систем, так і інформаційних систем в цілому.

КЛЮЧОВІ СЛОВА: інформаційна система, мережа, функціональна стійкість, надійність, обмежена апріорна інформація, визначальні випадкові величини, резерв часу.

На сьогоднішній день серйозної революції зазнає сектор телекомунікаційного зв'язку. Що, в свою чергу, виступає рушійною силою у формуванні способів проектування, розгортання та експлуатації інформаційних систем, мереж і послуг, які необхідні користувачу. Тому, дослідження, які стосуються функціонування великих інформаційних систем як в Україні, так і у інших країнах світу є актуальними та економічно ефективними.

Інформаційні системи постійно взаємодіють із зовнішніми впливами (конфліктами). Це обумовлює наявність в них механізмів, які мають забезпечувати нову якість – здатність збереження і/або відновлення своїх функцій (їхню стійкість) в умовах різного роду несприятливих впливів, а саме функціональної стійкості. Функціональна стійкість інформаційних систем являє собою інтегральну властивість, що включає надійність, живучість і безпеку. Відповідно, оцінка показників функціональної стійкості, необхідна для порівняння різних варіантів проектування.

На стадії проектування і конструювання інформаційних систем використовуються показники надійності, які трактують як характеристики імовірнісних математичних моделей створюваних об'єктів, а на стадії експериментального відпрацювання, випробувань і експлуатації показниками надійності є статистичні оцінки відповідних імовірнісних характеристик.

При оцінці показників надійності інформаційних систем часто відсутні необхідні вихідні дані для апріорних імовірнісних розрахунків, а статистична оцінка ускладнена невеликим обсягом випробувань, за якими можна визначити тільки оцінки моментів визначальних випадкових величин процесу функціонування інформаційних систем або її складових частин. У цій ситуації необхідно обґрунтовувати деякі характеристики інформаційних систем, наприклад, резерв часу, гарантовані точні границі ймовірності безвідмовної роботи системи та коефіцієнта готовності.

Отже, оцінки показників надійності необхідно використовувати при проектуванні функціонально стійких інформаційних систем враховуючи резерв часу різного цільового призначення при наявності обмеженої апріорної інформації.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Вишнівський В.В. Оцінка показників надійності інформаційних систем при обмеженій апріорній інформації / [В. В. Вишнівський, Ю. В. Каргаполов, Ю. В. Березовська та інші] // Sciences of Europe. – Praha, Czech Republic, 2021. – Vol. 1, No. 63. – PP. 8–14.
2. Березовська Ю.В. Забезпечення функціональної стійкості інформаційної
3. системи при обмеженій вихідній інформації про визначальні випадкові величини /

Ю. В. Березовська // Телекомунікаційні та інформаційні технології. – № 4(69). – К.: ДУТ, 2020. – С. 69–78.
4. Іщеряков С.М. Функціональна стійкість інформаційних мереж при наявності обмеженої апріорної інформації про надійність / С. М. Іщеряков, С. В. Прокопов, Ю. В. Каргаполов, Ю. В. Березовська // Зв'язок. – К.: ДУТ, 2020. – № 6(148). – С. 42–46.

НОВІ ТЕХНОЛОГІЇ, ЩО РОЗВИВАЮТЬСЯ ТА ФОРМУЮТЬ ІНДУСТРІЮ ОНЛАЙН-ІГОР

Vyshnivskyi V. – Doctor of Computer Science, Department of Computer Sciences, State University of Telecommunications, Kyiv, Ukraine.

Katkov Y. – Doctor of Computer Science, Department of Computer Sciences, State University of Telecommunications, Kyiv, Ukraine.

ABSTRACT

Technological trends in the development of new intelligent technologies used in the online gaming industry and moving forward are considered. Among such new intelligent technologies should be identified: virtual reality and augmented reality games (Virtual Reality and Augmented Reality Gaming); Artificial Intelligence Technologies; Blockchain Technology; wearable technology (Wearables Technology).

