Інститут систем управління
МНО Азербайджанської республіки

Національний технічний університет
"Харківський політехнічний інститут"

Харківський національний
університет радіоелектроніки

Національний аерокосмічний університет
імені М. Є. Жуковського
"Харківський авіаційний інститут"

Університет технології і гуманітарних наук
(м. Бельсько-Бяла, Польща)

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

Тези доповідей дванадцятої міжнародної
науково-технічної конференції

21 – 22 листопада 2024 року

Том 1: секції 1, 2, 3

Баку – Харків – Бельсько-Бяла –2024

УДК 004 : 681.3 doi: https://doi.org/10.32620/PI.24.t1

У збірнику подано тези доповідей дванадцятої міжнародної науково-технічної конференції “Проблеми інформатизації”. Розглянуті питання за такими напрямами: інформатизація навчального процесу; застосування, експлуатація та безпека функціонування телекомунікаційних систем та мереж; комп’ютерні методи і засоби інформаційних технологій та управління; методи швидкої та достовірної обробки даних в комп’ютерних системах та мережах; цивільна безпека та захист критичної інфраструктури(інформаційна підтримка); сучасні інформаційно-вимірювальні системи.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Співголови оргкомітету:

ГАШИМОВ Ельшан Гіяс огли (*д.н.б. & в.н., проф., ІСУ АР, Баку, Азербайджан*);
КАРПІНСЬКІ Міколай (*д.н., проф., Університет Бельсько-Бяла, Польща*);
КОВАЛЕНКО Андрій Анатолійович (*д.т.н., проф., ХНУРЕ, Харків, Україна*);
КУЧУК Георгій Анатолійович (*д.т.н., проф., НТУ «ХПІ», Харків, Україна*);
ФЕДОРОВИЧ Олег Євгенович (*д.т.н., проф., НАУ «ХАІ», Харків, Україна*).

Члени оргкомітету:

ГЛАВЧЕВ Максим Ігорович (*к.е.н., доц., НТУ «ХПІ», Харків, Україна*);
ГЛИВА Валентин Анатолійович (*д.т.н., проф., КНУБА, Київ, Україна*);
ДОРОНІН Євген Володимирович (*к.т.н., доц., НАУ, Київ, Україна*);
ЗАЙЦЕВА Єлєна (*к.т.н., проф., Університет міста Жиліна, Жиліна, Словаччина*);
ЗАПОЛОВСЬКИЙ Микола Йосипович (*к.т.н., проф., НТУ «ХПІ», Харків, Україна*);
КАЛІНІН Євгеній Іванович (*д.т.н., проф., НУ БрПкУ, Київ, Україна*);
КОЛОМІЙЦЕВ Олексій Володимирович (*д.т.н., проф., НТУ «ХПІ», Харків, Україна*);
КОСЕНКО Віктор Васильович (*д.т.н., проф., ДП "ПД ПКНДІ АП", Харків*);
КРАСНОБАЄВ Віктор Анатолійович (*д.т.н., проф., ХНУ, Харків, Україна*);
ЛЕВАШЕНКО Віталій (*к.т.н., проф., Університет міста Жиліна, Жиліна, Словаччина*);
ЛЕВЧЕНКО Лариса Олексіївна (*д.т.н., доц., НТУУ «КПІ», Київ, Україна*);
ЛЕЩЕНКО Олександр Борисович (*к.т.н., доц., НАУ «ХАІ», Харків, Україна*);
МІХАЛЬ Олег Пилипович (*д.т.н,, доц., ХНУРЕ, Харків, Україна*);
МОЖАЄВ Олександр Олександрович (*д.т.н., проф., ХНУ ВС, Харків, Україна*);
ПОДОРОЖНЯК Андрій Олексійович (*к.т.н., доц., НТУ «ХПІ», Харків, Україна*);
РУБАН Ігор Вікторович (*д.т.н., проф., ХНУРЕ, Харків, Україна*);
РУДНИЦЬКИЙ Володимир Миколайович (*д.т.н., проф., ДНДІ ОВТ, Черкаси, Україна*);
СЄВЄРІНОВ Олександр Васильович (*к.т.н., доц., ХНУРЕ, Харків, Україна*);
СЕМЕНОВ Сергій Геннадійович (*д.т.н., проф., ПУ, Краків, Польща*);
СМІРНОВ Олександр Анатолійович (*д.т.н., проф., ЦНТУ, Кропивницький, Україна);*
ТРЕТЬЯКОВ Олег Вальтерович (*д.т.н,, проф., НАУ, Київ, Україна*);
ТРИСТАН Андрій Вікторович (*д.т.н., проф., ДНДІ ОВТ, Черкаси, Україна*);
ШЕФЕР Олександр Віталійович (*д.т.н., проф., ПНТУ, Полтава, Україна*).

Секретаріат оргкомітету:

КУЧУК Ніна Георгіївна (*д.т.н., проф., НТУ «ХПІ», Харків, Україна*);
ЛЯШЕНКО Олексій Сергійович (*к.т.н,, доц., ХНУРЕ, Харків, Україна*).

Institute of Control Systems
of the Ministry of Science and Education
of the Republic of Azerbaijan

National Technical University
Kharkiv Polytechnic Institute

Kharkiv National University
of Radio Electronics

National Aerospace University
Kharkiv Aviation Institute

University of Bielsko-Biala

PROBLEMS OF INFORMATIZATION

Proceedings of 12-th International
Scientific and Technical Conference

November 21 – 22, 2024

VOLUME 1: SECTIONS 1, 2, 3

Baku – Kharkiv – Bielsko-Biala –2024

UDC 004 : 681.3 doi: https://doi.org/10.32620/PI.24.t1

The collection presents abstracts of reports of the twelfth international scientific and technical conference "Problems of Informatization". Issues in the following areas are considered: informatization of the educational process; application, operation and safety of telecommunication systems and networks; computer methods and means of information technology and management; methods of fast and reliable data processing in computer systems and networks; civil security (information support); modern information and measurement systems.

ORGANIZING COMMITTEE

Дванадцята міжнародна науково-технічна конференція "Проблеми інформатизації" проводиться 21 та 22 листопада 2024 року в режимі ONLINE.

Тези доповідей доступні в INTERNET.

ТОМ 1

СЕКЦІЯ 1. Інформатизація навчального процесу.

Керівниця секції: д.т.н. проф. Н. Г. Кучук, НТУ «ХПІ», Харків.
Секретарка секції: к.т.н. О. М. Бельорін-Еррера, НТУ «ХПІ», Харків.

СЕКЦІЯ 2. Застосування та експлуатація телекомунікаційних систем та мереж.

Керівник секції: д.т.н. проф. Г. А. Кучук, НТУ «ХПІ», Харків.
Секретар секції: к.т.н. доц. С. С. Бульба, НТУ «ХПІ», Харків.

СЕКЦІЯ 3. Безпека функціонування телекомунікаційних систем та мереж.

Керівник секції: д.т.н. проф. О. О. Можаєв, ХНУВС, Харків.
Секретар секції: к.т.н. доц. О. В. Сєвєрінов, ХНУРЕ, Харків.

ТОМ 2

СЕКЦІЯ 4. Комп'ютерні методи і засоби інформаційних технологій та управління.

Керівники секції: д.т.н. проф. І. В. Рубан, ХНУРЕ, Харків.
д.т.н. проф. А. А. Коваленко, ХНУРЕ, Харків.
Секретар секції: к.т.н. доц. О. С. Ляшенко, ХНУРЕ, Харків.

ТОМ 3

СЕКЦІЯ 5. Методи швидкої та достовірної обробки даних в комп'ютерних системах та мережах.

Керівник секції: д.т.н. проф. В. А. Краснобаєв, ХНУ, Харків.
Секретар секції: к.т.н. Д. О. Лисиця, НТУ «ХПІ», Харків.

СЕКЦІЯ 6. Цивільна безпека та захист критичної інфраструктури.

Керівник секції: д.т.н. проф. О. В. Третьяков, ДУ «КАІ», Київ.
Секретар секції: к.т.н. доц. Є. В. Доронін, ДУ «КАІ», Київ.

СЕКЦІЯ 7. Сучасні інформаційно-вимірювальні системи.

Керівник секції: д.т.н. проф. О. В. Коломійцев, НТУ «ХПІ», Харків.
Секретар секції: к.т.н. доц. А. О. Подорожняк, НТУ «ХПІ», Харків.

СЕКЦІЯ 1
ІНФОРМАТИЗАЦІЯ НАВЧАЛЬНОГО ПРОЦЕСУ

Керівниця секції: д.т.н. проф. Н. Г. Кучук, НТУ «ХПІ», Харків
Секретарка секції: к.т.н. О. М. Бельорін-Еррера, НТУ «ХПІ», Харків

CRITICAL REVIEW OF EMERGING TRENDS IN AI INTEGRATION WITHIN HIGHER EDUCATION RESEARCH

Yadigarova L.A.
Institute of Education of the Republic of Azerbaijan,
Baku Slavic University, Baku, Azerbaijan

The integration of Artificial Intelligence (AI) into higher education has gained significant importance, particularly over the last five years. This technological advancement has been transforming various aspects of higher education, including teaching, learning, research, and administration [1–7].

AI's capacity to automate daily tasks, personalize learning experiences, and analyse huge datasets has the potential to revolutionize institutional effectiveness and efficiency.

The transformative potential of AI in higher education is increasingly viewed as inevitable. Higher Education Institutions (HEIs) around the world are now faced with the imperative of embracing the opportunities presented by AI, such as enhanced student engagement, effective resource management, and improved decision-making processes, while also critically assessing the challenges it poses.

Previous studies demonstrate that the integration of AI technology in educational settings has a substantial positive impact on student engagement and academic achievement [5].

Some studies conducted in this sphere show a high interest among teachers in the opportunities offered by AI to improve the quality of teaching and learning in the university classroom. They expect AI to facilitate various educational aspects, from lesson planning to the creation of materials and activities to promote creativity and interactive learning [1].

There is also evidence regarding the use of AI-powered solutions in several functions in education such as admissions, enrolment management, and student support services by providing personalized learning platforms and adaptive tutoring systems [3].

The transformative and disruptive impact of AI is most evidently demonstrated in its capacity to foster interdisciplinary research. AI's ability to quickly and efficiently analyse datasets from diverse academic fields allows researchers to collaborate with other researchers and make connections they might not have otherwise considered, creating opportunities to novel interdisciplinary projects and cooperations [2]. Particularly in this stage of the world development where interdisciplinary research outcomes are expected and required to contribute to social

impact, the use of AI for promoting and conducting interdisciplinary research has critical implications.

Along with the opportunities there also some challenges and risks have been mentioned. These challenges include ethical concerns, data privacy issues, the risk of bias in AI algorithms, and the potential for widening inequalities if access to AI technologies is not equitably distributed [4]. To mitigate these risks, higher education institutions must adopt a proactive approach, which involves not only integrating AI into their central functions but also creating an environment for ethical use of AI.

This requires continuous research into the implications of AI, comprehensive policy frameworks, and a commitment to developing the digital literacy of both faculty and students [3]. By considering these aspects, HEIs can ensure that AI fosters educational outcomes while safeguarding against its potential negative effects.

To conclude, it should be noted that the integration of AI into higher education offers vast potential to enhance academic and administrative processes, facilitate innovation, effectiveness and efficiency across HEIs. However, to fully harness these benefits, higher education institutions must proactively consider ethical concerns and ensure equitable access to AI technologies, fostering a balanced and inclusive approach to AI integration.

References

1. Ateeq, A., Alaghbari, M. A., Alzoraiki, M., Milhem, M., & Hasan Beshr, B. A. (2024). Empowering Academic Success: Integrating AI Tools in University Teaching for Enhanced Assignment and Thesis Guidance. *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems, ICETSIS 2024*, 297–301. https://doi.org/10.1109/ICETSIS61505.2024.10459686

2. Butson, R., & Spronken-Smith, R. (2024). AI and its implications for research in higher education: a critical dialogue. *Higher Education Research and Development*, *43*(3), 563–577. https://doi.org/10.1080/07294360.2023.2280200

3. Murdan, A. P., & Halkhoree, R. (2024). Integration of Artificial Intelligence for educational excellence and innovation in higher education institutions. *1st International Conference on Smart Energy Systems and Artificial Intelligence, SESAI 2024*. https://doi.org/10.1109/SESAI61023.2024.10599402

4. Samman, A. M. A. (2024). Harnessing Potential: Meta-Analysis of AI Integration in Higher Education. *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems, ICETSIS 2024*, 1656–1662. https://doi.org/10.1109/ICETSIS61505.2024.10459420

5. 5.Vrana, R. (2024). Exploring the Impact of AI on Teaching in Higher Education: an Exploratory Study. *2024 47th ICT and Electronics Convention, MIPRO 2024 - Proceedings*, 391–397. https://doi.org/10.1109/MIPRO60963.2024.10569342

6. Agayev, S.O., Talibov, A.M. and Hashimov, E.G. (2016). Modern pedagogical technologies in military education. Textbook. Part I.// - Baku: Military Publishing House. 2016. 152 p.

7. Piriyev H. K. et al. Some issues of pedagogical staff training for special-purpose higher education institutions //Military knowledge. – 2014. – №. 4. – p. 3-9.

USING AUTHENTIC MATERIAL FROM THE REAL WORLD TO TEACH ENGLISH

Aghayeva Ja.
Military Institute named after Heydar Aliyev

Research has shown that incorporating blogs in language learning can lead to increased cultural interaction and engagement. Travel blogs, specifically, offer a unique platform for learners to explore diverse linguistic styles, rhetorical strategies, and cultural nuances present in authentic travel narratives. Through exposure to these materials, students can develop a heightened sensitivity to language use, rhetorical devices, and cultural references, thereby improving their overall rhetorical awareness. In essence, the integration of authentic materials from travel blogs in language learning environments provides a rich and dynamic resource for enhancing students' rhetorical awareness by bridging the gap between language learning and real-world communication contexts.

Using travel blogs in language learning offers several benefits, including:

Cultural Immersion: Travel blogs provide learners with authentic, real-life language contexts that immerse them in the culture and language of the destination. This helps learners develop a deeper understanding of the culture and language, enhancing their overall language proficiency.

Authentic Language Use: Travel blogs offer learners exposure to authentic language use, including idioms, colloquialisms, and rhetorical devices. This helps learners develop a more nuanced understanding of language and its various forms.

Practical Language Skills: Travel blogs provide learners with practical language skills, such as reading comprehension, vocabulary acquisition, and writing skills. These skills are essential for effective communication in real-life situations.

Enhanced Cultural Awareness: Travel blogs help learners develop cultural awareness by exposing them to local customs, traditions, and values. This enhances their understanding of the culture and language, making them more effective communicators.

Increased Motivation: Travel blogs can be highly engaging and motivating for learners, as they provide a tangible connection to the language and culture. This can lead to increased learner motivation and a more enjoyable learning experience.

Improved Language Fluency: By using travel blogs, learners can improve their language fluency by practicing reading comprehension, vocabulary acquisition, and writing skills. This helps learners develop a more natural and spontaneous language use.

Reflective Learning: Travel blogs encourage learners to reflect on their language learning journey, documenting their progress, new vocabulary, and cultural experiences. This reflective practice helps learners identify areas for improvement and track their progress over time.

Access to Real-Life Language Contexts: Travel blogs provide learners with real-life language contexts that are relevant to their interests and goals. This helps learners develop a more practical and functional language proficiency.

Enhanced Intercultural Competence: Travel blogs help learners develop intercultural competence by exposing them to different cultural perspectives and values. This enhances their ability to communicate effectively across cultural boundaries.

Increased Autonomy: Travel blogs empower learners to take control of their language learning by providing them with a platform to practice and reflect on their language skills. This autonomy fosters a sense of ownership and responsibility in the learning process.

By incorporating travel blogs into language learning, learners can develop a more comprehensive understanding of the language and culture, leading to improved language proficiency and enhanced intercultural competence.

References

1. Ellis, R. (2003). Task-based language learning and teaching. Oxford: Oxford University Press.
2. Grellet, F. (1981). Developing reading skills. Cambridge: Cambridge University Press.
3. Krashen, S. D. (1985). The Input Hypothesis: Issues and implications. New York, NY: Longman.
4. Montero, M. (n.d.). Integrating Authentic Texts into Your Curriculum. Teaching with a Mountain View.
5. Agayev, S.O., Talibov, A.M. and Hashimov, E.G. (2016). Modern pedagogical technologies in military education. Textbook. Part I.// - Baku: Military Publishing House. 2016. 152 p.
6. Piriyev H. K. et al. Some issues of pedagogical staff training for special-purpose higher education institutions //Military knowledge. – 2014. – №. 4. – p. 3-9.
7. Mammadova M.F. (2021) " Linguo didactic aspects of English learning in High Military Institutions monography" p.400

DEVELOPMENT OF INFORMATION TECHNOLOGY IN TEACHING A FOREIGN LANGUAGE

Akbarova S.S.
Military Institute named after Heydar Aliyev, Baku

The development of Information Technology (IT) in teaching is one of the main components of the modern education system. These technologies are aimed at increasing the efficiency of the learning and educational process, ensuring the active participation of learners and making the learning environment more interactive. IT also provide ample opportunities for teachers to change and improve teaching methods.

IT adaption process and innovation in education. IT allow innovative approaches to improve the quality of education. They make learning in the classroom fun and interactive. In the use of digital resources, online educational platforms, e-books, videos and interactive games are the resources that learners use in the learning

process. Application of IT in teaching and online educational platform. Platforms such as Coursera, edx, Moodle offer a wide variety of curricula, seminars and courses worldwide. Learners have the opportunity to learn at their own pace and gain new knowledge.

Presentation tools. Tools such as PowerPoint, Prize and Google Slides increase the active participation of trainees through interactive discussions carried out during presentations.

Simulation and model creation. Virtual laboratories and simulation programs allow learners to revive situations and gain practical experience.

Changing the role of teachers. Mentor and professional development. Modern teachers should be mentors who not only provide knowledge, but also direct discussions and encourage learners to seek the right information. Regular instructional programs are needed for teachers to master and implement new technologies. Learners active participation and individual learning opportunities. Information technology allows learners to choose their own learning methods and solve issues individually.

Group projects through interactive platforms allow learners to collaborate and learn together.

Digital libraries and resources. Digital libraries and educational resources offer language learners a vast database of information.

These resources allow students to read, listen to, and watch materials on various topics. Utilizing e-books, audio materials, and videous makes language learning more diverse and enriching.

Video conferencing and online lessons. Video conferencing technologies and online lessons enable students to communicate with teachers and other students from different parts of the world.

This provides an opportunity to apply language skills in real time and to develop communication skills with people from different cultures.

Online test and assessment. Interactive test and assessment tools offer extensive opportunities for students to regularly check and improve their language skills. Online tests and quizzes are useful for identifying students weaknesses and helping them to improve.

References

1. Marcinek A. (2014). Technology and Teaching: Finding a Balance. Retrieved from http://www.edutopia.org/blog/technology-and-teaching-finding-balance-andrew-marcinek

2. Agayev, S.O., Talibov, A.M. and Hashimov, E.G. (2016). Modern pedagogical technologies in military education. Textbook. Part I.// - Baku: Military Publishing House. 2016. 152 p.

3. Piriyev H. K. et al. Some issues of pedagogical staff training for special-purpose higher education institutions //Military knowledge. – 2014. – №. 4. – p. 3-9.

4. Pritchard A. (2007). Effective teaching with internet technologies. London, UK: Paul Chapman Publishing.

AN ALGORITHM FOR AUTOMATICALLY GENERATING LEARNING PATHS USING CONCEPT MAPS IN COMPUTER SCIENCE EDUCATION

Aliyeva A.E.
Institute of Control Systems, Baku, Azerbaijan

In computer science education, creating tailored learning paths for students is essential for optimizing learning efficiency and improving knowledge retention. An automatic learning path generation algorithm based on concept maps, will design to personalize educational experiences in computer science courses [1-4].

The algorithm dynamically generates concept-based learning sequences by analyzing inter-concept dependencies, student knowledge levels, and pedagogical goals.

The proposed method enables a more interactive and adaptive learning experience, facilitating mastery of complex topics in a logical, sequential manner. The effectiveness of the algorithm is demonstrated through case studies on computer science curricula, showing how it enhances student learning out-comes.

The aim of the article given the complex nature of computer science education, with topics ranging from introductory programming to advanced algorithms, a personalized learning path is crucial for efficient learning. However, manually constructing learning paths for each student is labor-intensive and infeasible in large-scale educational environments.

The need for an automated system that can adaptively guide students through a computer science curriculum, taking into account their prior knowledge, understanding of concepts, and learning goals, motivates the development of this concept map-based algorithm [5].

References

1. Cañas, Alberto J., and Joseph D. Novak. The theory underlying concept maps and how to construct them. Florida Institute for Human and Machine Cognition. 2006. Vol. 1, No. 1, p. 1-31.

2. Bai, S. M. and Chen, S. M. “Evaluating students’ learning achievement using fuzzy membership functions and fuzzy rules,” Expert Systems with Applications, 2008. Vol. 34, No. 1, pp. 339-410.

3. Chen, S.M., Sue, P.J. A new method to construct concept maps for adaptive learning systems. In: Proceedings of the Ninth International Conference on Machine Learning and Cybernetics, Qingdao. 2010. pp.2489—2494.

4. Agayev S. O., Talibov A. M., Hashimov E. G. Modern pedagogical technologies in military education. Textbook. Part I //Baku: Military Publishing House. – 2016.

5. Piriyev H. K. et al. Some issues of pedagogical staff training for special-purpose higher education institutions //Military knowledge. – 2014. –№. 4. –p. 3-9.

6. Automatically constructing grade membership functions of fuzzy rules for students’ evaluation Expert Systems with Applications, 2008. Vol. 35, No 3, pp. 1408-1414.

SOCIO-CULTURAL IMPORTANCE OF THE QUALITY OF EDUCATION

Aliyeva V.E.
Military Institute named after H.Aliyev, Baku, Azerbaijan

Modernization of education is an objective process that determines its reform, the formation of new meanings and values, approaches to the content of education and teaching methods, monitoring and evaluation of the results of educational activities. The modernization program for the development of the country is based on the principle of the development of the education system, and therefore education should be capable of everything that supports the trends of modern, advanced, objective social development. The establishment of the state education policy of the XXI century, in this case, is based on the motto "accessibility - quality - efficiency". It is an integrated system that synthesizes all stages of education and is the basis of a social indicator of the quality of education.

In the socio-cultural approach, society, cultural phenomenon, education and personality act as socio-cultural systems interacting with each other. Culture determines not only the external environment of education, but also the "inner world", its structure. It is no coincidence that researchers have recently used the concept of "cultural-educational space", thereby considering education as a spiritual-cultural process. The quality of education is the assessment of the integrity of the educational content, learning technologies, monitoring methods and self-determination of the subject's life in terms of individual development and the demands of society in new socio-economic conditions. From this point of view, the quality of education is considered as a concept, it reflects the ability to ensure the achievement of the goals set for the education system, to meet the needs of a certain person for education, and to meet the needs of society and the economy. The exceptional importance of ensuring the quality of education is determined today by the following objective reasons:

First, scientific and technological progress is accelerating, and the level and extent of education is increasingly dependent on the development of society. In such conditions, higher education is widespread and it is required to create conditions for the development of creative abilities of those entering higher education institutions, and vocational education is delivered to the general population.

Secondly, it is necessary for the society to gradually move from the industrial stage of the economy to the information economy and the stage of formation of information civilization. This process is mainly associated with the increasing economic and social role of universities and their graduates.

Thirdly, with the development of the world information civilization, the globalization process is developing rapidly, part of which is the collection of scientific data in accordance with the Bologna process, the harmonization of the work quality level of the education systems of different countries, the conformity of young people to certain universal criteria and standards, especially graduates and students. related to the provision of an international education that requires

international mobility, their employment and the recognition of educational certificates. Fourthly, taking into account the rapid development of Azerbaijan in the field of education, the question of its material and technical base taking its place among the technologically, economically and culturally developed countries of the world is sharply reflected. Today, the reform process of the educational system is actively developing, accompanied by the widespread use of effective mechanisms for the implementation of educational goals and the application of scientific methods for evaluating educational achievements.

The next important task to ensure the quality of education is related to the development and change of teachers of various educational technologies. The quality of education depends on how and what technologies the teacher depends on, how he can change his methodical tools according to the characteristics of the students. Humanity, indeed, has become a historical new place when the person himself, his educational and professional skills, moral characteristics became the main source of development. The vital activity of mankind is focused on very complex objects and is characterized by high technology.

References

1. Agayev, S.O., Talibov, A.M. and Hashimov, E.G. (2016). Modern pedagogical technologies in military education. Textbook. Part I.// - Baku: Military Publishing House. 2016. 152 p.
2. Piriyev H. K. et al. Some issues of pedagogical staff training for special-purpose higher education institutions //Military knowledge. – 2014. – №. 4. – p. 3-9.
3. Piriyev H.K. et al. Provide interactive training methods. Methodological materials // - Baku: Military publishing house, 2016, 33 p.
4. Piriyev H.K. et al. Training methods in military education. Methodological materials // - Baku: Military publishing house, 2017, 52 p
5. Nazarov M.H., Babayeva A.R. General foundations of culture and education. Teaching materials / Baku-Mutercim - 2016, 200 p.
6. Nazarov M.H. Sociocultural problems of education in modern times. Monograph. - Baku: Mutercim, 2018. - 296 p.
7. Mammadzade R. Quality in education as one of the leading directions. Baku: "Teacher", 2010. - 170 p.

MECHANİSMS OF APPLİCATİON OF MODERN TRENDS İN THE EDUCATİONAL PROCESS

Shamshiyeva N.S.
Military Institute named after Heydar Aliyev, Azerbaijan

Education is a strategic field for every country and one of the main elements of its socio-cultural strength. In modern times, the deepening of the globalization process and the constant strengthening of the competition between countries in the socio-economic field make continuous improvement of the quality of education, which is the main driving force of state development, a priority issue.

In this regard, large-scale reforms are currently being carried out in all countries of the world, which significantly affect the improvement of the quality of education.

The application of international experience in training is determined by its modernity and efficiency. It aims to adapt education in the local environment to the new pragmatic values in terms of form and content. STEM - science, technology, engineering, math, which is one of the most widely applied international practice models in modern education systems, IB - International Baccalaureate, Digital learning, Distance learning: Microsoft Outlook; Zoom); e-Twinning – pairing model, etc. are more successful examples.

The study of the current experiences of foreign countries in the field of training, the integration of creative tendencies with our national-spiritual characteristics, is aimed at ensuring the transition from traditional methods to new values in our education. Studying education based on experiences that create new knowledge mainly has the following goals:

- To use the opportunities of the global network to form communication skills;
- International experience - to strengthen competitiveness;
- Bringing foreign work experience to life experience and achieving it;
- To participate in international projects based on quality in education;
- Designing the content of the educational program according to international practice examples.

At present, the application of modern trends in general and professional education in Azerbaijan and the requirements for it are constantly changing as the society develops in terms of its multispectral interests, it exudes new shades of meaning and is aimed at the full realization of national interests.

It is very gratifying that today's socio-political changes in our society, economic progress, cultural outlook formation factors, activities aimed at protecting national and moral values, and civic responsibility are widely reflected in the new content of the educational process. In the future, the development of education in this direction will contribute to raising the reputation of our country in the international world.

References

1. Veysova Z, (2007) Active (interactive training). Resources for teachers, UNICEF.
2. Brighton, K. (2007) Coming of age: The education and development of young adolescents. Westerville, OH: National Middle School Association.
3.Agayev S.O. et al. (2016). Modern pedagogical technologies in military education. Textbook. Part I.// - Baku: Military Publishing House. 2016. 152 p.
4.Piriyev H. K. et al. Some issues of pedagogical staff training for special-purpose higher education institutions //Military knowledge. – 2014. – №. 4. – p. 3-9.
5. Dr. Ismail Al- Rawi, Arab Open University, “Teaching Methodology and its Effects on Quality Learning”, Journal of Education and Practice www.iiste.org ISSN 2222-1735 (Paper) ISSN 2222-288X (Online) Vol.4, No.6, 2013

POSSIBILITIES OF APPLYING INFORMATION TECHNOLOGIES IN THE FORMATION OF THE DIDACTIC DESIGN MODEL OF MILITARY ENGINEER TRAINING

Dadashov A.S.
Educational Institute of the Republic of Azerbaijan
Military Institute named after H.Aliev, Baku, Azerbaijan

The effect of the rapid development of engineering in the context of the information technology era, the integration of information technologies (IT) into the didactic process of military engineer training - training programs is not only useful, but also an important and urgent issue.

The didactic design model aimed at the systematic planning and implementation of military educational processes can be significantly improved by the application of IT.

This thesis explores the various possibilities and benefits of incorporating IT into a didactic design model for military engineer training. These include: improving learning experiences; personalized learning paths; collaborative learning platforms; and effective resource management: refers to.

One of the main advantages of using IT in military engineer training is the enhancement of learning experiences. Virtual Reality (VR) and Augmented Reality (AR), which are among the benefits of modern technology for education, can simulate real-world scenarios and provide students with immersive and interactive environments.

These technologies enable the creation and replication of all possible scenarios of complex engineering tasks and battlefield conditions, allowing trainees to practice and develop their skills in a safe and controlled environment [1]. IT facilitates the creation of personalized learning paths tailored to the individual needs and progress of each learner.

Adaptive learning systems use data analytics to monitor performance and adjust training content accordingly. This ensures that trainees receive the appropriate level of challenge and support, optimizing learning outcomes [2]. Collaborative learning group activities and integrative studies are an important aspect of military training, and IT can significantly enhance this component. Electronic environments, online platforms, and tools such as Learning Management Systems (LMS) and collaborative software allow students to collaborate on projects, share knowledge, and receive feedback from instructors and peers. These platforms also support asynchronous learning, allowing learners to access resources and complete tasks at their own pace [3].

The use of IT in didactic design also increases the efficiency of resource management. Digital libraries, databases, and cloud-based storage solutions provide easy access to a wide variety of learning materials. This reduces the dependence on physical resources and allows for quick updating and dissemination of information. In addition, IT allows monitoring and analysis of resource use, helps to optimize the allocation of training materials and equipment.

Real-time assessment and feedback are considered essential for effective training. IT tools such as online quizzes, simulations and performance tracking systems provide trainees with immediate feedback and help them identify areas for improvement. Instructors can also use these tools to monitor real-time progress and adjust instructional strategies to ensure learning objectives are being met effectively [4]. It is a clear issue that in modern times, traditional training does not ensure the intellectual development and other qualities of students, including IT skills, to a high level.

As a modern characteristic of developmental training - since IT is of particular importance in training, the application of this method significantly increases the creative potential of graduates in their careers, fundamentally different from traditional training technologies due to their goals and tasks, the characteristics of the activities of learners and educators [5-6].

In conclusion, the integration of information technology into the didactic design model of military engineer training contains numerous opportunities to increase the effectiveness and efficiency of training programs.

From immersive learning experiences and personalized learning paths, to collaboration platforms and efficient resource management, IT provides the most powerful tools military engineers need to prepare for the challenges of modern military operations.

As technology continues to advance, its role in military engineer training will undoubtedly become even more important in imparting the knowledge, skills, and attitudes that drive innovation and excellence in the field.

References

1. Khizhnaya A. V., Kutepov M. M., Gladkova M. N., Gladkov A. V., Dvornikova E. I. (2016). Information technologies in the system of military engineer training of cadets. International journal of environmental & science education. 2016. Vol. 11, No. 13. P. 6238-6245.

2. Žogla, I. (2019). Principles of learner learning-centred didactic in the context of technology-enhanced learning. In: Daniela, L. (eds) Didactics of smart pedagogy. Springer, Cham. 2019. P. 71-94. DOİ: https://doi.org/10.1007/978-3-030-01551-0_4

3. Valverde-Berrocoso, J., Fernández-Sánchez, M.R. (2020). Instructional design in blended learning: theoretical foundations and guidelines for practice. In: Martín-García, A. (eds) Blended Learning: Convergence between technology and pedagogy. Lecture Notes in Networks and Systems. Springer, Cham. 2020. Vol 126, P. 113-140. DOİ: https://doi.org/10.1007/978-3-030-45781-5_6

4. Dadashov A. S. (2023). Designing military engineering training based on the model of didactic justification. Journal of Defense Resources Management. 2023. V.14, N2. p.87-96.

5. Agayev, S.O., Talibov, A.M. and Hashimov, E.G. (2016). Modern pedagogical technologies in military education. Textbook. Part I.// - Baku: Military Publishing House. 2016. 152 p.

6. Piriyev H. K. et al. Some issues of pedagogical staff training for special-purpose higher education institutions //Military knowledge. – 2014. – №. 4. – p. 3-9.

APPLICATION OF PROGRAMS FOR CREATING SIMULATIONS AND MODELS IN TEACHING PHYSICS

Humbatova Kh.Z.
Military Institute named after H.Aliev, Baku, Azerbaijan

Physics is a science that relies on experiments and observations to understand the laws of nature. However, some physical phenomena may be difficult or impossible to observe or experiment in real life. Simulation and modeling programs are invaluable tools to overcome these limitations. The advantages, methods, potential difficulties and future prospects of applying simulation and model creation programs in physics education will be explored.

1. Advantages of simulation and model creation programs.

Visualizing abstract concepts: Simulations help learners better understand complex physical phenomena by visually depicting them. For example: abstract concepts such as atomic structure, planetary motion or electric fields can be more clearly described through simulations.

Conducting experiments safely: Some physical experiments can be dangerous or financially expensive. Simulations allow learners to conduct such experiments safely or inexpensively. For example: experiments involving explosions, radioactive substances or high-voltage electric currents can be conducted safely in a simulation environment.

Repetition of experiments: Through simulations, experiments can be repeated any number of times. It helps learners better understand physical phenomena and analyze results. By changing parameters, learners can obtain different results and better understand cause-effect (induction-deduction) relationships.

Personalized learning: Simulation programs allow learners to learn at their own pace and according to their needs. Students have the opportunity to study the functions of the program and conduct their own independent research.

Increasing motivation: Interactive simulations help learners to show more interest in the learning process and increase their motivation.

2. Application methods of simulation and model creation programs.

Organization of lessons: Simulations can be used as the main part of lessons or as additional material.

Labs: Virtual labs can be used as a substitute or supplement to real labs.

Projects: Learners can design projects that model various physical phenomena using simulation software.

Assessment: Simulations can be used to assess learners' knowledge.

3. Potential difficulties.

Technical challenges: Simulations can be used as the main part of lessons or as supplementary material.

Laboratory work: Technical problems may arise with the use of programs.

Teacher training: It is important that teachers have the necessary knowledge and skills to use simulation programs effectively.

4. Future prospects.

In the future, simulation and model creation programs are expected to be more widely used in Physics education.

The development of virtual and augmented reality technologies will allow creating more realistic and interactive simulations.

References

1. Winsberg, Eric (2003), Simulated Experiments: Methodology for a Virtual World.
2. Roger D.Smith: "Simulation: The Engine Behind the Virtual World", eMatter, December 1999.
3. Agayev S.O. et al. (2016). Modern pedagogical technologies in military education. Textbook. Part I.// - Baku: Military Publishing House. 2016. 152 p.
4. Piriyev H. K. et al. Some issues of pedagogical staff training for special-purpose higher education institutions //Military knowledge. – 2014. – №. 4. – p. 3-9.
5. A.Borshchev, A.Filippov: "From System Dynamics and Discrete Event to Practical Agent–Based Modeling: Reasons, Techniques, Tools", The 22nd International Conference of the System Dynamics Society, July 2004, Oxford, England
6. Хемди А.Таха. Глава 18. Имитационное моделирование // Введение в исследование операций (7–е изд). М.: «Вильямс». 2007 [Operations Research: An Introduction].

ANALYSIS OF THE ROLE OF INFORMATIZATION IN TEACHING A FOREIGN LANGUAGE

Javadova T.A.
Military Institute named after Heydar Aliyev, Baku, Azerbaijan

The rapid development of Information Technology in the modern world has significantly changed all areas of the education system, including teaching a foreign language. Informatization not only opens up new opportunities for the educational process, but also poses new problems [1-7].

The pros and cons of the role of informatization in teaching a foreign language, its impact on students and teachers, as well as future prospects will be analyzed.

1. Positive aspects of informatization

Learning thanks to online platforms and interactive programs in personalization, learners can learn at their own pace and according to their needs. Creating personalized learning plans and tracking the progress of trainees becomes even easier. In the interactivity of learning, games, simulations, virtual reality and augmented reality technologies make the learning process more interesting and attractive. Learners become active participants, not passive listeners. In easy access to resources, online dictionaries, grammar exercises, audio and video materials, as well as information from different cultures are easily accessible to learners. This makes the learning process more richly comprehensive.

The effectiveness of the assessment. Automated assessment systems save teachers ' time and allow students to more objectively assess their knowledge.

2. Negative aspects of informatization. Technological dependence excessive use of technology can negatively affect the development of critical thinking and problem-solving skills of learners. Not all learners may have equal access to computer science technologies.

This can increase the impact of socioeconomic differences in education. Technical difficulties and technical problems, lack of internet or improper operation of technology can not only disrupt the learning process, but also reduce the motivation of learners.

Training of teachers. It is important for teachers to have the necessary knowledge and skills to effectively use information technology. Otherwise, the introduction of technologies can negatively affect the quality of teaching. Information security the use of online platforms also includes risks associated with information security. In the future, the impact of informatization on foreign language education is steadily increasing.

Interactive learning programs. With the development of information technology, interactive learning programs have started to be used in foreign language teaching. These programs offer various learning materials and resources to help students enhance and deepen their language skills. Examples include applications like Duolingo, Rosseta Stone, and Babbel. These programs make the language learning process more engaging and effective for students.

Virtual reality (VR) and Augmented Reality (AR). Virtual and augmented reality technologies make language teaching more interactive and appealing. Through these technologies, students can learn languages in environments where different languages are spoken. Virtual and augmented reality strengthen the practical aspect of language learning and provide students with opportunities to apply their language skills in real-life situations.

References

1. Bax S. (2003). CALL-past, present and future. Retrievd from http://u.arizona.edu/~jonrein/internettech10/bax_03.pdf

2. Bax S. (2011). Normalisation revisited: The effective use of technology in language education. Computer-Assisted Language Learning and Teaching.

3.Agayev, S.O. et al. (2016). Modern pedagogical technologies in military education. Textbook. Part I.// - Baku: Military Publishing House. 2016. 152 p.

4.Piriyev H. K. et al. Some issues of pedagogical staff training for special-purpose higher education institutions //Military knowledge. – 2014. – №. 4. – p. 3-9.

5. Chapelle C.A. (2001). Computer applications in second language acquisition: Foundations for teaching testing and research. Cambridge: Cambridge University Press.

6. Delcloque P., The History ofComputer Assisted Language Learning: WebExhibition. ICT for Language Teachers. ICT4LT. October 3.

7. Dewey J. Democracy and education. New York: Macmillan. https://archive.org/stream/democracyandeduc00deweuoft/democracyandeducdeweuoft_djvu.txt

TECHNOLOGY-ENHANCED LANGUAGE LEARNING

Minavvar Mammadova
Military Institute named after Heydar Aliyev, Baku, Azerbaijan

To emphasize the growing invisibility of the tool and the shift in emphasis on the uses of the tool, it would seem appropriate to employ a different term to characterize this period in the evolution of computer use in language teaching. Whereas in phase one and two, we referred to computer-Assisted Language Learning, we will now instead adopt use the term Technology-Enhanced Language Learning.

The distinction between CALL and Technology-Enhanced Language Learning (TELL) is that the computer simultaneously becomes less visible yet more ubiquitous.

The change in emphasis from computer to technology places direct importance on the media of communication made possible by the computer, which itself often remains unseen, rather than on the computer itself.

Whereas in CALL, the computer assisted learning, it might be said that in TELL, the computer supports learning. T

his third phase of technology use in second-and foreign-language teaching is characterized by the use of multimedia and the internet. It can also be characterized by a clearly delineated move away from behaviorist, drill and practice type software and a move towards more constructivist uses of the tool.

It also represents a certain rejection of Communicative CALL. Though communicative CALL was seen as an advance over behavioristic CALL, it too began to come under criticism.

The third phase of use of computers in teaching second languages is an Integrative CALL.

The term integrative to refer to efforts at developing models which would integrate various aspects og language learning for example using task- or project based approaches.

References

1. Ellis, R. (2003). Task-based language learning and teaching. Oxford: Oxford University Press

2. Smith, R.C. (2019) Using Technology in the classroom; A Guide to integrating Digital tools to Enhance Language Learning

3.Agayev, S.O. et al. (2016). Modern pedagogical technologies in military education. Textbook. Part I.// - Baku: Military Publishing House. 2016. 152 p.

4.Piriyev H. K. et al. Some issues of pedagogical staff training for special-purpose higher education institutions //Military knowledge. – 2014. – №. 4. – p. 3-9.

THE EVOLUTION OF THE USE TECHNOLOGY IN FOREIGN LANGUAGE TEACHING

Khanim Yolchiyeva
Azerbaijan National Aviation Academy, Baku, Azerbaijan

The literature on the use of technology and, more specifically computers in language learning, has centered largely around discussions and debates of pedagogical merits of technological devices. Approaches, typologies, phases, methods; all have served as focal points for organizing the past 50 years of technology use in language learning.

Indeed, it is the way the computer is used and the context in which it is used that determines the efficacy.

When we think about computer use, we must beware of technocentric thinking or the tendency to give centrality to a technical object such as a computer.

For the purposes of this review therefore, it is the approach that has been taken to use of technology in language learning that will serve as the organizing factor. These are some of the issues that will be explored in this review of technology use from the behavioristic language laboratory of the 1970s to the constructivist learning environments of the Internet at the end of the nineties.

With the demise of the audio-lingual method and the increased interest in Communicative Language Teaching, laboratory use appeared less and less relevant to the goals of language teaching.

Instructional CALL has been described as follows:

- materials are presented in a highly-structured, predetermined manner;
- repetitive language drills and practice are the main substance;
- students are passive responders, not initiators;
- the computer functions as an authoritative instructor;
- a detailed set of high-and- low-level learning objectives is provided;
- learning paths are predetermined;
- the computer instructs the student: students learn from the computer.