KEYWORDS: intelligent technologies, online gaming industry.

АНОТАЦІЯ

Розглядаються тенденції розвитку нових інтелектуальних технологій, що використовуються в індустрії онлайн-ігор та забезпечують рух уперед. Серед таких нових інтелектуальних технологій треба визначити: віртуальна реальність та ігри з доповненою реальністю (Virtual Reality and Augmented Reality Gaming); технології на основі штучного інтелекту (Artificial Intelligence Technologies); технологія блокчейн (Blockchain Technology); носімі технології (Wearables Technology).

КЛЮЧОВІ СЛОВА: інтелектуальні технології, індустрія онлайн-ігор.

Технологічні тренд розвитку нових інтелектуальних технологій, що використовуються в індустрії онлайн-ігор, рухають світ уперед, у світле майбутнє. За останні кілька років індустрія онлайн-ігор досягла великих успіхів тому, що вони швидко скорочують розрив із відеоіграми, надаючи геймерам незабутні враження.

В основі такого стрімкого розвитку онлайн-ігор нові інтелектуальні технології, що застосовуються для створення цих онлайн-ігор. Дійсно, нові ігрові функції або варіанти мобільних ігор розвиваються з запаморочливою швидкістю на основі цих нових інтелектуальних технологій. У наші дні мобільні ігрові програми досить популярні. Навіщо сидіти за комп'ютером або ноутбуком, якщо можна грати на телефоні або планшеті? Індустрія розвивається і через кілька років ми зможемо підключатися до казино за допомогою технологій та програм, що находяться в IoT (internet of things) пристроях.

Особливостями застосування останніх технологічних тенденцій є те, що їх застосовують на благо гравців. Наприклад, завдяки застосуванню нових інтелектуальних технологій в ігри тепер легше грати, ніж будь-коли, і вони більш мобільні, ніж будь-коли. Нові технології забезпечують кращий досвід, забезпечують динаміку, непередбаченість та можливість навчатися. Те, що раніше було надуманою фантазією, стало віртуальною реальністю. Тепер можна швидко перейти в мобільну версію гри та грати в ігри прямо з браузера, що раніше було неможливо. Це стосується не лише мобільних ігор.

Серед таких нових інтелектуальних технологій треба визначити:

- віртуальна реальність та ігри з доповненою реальністю (Virtual Reality and Augmented Reality Gaming);
- технології на основі штучного інтелекту (Artificial Intelligence Technologies);
- технологія блокчейн (Blockchain Technology);
- носімі технології (Wearables Technology);
- азартні ігри на мобільних пристроях (Gambling on mobile devices).

Віртуальна реальність та ігри з доповненою реальністю (Virtual Reality and Augmented Reality Gaming). Віртуальна реальність (VR) та доповнена реальність (AR) – це дві розробки, які можуть бути пов'язані з іграми. Сегменти віртуальної реальності були додані у відеоігри, які широко вважаються майбутніми технологічними тенденціями. Ігри віртуальної реальності вже доступні для покупки. Ця технологія все ще занадто дорога для того, щоб ці ігри набули широкого поширення, але віртуальна реальність дає те, чого не може жодна інша гра. Хоча для розвитку цієї технологічної тенденції можуть знадобитися роки, вона, безсумнівно, змінить ігрове середовище, яким ми його знаємо.

Технології штучного інтелекту (Artificial

Intelligence Technologies). Існує безліч технологій, пов'язаних із штучним інтелектом, які мають свої власні напрямки математичних та інженерних досліджень. Нині штучний інтелект зробив великий внесок у розвиток науки і техніки та як одна з найважливіших галузей. Штучний інтелект, технологія комп'ютерної гри грає активну роль розумному прийнятті рішень. Як результат власного складного правила руху та менший середній компонентний фактор у процесі його формування, комп'ютерна гра дуже допомагає розумним прийняття рішення, або допомагає до пошуку оптимального методу вчинення ходів.

Розглянемо найактуальніші технології штучного інтелекту для застосування в індустрії онлайн-ігор:

Автоматичне розпізнавання мови (Automatic speech recognition). Автоматичне розпізнавання мовлення стосується акустики, яка розпізнає фонеми в голосовому сигналі. Системи розпізнавання голосу обробляють сигнал, зібраний мікрофоном, для ідентифікації слів, сказаних користувачем.

Обробка природної мови (Natural language processing - NLP). У той час як розпізнавання мови зосереджено на чистому перетворенні голосу в текст, NLP обробки природної мови більш тісно пов'язана з областю лінгвістики, і її мета зрозуміти, що користувач має на увазі, коли робить певну команду, питання або затвердження. письмовий чи усний і чого він очікує досягти. Крім того, він аналізує настрій, щоб знайти суб'єктивні закономірності. Коротше кажучи, це поле, яке допомагає спілкуванню (в основному звуковому та письмовому) між машиною та людиною, створює візуальне та мовленнєве розпізнавання в штучному інтелекті.

Візуальне розпізнавання (Visual recognition) ґрунтується на обробці зображення або відеосигналу з метою розпізнавання образів, форм та, у кращому разі, точного визначення різних елементів зображення.

Розпізнавання тексту (Text recognition) можна розглядати як частину візуального розпізнавання, оскільки його основною метою є розпізнавання та ідентифікація тексту у форматах зображень. Для цієї роботи зазвичай використовуються інструменти OCR (Optical Character Recognition - оптичне розпізнавання символів).

Великі дані (Big Data). Не вдаючись у технічні подробиці Big Data можна розглядати як великий обсяг даних, що підлягають структуризації. Big Data має власні технології структурування для їх обробки. Big Data життєве важливо задля досягнення цілей як у аналізі бізнес-аналітики, так і у застосуванні певних алгоритмів машинного навчання.

Експертні системи (Expert systems) які містять усі можливі знання людини з певної теми. Класичним прикладом є системи, що грають у шахи, які використовують цілий набір ходів та стратегій, введених у їхню пам'ять, для визначення найкращого ходу (зазвичай на основі дерев рішень).

Робототехніка (Robotics). Робототехніка охоплює широкий спектр пристроїв. Щоразу, коли система або робот демонструють ознаки інтелекту, наприклад, здатність приймати рішення, якими б простими вони не були, можемо говорити про штучний інтелект. Треба розуміти, що штучний інтелект не обов'язково має бути особливо складним, він існує на всіх рівнях, навіть на самих базових, і його потрібно відрізняти від здатності вчитися у машин; тобто машинного навчання.

Машинне навчання (Machine Learning) в рамках штучного інтелекту намагається змусити систему вчитися і пов'язувати інформацію так, як це зробив би чоловік. І тому він використовує алгоритми, здатні виявляти закономірності у попередніх даних, здатні створювати прогнози у майбутнє, і навіть нові тенденції, такі як глибоке навчання та її алгоритми нейронної мережі. Для ігор доцільне використовувати різноманітні алгоритми машинного навчання, наприклад, глибоке навчання або когнітивний інтелект.

Глибоке навчання - це система навчання, яка заснована на функціонуванні нейронних мереж людського мозку для обробки інформації з дуже складною математичною основою, вона спирається на досвід (тобто попередні дані, що генеруються середовищем або самогенеруються), вона не починається зі строгих вказівок, що визначають - що правильно, а що ні), або

Когнітивний інтелект є комбінацією раніше згаданих технологій з метою створення сервісів штучного інтелекту, здатних розуміти людину, забезпечує об’єднання візуального розпізнавання, звуку, розуміння прочитаного, NLP та машинного навчання для створення систем, здатних розуміти інформацію, яка пов’язана з людською взаємодією, і відповідним чином реагувати.

Технологія блокчейн (Blockchain Technology). Це технологія про що ніколи раніше не замислювався гравець. Деякий час гравці могли грати на реальні гроші за допомогою банківських переказів або кредитних/дебетових карток, перш ніж цифрові електронні гаманці зрівняли правила гри. Вони були першим кроком у напрямку біткойн-геймінгу, який нині зростає. Гравці тепер можуть використовувати біткойни для онлайн-ставок завдяки технології блокчейн.