References

1. Levy, M (2009) Technologies in Use for second language learning. Modern Language Journal

2. Mammadova M.F. “Practical trainings and laboratory drills” 2008, Ministry of Education in Azerbaijan, p.80

3. Smith, R.C. (2019) Using Technology in the classroom; A Guide to integrating Digital tools to Enhance Language Learning

4.Agayev, S.O. et al. (2016). Modern pedagogical technologies in military education. Textbook. Part I.// - Baku: Military Publishing House. 2016. 152 p.

5.Piriyev H. K. et al. Some issues of pedagogical staff training for special-purpose higher education institutions //Military knowledge. – 2014. – №. 4. – p. 3-9.

ГЕЙМІФІКАЦІЯ В ОСВІТНІХ ПРОЦЕСАХ: ПЕРЕВАГИ ТА ВИКЛИКИ ВПРОВАДЖЕННЯ

Лященко В.О., Гук А.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Гейміфікація в освітніх процесах стає все більш популярним підходом для підвищення залученості та мотивації учнів. Використання ігрових елементів, таких як бали, рівні, досягнення та змагання, дозволяє покращити ефективність навчання, сприяючи активній участі та взаємодії учнів з матеріалом. Однією з основних переваг гейміфікації є можливість адаптації навчального процесу до індивідуальних потреб учнів, що допомагає створювати персоналізовані траєкторії навчання та підвищувати успішність.[1]

Однак впровадження гейміфікації також супроводжується певними викликами. Одним із таких є необхідність розробки якісного контенту та інструментів для створення ігрових сценаріїв, що вимагає значних зусиль з боку викладачів та розробників освітніх платформ. Також існує ризик надмірного фокусування учнів на ігрових досягненнях, що може відволікати їх від основних навчальних цілей.[2]

Гейміфікація також вимагає врахування психологічних аспектів учнів, оскільки не всі підходи до гейміфікації можуть бути однаково ефективними для різних груп студентів. Важливо знайти баланс між ігровими елементами та навчальним змістом, щоб забезпечити гармонійне поєднання мотивації та розвитку компетенцій.[3]

Метою доповіді є аналіз переваг та викликів впровадження гейміфікації в освітніх процесах, розгляд успішних прикладів її застосування та визначення ключових факторів, що впливають на ефективність цього підходу в освіті.

Список літератури

1. Алфьоров Г.О. Гейміфікація в освіті: Залучення студентів через гру" – Київ: Видавничий дім "Освіта та розвиток, 2013. – 113 с.

2. Мінкін Д.В. Виклики впровадження гейміфікації в навчанні: Баланс між розвагами та навчанням" – Київ: Видавництво "Освітні технології, 2019. – 289 с.

3. Марчук О.Г. Психологічні аспекти гейміфікації в освіті: Що працює для різних учнів – Київ: Інститут освітніх досліджень, 2017. – 272 с.

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В АДАПТИВНОМУ НАВЧАННІ: АВТОМАТИЗАЦІЯ ПРОЦЕСУ НАВЧАННЯ

Дерев'янко К.А., Гук А.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Штучний інтелект (ШІ) відіграє ключову роль у розвитку адаптивного навчання, що дозволяє автоматизувати процеси освіти та підвищити їх

ефективність. Використання ШІ в освітніх платформах забезпечує персоналізацію навчальних програм, які підлаштовуються під індивідуальні потреби та здібності кожного студента.

Алгоритми ШІ здатні аналізувати навчальні досягнення учнів, виявляти прогалини в знаннях і автоматично пропонувати відповідні навчальні матеріали, що дозволяє оптимізувати процес навчання та підвищити його результативність.[1]

Одним із важливих аспектів автоматизації процесу навчання за допомогою ШІ є створення динамічних навчальних маршрутів. Ці маршрути коригуються в реальному часі на основі прогресу учня, що дозволяє максимально адаптувати матеріали до його потреб. Крім того, ШІ дозволяє автоматизувати оцінювання знань, забезпечуючи миттєвий зворотний зв'язок та рекомендації для подальшого навчання. Ці можливості дозволяють значно знизити навантаження на викладачів і зробити навчальний процес більш ефективним.[2]

Метою доповіді є розгляд ролі штучного інтелекту в адаптивному навчанні, аналіз його можливостей для автоматизації навчального процесу, а також оцінка впливу на підвищення ефективності освіти та індивідуалізацію навчальних програм.

Список літератури

1. Симонюк О. В. Штучний інтелект в адаптивному навчанні: Персоналізована освіта в масштабах – Київ: Видавничий дім "Освіта", 2013. – 332 с.

2. Марченко С. О. Автоматизовані навчальні маршрути: Реальна адаптація за допомогою ШІ – Київ: Інститут цифрової освіти, 2018. – 293 с.

РОЛЬ ЛЮДИНИ В СИСТЕМІ «ЛЮДИНА-МАШИНА»

Меденицький О.Д., Кучук Н.Г.
Харківський національний університет радіоелектроніки, Харків, Україна

Система «людина-машина» є окремим випадком складних інформаційних систем, в яких функціонування машини та діяльність людини-оператора пов'язані єдиним інформаційним процесом. [1] розрізняють кілька типів операторської діяльності.

Ці типи класифікуються залежно від основної функції, що виконується людиною-оператором, та частки образного, понятійного, сенсомоторного компонентів, включених в операторську діяльність. А саме, оператор-технолог, оператор-маніпулятор, оператор-спостерігач (контролер), оператор-дослідник та оператор-керівник.

При організації взаємозв'язку людини і машини в системі «людина-машина» основна роль належить не так анатомічним і фізіологічним, скільки психологічним властивостям людини: сприйняттю, пам'яті, мисленню, увазі [2]. Тому від психологічних властивостей людини багато в чому залежить її інформаційна взаємодія з машиною.

Список літератури

1. Albers S. Using a simulation model to represent the time dependence of human reliability / S. Albers // Proc. 5-th. EuRe Data Conf. Berlin. – 2020. – P. 445-453.
2. LeCun Y. Convolutional networks for images, speech, and time series / Y. LeCun, Y. Bengio. – London: THE MIT PRESS, 2021. – 1290 p.

ЕЛЕКТРОННІ ПІДРУЧНИКИ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ ЯКОСТІ ОСВІТИ

Колєнов І.Є., Мороз А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Електронні підручники стають важливим інструментом для підвищення якості освіти, надаючи учням і студентам доступ до інтерактивних навчальних матеріалів, актуальної інформації та мультимедійних елементів, що сприяють кращому розумінню матеріалу.

Впровадження електронних підручників дозволяє навчальним закладам зменшити витрати на друковані видання та забезпечити постійний доступ до оновлених матеріалів.[1]

Електронні підручники забезпечують адаптивність навчання, дозволяючи вчителям і учням налаштовувати навчальний процес відповідно до індивідуальних потреб і швидкості засвоєння знань. Важливою перевагою є можливість інтеграції з іншими цифровими освітніми інструментами, такими як віртуальні класи, системи управління навчанням (LMS), що сприяє комплексному підходу до навчання.[2]

Важливим аспектом є також екологічність електронних підручників, оскільки їх використання зменшує потребу в папері та друкованій продукції, що позитивно впливає на навколишнє середовище. У зв'язку з цим, електронні підручники підтримують принципи сталого розвитку в освіті. Однак впровадження електронних підручників також стикається з певними викликами, такими як необхідність навчання викладачів та студентів для ефективного використання нових технологій, а також забезпечення доступу до інтернету та електронних пристроїв у всіх навчальних закладах.[3]

Метою доповіді є аналіз впливу електронних підручників на якість освіти та розгляд можливостей їх подальшого впровадження для поліпшення навчального процесу в освітніх установах.

Список літератури

1. Швець А.М. Електронні підручники у сучасній освіті: Інтерактивність та доступність – Київ: Освіта, 2022. – 252 с. – (Сучасні освітні технології).
2. Мельничук М.Я. Цифрові ресурси в навчанні: Переваги та можливості – Львів: Видавництво "Наука і освіта", 2021. – 331 с. – (Інновації в освіті).
3. Попоп С.Г. Інноваційні технології в освіті: Вплив на навчальний процес – Харків: Вид-во "Промінь", 2023. – 246 с. – (Сучасні підходи до навчання).

АНАЛІЗ НАВЧАЛЬНОЇ ТА ОСВІТНЬОЇ ІНФОРМАЦІЇ

Лисиця Д.О.
Національній технічний університет «ХПІ», Харків, Україна

Метою доповіді є аналіз основних аспектів навчальної та освітньої інформації при розробці комп'ютерних систем.

Навчальна інформація – ширше поняття проти освітньої інформацією. Воно використовується при підготовці та використанні тренажерів у програмуванні [1], при використанні та підготовці штучних нейронних мереж, при підготовці інтелектуальних систем, підготовці кіберфізичних систем, при налагодженні програм, створенні віртуального моделювання, при тестуванні програмного забезпечення. Освітня інформація – це інформація, яку застосовують у сфері освіти. Вона характеризується двома односпрямованими потоками. Перший основний потік – "інформуючий" спрямований від об'єкта або суб'єкта навчання до учня. Другий потік направлений від учня до викладача або системи тестування. Він є контрольним чи тестуючим. Односпрямованість потоків в освітній інформації дає підставу розглядати їх як інформаційний вплив. Навчальна інформація містить додаткові інформаційні потоки, що ставить завдання їхнього моделювання. Наприклад, нейронну мережу навчають на умовах завдання (вхідна множина) та відомих рішеннях (вихідна множина). При цьому дотримуються відносини пропорційності для застосування та відношення інформаційної відповідності для умов і завдань. Для потоку має місце інтерактивність чи інформаційне взаємодія, а чи не вплив як у Educational information. Звідси перша відмінність є потоковою і полягає у використанні взаємодії замість дії, або заміну односпрямованості на двоспрямованість.

Список літератури

1. Ярошенко Т. О. Дистанційне навчання в системі вищої освіти: сучасні тенденції [електронний ресурс] / Ярошенко Т. О. // Інженерні та освітні технології. – 2019. – Т. 7, № 4. – С. 8-21. – doi.org/10.30929/2307-9770.2019.07.04.01.

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У НАВЧАЛЬНИХ СИСТЕМАХ

Бутенко Б.В., Кучук Г.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні автоматизовані навчальні системи представляють складні програмні комплекси, функціонування яких потребує обробки великих масивів даних як реального часу. Ця вимога зумовила необхідність застосування нетрадиційних технологій, передусім технологій із використанням штучного інтелекту. Технології штучних нейронних мереж відносяться технологіям штучного інтелекту, в основі яких лежить імітація принципів функціонування людського мозку. Сучасні нейронні мережі широко застосовуються на

вирішення завдань класифікації, розпізнавання, передбачення, управління процесом у випадках, коли умова завдання важко чи неможливо формалізувати.

У навчальних системах нейромережні технології застосовуються до створення програмних продуктів, основу яких лежить технологія нейронних мереж, для автоматизації створення та оптимізації функціонування різних складових освітнього процесу. Нейронні мережі використовуються для оцінки результатів тестування студентів. Застосування нейронних мереж дозволяє отримати більш точну картину знань учнів, виявити прогалини у знаннях учнів, підвищити об'єктивність тестування. Нейронні мережі в освіті так само використовуються для вирішення завдань, близьких до завдань класифікації, в яких необхідно виконати аналіз великої кількості чинників, що важко формалізуються. До таких завдань належить завдання складання достовірного рейтингу викладачів на основі опитування студентів [1], завдання оцінки діяльності та класифікації закладів вищої освіти.

Список літератури

1. Kim J. Bentley P. Towards an artificial immune system for network intrusion detection: an investigation of dynamic clonal selection./ J. Kim J., P. Bentley// In Proc. Congress on Evolutionary Computation – Honolulu: HI, USA– 2002. – P.1244-1252.

ВПЛИВ ЦИФРОВИХ ОСВІТНІХ ПЛАТФОРМ НА ЕФЕКТИВНІСТЬ ДИСТАНЦІЙНОГО НАВЧАННЯ

Показій К.О., Тимошенко Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Зі стрімким розвитком цифрових освітніх платформ постає питання про їхній вплив на ефективність дистанційного навчання. Використання цифрових платформ надає можливість не лише інтегрувати різні форми навчання, але й забезпечити адаптацію матеріалу до індивідуальних потреб студентів, що робить навчання гнучкішим та зручнішим [1]. Аналіз ефективності таких платформ вимагає розгляду різних аспектів: доступності навчальних матеріалів, підтримки інтерактивних елементів та можливостей комунікації між викладачем і студентом. Важливим є також питання зворотного зв'язку, що дозволяє оперативно реагувати на потреби учнів і покращувати якість викладання. Окрім того, технології штучного інтелекту та машинного навчання, інтегровані в платформи, можуть допомогти аналізувати результати студентів, автоматизувати оцінювання та надавати рекомендації для індивідуального навчання [2]. Завдяки широкому впровадженню цифрових освітніх платформ суттєво змінюються методи подачі інформації та підходи до оцінювання знань. Однією з ключових переваг цих платформ є можливість доступу до навчальних матеріалів з будь-якого місця та в будь-який час, що сприяє підвищенню самостійності студентів і створенню індивідуалізованих траєкторій навчання [3]. Додатково, платформи дозволяють організовувати навчальний процес більш

гнучко, забезпечуючи синхронне та асинхронне навчання, що особливо актуально для тих, хто поєднує навчання з роботою або іншими обов'язками.

Метою доповіді є вивчення впливу цифрових освітніх платформ на ефективність дистанційного навчання, аналіз переваг та викликів їх використання, а також розгляд потенціалу подальшого розвитку таких платформ у контексті сучасної освіти.

Список літератури

1. Волошин М.О. Цифрові освітні платформи та майбутнє освіти – Київ: Видавничий дім "Освіта", 2023. – 310 с.

2. Назаров О.О. Штучний інтелект у персоналізованому навчанні: Нова ера цифрової освіти – Київ: Науковий центр освітніх технологій, 2023. – 280 с.

3. Максимов Л.П. Гнучкість та доступність в онлайн-навчанні – Київ: Інститут дистанційної освіти, 2023. – 260 с.

АСПЕКТИ ЗАСТОСУВАННЯ МЕСЕНДЖЕРА DISCORD ПРИ ДИСТАНЦІЙНОМУ НАВЧАННІ

Правдіна О.М., Архипцева Н.О., Мягков В.Ю. Єрьомін Д.А.
Харківський радіотехнічний фаховий коледж, Харків, Україна

Одна з проблем дистанційного навчання – це організація комунікації в процесі дистанційного навчання: між викладачем і студентами, студентів між собою. Використання сучасних месенджерів – це одна з можливостей вирішити ці труднощі у викладанні та полегшити можливість використання навчального матеріалу студентами. Мета досліджень – обґрунтувати (вибрати) основні параметри вибору програми Discord, що забезпечує якість дистанційного освітнього процесу при викладанні загальноінженерних і спеціальних дисциплін та використанні графічного матеріалу. У доповіді наводяться результати дослідження використання месенджера Discord при дистанційному навчанні.

Для вирішення завдань, поставлених перед освітою, потрібно застосовувати нові технології навчання та давати студентам нові знання та ідеї, нові способи постійного оновлення знань та нового мислення. Одним із додатків став Discord – це безкоштовний месенджер з підтримкою IP-телефонного зв'язку, відеоконференцій, призначений для використання різними спільнотами за інтересами [1]. Комунікаційна платформа Discord є універсальним рішенням для викладачів ЗФПО, які потребують надійної та перевіреної програми для навчання. Користувачі, виділені у певні групи (курси, академічні групи, підгрупи тощо) під час використання платформи Discord отримують низку додаткових переваг: зниження витрат за зв'язок, розширення функціональних можливостей порівняно із звичайною телефонією, доступ до всіх функцій сервісу в будь-якій географічній точці, що особливо актуально за необхідності організувати віддалену роботу студентів, набір функцій можна налаштовувати під конкретні завдання різноманітних форм навчання [2]. Платформа Discord містить різні функції: сервери, голосові канали, текстові канали та опцію Go Live для проведення

трансляції екрану [3]. Завдяки якісним безкоштовним можливостям групового спілкування в будь-якому з видів зв'язку в Discord освітяни застосовують його адаптуючи під власні завдання в молодіжному середовищі.

Список літератури

1. https://discord.com/.
2. https://support.discord.com/hc/ua/articles/360034561191
3. https://nus.org.ua/articles/use-v-odnomu-mistsi-yak-programa-discord-dopomozhe-organizuvaty-dystantsijne-navchannya/

ЕФЕКТИВНІСТЬ ЗАСТОСУВАННЯ ВІРТУАЛЬНИХ ЛАБОРАТОРІЙ У ФОРМУВАННІ ПРАКТИЧНИХ НАВИЧОК СТУДЕНТІВ ТЕХНІЧНИХ СПЕЦІАЛЬНОСТЕЙ

Кураков Я.С., Томак В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком інформаційних технологій віртуальні лабораторії все більше мають попит в освіті, особливо в технічних дисциплінах. Вони дозволяють студентам безпечно та ефективно відпрацьовувати практичні навички, які важко або дорого реалізувати у фізичному середовищі. Особливу актуальність такого типу лабораторії набули у теперішній час, коли під час пандемії і військового стану багато навчальних закладів проводять навчальний процес дистанційно, з використанням спеціалізованих сервісів Інтернет. Застосування віртуальних лабораторій у навчальному процесі сприяє формуванню у студентів прикладних компетенцій, що особливо важливо для спеціальностей, пов'язаних з мережною і комп'ютерною інженерією, комп'ютерними науками, фізикою та математикою, тощо [1, 2].

Метою доповіді є дослідження впливу віртуальних лабораторій на формування практичних навичок та підвищення рівня підготовки студентів, що навчаються на технічних спеціальностях. У доповіді представляються і обґрунтовуються результати експериментального використання віртуальних лабораторій у навчальному процесі та проаналізовано їх ефективність на основі зворотного зв'язку від студентів та викладачів. Зокрема наведені дані демонструють, що застосування віртуальних лабораторій дозволяє не тільки покращити засвоєння теоретичних знань, але й сприяє розвитку практичних навичок у середовищі, наближеному до реальних умов.

Показано, що розвиток віртуальних лабораторій в Україні і в усьому світі стає актуальним завдяки можливості інтеграції новітніх технологій, таких як віртуальна та доповнена реальність, штучний інтелект та хмарні обчислення. Це дозволяє створювати високоякісні симуляції, що відтворюють складні технологічні процеси, доступні студентам з будь-якого місця та у будь-який час. Такий підхід значно розширює можливості для дистанційного навчання та сприяє залученню студентів до навчального процесу, одночасно підвищуючи рівень їх практичної підготовки та конкурентоспроможності на ринку праці [3].

Список літератури

1. Коваленко А. А., Кучук Г. А. Віртуальні лабораторії у вищій освіті: огляд інноваційних підходів та методик. Освітні інновації. 2021. Т. 3, № 2. С. 42–47.

2. Петров В. Г., Іванов А. Б. Технології віртуальної та доповненої реальності у підготовці технічних спеціалістів. Сучасні тенденції в освіті. 2022. Т. 4, № 1. С. 12–18.

3. Smith J., Brown L. Virtual Laboratories in Engineering Education: Opportunities and Challenges. Journal of Educational Technology. 2020. Vol. 15, No. 3. Pp. 223–229.

ВИКОРИСТАННЯ ДИСТАНЦІЙНИХ ОСВІТНІХ СИСТЕМ ЯК ВАРІАНТ ІНФОРМАТИЗАЦІЇ НАВЧАЛЬНОГО ПРОЦЕСУ

Татарников А.О., Замета М.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Інформатизація навчального процесу змінює способи подання інформації. В освітньому середовищі все менше використовуються традиційні методи викладання, де світогляд освітян обмежується досліджуваними темами. Завдяки технічному прогресу на заміну пасивного навчання активно обговорюються впровадження інтерактивних симуляцій та віртуальних лабораторій.

Метою доповіді є розробка та використання дистанційних онлайн освітніх систем для подолання низки проблем, що виникли внаслідок встановлення традиційних методів викладання, як шаблону для використання. Введення в освітній процес методів інформатизації відбувається шляхом надання доступу до різноманітних джерел інформації: від спілкування з тематичними експертами до використання онлайн-бібліотек. Створення інтерактивного середовища навчання дозволить студенту або учню стати основним учасником освітнього процесу. Таким чином, навчання стає персоналізованим – адаптування навчального процесу до індивідуальних потреб кожного студента враховує його темп та стиль сприйняття інформації. У висновку підвищується ефективність управління освітнім процесом, в якому набагато легше відстежувати прогрес студентів та аналізувати результати навчання. Основний функціонал такої системи має включати: навчальний матеріал у декількох варіаціях для індивідуалізації стилю сприйняття (відео, текстовий супровід, подкаст), рефлексія (нотатки або швидке опитування), практичне застосування вивченого та додатковий обсяг інформації. Така система дозволить здобувачу не залежати від графіка занять, суб'єктивної думки викладача, його форми викладання та стресу під час перевірки знань. Отже, створення подібної системи зможе об'єднати різноманітні типи інформатизації навчального процесу, що допоможе подолати проблеми відсутності персоналізації, вузьконаправленості наявних інструментів практикування знань та подолання освітніх втрат та розривів.

Список літератури

1. Навчальні втрати в умовах війни: як учителю їх діагностувати та компенсувати - Державна служба якості освіти України. *Державна служба якості освіти України*. URL: https://sqe.gov.ua/navchalni-vtrati-v-umovakh-viyni-yak-uchi/

ДО ПИТАННЯ ВИЯВЛЕННЯ АКАДЕМІЧНОГО ПЛАГІАТУ ЗОБРАЖЕНЬ

Главчева Ю.М., Главчев М.І.
Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

Запобігання плагіату зображень є важливим аспектом захисту авторських прав і підтримання етичних стандартів у цифровому суспільстві. У сучасному світі, де обмін зображеннями є надзвичайно швидким і простим завдяки інтернету, проблема академічного плагіату стає все більш актуальною. Незаконне використання чужих зображень в академічних роботах порушує права авторів та є академічним плагіатом. Саме тому існує потреба у розробці ефективних методів виявлення цього порушення, які дозволять захистити інтелектуальну власність та забезпечити справедливе використання візуальних матеріалів.

Метою доповіді є виявлення проблем, що існують у підходах до визначення ознак академічного плагіату зображень при перевірці академічних робіт.

В доповіді аналізуються підходи до виявлення подібності зображень. Серед найбільш поширених підходів можна виділити наступні:

– порівняння за візуальними характеристиками,
– глибоке навчання,
– аналіз ключових точок,
– хешування зображень.

Пошук ефективних алгоритмів триває постійно [1]. Але є певні обмеження, які не дають можливості виявити всі зміни та маніпуляції, доступні користувачам. Це зміна кольору, додавання шуму, масштабування, обрізка, обертання, накладення водяних знаків, тощо.

Процес точного порівняння зображень може потребувати значних обчислювальних ресурсів та часу, особливо при використанні глибокого навчання або аналізу великої кількості ключових точок. Зображення зі схожими візуальними характеристиками складно аналізувати, що може призвести до хибних висновків в результаті.

Таким чином, існуючі обмеження та недостатня точність результатів вказаних підходів ускладнюють їх використання на практиці для виявлення ознак академічного плагіату зображень. Перспективним напрямом може бути комбінування підходів для досягнення їх більш ефективної роботи.

Список літератури

1. Parmar S., Jain B. VIBRANT-WALK: An algorithm to detect plagiarism of figures in academic papers. *Expert Systems with Applications*. 2024. P. 124251. URL: https://doi.org/10.1016/j.eswa.2024.124251.

СЕКЦІЯ 2
ЗАСТОСУВАННЯ ТА ЕКСПЛУАТАЦІЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Керівник секції: д.т.н. проф. Г. А. Кучук, НТУ "ХПІ", Харків
Секретар секції: к.т.н. доц. С. С. Бульба, НТУ "ХПІ", Харків

RESEARCH CHARACTERISTICS OF THE THROUGHPUT MULTISERVICE TELECOMMUNICATION NETWORKS

Ibrahimov B.G.[1,2], Dunyamaliyev T.O.[2]
[1]Azerbaijan Technical University, Baku, Azerbaijan
[2] Baku Engineering University, Baku, Azerbaijan

This paper examines and studies the characteristics of the throughput of multiservice telecommunication networks, taking into account the quality indicators packet flow processing in the case using such service methods as FIFO (First-In, First-Out). It is assumed that priority queues (PQ) are used to allocate a fixed bandwidth ΔF_k to each load class, for queuing systems (QS) M/M/1/m [1-3].

By applying the adaptive bandwidth sharing service method proposed by [2], it is possible to increase the loading coefficient of the channel resource N1 by using the free resource N1 to process class-2 packets.For this model servicing two classes narrowband telecommunication networks flows, there are expressions that allow us to determine the waiting time for clas-2 packets. However, the proposed mathematical expressions are not applicable to assessing the quality of service for traffic packet flows in multiservice telecommunication networks.

The model under consideration is a queuing system with $M_1/M/N_r/N_b$ data integration - M_1 is a load class with a Poisson distribution of the input flow, M is an exponential distribution of service time, N_r is the number channel resource units, N_b is the buffer capacity [2-7].

The first load class has the highest priority. The second load class has a higher priority in relation to the third. Each load class is allocated its own buffer –N_{b1} is the maximum permissible queue length of the 1-st class, N_{b2} is the 2-nd class, N_{b3} is the 3-rd class.

In this system, we introduce the concept of a unit channel resource n as the greatest common divisor of the requirements for the amount transmission bandwidth required to service the message each of the information load flows located in a multiservice telecommunications network. As a result, we have an integer representation of the channel speed in the form of units channel resource [2]:

$$N = V_n(N) = \frac{1}{n} \cdot V_k , \qquad (1)$$

where $V_k -$ is the channel transmission speed, bps.

A channel with a capacity $C_{\max}(N)$ units of channel resource is divided into three parts:

$$C_{\max}(N) = C_{\max}(N_1) + C_{\max}(N_2) + C_{\max}(N_3), \quad (2)$$

Where $C_{\max}(N_1), C_{\max}(N_2), C_{\max}(N_3) -$ the number units channel resource allocated for processing the 1-st, 2-nd and 3-rd load classes, respectively.

The signs of a moving boundary (adaptive division) are that class-2 load packets can occupy a free channel resource N_1. If there is a channel resource that is not occupied by processing higher class loads, it can be used to transmit class-3 packets.

We obtain analytical expressions as probability-time characteristics for studying the throughput of the service method with adaptive resource sharing. For this, we consider the model in the region without overloads:

$$\rho(N_2) = [(\lambda_2 / C_{\max}(N_2)] \cdot L_n < 1, \rho(N_3) = [(\lambda_3 / C_{\max}(N_3)] \cdot L_n < 1, \quad (3)$$

where $\rho(N_i) -$ is the loading coefficient N_i number units of the channel resource [1–3].

Thus, using the results given by formulas (1), (2) and (3) it is possible to determine some important probabilistic-time characteristics throughput capacities taking into account the number of units channel resource.

References

1. Merindol P. Improving Load Balancing with Multipath Routing // Proc. of the 19-th International Conference on Computer Communications and Networks, IEEE. 2018. pp.54–61.

2. Ibrahimov B.G., Humbatov R.T., Alieva A.A., Ibrahimov R.F. Approaches to the analysis of performance indicators of multiservice telecommunication networks based on SDN technology//Information Technologies, Vol. 27, No. 8, 2021. P. 419–424.

3. Ibrahimov B.G. et al Research throughput multiservice telecommunication networks // Сучасні напрями розвитку інформацийно-комунікаційних технологій та засобів управління. Матеріали 10-і міжн. НТК, 9-10 квитня 2020. Том 1. Баку-Харків-Жиліна, 2020, с.30.

4. Bianchi G. Performance analysis of the IEEE 802.11 distributed coordination function //Selected Areas in Communications, IEEE Journal on. 2010. V. 18. No.3. pp. 535-547.

5. Ibrahimov, B.G. et al. Analysis and Selection Performance Indicators Multiservice Communication Networks Based on the Concept NGN and FN // -Kharkiv: Computer and information systems and technologies, -2021.–p.96-98.

6. Hasanov A. H. et al. Comparative analysis of the efficiency of various energy storages //Advanced Information Systems. – 2023. – Т. 7. – №. 3. – С. 74-80.

7. Ibrahimov B. G. Research quality of functioning of the efficiency optical telecommunication systems using spectral technologies / B. G. Ibrahimov, E. G. Hashimov // Проблеми інформатизації : тези доп. 11-ї міжнар. наук.-техн. конф., 16-17 листопада 2023 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Нац. ун-т оборони Азерб. республіки [та ін.]. – Харків : Impress, 2023. – С. 29-30.

8. Hasanov M. H. et al. Research efficiency optical transport networks with use transferring and reception optoelectronics module //International Journal of Research-Granthaalayah. – 2018. – Т. 6. – №. 2. – С. 324-330.

RADIOELECTRONICS IS THE FUTURE ACTIVITY OF WARFARE

Rustamov A.R.[1,2], Jabarova H.[2]
[1]National Defense İnstitute, Baku, Azerbaijan
[2]Azerbaijan Technical University, Baku, Azerbaijan

REW (radio electronic warfare) is the collection and analysis of data that can be found from publicly available sources. [1]. REW is one of the main factors that decide the fate of war. REW can be used to detect surveillance targets, control operations and protect information to a high degree. Control and management operations, radio-electronic defense, counterattack, or hybrid defense strategies are assigned to these systems [2, 3]. This thesis aims to explore real-life applications and case studies of REW.

Radio-electronic warfare controls and is used for different purposes. The main purpose of radio-electronic warfare is to provide protection against the enemy and to attack it using radio-electronic means and techniques. The primary goal of REW is to control the electromagnetic spectrum, either by denying the opponent its advantages or ensuring friendly forces have unimpeded access to it. This spectrum includes radio waves, microwaves, infrared, visible light, and other forms of electromagnetic energy. Radio-electronic warfare is used in military operations, security, defense, automated control etc.

Radio-electronic warfare (REW), also known as electromagnetic warfare, is a strategic military activity that revolves around manipulating the electromagnetic spectrum. Here are some of the key types of radio-electronic warfare. EW involves various methods: Electronic Defense (ED): Measures to protect friendly systems from EA, Electronic Surveillance (ES): Gathering intelligence by monitoring and analyzing EM emissions, EM Compatibility and Deception,Techniques to confuse or mislead enemy sensors, Spectrum Management: Efficiently allocating and using EM frequencies, Managing friendly EM emissions to avoid detection, Reprogramming: Altering system parameters during operations, Domains: EW operates across various domains, Land: Jamming enemy communications or RADAR, Sea: Disrupting naval systems, Air Targeting airborne assets, Cyberspace: Interfering with digital communication [4].

EW involves various types: Electronic Attack (EA): Offensive use of EM energy to disrupt or damage enemy communication, radar, or other assets; Cyber Attacks: Using computer-based techniques to disrupt or damage enemy electronic systems, networks, or information systems; Electronic Protection (EP): Encryption, Frequency Hopping, Shielding; Encryption: Encoding sensitive information to prevent unauthorized access or interception; Electronic Support (ES): Signal Intelligence, electronic surveillance, Reconnaissance, Gathering information by intercepting and analyzing electronic signals emitted by enemy systems, including radars, communication systems and electronic warfare platforms, Additionally - Directed energy weapons, Counter-IED systems, Anti-Access/Area Denial (A2/AD), Electronic warfare support measures [5].

Thus, electronic warfare holds promise but also uncertainty. Resilient communication systems, spectrum management, and ethical considerations are vital for overcoming these challenges and maintaining an advantage on the silent battlefield of the future.

References

1. https://link.springer.com/chapter/10.1007/978-3-030-01358-5_16#Bib1
2. Electronic Warfare: The Silent Battlefield of the Future Explained | Defensebridge
3. Hasanov A. H., Hashimov E. G. Analysis of the effectivness of communication and automated management systems //Modern directions of development of information and communication technologies and management tools, 2022. T. 1. P. 1-4.
4. Army must overcome these two primary electronic warfare challenges (c4isrnet.com)
5. Challenges and Considerations of Electronic Warfare in an Interconnected World (skyradar.com)

DEVELOPMENT OF FLIGHT CONTROLLERS OF FIXED-WING UNMANNED AERIAL VEHICLES

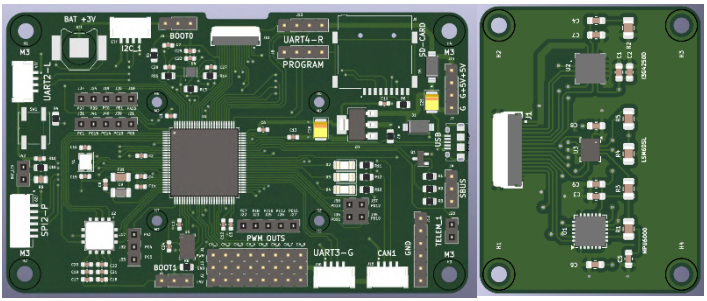
Heydarov N.N.
Institute of Control Systems; Institute of Radiation Problems, Baku, Azerbaijan

The flight controller is the primary control unit in Unmanned Aerial Vehicles (UAV). This device processes data from various sensors such as gyroscopes, accelerometers, magnetometers, barometers, LIDAR, and GPS and sends signals to control mechanisms of UAVs.

The signals sent regulate the UAV's stability in the air and stable flight. Additionally, the flight controller also provides autonomous flight (based on pre-programmed missions) using GPS data. Modern UAVs are equipped with advanced flight controllers that incorporate complex algorithms for diverse tasks. Although some of these controllers are open-source, certain parts in the code remain closed, making it impossible to modify those parts. Additionally, these algorithms and schemes can be placed on sites accessible to any specialist, which poses a risk to data security and reliability [1–5]. The requirement of UAVs to perform important missions in military and many civil matters makes the issue of meeting the requirements of the flight controller circuit, sensors and control algorithm relevant. The purpose of this thesis is to develop a flight controller and special attention is paid to the sensors used in the UAV flight controller, as well as the electrical circuit of the device and the printed circuit board.

The developed flight controller utilizes a 32-bit STM32F427 microcontroller with 2 MB flash, 256+4 KB RAM, and a 180 MHz clock frequency. This microcontroller supports various communication protocols, enabling data acquisition from different sensors. At the same time, its twelve 16-bit and two 32-bit timers allow for precise control of the control elements of UAVs. Various types of sensors were employed in flight controllers to determine the position and

coordinate of UAVs in space and to maintain their stability. Since flight stabilization primarily relies on data from accelerometers and gyroscopes, it is advisable to use high-precision sensors based on at least two distinct working principles from different manufacturers [5]. All the sensors used are connected to the microcontroller via I2C or SPI protocols. The reason for measuring the same quantity determined during the measurements by two or more sensors is to filter the data within the stabilization algorithm and calculate the average value. Additionally, if any of the sensors fails, the system can still maintain stabilization based on the data from other sensors. The printed circuit board of flight controller consists of two parts (Fig. 1). The part shown in (a) consists of a microcontroller, a power circuit, a barometer, an accelerometer, a magnetometer, various control components, and a connector connected to external sensors, and part (b) consists of an accelerometer and a gyroscope.



a b

Figure 1 – Realistic view of flight controller

The circuit containing the primary sensors is protected from vibrations and electromagnetic waves by being placed in a flexible and metallic enclosure. The prepared flight controller was tested in laboratory conditions, and data from all sensors were processed and appropriate commands were sent to control components.

References

1. Bayramov A. A. et al. SMART control system of systems for dynamic objects group //Bulgarska Voenna Misal. – 2018.

2. Bayramov, A.A., Hashimov, E.G. Development of UAV SoS flight combat reconnaissance mission program // Advanced İnformation Systems, 2019, vol 3, №1, p.p.152-156. DOI: 10.20998/2522-9052.2019.1.25

3. Hashimov E. G. About one method of navigation task solution //AHMC after H. Aliyev. Scientific Review. – 2013. – T. 1. – №. 20. – C. 45-49.

4. Hashimov E. G. et al. Development of the multirotor unmanned aerial vehicle //National security and military sciences. – 2017. – T. 3. – №. 4. – C. 21-31

5. Jee, Gopal, V. Brinda, V. R. Lalithambika, and M. V. Dhekane. "Influence of accelerometer location on autopilot stability of reusable launch vehicle attitude control system." *IFAC Proceedings Volumes* 47, no. 1 (2014): 205-210.

RESEARCH OF THE BANDWIDTH RADIO ENGINEERING SYSTEMS USING MIMO TECHNOLOGY

Huseynov B.F.
Azerbaijan Technical University; Baku, Azerbaijan

At present, the rapid development multiservice telecommunication networks, given the intensive growth in the volume transmitted useful and service traffic packet flows, requires the creation noise-resistant radio engineering systems using MIMO (Multiple Input Multiple Output) technology with increased performance radio communication networks [1].

However, in real radio engineering systems there are various distortions, such as interference and multipath fading, which can significantly affect the quality of radio signal reception. Radio communication is an integral element of a modern multiservice telecommunication network. This determines the requirements for the simplicity of its communication organization, high throughput and mobility, simple recovery and low cost radio channels when using MIMO technology [1]. In addition, the MIMO processing mode was widely introduced into practice at the stage of the emergence 4G-LTE and 5G-NR (New Radio) mobile communication networks.

Fig. 1 shows the structural model of the radio engineering complex system using MIMO [1]. This diagram (Fig. 1) represents a radio communication system with the number transmitting antennas M and the number receiving antennas N. Antennas $Tx_1,...,Tx_M$ transmit signals $S_1,...,S_M$ to receiving antennas $Rx_1,...,Rx_N$.

In each receiving antenna, the signals coming from all transmitting antennas are summed. The received signals in antennas $Rx_1,...,Rx_N$ are designated as $y_1,...,y_N$.

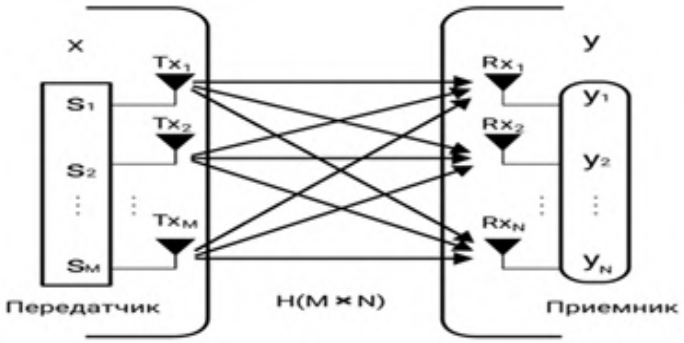


Figure 1 – Structural model of the system of radio engineering complexes with MIMO

In this regard, the task of determining the potential capabilities of radio engineering systems for this mode has become especially relevant. The known results related to this issue were obtained based on the approach associated with maximizing the channel capacity according to Shannon [2]. The MIMO capacity when using the Alamouti scheme is determined by the formula [1]:

$$C_{\max}(A) = \Delta F_k \cdot \sum_{i=1}^{m} [1 + (P_0 \cdot \lambda_i / M)], \quad (1)$$

where ΔF_k – channel bandwidth; P_0 – maximum permissible broadcast level; λ_i – eigenvalues of the matrix **H**.

Based on (1) it can be determined at the reception $SNR(P_0)$:

$$SNR(P_0) = 10\ell g[P_0 \cdot (\lambda_i / M)], \text{ dB}. \quad (2)$$

From (1) and (2) it is evident that the Alamouti scheme can lead to losses expressed as an effective reduction by M times of the SNR(P_0) present in the performance formula.

The most important task in the development radio engineering systems for transmitting discrete messages is the constant increase in their noise immunity under conditions harmful influence various sources interference and linear distortions in the radio communication channel with increased transmission speed. As an indicator noise immunity, the probability of erroneous reception a bit is usually used, which significantly depends on the type manipulation and coding used in the channels message transmission (CMT). At present, in CMT, including military ones, due to the strict requirements imposed on them for the speed data transmission and the volume transmitted information, signals with M-QAM (Quadrature amplitude modulation) are used. Now we can determine the probability erroneous reception at least one of the m subcarriers when receiving M-QAM signals against an Additive white Gaussian noise (AWGN) background, which is expressed as [2]:

$$P_{SER}(h) = 1 - \{\frac{1}{2^{m-1}\sqrt{2\pi}} \int_{-\infty}^{\infty} [1 + erf(u/\sqrt{2})]^{m-1} \cdot \exp[-0.5(u - \sqrt{2P_S T_S / N_0})^2]^m du\}^m. \quad (3)$$

Expression (3) determines the probability error per symbol, which is the SER characteristic (SER – Symbol Error Rate) of the demodulator and characterizes the probability of erroneous reception of a bit when receiving M-QAM signals against the background AWGN.

References

1. Hampton J.R. Introduction to MIMO Communications. UK, Cambridge University Press, 2014. 288 p.

2. *Sklar B.* Digital Communications: Fundamentals and Applications. 2nd edition. Prentice Hall Communications Engineering and Emerging technologies series. 2017.1104 p.

3. Ibrahimov B.G. et al. Research throughput multiservice telecommunication networks // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали 10-і міжнародної НТК, 9-10 квитня 2020. Том1. Баку-Харків-Жиліна, 2020, с.30.

4. Ibrahimov B. G. Research quality of functioning of the efficiency optical telecommunication systems using spectral technologies// Проблеми інформатизації : тези доп. 11-ї міжнар. наук.-техн. конф., 16-17 листопада 2023 р.: [у 3 т.]. Т. 1. – Харків : Impress, 2023. – С. 29-30.

RESEARCH SOME FEATURES MACHINE LEARNING TECHNIQUES IN MILITARY TELECOMMUNICATIONS SYSTEMS

Ibrahimov B.G.[1,2], Hasanov A.H.[2]
[1]Azerbaijan Technical University, Baku, Azerbaijan
[2]National Defense University, Baku, Azerbaijan

The rapid development of the infrastructure of the digital economy requires new effective approaches to building military telecommunications systems based on the basic principles of future FN (Future Network) networks with increased performance using machine learning methods. Recently, in telecommunications systems, data mining methods, especially machine learning methods, are increasingly being effectively used to solve a wide range problems, incl. and for classification and clustering of traffic [1, 6]. End-to-end digital technologies are widely used to create highly efficient military telecommunications systems. These include, first of all, technologies such as artificial intelligence (Artificial Intelligence, AI), SDN (Software Defined Networking), NFV (Network Functions Virtualization), IMS (Internet Protocol Multimedia Subsystem), cloud computing, and machine learning methods (Machine Learning, ML) [1].

Machine learning methods are a class artificial intelligence methods, the characteristic feature of which is not the direct solution of a problem, but learning through the use of solutions to many similar problems. Machine learning is the algorithms and learning methods used to create them. The essence of machine learning is teaching algorithms to make predictions based on data [2].