Носімі технології (Wearables Technology). Для усунення бар'єрів, що дозволяють використовувати технологічні пристрої, що носяться, меншого розміру і з більшою швидкістю відгуку, потрібен IP-пристрій (Arm IP) з низьким енергоспоживанням, який може забезпечити продуктивність в умовах обмежень за розміром і потужністю. Arm IP у поєднанні з інструментами розробки програмного забезпечення забезпечують безпечну і гнучку обробку даних в електроніки з найменшими розмірами кремнію. У наші дні мобільні ігрові програми досить популярні. Індустрія ігор розвивається по-різному, і через кілька років ми зможемо підключатися до серверів ігор за допомогою технологій та програм, що находяться в IoT (internet of things) пристроях. Оскільки розробники продовжують впроваджувати інновації, ми можемо очікувати появи нових при-

вабливих пристроїв, що носяться, які легко інтегруються в наше життя. Привнесення «невидимок» в простір пристроїв, що носяться, пов'язане з мініатюризацією технології і впровадженням її в предмети повсякденного побуту, такі як одяг і взуття. У той час як смарт-годинник та фітнес-трекер сьогодні є найбільш звичними пристроями, Arm IP пропонує новий набір форм-факторів за межами зап'ястя, які обіцяють змінити життя мільйонів людей.

Азартні ігри на мобільних пристроях (Gambling on mobile devices). Азартні ігри онлайн починаючи з 2000-х років набули популярності. Дійсно, можливість грати в рулетку, блекджек або ігрові автомати онлайн вразила гравців. Це дало ігровому світу нові можливості грати безкоштовно і практикуватися, а не відразу ризикувати реальними грошима. Це також дозволило геймерам грати, не виходячи з власного дому, а не їхати до найближчого казино. Згодом азартні ігри стали настільки популярними, що індустрія ігор почала шукати способи покращити його роботу за допомогою мобільних пристроїв. Мобільний гемблінг був наступним кроком в індустрії, і він з'явився швидко. Мобільні азартні ігри будуть на рекордно високому рівні 2022 року, що дозволить гравцям вперше робити ставки на ходу.

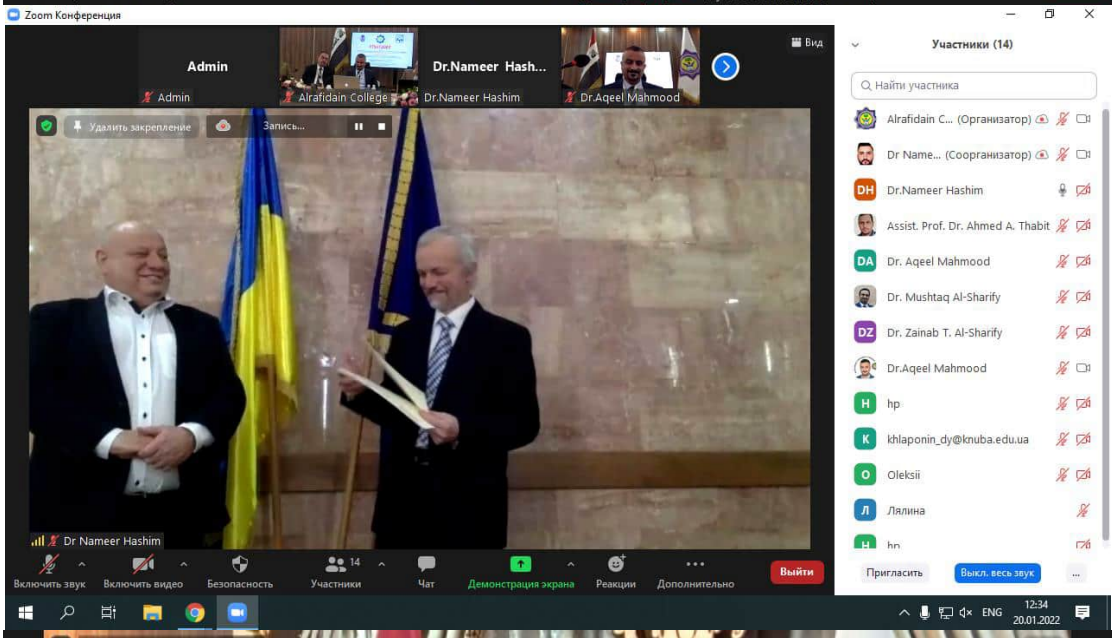
Таким чином, інтелектуальні технологічні тенденції рухають індустрію онлайн-ігор уперед, у світле майбутнє. Очікується, що технологічні досягнення змінять те, як ми граємо в онлайн-ігри, у міру того як ми рухаємося до кращого майбутнього. Це зовсім не негативна річ. Сектор онлайн-ігор швидко змінюється і технологічні досягнення, які він охоплює, покращують світ онлайн-ігор. Можна стверджувати, що онлайн-ігри стануть ще популярнішими у майбутньому, оскільки вони покладаються на нові технології, щоб забезпечити кращий досвід.