Considering the target settings being studied for creating FN telecommunication systems based on ITU-T recommendations, Y.3001 [1, 2] and the end-to-end digital technologies used above open up new opportunities for dynamic classification and clustering of multimedia traffic. In this case, it is necessary to take into account a wide range of infocommunication services, taking into account the numerous requirements of the QoS (Quality of Service) and QoE (Quality of Experience) parameters.

Therefore, the tasks of analysis and research of some features of machine learning methods in military telecommunication systems based on FN when using end-to-end digital technologies are the most relevant.

In a military telecommunications system for transmitting, processing and receiving multimedia traffic, as well as for ensuring network security and classifying traffic flows. Machine learning methods are widely used, which are based on three key elements [1, 2]:

1. In a telecommunications system, collecting an experimental set of various data (Data set), which can be Internet traffic, network flows, logs, email messages, multimedia traffic, user activity and much more, where the more and more diverse the training data, the more accurate the prediction result will be. The effectiveness of machine learning depends on the quality of the data set.

2. In a communication system, the selection of attributes - features that characterize the data being processed, which, depending on the task being solved,

can be hundreds of attributes, which can be metadata associated with the analyzed file - name, creation date, size, presence of network connections, access to the registry.

3. In the telecommunications system, the selection of existing or development of new algorithms and machine learning methods to ensure quality of service in a multi-service communication network in real time. The correct choice of an algorithm, model or method that performs a search based on certain characteristics of what is being sought in the dataset is a compromise between the speed of the algorithm and its complexity.

Considering the above, in this work, an important place is occupied by the issues of classification and clustering ML and metrics for assessing the effectiveness of processing results. Based on the mathematical formulation of the classification problem, a wide range of existing methods and algorithms are considered:

linear classifier,

logistic regression,

Bayesian classifier,

naive Bayes classifier,

k nearest neighbors (KNN),

algorithms based on decision trees (CART, C4.5, CHAID, decision forest, random forest),

ensemble algorithms.

Methods for composing learning algorithms boosting, bagging and stacking are considered.

References

1. Sheloukhin O. I., Erokhin S. D., Polkovnikov M. V. Machine learning technologies in network security. Moscow: Hotline - Telecom, 2021.360 p.

2. Краснова, И.А. Анализ влияния параметров алгоритмов Machine Learning на результаты классификации трафика в режиме реального времени // T-Comm: 2021. Т.16, №9. - С. 24-35.

3. Ibrahimov B. G., Hasanov A. H. The investigation and evaluation multiservice network NGN/IMS for multimedia traffic //Synchroinfo journal. 2020. Т. 6. №. 3. С. 10-13.

4. Ibrahimov B. G., Alieva A. A. Research and Analysis Indicators of the Quality of Service Multimedia Traffic Using Fuzzy Logic //Advances in Intelligent Systems and Computing. – 2021. – Т. 1306. – С. 773-780.

5. Ibrahimov B.G. et al. Research throughput multiservice telecommunication networks // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали 10-і міжн. НТК, 2020. Том1. Баку-Харків-Жиліна, 2020, с.30.

6. Ibrahimov B. G. Research quality of functioning of the efficiency optical telecommunication systems using spectral technologies / B. G. Ibrahimov, E. G. Hashimov // Проблеми інформатизації : тези доп. 11-ї міжнар. наук.-техн. конф., 16-17 листопада 2023 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Нац. ун-т оборони Азерб. республіки [та ін.]. – Харків : Impress, 2023. – С. 29-30.

7. Hasanov M. H. et al. Research efficiency optical transport networks with use transferring and reception optoelectronics module //International Journal of Research-Granthaalayah. – 2018. – Т. 6. – №. 2. – С. 324-330.

ANALYSIS OF THE NORMALIZED CAPACITY OF TELECOMMUNICATION SYSTEMS

Ibrahimov B.G.[1,2], Namazov M.B.[1,2], Mirzoev O.G.[2]
[1]Azerbaijan Technical University; Baku, Azerbaijan
[2] Baku Engineering University, Baku, Azerbaijan

Modern telecommunication systems widely use technology that uses multiple transmitting and multiple receiving antennas (MIMO, Multiple Input Multiple Output - many inputs, many outputs) in combination with coding and modulation algorithms [1, 6].

In a telecommunications system based on MIMO technology, it can significantly improve the efficiency of radio and communication systems compared to traditional systems with one transmitting and one receiving antenna.

However, in the presence of fading with significant spatial correlation in the radio channel, the efficiency of MIMO systems noticeably decreases [2].

When developing communication systems, it is necessary to take into account the spatial correlation of fading, which is usually described by a large number of parameters [1].

The studies have shown that one of the most important characteristics of the quality of functioning of telecommunication systems based on modern wireless cellular communication technologies is the normalized throughput of the systems.

To study the normalized throughput performance, consider a MIMO system with M transmit antennas and N receive antennas.

It is assumed that the investigated signal of MIMO systems at the receiver input has the following form [2]:

$$Y = H \cdot s + n, \tag{1}$$

where $Y -$ is the vector of received signals of dimension $N \times 1$; $H -$ complex channel matrix of dimension $N \times M$; $s -$ is a vector of transmitted complex information symbols of dimension $M \times 1$; $n -$ complex Gaussian random vector of dimension $N \times 1$ with zero mean and correlation matrix:

$$E\{n \cdot n'\} = \sigma_n^2 \cdot I = (0.5\Delta F_k \cdot N_0) \cdot I, \tag{2}$$

where $I -$ is the identity matrix of dimension, $N \times N$; σ_n^2 is the noise dispersion in one receiving antenna.

Each element h_{ij} of the MIMO communication channel matrix H is a complex transmission coefficient from the $j-$th transmit antenna to the $i-$th receive antenna.

The total power radiated by all transmit antennas is:

$$P_m = E[s's] = M \cdot \sigma_S^2, \tag{3}$$

where σ_S^2 is the dispersion of the signal emitted by one antenna and is equal to: $\sigma_S^2 = N_0 \cdot \Delta F_S$.

Taking into account formulas (1), (2) and (3), it is necessary to emphasize that the elements of the vector s of complex information symbols are assumed to be independent discrete random variables with unit variances. The variances of the elements of the vector s and are equal to unity. In this case, it is assumed that Rayleigh fading occurs in the MIMO radio system. This means that each element of the MIMO radio channel matrix H is a complex Gaussian random variable with zero mean. In this case, the elements of matrix H can be uncorrelated or correlated with each other.

Based on formula (1), (2) and (3), we consider the normalized throughput $C_{\max.nor.}(M, V_b)$ of the system of radio engineering complexes using MIMO technology with a given complex matrix H is determined by the relation [1, 2]:

$$C_{\max.nor.}(M, V_b) = \log_2 \det\left(1 + \frac{\rho(P_m)}{M} H \cdot H'\right), \text{ bps/Hs.} \qquad (4)$$

Relation (4) is a generalization of the known K. Shannon formula to the case of a MIMO communication channel for telecommunication systems, radio engineering complexes and mobile communication networks.

If the channel matrix **H** is a deterministic matrix, then the specific throughput $C_{\max.nor.}(M, V_b)$ will be a deterministic quantity. However, due to the presence of fading in real communication channels, the elements of the matrix **H** are random variables.

References

1. Biglieri E., Calderbank R., Constantinides A., et. al. MIMO Wireless Communication. Cambridge. U.K. Cambridge Univ.Press, 2007.-386 P.

2. MIMO System Technology for Wireless Communications. Edited by Tsoulos G. USA, FL, Boca Raton, CRC Press, 2006. -244 P.

3. Ibrahimov B. G. et al. The investigation and evaluation multiservice network NGN/IMS for multimedia traffic //Synchroinfo journal. –2020. –T.6. –№.3. –C. 10-13.

4. Ibrahimov B. G., Alieva A. A. Research and Analysis Indicators of the Quality of Service Multimedia Traffic Using Fuzzy Logic //Advances in Intelligent Systems and Computing. – 2021. – T. 1306. – C.773-780.

5. Ibrahimov B.G. et al. Research throughput multiservice telecommunication networks // Сучасні напрями розвитку інформацийно-комунікаційних технологій та засобів управління. Матеріали 10-і міжнародної НТК, 9-10 квитня 2020. Том1. Баку-Харків-Жиліна, 2020, с.30.

6. Ibrahimov B. G. Research quality of functioning of the efficiency optical telecommunication systems using spectral technologies / B. G. Ibrahimov, E. G. Hashimov // Проблеми інформатизації : тези доп. 11-ї міжнар. наук.-техн. конф., 16-17 листопада 2023 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Нац. ун-т оборони Азерб. республіки [та ін.]. – Харків : Impress, 2023. – С. 29-30.

RESEARCH OF RECEPTION IMMUNITY IN COMMUNICATION SYSTEM USING MIMO TECHNOLOGY

Ibrahimov B.G. [1, 2], Isayev Y.S. [1, 2]
[1]Azerbaijan Technical University; Baku, Azerbaijan
[2]National Defense University; Baku, Azerbaijan

This article examines the study of the noise immunity of MISO (Multiple-input and single-output) and MIMO (Multiple Input Multiple Output) radio channels with space-time noise-correcting coding.

Here, the main assumptions are the presence of common Rayleigh-type signal fading and additive white Gaussian noise in the communication channel, as well as the presence of a message on the receiving side about complex channel factors [1-7].

It is known that the quality of any communication channel is usually assessed by the totality their properties, determined by the corresponding indicators [1, 2]. One of the main properties radio channels is their noise immunity, assessed by the probability of an error per elementary symbol.

Analytical expressions for determining the probability an error in communication channels depend on the type modulation and the variant of the criterion for making a decision on the transmitted symbol implemented on the receiving side.

Such expressions are known for a number of simple cases.

In certain situations, the assessment of the noise immunity of a channel implementation option in a communication system is carried out using simulation models [1, 2, 3].

A significant complication of expressions occurs when assessing the noise immunity of signal reception in communication channels with fading [1,2, 3].

It is known [1, 2, 3] that the cause of signal fading at the reception point is multipath propagation of radio waves, and this phenomenon is combated by forming a set parallel channels through:

diversity reception (SIMO channels),

diversity transmission (MISO),

or the use of multiple receiving and multiple transmitting antennas (MIMO).

Let additive white Gaussian noise with zero mean and variance act at the input of each receiving antenna, and let the noise parameters σ_n^2 on the time interval $0 \le t \le \tau$ and $\tau \le t \le 2\tau$ be independent and equal.

It is assumed that the mutual arrangement of the transmitting antennas is such that a complete absence of fading correlation is ensured.

The complex channel factors between the transmitting and receiving antennas are known and unchanged over the interval under consideration $0 \le t \le 2\tau$ [2].

For such conditions, analytical expressions were obtained to determine the error probability for the MISO scheme [2, 3]:

$$P_{BER} = 0.5 - 0.5F\left[\sqrt{\frac{4E_S \cdot (1-\rho_S)}{N_0} \cdot (M \cdot \xi)^2}\right], \quad (1)$$

where $N_0 -$ spectral power density of interference; $E_S -$ energy of the transmitted signal via communication channels.

The bit error probability for a system MIMO is expressed as follows [2, 3]:

$$P_{BER} = 0.5 - 0.5F[\sqrt{\frac{2E_S \cdot (1-\rho_S)}{N_0} \cdot (M \cdot \xi)^2}] \ . \quad (2)$$

Formulas (1) and (2) define the parameters of the reception resistance and characterize the quality of the communication systems using technologies MISO and MIMO.

To determine the average probability error for all possible values of the multiplier $(M \cdot \xi)^2$ it is necessary to determine the distribution density of this random variable.

Thus, a comparison of the obtained analytical expressions with known studies allows us to conclude that the introduction of joint diversity of transmitting and receiving antennas using space-time coding increases the diversity factor.

References

1. Sklyar B. Digital communications. Theoretical foundations and practical application, 2nd ed.: trans. from English. M.: OOO ID Williams, 2016. 1104 p.

2. Bayram Ibrahimov. Investigation of Noise Immunity telecommunication systems according to the criterion energy efficiency //Transport and Telecommunication. Vol. 24, no.4, 2023. pp.375 - 384.

3. Biglieri E., Calderbank R., Constantinides A., et. al. MIMO Wireless Communication. U.K, Cambridge: Cambridge Univ. Press, 2007. – 356 P.

4. Hasanov M. H., Ibrahimov B. G., Mardanov N. T. Research and analysis performance indicators NGN/IMS networks in the transmission multimedia traffic //2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). – IEEE, 2019. – C. 1-4.

5. Ibrahimov B. G., Alieva A. A. Research and analysis indicators of the quality of service multimedia traffic using fuzzy logic //International Conference on Theory and Applications of Fuzzy Systems and Soft Computing. – Cham : Springer International Publishing, 2020. – C. 773-780.

6. Ibrahimov B.G. et al. Research throughput multiservice telecommunication networks // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали 10-і міжнародноі НТК, 9-10 квитня 2020. Том1. Баку-Харків-Жиліна, 2020, с.30.

7. Ibrahimov B. G. Research quality of functioning of the efficiency optical telecommunication systems using spectral technologies / B. G. Ibrahimov, E. G. Hashimov // Проблеми інформатизації : тези доп. 11-ї міжнар. наук.-техн. конф., 16-17 листопада 2023 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Нац. ун-т оборони Азерб. республіки [та ін.]. – Харків : Impress, 2023. – С. 29-30.

ANALYSIS OF SOFTWARE-CONFIGURABLE COMMUNICATION NETWORK OPERATION MODEL

Ismayilov T.A.[2], Ibrahimov B.G.[1]
[1]Azerbaijan Technical University; Baku, Azerbaijan
[2]Azerbaijan State Agrarian University; Ganja, Azerbaijan

Currently, due to the rapid development multiservice communication networks based on the architectural concepts of NGN and FN using modern technologies SDN (Software Defined Networking), NFV(Network Functions Virtualization), IoT (Internet of Things), IMS (Internet Protocol Multimedia Subsystem) and wireless communication technologies, multifunctional terminal devices and network resources are becoming increasingly more complex and diverse [1-6].

It should be noted that the development SDN, NFV, IMS and IoT technologies has led to high growth in on-demand multimedia traffic - audio, video and images, which is latency sensitive and requires more bandwidth for multimedia applications.

All this imposes new requirements in terms ensuring quality of service QoS (Quality of Service), QoE (Quality of Experience) and efficient transportation useful and service traffic to multiservice networks with packet switching, taking into account modern trends in the development technologies such as SDN, NFV, IoT, OFDM (Orthogonal Frequency-Division Multiplexing), IMS, MIMO (Multiple Input Multiple Output), and ML (Machine Learning).

One of the key performance indicators of an SDN network is the coefficient effective use network and information resources of multiservice networks based on FN when servicing the $i-$ th stream of a traffic packet and is expressed as follows:

$$\rho_i(H,\lambda_i)=[B_i^{(1)}\cdot f(H)\cdot\lambda_i/(C_{\max}(\lambda_i)\cdot N_k)]\le 1, \quad (1)$$

where $f(H)=2H$ is a function that takes into account the self-similarity property of incoming packets of useful and service traffic; H is the Hurst coefficient for the traffic flow and is equal to $H=1-0,5\beta$, $0<\beta<1$; $B_i^{(1)}-$ average value of service duration packet flows of the $i-$-th traffic; $C_{\max}(\lambda_i)-$the maximum value of the bandwidth switch and controller using the Open Flow protocol, depending on the intensity of the incoming traffic packet flow, is:

$$C_{\max}(\lambda,H)=N_k\cdot\sum_{i=1}^{n}V_{i.k}(b)\cdot K_{i.c}(\lambda_i,H)\ ,\quad i=\overline{1,n}\ , \quad (2)$$

where $K_{i.c}(\lambda_i)-$traffic compression ratio of the $i-$th packet stream $K_{i.c}(\lambda_i,H)\ge 4,...,8.$

Taking into account the informative characteristics source $I(X,Y)$, the bandwidth $C(h,m)$ of the communication channel is expressed as follows:

$$C(h,m) = \max_{p(x)} I(X,Y)/T = \max[V_b(b_i)\cdot(1-\frac{r}{n})], \quad (3)$$

where $T-$ duration of multi-position signal; $r-$ duration of multi-position signal; $V(b_i)-$ bit rate of discrete signals with binary element b_i and is equal to

$$V(b_i) = R_k(1/T)\cdot \ell og_2 m, \quad (4)$$

where R_k- is the code rate and is equal to $R_k = (k/n) < 1$, k and $n-$ are the number of information and general symbols in the code combination, respectively; $m-$ code base or volume of code alphabet.

Expressions (1), (2), (3) and (4) characterize the quality of communication, taking into account the quality of service indicators QoS and QoE.

To effectively organize the management, maintenance and optimization of multiservice networks, it is necessary to use more intelligent data and machine learning technology.

However, in multi-service networks with traditional NGN and FN control architectures, machine learning methods are difficult to apply to control and manage these networks.

The construction of multiservice packet switching networks based on SDN, IMS and NFV has provided new opportunities for intelligent control and management infrastructure.

SDN capabilities such as logically centralized management, global network view, software-level traffic analysis, dynamic updating of forwarding rules, and others facilitate the use of machine learning methods.

References

1. Bayram Ibrahimov. Investigation of noise immunity telecommunication systems according to the criterion energy efficiency//Transport and Telecommunication. Vol. 24, no.4, 2023. pp. 375 - 384.

2. Шелухин О. И., Ерохин С.Д., Полковников МВ. Технологии машинного обучения в сетевой безопасности. М.: Горячая линия – Телеком, 2021. – 360 с.

3. İbrahimov B. et al. Research and analysis indicators fiber-optic communication lines using spectral technologies //Advanced information systems. – 2022. – Т. 6. – №. 1. – С. 61-64.

4. Hasanov A. H., Hashimov E. G. Analysis of the effectivness of communication and automated management systems //Modern directions of development of information and communication technologies and management tools, Abstracts of reports of the 12th Int. Scientific and Technical Conf. – 2022. – Т. 1. – С. 1-4.

5. Ibrahimov, B.G., Hashimov, E.G. Analysis and Selection Performance Indicators Multiservice Communication Networks Based on the Concept NGN and FN // -Kharkiv: Computer and information systems and technologies, -aprel, - 2021. –p.96-98. DOI:https://doi.org/10.30837/csitic52021232904

6. Hasanov M. H. et al. Research and analysis performance indicators NGN/IMS networks in the transmission multimedia traffic //2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). – IEEE, 2019. – С. 1-4.

ANALYSIS OF MULTISERVICE COMMUNICATION NETWORKS OF THE FIFTH AND SUBSEQUENT GENERATIONS

Ibrahimov B.G.[1], Javadova M.M.[2]
[1]Azerbaijan Technical University; Baku, Azerbaijan
[2]Azerbaijan Construction and Architecture University, Baku, Azerbaijan

It is worth noting that in 2012, the ITU-R sector of the International Telecommunication Union launched the IMT for 2020 and beyond research program, which combines research on fifth generation (5G - Generation) communication networks around the world.

In 2015, ITU-R organized the IMT-2020 FG working group and issued Recommendation ITU-R M.2083-0 "IMT Vision – Framework and overall objectives for the future development of IMT to 2020 and beyond." The new networks were called 5G/IMT-2020 [1-6].

They became a new era of services and communication networks, defining an interconnected set of new concepts, technologies and approaches 5G networks are based on two main approaches: ultra-dense communications networks, containing up to 1 million devices per square kilometer, and ultra-low latency networks, which set requirements for round-trip delay of data transmission up to 1 ms.

As a result, ITU-R identified three main services for 5G networks [1]:

- Enhanced mobile broadband;
- Ultra-reliable machine-to-machine communication with ultra-small delays;
- Mass machine-to-machine communication.

A large number of research papers have provided insight into the challenges of building 5G/IMT-2020 networks and systems and have shaped the research direction for future networks. At the same time, in the 5G/IMT-2020 networks under construction, only the first enhanced mobile broadband service has been implemented in practice [2].

In 2018, ITU-T organized the FG NET-2030 working group for the study and standardization of the sixth generation of communication networks - 6G / - NET-2030 or Network 2030.

Therefore, the achieved positive results of the new proposed methods in the development and research models and methods for reducing network traffic delays modern data transfer services and the creation new methods for unique identification of data exchange participants seem relevant.

Taking into account the above tactile Internet and Internet skills, human-machine interaction, telepresence systems and human-controlled avatars, intelligent transport systems and unmanned vehicles - require greater bandwidth, as well as ensuring synchronization and response to events in real time with delays corresponding to the possibilities of perception and reaction of the human body, and in some cases significantly less [1, 2].

In this case, the second factor that unites both the presented promising services and existing communication services is that they must be provided in

accordance with high security requirements, including reliable identification of participants in the service provision process and protection against their substitution.

Thus, an integrated approach is needed that takes into account the main features of the development modern communication networks and new promising services provided to users of these networks, such as high requirements for channel capacity, low data transmission delay, which should not exceed a few milliseconds, increased requirements for the reliability of mutual identification devices exchanging data.

As a result, an important scientific and technical problem arises in creating a methodology for reducing network delays and ensuring reliable identification of participants when transmitting data within various modern communication services.

In this work, in contrast to known approaches to methods for reducing network latency, it offers approaches based on methods for compensating network delay on the user side and a set of network coding and identification methods, including interrelated approaches used at the lower and upper levels of the network model [1, 2].

Thus, the proposed methodology required research and the formation of a logically completed set of all the above approaches.

References

1.Vladimirov S.S. Koucheryavy E.A. Unique Degradation of Flash Memory as an Identifier of ICT Device / // IEEE Access. 2019. Vol. 7. P. 107626-107634.

2.Ibrahimov, B.G., Hashimov, E.G. Analysis and Selection Performance Indicators Multiservice Communication Networks Based on the Concept NGN and FN // -Kharkiv: Computer and information systems and technologies, -aprel, - 2021. –p.96-98. DOI:https://doi.org/10.30837/csitic52021232904

3.Hasanov M. H. et al. Research and analysis performance indicators NGN/IMS networks in the transmission multimedia traffic //2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). – IEEE, 2019. – С. 1-4.

4.Ibrahimov B. G., Alieva A. A. Research and analysis indicators of the quality of service multimedia traffic using fuzzy logic //International Conference on Theory and Applications of Fuzzy Systems and Soft Computing. – Cham : Springer International Publishing, 2020. – С. 773-780.

5.Ibrahimov B.G. et al. Research throughput multiservice telecommunication networks // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали 10-і міжнародної НТК, 9-10 квітня 2020. Том1. Баку-Харків-Жиліна, 2020, с.30.

6.Ibrahimov B. G. Research quality of functioning of the efficiency optical telecommunication systems using spectral technologies / B. G. Ibrahimov, E. G. Hashimov // Проблеми інформатизації : тези доп. 11-ї міжнар. наук.-техн. конф., 16-17 листопада 2023 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Нац. ун-т оборони Азерб. республіки [та ін.]. – Харків : Impress, 2023. – С. 29-30.

METHODS OF CLASSIFICATION AND FORECASTING NETWORK TRAFFIC BASED ON MACHINE LEARNING

Ibrahimov B.G.[1], Rafizade U.R.[2]
[1]Azerbaijan Technical University, Baku, Azerbaijan
[2]Azerbaijan Technology University, Azerbaijan

The dynamic nature user behavior, the exponential growth of data traffic and its variability are associated with the increasing demand for applications that process and manage large volumes of data in real time (DIA). The emergence new technologies such as ML, the continuous evolution of communication standards and the increase in the number of connected terminal devices are turning multiservice telecommunication networks into complex ecosystems that require intelligent management and optimization [1-5]. All of the above speaks to problems that require innovative solutions and a paradigm shift towards intelligent and adaptive approaches.

Given the above, let us consider the use of machine learning in forecasting and classifying network traffic (useful and service types).

One of the important networks - the Internet continues to demonstrate a trend explosive growth - the number connected users, terminal devices and data transfer volumes is increasing exponentially.

ITU-T and ITU-R estimate that there will be 6.54 billion Internet users by 2025, with 27.1 billion devices online in 2024 [1, 2]. Global fixed broadband speeds will reach 110.4 Mbps by 2023, up from 45.9 Mbps in 2018. Modern technologies such as artificial intelligence (AI), ML, LTE, Big Data, the Internet of Things (IoT), intelligent technologies and 5G-NR networks require not only modern technical solutions, but also efficient and programmable control over the communication network [3].

With such scale and growth rates, it is becoming increasingly difficult to maintain effective network interaction, control, manage, monitor, classify and predict traffic in communication networks.

In Rec.Y.3172 [1-3], machine learning is defined as processes that enable computing systems to understand data and extract knowledge from it. The ability to accurately predict network traffic is fundamental to ensuring efficient resource allocation, developing future-proof network architectures, and optimizing quality of service (QoS).

Artificial intelligence (AI) algorithms are able to discern complex patterns and correlations in large and diverse data sets. One of the key elements in Rec.Y.3172 is a machine learning pipeline, which is a set of logical nodes, each with specific functionality, that can be combined to form a machine learning application in a telecommunications network [1].

Based on the above, Figure 1 shows an example of the implementation of a high-level architecture in the IMT-2020 network [2, 3].

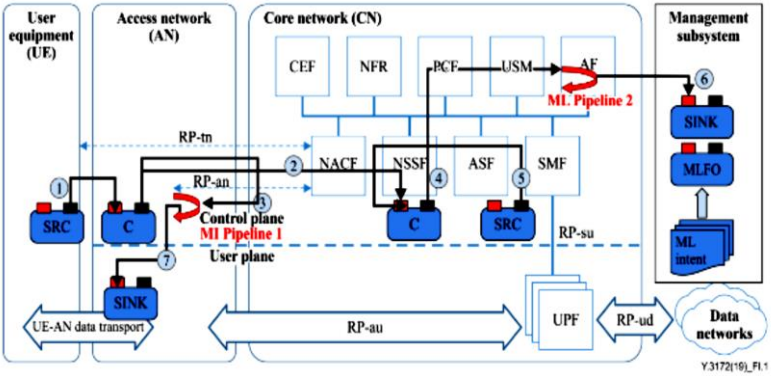


Fig. 1. Structural diagram for the implementation high-level architecture in the IMT-2020 network

From Fig. 1 it is clear that the scheme during implementation is presented as follows: the ML pipeline shows the positions of the ML pipeline nodes, wherever these nodes are located, for example, CN, AN, UE or control functions [3]. By being integrated into the main network management models, the pipeline provides transparent monitoring, traffic classification and control over the functioning of communication systems.

However, traffic forecasting methods can often be applied at different time scales or independent of time: short-term (within minutes, hours and days) or long-term (weeks, months and years) in local and wide area networks.

References

1. Chen A., Law J., Aibin M. A Survey on Traffic PredictionTechniques Using Artificial Intelligence for Communication Networks. Telecom 2021, №2, pp. 518-535.

2. Hasanov A. H., Hashimov E. G. Analysis of the effectivness of communication and automated management systems //Modern directions of development of information and communication technologies and management tools, Abstracts of reports of the 12th Int. Scientific and Technical Conf. – 2022. – T. 1. – C. 1-4.

3. Recommendation Y.3172 «Architectural framework for machine learning in future networks including IMT-2020». ITU-T, Geneva. June 2019.

4. Ibrahimov B.G. et al. Research throughput multiservice telecommunication networks // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали 10-і міжнародної НТК, 9-10 квитня 2020. Том1. Баку-Харків-Жиліна, 2020, с.30.

5. Ibrahimov, B.G. Analysis and Selection Performance Indicators Multiservice Communication Networks Based on the Concept NGN and FN // -Kharkiv: Computer and information systems and technologies, -aprel, - 2021. –p.96-98. DOI:https://doi.org/10.30837/csitic52021232904

6. Hasanov M. H. et al. Research and analysis performance indicators NGN/IMS networks in the transmission multimedia traffic //2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). – IEEE, 2019. – C. 1-4.

RESEARCH OF TRANSMISSION CAPACITY RADIO ENGINEERING SYSTEMS USING MIMO TECHNOLOGY

Ibrahimov B.G.[1], Yakhyaev B.M.[2]
[1]Azerbaijan Technical University; Baku, Azerbaijan
[2]National Aerospace Agency, Baku, Azerbaijan

Conducted studies have shown [1,6] that one of the bottlenecks in organizing communications in radio engineering complexes between users is the throughput of the radio channel. However, in [1,2] it was established that one of the ways to increase the capacity of mobile radio channel systems is to expand its frequency band. However, the radio frequency spectrum resource is limited. To launch a mobile cellular communication system 4G-LTE (Long Term Evolution) and 5G–NR-U (New Radio-Unilence), the operator community speaks of the need to allocate a certain total frequency band.

Let's say for 5G–NR-U a minimum total frequency band of 400 MHz is required, and taking into account the millimeter-upper and decimeter-lower wavelength ranges, it's about 5 GHz [1, 2].

With the constant increase in load on the public telephone network and wireless communication network, it becomes vitally necessary to significantly increase the spectral efficiency and noise immunity of the communication system, reduce the need for scarce frequency resources, reduce the costs of deployment and operation of modern and future communication systems, increase throughput and operational reliability communication systems.

It is known that to calculate the system capacity of radio engineering complexes with one transmitting and one receiving part of the system - the antenna, Shannon's formula is used, which is expressed as follows:

$$C_{\max}(P_S, V_b) = \Delta F_k \cdot \log_2[1 + P_S / (2\sigma_n^2)], \quad (1)$$

where σ_n^2 – is the noise power in the presence of a heterogeneous source of interference, including general fading, and is equal to

$$\sigma_n^2 = \Delta F_k \cdot N_0 \ , \quad (2)$$

ΔF_k – communication channel width, Hs; P_S – power of the transmitted signal through communication channels, Vt; N_0 – is one-sided (at positive frequencies) power spectral density of white noise and is equal to $N_0 = 0.5(NF \cdot G - 1) \cdot (h_0 \cdot f_0)$, (Vt/Hz), NF and G are the noise figure and the gain of the amplifier signals in the demodulator, respectively; h_0, f_o – respectively Planck coefficient and signal frequency [1].

According to formula (1) and (2), it follows that throughput can be increased by improving the communication channel width ΔF_k , increasing signal power P_S and reducing interference power [2].

However, taking into account the above indicators for telecommunication systems, radio engineering complexes and mobile cellular networks with one antenna for both transmission and reception, the increase in throughput is very limited.

One of the effective approaches to increase the throughput of wired communication systems, radio systems and mobile wireless communication networks is the use of multi-antenna transmission technology MIMO (Multiple Input Multiple Output - MIMO). The main difference between this technology and the classical one is the use of several antennas on both the transmitting and receiving sides [1, 2].

Systems radio engineering complexes and wireless communication networks with many transmitting and many receiving antennas provide high spectral efficiency, thanks to spatial multiplexing of signals and spatial diversity of antennas, making it possible to reduce the bit error rate (BER).

However, the complexity of the system and the cost manufacturing radio frequency paths increases noticeably with the increase in the number of active antennas.

It is possible to significantly reduce these costs while maintaining the main advantages multi-antenna systems by using an approach known as antenna switching [1]. A limited number of radio frequency paths can be optimally assigned receiving and transmitting antennas. In this case, antenna switches with losses of about 1.0 dB are used.

At the same time, the noise immunity of the MIMO communication system increases both with an increase in the number of active antennas-radio paths and with an increase in the total number of antennas-passive antennas.

References

1. Бакулин М. Г., Варукина Л. А., Крейнделин В. Б. Технология MIMO: принципы и алгоритмы. – М.: Горячая линия – Телеком, 2014. – 244 с.

2. Бокк Г.О. MIMO: Оптимизация управления числом логических каналов // Электросвязь, 2017. – № 1. – С. 40-44.

3. Ibrahimov B.G. et al. Research throughput multiservice telecommunication networks // Сучасні напрями розвитку інформацийно-комунікаційних технологій та засобів управління. Матеріали 10-і міжнародноі НТК, 9-10 квитня 2020. Том1. Баку-Харків-Жиліна, 2020, с.30.

4. Ibrahimov B. G. Research quality of functioning of the efficiency optical telecommunication systems using spectral technologies / B. G. Ibrahimov, E. G. Hashimov // Проблеми інформатизації : тези доп. 11-ї міжнар. наук.-техн. конф., 16-17 листопада 2023 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Нац. ун-т оборони Азерб. республіки [та ін.]. – Харків : Impress, 2023. – С. 29-30.

5. Ibrahimov B. G. et al. The investigation and evaluation multiservice network NGN/IMS for multimedia traffic //Synchroinfo journal. –2020. –Т.6. –№.3. –С. 10-13.

6. Ibrahimov B. G., Alieva A. A. Research and Analysis Indicators of the Quality of Service Multimedia Traffic Using Fuzzy Logic //Advances in Intelligent Systems and Computing. – 2021. – Т. 1306. – С.773-780.

VISUAL POSITIONING OF THE DRONE IN CONDITIONS OF IMPOSSIBILITY OF USING EXTERNAL NAVIGATION SIGNALS

Hurtovyi O., Yaremenko A.
National Aerospace University "Kharkiv Aviation Institute"
Kharkiv, Ukraine

In recent years, the development of software and components for quadcopters has gained keen interest. Research and development is concentrated in various directions.

The most relevant: reconnaissance, assault, electronic warfare and others. But one of the little-explored directions remains the fully autonomous flight of a copter when GPS or communication with the operator is lost.

The main goal of the report is to clarify the working principle of the algorithm for finding the coordinates of detected objects, and finding their own coordinates during further data processing of several fixed objects.

During the development of the algorithm for finding the coordinates of objects, it became known that there are several methods of calculating possible points of UAV location.

This is primarily related to the number of fixed objects and their data.

Experiments and method analysis have shown that the highest accuracy is achieved when the number of fixed objects is 3 or more. Hence, the lateration principle is used to determine the coordinates of the drone based on measuring the distances from this object to several other landmarks.

Required complete autonomy of the drone, the testing process absolutely does not support a network connection, including GPS data [1].

Calculating the distance to an object detected by the camera using Python programming methods accurately determines its spatial coordinates (X, Y, Z).

After that, equations are calculated to determine your location in three-dimensional space.

Thus, on the basis of geospatial data, a self-positioning system that can work autonomously has been built.

The development was carried out using basic functions for fast data processing, their calculation and optimization of location processes to continue the implementation of the assigned task [2].

References

1. Д.Аверін, В.Боровицький, і В.Микитенко, «СИСТЕМИ ПОЗИЦІОНУВАННЯ ДЛЯ ДРОНІВ, ЯКІ ВИКОРИСТОВУЮТЬ ЦИФРОВІ КАМЕРИ», Bull. Kyiv Polytech. Inst. Ser. Instrum. Mak., вип. 63(1), с. 20–25, Лип 2022.

2. K. Dergachov *et al.*, "GPS Usage Analysis for Angular Orientation Practical Tasks Solving," *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2022, pp. 187-192, doi: 10.1109/PICST57299.2022.10238629.

REGION OF INTEREST SEARCH IN A VIDEO STREAM USING BRIGHTNESS DIFFERENCES MATRIX COMPARISON METHOD

Dergachov K., Ovdiyuk Eu.
National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine

In recent years, the robotics industry has experienced significant growth. The research of methods to find the region of interest (ROI) in a video stream frame is of critical importance in modern aircraft and unmanned aerial vehicles (UAVs) control systems [1]. One of the key metrics for evaluating the effectiveness of search algorithms is the simplicity and speed of computations, which enables the use of simple, reliable, and energy-efficient hardware for light and ultralight aircraft.

The purpose of this report is to describe the solution to the task of identifying the region of interest in a video stream frame, either by a user or automatically, and subsequently tracking the region of interest in the incoming video stream. The report presents the results of measuring the search speed dependency on the size of the sought region, while varying one of the search parameters—the number of pixels (for 5, 10, and 15 pixels) along two axes in different directions. The results of the processing time per frame with a constant size depending on the search area and the size of the sought frame are also shown.

The data presented indicates that the search time increases linearly with the size of the sought region. Similarly, increasing the search area also linearly increases the search time, which is particularly relevant in cases of low bitrate in the incoming video stream or when the object in the region of interest moves quickly across the frame. Further research into the possibility of dynamically adjusting this parameter based on the minimum found absolute difference is recommended.

Additionally, during the analysis of the method and the experiments conducted, an approach to optimize the search time was developed by skipping pixels in the incoming frame until the minimum absolute difference was found, followed by an additional search near the previously skipped coordinates.

The developed method does not use complex computations, making it possible to use low-performance hardware in combination with an optimized search algorithm.

Experiments also demonstrated that the frame resolution, the source of the incoming video stream, and the focus of the object do not significantly affect the accuracy of determining the coordinates of the region of interest.

References

1. Shmelova, T., Sikirda, Y., Rizun, N., Kucherov, D., & Dergachov, K. (2019). Automated Systems in the Aviation and Aerospace Industries.

МОДЕЛЮВАННЯ ПОЛЬОТНИХ ВИПРОБУВАНЬ ПРИ РОЗРОБЦІ СИСТЕМИ ВІЗУАЛЬНОГО НАВЕДЕННЯ БПЛА

Дубінін В.А., Пугач. Д.В., Дергачов К.Ю.
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Системи наведення БПЛА на ворожу ціль є однією з пріоритетних напрямів розвитку сучасного озброєннядля протидії російській агресії. Водночас створення таких систем потребує значних матеріальних ресурсів через регулярні пошкодження та втрати БПЛА під час тестування та налагодження алгоритмів їх керування [1].

Крім того, сам процес вимагає участі операторів для проведення льотних випробувань.

Також, ускладнюючим фактором є необхідність тестування системи в різних умовах навколишнього середовища, таких як недостатня або надмірна освітленість, підвищена хмарність тощо, що впливає на роботу алгоритмів керування [2].

Тому робота над системою моделювання льотних випробувань є важливим науковим завданням для істотного підвищення ефективності розробки систем наведення.

Метою доповіді є створення віртуального середовища, яке дозволить симулювати польотні випробування БПЛА для перевірки ефективності алгоритмів наведення та наддасть детальний звіт про їх роботу на кожному етапі випробування.

В доповіді наводяться результати порівняння ефективності алгоритмів наведення, інформацію про роботу яких було зібрано за допомогою системи моделювання льотних випробувань.

Тестування проводилися за трьох різних умов освітлення та різних траєкторій польоту цілі.

В результаті отримано детальну статистику роботи алгоритмів під час обробки кожного кадру відеопотоку з бортової камери, а саме:

ступінь відхилення від цілі,

точність виявлення та час утримання цілі,

швидкість обробки кадру,

залежність цих показників від умов проведення тестування.

Список літератури

1. A. Kulik and K. Dergachev, "Intelligent transport systems in aerospace engineering," in Intelligent Transportation Systems – Problems and Perspectives, Cham, Switzerland: Springer International Publishing, 2015. 243-303 с.

2. M. Y. Arafat, M. M. Alam, and S. Moh, "Vision-based navigation techniques for unmanned aerial vehicles: Review and challenges," Drones 2023. Т.7, № 2, 89 с

НОВІТНІ ТЕХНОЛОГІЇ ДЛЯ ПІДВИЩЕННЯ СТІЙКОСТІ СИСТЕМ НАВЕДЕННЯ УДАРНИХ БПЛА

Дергачов К.Ю., Кулагін О.К.
Національний аерокосмічний університет імені М.Є. Жуковського
"Харківський авіаційний інститут", Харків, Україна

Аналіз застосування безпілотних літальних апаратів (БпЛА) у війні із російською федерацією показав їх високу ефективність як засобу ураження озброєння та військових обєктів. Широке застосування новітніх технологій суттєво розширюють можливості розвідувально-ударних БПЛА, роблять можливим кероване застосування цілих "роїв" різноманітних БПЛА [1]. Але, ефективність застосування БпЛа суттєво залежить від досвіду оператора та стійкості БпЛА до впливу природних, кліматичних, вибухових, радіоелектронних, електромагнітних та інших факторів. Особливою проблемою для застосування ударних БпЛА є система генерації радіоперещкод навколо об'єкту, що прикривається. Радіус дії таких систем радіоелектронної боротьби зазвичай складає від 100 до 500 м, але цього достатньо, щоб БпЛА був втрачений і не влучив в ціль [2].

Метою доповіді є визначення вимог до сучасних розвідувально-ударних та ударних БпЛА, пошук шляхів вдосконалення їх систем наведення, автозахоплення та супроводження, систем прогнозування траєкторії рухомих цілей і наведення в упереджену точку зустрічі із ціллю, застосування складних систем управління польотом, які комплексують інерційну, супутникову навігаційну та зорово-сенсорну систему наведення з елементами штучного інтелекту.

В доповіді розглядаються нові технологічні тренди для удосконалення спроможностей сучасних високотехнологічних БПЛА. Значна увага приділена використанню технологій штучного інтелекту (Artificial Intelligence, AI), машинного зору (Machine Vision, MV), аналітики великих масивів даних (Big Data), а також новим стандартам високошвидкісного бездротового 5G зв'язку [3].

Список літератури

1. Dale F. Reding, Angelo De Lucia, Alvaro Martin Blanco, Laura A. Regan, Daniel Bayliss. Science & Technology Trends 2023-2043. Across the Physical, Biological, and Information Domains. Volume 1: Overview. March, 2023. NATO Science & Technology Organization, Office of the Chief Scientist, Brussels, Belgium. – 140 c. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf.

2. Dergachov K., Bahinskii S., Piavka I. The Algorithm of UAV Automatic Landing System Using Computer Vision //2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT). – IEEE, 2020. – С. 247-252.

3. John Keller. What 5G means to the military // The Military & Aerospace Electronics, Dec. 2, 2020. URL: https://www.militaryaerospace.com/rf-analog /article/14188341/military-5g-communications

АЛГОРИТМ ВІЗУАЛЬНОЇ НАВІГАЦІЇ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ ПО КЛЮЧОВИМ ТОЧКАМ

Кисельов А.В., Дергачова Д.К., Оніщук Р.І.
Національний аерокосмічний університет імені М. Є. Жуковського
“Харківський авіаційний інститут”, Харків, Україна

В останній час використання безпілотних літальних апаратів (БПЛА) може проходити в складних умовах та відсутності зовнішніх навігаційних сигналів. Одним із шляхів підвищення ефективності використання БПЛА є застосування методів візуальної навігації.

Застосування алгоритмів візуальної навігації БПЛА є особливо ефективним в умовах, коли GPS недоступний або ненадійний, коли потрібна висока точність, а також у закритих або складних для навігації середовищах. Вони дозволяють забезпечити автономність та надійність польотів у реальному часі, навіть за відсутності зовнішніх навігаційних систем.

Основним етапом алгоритмів візуальної навігації є виявлення об'єктів та орієнтирів, завдяки тому, що камери безпілотних літальних апаратів постійно фіксують об'єкти та орієнтири, які можуть бути використані для навігації, спеціальні алгоритми комп'ютерного зору, такі як розпізнавання зображень чи класифікація об'єктів, допомагають БПЛА коригувати курс, орієнтуючись ці об'єкти.

В доповіді запропонований новій алгоритм візуальної навігації БПЛА по ключовим точкам, що відрізняється від відомих наявністю попередньою обробкою візуальних даних та нормалізацію зображення.

Метою доповіді є представлення результатів дослідження, а також нового підходу по вдосконаленню алгоритмів візуальної навігації, заснованого на попередній обробці візуальної інформації та нормалізації зображень.

В доповіді пропонується детальне пояснення запропонованого алгоритму візуальної навігації безпілотних літальних апаратів по ключовим точкам, а також порівняння ефективності його роботи з існуючими алгоритмами на основі аналізу отриманих статистичних даних, а також розглядаються особливості реалізації алгоритму засобами мови Python з ресурсами бібліотеки OpenCV.

Список літератури

1. Shmelova, T., et al. "Automated Systems in the Aviation and Aerospace Industries." (2019).

2. K. Dergachov *et al.*, "GPS Usage Analysis for Angular Orientation Practical Tasks Solving," *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2022, pp. 187-192, doi: 10.1109/PICST57299.2022.10238629.

ОПТИМІЗАЦІЯ ВИКОРИСТАННЯ РЕСУРСІВ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ: НОВІ ТЕХНОЛОГІЇ ТА ПІДХОДИ

Лященко В.О., Гук А.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Оптимізація використання ресурсів у телекомунікаційних мережах стає критично важливою з огляду на зростання обсягів переданих даних і потребу забезпечення високої якості обслуговування користувачів. Сучасні технології, такі як віртуалізація мережевих функцій (NFV) та програмно-визначені мережі (SDN), дозволяють гнучко керувати ресурсами мережі, динамічно їх розподіляючи залежно від поточних потреб. Це дає змогу підвищити ефективність використання пропускної здатності, зменшити затримки та знизити енергоспоживання.[1]

Застосування штучного інтелекту (ШІ) та машинного навчання (МН) у процесах управління мережею дозволяє автоматизувати процеси моніторингу та оптимізації, підвищуючи швидкість прийняття рішень та точність розподілу ресурсів. Алгоритми ШІ можуть аналізувати трафік у мережі в реальному часі та передбачати можливі пікові навантаження, що дозволяє заздалегідь коригувати налаштування мережі для уникнення перевантажень.[2]

Крім того, нові підходи до енергоефективності в телекомунікаційних мережах, такі як використання відновлюваних джерел енергії та енергоефективні апаратні рішення, допомагають знижувати витрати на енергію та мінімізувати екологічний вплив телекомунікаційних систем.[3]

Метою доповіді є огляд сучасних технологій та підходів до оптимізації використання ресурсів у телекомунікаційних мережах, а також аналіз їхньої ефективності в різних сценаріях використання.

Список літератури

1. Дорошевич Н.О. SDN і NFV: Гнучке управління ресурсами телекомунікаційних мереж – Київ: Видавничий дім "Телеком Інновації", 2010. – 342 с.
2. Маслюк В.В. Штучний інтелект у телекомунікаціях: Автоматизація управління та оптимізації – Харків: Видавництво "Цифрові рішення", 2016. – 211 с.
3. Остапов Д.С. Енергоефективність у телекомунікаційних мережах: Новітні технології та рішення – Львів: Інститут телекомунікацій, 2009. – 298 с.

БАЛАНСУВАННЯ НАВАНТАЖЕННЯ В МЕРЕЖІ SDN

Радченко В.О., Кучук Н.Г.
Харківський національний університет радіоелектроніки, Харків, Україна

Розглядаючи балансування навантаження віртуальних машин бачимо, що воно складається з двох частин: обчислення балансування навантаження ресурсів та пошук оптимальних шляхів міграції та скорочення часу

Частина балансування є проблемою пошуку підходящої відповідності Фп. У випадку, якщо мережа знає, що балансує навантаження ВМ. Набори - це набір мігрантів ВМ та набір ФМ призначення. Детальніше про ВМ та ФМ розглянуто в попередньому розділі. Проблема пошуку оптимальних шляхів для всіх міграцій відповідно до часу міграції може бути представлена як проблема багатопотокового потоку з мінімальними витратами [1]. Завданням є пошук шляхів із мінімальними витратами від джерела до місця призначення для кожної міграції, що задовольняє обмеженням.

Було виведено метрики як середнє завантаження фізичних машин, та поріг відхилення (середнє квадратичне відхилення) для кожного типу ресурсів. Як висновок, мінімізація середнього квадратичного призводить до балансування навантаження. Оскільки час необхідний для вирішення таких проблем зростає експоненціально із збільшенням розміру проблеми, було запропоновано використати мурашиний алгоритм для прискорення часу міграції. Був детально розібраний мурашиний алгоритм, всі його переваги та недоліки, та запропоновано покращити даний алгоритм для конкретної ситуації. Написаний псевдокод звичайного мурашиного алгоритму.

Розроблений мурашиний алгоритм для балансування навантаження, де кожна мураха відповідає за пошук плану міграції паралельно для всіх віртуальних машин. Також був написаний псевдокод для даного модифікованого мурашиного алгоритму.

Список літератури

1. Ярошенко Т. О. Дистанційне навчання в системі вищої освіти: сучасні тенденції [електронний ресурс] / Ярошенко Т. О. // Інженерні та освітні технології. – 2019. – Т. 7, № 4. – С. 8-21. – doi.org/10.30929/2307-9770.2019.07.04.01.

УПРАВЛІННЯ НАВАНТАЖЕННЯМ У РОЗПОДІЛЕНИХ СИСТЕМАХ ТА ПАРАДИГМА МОБІЛЬНИХ АГЕНТІВ

Момотов Є., Можаєв О.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Розподіленим системам необхідно виконувати балансування навантаження на своїх хостах, щоб обчислення виконувались якомога швидше. Дослідження у цій галузі показали появу парадигми мобільних агентів як перспективне рішення.

Метою доповіді є дослідження управління навантаженням у розподілених системах. На практиці парадигма використовується, щоб запропонувати підхід до балансування навантаження, яке використовує переваги мобільності агентів, зокрема, на етапі збирання інформації. Необхідно мати загальне системне бачення при одночасному зниженні витрат на мережеву зв'язок, а також інших переваг, таких як відмовостійкість та розширюваність для великомасштабних мереж. Таким чином, мета полягає в

тому, щоб покращити розподіл навантажень збалансованим таким чином, щоб максимально наблизити навантаження до середнього навантаження системи. Результати експериментів показують ефективність запропонованого підходу до балансування навантажень та скорочення часу відгуку.

Тенденція комп'ютерного світу до "розподілених систем" більше не передбачає роботу одного комп'ютера без взаємодії чи співробітництва з іншими комп'ютерами. У доповіді представлені дві взаємопов'язані галузі досліджень: "Мобільні агенти" та "балансування навантаження".

Список літератури

1. Zhou F, Chen Z, Guo S, Li J. Maximizing lifetime of data-gathering trees with different aggregation modes in WSNs. IEEE Sens J. 2016; 16(22):8167-8177.

ПОРІГ ЗАВАДОСТІЙКОСТІ СИСТЕМ ЗВ'ЯЗКУ 5G

Бельорін-Еррера О.М.[1], Чепела С.П. [2]
[1] Національній технічний університет «ХПІ», Харків, Україна
[2] Харківський національний університет радіоелектроніки, Харків, Україна

У системах зв'язку покриття вимірюється максимально допустимими загальними втратами в тракті (Maximum Allowable Path Loss, MAPL), які позначають верхню межу втрат у каналі, при якому забезпечується допустимий рівень відношення потужності прийнятого сигналу до загальної потужності шуму та перешкоди (відношення сигнал-шум-перешкода), Signal-to-Interference-plus-Noise Ratio, SINR), тобто. при якому забезпечується SINR вище порога завадостійкості. На це впливають різні фактори, такі як потужність передачі, коефіцієнт посилення антени, частота, що несе, ширина смуги частот, загальні характеристики системи і продуктивність приймача. Серед перерахованих факторів несуча частота надає прямий і один з найбільш серйозних впливів на загальні втрати в тракті (Pathloss, PL), тому що чим вище частота, що несе, тим вище ослаблення радіосигналу при проходженні через канал зв'язку. У порівнянні з 4G LTE, системи зв'язку 5G стандарту NR працюють на відносно вищій частоті, що несе, в середньочастотному діапазоні.

Таким чином, очевидно, що більш високі втрати потужності сигналу при поширенні в бездротовому каналі ворюють необхідність зниження порога перешкодостійкості системи 5G n для підтримки стабільного обслуговування користувачів на краю осередку стільникових мереж 5G, особливо для типу NSA розгортання.

Досить низький поріг стійкості до перешкод є одним з основних критеріїв, які компанії враховують при розгортанні мереж стільникового зв'язку, оскільки воно безпосередньо впливає на стабільність обслуговування користувачів. Цей показник є ключовим обслуговування голосового зв'язку, тобто найбільш поширеного варіанта використання

систем зв'язку і має особливе значення при комерціалізації систем мобільного зв'язку, і для якого типовий користувач завжди чекає на повсюдне покриття.

Список літератури

1. G. Ermolaev, Advanced Approach for TX Impairments Compensation Based on Signal Statistical Analysis at the RX Side / G. Ermolaev, O. Bolkhovskaya, A. Maltsev // 2021 Wave Electronics and its Application in Information and Telecommunication Systems – 2021 – pp. 1-5 – DOI: 10.1109/WECONF51603.2021.9470687.

ОПТИМІЗАЦІЯ ПЕРЕДАЧІ ДАНИХ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ ДЛЯ СУЧАСНИХ ДОДАТКІВ

Дерев'янко К.А., Гук А.С.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком сучасних додатків, таких як потокове відео, онлайн-ігри та системи реального часу, оптимізація передачі даних у телекомунікаційних мережах стає критично важливою.

Високі вимоги до пропускної здатності, затримки та надійності зумовлюють необхідність удосконалення існуючих алгоритмів та протоколів передачі даних. Важливу роль у цьому процесі відіграють технології 5G, які забезпечують значно вищу швидкість передачі даних і низькі затримки, що дозволяє підтримувати роботу складних додатків із високими вимогами до продуктивності [1].

Одним із ключових підходів до оптимізації передачі даних є використання технологій програмно-визначених мереж (SDN) та віртуалізації мережевих функцій (NFV), які дозволяють динамічно керувати мережевими ресурсами та ефективно розподіляти трафік. Це забезпечує гнучкість та масштабованість мереж, необхідні для підтримки сучасних додатків, що вимагають високої продуктивності. Крім того, впровадження механізмів QoS (Quality of Service) дозволяє гарантувати необхідну якість обслуговування для критично важливих додатків, забезпечуючи мінімальні затримки та безперебійну роботу [2].

Метою доповіді є аналіз сучасних підходів до оптимізації передачі даних у телекомунікаційних мережах для підтримки вимог сучасних додатків, таких як потокові сервіси та додатки реального часу, а також огляд інноваційних рішень, що забезпечують високу продуктивність та надійність мереж.

Список літератури

1. Василюк Д.В. 5G та майбутнє передачі даних: Відповідь на вимоги сучасних додатків" – Київ: Видавничий дім Телеком, 2011. – 325 с.

2. Максименко К.А. SDN та NFV в оптимізації даних: Гнучке управління мережею для високопродуктивних додатків" – Київ: Технічний університет, 2023. – 310 с.

5G МЕРЕЖІ: ПЕРСПЕКТИВИ РОЗВИТКУ ТА ВПЛИВ НА ТЕЛЕКОМУНІКАЦІЙНІ ПОСЛУГИ

Показій К.О., Тимошенко Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

З появою технології 5G телекомунікаційна індустрія вступила в нову еру розвитку, що обіцяє значні зміни в наданні послуг та взаємодії користувачів з мережею. 5G забезпечує набагато вищу швидкість передачі даних, низькі затримки та можливість підключення великої кількості пристроїв одночасно, що відкриває нові можливості для різноманітних додатків та сервісів, включно з Інтернетом речей (IoT) і смарт-містами [1].

Перехід до 5G також впливає на зміну інфраструктури мереж та вимоги до телекомунікаційних операторів, що зобов'язані впроваджувати нові архітектури, такі як програмно-визначені мережі (SDN) і мережі з віртуалізацією функцій (NFV), щоб забезпечити гнучкість і масштабованість. При цьому, послуги, які пропонують оператори, стають більш персоналізованими завдяки можливостям аналітики великих даних і штучного інтелекту, що дозволяє адаптувати мережу під конкретні потреби користувачів і бізнесів [2].

Проте, впровадження 5G також стикається з викликами, серед яких необхідність розбудови щільної мережі базових станцій та інвестицій в модернізацію інфраструктури. Додатково, питання кібербезпеки в 5G стає критичним, оскільки збільшується кількість підключених пристроїв і складність мережевих систем [3–6].

Метою доповіді є аналіз перспектив розвитку 5G технології, її впливу на телекомунікаційні послуги, а також обговорення потенціалу та викликів, з якими стикається індустрія у процесі впровадження нових стандартів зв'язку.

Список літератури

1. Василенко Т.М. Мережі 5G: Новий горизонт для телекомунікацій – Київ: Академія зв'язку, 2021. – 320 с.

2. Остапов Д.В. SDN та NFV: Інструменти трансформації мереж 5G – Київ: Видавничий дім "Телеком", 2023. – 270 с.

3. Бондаренко М.В. Виклики та можливості розгортання 5G: Безпека та інфраструктура – Київ: Технічний університет, 2023. – 290 с.

4 Ismail, S.F., Kadhim, D.J. Towards 5G Technology: Insights into Resource Management for Cloud RAN Deployment. IoT. 2024. Vol. 6, is. 2. Pp. 409–448. DOI: 10.3390/iot5020020

5. Ye, F., Li, J., Zhu, P., Wang, D., You, X. Intelligent Hierarchical NOMA-Based Network Slicing in Cell-Free RAN for 6G Systems. IEEE Transactions on Wireless Communications. 2024. Vol. 23, is. 5. Pp. 4724–4737. Doi: 10.1109/TWC.2023.3321717

6. Chowdhury, M. Campaign: A Personalized Offloading, Semantic Communication, Latency-aware Resource Slicing and SFC Orchestration for SDN and NFV Empowered 6G Serverless Computing Network. IAENG International Journal of Computer Science. 2024. Vol. 51, is. 10. Pp. 1480–1515. URL: https://www.iaeng.org/journals.html

ПОРІВНЯННЯ МЕТОДІВ РОЗРОБКИ МОДЕЛЕЙ СЕРИДОВИЩА ДЛЯ ВИКОРИСТАННЯ В ФУНКЦІОНАЛЬНІЙ ДІАГНОСТИЦІ

Кривицький А.О., Філіппенко І.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Верифікація коректної роботи критичних систем та/або систем що працюють в екстремальних умовах має значний вплив на безпеку і прогнозованість роботи таких систем, що визначає необхідність вирішення задач верифікації їх роботи та запобігання фальсифікації результатів. Одним із методів такої верифікації може бути функціональна діагностика об'єкту в режимі імітаційного моделювання [1].

Імітаційне моделювання потребує розробки моделей і методів імітації середовища роботи діагностованого об'єкту зі ступенем кореляції відповідним до стандартів індустрії, наприклад: DO-178C [2] для програмного забезпечення авіаційного бортового радіоелектронного обладнання або IAEA Safety Standards [3] для обладнання атомних станцій.

Окрім розробки моделей середовища з високою кореляцію до реальних умов необхідно також забезпечити можливість роботи системи верифікації в режимі реального часу.

Метою доповіді є побудова моделі середовища для функціональної діагностики програмно-апаратного комплексу, а саме компоненту бортового обладнання літального апарату відповідно до стандарту DO-178C[2].

В доповіді наводиться аналіз методів розробки моделі, що використовується для імітаційного моделювання програмно апаратної системи.

Також проводиться порівняння моделі розробленої на основі математичного моделювання середовища роботи системи, моделі середовища створеної з запису параметрів реального середовища за допомогою використання системи логування параметрів та спрощеної моделі реального середовища.

Порівняння наведених моделей дає можливість зробити висновок про ступінь кореляції моделей з реальним світом в порівнянні з еталонною моделлю, а також зробити висновок щодо відповідності запропонованих моделей стандартам верифікації що накладаються на зазначений тип програмно-апаратної системи.

Список літератури

1. Law A. Simulation Modeling and Analysis with Expertfit Software. 4th ed. McGraw-Hill Science/Engineering/Math, 2006. 768 p.

2. Brosgol B. Do-178c. *the 2011 ACM annual international conference*, Denver, Colorado, USA, 6–10 November 2011. New York, New York, USA, 2011. URL: https://doi.org/10.1145/2070337.2070341 (date of access: 31.10.2024).

3. Iaea. Safety of Nuclear Power Plants: Design (Safety Standards Series). International Atomic Energy Agency, 2000. 67 p.

АВТОМАТИЗАЦІЯ НАЛАШТУВАННЯ МЕРЕЖНОГО ОБЛАДНАННЯ ЗА ДОПОМОГОЮ ІНСТРУМЕНТУ EXPECT

Кобеляцький В.В., Скорик Ю.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Проведення налаштування та правильне підтримання працездатності мережі є доволі складним завданням. Немає складнощів провести конфігурацію маленької локальної мереіжі, але якщо вона має 100 чи 1000 хостів, то вже потребується багато часу, щоб провести всі налаштування. Налаштування вручну займає доволі багато часу і такі налаштування можуть бути не дуже точними.

На теперішній час за допомогою автоматизації вирішуєть багато завдань. Наразі відомо безліч методів, які написані на різноматних програмних мовах.

За головним показником обирають ступінь розуміння і швидкість роботи.

Тому, одне з завдань для цих методів, це вибір оптимального варіанта, який підходить для кращої автоматичної конфігурації мережного обладнання, наприклад засіб для створення скриптів – Expect.

Expect можна застосовувати окремим додатком, або ж в середині іншої системи.

Метою доповіді є аналіз досліджуваної мережі, її структури та протоколів, які використовуються у мережі. Завдання включає автоматизацію налаштування мережного обладнання для скорочення часу конфігурації мережі, а також використання інструменту Expect для створення скриптів.

У роботі розглянута і проаналізована мережа компанії.

Проаналізовані протоколи для подальшого збільшення відмовостійкості наданої мережі.

Застосовується протокол ERPS, так як він зможе відновити працездатність менше ніж за секунду.

За допомогою засобу Expect був написаний скрипт. Було проведено перевірку працездатності цього скрипта [1-3].

Завдяки представленному скрипту, адміністратор зможе простіше працювати із мережею, так як доволі багато функцій було автоматизовано. Час, необхідний для проведення конфігурування мережного обладнання поменшено з 15 хвилин до 30 секунд.

Список літератури

1. Оліфер В., Оліфер Н. Комп'ютерні мережі. Принципи, технології, протоколи: Ювілейне видання. 2020. 1008 с.
2. Brown James T. The Handbook of Program Management: How to Facilitate Project Success with Optimal Program Management, Second Edition. 2014. 336 p.
3. Libes D. Exploring Expect: A Tcl-based Toolkit for Automating Interactive Programs 1st Edition. 2015. 205p.

АНАЛІЗ МЕТОДІВ МОДУЛЯЦІЇ СИГНАЛІВ У ЦИФРОВИХ СИСТЕМАХ ПЕРЕДАЧІ ДАНИХ

Плех О.А., Скорик Ю.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Забезпечення якісної та надійної передачі інформації у сучасних цифрових телекомунікаційних системах є важливим завданням інженерії сьогодення. Зі збільшенням обсягів інформації, що передається, вимог до швидкості, достовірності та завадозахищеності, виникає потреба у використанні більш досконалих методів модуляції, здатних забезпечити стабільність і високу пропускну здатність каналів зв'язку.

У системах зв'язку важливим завданням є своєчасне і точне виявлення сигналів, що передаються, а також розрізнення їх у середовищі, де можливі перешкоди. Процеси передачі даних вимагають використання гнучких та оптимальних рішень, що дозволяють підібрати найбільш ефективні методи модуляції залежно від умов передачі та типу даних.

Цифрові методи модуляції грають ключову роль у покращенні показників швидкості, завадозахищеності, та достовірності передачі інформації, що забезпечує стабільну роботу сучасних мереж [1].

Метою доповіді є аналіз методів модуляції сигналів у цифрових системах передачі даних для визначення оптимальних параметрів, які підвищують ефективність системи передачі.

У доповіді представлені результати аналізу методів модуляції для цифрових систем передачі даних. Наведені дані показують, що вибір оптимального методу модуляції залежить від умов середовища передачі, таких як рівень завадостійкості, смуга пропускання каналу та енергетичний ресурс системи. АМ/БДС визнана оптимальною для систем, де є обмеження частотного ресурсу, тоді як ортогональна модуляція з когерентною демодуляцією забезпечує кращу ефективність при обмеженому енергетичному ресурсі [2].

Крім того, у випадках, коли передача здійснюється через смугу, обмежену стандартним телефонним каналом, частотна модуляція (ЧМ) забезпечує швидкість до 1200 біт/с. Використання більш високих швидкостей, таких як 9600 біт/с, доцільніше з багатопозиційними методами, такими як АМ-ФМ із когерентною демодуляцією, де 8-позиційна АМ-ФМ має переваги над 8-позиційною ФМ.

Список літератури

1. Безрук В. М. Інформаційні мережі зв'язку : навч. посіб. Ч.1 : Математичні основи інформаційних мереж зв'язку / В. М. Безрук, Ю. М. Бідний, А. В. Омельченко ; МОНМС України, Харк. нац. ун-т радіоелектроніки. – Харків : ХНУРЕ, 2011. – 292 с.

2. Нефедов В. І. Теорія електрозв’язку. Київ : Магнолія, 2018. 495 с. URL: https://web.posibnyky.vntu.edu.ua/firen/6bilynskyj_elektronni_systemy/32.htm

ЛІНІЙНЕ ПРОГРАМУВАННЯ ЯК РІШЕННЯ БАГАТЬОХ ТРАНСПОРТНИХ ЗАДАЧ

Козін А.О., Скорик Ю.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Транспортна задача є однією з найпоширеніших спеціальних задач лінійного програмування, до якої, окрім власне задачі оптимізації транспортних перевезень, зводять задачі з оптимізації маршрутизації обчислювальних і телекомунікаційних мереж, управління капіталом, обслуговування великих систем тощо.

В телекомунікаціях їх використовують для оптимізації розподілу мережевих ресурсів і зменшення витрат на передачу даних. Вони допомагають ефективно спрямовувати трафік між вузлами, мінімізуючи затримки та уникаючи перевантаження каналів. Такі задачі важливі для забезпечення якості обслуговування, особливо у великих мережах із високими вимогами до швидкості та стабільності.

Оптимальні рішення дозволяють балансувати навантаження на маршрутах, що знижує ймовірність збою або простоїв. Лінійне програмування також допомагає при плануванні розширення мережі, забезпечуючи ефективне використання нових ресурсів із мінімальними витратами.

При цьому використовуються математичні моделі, які враховують різні обмеження, такі як пропускна здатність і доступні маршрути [1]. Завдяки цьому забезпечується надійний і стабільний зв'язок навіть при високих навантаженнях.

Метою доповіді є використання в телекомунікаціях задачі лінійного програмування для вирішення багатьох транспортних задач, таких як оптимізація маршрутизації трафіку, розподіл мережевих ресурсів і мінімізація затримок передачі даних [2].

В доповіді наводяться результати розрахунків оптимізації маршрутів трафіку між вузлами мережі. Суть полягає в тому, щоб мінімізувати затримки або максимізувати пропускну здатність, розподіляючи навантаження на різні маршрути. А також, щоб уникнути перевантаження певних сегментів мережі, застосовують транспортні задачі для балансування трафіку. Це дозволило рівномірно розподілити трафік між доступними ресурсами, забезпечуючи стійку роботу мережі.

Лінійне програмування надає інструменти для моделювання цих задач, які можна вирішувати за допомогою спеціалізованих алгоритмів, таких як симплекс-метод або метод гілок та меж.

Список літератури

1. Глушик М. М., Копич І.М., Пенцак О.С., Сороківський В.М. Математичне програмування. 2005. 215 с.

2. Bazaraa Mokhtar S. Linear Programming and Network Flows. 2010. 768 p.

РОЛЬ ПРОГРАМНО-ВИЗНАЧУВАНИХ МЕРЕЖ (SDN) У ЗАБЕЗПЕЧЕННІ ПРОДУКТИВНОСТІ ТА БЕЗПЕКИ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ

Головенко О.О., Харченко Н.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Програмно-визначувані мережі (SDN) – це сучасний підхід до управління мережами, який дозволяє централізовано контролювати мережу за допомогою програмного забезпечення. Це робить мережі більш гнучкими, ефективними та безпечними [1, 2].

Основна ідея SDN полягає в тому, що контрольний рівень мережі відокремлюється від передавального.

Це означає, що всі рішення щодо маршрутизації та управління трафіком приймаються централізовано за допомогою спеціальних програмних контролерів. Це забезпечує просте та гнучке управління мережею, дозволяючи швидко адаптувати її до змінних вимог.

Метою цієї доповіді є порівняльний аналіз можливостей між традиційними мережами та SDN, щоб показати переваги та недоліки кожного підходу в контексті продуктивності та безпеки.

Особливу увагу буде приділено підвищенню рівня безпеки в SDN. Централізоване управління дозволяє швидко впроваджувати політики безпеки та реагувати на загрози.

Контролери можуть автоматично виявляти та запобігати атакам, забезпечуючи високий рівень захисту мережі. Крім того, SDN дозволяє сегментувати мережу, що зменшує ризик поширення загроз. Гнучкість впровадження забезпечується можливістю швидкої адаптації мережі до змінних вимог, що підвищує продуктивність та ефективність управління трафіком [3].

Для демонстрації цих переваг буде розроблено прототип системи на основі SDN, який включатиме створення симулятора або тестового середовища для перевірки розроблених рішень.

Список літератури:

1. Software-defined networking (SDN): визначення й особливості програмно-визначених мереж – Потужна Марія – режим доступу: https://netwave.ua/software-defined-networking-sdn-viznachennya-j-osoblivosti-programno-viznachenih-merezh/

2. Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. Proceedings of the IEEE, 103(1), 14-76.

3. Nunes, B. A. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. IEEE Communications Surveys & Tutorials, 16(3), 1617-1634.

ПРОЕКТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Скорик Ю.В., Бєлих К.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Проектування локальної мережі залишається актуальним сьогодні через зростаючу залежність організацій від цифрових інструментів та мережних ресурсів. Оптимально спроектована локальна мережа забезпечує надійність, швидкість передачі даних, безпеку, а також можливість легко масштабувати та адаптувати мережу під нові потреби бізнесу. Крім того, сучасні тенденції, такі як робота з великими обсягами даних, хмарні сервіси та віддалена робота, підвищують вимоги до якості та стабільності мереж, що робить її ретельне проектування особливо важливим.

Для проектування локальної мережі зв'язку необхідно скласти технічні вимоги для мережі. З властивостей виходять умови, які потрібно враховувати при складанні проекту. Весь процес конструювання починається зі складання технічного завдання. В ньому містяться такі вимоги: норми з безпеки відомостей; забезпечення всім підключеним комп'ютерам доступу до інформації; параметри по продуктивності: час реакції від запиту користувача до відкриття потрібної сторінки, пропускна здатність, тобто обсяг даних в роботі і затримка передачі; умови надійності, тобто готовність тривалої, навіть постійної роботи без перебоїв; заміну комплектуючих - розширення сітки, додаткові включення або монтаж апаратури інший потужності; забезпечення централізованого та дистанційного управління; інтеграцію різних систем і програмних пакетів. Далі обирається вид топології, що буде використовуватися в мережі. Потім потрібно розташувати кабінети працівників та керівництва відповідно до обраної топології. Необхідно обрати протокол, що буде використовуватися на канальному рівні, щоб він міг задовольнити всі технічні вимоги. Та обрати кабель, що буде використовуватися в системі. Потрібно приділити особливу увагу допрограмного і апаратного забезпечення, щоб була можливість модернізації системи та простота її модернізації, це забезпечить високу продуктивність, та можливість в збільшенні потужності мережі.

Метою доповіді є спроектувати локальну мережу для підприємства, проведення аналізу цієї мережі.

У роботі спроектована і проаналізована мережа компанії. Обрана мережна технологія. Обрано тип кабелю для кожної підсистеми мережі. Обрано перелік активного обладнання, необхідного, для розгортання мережі. Виконано побудову віртуальної мережі, відповідної до спроектованої у програмі Cisco Packet Tracer, що допомогає проаналізувати дану мережу.

Список літератури

1. Peterson, Larry L. Computer Networks. 2021. 848 p.
2. Murray B. Computer Networking: The Complete Guide. 2020. 1200 p.

ВДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ КОНТЕНТОМ AEM ДЛЯ РОЗРОБКИ ВЕБСАЙТІВ ТЕЛЕКОМУНІКАЦІЙНИХ КОМПАНІЙ

Чистюк Д.С., Чеботарьова Д.В.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасну епоху цифрових технологій попит на швидкі та надійні телекомунікаційні послуги продовжує зростати. Здатність надавати персоналізований, ефективний і масштабований вебсервіс стає ключовою конкурентною перевагою. Індивідуальний підхід дозволяє збільшити результативність компаній, підвищити продажі та знизити витрати на залучення нових клієнтів. Для досягнення цього важливу роль відіграють системи керування контентом (CMS), що допомагає користувачам створювати, керувати, зберігати та змінювати контент вебсайту. Функціонально CMS поділяється на два основні компоненти: Content Management Application (CMA) і Content Delivery Application (CDA) [1, 2]. CMA забезпечує зручний інтерфейс, що дозволяє користувачам створювати різні типи контенту або змінювати наявний, а CDA відповідає за публікацію цього контенту.

Разом ці компоненти утворюють ядро CMS, яке об'єднує процес управління контентом та його відображення.

Однією з нових потужних та гнучких CMS є Adobe Experience Manager (AEM) [1].

Метою доповіді є вдосконалення системи AEM для розробки вебсайтів телекомунікаційних компаній шляхом створення спеціалізованих компонент .

Незважаючи на те, що AEM пропонує великий набір функціональних можливостей, його конфігурація за замовчуванням часто є загальною, а отже вимагає суттєвих налаштувань та модифікацій для задоволення конкретних потреб.

В роботі проводиться глибоке дослідження та вдосконалення системи управління контентом AEM для потреб телекомунікаційних вебсайтів. Створюються спеціалізовані компоненти, кастомізовані workflow та інші рішення, що спрощують розробку, підтримку та розширюють функціональність CMS.

Таким чином, вдосконаленна платформа AEM дасть можливість телекомунікаційним компаніям створювати функціональні, швидкі та безпечні вебсайти, що відповідатимуть високим стандартам продуктивності та взаємодії з користувачами.

Список літератури

1. What is a content management system (CMS) and how does it work? [Електронний ресурс] // Adobe Experience Cloud Team. – 2024. – Режим доступу до ресурсу: https://business.adobe.com/blog/basics/what-is-a-cms-and-how-does-it-work.

2. What is CMS: Your Essential Guide to Content Management Systems [Електронний ресурс] // scandiweb. – 2024. – Режим доступу до ресурсу: https://scandiweb.com/blog/what-is-cms-guide-to-content-management-systems/.

ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОЇ МАРШРУТИЗАЦІЇ ПОТОКІВ ТРАФІКУ В МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ IP/MPLS

Наливайко В.М., Колтун Ю.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Важливою особливістю сучасних мультисервісних (ММЗ) IP-мереж є підтримка необхідної якості обслуговування (QoS), що у значній мірі реалізується за рахунок забезпечення ефективної маршрутизації потоків трафіку, де одним із рішень виступає використання технології багатопротокольної комутації за мітками (MPLS).

Технологія MPLS здійснює безпечну і ефективну передачу даних і використовується для зменшення часових затримок при передачі пакетів по мережі, управління маршрутизацією трафіку, а також дає змогу використовувати задану маршрутизацію, класифікацію і пріоритезацію трафіку [1].

Метою доповіді є постановка і аналіз задачі по реалізації процесів ефективної маршрутизації потоків трафіку в ММЗ на базі технологій IP/MPLS. Аналіз потоків трафіку в таких мережах проводиться із метою знаходження оптимальних маршрутів, мінімізації їх числа і частки безпосередньо самого трафіку, а також для забезпечення рівномірного розподілу навантаження на основі функцій балансування трафіку [2].

У доповіді наводяться основні поняття, критерії та обмеження для поставленої задачі маршрутизації. Аналізуються питання управління трафіком в ММЗ IP/MPLS із використанням протоколу динамічної маршрутизації OSPF на основі визначення вагових коефіцієнтів ланок виходячи з вимог до пропускної здатності мережі. Вирішується задача оптимального пошуку маршрутів з метою мінімізації максимального завантаження ланки у разі задовільнення вимог до пропускної здатності, кількості переприйомів, з можливістю відключень заданих мережних вузлів та ланок від маршрутів [2]. Показано, що розв'язання цієї задачі ґрунтується на алгоритмі пошуку найкоротшого шляху для вирішення задачі про максимальний потік. Також запропонований підхід, який залежно від стану мережі та інформації про поточні стани маршрутів, дозволяє здійснювати балансування навантаження в ММЗ IP/MPLS з метою запобігання перевантажень.

Список літератури

1. Volodymyr B. Mankovskiy, Oleksandr I. Romanov Service model of the voice traffic in multiprotocol label switching networks [Електронний ресурс] // Information and Telecommunication Sciences, 2013, Volume 4, Number 1. – pp. 33 – 38. – Режим доступу до ресурсу: http://infotelesc.kpi.ua/article/view/30224/26952.

2. *Cerav S. K., Mathar R.* An Off-Line Traffic Engineering Model for MPLS Networks [Електронний ресурс] // Proceedings of the 27th Annual IEEE Conference on Local Computer Networks, 2002. – pp. 166 – 174. – Режим доступу до ресурсу: https://ti.rwth-aachen.de/publications/output.php?id=5&table=proceeding&type=pdf.

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ОПТИМІЗАЦІЇ МЕРЕЖЕВОГО ТРАФІКУ

Гетьман К.Р., Чеботарьова Д.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Зростання обсягів даних та кількості підключених пристроїв у сучасних мережах створює значне навантаження на інфраструктуру, що може призвести до затримок, зниження якості обслуговування та збільшення ризиків перевантаження системи. У зв'язку з цим виникає необхідність впровадження ефективних методів оптимізації мережевого трафіку, які б забезпечували стабільну, швидку та безпечну роботу мереж навіть в умовах високого навантаження. Використання цих методів дозволяє оптимізувати мережевий трафік, а також забезпечити гнучкість і масштабованість інфраструктури.

Метою доповіді є аналіз сучасних методів оптимізації мережевого трафіку, які покращують управління потоками даних для забезпечення стабільності, швидкості та безпеки трафіку в умовах високого навантаження.

Мережі з програмним забезпеченням (Software-Defined Networking, SDN) полегшують організаціям розгортання додатків і забезпечують гнучку доставку, пропонуючи можливість масштабування мережевих ресурсів у відповідності з потребами додатків і даних, а також знижуючи капітальні та операційні витрати. SDN - це інноваційний підхід до проектування, впровадження та управління мережами, який розділяє управління мережею і процес пересилання для покращення взаємодії з користувачем [1].

Мережа доставки контенту (Content Delivery Network, CDN) - це мережа серверів, які кешують або зберігають вебконтент та інтелектуально доставляють його користувачам на основі їхнього географічного розташування. Коли користувачі запитують контент, запит перенаправляється на найближчий сервер CDN. Ці CDN-сервери, як правило, розміщені у провайдерів, з якими CDN має альянси [2].

Сучасні методи оптимізації мережевого трафіку, такі як SDN та CDN, значно підвищують ефективність та гнучкість мережевої інфраструктури. Ці технології дозволяють забезпечити стабільну роботу мережі навіть при високому навантаженні, що є ключовим у сучасному цифровому середовищі.

Список літератури

1. Benzekki, K., El Fergougui, A., and Elbelrhiti Elalaoui, A. (2016) Software-defined networking (SDN): a survey. *Security Comm. Networks*, 9: 5803–5833. doi: 10.1002/sec.1737.

2. M. Ghaznavi, E. Jalalpour, M. A. Salahuddin, R. Boutaba, D. Migault and S. Preda, "Content Delivery Network Security: A Survey," in IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2166-2190, Fourthquarter 2021, doi: 10.1109/COMST.2021.3093492.

АРХІТЕКТУРА ІНТЕЛЕКТУАЛЬНОЇ ОРКЕСТРАЦІЇ ХМАРНИХ ОБЧИСЛЕНЬ В СЕРЕДОВИЩІ ТАКТИЛЬНОГО ІНТЕРНЕТУ

Ярошевич Р., Ситник О.В., Коваленко А.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Тактильний Інтернет сприяє розвитку різноманітних застосунків, які характеризуються складністю, обчислювальними навантаженнями та низькими вимогами до затримок. Перенесення обчислень до границі мережі допомагає знижувати затримки, але потребує інтелектуального керування через обмежені ресурси та вимоги до безпеки і надійності [1]. Оркестрація, керована штучним інтелектом (ШІ), стає ключем до підвищення продуктивності таких систем. Методи машинного навчання можуть динамічно розподіляти та координувати ресурси в розподіленій граничній інфраструктурі.

Метою доповіді є побудова у архітектуру інтелектуального керування хмарними обчисленнями, яка має на меті розширити існуючі платформи керування на границі мережі, за рахунок інтеграції можливостей інтелектуальної оркестровки. Це значно зменшить затримки завдяки обробці даних ближче до джерела, забезпечуючи швидший час відгуку для додатків, підвищить енергоефективність, мінімізуючи передачу даних між центральними хмарами і кінцевими пристроями, що сприяє підвищенню стійкості комп'ютерної мережі. Оркестрування передбачає інтелектуальне та автоматизоване забезпечення, конфігурацію, координацію та відстеження стану ресурсів, та реагування на події, а також прийняття оптимальних рішень щодо, наприклад, планування, розміщення, міграції або консолідації, на основі різних критеріїв оптимізації. Архітектура складається з трьох рівнів:

- вузли граничних обчислень – обробляють дані на границі мережі для швидко реагувати на запити користувачів і зниження затримки в мережі;
- хмарний рівень – централізований рівень для масштабування і координації ресурсів в різних частинах мережі, який зберігає велику кількість даних і забезпечує потужні обчислювальні можливості для складних завдань, що надходять із граничних вузлів;
- рівень оркестрації, керований штучним інтелектом – використовує алгоритми ШІ для оптимізації ресурсів у режимі реального часу.

Оптимальний розподіл ресурсів у хмарних обчисленнях є важливою проблемою, яку необхідно вирішити, щоб максимізувати використання інфраструктури, за умови дотримання певних вимог до продуктивності або часу відгуку додатків, узгоджених з користувачами.

Список літератури

1. А. А. Коваленко, Р. О. Ярошевич, Моделювання передтуманних обчислень для тактильного Інтернету. Вісник ВПІ, вип. 1, с. 65–73, Лют. 2024. – https://doi.org/10.31649/1997-9266-2024-172-1-65-73

МЕТОДИ АДАПТАЦІЇ ПРОТОКОЛУ TCP ДО ПОТОЧНОГО МЕРЕЖЕВОГО СТАНУ

Козін М.В., Сокирко М.А., Янковський О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Обсяг даних, що передається в мережі, постійно зростає і може викликати багато проблем, одна із яких називається перевантаженням мережі (Network Cognestion). Перевантаження мережі – це стан мережі, при якому вузол або канал передають так багато даних, що це може погіршити якість мережевих послуг та призводить до затримки в чергах пристроїв, втрати пакетів даних і блокуванню нових з'єднань [1].

Протокол керування передачею (TCP) розроблено для надійної передачі даних через Інтернет. На продуктивність TCP дуже сильно впливають його алгоритми контролю перевантажень, які обмежують обсяг трафіку, який відправник може передати на основі наскрізних оцінок доступної ємності мережі [2]. Протокол TCP, незважаючи на свою ефективність для забезпечення стабільності трафіку, має суттєві обмеження при роботі з програмами, які генерують дані змінними порціями (пакетний трафік) [3]. Стандартні алгоритми TCP не дозволяють таким програмам ефективно використовувати пропускну здатність мережі, особливо на довгих маршрутах з великим RTT, що може призводити до неефективного використання мережевих ресурсів та знижує загальну продуктивність мережі.

Метою доповіді є аналіз різноманітних причин неефективної роботи TCP з пакетним трафіком та виявлення методів, які дозволять програмам більш ефективно використовувати мережеві ресурси. Проведено детальний аналіз роботи стандартних алгоритмів TCP з пакетним трафіком. Було виявлено, що основною причиною неефективності є нездатність алгоритмів швидко адаптуватися до змін у поточному мережевому стані.

В доповіді розглянуті алгоритми, які дозволяють таким програмам з пакетним трафіком швидко адаптуватися до змін мережевих умов та ефективно використовувати доступну пропускну здатність. Доповідь спрямована на визначення переваг та недоліків існуючих алгоритмів, що надає змогу визначити найбільш перспективні напрями їх розвитку.

Список літератури

1. Biswas, Md Israfil. "Internet congestion control for variable-rate TCP traffic." Thesis, University of Aberdeen, 2011.

2. Amit Aggarwal, Stefan Savage, and Thomas Anderson. "Understanding the Performance of TCP Pacing", March 30, 2000, IEEE InfoCom 2000.

3. Mohd Murtadha Mohamad, Mudassar Ahmad, Md Asri Ngadi "Experimental evaluation of TCP congestion control mechanisms in short and long distance networks", Journal of Theoretical and Applied Information Technology 71(2):153-166, 2015

УПРАВЛІННЯ ЧЕРГАМИ МАРШРУТИЗАТОРІВ

Біленко М.К., Бочко В.О., Партика С.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Схеми активного управління чергами маршрутизаторів (AQM) використовуються для забезпечення якості обслуговування (QoS) у телекомунікаційних мережах. Однак вони чутливі до налаштувань параметрів і мають слабкі сторони у виявленні та контролі перевантаження в умовах динамічно змінюваних мережевих станів [1].