ВИКОРИСТАНА ЛІТЕРАТУРА

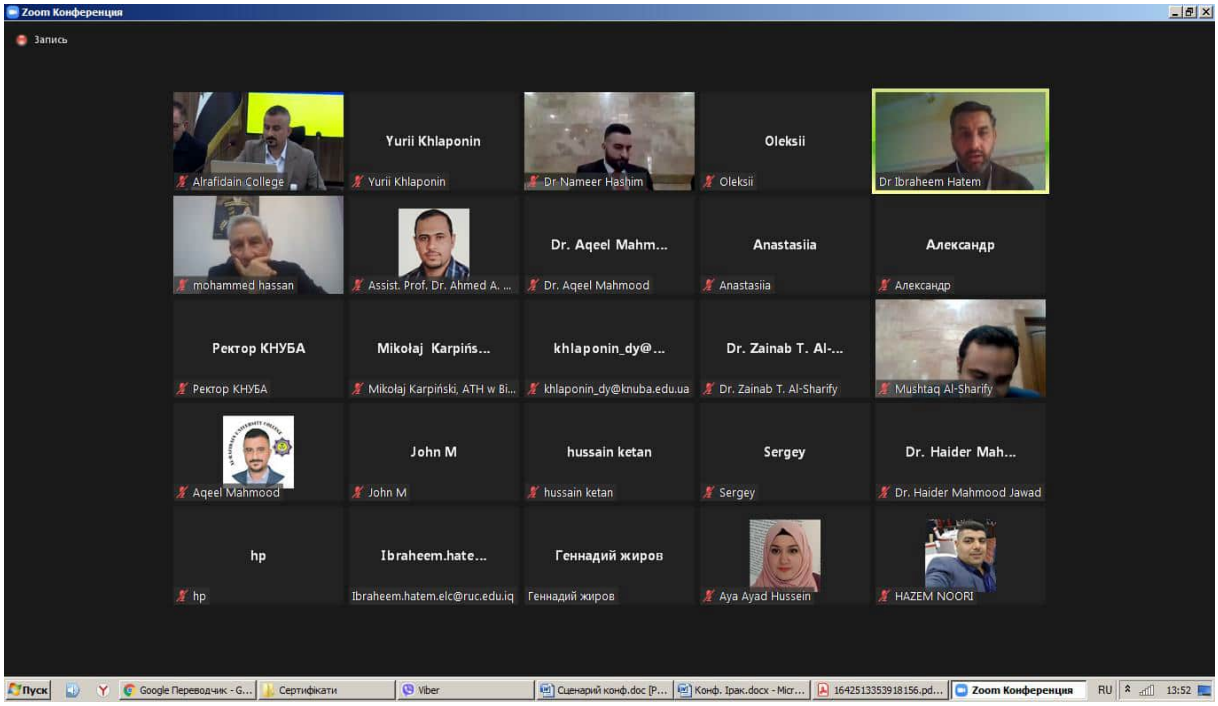
1. "What is Natural Language Processing? Intro to NLP in Machine Learning". GyanSetu!. 2020-12-06. Retrieved 2021-01-09.
2. Matthews, Emma (August 25, 2020). "Why Among Us is the best game to watch on Twitch right now". PC Gamer. Archived from the original on September 9, 2020. Retrieved September 8, 2020.
3. Antonovici, Anatol (March 23, 2021). "Bitcoin Mining Adds to Existing Shortage in Semiconductor Market, Chip Prices Surge". Yahoo News. Retrieved April 20, 2021.
4. Administration. "Centre for Language Technology (CLT)". Macquarie University. Retrieved 2021-01-11.
5. "Top Countries & Markets by Game Revenues". Newzoo. Archived from the original on December 16, 2021. Retrieved January 6, 2022.