Ще одним недоліком алгоритмів AQM є те, що вони застосовуються лише до марковських моделей мереж, які вважаються моделями трафіку з короткостроковою залежністю (SRD) [2]. Однак вимірювання трафіку в комунікаційних мережах показали, що мережевий трафік може мати властивості самоподібності, а також довгострокової залежності (LRD). Тому важлива розробка нових алгоритмів не тільки для контролю перевантаження, але й для здатності передбачати початок перевантаження в мережі [3].

Метою доповіді є огляд нових методів контролю перевантаження комунікаційних мереж, які використовують різні характеристики трафіку, такі як довгострокова залежність (LRD), що раніше не використовувалися в методах контролю перевантаження.

Розглянуто важливу проблему дотримання обмежень QoS, таких як середня затримка, що є надзвичайно важливим для забезпечення задовільної передачі даних у реальному часі через мультисервісні мережі, такі як Інтернет, які спочатку не були призначені для цієї мети. Запропоновано алгоритм для забезпечення стратегії управління буфером із застосуванням рухомого порогу довжини черги. Алгоритм дозволяє контролювати середню затримку пакетів шляхом динамічного регулювання порогу.

В доповіді також розглянуті алгоритми, здатні не тільки контролювати перевантаження, але й передбачати його початок, що є важливим для забезпечення якості обслуговування у динамічно змінюваних мережевих ситуаціях.

Список літератури

1. Zadeh H. Y., Habibi A., Jafarkhani H., Bauer C. “Optimal Statistical Tuning of the RED parameters,” in Proceedings of IEEE ICC, pp. 27-32, Beijing, China, May 2008.

2. W. Chen, Y. Li, and S. H. Yang, “An average queue weight parameterization in a network supporting TCP flows with RED,” in Proceedings of the 2007 IEEE International Con- ference on TuesM02 Networking, Sensing and Control, pp. 590–595, London, UK, April 2007.

3. Z. H. A. O. Yu-hong, Z. H. E. N. G. Xue-feng and T. U. Xu-yan, “Research on the improved way of RED algorithm S-RED,” International Journal of u-and e-Service, Science and Technology, vol. 9, no. 2, pp. 375–384, 2016.

МЕТОДИ КОНТРОЛЮ ПЕРЕВАНТАЖЕННЯ В БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ

Боклаг Л.О., Москвіна О.Л., Коротич А.Ю., Партика С.О.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком безпровідних мереж, сенсорні мережі (WSN) стають основою багатьох застосувань, від моніторингу навколишнього середовища до захисту критичної інфраструктури. Характер застосування мереж WSN, обмеження ресурсів, кількість розгорнутих датчиків і високий трафік сенсорних вузлів призводять до перевантаження в цих мережах.

Контроль перевантаження стає ще більш складним для WSN через обмежені ресурси щодо обробки інформації, зберігання, можливостей передачі та, що найважливіше, ресурсів джерела живлення. Перевантаження виникає головним чином, коли вимоги до мережі перевищують доступні ресурси, що призводить до зниження продуктивності та надійності, тому стає необхідністю вирішувати цю проблему оптимальним чином, щоб подовжити термін служби мережі. Як правило, WSN призначені для дуже гнучкої та періодичної роботи в важкодоступних середовищах, і передбачається, що вони будуть працювати з мінімальним ручним втручанням. Отже, мережі такого типу повинні бути самовідновлюваними і стійкими до відмови [1].WSN повинні бути надійними, і на додаток до стійкості у разі збою вузла, WSN також мають бути стійкими до зовнішніх перешкод. Оскільки ці мережі часто співіснують з іншими безпровідними системами, вони повинні мати можливість відповідним чином адаптувати свою поведінку. Використання зв'язку з розширеним і багатоканальним спектром може значно підвищити стійкість до зовнішніх перешкод [2].

Метою доповіді є аналіз основних механізмів контролю перевантаження у безпровідних сенсорних мережах, зосередження уваги на їх класифікації та виявленні найбільш поширених рішень, які можуть покращити продуктивність і надійність мереж. Особлива увага приділяється огляду чинників, що спричиняють перевантаження. Розглядаються різноманітні стратегії, що забезпечують ефективність роботи WSN та підкреслюється важливість постійного вдосконалення механізмів контролю перевантаження в умовах швидко змінюваного середовища функціонування.

Список літератури

1. Rezaee A., Yaghmaee M., Rahmani A. HOCA: Healthcare Aware Optimized Congestion Avoidance and control protocol for wireless sensor networksю. Journal of Network and Computer Applications. Volume 37, January 2014, Pages 216-228.

2. Angulara M.; Bala M.; Khullar V. A Survey on Various Congestion Control Techniques in Wireless Sensor Networks. IJRITCC 2022, 10(8); DOI: https://doi.org/10.17762/ijritcc.v10i8.5667.

АКТИВНЕ УПРАВЛІННЯ ЧЕРГАМИ ДЛЯ ПІДТРИМКИ TCP-ПОТОКІВ ІЗ ВИКОРИСТАННЯМ СПОСТЕРІГАЧА ЗБУРЕНЬ ТА ПРЕДИКТОРА СМИТА

Бойко М.Г., Мукановський Я.В., Партика С.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Протокол керування передачею (TCP) використовується для підтримки Інтернет-з'єднань завдяки його високій надійності. Проте, зростання обсягу TCP-потоків призводить до переповнення черг маршрутизаторів. Коли буфер маршрутизатора заповнюється, усі нові пакети, що надходять, відкидаються, доки не з'явиться місце у черзі. Втрата пакета сигналізує про перевантаження, відправник зменшує своє вікно передачі і таким чином знижує швидкість відправки пакетів [1,2], що може викликати явище глобальної синхронізації та привести до зниження пропускної здатності мережі. Для запобігання цьому, використовуються методи активного управління чергами (AQM) [3], які скидають пакети ще до переповнення буфера, запобігаючи затримкам та глобальній синхронізації.

При управлінні перевантаженням в AQM виникає проблема впливу похибок та затримки передачі (RTT) [4]. Деякі методи компенсують або затримку, або похибку, але не обидві одночасно [5].

Метою доповіді є огляд методу управління перевантаженням TCP/AQM, який використовує спостерігач збурень і предиктор Смита (SP). SP ефективно компенсує затримку, але не враховує зміни параметрів мережі. Для управління змінами параметрів використовується спостерігач збурень. Розглянутий метод об'єднує спостерігач збурень і SP та покращує TCP/AQM при великих значеннях RTT.

Метод спрямований на підвищення пропускної здатності мережі і стабілізацію довжини черги, що покращує ефективність передачі даних у мережі навіть за умов високого навантаження.

Список літератури

1. V. Jacobson, ‘‘Congestion avoidance and control,’’ ACM SIGCOMM Comp. Commun. Review, vol. 18, no. 4, pp. 314–329, Aug. 1998.

2. S. Low, F. Paganini, and J. Doyle, ‘‘Internet congestion control: An analytical perspective,’’ IEEE Cont. Sys. Mag., vol. 22, no. 1, pp. 28–43, Feb. 2002.

3. W. Lautenschlaeger and A. Francini, ‘‘Global synchronization protection for bandwidth sharing TCP flows in high-speed links,’’ in Proc. 16th IEEE Int. Conf. High Perform. Switching Routing (HPSR), Jul. 2015, pp. 1–8.

4. X. Chen, S. Wong, and C. K. Tse, ‘‘Adding randomness to modeling Internet TCP-RED systems with interactive gateways,’’ IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 57, no. 4, pp. 300–304, Apr. 2010.

5. S. K. Mohapatra, S. K. Bisoy, and P. K. Dash, ‘‘Stability analysis of active queue management techniques,’’ in Proc. 1st Int. Conf. Man Mach. Interfacing (MAMI), Dec. 2015, pp. 1–6.

МЕТОДИ БУФЕРИЗАЦІЇ ПАКЕТІВ В МАРШРУТИЗАТОРАХ IP-МЕРЕЖ

Вірко А.О., Пилипенко А.О., Янковський О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Буферизація пакетів – це фундаментальний механізм, що лежить в основі функціонування сучасних IP-мереж. Він забезпечує плавну передачу даних навіть за умов змінного навантаження та різноманітних затримок у мережі. Маршрутизатор, як ключовий елемент мережі, активно використовує буфери для тимчасового зберігання пакетів, що очікують на обробку або передачу [1].

Необхідність буферизації обумовлена різницею в швидкостях передачі даних між різними сегментами мережі, випадковими затримками в каналах зв'язку, а також необхідністю обробки пакетів у маршрутизаторах. Буфери дозволяють згладжувати піки навантаження, уникати втрати пакетів та забезпечують стабільну роботу мережі.

Коли пакет надходить в маршрутизатор, він поміщається в приймальний буфер, де чекає своєї черги на обробку.

Далі, маршрутизатор визначає найкращий шлях для передачі пакету до місця призначення і відправляє його.

Цей процес може бути ускладнений різними факторами, такими як затримками в мережі, різними швидкостями передачі даних та зміною в завантаженні мережі.

Саме тут і проявляється важливість буферизації [2, 3].

Метою доповіді є аналіз сучасних методів буферизації пакетів в маршрутизаторах IP-мереж, порівняння їх ефективності в умовах різного навантаження та вимог до якості обслуговування, а також огляд перспектив застосування нових технологій, таких як машинне навчання, для оптимізації процесів буферизації.

Особлива увага в доповіді приділена впливу алгоритмів буферизації на затримку пакетів, джиттер, втрату пакетів та загальну пропускну здатність мережі.

Крім того, приведено порівняльний аналіз традиційних алгоритмів (FIFO, WFQ, RED) та сучасних адаптивних методів, заснованих на машинному навчанні.

Список літератури

1. Wetherall D. Computer Networks, EBook Subscription, Global Edition. 5-те вид. Pearson Education, Limited, 2021. 947 с.

2. M. Welzl, Network Congestion Control: Managing Internet Traffic, p. 282, Wiley, Hoboken, NJ, USA, 2005.

3. Kurose J. F. Computer Networking: A Top-Down Approach. 7-ме вид. Pearson Education, Limited, 2016. 864 с.

АЛГОРИТМИ AQM ДЛЯ БОРОТЬБИ З ПЕРЕВАНТАЖЕННЯМ

Крилов М.В., Димчук М.І., Бородай В.Р., Єрошенко О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі, де безперервний потік інформації є невід'ємною складовою функціонування різноманітних систем зв'язку, управління чергами маршрутизаторів набуває особливої актуальності. Широке поширення комп'ютерних мереж є наслідком багатьох факторів, а підключені до них користувачі створюють велике навантаження на мережеві ресурси та пристрої [1,2]. В результаті кількість даних, що передаються через мережеві пристрої, такі як комп'ютери та маршрутизатори, значно збільшується.

Перевантаження відіграє помітну роль у погіршенні продуктивності мереж, збільшує затримку в чергах маршрутизаторів, викликає втрати пакетів і зменшує кількість пакетів, переданих до місця призначення. Для подолання такої проблеми, було розроблено та вдосконалено багато алгоритмів активного керування чергами (AQM) з метою виявлення перевантаження на ранній стадії та покращення продуктивності мереж [3]. Незважаючи на те, що ці алгоритми мають великий вплив на зменшення затримок, вони мають деякі обмеження. Майже всі вони потребують адаптації до специфіки мережі та не завжди підходять для динамічних умов функціонування [4].

Метою доповіді є порівняння алгоритмів активного управління чергами (AQM) у маршрутизаторах, їх вплив на ефективність та стабільність мережевих з'єднань.

У доповіді розглядаються основні алгоритми AQM, їх вплив на затримки, пропускну здатність та втрати пакетів, а також їх застосування в сучасних мережах. Кожен з цих алгоритмів має унікальні механізми для забезпечення стабільної якості обслуговування і ефективного використання мережевої смуги пропускання.

Представлено модифікований алгоритм управління чергою маршрутизатора, який дозволяє зменшити середню довжину черги та значно підвищує мережеву продуктивність у порівнянні з іншими алгоритмами.

Список літератури

1. Welzl, M. Network Congestion Control: Managing Internet Traffic, 1st ed.; Wiley: Hoboken, NJ, USA, 2005; pp. 10–12.

2. Baklizi, M.; Ababneh, J. A Survey in Active Queue Management Methods According to Performance Measures. Int. J. Comput. Trends Technol. 2016, 38, 145–152.

3. Khatari, M.; Samara, G. Congestion control approach based on effective random early detection and fuzzy logic. MAGNT 2015, 3, 180–193.

4. Baklizi, M.; Ababneh, J.M.; Abdallah, N. Performance investigations of flred and agred active queue management methods. In Proceedings of the Academicsera 13th International Conference, Istanbul, Turkey, 23–24 February 2018; p. 14.

КОМПЛЕКСНА БОРОТЬБА З ПЕРЕВАНТАЖЕННЯМ В IP-МЕРЕЖАХ

Соколовський С.О., Афанков М.В., Ключка М.І., Янковський О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Одним із ключових механізмів запобігання мережевим перевантаженням є TCP (Transmission Control Protocol). TCP використовує алгоритм AIMD (Additive Increase, Multiplicative Decrease), який знижує швидкість передачі даних у разі виявлення втрат пакетів.

Серед новітніх підходів виділяють TCP Cubic та BBR (Bottleneck Bandwidth and Round-trip propagation time), що адаптовані до сучасних вимог мереж. TCP Cubic завдяки нелінійному приросту вікна передачі швидше відновлює швидкість після зниження пропускної здатності, тоді як BBR орієнтується на пропускну здатність каналу, що дозволяє оптимально використовувати доступні ресурси [1, 2].

Для подальшого зниження затримок та уникнення переповнення черг у маршрутизаторах широко використовуються алгоритми AQM, що активно керують чергами пакетів. Один з ранніх, але популярних алгоритмів, Random Early Detection (RED), випадково відкидає пакети при високому завантаженні черги, сприяючи уникненню її переповнення. Інноваційні алгоритми такі, як CoDel (Controlled Delay) і PIE (Proportional Integral Controller Enhanced), забезпечують динамічне регулювання, враховуючи рівень затримки в черзі. CoDel забезпечує контроль затримки без необхідності налаштування порогів довжини черги, а PIE пропонує контроль відкидання пакетів, що знижує вплив затримок та сприяє стабільності трафіку [3, 4].

Метою доповіді є аналіз сучасних методів для зниження перевантажень в комп'ютерних мережах, зокрема різновидів протоколу TCP та алгоритмів активного управління чергами (Active Queue Management, AQM), які сприяють стабільності передачі даних та зменшують затримки.

Таким чином, комплексне поєднання технологій, таких як, сучасні версії TCP та алгоритми AQM, забезпечує ефективну боротьбу з перевантаженнями, покращуючи продуктивність і надійність комп'ютерних мереж.

Список літератури

1. Ha, S., Rhee, I., & Xu, L. (2008). CUBIC: A new TCP-friendly high-speed TCP variant. *ACM SIGOPS Operating Systems Review*, 42(5), 64-74.

2. Cardwell, N., Cheng, Y., Gunn, C. S., Yeganeh, S. H., & Jacobson, V. (2016). BBR: Congestion-based congestion control. *Communications of the ACM*, 60(2), 58-66.

3. Nichols, K., & Jacobson, V. (2012). Controlling Queue Delay. *Communications of the ACM*, 55(7), 42-50.

4. Pan, R., Natarajan, P., Baker, F., & Prabhu, G. (2013). PIE: A lightweight control scheme to address the bufferbloat problem. *IEEE 14th International Conference on High Performance Switching and Routing (HPSR)*, 148-155.

ПРОПОЗИЦІЇ ЩОДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ СИСТЕМ РАДІОЗВ'ЯЗКУ ТА РАДІОЛОКАЦІЇ ВІД АКТИВНИХ ЗАВАД

Кузнєцов О.Л., Нос А.І., Болбас Ю.О.
Харківський національний університет Повітряних Сил
імені Івана Кожедуба», Харків, Україна
Коломійцев О.В.
Національний технічний університет
«Харківський політехнічний університет», Харків, Україна

Вплив тропосферних неоднорідностей та підстильної поверхні у багатьох випадках визначає ефективність функціонування систем радіозв'язку та радіолокації. Зокрема, флуктуації фронту завадових хвиль, що виникають внаслідок цього впливу, призводять до зниження завадозахищеності багатоканальних цифрових систем радіозв'язку і радіолокації.

Таким чином, підвищення ефективності захисту систем радіозв'язку від активних завад є актуальним науково-технічним завданням.

Метою доповіді є представлення результатів оцінки можливості підвищення ефективності захисту систем радіозв'язку та радіолокації від активних завад.

У доповіді проведено аналіз залежності коефіцієнта подавлення активної завади від ступеня впливу фазових флуктуацій в елементах приймальної апертури при фіксованих значеннях відхилень кута приходу завади від напрямку максимуму бічної пелюстки діаграми спрямованості антени та від розмірів і рознесення фазових центрів основної та допоміжної антен системи радіозв'язку або радіолокації. Визначено умови найкращого подавлення активної завади в системах радіозв'язку. Надано пропозиції щодо врахування впливу флуктуацій фазового фронту хвилі активної завади при її компенсації в системах радіозв'язку і радіолокації.

Список літератури

1. Карлов В.Д., Родюков А.О, Пічугін І.М. Статистичні характеристики радіолокаційних сигналів відбитих від місцевих предметів в умовах аномальної рефракції. *Наука і техніка Повітряних Сил Збройних Сил України*. – 2015. – Вип. 4 (21). – С. 71-74. http://nbuv.gov.ua/UJRN/Nitps_2015_4_19.

2. Karlov V., Kuznietsov O., Kolomiitsev O., Krasnoshapka I., Petrushenko I., Strutsinskiy O. Можливості врахування впливу тропосфери при вимірюванні кутових координат та висоти аеродинамічного об'єкта. *Системи управління, навігації та зв'язку*. – 2022. – Т. 3 (69). – С. 121-127. doi:https://doi.org/10.26906/SUNZ.2022.3.121.

3. Карлов В.Д., Кузнєцов О.Л., Бєлоусов В.В., Тузіков С.А., Олещук М.М., Петрушенко В.М. Точність вимірювання кутових координат аеродинамічних об'єктів в умовах тропосферної рефракції. *Системи управління навігації та зв'язку*. – 2021. – № 1(63). – С. 146-152. https://journals.nupp.edu. ua/sunz/issue/view/74/41.

A STUDY ON REAL-TIME NOISE SUPPRESSION AND ECHO CANCELLATION IN WEBRTC USING CONVOLUTIONAL NEURAL NETWORKS

Minglei Zhou, Nina Kuchuk
National Technical University «KhPI», Kharkiv, Ukraine

One very important challenge arises when real-time voice applications, including teleconferencing and VoIP, use WebRTC-based solutions, which is dealing with acoustic echo and ambient noise, thus directly affecting speech clarity and the overall user experience. Acoustic echo comes through feedback when the sound from the loudspeaker gets picked up by the microphone, therefore degrading the conversation quality.

While classical AEC algorithms, such as AEC3 from WebRTC, have been very effective in canceling linear echo for many situations, they typically perform poorly against nonlinear distortions introduced by hardware and cannot handle double-talk situations where both near-end and far-end speakers are talking simultaneously.

Recent works have demonstrated the promise of using convolutional neural networks with the rise of deeplearning: it learns intrinsic signal patterns, hence can make a better prediction of the echo behavior in an AEC system. However, most of these deep learning-based solutions are computation-intensive and hence not practical for real-time applications on devices with limited processing capabilities such as smartphones and other embedded systems.

This paper presents an advanced noise and echo suppression system, which enhances the capabilities of AEC3 in WebRTC by leveraging deep learning to overcome some of its shortcomings.

It utilizes Melspectrogram features, which do indeed offer a frequency representation of audio that matches quite well with human auditory perception. It also applies MobileNetV3, an extremely efficient CNN architecture for the improvement of noise suppression and echo cancellation performances.

Depthwise separable convolutions and attention mechanisms are utilized in MobileNetV3 for the model to pay its attention to the most informative parts of the audio signal, leading to high accuracy without increasing computational demands.

References

1. Abhishek Deb, Asutosh Kar, and Mahesh Chandra, “A technical review on adaptive algorithms for acoustic echo cancellation,” in International Conference on Communication and Signal Processing. IEEE, 2014, pp. 041–045.

2. Guillaume Carbajal, Romain Serizel, Emmanuel Vincent, and Eric Humbert, “Multiple-input neural network-based residual echo suppression,” in ICASSP IEEE, 2018, pp. 231–235.

CHARACTERISTICS OF MAIN SERVICES IN 5G/6G NETWORKS

Shefer Oleksandr, Myhal Stanislav
National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine

Latency is critical in modern applications such as healthcare, autonomous driving, smart homes, and smart industries. These applications require ultra-high reliability, high availability, and ultra-low response times. The requirements of these applications differ from one another, yet they all share common constraints in terms of latency, reliability, and availability. Latency and reliability requirements impose limitations on the development of telecommunications networks that will support these applications. These applications fall into a specific category of 5G/6G services known as uRLLC services, which demand extreme latency and reliability.

uRLLC applications have varying latency requirements, which can be divided into three main groups.

The first group includes uRLLC applications that require end-to-end latency of around 5 ms, such as augmented and virtual reality applications.

The second group consists of applications that need 1 ms latency, such as Tactile Internet.

The third group comprises sub-millisecond applications, such as holographic communication.

The purpose of this report is to conduct a detailed review of some popular uRLLC applications.

Smart Factories. The use of devices and precision are controlled in real time for rapid production and to facilitate the recycling process. The presence of a large number of production lines presents a serious challenge in terms of latency and reliability. Therefore, most services require very low latency of up to 5 milliseconds.

Intelligent Transportation Systems. Autonomous driving and traffic facilitation require scalable infrastructure, highly reliable communication with very low latency, and special stations to ensure road safety. The maximum allowable latency for most automotive applications is 5 milliseconds.

Robots and Remote Control. Examples of robots and remote control include remote surgical operations in areas affected by natural and man-made disasters or military conflicts.

Virtual Reality (VR). Many applications requiring very high sensitivity and accuracy in data processing, such as remote surgery, rely on VR technology. Supporting these services requires extremely low response times.

Augmented Reality (AR). AR technology is used in a range of applications, including remote learning, medical services, gaming, smart cities, and firefighter training without human casualties. These applications require end-to-end latency of no more than 5 milliseconds to achieve the necessary Quality of Experience (QoE).

Healthcare. This includes remote surgeries, remote diagnostics, and performing hazardous operations using robotic systems with human involvement.

These applications rely on real-time communication with very low latency to transmit human sensations to tactile robots with maximum sensitivity. Such applications require continuous latency within 1–5 milliseconds.

Smart Grids. Smart grids have strict requirements in terms of reliability and latency, so very low latency is required to meet these requirements and support the applications using smart grid technology.

Tactile Internet. This represents the fourth wave of traditional Internet, enabling the real-time transmission of human sensations and actions. The primary application supporting Tactile Internet is tactile communications, which require continuous latency of no more than one millisecond. This latency challenge is associated with physical parameters defined by human sensations.

Ultra-Dense Networks (IoT). The Internet of Things (IoT) is a rapidly growing network of interconnected devices that can interact primarily with each other and with other networks. As the number of connected devices grows, so does the need to support these connections, making ultra-dense IoT networks essential to ensure high connectivity and bandwidth in network architecture, which enables efficient data transmission between multiple devices.

This type of network is specifically designed to provide IoT networks with security and energy efficiency, ideal for applications requiring a large number of connected devices in a limited space, such as "smart cities," manufacturing automation, and healthcare.

The potential benefits of ultra-dense IoT networks in 6G are immense, including a wide range of new applications and services, higher data transmission speeds, more secure data transmission, and more efficient spectrum utilization. Additionally, applications and services in such networks will be able to serve millions of devices connected within a limited area, allowing for more efficient data collection and analysis.

References:

1. Lu Y., Maharjan, S., Zhang Y. Adaptive edge association for wireless digital twin networks in 6G. IEEE Internet of Things Journal. 2021. Vol. 8, is. 22. Pp. 16219 – 16230. Doi: 10.1109/JIOT.2021.3098508

2. ITU-R Recommendation M.2083-0. IMT Vision, Framework and overall objectives of the future development of IMT for 2020 and beyond: ITU-R, Sep. 2015.

3. Ateya, A.A., Muthanna, A., Koucheryavy, A., Khayyat M. Toward Tactile Internet. 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT 2019). 2019. Doi: 10.1109/ICUMT48472.2019.8970990

4. ITU-T Recommendation Y.3104. Architecture of the IMT-2020 network. ITU-T. Geneva. December, 2018.

5. Kharche, S., Dere, P. Interoperability Issues and Challenges in 6G Networks. Journal of Mobile Multimedia. 2022. Vol. 18, is. 5. Pp. 1445–1470. Doi: 10.13052/jmm1550-4646.1856

СЕКЦІЯ 3
БЕЗПЕКА ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Керівник секції: д.т.н. проф. О. О. Можаєв, ХНУВС, Харків
Секретар секції: к.т.н. доц. О В. Сєвєрінов, ХНУРЕ, Харків

ON THE GENERATION OF PSEUDORANDOM NUMBERS WITH UNIFORM DISTRIBUTION

Babayev E.M., Pashayev A.B.
Institute of Control Systems, Baku, Azerbaijan

PRNGs (Pseudo-Random Number Generators) are widely used in cryptographic systems. PRNGs are computer programs that always generate the same sequence of pseudorandom numbers for a given input parameter through special algorithms [1]. In cryptographic systems, sequences of pseudorandom numbers with a uniform distribution are used to obtain a long key from a small password. The non-uniform distribution of such a sequence of numbers may cause some numbers to be generated more often than others. This, in turn, leads to the prediction of the generated numbers. The fact that such a sequence of generated numbers is close to a uniform distribution ensures randomness. A uniform distribution describes situations where each possible outcome in an experiment has an equal probability of occurring:

$$P(X = x_i) = \frac{1}{n}, \quad (1)$$

where $x_i \in \{x_1, x_2, \dots, x_n\}$. The randomness of such generated sequence of numbers is measured by Shannon's entropy formula. Entropy is a measure of uncertainty and is calculated by the following formula:

$$H = -\sum_{i=1}^{n} P_i \log P_i , \quad (2)$$

where P_i is the probability of the ith outcome. The logarithmic base is usually taken as 2. According to Shannon, H takes the maximum value when P_i probabilities are equal. This value is equal to $\log n$ when $P_i = \frac{1}{n}$ for a given n [2]. “Perfect systems in which the number of cryptograms, the number of messages, and the number of keys are all equal are characterized by the properties that (1) each message M is connected to each cryptogram E by exactly one line, (2) all keys are equally likely” [3]. In this instance, achieving perfect secrecy is possible. This feature can be used to generate cryptographic keys.

The aim of this research work is to find an algorithm that generates a sequence of pseudorandom numbers with a uniform distribution.

To solve the problem, the distribution of the values of the function $f_n = \frac{\sin(\lambda n)}{\alpha}, n = 1,2,\dots,N$ in the range [-1;1] is considered. Where $0 < \alpha < 1$, and it is clear that $f_n \in \left[\frac{-1}{\alpha}, \frac{1}{\alpha}\right]$. We add a function in the following form:

$$p_n = \begin{cases} f_n & if \ |f_n| \le 1, \\ 1 - f_n & if \ f_n > 1, \\ -1 - f_n & if \ f_n < -1. \end{cases} \quad (3)$$

To check that the function is uniform distributed in the interval [-1,1], divide the interval [-1,1] into m equal parts. Let's examine how many values of the function p_n fall into each interval $b_i = [b_1; b_2], i = 1,2,\dots,m$ that we obtain. In this case, the elements of p_n that do not fall within the range [-1;1] are discarded. Software has been created and numerical experiments have been conducted to verify that the function generates random numbers with a uniform distribution.

During the experiments, such values of the parameters α and λ are selected such that the distribution of the sequence is close to a uniform distribution. The conducted experiments demonstrates that sequences obtained at values of the parameter α close to 0 (for example, $\alpha = 0{,}1$; $\alpha = 0.2$) are close to a uniform distribution. At larger values of the parameter α, the obtained sequences are not uniformly distributed.

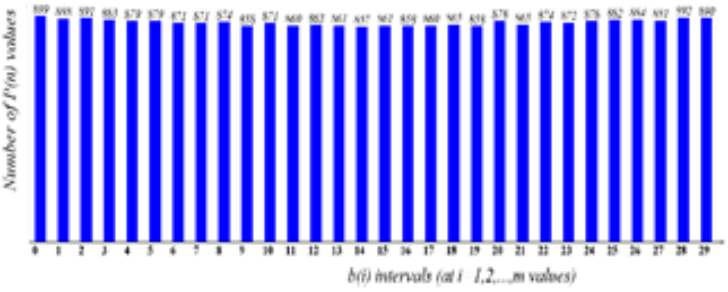


Figure 1 – The result of the experiment
when α=0.2; n=100000; λ=3.2; m=30

As a result, the proposed algorithm is simple and generates numbers with a uniform distribution.

References

1. William Stallings. Cryptography and Network Security: Principles and Practice. 7th ed., Pearson, 2017. – 753 p.

2. C. E. Shannon. A mathematical theory of communication. The Bell System Technical Journal. July, – 1948. Vol.27, №3, – P. 379-423.

3. C. E. Shannon. Communication Theory of Secrecy Systems. The Bell System Technical Journal. October, – 1949. Vol.28, №4, – P. 656-715.

RESEARCH MONITORING METHODS OF INFORMATION SYSTEMS AND NETWORKS SPECIAL PURPOSE

Hasanov A.H.[2], Ibrahimov B.G.[1,2], Hashimov E.G.[1,2]
[1]Azerbaijan Technical University; Baku, Azerbaijan
[2] National Defense University; Baku, Azerbaijan

Based on the research it was established [1, 6] that the quality of operation of information and telecommunication networks for special purposes significantly depends on the quality of operation of fiber-optic transmission systems (FOTS), optical means and fiber-optic communication lines (FOCL) based on WDM/DWDM and HDWDM (Wavelength Division Multiplexing/Dense WDM&High Dense WDM) technologies.

To solve this problem, automated monitoring systems for information systems and special-purpose communication networks using spectral division multiplexing (SDM) technology are studied.

The conducted studies [2, 3] have shown that improving the quality of operation of information systems and special-purpose networks based on fiber-optic communication lines, consisting of PROM, FOC and POM, requires solving a whole range problems, including monitoring, diagnostics, control and management of the telecommunications network, planning and effective placement of network infrastructure and the development of new services that provide high-quality service and increased user satisfaction.

The solution to these problems lies in the sphere of management, control and monitoring of the process of operation of information systems and networks using fiber-optic networks of communication operators. However, this is one of the most important and complex tasks in information systems and special-purpose communication networks, therefore, telecommunication companies always pay a lot of attention to this problem.

In order to effectively manage information systems and special-purpose networks using advanced technologies, it is necessary to constantly monitor a variety of parameters of its network infrastructure.

The values of these parameters form a database for analyzing the operation of information systems and networks using fiber-optic transmission systems - FOTS.

Analysis of the operation of these systems is extremely necessary for the timely detection of emerging problems and localization of their sources.

One of the possible approaches to solving such problems is based on a qualitative analysis of information network monitoring distributed telecommunication networks.

In this work, the object of the study is the information system of automatic monitoring for fiber-optic communication lines, and the analyzed material is the documentation, timely detection and prompt elimination damage occurring in the PROM, FOC and POM.

In this case, a passive information network monitoring scheme is used, which is carried out without violating the integrity of the telecommunications network.

We examined the structural diagram of the monitoring system of the FOTS network link using the control system, which consists of a monitoring and control system, a source and consumer of content, a model of the transport information system and network, as well as a database (DB) and a PC with a printing device for collecting, storing and documenting the results of the monitoring system.

Remote control of information systems using optical fibers is performed by an optical pulse reflectometer, diagnosing the state of the fiber by the backscattering of a light wave when introducing probing pulses into the fiber. At the same time, the system allows monitoring of communication networks using hardware and software complexes, both free and busy communication paths.

Thus, on the basis of the proposed structural and functional diagram of the monitoring system of the link of the information system and the network, the problem of multiple centralized control of the state of telecommunication networks is solved with the purpose of its documentation, timely detection and prompt elimination of damage occurring in the system as a whole. These capabilities of the monitoring and control system significantly reduce the time required to find faults and simplify preventive maintenance of information systems and special-purpose networks.

References

1. Zarkevich E. A., Sklyarov O. K., Ustinov S. A. Testing and monitoring of parameters in WDM networks. Continuous monitoring and measurement of system parameters in WDM networks //Technologies and means of communication.2002. p.10-14.

2. Portnov E.L., Fatkhulin T.D. Technologies aimed at achieving high speed transmission in modern coherent DWDM communication systems. T-Comm. 2015. Vol 9. No.8, pp. 34-37.

3. Hasanov M. H. et al. Research and analysis performance indicators NGN/IMS networks in the transmission multimedia traffic //2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). – IEEE, 2019. – С. 1-4.

4. Ibrahimov B. G., Alieva A. A. Research and analysis indicators of the quality of service multimedia traffic using fuzzy logic //International Conference on Theory and Applications of Fuzzy Systems and Soft Computing. – Cham : Springer International Publishing, 2020. – С. 773-780.

5. Ibrahimov B.G. et al. Research throughput multiservice telecommunication networks // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали 10-і міжнародноі НТК, 9-10 квитня 2020. Том1. Баку-Харків-Жиліна, 2020, с.30.

6. Ibrahimov B. G. Research quality of functioning of the efficiency optical telecommunication systems using spectral technologies / B. G. Ibrahimov, E. G. Hashimov // Проблеми інформатизації : тези доп. 11-ї міжнар. наук.-техн. конф., 16-17 листопада 2023 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Нац. ун-т оборони Азерб. республіки [та ін.]. – Харків : Impress, 2023. – С. 29-30.

7. Hasanov M. H. et al. Research efficiency optical transport networks with use transferring and reception optoelectronics module //International Journal of Research-Granthaalayah. – 2018. – Т. 6. – №. 2. – С. 324-330.

INFORMATION SECURITY RESEARCH SPECIAL-PURPOSE TELECOMMUNICATION SYSTEMS USING MACHINE LEARNING TECHNOLOGY

Ibrahimov B.G.[1,2], Hashimov E.G.[1,2]
[1]Azerbaijan Technical University; Baku, Azerbaijan
[2] National Defense University; Baku, Azerbaijan

Currently, the development of a new sector of a single information space based on the architectural concepts of the next NGN (Next Generation Networks) network and the future FN (Future Networks) generation requires the construction special-purpose multiservice telecommunications systems using machine learning technology [1, 5].

An important direction here is to increase information security in the telecommunications system using methods and tools cryptography and steganography using machine learning technology.

It is worth noting that the use of machine learning technology (ML) in the field of information security, cryptography and steganography, as well as cybersecurity, is extremely in demand for specialists in telecommunication systems. In particular, machine learning tools are used to identify threats to network security and, accordingly, threats to confidential data stored and transmitted over communication channels in these networks [1, 6].

In the telecommunications system, it is necessary to detect and resist network attacks, analyze and eliminate vulnerabilities, fill the knowledge base about cyber threats, and engage in cyber intelligence.

Given the focus of the further presentation, in this case classical ML methods are explored, including classification algorithms using neural networks and deep learning networks. Also analyzed are Deep Neural Network (DNN), Convolutional Neural Network (CNN), Generative Adversarial Network (GAN), Recursive Neural Network (RNN), neural networks, using LSTM (Long Short-Term Memory) architecture [1, 2, 6].

However, the huge volume of data transmitted via communication channels and numerous information security tasks do not allow real-time analysis in special-purpose communication systems.

ML and artificial intelligence technologies, which are well suited for studying network traffic as useful and service traffic, help identify "normal" traffic - including user actions - and separate it from suspicious and potentially dangerous traffic, help solve such problems [1, 6].

It should be noted that in recent years, the Ministry of Defense has been considered one of the key tools for ensuring cybersecurity in the special-purpose telecommunications system.

The most promising and relevant technology at present is automated ML, which is a set of instrumental and methodological tools that make it possible to significantly reduce the share of human participation in the creation artificial

intelligence systems, including by means of automatic validation of modeling results [1, 2].

In this paper, methods detection and classification of computer attacks and network anomalies in the communication system are analyzed. Behavioral methods, methods based on knowledge, methods of computational intelligence are considered.

Next, the problem predicting anomalous events in a telecommunication system is considered. For the task of predicting and detecting intrusions in a communication system, a wide range of specialized systems are used [6].

Thus, when solving problems of forecasting telecommunication systems, control system tools, network protocol analyzers, load testing systems, and network monitoring systems are used [1, 2].

At the same time, problems of protecting information resources in a telecommunication system are solved with the help of firewalls (Firewalls), antiviruses, attack detection systems (IDS), integrity monitoring systems, cryptographic and steganographic methods and security tools.

Next, it is worth considering the features of detection and classification of network attacks using the IForest, Random Forest, and hybrid artificial neural networks algorithms [2, 6].

Methods for expanding the composition network attack features by introducing additional parameters are analyzed. In particular, the influence fractal dimension on the quality of binary classification of network attacks is assessed. Examples of the implementation of fuzzy classification network attacks are considered using the Mamdani and Takagi-Sugeno algorithms.

References

1. Vyugin V.V. Mathematical foundations of machine learning and forecasting. MCMS, 2014. - 305 p.

2. Nguyen T.T. Armitage G. (2008). A survey of techniques for internet traffic classification using machine learning. *IEEE Commun. Surveys Tuts*., vol. 10, no. 4, pp. 56-76.

3. Ibrahimov, B.G., Hashimov, E.G. Analysis and Selection Performance Indicators Multiservice Communication Networks Based on the Concept NGN and FN // -Kharkiv: Computer and information systems and technologies, -aprel, - 2021. –p.96-98. DOI:https://doi.org/10.30837/csitic52021232904

4. Ibrahimov B. G., Hasanov A. H. The investigation and evaluation multiservice network NGN/IMS for multimedia traffic //Synchroinfo journal. – 2020. – Т. 6. – №. 3. – С. 10-13.

5. Ibrahimov B. G., Alieva A. A. Research and Analysis Indicators of the Quality of Service Multimedia Traffic Using Fuzzy Logic //Advances in Intelligent Systems and Computing. – 2021. – Т. 1306. – С. 773-780.

6. Sheloukhin O.I., Erokhin S. D., Polkovnikov M. V. Machine learning technologies in network security. Moscow: Hotline - Telecom, 2021. 360 p.

7. Hasanov M. H. et al. Research and analysis performance indicators NGN/IMS networks in the transmission multimedia traffic //2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). – IEEE, 2019. – С. 1-4.

ANALYSIS OF SOME QUESTIONS ON SYSTEMS FOR BREAKING AND COMPUTER ATTACK DETECTION

Ibrahimov B.G.[1,2], Mammadov E.V.[2]
[1]Azerbaijan Technical University; Baku, Azerbaijan
[2]National Defense University; Baku, Azerbaijan

It should be noted that the most important attribute of our time is global information integration, based on the construction of enterprise-scale computer networks and their unification via the Internet. The complexity of the logical and physical organization modern networks leads to objective difficulties in solving issues network management and protection. In the process operating computer networks, administrators have to solve two main problems [1]:

1. Diagnose the operation of the network and the servers, workstations and related software connected to it.

2. Protect network information resources from unauthorized hacker activity, viruses, network worms, etc., i.e. ensure their confidentiality, integrity and availability.

When solving problems related to diagnostics and protection of network resources, the central issue is the prompt detection network conditions that lead to the loss full or partial functionality, destruction, distortion or leakage of information, which are the result of failures, random failures or the result of an intruder gaining unauthorized access to network resources, penetration of network worms, viruses and other threats to information security. Early detection of such conditions will allow timely elimination of their cause, as well as prevent possible catastrophic consequences.

A wide range specialized systems are used to detect them. Thus, when solving network diagnostic problems, control system tools, network protocol analyzers, load testing systems, and network monitoring systems are used.

Problems of protecting network information resources are solved with the help firewalls, antiviruses, intrusion detection systems (IDS), integrity control systems, and cryptographic protection tools [1, 2].

The characteristic features of the use of these systems are either their periodic and short-term use to solve a specific problem, or their constant use, but with static settings.

Currently, research in this area is being conducted by large foreign commercial companies.

The general approach underlying this research is to find methods of analysis that allow identifying abnormal states of information resources in the form of deviations from the usual (“normal”) state.

These deviations may be the result of hardware and software failures, as well as the consequences of network attacks by hackers. This approach will theoretically allow us to detect both known and new types of problems [1, 2].

The overall efficiency of solving the issues of diagnostics and protection of network resources depends on the efficiency and accuracy of the device that

determines the "normal" state and records deviations. Of particular importance at the moment is the problem of detecting abnormal states in the operation of the network that have a distributed nature in time (ARV). ARVs can be the result of specially disguised network attacks by intruders, hidden hardware and software failures, new viruses, etc.

An attack on an information system is a deliberate action by an intruder that exploits the vulnerabilities of an information system and results in a violation of the availability, integrity and confidentiality of the information being processed.

Eliminating the vulnerability of an information system leads to the elimination of the very possibility of implementing attacks.

There are three types of attacks [1, 2]:

Reconnaissance. These attacks include ping sweeps, DNS zone transfers, email reconnaissance, TCP or UDP port scanning, and possibly analysis of publicly accessible servers.

Exploit (to use for one's own benefit, to abuse) is a computer program, a piece of software code, or a sequence of commands that takes advantage of vulnerabilities in software and is used to carry out an attack on a computing system.

The goal of an attack can be either to seize control of the system (privilege escalation) or to disrupt its functioning (DoS attack). Attackers will take advantage of hidden capabilities or errors to gain unauthorized access to the system.

Denial of Service (DoS) - In this attack, the attacker attempts to destroy a service (or computer), overload the network, overload the CPU, or fill up the disk.

References

1. Sheloukhin O. I., Sakalema D. Zh., Filinova A. S. Detection of intrusions into computer networks (network anomalies). Textbook for universities. / Edited by professor O. I. Sheloukhin - M .: Hotline-Telecom, 2016. – 220 s

2. Paxson V. Bro: A System for Detecting Network Intruders in RealTime. // Computer Networks. 1999. 31 (23-24). P. 2435–2463.

3. Ibrahimov B.G. et al. Research throughput multiservice telecommunication networks // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали 10-і міжнародної НТК, 9-10 квітня 2020. Том1. Баку-Харків-Жиліна, 2020, с.30.

4. Hasanov M. H. et al. Research efficiency optical transport networks with use transferring and reception optoelectronics module //International Journal of Research-Granthaalayah. – 2018. – Т. 6. – №. 2. – С. 324-330.

5. Ibrahimov B. G. Research quality of functioning of the efficiency optical telecommunication systems using spectral technologies / B. G. Ibrahimov, E. G. Hashimov // Проблеми інформатизації : тези доп. 11-ї міжнар. наук.-техн. конф., 16-17 листопада 2023 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Нац. ун-т оборони Азерб. республіки [та ін.]. – Харків : Impress, 2023. – С. 29-30.

6. Hasanov M. H. et al. Research efficiency optical transport networks with use transferring and reception optoelectronics module //International Journal of Research-Granthaalayah. – 2018. – Т. 6. – №. 2. – С. 324-330.

RESEARCH INDICATORS OF INFORMATION EFFICIENCY MULTISERVICE COMMUNICATION NETWORKS

Karimov V.R.
Institute of Control Systems NASA, Baku, Azerbaijan

The development existing multiservice communication networks (MCN) based on the basic principles of the ITU-T FG NET-2030 Focus Group places new demands on their information efficiency (IE) and the quality of the provided infocommunication services in terms QoS (Quality of Service) and QoE (Quality of Experience) [1-3].

In the work [3-8] the performance characteristics of the electrical communication system and telecommunication networks (TN) were investigated, which were considered as a set of separately functioning elements of communication systems.

At the same time, the TN is a complex system characterized by a hierarchical structure, the presence direct, reverse and cross-links between the elements of the communication system. Therefore, it is necessary to consider the work of the as a whole, for which it is necessary to determine the algorithms of its functioning taking into account the interaction high-speed characteristics IE. To solve such problems, we will use a system approach - a system analysis indicators information efficiency in the MCN [1, 4]. A generalized characteristic of the efficiency communication systems is the channel utilization coefficient by throughput- IE, which characterizes the actual speed information transfer in relation to the throughput $C_{\max}$ of the communication channel [1, 6]:

$$\eta_{IE}(b_i) = [V_b(b_i) / C_{\max}] < 1, \quad V_b(b_i) < C_{\max}, \tag{1}$$

where $V_b(b_i)$ – bit rate transmission signals with a binary element in a communication network b_i, $b_i = \{0,1\}$; $\eta_{IE}(b_i)$ – information efficiency MCN when transmitting binary signals with an element b_i, $\eta_{IE}(b_i) \le 1$;

$C_{\max}$ - the maximum value communication channel capacity in the MCN.

From (1) it follows that the limiting values of the MCT efficiency indicators are achieved at $V_b(b_i) = C_{\max}$.

One of the important indicators of the information efficiency MCN is the maximum value of the bandwidth of a discrete communication channel and is expressed as follows [6]:

$$C_{\max} = \max_{V_b(b_i)} [\Delta F_S \cdot \ell og_2(1 + h_b^2)], \tag{2}$$

where h_b^2 – signal-to-noise ratio at the demodulator input when using quadrature amplitude modulation (M-QAM) and phase modulation (M-PM) signals and is equal to [5, 6]:

$$h_b^2 = E_b / N_o = SNR(P_S, E_b), \quad (3)$$

where $SNR(P_S, E_b)$ – Signal to–Noise Ratio with parameter P_S and E_b ; E_b – bit energy and determines the energy spent on the transmission of one bit of the message and is equal to $E_b = E_S /(R_k \cdot \ell og_2 m)$, E_S – signal energy; N_0 – one-sided (at positive frequencies) power spectral density of white noise and is equal to

$$N_0 = 0.5(NF \cdot G - 1) \cdot (h_0 \cdot f_0), \text{ (Vt/Hz)},$$

where NF and G – noise figure and signal gain of the amplifier in the demodulator, respectively; h_0, f_o – respectively the Planck coefficient and signal frequency [6].

From the latest obtained analytical expressions, it characterizes the quality of the MST operation and determines the coefficient effective use of the channel capacity by signal power, taking into account the parameters N_0 and E_b.

References

1. Valiyev V. M., Ibrahimov B. G., and Alieva A. A. (2020) About one resource control task and optimization throughput in multiservice telecommunication networks. *T-Comm*, 14(6), 48-52.

2. Ibrahimov B.G. et al. Research and analysis indicators fiber-optic communication lines using spectral technologies//Advanced Information Systems.2022.Vol.6, No.1. pp.61-64.

3. Ibrahimov B.G., Alieva A.A. (2021). Research and Analysis Indicators the Quality of Service Multimedia Traffic Using Fuzzy Logic. In: Aliev R.A. etc. 14th International Conference on Theory and Application of Fuzzy Systems and Soft Computing-ICAFS-2020. ICAFS 2020. Advances in Intelligent Systems and Computing. Vol.1306. Springer, Cham. pp.773-780.

4. Ibrahimov B.G. et al. Analysis performance indicators multiservice telecommunication networks of the next generation using software-defined network technologies//Bulletin of Computer and Information Technologies, No.5, 2019. pp.39-44.

5. Ibrahimov B.G.. Investigation of noise immunity telecommunication systems according to the criterion energy efficiency//Transport and Telecommunication. Vol. 24, NO.4, 2023. pp. 375 - 384.

6. Ibrahimov, B.G., Hashimov, E.G. Analysis and Selection Performance Indicators Multiservice Communication Networks Based on the Concept NGN and FN // -Kharkiv: Computer and information systems and technologies, -aprel, - 2021. –p.96-98. DOI: https://doi.org/10.30837/csitic52021232904

7. Ibrahimov B.G. et al. Research throughput multiservice telecommunication networks // Сучасні напрями розвитку інформацийно-комунікаційних технологій та засобів управління. Матеріали 10- і міжнародної науково-технічної конференції, 9-10 квитня 2020. Том1. Баку-Харків-Жиліна, 2020, с.30

8. Hasanov M. H. et al. Research efficiency optical transport networks with use transferring and reception optoelectronics module //International Journal of Research-Granthaalayah. – 2018. – Т. 6. – №. 2. – С. 324-330.

RESEARCH MAIN MECHANISMS OF IMPLEMENTATION COMPUTER ATTACKS

Ibrahimov B.G.
Azerbaijan Technical University, Baku, Azerbaijan
Valiyev F.E.
Institute of Control Systems, Baku, Azerbaijan

It should be noted that traditional means protection, such as firewalls or filtering mechanisms in routers, come into play only at the second stage of the attack, completely “forgetting” about the first and third [1].

This means that the attack that is often carried out is very difficult to stop even with powerful and expensive means protection. An example of this is distributed attacks [2, 3].

It would be logical for the protection tools to start working already at the first stage, i.e. to prevent the possibility of collecting information about the attacked system.

This would allow, if not to completely prevent the attack, then at least to significantly complicate the intruder's work.

Traditional tools also do not allow detecting attacks that have already been carried out and assessing the damage after their implementation, i.e. they do not work at the third stage of the attack.

Consequently, it is impossible to determine measures to prevent such attacks in the future.

Taking into account the above, let us consider the main mechanisms for implementing computer attacks [1-5].

The first stage of implementing attacks is collecting information about the attacked system or node. It includes such actions as determining the network topology, type and version of the operating system attacked node, as well as available network and other services, etc. These actions are implemented using various methods [1].

Studying the environment: At this stage, the attacker examines the network environment around the intended attack target. Such areas include, for example, the nodes "victim's" Internet provider or the nodes of the remote office of the company being attacked.

At this stage, the attacker may attempt to determine the addresses "trusted" systems, such as the partner network and nodes that are directly connected to the target of the attack, such as an ISP router, etc. Such actions are quite difficult to detect, as they are performed over a fairly long period of time and outside the area controlled by security tools - firewalls, intrusion detection systems, etc [1].

Network topology identification. There are two main methods of network topology identification used by attackers [1, 3]: -TTL modulation;-Record route.

The first method is used by the programs traceroute for Unix and tracert for Windows.

They use the Time to Live field in the IP packet header, which changes depending on the number of routers the network packet has passed [1].

Identification nodes: Identification of a node is usually carried out by sending the ECHO REQUEST command of the ICMP protocol using the ping utility.There are freely available programs that automate and speed up the process of parallel identification of a large number of nodes, such as fping or nmap.

Identification of services or port scanning: Identification of services is usually done by detecting open ports (port scanning). Such ports are very often associated with services based on TCP or UDP protocols.

Various programs can be used to identify services and scan ports, including freely available ones, such as nmap or netcat [1].

Operating system identification: The main mechanism for remote OS identification is the analysis of responses to queries that take into account different implementations of the TCP/IP stack in different operating systems. Each OS has its own implementation of the TCP/IP protocol stack, which allows using special queries and responses to determine which OS is installed on the remote node.

Determining the role of the node: The penultimate step in the stage collecting information about the attacked node is determining its role, for example, performing the functions of a firewall or a Web server. This step is performed based on already collected information about active services, node names, network topology [1, 3].

Identifying node vulnerabilities [1]: The final step is searching for vulnerabilities. At this step, the attacker uses various automated tools or manually identifies vulnerabilities that can be used to carry out an attack.

References

1. Sheloukhin O. I., Sakalema D. Zh., Filinova A. S. Detection of intrusions into computer networks (network anomalies). Textbook for universities. / Edited by Professor O. I. Sheloukhin - M .: Hotline – Telecom, 2016.220 p.

2. Komar M.P. Network traffic analysis system for detecting computer attacks // Bulletin of Brest State Technical University. Series "Physics, Mathematics and Computer Science". 2020. No. 5. pp. 14 -16.

3. Sheluhin O.I., Atayero A.A. Integrated Model for Information Communication Systems and Metworks // Design and Development. IGI Global, USA. 2012. 462 p.

4. Hasanov A. H., Hashimov E. G. Analysis of the effectivness of communication and automated management systems //Modern directions of development of information and communication technologies and management tools, Abstracts of reports of the 12th Int. Scientific and Technical Conf. – 2022. – T. 1. – C. 1-4.

5. Ibrahimov B. G. Research quality of functioning of the efficiency optical telecommunication systems using spectral technologies / Проблеми інформатизації : тези доп. 11-ї міжнар. наук.-техн. конф., 16-17 листопада 2023 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 3 т.]. Т. 1. – Харків : Impress, 2023. – С. 29-30.

INFORMATION SECURITY OF TELEMETRY DATA

Hazarkhanov A.T., Hashimov E.G.
Military Institute named after Heydar Aliyev, Baku, Azerbaijan
Neymatov V.A.
Azerbaijan State Oil and Industry University, Baku, Azerbaijan

When collecting and transmitting telemetric information (TMI), the problem of data security becomes especially relevant. In the process of studying the problem in order to find more advanced methods, it was decided to use as a basis the methods presented in works [1] and [2]. In article [1], in order to ensure the integrity and completeness of the accumulated data on the state of individual functional subsystems of aircraft, and intended for transmission to a ground enterprise, a method is proposed, the implementation of which is carried out by comparing the accumulated data with the generated data (specified data), the primary source of which is the same ground enterprise.

In the work [2] to ensure the necessary required reliable protection of TMI from unauthorized access and interference, a structural-algorithmic method is proposed, according to which residual images are used. According to the authors, if the transmitted data is presented in the amount of two or more residual images, then during the process of converting them into a word-measurement, individual shortcomings are revealed, being available for their elimination. The method we proposed provides for a comprehensive approach, in which the specified data, like telemetry, are compared with each other in the form of residual images.

References

1.Guzairov M.B., Frid A.I., Vulfin A.M., Berkholz V.V. Support for decision-making in the task of ensuring information security of aviation telemetry systems. Proceedings of the International Symposium "Reliability and Quality", 2020, Vol. 1. Pp. 178-183

2.Rudnev A.N., Vas'kovsky A.S., Komolov M.V. Non-cryptographic protection system for telemetry information. Information Society Technologies. T-Comm, #11-2012. Pp. 48-50

3. Hasanov A.H. Analysis of the effectivness of communication and automated management systems // Modern directions of development of information and communication technologies and management tools, Abstracts of reports of the 12th Int. Scientific and Technical Conf. – 2022. – T. 1. – C. 1-4.

ЗАХИСТ ВІД ФІШИНГОВИХ АТАК ТА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Лященко В.О., Гук А.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Захист від фішингових атак та соціальної інженерії в телекомунікаційних мережах стає все більш важливим через зростання кількості кіберзагроз, націлених на отримання конфіденційних даних користувачів. Фішингові атаки,

що використовують соціальну інженерію для маніпуляцій користувачами, становлять серйозну загрозу, оскільки здатні обійти технічні засоби захисту, впливаючи безпосередньо на людський фактор. Ефективні методи протидії включають впровадження сучасних систем багатофакторної автентифікації (MFA), що значно ускладнюють доступ до мереж навіть у разі компрометації облікових даних [1]. Важливою складовою захисту є також підвищення обізнаності користувачів щодо технік соціальної інженерії та навчання співробітників основам кібергігієни. Проведення регулярних тренінгів з виявлення фішингових атак та небезпечних комунікацій дозволяє значно знизити ризики таких інцидентів [2]. Інші технічні рішення включають використання автоматизованих систем виявлення фішингових загроз, таких як інтелектуальні фільтри для електронної пошти та інтеграція з базами даних відомих зловмисних доменів. Ці заходи сприяють вчасному виявленню потенційних загроз і захисту кінцевих користувачів від небажаного впливу [3].

Метою доповіді є розгляд сучасних методів захисту від фішингових атак та соціальної інженерії в телекомунікаційних мережах, аналіз ключових викликів і шляхів їх вирішення.

Список літератури

1. Кузьменко М.В. Мультфакторна автентифікація як метод захисту від фішингу – Київ: Видавничий дім "Кібербезпека", 2010. – 210 с.

2. Савчук Г.Д. Підвищення обізнаності користувачів: навчання кібергігієни – Київ: Видавництво "Інформаційна безпека", 2013. – 340 с.

3. Левченко П.О. Автоматизовані системи виявлення фішингових загроз у телекомунікаційних мережах – Київ: Інститут телеком. технологій, 2019. – 307 с.

ЗАХИСТ ДАНИХ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ: МЕТОДИ ШИФРУВАННЯ ТА АВТЕНТИФІКАЦІЇ

Дерев'янко К.А., Гук А.С.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком телекомунікаційних систем та зростанням обсягів переданої інформації питання захисту даних стає дедалі актуальнішим. Для забезпечення конфіденційності, цілісності та автентичності інформації, що передається через мережі, ключову роль відіграють методи шифрування та автентифікації. Сучасні криптографічні алгоритми, такі як AES (Advanced Encryption Standard) та RSA, забезпечують високий рівень захисту, роблячи передані дані недоступними для несанкціонованого доступу або втручання. Використання цих методів є необхідним для захисту приватних та конфіденційних комунікацій, включаючи фінансові транзакції та особисті дані користувачів [1]. Автентифікація, яка гарантує ідентифікацію користувачів та пристроїв, є ще одним важливим компонентом захисту даних. У телекомунікаційних системах широко застосовуються двофакторна автентифікація (2FA) та протоколи, такі як OAuth і Kerberos, які забезпечують безпечний обмін даними між клієнтами

та серверами. Ці технології не тільки підтверджують особу користувача, але й захищають від атак типу «людина посередині» (MitM) та несанкціонованого доступу до ресурсів мережі [2]. **Метою доповіді є** огляд сучасних методів шифрування та автентифікації, які використовуються для захисту даних у телекомунікаційних системах, аналіз їхньої ефективності та надійності, а також перспективи розвитку новітніх технологій у цій сфері.

Список літератури

1. Осламенко Д.Д. AES та RSA: Основи шифрування даних у сучасних телекомунікаційних мережах – Київ: Видавничий дім "Безпека", 2009. – 282 с.

2. Кривонос В.М. Протоколи автентифікації в телекомунікаціях: Захист доступу за допомогою 2FA та OAuth – Київ: Видавництво "Телекомунікації", 2017. – 279 с.

КІБЕРБЕЗПЕКА В ЕПОХУ 5G: НОВІ ВИКЛИКИ ТА СТРАТЕГІЇ ЗАХИСТУ

Показій К.О., Тимошенко Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком 5G технологій виникають нові виклики у сфері кібербезпеки, що пов'язані зі збільшенням кількості підключених пристроїв, масштабністю мереж та складністю їх інфраструктури. 5G надає можливість підключати значну кількість пристроїв, зокрема в межах Інтернету речей (IoT), що розширює поверхню для атак і збільшує потенційні вразливості [1]. Однією з ключових загроз в епоху 5G є складність управління безпекою в розподілених і віртуалізованих мережах, які використовують програмно-визначені мережі (SDN) та мережеві функції віртуалізації (NFV). Ці технології покладаються на програмне забезпечення, яке може стати об'єктом кібератак, якщо не будуть впроваджені належні заходи захисту. Особливо вразливими є інфраструктури критичних галузей, де збій або атака на мережу можуть мати серйозні наслідки для безпеки й економіки [2]. Для вирішення цих викликів важливим є розробка нових стратегій захисту, що включають використання штучного інтелекту та машинного навчання для автоматизованого виявлення і запобігання загрозам у реальному часі. Додатково, потрібно забезпечувати сегментацію мережі для ізоляції атак та зниження ризику їх поширення, а також впроваджувати нові стандарти шифрування та аутентифікації для забезпечення захисту даних під час їх передачі в 5G мережах [3].

Метою доповіді є розгляд нових викликів кібербезпеки, які постають з впровадженням 5G технологій, та аналіз ефективних стратегій захисту, що допоможуть знизити ризики кібератак і забезпечити надійне функціонування телекомунікаційних мереж.

Список літератури

1. Ткаченко О.В. Виклики кібербезпеки 5G: Інтернет речей та розширююча поверхня атак – Київ: Технічний університет, 2023. – 250 с.

2. Кравченко Д.П. Забезпечення SDN та NFV у мережах 5G: Основні аспекти – Київ: Інститут інформаційних технологій, 2023. – 200 с.

3. Ковальчук М.В. Штучний інтелект та машинне навчання в кібербезпеці: Новий підхід для 5G – Київ: Науковий світ, 2023. – 280 с.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ В МЕРЕЖАХ LTE ТА 5G

Ляшенко Г.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день мобільні технології надають широкі можливості та використовуються практично у всіх сферах повсякденного життя. Це дозволяє користувачам отримувати різні послуги дистанційно. Одними з найпоширеніших послуг, що надаються онлайн та потребують високого рівня захисту даних є мобільні платежі, доступ до хмарних сервісів, використання IoT-пристроїв. Збільшення кількості послуг, що надаються через Інтернет, та кількості користувачів ставлять нові задачі для розвитку мобільних мереж для підтримки зростання об`єму трафіка та широкого спектру пристроїв.

Метою доповіді огляд еволюції стандартів мобільних мереж, аналіз особливостей мереж LTE та 5G, включаючи особливості їх архітектури, основних компонентів, технологій, таких, як MIMO, NFV, Edge computing, Network slicing[1, 2]. Аналіз роботи систем віддаленої біометричної автентифікації та особливості їх використання в мобільних мережах [3,4].

Враховуючи можливі атаки при передачі даних мережею та важливість захисту даних біометрична автентифікація стає все більш популярною в сучасних інфокомунікаційних системах, завдяки високому рівню безпеки та зручності у використанні. У контексті мереж LTE та 5G, які забезпечують високу швидкість передачі даних та мають потенційні загрози безпеці, біометричні технології можуть суттєво підвищити захист даних користувачів.

В доповіді наводяться результати аналізу використання біометричної автентифікації в мобільних мережах, що дозволяє підвищити безпеку користувачів та зручність використання мережних послуг [2].

Список літератури

1.Zarrinkoub H. Understanding LTE with MATLAB - From Mathematical modeling to simulation and prototyping / Houman Zarrinkoub. [S. l.] : John Wiley & Sons, Inc., 2014.

2.Astrakhantsev, A., Liashenko, G., & Shcherbak, A. (2020). Noise resistance of remote authentication via lte network. Information and Telecommunication Sciences, 38-43.

3.Скорик Юлія, Безрук Валерій. Вибір переважного методу біометричної автентифікації. International Science Journal of Engineering & Agriculture Vol. 2, No. 4, 2023, pp. 28-34.

4.Ляшенко Г. Є., Астраханцев А. А. Дослідження ефективності методів біометричної автентифікації. Системи обробки інформації. 2017. № 2(148). С. 111–114.

СУЧАСНІ МЕТОДИ ЗАХИСТУ ТА УПРАВЛІННЯ КОРПОРАТИВНИМИ МЕРЕЖАМИ

Ліннік М.В., Скорик Ю.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні корпоративні мережі є складними та багаторівневими системами, вимагаючи інтегрованих підходів до їх захисту й управління. Зі зростанням кіберзагроз та збільшенням кількості підключених пристроїв постає потреба у впровадженні новітніх методів безпеки та контролю. Сучасні технології забезпечують можливості для гнучкого управління доступом, моніторингу трафіку та реагування на інциденти в режимі реального часу.

Метою доповіді є методи захисту та управління корпоративними мережами.

Сучасні системи управління корпоративними пристроями дають можливість компаніям забезпечувати безпеку й ефективність використання своїх ресурсів, знижуючи ризики витоку даних і підвищуючи продуктивність працівників. Microsoft Intune і Jamf Pro є двома з найкращих рішень для управління пристроями корпоративної мережі, які дозволяють централізовано контролювати налаштування, доступ, політики безпеки й оновлення програмного забезпечення на всіх підключених пристроях.

У роботі наводиться порівння Microsoft Intune і Jamf Pro. Як Microsoft Intune, так і Jamf Pro надають можливості для створення і застосування політик доступу та безпеки, що є критично важливими для захисту корпоративних мереж. Завдяки цим інструментам можна контролювати використання облікових записів, забезпечувати відповідність політик вимогам компанії та стандартам безпеки, а також здійснювати регулярний моніторинг стану пристроїв і реагувати на загрози в режимі реального часу. Обидва рішення також підтримують інструменти для звітування та аналітики, що допомагають адміністраторам отримувати актуальну інформацію про стан мережі та пристроїв [1, 2].

Управління пристроями корпоративної мережі за допомогою Microsoft Intune і Jamf Pro є важливим елементом сучасної стратегії безпеки для компаній. Ці інструменти дозволяють централізовано встановлювати та контролювати політики безпеки, управляти і налаштовувати пристрої на різних операційних системах.

Список літератури

1. Christiaan Brinkhoff. Mastering Microsoft Intune - Second Edition: Deploy Windows 11, Windows 365 via Microsoft Intune, Copilot and advance management via Intune Suite. 2024. 988 p.

2. Manish Bangia. Microsoft Intune Administration: Learning Intune concepts and migrating endpoint devices from SCCM. 2020. 760 p.

ВПЛИВ АТАК НА БЕЗДРОТОВІ МЕРЕЖІ WI-FI 6E

Мамедов Д.К., Фодченко А.В., Харченко Н.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток мобільних пристроїв призвів до зміни напрямку еволюції телекомунікаційних технологій. Тож особливого поширення набула реалізація технологій бездротової передачі даних, відома як Wi-Fi. Wi-Fi реалізує технології, описані в стандарті IEEE 802.11 та у багатьох поправках до нього.

В даний час останньою поширеною поправкою є стандарт IEEE 802.11ax, що отримав назву «Wi-Fi 6E». Так як, з огляду захисту інформації, бездротові мережі є найбільш вразливими до атак зловмисників. У мережах Wi-Fi слід особливу увагу приділяти питанням її захисту, та керуватися принципами інформаційної безпеки, які полягають у забезпеченні конфіденційності та цілісності інформації, а також доступу до цієї інформації [1]. Стандарт IEEE 802.11ax вводить новий частотний діапазон 6 ГГц і забороняє для нього використання деяких pre-RSNA (WEP, Shared Key Authentication, Open System Authentication without encryption) та RSNA (WEP, TKIP) алгоритмів, а також додає обов'язковий захист кадрів управління [2]. Оскільки більшість корпоративних мереж досі базується на Wi-Fi 5, новий частотний діапазон 6 ГГц залишається недоступним для інфраструктури.

Метою доповіді є аналіз стандарту IEEE 802.11ax та його чутливості до зовнішніх атак.

В доповіді наводяться результати тестування мережі, що працює на стандарті Wi-Fi 6E. Аналіз результатів показав, що атаки залишаються актуальними для мереж останнього покоління і негативно впливають на працездатність.

Розглянуто загрозу нового частотного діапазону 6 ГГц: основна проблема полягає в тому, що обладнання в корпоративних мережах базується на Wi-Fi 5 і не працює на 6 ГГц. У зв'язку з цим велику загрозу становлять атаки, засновані на створенні підроблених точок доступу, наприклад атаки типу «злий двійник».

Список літератури

1. Architecting Next Generation Wireless Network with Catalyst Wi-Fi 6E Access Points // Cisco Live URL: https://www.ciscolive.com/c/dam/r/ciscolive/globalevent/docs/2022/pdf/BRKEWN-2024.pdf

2. 802.11ax-2021 - IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks-- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN // IEEE STANDARTS ASSOCIATION URL:https://ieeexplore.ieee.org/document/9442429

СУЧАСНІ ПІДХОДИ ДО КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Стрілковський Є.Е., Горбов В.О., Партика С.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сьогодні кібербезпека є однією з найактуальніших тем у сфері інформаційних технологій, оскільки сучасний світ дедалі більше залежить від цифрових систем та мереж. В умовах глобалізації та активного розвитку мережі Інтернет, зростає кількість загроз для конфіденційності, цілісності та доступності інформації. Поширення хмарних обчислень, Інтернету речей та інших технологій створює додаткові виклики для захисту даних [1].

Завданням кібербезпеки є виявлення, запобігання та нейтралізація кіберзагроз, а також забезпечення захисту даних у цифровому просторі. Ключовими елементами кібербезпеки є системи контролю доступу, шифрування, антивірусний захист, системи виявлення та попередження вторгнень (IDS/IPS), а також засоби аналізу поведінки користувачів для виявлення потенційних атак. З розвитком технологій з'являються нові методи забезпечення кібербезпеки. Один з них – використання штучного інтелекту та машинного навчання, що дозволяє автоматично виявляти аномалії та реагувати на загрози у реальному часі [2].

Іншим підходом до підвищення рівня кібербезпеки є концепція Zero Trust (нульова довіра). Такий підхід підвищує рівень захисту, оскільки система не довіряє жодному елементу мережі автоматично, а лише після верифікації [3].

Метою доповіді є огляд сучасних підходів до забезпечення кібербезпеки та аналіз їх ефективності у боротьбі із сучасними кіберзагрозами. Наведено результати дослідження ключових методів захисту інформації в умовах стрімкого розвитку технологій, а також визначено перспективні напрямки розвитку кібербезпеки.

Показано, що сучасні підходи до кібербезпеки, такі як штучний інтелект, Zero Trust та інші технології, дозволяють ефективно боротися із кіберзагрозами та знижувати ризики для інформаційних систем, створюючи більш безпечний кіберпростір.

Список літератури

1. Shinde, P. P., & Thool, R. C. "Intrusion Detection System for Cloud Computing." Proceedings of the International Conference on Advanced Computing, (2012). 67-74.

2. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. Network Anomaly Detection: A Machine Learning Perspective. CRC (2014). 2, 160.

3. Ворохоб М., Киричок Р., Яскевич В., Добришин Ю. Сучасні перспективи застосування концепції Zero Trust при побудові політики інформаційної безпеки підприємства. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», (2023).1(21), 223–233.

WATERMARK STEGANOGRAPHY BASED ON THE NOVEL ENHANCED QUANTUM IMAGE REPRESENTATION MODEL

Fediushyn O.I., Holovko Y.V.
Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

Watermarking digital images is vital for copyright protection, identity verification, and source tracing. Traditional digital watermarking schemes have limitations, such as low reliability and low security, which can lead to loss or destruction of watermarks. To solve these problems, we can propose quantum imaging technology [1-4], which has become widespread in recent years. This technology utilizes the properties of quantum superposition and entanglement to enhance the security and robustness of watermarks on digital images, thereby protecting the security and privacy of digital images.

The aim of the paper is to model watermarking using the NEQR model using quantum computing, demonstrating its potential for enhanced image protection and integrity. There are various methods of image representation: Qubit Lattice [4-5], Entangled image, Real Ket, Flexible Representation of Quantum Images (FRQI) [1], Novel Enhanced Quantum Image Representation (NEQR) [2, 4].

FRQI uses normalized superposition to store all pixels of an image, the same operations can be performed on all pixels at the same time, and therefore FRQI can alleviate the computational problem of image processing. The main limitation of FRQI is that it only uses one qubit to store the grayscale information for each pixel of the image, so some digital image processing operations, such as certain complex color operations, cannot be performed based on FRQI.

The NEQR model uses a linear, independent base state of a qubit sequence to store the grayscale value for each pixel. Thus, to store a digital image using quantum mechanics, NEQR uses two intertwined qubit sequences that represent the grayscale information and positions of all pixels in the image.

In the FRQI representation, the grayscale information of an image is encoded using a single qubit, while in NEQR, the grayscale information is encoded in basis qubit states, since each basis qubit state is linearly independent, the image processing task becomes much simpler than in FRQI.

The method reduces the overall computational complexity from (24n) to (22n) [2]. It focuses on the shortcomings of the FRQI model and stores information based on a qubit sequence, which allows for a halving of the computational complexity and a 1.5-fold improvement in compression ratio.

The color scheme of an image consists of three intensity values known as RGB values of an image, the intensity of each color can vary from 0, where 0 means black and 255 means white. To encode each intensity ($2q = 255$), where q is the number of qubits needed to encode different intensities of a particular color, and to encode a position we need a different set of qubits. Since we will be representing a two-dimensional (2x2) pixel image, we will define the position of the image by its row and column, Y, X, respectively, and the color by

$$f\left(Y,X\right)=C_{YX}^{q-1}C_{YX}^{q-2}\ldots C_{YX}^{1}C_{YX}^{0},$$
$$C_{YX}^{q}\in\left[0,1\right],\ f\left(Y,X\right)\in\left[0,2^{q}-1\right]. \quad (1)$$

Like digital watermarks, quantum watermarks aim to protect the copyright of an image and authenticate its owner by means of visible or invisible signals (mostly logos) embedded in the image container (or media). Most quantum watermarking strategies are based on FRQI for media images and watermark logos. The NEQR model [2, 4, 6], which stores color information in the ground state of a quantum sequence, uses a total of 2n+q qubits to represent an image, where n represents position coordinate information and q represents color information. This allows for precise manipulation of color information and makes certain image operations that were previously complex simple and convenient.

References

1. P. Q Le., F. Dong and K. Hirota "A flexible representation of quantum images for polynomial preparation, image compression, and processing operations," Quantum Information Processing, vol. 10, pp. 63–84, 04 2010.

2. Y. J. Zhang, K. Lu, Y. Gao and M. Wang "Neqr: a novel enhanced quantum representation of digital images," Quantum Information Processing, vol. 12, pp. 2833–2860, 2013.

3. M. A. Nielsen and I. L. Chuang Quantum computation and quantum information. Cambridge University Press, 2019.

4. Methods of Information Protection Based on Quantum Image Steganography / O.I. Fediushyn, Y.V. Holovko, et al. Radiotekhnika: All-Ukr. Sci. Interdep. Mag. 2024. № 218.

5. Venegas-Andraca S. and Bose S. Storing, processing, and retrieving an image using quantum mechanics, in Proc. SPIE Conf. Quantum Information and Computation, (2003), pp. 134–147.

6. RG. Zhou, Luo et al. A Novel Quantum Image Steganography Scheme Based on LSB. Int J Theor Phys 57, 1848–1863 (2018). https://doi.org/10.1007/s10773-018-3710-x.

ДОСЛІДЖЕННЯ МНОЖИНИ ТРИРОЗРЯДНИХ ЛОГІЧНИХ ОПЕРАЦІЙ ДЛЯ МАТРИЧНОГО КРИПТОПЕРЕТВОРЕННЯ

Антоненко О.О., Приступа А.Ю., Емінов Р.Т., Можаєв О.О.
Харківський національний університет Внутрішніх справ, Харків, Україна

Основу гарантування інформаційної безпеки в інформаційно-телекомунікаційних системах становлять криптографічні методи та засоби захисту інформації. Слід врахувати, що найбільш надійний захист можна забезпечити тільки за допомогою комплексного підходу, тобто рішення задачі має являти собою сукупність організаційно-технічних та криптографічних заходів [1,2].

В основі криптографічних методів лежить поняття криптографічного перетворення інформації, створеного за певними математичними законами, з метою виключити доступ до цієї інформації сторонніх користувачів, а також з метою забезпечення неможливості безконтрольного отримання інформації з боку тих самих осіб [3].

Метою доповіді є побудова методики синтезу логічних функцій на основі методу перебору, що дозволить повисити ефективність збору інформації про логічні функції декількох змінних, які можуть використовуватися в криптографії, та визначення їх особливостей.

В доповіді наводяться результати досліджень множини трирозрядних логічних операцій для матричного криптоперетворення. Наведені дані показують, що для синтезу трирозрядних операцій криптографічного перетворення можуть використовуватися різні елементарні логічні операції.

На основі аналізу експериментальних досліджень встановлено, що шість операцій утворюють групу операцій криптографічного перетворення, в якій повторне перетворення інформації другою операцією приведе до перетворення інформації третьою операцією з цієї групи.

Список літератури

1. Глинчук, Людмила Ярославівна. Криптологія [Текст] : навч.-метод. посіб. / Л. Я. Глинчук ; Східноєвроп. нац. ун-т ім. Лесі Українки. - Луцьк : ВежаДрук, 2014. - 163 с. : рис., табл. - Бібліогр.: с. 157-158.

2. Горбенко, Іван Дмитрович. Прикладна криптологія. Теорія. Практика. Застосування / Горбенко І. Д., Горбенко Ю. І. ; Харк. нац. ун-т радіоелектроніки, Х. : Форт, 2013. - 878 с.

3. Козіна, Г. Л. Криптографія від історії до сучасних стандартів [Текст] : навч. посіб. / Г. Л. Козіна. - Запоріжжя : НУ "Запорізька політехніка", 2020. - 192 с.

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВБУДОВУВАННЯ ДАНИХ В ЧАСТОТНУ ОБЛАСТЬ ЗОБРАЖЕНЬ

Лисенко С.О., Стрєлка Р.В., Єрмак В.М., Рог В.Є.
Харківський національний університет Внутрішніх справ, Харків, Україна

Інформація є одним з цінних предметів сучасного життя. Отримання доступу до неї з появою глобальних комп'ютерних мереж стало неймовірне простим. В той же час, легкість і швидкість такого доступу значно підвищили і загрозу неавторизованого доступу до інформації. Завдання надійного захисту авторських прав, конфіденційних даних від несанкціонованого доступу є однією з давніх й невирішених на сьогодні проблем. Приховування факту існування вбудованих даних при їх передачі, зберіганні або обробці є завданням стеганографії - науки, яка вивчає способи і методи приховання конфіденційних відомостей [1, 2].

Метою доповіді є дослідження процесу вбудовування даних в частотну область зображень, що дозволить покращити захист авторських прав в ряді прикладних галузей. В доповіді було розглянуто автоматизовану систему управління виробництвом друкарської продукції та створення систем приховання даних на основі різних стеганографічних методів. В результаті аналізу методів вбудовування даних в просторову та частотну області зображень встановлено, що найбільш простим з точки зору практичної

реалізації є методи вбудовування даних в просторову область зображень. Але ці методи мають деякі недоліки. Так, стискування зображень приводить до повного знищення вбудованої в просторову область інформації. Цей недолік усувається, якщо інформацію вбудовувати в частотну область зображень.

Список літератури

1. Конахович Г., Прогонов Д., Пузиренко О. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних : підручник. Київ : Центр учб. літ., 2018. 558 с. URL: https://pdf.lib.vntu.edu.ua/books/2019/Konahovich_2018_558.pdf..

2. Денисюк В. Стеганографічний алгоритм захисту даних з використанням файлів зображень. Ефективна економіка. 2017. № 5. URL: http://www.economy.nayka.com.ua/?op=1&z=5584.

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО СТВОРЕННЯ ЗАХИЩЕНОЇ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ НА ПРИВАТНОМУ ПІДПРИЄМСТВІ ЗА ТЕХНОЛОГІЄЮ WI-FI

Комаренко О.О., Гончар В.О., Лесінський В.В., Пересічанський В.М.
Харківський національний університет Внутрішніх справ, Харків, Україна

З прогресом технологій зловмисники намагаються перебороти всі перешкоди, що стоять на їх шляху. Фізичне вторгнення на об'єкт захисту може призвести до серйозних наслідків, і саме тому необхідно знати, як захищати себе від таких подій. **Метою доповіді** є розробка пропозицій щодо створення захищеної локальної обчислювальної мережі з використанням технології Wi-Fi [1, 2]. Основою для створення захищеної локальної мережі є застосування моніторингу радіосигналів та бездротових пакетів даних в Wi-Fi мережах. На базі цього моніторингу можливо створити систему, яка забезпечить виявлення фізичного вторгнення на об'єкт захисту. Аналіз Wi-Fi даних дозволяє визначити незаконний доступ до мережі шляхом аналізу мак-адрес. Такий аналіз дозволяє виявити небажаних користувачів, які намагаються отримати доступ до мережі. Для застосування аналізу Wi-Fi пакетів і виявлення фізичного вторгнення існують різноманітні інструменти і програмні засоби, такі як Wireshark, Aircrack-ng та високоточні аналізатори Wi-Fi трафіку. В результаті проведеного аналізу встановлено, що перевагами даного методу є швидке виявлення фізичного вторгнення та можливість реагування в реальному часі, однак існують обмеження, такі як можливість фальсифікації трафіку та обмежена ефективність в захищених мережах.

Список літератури

1 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.

2. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В. Л. Бурячок, Г. М. Гулак, В. Б. Толубко. – К.: ДУТ, 2015. – 449 с.

ДОСЛІДЖЕННЯ РИЗИКІВ ВИЯВЛЕННЯ ЗБОЇВ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІЦІ ЗА ДОПОМОГОЮ НЕЙРОННОЇ МЕРЕЖІ

Гаврилов Д.І., Кравцова Є.В., Заречний І.О., Пересічанський В.М.
Харківський національний університет Внутрішніх справ, Харків, Україна

В теперішній час зростає вплив ризиків різноманітних видів збоїв, які можуть виникати в цифрових пристроях на виході логічних елементів, на якість функціонування таких пристроїв. Тому виникає актуальне завдання дослідження цих ризиків

Це завдання зводиться до розробки деякої системи класифікації сигналів, отриманих з виходу елемента проектованого пристрою, що повинне сигналізувати проектувальникові про можливу проблему. Завдання ускладнюється тим, що збої того самого класу не тільки можуть являти собою сигнали різної форми, але й бути розподіленими за часом.

Метою доповіді є дослідження ризиків виявлення збоїв обчислювальної техніці за допомогою нейронної мережі.

Найбільш зручним методом рішення завдань подібного виду є використання апарата штучних нейронних мереж [1,2]. Як середовище розробки було обрано інструментарій NNTool середовища MatLab. Із пропонованих в MatLab можливих варіантів нейронних мереж, найбільш підходящою для рішення поставленого завдання виявилася нейронна мережа Feed Forward Back Propagation.

У завданнях класифікації, до яких відноситься дана задача, кількість виходів мережі відповідає числу поділюваних мережею класів. Цей факт повинен бути врахований при виборі архітектури мережі й на етапі формування цільових даних.

Мережа класифікації дає найбільше значення на виході, що відповідає підходящому класу. При добре сконструйованій і навченій мережі значення інших виходів будуть помітно менші.

Тому для рішення нашого завдання обрана мережа Feed-forward backprop із п’ятнадцятьма сигмоподїдними нейронами першого шару й тринадцятьма лінійними нейронами другого шару. У результаті проведених експериментів з використанням утиліти NNTool і за допомогою команд отримана коректна працююча нейронна мережа.

Список літератури

1. Нильсен М.А. Нейронні мережі та глибоке навчання. Determination Press, 2017.

2. Q. Cao, L. Shen, W. Xie, O. M. Parkhi, A. Zisserman. VGGFace2: A dataset for recognising face across pose and age. International Conference on Automatic Face and Gesture Recognition. URL:
http://www.robots.ox.ac.uk/~vgg/publications/2018/Cao18/cao18.pdf.

ДОСЛІДЖЕННЯ МОДЕЛЕЙ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ

Гнусов Ю.В., Дроженко Є.В.
Харківський національний університет внутрішніх справ, Харків, Україна

Через такий швидкий перехід до цифрового світу збільшилася кількість інцидентів в сфері інформаційної безпеки. Старі загрози, отримали нові неочікувані уразливості.

Чіткого визначення поняття загроза не існує. Тому у різних наукових виданнях та законодавчих документах воно трактується по-різному. Наприклад wikipedia трактує поняття загрози(в загальному розумінні) - як потенційно можлива подія, дія (вплив), процес або явище, які можуть призвести до нанесення шкоди чиїмось інтересам[1]. В книзі[2] розуміється, що загроза - це будь-які обставини чи події, що можуть спричинити порушення політики безпеки інформації та(або) нанести збитки ІКС. Тобто загроза – це будь-який потенційно можливий несприятливий вплив.

Поняття загрози має велику кількість визначень, та всі вони сильно залежать від сфери використання. Але попри таку різноманітність визначень, всі вони мають спільну рису – порушення властивостей інформації.

Поняття загроз та уразливостей інформаційної системи тісно пов’язані між собою. Якщо вважати загрозу, як безпосереднє джерело негативних впливів на інформаційну систему, то уразливість – нездатність системи протистояти цим негативним впливам.

Метою доповіді є системний аналіз загроз та уразливостей цілісності інформації.

В результаті, як виявилося на практиці найчастіше використовується класифікація загроз, що ґрунтується на базових властивостях інформації (конфіденційності, цілісності або доступності). Також детально було розглянуто основні загрози цілісності інформації протягом її життєвого циклу, що не тільки дало змогу впевнитися в тому, що властивість цілісності не менш важлива чим конфіденційність або доступність. Окрім того було проаналізовано збитки від реалізації загроз, та актуальні шляхи через які відбуваються витоки інформації. Співвідношення уразливостей цілісності і уразливостей загалом в деяких випадках показувало високі значення. Наприклад, серед уразливостей програмного забезпечення віртуалізації 59.4% усіх уразливостей для цілісності.