ФОТО З КОНФЕРЕНЦІЇ


Запись...
Вид
Говорит:
Alrafidain College
Включить звук
Включить видео
Безопасность
Участники
Чат
Демонстрация экрана
Пауза/остановить запись
Реакции
Выйти


Zoom Конференция
Admin
Dr.Nameer Hash...
Dr.Aqeel Mahmood
Участники (14)
Найти участника
Dr Nameer Hashim
Включить звук
Включить видео
Безопасность
Участники
Чат
Демонстрация экрана
Реакции
Дополнительно
Выйти
Пригласить
Выкл. весь звук
ENG
12:34
20.01.2022


Запись...
Вид
Говорит:
Alrafidain College
Включить звук
Включить видео
Безопасность
Участники
Чат
Демонстрация экрана
Пауза/остановить запись
Реакции
Выйти


Zoom Конференция
Запись
Alrafidain College
Yurii Khlaponin
Yurii Khlaponin
Dr Nameer Hashim
Oleksii
Oleksii
Dr Ibraheem Hatem
mohammed hassan
Assist. Prof. Dr. Ahmed A. ...
Dr. Aqeel Mahm...
Dr. Aqeel Mahmood
Anastasiia
Anastasiia
Александр
Александр
Ректор КНУБА
Ректор КНУБА
Mikołaj Karpiń...
Mikołaj Karpiński, ATH w Bi...
khlaponin_dy@...
khlaponin_dy@knuba.edu.ua
Dr. Zainab T. Al-...
Dr. Zainab T. Al-Sharify
Mushtaq Al-Sharify
Aqeel Mahmood
John M
John M
hussain ketan
hussain ketan
Sergey
Sergey
Dr. Haider Mah...
Dr. Haider Mahmood Jawad
hp
hp
Ibraheem.hate...
Ibraheem.hatem.elc@ruc.edu.iq
Геннадий жиров
Геннадий жиров
Aya Ayad Hussein
HAZEM NOORI
Пуск
Google Переводчик - G...
Сертифікати
Viber
Сценарий конф.doc [P...
Конф. Ірак.docx - Micr...
1642513353918156.pd...
Zoom Конференция
RU
13:52

Наукове видання

І міжнародна науково-практична конференція “Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей”

ТЕЗИ ДОПОВІДЕЙ УЧАСНИКІВ

І МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ “НОВІТНІ ТЕХНОЛОГІЧНІ ТЕНДЕНЦІЇ ІНТЕЛЕКТУАЛЬНОЇ ІНДУСТРІЇ ТА ІНТЕРНЕТУ РЕЧЕЙ”

19-20 СІЧНЯ 2022 РОКУ

Підписано до друку 18.01.2022. Формат 60x90/16
Ум. друк. арк. 3,25. Обл. вид. 0,9

Видавець і виготовлювач
Київський національний університет будівництва і архітектури
Повітрофлотський проспект, 31. Київ, Україна, 0380