Список літератури

1. Класифікація загроз інформаційній безпеці [Электронный ресурс] // Режим доступа: https://sites.google.com/site/infobezosob/klasifikacia-zagroz-informacijnij-bezpeci - 10.10.2024.

2. Гайрановський М.В. Безпека інформаційно-комунікаційних систем, підручник – метод. пособие [Текст] / М.В. Гайрановський, О.М. Новіков – Київ: Видавнича група BHV, 2009. – с. 18– 35.

ДОСЛІДЖЕННЯ КОНЦЕПЦІЇ ВІДДАЛЕНОГО РОБОЧОГО МІСЦЯ

Цуранов М.В., Музика А.С.
Харківський національний університет внутрішніх справ, Харків, Україна

Пандемія COVID-19 та військові дії значно змінили економічну ситуацію в світі в гіршу сторону та змусили припинити роботу більшості підприємств. Багатьом компаніям довелося адаптуватися до повномасштабної війни щоб продовжити свою діяльність. Одним з таких видів адаптації стала дистанційна робота співробітників всередині багатьох компаній. Так само дистанційна робота відмінно проявила себе і в системах освіти в різних навчальних закладах, таких як школи, училища, університети. Таким чином з'явилася концепція – "Робота з дому" (РЗД). Концепція роботи з дому є новою для більшості працівників. Оскільки працівники переживають нове середовище, важливим питанням стало виявлення відмінностей роботи співробітників вдома порівняно з роботою в офісі. Але за даними статистики «Owl Labs», компанії, яка виробляє пристрої для відеоконференц зв'язку, можна сказати, що готовність та бажання працювати вдома виявило 42% працівників, інші 58% поки що не впевнені в такому виборі. [1]

Був проведене аналіз у якому прийняло участь 18 країн. У всіх країнах спостерігався стрибок числа віддалених робочих позицій – від 1,5-кратного збільшення в Канаді до 4,9-кратного збільшення в Бразилії. В цілому найбільше зростання спостерігалося в європейських і латиноамериканських країнах, в той час як в північноамериканських і азіатських країнах зростання було відносно нижче. Україна не приймала участі в такому аналізі, але за власними спостереженнями можна сказати що зростання віддалених вакансій можно співвідносити до європейських країн. [2]

Метою доповіді є дослідження можливих концепцій віддалених робочих місць з налаштуванням функцій безпеки.

Слід зазначити, що найбезпечнішою концепцією слід вважати віддалені робочі столи, але й найдорожчою серед представлених, що робить її використання доцільним лише у випадках коли необхідно забезпечити максимально безпечний рівень роботи віддаленого співробітника. Із інших концепцій слід відмітити подвійну операційну систему та підготовку віртуальних робочих станцій, які на відміну від інших за свою ціну можуть забезпечити достатній рівень безпеки.

Список літератури

1. 2020's Remote Work Statistics URL: https://review42.com/remote-work-statistics/ (дата звернення: 03.09.2024)

2. Global Data Shows Surge in Remote Work. URL: https://business.linkedin.com/talent-solutions/blog/trends-and-research/2020/global-data-shows-surge-in-remote-work (дата звернення: 03.09.2024)

РОЗРОБКА СИСТЕМИ УПРАВЛІННЯ ЗАТРИМКАМИ ЧАСУ ПРИ ОНОВЛЕННІ ДАНИХ В ГІБРИДНИХ ХМАРНИХ СИСТЕМАХ

Шевченко І.О., Дуков А.В., Лисенко Д.О., Рог В.Є.
Харківський національний університет Внутрішніх справ, Харків, Україна

На сьогоднішній день хмарні обчислення використовують мільярди фізичних пристроїв по всьому світу, які підключені до Інтернету, та за допомогою хмарних систем аналізують і обробляють величезну кількість даних. Гібридна хмарна система особливо цінна для динамічних або дуже мінливих навантажень. У зв'язку з можливими перебоями в роботі різних провайдерів багато користувачів вдаються до реплікації даних.

Метою доповіді є розробка системи управління затримками часу при оновленні даних в гібридних хмарних системах.

Проведений огляд архітектури існуючої гібридної хмарної системі з налагодженим механізмом управління затримками часу показав, що для необхідно вирішити проблему нелінійної залежності завдань та проблему підтримки адаптивного рівня узгодженості даних. У ході досліджень було реалізовано систему управління затримками часу при оновлені даних у гібридних хмарних системах, яка складається з наступних частин: будування гібридної хмарної системи, обчислення затримок, впровадження затримок. Після реалізації системи управління затримками було виявлено, що вона обчислює та впроваджує затримки точніше за все, коли усі сервери баз даних налаштовані зі схожими конфігураціями.

Список літератури

1. Хмарні технології // електрон. текст. дані URL: https://dduvs.in.ua/wp-content/uploads/files/Structure/library/student/lectures/2020 /eib/N/011.docx

2. Гібридна хмарна система // електрон. текст. дані URL:https://azure.microsoft.com/ru-ru/overview/what-are-private-public-hybrid-clouds/

ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІС ЗА ДОПОМОГОЮ МЕТОДІВ НЕЧІТКОЇ ЛОГІКИ

Якименко І.В., Хавіна І.П
Харківський національний університет внутрішніх справ, Харків, Україна
Зав'ялова О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному середовищі зростаючих кіберзагроз інформаційні системи (ІС) потребують комплексного підходу до забезпечення безпеки, що включає оцінку ризиків як ключовий елемент захисту. Традиційні методи аналізу ризиків можуть виявитися недостатньо ефективними в умовах великої кількості факторів і значного рівня невизначеності. Методи нечіткої логіки дозволяють застосовувати багатофакторні та адаптивні підходи до оцінки

ризиків, що особливо важливо при аналізі ризиків для інформаційних систем різних типів [1].

У роботі [2] аналізуються різні моделі оцінки ризиків інформаційної безпеки, де підкреслено, що традиційні підходи часто обмежені через неврахування різноманітності потенційних загроз і невизначеності параметрів системи. В той же час, використання нечітких множин дає змогу проводити детальну і комплексну оцінку, враховуючи не лише ймовірність та наслідки загроз, але й ступінь вразливості інформаційних ресурсів.

Мета дослідження полягає в розробці рекомендацій щодо використання методів нечіткої логіки для оцінки ризиків інформаційної безпеки ІС, що дозволить створити систему, яка враховуватиме множинні фактори ризику і надають гнучкі можливості для адаптації під різні типи загроз та рівні захищеності. Підхід на основі нечіткої логіки є особливо важливим для систем, що функціонують у середовищах з високим ступенем автоматизації, оскільки дозволяє зменшити ймовірність помилкових рішень у ситуаціях з нестабільними даними та змінними параметрами.

У роботі аналізуються загрози інформаційної безпеки ІС та обираються найбільш значущі критерії. Урахування вагових коефіцієнтів впливу критеріїв в класичній постановці не містить труднощів при застосування, а прикладів застосування у нечіткій постановці в досяжному інформаційному просторі авторами не виявлено. Тому запропоновано нові підходи стосовно урахування вагових коефіцієнтів загального впливу критеріїв при нечіткої постановці задачі. Для розв'язання завдання оцінки ризиків ІС використовуються три системи нечіткого висновку: одна для оцінки ймовірності реалізації загрози, інша для оцінки ймовірних збитків та остання для оцінки ризику інформаційної безпеки системи. Наведено тестові приклади розрахунків оцінки ризику ІБ. Реалізована експертна система за допомогою Fuzzy Logic [3]. Результати роботи системи є основою для підтримки прийняття рішень у системах управління інформаційною безпекою. Проведене комп'ютерне моделювання стосовно урахування вагових коефіцієнтів загального впливу критеріїв у нечіткій постановці показало працездатність підходу. Застосування методів нечіткої логіки для оцінки ризиків інформаційної безпеки може значно підвищити ефективність заходів захисту ІС та знизити ймовірність інцидентів. Використання таких підходів дозволяє створити комплексну систему оцінку ризиків та автоматизувати процес підтримки прийняття рішень у системах управління захистом ІБ.

Список літератури

1.Прохорова О.М. Моделі і методи нечіткої логіки: навч. посіб. [Рукопис] / О.М. Прохорова, Н. В. Кальчук; *НАУ "ХАІ"*. – Х., 2021. – 166 с.

2.Замула А. А., Северинов А. В., Корниенко М. А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации //*Наука і техніка Повітряних Сил Збройних Сил України*. – 2014. – №. 2. – С. 133-138.

3. Matlab-online. https://nl.mathworks.com/products/matlab-online.html

ДОСЛІДЖЕННЯ ЗМІСТУ ОРГАНІЗАЦІЙНОЇ СКЛАДОВОЇ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ

Гончаров К.В., Хавіна І.П
Харківський національний університет внутрішніх справ, Харків, Україна
Зав'ялова О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах інформаційної безпеки інформаційних систем (ІС) все більш важливим стає використання комплексної системи захисту інформації (КСЗІ), яка забезпечує захист не тільки за допомогою технічних, але і організаційних заходів. Організаційна складова є важливою частиною для забезпечення загальної безпеки системи, оскільки вона включає заходи адміністративного, обмежувального та регуляторного характеру, які дозволяють координувати та оптимізувати дії учасників процесу [1]. У рамках цієї роботи розглянуто зміст і значення організаційної складової КСЗІ, що передбачає визначення основних документів, а також важливість застосування методів кількісної оцінки її ефективності [2].

Організаційна складова КСЗІ включає комплекс заходів, серед яких: розроблення документів з різних напрямів захисту інформації в АС; внесення змін і доповнень до чинних в АС документів з урахуванням змінення умов (обставин); розроблення й впровадження нових організаційних заходів із захисту інформації; обґрунтування необхідності застосування та впровадження нових засобів захисту інформації; координація робіт з іншими підрозділами організації або зовнішніми організаціями на всіх етапах життєвого циклу АС; перегляд результатів виконання затверджених заходів і робіт із захисту інформаціїЗгідно з нормативними вимогами, організації зобов'язані дотримуватися законодавства у сфері захисту персональних даних та інформаційної безпеки ІС.

Метою доповіді є апробація запропоновано підходу до кількісної оцінки ризиків ІБ з урахування додержання норм та організаційних заходів на підприємстві. На основі побудованої математичної моделі системи захисту проведено аналіз системи захисту та отримано список ранжируваних засобів контролю за підсумковим впливом на актуальні загрози ІС. Моніторинг ІБ заснований на запропонованому підході дозволить підтримувати ІБ в актуальному стані, оперативне розробляти рекомендації щодо зниження рівня ризику і вживати ефективних заходів по усуненню можливих (або виявлених) загроз.

Список літератури

1. Озарко, К. і Андрухів, Т. (2022) «Особливості формування оптимальних організаційних структур управління іт-бізнесом як елемент його інформаційної безпеки», Економіка та суспільство, (43). doi: 10.32782/2524-0072/2022-43-21.

2. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Ігнатьєв Ю.Ю., Тулупов В.В.
Харківський національний університет внутрішніх справ, Харків, Україна

В сучасному світі проблеми забезпечення інформаційної безпеки привертають пильну увагу як фахівців в області комп'ютерних систем і мереж, так і численних користувачів, включаючи компанії, що працюють в сфері електронного бізнесу.

Актуальність теми полягає в тому, що неможливо досягти необхідного рівня безпеки комп'ютерних систем і мереж без знання і компетентного застосування сьогоденних технологій, стандартів, протоколів і засобів забезпечення кібербезпеки.

Наприклад, проблема втрати хоча б одного з декількох серверів з даними все одно може спричинити загрозу цілісності та повноти інформації. З огляду на ситуацію в світі та нові військові конфлікти, виникає гостра необхідність у створенні рішення для подолання цих проблем.

Метою доповіді є аналіз методів та засобів, що застосовуються для протидії кіберзлочинам в електронних комунікаціях.

В доповіді наводяться визначення загальних проблем міжмережевої взаємоії та процесу аналізу кіберзагроз.

Розглянуто спеціальні політики безпеки мережевої взаємодії, основні види кіберзагроз, програмно-апаратні, мережні та хмарні засоби протидії кіберзагрозам.

Проаналізовано, які переваги надає впровадження сучасних освітніх технологій та навчання в галузі кібербезпеки. Розглянуто питання необхідності політик та процедур безпеки.

Досліджено причини необхідності впровадження освіти та навчання в галузі кібербезпеки.

Розглянуто переваги створення культури обізнаності про кібербезпеку.

У висновках слід відмітити особливості кожного розглянутого засобу протидії кіберзлочинності та визначити необхідність їх застосування.

Список літератури

1. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

2. Тулупов В.В., Чуєв В.О. Аналіз систем убезпечення віддаленого доступу в розподілених обчислювальних системах. Проблеми інформатизації: одинадцята міжнародна науково–технічна конференція С.– 21. doi: https://doi.org/10.32620/PI.23.t2

USE OF ARTIFICIAL INTELLIGENCE IN AUTHENTICATION ALGORITHMS BASED ON ZERO WATERMARKS

Poddubnyi V.O., Gvozdov R.Y., Sievierinov O.V.
Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

In recent years, artificial intelligence has made significant progress, it is no longer a highly specialized technology that is developed for specific tasks, it is a multifunctional tool that is used daily by scientists and engineers in various fields of activity. Zero digital watermarks are a fairly new technology that is currently undergoing a process of rapid modernization [1]. Having previously appeared as a technology for checking the authorship of objects without their modification (as in a "normal" watermark), authentication methods based on a zero watermark appeared [1]. Combining artificial intelligence and zero-watermarking technologies for authentication algorithms can improve the common schema of zero-watermarking technologies. **The purpose of the report** is to analyze promising ways of integrating AI into such algorithms.

Artificial intelligence is used in many areas of human life, such as medicine, entertainment, education, security, data analysis, photo editing, and others.

AI has been very active in the field of image processing, be it medical images, real-time video from a drone or a car.

Also, AI is actively used to detect anomalous activity, finding objects or sets of data that do not correspond to a common pattern.

Generation of new content according to given key parameters is also one of the functions of AI.

These basic tasks can help in a zero-watermark based authentication algorithm. We will consider them in more detail in the following sections [2].

A traditional digital watermark hides information about the owner or creator of an image or images somewhere in that image.

This hidden information can later be used for many purposes: preserving the integrity of the image, detecting intentional or accidental tampering, protecting data copyright, etc.

Zero digital watermarking (zero watermark) is a method of creating a watermark for images, which aims to minimize the effect of the watermark on the visual quality of the image. This method uses the " zero visibility " (zero visibility), which means that the watermark is invisible to the human eye[3, 4].

In this paper, we will not focus on the principles of operation of a specific watermark algorithm, or on a specific authentication scheme [5].

So, as described in the previous sections, a promising way to combine AI and zero watermarks for authentication algorithms is:

- using AI to generate insults;
- using AI in the watermarking algorithm to detect key image parameters;
- using AI in the watermarking algorithm for image preprocessing;
- detection of anomalies in authentication algorithms.

AI can be used to generate unique images that will serve as the user's key. The user can generate such an image with the help of key phrases and salts (for example, the user ID in the system), which will serve to restore the image key. Such generation is necessary to standardize the types of key-images in the system, their better processing by the algorithm itself, and to preserve the confidentiality of the image x confidence that such an image did not exist before.

In the watermarking algorithm itself, AI can perform the role of detecting key image parameters working according to the given keys. Currently, this is done by mathematical functions, but the use of AI can make the algorithm more flexible and stable. AI can be used before image processing, finding areas of interest in the image and discarding "graphic garbage" caused by image corruption. In combination with classical mathematical algorithms, this can increase the stability of the zero sign algorithm.

In the authentication algorithm itself, AI can be used to find authentication anomalies. In this way, AI can detect attempts to sort key-images by analyzing patterns between sets of data transmitted by the user. Also, AI can monitor abnormal user behavior that is not typical for him (login at certain times of the day, log in from other addresses, etc.).

The AI techniques described above can help improve the digital watermark and authentication algorithm, but the use of AI is not limited to them.

Therefore, the use of AI in authentication algorithms based on zero watermarks can improve their performance.

AI can serve as an auxiliary tool in such algorithms, performing only specific operations (such as generating an image or searching for anomalies), as well as the main method of watermarking. AI can be used in combination with classical mathematical algorithms and authentication protocols, its flexibility allows to be a multifunctional tool. Forms and methods of combining AI and authentication algorithms based on zero watermarks are quite interesting and promising, so they require further research.

References

1. A. Zulfiqar and MH Fazal-e-Amin, "A Novel Fragile Zero Watermarking Algorithm for Digital Medical Images", Electronics, vol. 11, 710, 2022, doi : https://doi.org/10.3390/electronics1105 0710

2. Stuart Russell, Peter Norving, " Artificial Intelligence: A Modern Approach", Third Edition, Pearson Education, Inc. 2010

3. Zheng Q., Liu N. and Cao B., "Zero-Watermarking Algorithm in Transform Domain Based on RGB Channel and Voting Strategy", J Inf Process Syst, vol. 16, no. 6

4. Asha Rani, Amandeep K. Bhullar, Deepak Dangwal, Sanjeev Kumar. A Zero-Watermarking Scheme using Discrete Wavelet Transform. – Procedia Computer Science – 2015 – Volume 70. – pp. 603-609;

5. Gvozdov, R., Poddubnyi, V., Sieverinov, O., Buhantsov, A., Vlasov, A., Sukhoteplyi, V. Method of Biometric Authentication with Digital Watermarks // IEEE 8th International Conference on Problems of Infocommunications, Science and Technology, PICS&T 2021 - Proceedings, 2021, pp. 569–571.

DETECTION OF ACOUSTO-ELECTRIC CHANNELS OF INFORMATION LEAKAGE

Pavlenko Y.S., Oleynikov A.M.
Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

Acousto-electric information leakage channels (AEILC) are channels that arise from the conversion of acoustic signals into electrical signals, which can be intercepted by malicious actors. These channels may be unintentionally created due to the design features of electronic devices.

Methods for studying acousto-electric information leakage channels include analysis of device designs, measurement of acoustic signals, modeling of acousto-electric conversions, expert examination.

Studying the design of electronic devices aims to identify potential paths for acoustic information leakage, using specialized equipment to measure the level of acoustic noise generated by electronic devices. Creating mathematical models to predict the level of acoustic signals that could be intercepted by attackers, and involving experts in acoustics and electronics to conduct research and develop recommendations for information protection [1-3].

The purpose of the analysis is to objectively determine whether signals from technical devices go beyond the controlled area, in particular, to identify information leakage channels. In this context, various potential leakage paths are considered, and the risk level for each of them is assessed.

A classification of information leakage channels, covering both direct and indirect acousto-electric pathways, is provided. Mathematical models describe channel mechanisms, clarifying conditions for potential leakage. Detection methods include signal analysis, noise measurements, and advanced modeling of signal transformations to identify acousto-electric leakage risks effectively [4, 5].

References

1 Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Київ: ДУТ-КНУ, 2016. 178 с.

2 Голев Д., Кононович В., Хомич С. Методики оцінки інформаційної захищеності телекомунікацій. Одеса: ОНАЗ, 2013. 218 с.

3 Засоби та системи технічного захисту інформації: Навчальний посібник для студентів ЗВО / І.Є. Антіпов, А.М. Олейніков, Ю.В. Ликов, В.Д. Кукуш, І.О. Милютченко. Харків: ХНУРЕ, 2019. 216 с.

4 Олейніков А.М. Методи та засоби захисту інформації Навчальний посібник для студентів вищих навчальних закладів (з грифом МОН України). Харків: НТМТ, 2014. 298с.

5 Солодкий В., Тимофеев В. Технічні засоби захисту інформації з обмеженим доступом. Харків : ХНУРЕ, 2013. 229 с.

INVESTIGATION AND COMPARATIVE ANALYSIS OF FULEECA AND BISCUIT POST-QUANTUM DIGITAL SIGNATURE ALGORITHMS

Telnova A.A., Hrinenko T.O.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
Nariezhnii O.P.
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine

The first quantum processors began to appear in the early 2000s, and their development has not stopped since then. The development of quantum processors raises the issue of developing cryptographic algorithms whose stability will remain satisfactory even after the creation of quantum computers whose power will be sufficient to pose a threat to all modern cryptography.

Among others, this issue is being studied by the NIST organization – the National Institute of Standards and Technology. Thus, in response to the significant development and progress of quantum computing, in December 2016, NIST published a public call for applications for participation in the Post-quantum cryptography standardization process to select quantum-resistant cryptographic algorithms [1].

The purpose of the work is to study and analysis the FuLeeca and Biscuit algorithms that participate in the NIST competition to determine their ability to ensure the security of electronic signatures in the post-quantum period, to assess their effectiveness and practicality of implementation in various systems, and to identify possible areas for improving these algorithms.

The paper discusses the basics of FuLeeca and Biscuit algorithms, including quasi-cyclic Lie codes and multidimensional computation; analyses the speed of key generation, signature, and signature verification for both algorithms; estimates the computing resource requirements and implementation efficiency; assesses the resistance of the algorithms to classical and quantum attacks; and identifies the advantages and disadvantages of each algorithm in the context of modern threats. As a result of the study, the FuLeeca and Biscuit algorithms were compared by various criteria.

The data show that FuLeeca demonstrates high speed and efficiency and ease of implementation. Biscuit provides high resistance to quantum attacks due to its utilization, but requires more computing resources. Therefore, FuLeeca is suitable for applications that require high performance and speed of key and signature generation, but can reduce security requirements. Biscuit is recommended for critical applications with high security requirements where the main factor is resistance to quantum attacks, such as in government and military systems.

References

1. Additional PQC Digital Signature Candidates Announced | Computer Security Resource Center. URL: https://csrc.nist.gov/news/2023/additional-pqc-digital-signature-candidates (date of access: 25.05.2024).

ВИКОРИСТАННЯ СИСТЕМ EDR ДЛЯ ПРОТИДІЇ ШКІДЛИВОМУ ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННЮ

Сєвєрінов О.В., Балагура Д.С., Семенова К.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Кіберінциденти з атаками на інформаційні системи українського бізнесу показала, що класичні способи захисту виявляються безсилими проти шкідливого програмного забезпечення, нових вірусів, особливо вірусів-шифрувальників.

Метою доповіді є аналіз нових рішень виявлення та реагування на сучасні загрози кінцевим точкам (EDR).

Виявлення та реагування на загрози кінцевим точкам (EDR) - це основний спосіб забезпечення кібербезпеки, який масово використовується на сьогодні [1-3].

EDR пропонується як ідеальна відповідь на швидкозмінну ситуацію загроз, з якою до того часу боролися, насамперед, за допомогою AV-рішень. Ці загрози включали експлойти, шкідливе програмне забезпечення нульового дня та безфайлові атаки.

Попри те, що на сьогодні, традиційні EDR визнано досить ефективним проти багатьох передових загроз, існує нова та покращена категорія рішень "EDR наступного покоління". Окрім звичайних можливостей нове покоління включає додатковий рівень захисту від основних векторів атак (таких як користувачі та мережі) [1-3].

Щоразу, коли зловмисник виявляє активність, виникає аномалія в інформаційній системі. Це основне припущення, яке потрібно взяти до уваги, бо дії, спрямовані на компрометацію даних та ресурсів, не є звичайною діяльністю. Можливість ідентифікувати ці дії - це те, що дозволяє програмним та програмно-апаратним рішенням безпеки та аналітикам загроз ідентифікувати та заблокувати атаку.

Ці аномалії відбуваються в трьох основних місцях: виконання процесів, мережевий трафік або активність користувачів. EDR чудово справляється із цією задачею, оскільки знаходиться на кінцевій точці та контролює поведінку процесу. Це означає, що організація отримує надійний захист від таких видів загроз. Але мережевий трафік та поведінка користувачів також є критичними областями, і основні вектори можуть працювати там, не викликаючи жодних ознак аномалій. EDR майже повністю сліпий до таких видів загроз [4].

Більшість зловмисників, з часом, стають все далі просунутими в підборі сценаріїв, і одна з речей, на яку вони звертають увагу, це те, які заходи захисту застосовуються.

Для протидії цим загрозам необхідно використовувати EDR нового покоління NG EDR, яка є комплексною системою з набором технологій, призначених для моніторингу, зображення і зберігання даних, які відстежують всі дії, що відбуваються в кінцевих точках. Ці дані збираються в

централізованому сховищі, де аналізуються. Захист проводиться в реальному часі, і якщо в процесі аналізу EDR виявить в якійсь із точок ознаки злому, автоматично починають використовуватися можливості швидкого реагування, а після усунення загрози відбувається відновлення до безпечних параметрів функціонування.

Основною метою NG EDR є ефективно та постійно захищати дані та інформаційні системи кінцевого користувача від шкідливого програмного забезпечення.

В роботі отримані результати порівняльного аналізу рішень класу виявлення та реагування на загрози на кінцеві точки наступного покоління (NG EDR) та традиційних антивірусів (Legacy AV) [5].

Включення NG EDR в організаційну архітектуру безпеки розширює можливості виявлення, реагування та відновлення після інцидентів кібернетичного характеру.

Таким чином, враховуючі стрімкий розвиток індустрії розробки шкідливого програмного забезпечення як в комерційних цілях (отримання фінансової вигоди), так в політичних (підміна контенту для дискримінації уряду, кіберрозвідка, кібервійна тощо) можна зробити висновки про необхідність використання передових технологій для захисту кінцевих точок в інформаційних системах з використанням NG EDR.

Цей проактивний підхід дозволяє організаціям нейтралізувати потенційні загрози ще до того, як вони зможуть скористатися наявними вразливими місцями, що значно покращує їхні позиції у сфері безпеки. Це дасть змогу протистояти новим викликам кіберагресії по відношенню не тільки користувача, але і держави в цілому.

Список літератури

1. What You Need to Know About Next Gen EDR. URL: https://threatpost.com/next-gen-edr/148626/

2. Баклан Я.А., Сєвєрінов О.В. Аналіз систем захисту кінцевих точок від складних загроз EDR (Endpoint Detection and Response) // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: матеріали дванадцятої міжнар. наук.-практ. конф. 2022. Баку–Харків–Жиліна.

3. Шуліка, К., Балагура, Д., Смірнов, А., Непокритов, Д., Литвин, А. (2024) «Метод використання сучасних систем захисту кінцевих точок (EDR) для убезпечення від комплексних атак», *Сучасний стан наукових досліджень та технологій в промисловості*, (2(28), с. 182–195. doi: 10.30837/2522-9818.2024.2.182.

4. Шуліка, К., Балагура, Д., Сидоренко, З. (2024). Аналіз методів обходу сучасних систем захисту кінцевих точок EDR. *Радіотехніка*, *2*(217), 64–68. https://doi.org/10.30837/rt.2024.2.217.05.

5. What is Next Generation Endpoint Security? URL: https://www.sentinelone.com/cybersecurity-101/endpoint-security/next-generation-endpoint-security/

ЗАХИСТ ІНФОРМАЦІЇ У СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Деркач Я.О., Агеєв Д.В.
Харківський національний університет радіоелектроніки, Україна

Відповідно до сучасних досліджень [1, 2] на IoT припадає понад 30% усіх підключених до мережі пристроїв середнього підприємства. 57% цих пристроїв уразливі до атак середнього або високого рівня.

Крім того, база даних Gartner Machina IoT Forecast прогнозує, що до 2030 року на підприємствах буде понад 18 мільярдів підключених пристроїв.

Крім того, 98% усього трафіку Інтернету речей є незашифрованим.

Незашифровані дані, що надходять із некерованих пристроїв IoT, потенційно можуть призвести до витоку даних або успішної атаки програм-вимагачів.

Метою доповіді є аналіз методів захисту інформації у системах інтернету речей.

Проведений аналіз показав, що поширеними атаками на IoT є [2-4]:

- DDoS-атака. Аномально висока активність може призвести до значних затримок у роботі системи або взагалі її зупинки. Вдало скоригована та налаштована DDoS-атака може викликати системну помилку компонента безпеки, приховуючи реальні шкідливі дії;
- експлойт програмного забезпечення. багато кіберзлочинців використовують відомі вразливості в програмній частині пристрою для проведення атаки;
- MITM-атака. Хакери можуть перехопити мережевий трафік (вставши посеред каналу передачі між пристроєм відправником та пристроєм одержувачем) та отримати облікові дані або конфіденційну інформацію, яку пристрої IoT передають через корпоративні мережі;
- фізичне втручання. Простого підключення кіберзлочинцем USB флешки зі шкідливим кодом, до зовнішнього пристрою IoT достатньо, щоб поширити шкідливе програмне забезпечення через мережу і шпигувати по комунікаціях, що проходять в ній;
- брутфорс атаки. В компаніях зазвичай не приділяється достатньо уваги парольній безпеці пристроїв IoT, що робить їх вразливими до потенційних атак грубою силою.
- перехоплення прошивки. Якщо оновлення мікропрограми пристрою не було підписано криптографічно або прошивка передається по незахищеному каналу зв'язку – це дозволяє зловмисникам перехопити її та завантажувати шкідливе ПЗ на пристрої під виглядом апдейтів.

Для захисту від цих атак необхідно використовувати низку заходів [2-4].

1. Управління поверхнею атаки, інвентаризація та моніторинг усіх пристроїв. Адміністратори безпеки повинні знати точну кількість використовуваних пристроїв, а також ідентифікатори виробників, серійні номери, версії обладнання та прошивки. Моніторинг, аналіз та звітність у

режимі реального часу є вкрай важливими для організацій, щоб мати можливість керувати ризиками Інтернету речей.

2. Сегментація мережі. Сегментація запобігає отриманню зловмисником доступу до всієї мережі організації, обмежуючи поверхню атаки та мінімізуючи збитки.

3. Встановлення надійних паролів для IoT. Пароль має бути стійким для підбору, унікальним для кожного захищеного пристрою та відповідати політикам керування паролями організації.

4. Захист пристроїв IoT фізично. Фізичний захист пристроїв має дуже велике значення, оскільки IoT пристрої, доступні ззовні, можуть зазнати фізичного втручання зловмисників з метою отримання несанкціонованого доступу або завантаження в систему шкідливого ПЗ.

5. Своєчасні оновлення прошивок. Регулярне оновлення ПЗ значно покращує загальну безпеку IoT.

Виявлення атак і захист мережі IoT стали дуже складним завданням для механізмів безпеки, таких як системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS). Це призводить до великої затримки у виявленні атак і до збільшення кількості помилкових спрацьовувань, що генеруються поточними системами моніторингу. Для вирішення цього завдання необхідно для захисту в системах інтернету речей застосувати методи машинного навчання.

Перетворення захисту IoT пристроїв в автоматизовані політики, які захищають IoT в інфраструктурі, може зробити систему інтернету речей організації менш ризикованою.

Поєднання цих політик з повним спектром хмарних і локальних служб безпеки, щоб блокувати всі відомі та невідомі загрози, спрямовані на IoT. пристрій – це кінцева мета захисту інформації.

Впровадження ефективних стратегій кібербезпеки, регулярне оновлення програмного забезпечення та освіта користувачів допоможуть мінімізувати ризики безпеки у системах інтернету речей.

Список літератури

1. Anand Oswal. Securing IoT without Added Burden. URL: https://www.paloaltonetworks.com/cybersecurity-perspectives/expanding-iot-visibility.

2. IoT security survey reveals alarming challenges and costs. URL: https://www.iot-now.com/2023/10/18/137178-iot-security-survey-reveals-alarming-challenges-and-costs/.

3. Ge, Mengmeng, et al. "Deep learning-based intrusion detection for IoT networks." *2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC)*. IEEE, 2019.

4. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671-2701.

5. Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal, 61(12), 9395-9409.

АНАЛІЗ МЕТОДІВ КОРЕГУВАННЯ ПОМИЛОК В СТЕГАНОГРАФІЧНИХ СИСТЕМАХ НА ОСНОВІ ДНК ПЕРЕТВОРЕНЬ

Чиркін А.О., Федюшин О.І., Євгеньєв А.М.
Харківський національний університет радіоелектроніки , Харків, Україна

Метою доповіді є аналіз методів корегування помилок з використанням ДНК перетворень. ДНК, як носій інформації набуває популярності через її високу щільність зберігання даних і стійкість до зовнішніх впливів.

В доповіді наводяться алгоритми корегування помилок в стенографічних системах із застосуванням перетворень ДНК. В таких ІС інформація кодується на молекулярному рівні за допомогою нуклеотидних послідовностей, що вимагає ефективних методів корекції помилок, оскільки під час зчитування можливі різні похибки, зокрема заміни, вставки або видалення нуклеотидів [1, 2]. Причини цих помилок можуть включати неточності при синтезі ДНК, деградацію молекул або похибки секвенування.

Одним із підходів до корекції помилок є використання кодів з корекцією помилок (ECC), таких як коди Хеммінга або Рід-Соломона, які дозволяють виправляти певну кількість помилок у послідовностях [3]. Іншим ефективним методом є повторне кодування, коли критичні ділянки даних дублюються для збільшення ймовірності їх правильного зчитування. Консенсусне секвенування також може використовуватися для зменшення кількості помилок: воно передбачає проведення множинного зчитування однієї й тієї ж ДНК-послідовності та аналіз отриманих результатів для виділення найбільш достовірної послідовності.

Адаптивні методи корекції включають використання машинного навчання для прогнозування помилок у ДНК-послідовностях та їх автоматичної корекції, що може значно підвищити точність стеганографічних систем. Порівняння різних підходів показує, що кожен метод має свої переваги та обмеження. Наприклад, коди Хеммінга прості в реалізації, але здатні виправляти лише обмежену кількість помилок, тоді як більш складні алгоритми, такі як Рід-Соломон, мають вищу ефективність, але потребують більше обчислювальних ресурсів. Застосування методів корекції помилок значно підвищує надійність передачі інформації та може збільшити ємність стеганографічних систем [1, 2].

Список літератури

1. Основи стеганографії та методи захисту інформації. – Київ: Київський національний університет імені Тараса Шевченка, 2018. – 100 с. У книзі розглянуто класичні та сучасні методи стеганографії.

2. Сєвєрінов О., Євген'єв А. DNA Cryptosystem Using a Simple Replacement. – Інформаційні системи та технології, 2018. – С. 1–12.

3. Кушнір О.І., Тимочко О.І., Сєвєрінов О.В. "Аналіз методів завадостійкого кодування у цифрових системах зв'язку." Системи обробки інформації 9 (2007): 63-65.

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ZERO-KNOWLEDGE PROOFS (ZKP) ДЛЯ ПІДВИЩЕННЯ КОНФІДЕНЦІЙНОСТІ В БЛОКЧЕЙНАХ

Федюшин О.І., Колесников Д.І.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі технологія блокчейн стрімко розвивається і знаходить застосування в різних галузях, таких як фінанси, логістика, медицина, управління даними та інші. Однак, незважаючи на децентралізовану природу і високу безпеку, блокчейни мають одну серйозну проблему – конфіденційність даних. Більшість публічних блокчейн-платформ, таких як Bitcoin та Ethereum, забезпечують прозорість транзакцій, що може призвести до витоку конфіденційної інформації.

Відкритий доступ до історії транзакцій може стати причиною небажаного відстеження фінансових операцій та особистих даних користувачів [1]. Технологія Zero-Knowledge Proofs (ZKP) пропонує вирішення цієї проблеми шляхом забезпечення конфіденційності та верифікації інформації без необхідності її розголошення.

Метою даної роботи є дослідження та аналіз технології Zero-Knowledge Proofs як засобу забезпечення конфіденційності в блокчейнах, а також визначення її ефективності у підвищенні рівня приватності транзакцій та даних у децентралізованих системах. В рамках роботи ставиться завдання вивчити основні види ZKP, принципи їхнього функціонування, особливості застосування та переваги у блокчейн-середовищі.

Предметом дослідження є технологія Zero-Knowledge Proofs як інструмент забезпечення конфіденційності в блокчейнах, зокрема її види, принципи функціонування та можливості застосування для підвищення рівня приватності транзакцій і захисту даних у децентралізованих системах.

Завдяки можливості підтвердження інформації без її розголошення, ZKP має потенціал стати ключовим елементом у багатьох галузях, сприяючи створенню безпечних і прозорих систем. Але також має і обмеження. Серед них – складність реалізації і високе обчислювальне навантаження, що може обмежити масштабованість рішень, особливо в публічних блокчейнах. Необхідно також враховувати криптографічні ризики [2] та можливі вразливості, що можуть бути використані для компрометації приватності.

Список літератури

1. Ben-Sasson E., Chiesa A., Garman C., Green M., Miers I., Tromer E., Virza M. Zerocash: Decentralized Anonymous Payments from Bitcoin. In: Proceedings of the IEEE Symposium on Security and Privacy. – 2014. – С. 459-474.

2. Groth J. On the Size of Pairing-Based Non-interactive Arguments. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Berlin, Heidelberg, 2016. – С. 305-326.

АНАЛІЗ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ ХМАРНИХ СЕРВІСІВ З ВИКОРИСТАННЯМ НЕЙРОННИХ МЕРЕЖ

Марчук І.Ю., Федюшин О. І.
Харківський національний університет радіоелектроніки, м. Харків, Україна
Сухотеплий В.М.
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна

Хмарні обчислення стали важливою частиною сучасного бізнесу, адже вони дозволяють зберігати дані та працювати з програмами без необхідності мати власні сервери чи інфраструктуру. Це зручно, економічно вигідно, а доступ до інформації можна отримати з будь-якого місця. Але разом із перевагами зростає і кількість ризиків, пов'язаних із безпекою: витік даних, кібератаки, зловживання доступом [1]. Щоб забезпечити належний рівень захисту, все частіше використовують нейронні мережі - технології, які здатні аналізувати великі масиви даних, швидко помічати підозрілу активність і запобігати загрозам.

Метою цього дослідження є аналіз загроз та вразливостей у хмарних сервісах і розробка методів підвищення рівня їх захисту за допомогою нейронних мереж. Предметом дослідження є технології та програмні засоби, які дозволяють моделювати загрози й аналізувати можливості захисту даних у хмарних системах [2, 3]. Це актуальне завдання, адже хмарні сервіси відкривають широкі можливості для бізнесу, дозволяючи зекономити на IT-інфраструктурі, забезпечувати гнучкість у масштабуванні та полегшувати роботу з даними. Застосування нейронних мереж для захисту хмарних сервісів відкриває великі перспективи в боротьбі з кіберзагрозами [4]. Однак виклики все ще залишаються: можуть траплятися технічні збої, інколи складно перенести дані на інші платформи, а налаштування не завжди дозволяють гнучко адаптувати систему під конкретні потреби. Саме тому постійне вдосконалення технологій безпеки є таким важливим. Завдяки інноваціям хмарні сервіси стають більш надійними й зручними у використанні, забезпечуючи ще більше можливостей для роботи з даними та захисту важливої інформації.

Список літератури

1. Джанг-Джаккард, Дж., & Непал, С. *Огляд нових загроз у кібербезпеці //* Журнал комп'ютерних та системних наук, 2014.
2. Kavetskyi M.S., Sievierinov O.V., Gvozdov R.Y., Smirnov A.O. Використання машинного навчання для класифікації атак типу DOS/DDOS. Radiotekhnika, 2024. - 217, С. 55-63.
3. Рудий С.В., Сєвєрінов О.В. Дослідження моделі безпеки при використанні хмарних сервісів // ЧДТУ, ВА ЗС АР, УТіГН, НТУ "ХПІ", ХНУРЕ, "ПД ПКНДІ АП", 2022.
4. Гудфеллоу І., Бенджіо Й., Курвіль А. *Глибинне навчання /* Вид-во МІТ, 2016.

АУДИТ БЕЗПЕКИ ПРИ РОЗРОБЦІ ЗАХИЩЕНОГО МЕСЕНДЖЕРУ

Федюшин О.І., Ольховський М.Е.
Харківський національний університет радіоелектроніки, Харків, Україна

Зростаюча популярність інтеграцій різних платформ комунікації підвищила потребу у розробці безпечних рішень, які забезпечують захищену передачу даних між різними месенджерами, такими як Telegram, Instagram, Teams та інші. Ризики, пов'язані з обміном конфіденційною інформацією в умовах багатоплатформенності, роблять питання безпеки особливо актуальним. У цьому контексті виникає необхідність у впровадженні надійних систем, які забезпечують конфіденційність, цілісність та доступність даних навіть при складних інтеграціях [1].

Зі збільшенням інтеграцій зростає і кількість можливих кіберзагроз, оскільки кожне нове підключення може стати ціллю для атаки. Зокрема, бот-конектори, що використовують API інших месенджерів, таких як Telegram чи Instagram, мають ризики вразливостей, пов'язаних із особливостями API або захистом сторонніх платформ. Це вимагає постійного аудиту безпеки, щоб вчасно виявити та нейтралізувати потенційні слабкі місця, не допустивши витоку даних або несанкціонованого доступу.В умовах, коли обмін повідомленнями може відбуватися одночасно через кілька платформ, важливо забезпечити високий рівень автентифікації та авторизації, а також постійний контроль над потоком даних між сервісами. Вибір відповідних технологій, таких як TLS [2] для шифрування з'єднань та OAuth [3] для контролю доступу, є ключовим елементом у побудові захищеного інтегрованого середовища. Це дослідження покликане визначити найбільш ефективні підходи до захисту даних при інтеграції з іншими платформами.

Метою доповіді є дослідження стадій розробки та проектування архітектури додатку з підтримкою інтеграцій, проведення аудиту безпеки додатку та усунення вразливостей з огляду на можливість підключення зовнішніх платформ. Аудит безпеки [4] дозволяє оцінити захищеність системи, виявити потенційні загрози та розробити рекомендації щодо підвищення рівня безпеки у середовищах з інтеграціями. Постійне вдосконалення заходів безпеки є необхідним для протидії новим загрозам і забезпечення високого рівня захисту в умовах змінюваного кіберсередовища.

Список літератури

1. Арчакова А.І., Сєвєрінов О.В. Аналіз забезпечення конфіденційності інформації в сучасних мессенджерах // Комп'ютерні та інформаційні системи і технології, 2019

2. Why use TLS 1.3? | SSL and TLS [Електронний ресурс] / Режим доступу: https://www.cloudflare.com/learning/ssl/why-use-tls-1.3/

3. OAuth 2.0 [Електронний ресурс] / Режим доступу: https://oauth.net/2/.

4. Audit of Session Secure Messaging Application [Електронний ресурс] / Режим доступу: https://blog.quarkslab.com/audit-of-session-secure-messaging-application.html.

СИСТЕМА АВТОМАТИЗАЦІЇ СКАНУВАННЯ ВРАЗЛИВОСТЕЙ ТА ГЕНЕРАЦІЇ ЗВІТІВ

Федюшин О.І., Ващенко І.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Сканери вразливостей відіграють важливу роль у забезпеченні безпеки веб-додатків. Ці інструменти автоматизують процес виявлення загроз, що дозволяє швидко знаходити відомі уразливості, оцінювати рівень їх небезпеки і планувати необхідні заходи захисту [1]. Існує безліч спеціалізованих утиліт, які забезпечують пошук різних типів вразливостей, проте кожен інструмент має свої особливості, і жоден з них не може забезпечити повне охоплення можливих загроз [2]. Використання лише одного сканера може призвести до пропуску певних вразливостей, тоді як комплексне тестування з використанням різних інструментів дозволяє підвищити якість і ефективність виявлення загроз [3].

Тема даної доповіді присвячена автоматизації процесу сканування вразливостей веб-додатків за допомогою інтеграції різних інструментів для тестування безпеки. Основна ідея полягає у створенні інтегрованого інструмента, який дозволяє запускати різні сканери однією командою, зберігати результати тестувань у єдиному звіті, а також реалізовувати кілька варіантів автоматизації пошуку вразливостей. Це дає змогу оптимізувати процес тестування, зменшити кількість рутинних операцій та спростити обробку отриманих даних. Запропонований підхід передбачає інтеграцію низки різноманітних утиліт для тестування вразливостей, кожна з яких виконує свою специфічну функцію. Окрім швидкості та зручності сканування це також дозволить більш гнучко автоматизувати нові перевірки в залежності від їх складності.

Метою доповіді є дослідження розробки інтегрованого інструмента з використанням існуючих і власних утиліт для пошуку проблем безпеки. Цей підхід забезпечує широке охоплення потенційних вразливостей і дозволяє централізовано керувати тестуванням, що є значною перевагою для великих проектів або для випадків, коли потрібна регулярна перевірка стану безпеки. У рамках цієї доповіді буде розглянуто архітектуру розробленого сканера, особливості взаємодії з кожним з інструментів, а також результати тестування на практичних прикладах.

Список літератури

1. Poddubnyi V., Sievierinov O., Pustomelnik O. Менеджмент вразливостей як складова частина політики безпеки ІТС / Системи управління, навігації та зв'язку. Збірник наукових праць 4.62 (2020): 55-58.

2. Why You Can't Trust A Single Security Scanner [Електронний ресурс] / Режим доступу: https://www.linkedin.com/pulse/why-you-cant-trust-single-security-scanner-alphabravogov

3. When is One Vulnerability Scanner Not Enough? [Електронний ресурс] / Режим доступу: https://thehackernews.com/2024/05/when-is-one-vulnerability-scanner-not.html

ЗАХИСТ МОБІЛЬНИХ ПРИСТРОЇВ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Федюшин О.І., Микитенко М.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Багатофункціональність та доступність мобільних пристроїв зробили їх привабливою мішенню для кіберзлочинців, які розробляють різноманітні типи шкідливих додатків для отримання несанкціонованого доступу до інформації, шпигунства, викрадення даних та фінансових махінацій [1]. На тлі цього зростає кількість атак на мобільні телефони, зокрема через шкідливі додатки, що створює серйозні ризики для користувачів. Згідно з останніми дослідженнями, кількість атак на мобільні пристрої зростає з кожним роком [2]. Наприклад, у 2023 році було виявлено понад 2 мільйони нових шкідливих додатків для мобільних телефонів [3]. Основними цілями таких атак є отримання доступу до конфіденційної інформації, фінансові операції та встановлення контролю над пристроєм. Часто користувачі недооцінюють небезпеку завантаження програм з неперевірених джерел або нехтують налаштуваннями безпеки, що полегшує роботу зловмисників. Це підвищує актуальність дослідження методів захисту мобільних телефонів від шкідливого програмного забезпечення.

Метою даної роботи є дослідження основних типів шкідливого програмного забезпечення, що загрожує мобільним телефонам, а також розробка рекомендацій щодо ефективного захисту користувачів від подібних загроз. Основний акцент робиться на методах захисту, що використовуються операційними системами Android та iOS, а також на аналізі ефективності сучасних антивірусних рішень і захисних систем.

Предмет дослідження – шкідливе програмне забезпечення для мобільних пристроїв та методи захисту від нього, що включають різні механізми безпеки та стратегії мінімізації ризиків інфікування.

Застосування багатофакторної автентифікації, контроль доступу додатків, шифрування даних, регулярні оновлення програмного забезпечення та використання антивірусних програм є ключовими заходами для забезпечення безпеки мобільних пристроїв. Важливо, щоб користувачі усвідомлювали необхідність дотримання цих заходів для захисту своїх даних і збереження конфіденційності.

Список літератури

1. Сєвєрінов, О. В., et al. "Аналіз загроз персональним даним в мобільному пристрої під час використання різноманітних додатків / Системи озброєння і військова техніка, 2016, №4 (48), С. 42-45.

2. Кількість користувачів смартфонів в Україні збільшилася до 85% — дослідження [Електронний ресурс]. – Режим доступу: https://ms.detector.media/

3. Платоненко А.В. Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах. Матеріали Науково-технічної конференції «Світ телекомунікації та інформатизації». – ДУТ. – 2015 р. – С. 40-44.

АНАЛІЗ ТА ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ТЕСТУВАННЯ СЕРВІСІВ ТА САЙТІВ

Суранов А.Р., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Тестування веб-ресурсів стає необхідним етапом для забезпечення їхньої продуктивності, безперебійної роботи і захисту від потенційних збоїв [1].

Метою доповіді є аналіз та розробка математичних моделей і методів тестування, які дозволяють оцінити надійність і функціональність веб-сервісів та сайтів, адаптованих до сучасних вимог високого навантаження та самоподібності запитів користувачів. **В доповіді** наводяться результати досліджень із використанням інструментів автоматизації тестування, зокрема QuickTest Professional (QTP) [2] та Apache JMeter [3], які дозволяють комплексно оцінити продуктивність системи. Застосування QTP забезпечує високу ефективність проведення функціонального тестування, дозволяючи автоматизувати перевірку регресії і, таким чином, знизити трудомісткість та зменшити ймовірність людських помилок. В автоматизованому режимі QTP протестована функціональність основних компонентів веб-сайтів, що дозволило переконатися у відповідності результатів роботи заявленим специфікаціям. Це особливо важливо для систем, де критичною є точність обробки запитів користувачів, як-от в платіжних та інформаційних сервісах.

Для дослідження продуктивності та масштабованості веб-сервісів було використано Apache JMeter, що надав змогу провести навантажувальні та стрес-тести системи. За допомогою JMeter було виконане моделювання навантажень від великої кількості одночасних користувачів, що дозволило виявити вузькі місця системи і провести оптимізацію для підтримання стабільної роботи. Ці результати свідчать про здатність веб-сервісів витримувати пікові навантаження і забезпечувати високу якість обслуговування в умовах інтенсивного трафіку.

Отримані результати показали, що створення детальної проектної документації є ключовим фактором успішного проведення тестування, оскільки вона містить інформацію про функціональні вимоги системи, її обмеження та очікувану поведінку. Також важливими є розробка та підтримка тестових планів, сценаріїв та чеклістів, які визначають послідовність та охоплення тестів. Документування результатів у вигляді баг-репортів і звітів сприяє вчасному виявленню та усуненню помилок, а також підвищує прозорість процесу тестування для всіх учасників проекту.

Список літератури

1. Д’якова Н.Є., Сєвєрінов О.В. Тестування вразливостей сучасних вебресурсів, НТУ «ХПІ»,. – 2022.

2. Mercury Interactive Corporation “Mercury QuickTest Professional Advanced Features User’s Guide", 1992-2006. https://support.microfocus.com.3. Apache Software Foundation “User`s Manual”, https://jmeter.apache.org/usermanual.

ОНЛАЙН-СЕРВІСИ З НАДАННЯ ПОСЛУГ ГЕНЕРУВАННЯ КЛЮЧОВИХ ДАНИХ

Гріненко Т.О., Гирченко І.Р.
Харківський національний університет радіоелектроніки, Харків, Україна

Аналіз та дослідження сервісів генерації ключових даних є критично необхідним для забезпечення безпеки сучасних інформаційних систем. На даний час існує багато методів побудови даних генераторів [1].

Онлайн-сервіси для генерації ключових даних відіграють важливу роль у криптографічних системах, забезпечуючи користувачів інструментами для створення унікальних криптографічних ключів та інших даних, необхідних для захисту конфіденційної інформації. Однак якість ключів, що генеруються цими сервісами, може варіюватися, і ненадійні платформи можуть продукувати слабкі ключі, що підвищує ризики для безпеки даних.

Метою доповіді є аналіз та дослідженні різноманітних сервісів та сайтів, які надають послуги з генерації ключових даних.

Зростання кількості сервісів для генерації ключових даних від класичних рішень, що базуються на локальних алгоритмах шифрування, до хмарних платформ, які надають централізоване управління ключами, обумовлює необхідність аналізу та дослідження якості надання послуг та захищеності від потенційних загроз [2, 3].

Найбільш поширеними на сьогодні є сервіси генерації ключових даних, які охоплюють як державні, так і міжнародні рішення, спрямовані на забезпечення безпеки. Серед них виділяються Персональний сервіс довірчих послуг, а також хмарні платформи, такі як AWS Key Management Service (KMS) і Google Cloud Key Management Service (KMS). Ці сервіси використовують алгоритми шифрування, такі як AES та RSA, забезпечують централізоване управління криптографічними ключами і автоматичне шифрування даних.

Вибір надійних рішень сервісів генерації ключових даних, які відповідають актуальним стандартам безпеки, дозволяє знизити ризики компрометації даних і підвищити рівень захисту конфіденційної інформації. У контексті постійно зростаючих загроз важливо забезпечити не лише надійність генерації ключів, але й їхнє ефективне управління в умовах швидко змінюваного технологічного середовища.

Список літератури

1. Сєвєрінов О.В. Аналіз методів побудови генераторів псевдовипадкових послідовностей / Системи обробки інформації, №8, 2013, С. 198-201.

2. Causevic, A., Sundmark, D., and Punnekkat, S. (2010). An industrial survey on contemporary aspects of software testing. In Software Testing, Verification and Validation (ICST), 2010 Third International Conference on, pages 393–401.

3. Kasurinen, J., Taipale, O., and Smolander, K. (2010). Software test automation in practice: empirical observations. Advances in Software Engineering, 2010.

ПІДВИЩЕННЯ БЕЗПЕКИ ХМАРНОГО СХОВИЩА З ВИКОРИСТАННЯМ ШИФРУВАННЯ НА СТОРОНІ КЛІЄНТА

Азаренко А.П., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Метою доповіді є дослідження та обґрунтування методів та засобів захисту даних у хмарному середовищі з метою підвищення їх безпеки.

Шифрування на стороні клієнта є важливим методом захисту даних у хмарному середовищі, який дозволяє користувачам повністю контролювати доступ до своїх файлів. Одним з популярних рішень є використання бібліотек типу OpenPGP.js або CryptoJS, які забезпечують шифрування даних прямо на клієнтському пристрої перед завантаженням їх у хмарне сховище. При такому підході ключі шифрування зберігаються лише у користувача, що унеможливлює доступ до розшифрованих даних для хмарного провайдера або третіх осіб навіть у випадку зламу сервера [1]. Також широко застосовуються симетричні алгоритми шифрування, такі як AES-256, які поєднують високу швидкість шифрування та високу стійкість до зламу.

При використанні цього методу захисту забезпечується надійне управління ключами, що може бути вирішено шляхом використання менеджерів ключів або програмного забезпечення з підтримкою двофакторної аутентифікації. Наприклад, Keybase забезпечує захищене зберігання ключів, що допомагає зменшити ризики втрати доступу [2]. Інше рішення – інтеграція з платформами, такими як Boxcryptor, яка забезпечує автоматичне шифрування файлів перед їх завантаженням у сервіси, такі як Google Drive чи Dropbox. Важливим аспектом є також вибір стратегії відновлення даних, що дозволить користувачам не втратити доступ до інформації у разі втрати ключів.

Шифрування на стороні клієнта значно підвищує безпеку хмарного зберігання, оскільки надає користувачам повний контроль над конфіденційністю своїх даних, навіть у разі компрометації сервера постачальника послуг. Використання бібліотек, таких як OpenPGP.js і CryptoJS, забезпечує зручне шифрування, тоді як рішення на кшталт Keybase і Boxcryptor підсилюють управління ключами та безпеку зберігання. Хоча такі рішення вимагають додаткових ресурсів і управлінських зусиль від користувача, вони значно знижують ризик несанкціонованого доступу та підвищують стійкість даних у хмарному середовищі.

Список літератури

1. Джексон, М. Cloud Security: Protecting Data with Encryption and Key Management. Tech Books, 2021.Митчелл, Стефен. Web Scraping with Python: Collecting More Data from the Modern Web. O'Reilly Media, Inc., 2018.

2. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, 2020.

ІНТЕГРАЦІЯ БЛОКЧЕЙНУ З ІНФОРМАЦІЙНИМИ СИСТЕМАМИ УПРАВЛІННЯ

Бураков А.Р., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Інформаційні системи управління підтримують ключові державні та фінансові функції, такі як реєстрація населення, облік податкових записів і проведення банківських операцій. Більшість з них базуються на принципах Web 2.0, використовуючи централізовані сервери і бази даних [1]. Такі системи стикаються з критичними викликами: обмеженою масштабованістю, єдиними точками відмови та ризиком зловживань з боку адміністраторів.

Це породжує потребу у підвищенні надійності, захищеності та доступності даних. Децентралізовані системи на основі блокчейну [2] пропонують альтернативу, завдяки зміні архітектури даних. Використання розподілених блоків, пов'язаних криптографічними ґешами, забезпечує високу стійкість до зовнішніх втручань та усуває єдині точки відмови, що підвищує надійність і незмінність інформації.

Метою доповіді є дослідження структури блокчейну та обґрунтування інтеграції технології блокчейн у інформаційні системи управління з метою підвищення їх безпеки.

Впровадження блокчейну для зберігання і верифікації записів у системах управління посилює контроль над достовірністю інформації та мінімізує адміністративні помилки. Крім того, смарт-контракти [3], що виконуються на блокчейні, дозволяють автоматизувати бізнес-процеси і транзакції, знижуючи витрати на адміністрування та пришвидшуючи реагування на інциденти. Наприклад, блокчейн допоможе протистояти атакам типу «відмова в обслуговуванні», що в централізованих системах може призвести до повного зупинення роботи; розподілена структура унеможливлює подібну вразливість. Отже, блокчейн є перспективним рішенням для систем управління інформацією, яке дозволяє значно покращити їх захищеність, прозорість і ефективність. Завдяки децентралізації та криптографічним методам, блокчейн забезпечує високий рівень захисту даних та стійкості до маніпуляцій, що робить його технологією майбутнього для інформаційних систем управління.

Список літератури

1. Awan Setiawan. Blockchain-Based Management Information Systems: Benefits and Challenges. 2024. *Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)*, *3*(01), 1–8. DOI: https://doi.org/10.58471/esaprom.v3i01.3783

2. Tobias Guggenberger. On the Design and Management of Blockchain-Based Information Systems. 2023. DOI: https://epub.uni-bayreuth.de/id/eprint/7254/

What are smart contracts on blockchain? IBM. URL: https://www.ibm.com/topics/smart-contracts (accessed October 30, 2024)

БЕЗПЕКА ВЕБ ДОДАТКІВ ПРИ ВИКОРИСТАННІ СИСТЕМ УПРАВЛІННЯ КОНТЕНТОМ

Бичковський І.Ю., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Безпека веб-додатків є важливим аспектом розробки та підтримки сучасних веб-ресурсів, особливо при використанні систем управління контентом (CMS), які автоматизують розгортання та керування контентом. Зростання популярності таких платформ, як WordPress, Joomla, PrestaShop та OpenCart, призводить до виникнення ризиків, пов'язаних із потенційними вразливостями [1].

Метою доповіді є обґрунтування методів та засобів захисту веб-додатків при використанні систем управління контентом.

Ризики та загрози безпеці CMS. Системи управління контентом можуть бути вразливими до кібератак через недосконалості в програмному коді, особливо якщо використовуються застарілі плагіни або ненадійні теми. Найпоширенішими загрозами є SQL-ін'єкції, міжсайтовий скриптинг (XSS), а також уразливості, пов'язані з неправильною конфігурацією доступів [1, 2]. Такі атаки можуть спричинити витік даних або злам облікових записів користувачів.

Захист на рівні серверу та CMS. Забезпечення безпеки потребує додаткових налаштувань серверу та конфігурації самої CMS. Важливо приділити увагу саме забезпеченню безпеки серверу, а саме: закриттю непотрібних в роботі портів, оскільки зазвичай для роботи веб-додатків достатньо залишати відкритими лише 80 та 443 порти й обмежувати доступ до адміністративної панелі серверу. Варто налаштовувати передачу даних за HTTPS, що попередить атаку типу “man-in-the-middle”[3].

Забезпечення безпеки веб-додатків при використанні CMS є комплексним завданням, яке потребує врахування особливостей архітектури платформи, регулярного оновлення компонентів і використання сучасних методів захисту. Важливим є налаштування серверу, включно з закриттям непотрібних портів, обмеженням прав доступу та додатковими заходами захисту з боку CMS, такими як політика безпеки контенту та резервне копіювання. Застосування цих заходів зменшить ризик компрометації даних, підвищить стабільність веб-ресурсів і збереже їхню функціональність.

Список літератури

1. Kolomiitsev, S. O., Sievierinov, O. V., Fedorchenko, V. M., & Sukhoteplyi, V. M. (2023). Аналіз плагінів двофакторної автентифікації для системи WordPress. Radiotekhnika, (214), 26-31.

2. Рассел, Джеймс. SQL Injection Attacks and Defense, Second Edition. Syngress, 2012.

3. Митчелл, Стефен. Web Scraping with Python: Collecting More Data from the Modern Web. O'Reilly Media, Inc., 2018.

ТЕСТУВАННЯ САЙТІВ ТА СЕРВІСІВ З НАДАННЯ ПОСЛУГ ГЕНЕРАЦІЇ КЛЮЧОВИХ ДАНИХ

Гріненко Т.О., Олійник Е.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Сервіси та сайти з надання послуг генерування ключових даних забезпечують основу для криптографічного захисту даних, що дозволяє зберігати конфіденційність та захищати від несанкціонованого доступу.

Метою доповіді є аналіз та дослідження процесів тестування сайтів та сервісів, що надають послуги генерування ключових даних. **В доповіді** наводяться результати досліджень сервісу з надання послуг генерації ключових даних та результати тестування функціональності сервісу.

Результати проведення чотирьох фокус-груп показали, що хоча основні процеси та сценарії тестування підтримуються, існує явна потреба в забезпеченні тестування більш складних сценаріїв у реалістичних умовах, а також у збільшенні ступеня автоматизації [1]. Інші дослідження також свідчать про низький рівень впровадження інструментів тестування [2]. Дослідження виявляють, що 70% помилок виникають на етапах вимог і дизайну. Питання щодо словника, процесів, документації, методів та моделей оцінювання процесів для тестування надані в стандарті ISO/IEC/IEEE 29119.

Тестування критичного ПЗ включає методи альфа- і бета-тестування, позитивного і негативного тестування, а також ручного та автоматизованого тестування. Для сайтів і сервісів із генерації ключів були розроблені чеклісти для кожного етапу, що містять кроки перевірки верифікації особистих даних, генерації ключа, а також захисту даних. Проведено тестування функціональності сервісу DepositSign [3], що є провідним українським постачальником електронних довірчих послуг, який забезпечує клієнтів кваліфікованими електронними підписами (КЕП) та хмарним зберіганням ключів. Усі тести пройдені успішно, що підтверджує відповідність системи вимогам і її працездатність у реальних умовах.

Таким чином, тестування сайтів та сервісів, що надають послуги генерування ключових даних, є першочерговим кроком у процесі забезпечення якості програмного забезпечення. Підвищення рівня автоматизації тестування може значно зменшити витрати часу та ресурсів.

Список літератури

1. Knauss, A., Berger, C., and Eriksson, H. (2016). Towards state-of-the-art and future trends in testing of active safety systems. In Proceedings of the 2nd International Workshop on Software Engineering for Smart Cyber-Physical Systems, pages 36–42.

2. Causevic, A., Sundmark, D., and Punnekkat, S. (2010). An industrial survey on contemporary aspects of software testing. In Software Testing, Verification and Validation (ICST), 2010 Third International Conference on, pages 393–401.

3. Електронний сервіс DEPOSITSIGN. URL: https://depositsign.com/ (дата звернення 03.06.2024).

МЕТОД ВИКОРИСТАННЯ КІБЕРПАСТОК В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

Сєвєрінов О.В., Ярова О.С.
Харківський національний університет радіоелектроніки, Харків, Україна

На даний час для забезпечення захисту інформації в ІКС організації все частіше використовуються кіберпастки (honeypot). Honeypot унікальні, вони працюють нестандартно, але дуже ефективно, що дає змогу швидко розвиватися сфері захисту інформації.

Метою доповіді є опис роботи і оцінка важливості кіберпасток в кіберпросторі для підвищення захисту інформації в ІКС. В доповіді наводиться імітаційна кібератака на кіберпастку і реакція на цю атаку KfSensor. Наведений приклад роботи кіберпастки показує принцип роботи KfSensor і принципи захисту інформації використання кіберпасток.

На прикладі роботи VMware Pro 17 з ОС Windows 10, KfSensor, та Kali Linux описаний процес роботи кіберприманки і атаки на неї. KFSensor діє як приманка, призначена для залучення та виявлення хакерів і хробаків шляхом імітації вразливих системних служб і троянів. KFSensor попередньо налаштований для моніторингу всіх портів TCP і UDP разом із ICMP.

Навмисно «зручна» комп'ютерна система дозволяє хакерам використовувати вразливості і наносити по ним «удари» по пустим системам або напівпустим (деяка інформація, яка не має цінності – фальшивки), щоб можна було вивчати як відбулася атака. Застосування пастки можливе до будь-якого обчислювального ресурсу від програмного забезпечення до файлових серверів і маршрутизаторів, які будуть аналізувати стан кожного з цих ресурсів і надавати дані про атаки, збої тощо, і одночасно з цим, намагатимуться заважати робити чорним капелюхам свою справу, при цьому аналізуючи все, що відбувається в Honeypot. Конкретна робота кіберпастки залежить від її алгоритмів і маштабування.

Наразі з розвитком інформаційної безпеки T-Pot – це все в одному, опціонально розповсюджена багатоархівна (amd64, arm64) платформа honeypot, яка підтримує понад 20 honeypots і незліченну кількість опцій візуалізації за допомогою Elastic Stack, анімованих карт атак у реальному часі та багатьох інструментів безпеки для подальшого покращення досвіду обману. Апгрейд H-Pot безперервний.

Список літератури

1. Honeypot і Honeynet. URL: https://www.security-insider.de/was-ist-ein-honeypot-a-703883/.

2. Виявлення загроз для iot-пристроїв засобами Honeypots. URL: http://elartu.tntu.edu.ua/bitstream/lib/30383/2/IMST_2019_Belma_A-Detection_of_threats_to_iot_devices_23.pdf.

3. Онлайн-платформа для спільної розробки програмного забезпечення і його використання GitHub. URL: https://github.com/paralax/awesome-honeypots.

ОПТИМІЗАЦІЯ УПРАВЛІННЯ ПРОЄКТАМИ З КІБЕРБЕЗПЕКИ З ВИКОРИСТАННЯМ ГІБРИДНИХ МЕТОДОЛОГІЙ

Савченко А.В., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Ризики кібербезпеки стають дедалі більшими та складнішими, ніж будь-коли, а існуючі стратегії кібербезпеки часто просто недостатні в сучасних умовах обмежених ресурсів, в яких працює більшість компаній [1]. Насамперед, малі та середні підприємства, серед інших компаній, глибоко відчувають потребу в ефективній системі управління ризиками [2]. З одного боку, такі стандарти, як ISO 27001:2013, сприяють навчанню з питань безпеки та надають системі структурований контроль; з іншого боку, у багатьох випадках малі та середні підприємства потребують більшої обізнаності у подальших труднощах щодо впровадження системи. Цей виклик підкреслює важливість більш гнучкого підходу, що включає розвиток безпеки та оперативну гнучкість.

Метою доповіді є визначення можливості використанні підходу що полягає у поєднанні Agile з основними принципами DevSecOps для створення проактивних засобів виявлення і виправлення вразливостей, а не дій, що проводяться в останню хвилину.

Гібридна методологія, яку являє собою поєднання Agile та принципів DevSecOps забезпечує безпеку на ранніх стадіях, а також підвищує задоволеність клієнтів завдяки швидкій розробці та підлаштуванню до потреб у безпеці, які можуть швидко змінюватися [3].

В доповіді наводяться основні аспекти впровадження гібридної методології. В рамках впровадження цієї методології визначення вимог безпеки є фундаментальним аспектом кожного Agile-спринту. Як і функціональні вимоги, цілі безпеки інтегруються в цілі спринту, а конкретні заходи безпеки плануються на кожну ітерацію. Ця інтегрована модель безпеки гарантує, що в кожному циклі розробки одночасно враховуються і функціональні критерії, і критерії безпеки. Відомо, що забезпечення безпеки це безперервний процес. Дослідження демонструє, що в рамках ітеративної, гнучкої моделі компанії можуть ефективно управляти оновленнями, гнучко коригувати свої стратегії і одночасно будувати стійку систему безпеки.

Список літератури

1. Stadnyk M., Palamar A. (2022) Project management features in the cybersecurity area. Scientific Journal of TNTU (Tern.), vol 106, no 2, pp. 54–62. DOI: https://doi.org/10.33108/visnyk_tntu2022.02.054

2. Antunes M., Maximiano M., Gomes R. J., Pinto D. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal, Journal of cybersecurity and privacy. Vol. 1. 2021. P. 219–238. DOI: https://doi.org/10.3390/jcp1020012

3. Tisdale, Susan M. (2016). Architecting A Cybersecurity Management Framework. Issues in Information Systems Volume 17, Issue IV, pp. 227-236.DOI: https://doi.org/10.48009/4_iis_2016_227-236.

ПРОТОКОЛИ SIP У VOIP ТА ЇХ БЕЗПЕКА

Пашков С.С., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Інтернет мережі достатньо давно і активно використовуються для для передачі голосових даних. Однак зазвичай це програмні механізми, що у більшості працюють на верхніх, прикладних рівнях. Разом з тим, існують протоколи, які дозволяють передавати голосові дані через Інтернет замість традиційних телефонних ліній, наприклад VoIP (Voice over Internet Protocol) та SIP (Session Initiation Protocol). Разом вони утворюють механізм, який дозволяє здійснити обмін даними між пристроями для встановлення з'єднання та забезпечення зв'язку, в тому числі запуску та завершення сесії (SIP) та забезпечити безпосередню передачу даних VoIP-сесій. SIP підтримує також мультимедійні функції, такі як відеодзвінки та обмін повідомленнями, тоді як VoIP самостійно обмежується голосовими даними.

Метою доповіді є визначення можливостей ефективного використання VoIP та SIP та аналіз безпеки зазначених протоколів.

В доповіді наводяться основні переваги використання протоколів, серед них:

- інтеграція та масштабованість. SIP дозволяє VoIP-системам легко інтегруватися з іншими бізнес-додатками, такими як CRM-системи, що значно покращує можливості обробки викликів, зберігання записів та обміну даними. Крім того, SIP забезпечує високу масштабованість, дозволяючи легко додавати нових користувачів та розширювати інфраструктуру в залежності від зростаючих потреб організації.

- гнучкість і сумісність. SIP став найпопулярнішим протоколом для підтримки VoIP-зв'язку завдяки своїй гнучкості, здатності підтримувати кілька каналів комунікації (голос, відео, обмін повідомленнями) та інтеграції з різними системами і пристроями. SIP-обладнання можна використовувати в різних умовах, від бізнес-офісів до великих корпорацій, завдяки можливості працювати з різними провайдерами. При цьому SIP-протокол включає методи безпеки, такі як використання захищених з'єднань через TLS (Transport Layer Security) і захищені транспортні протоколи для медіаданих. Він також забезпечує механізми резервного копіювання та швидкого відновлення зв'язку під час мережевих збоїв або кібератак, що робить його надійним вибором для корпоративних середовищ.

Список літератури

1 Software Advice. URL: SIP Protocol: What It Is & How It Works in a VoIP Call.
2 GetVoIP. URL: What is a SIP Protocol and How Does it Work?.
3 Cisco Press. URL: Overview of SIP > VoIP Protocols: SIP and H.323.
4 TechRadar. URL: SIP vs VoIP: A Guide for Businesses.
5 Ringy. URL: SIP vs VOIP: Differences, Similarities, and More.

МЕТОДИ ЗАХИСТУ ВІД SQL АТАК

Горбачов А.Р., Балагура Д.С.,
Харківський національний університет радіоелектроніки, Харків, Україна
Семеренко Ю.О.
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна

SQL-ін'єкція є одним з найбільш розповсюджених методів кібератак на сайти та програми, що використовують бази даних. Її суть полягає у впровадженні стороннього SQL-коду в запити. SQL-ін'єкції належать до числа найстаріших і найбільш небезпечних атак для веб-додатків [1].

Метою доповіді є вивчити методи захисту від атаки SQL-ін'єкцій на веб-додатки, а також визначити найбільш ефективні способи запобігання несанкціонованому доступу до баз даних.

В доповіді наводяться результати аналізу щодо ефективності різних методів захисту від SQL атак Знизити ймовірність успішності такої атаки можна, якщо застосовувати перевірку даних у запитах за допомогою додаткових механізмів попередньої обробки запитів. Важливо відокремлювати дані від команд і запитів, що можна зробити кількома способами:

1. Використання безпечного API, який мінімізує ризик впливу інтерпретатора або забезпечує параметризований інтерфейс. Також можна застосовувати інструменти об'єктно-реляційного відображення (ORM) [1].
2. Реалізація білих списків на сервері для перевірки вхідних даних. Цей метод не гарантує повного захисту, адже багато додатків використовують спеціальні символи (у текстових полях або API для мобільних додатків).
3. Екранування спеціальних символів для динамічних запитів із використанням синтаксису, відповідного інтерпретатору. Зазначимо, що елементи SQL, такі як назви таблиць або стовпців, не підлягають екрануванню, тому дані, введені користувачами, можуть нести потенційну небезпеку — це поширена проблема платформ для створення звітів.
4. Застосування контролю SQL для запобігання витоку даних [2].

Абсолютно безпечних систем не існує, але можна знизити ризик зламу. Для запобігання ін'єкціям важливо ретельно перевіряти всі параметри, що надходять від користувачів. Окремим методом є тестування системи на хаотичні SQL-ін’єкції. Це також дозволяє виявити слабкі місця та вжити заходів захисту.

Список літератури

1. Halde J. Basics of SQL Injection Analysis, Detection and Prevention. – LAP LAMBERT Academic Publishing, 2014.
2. Д’якова Н.Є., Сєвєрінов О.В. Тестування вразливостей сучасних вебресурсів, НТУ «ХПІ»,. – 2022.
3. Justin C. SQL Injection Attacks and Defense. – Syngress Date, 2009.

АНАЛІЗ ТА МЕХАНІЗМИ УДОСКОНАЛЕННЯ ЗАХИЩЕНОСТІ ОБЛІКОВИХ ЗАПИСІВ БЛОКЧЕЙН

Муравйов В.О., Балагура Д.С., Власов А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Забезпечення захищеності облікових записів у блокчейн-системах, які оперують значними фінансовими активами або мають важливу роль у виконанні смарт-контрактів, є одним з ключових викликів для сучасної криптографії. Використання приватних і публічних ключів забезпечує базовий рівень безпеки, проте цього недостатньо для комплексного захисту облікових записів користувачів від атак або втрати ключів.

Метою доповіді є розкриття методу Абстракції Акаунту, як такого, що дозволяє ідентифікувати та визначати обліковий запис не тільки як пару ключів, але і як окремий смарт-контракт [1], який може виконувати додаткові умови, серед яких можуть бути впроваджені різні варіанти додаткових механізмів захисту, такі як сесійні ключі або додаткові перевірки аутентифікації.

У цій роботі проведено аналіз поточного стану захищеності облікових записів у блокчейн-мережах, а також розглянуто основні загрози та вразливості, пов'язані з ними. Показано, що застосування Абстракції Акаунту дозволяє зменшити ці ризики шляхом впровадження додаткових рівнів перевірки та контролю. Проведено порівняння існуючих рішень на основі стандартної моделі облікових записів з тими, що реалізовані з використанням методу Абстракції Акаунту.

Основними перевагами використання методу Абстракції Акаунту є підвищена безпека [2], наприклад, інтеграція багатофакторної аутентифікації, або звичайного OAuth дозволяє проводити ідентифікацію користувача за декількома параметрами та каналами одночасно, використання сеансових ключів суттєво збільшує рівень безпеки з точки зори криптографічного захисту [3].

Крім того, метод Абстракції Акаунту відкриває нові можливості для створення більш гнучких бізнес-логік безпосередньо на рівні користувацьких облікових записів.

Список літератури

1. ERC 4337: account abstraction without Ethereum protocol changes. Vitalik Buterin. *www.medium.com*. URL: https://medium.com/infinitism/erc-4337-account-abstraction-without-ethereum-protocol-changes-d75c9d94dc4a.

2. Qin Wang, Shiping Chen. Account Abstraction, Analysed. *arXiv*. 2023. 2309.00448.

3. Sievierinov O., Kholosha O. Securing Bearer token in OAuth2.0 // COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES, 2021.

ОГЛЯД КРИПТОПРИМІТИВІВ, ОПТИМІЗОВАНИХ ДЛЯ ЗАСТОСУВАННЯ З ДОКАЗАМИ ІЗ НУЛЬОВИМ РОЗГОЛОШЕННЯМ

Гаража Р.Ю., Мельникова О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Докази із нульовим розголошенням здатні забезпечити високий ступінь конфіденційності даних користувача. Однак, особливості реалізації традиційних криптографічних примітивів та заснованих на них протоколів ускладнюють застосування їх варіантів із нульовим розголошенням.

Метою доповіді є визначення примітивів та протоколів, що оптимізують створення доказу із нульовим розголошенням. **В доповіді** наводиться перелік таких засобів та пропозиції щодо їх застосування.

Докази із нульовим розголошенням реалізовані на базі кінцевих полів. Це обумовлює непридатність перевірених часом примітивів: вони вимагають високих витрат на доведення факту виконання великої кількості побітових операцій, а також застосовують ненативні для алгоритмів доказів поля для операцій над еліптичними кривими [1, 2].

На сьогоднішній день існують оптимізовані ґеш-функції Poseidon та MiMC. Вони застосовуються для оптимізації побудови контуру (англ. circuit) доказу [3] та зменшення кількості обмежень (англ. constraints), що на нього накладаються, і на відповідність яким треба перевіряти виконання алгоритму. Оптимізація досягається за рахунок застосування функції губки [1].

До оптимізованих алгоритмів електронного цифрового підпису відноситься EdDSA на базі еліптичної кривої під назвою Baby-Jubjub із застосуванням функції ґешування MiMC-7 [2]. Ця комбінація дозволяє скоротити кількість обмежень, необхідних для доведення перевірки підпису, з приблизно 1,5 мільйонів до приблизно 7,5 тисяч.

Застосування зазначених криптопримітивів дозволяє реалізувати приватні децентралізовані облікові системи для фінансових організацій, у яких існують високі вимоги щодо конфіденційності даних [3].

Список літератури

1. Karthik Inbasekar. SoK: Hash functions in Zero Knowledge Proofs. URL: https://github.com/ingonyama-zk/papers/blob/main/sok_zk_friendly_hashes.pdf (дата звернення: 31.10.2024)

2. Iden3 Documentation Site. ED-DSA. URL: https://iden3-docs.readthedocs.io/en/latest/iden3_repos/research/publications/zkproof-standards-workshop-2/ed-dsa/ed-dsa.html (дата звернення: 31.10.2024)

3. Мельникова О. А., Гаража Р. Ю. Засоби втілення приватних блокчейн-ролапів для фінансових організацій [Текст] // Чотирнадцята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління»: Зб. матеріалів конференції. Т.2: секції 3, 4, 5, 6. — Харків: НУО АР, НТУ "ХПІ", ХНУРЕ, НАУ «ХАІ», УмЖ, 2024. — С. 49.

ЗАХИСТ МІКРОСЕРВІСІВ НА SPRING CLOUD ВІД АТАК ТИПУ DISTRIBUTED DENIAL OF SERVICE (DDOS)

Ляшко М.С., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

З появою та активним розвитком мікросервісної архітектури збільшилася кількість можливих атак на системи, що використовують ці підходи. Однією з найбільш небезпечних загроз для таких систем є атаки типу DDoS. У середовищі Java Spring існує потужний інструмент - Spring Cloud, який призначений для спрощення розробки мікросервісних архітектур. Spring Cloud надає набір інструментів для керування конфігурацією, сервісним відкриттям, балансуванням навантаження та обробкою відмов. Це дозволяє розробникам легко інтегрувати різні сервіси та забезпечувати їх надійну роботу, що особливо важливо у контексті захисту від DDoS-атак [1].

Метою доповіді є аналіз можливостей Spring Cloud при захисті від DDoS атак. Стратегії захисту від DDoS у Spring Cloud:

1. Rate Limiting (Обмеження частоти запитів). Одним з найбільш ефективних підходів для захисту від DDoS є обмеження кількості запитів до сервісу за певний час.

2. Load Balancing (Балансування навантаження). Балансування навантаження є критичним елементом для забезпечення стійкості системи до DDoS-атак. Це допомагає уникнути перевантаження одного інстансу, дозволяючи системі краще розподіляти ресурси,а витримувати високі навантаження.

3. Circuit Breaker (Переривник ланцюга). Переривник ланцюга (Circuit Breaker) – це патерн, що дозволяє запобігти подальшому навантаженню на систему, якщо сервіс перевантажений або не відповідає. Цей підхід дозволяє автоматично відключати запити до мікросервісів, які не можуть обробляти навантаження, щоб уникнути повного колапсу системи.

4. Кешування та відкладене виконання. Кешування може значно знизити навантаження на систему під час DDoS-атак. Замість того, щоб обробляти кожен запит у режимі реального часу, можна відповідати кешованими результатами для повторюваних запитів.

5. Автоматичне масштабування мікросервісів. Один із найефективніших способів боротьби з DDoS-атаками полягає в автоматичному масштабуванні інстансів мікросервісів у хмарному середовищі. Це дозволяє системі динамічно адаптуватися до змін у трафіку та зменшити ризик відмови через перевантаження.

Важливо враховувати, що автоматичне масштабування має бути поєднане з іншими стратегіями, такими як обмеження частоти запитів та кешування, щоб уникнути зайвого споживання ресурсів.

Список літератури

1. Spring Cloud. Spring.io. URL: https://spring.io/projects/spring-cloud..

ФІШИНГОВА АТАКА ТИПУ «ЗЛИЙ БЛИЗНЮК» (EVIL TWIN PHISHING)

Іващенко І.В., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Фішинг — це кібератака, що використовує шахрайські повідомлення або сайти для отримання конфіденційних даних чи поширення шкідливого ПЗ [1].

Evil Twin Phishing — це фальшива точка доступу Wi-Fi, що імітує законну, аби зловмисник міг перехоплювати інтернет-з'єднання користувачів [2]. Цей кіберміраж можна використовувати в етичних і неетичних цілях. Неетичні хакери використовують Evil Twins для перехоплення конфіденційних даних у користувачів, зокрема логінів та даних карток. Натомість етичні хакери застосовують цей метод для тестування мережевої безпеки, щоб виявляти та усувати вразливості до реальних атак [3].

Evil twin Wi-Fi з'єднання важко розпізнати без спеціальних інструментів. **Метою доповіді** є аналіз методів захисту від атак Evil Twin Phishing. Проведений аналіз дозволив визначити основні методи захисту від даних атак.

1. Використання VPN. Це захистить дані, навіть якщо користувач випадково підключиться до фальшивої мережі.

2. Відвідування лише HTTPS-сайтів. Це забезпечує шифрування з'єднання. Також можна встановити розширення HTTPS Everywhere.

3. Вимкнення автоматичного підключення, так пристрій не під'єднається до підроблених мереж.

4. Уникнення загальнодоступного Wi-Fi.

5. Обмеження онлайн-діяльності, потрібно не входити в облікові записи та не відкривати конфіденційні сайти через сумнівні з'єднання.

Атаки "злий близнюк" становлять значну кіберзагрозу. Щоб захиститися від них, важливо обережно користуватися бездротовими мережами та дотримуватися основних правил кібергігієни [4].

Список літератури

1. Matthew Kosinski. What is phishing? Видавець: IBM. URL: https://www.ibm.com/topics/phishing#:~:text=Contributor%3A%20Matthew%20Kosinski-,What%20is%20phishing%3F,a%20form%20of%20social%20engineering.

2. Yimin Song; Chao Yang; Guofei Gu. Who is peeping at your passwords at Starbucks? — To catch an evil twin access point. IEEE Xplore. URL: https://ieeexplore.ieee.org/document/5544302.

3. Andrew De Vito. Evil Twin WiFi Attack: A Step-By-Step Guide. StationX. URL: https://www.stationx.net/evil-twin-wifi-attack/.

4. Josue Ledesma. Evil Twin Attack: What it is, How to Detect & Prevent it. Varonis. URL: https://www.varonis.com/blog/evil-twin-attack

ЗАСТОСУВАННЯ ТРАНСФОРМЕРІВ ДЛЯ ВИЯВЛЕННЯ СКЛАДНИХ ВЕБ-АТАК У РЕАЛЬНОМУ ЧАСІ

Кавецький М.С., Руженцев В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Застосування трансформерів для виявлення складних веб-атак у реальному часі є новітнім підходом у сфері кібербезпеки. Трансформери, як-от модель BERT, здатні швидко аналізувати великі обсяги веб-трафіку, виявляючи аномальні шаблони та поведінку, які можуть свідчити про атаку. Їх висока чутливість до контексту та здатність навчатися на складних даних дозволяють досягти точності, недоступної традиційним методам. У поєднанні з потужністю обробки в реальному часі, трансформери відкривають нові можливості для захисту веб-додатків і мереж. Це робить їх перспективним інструментом для боротьби з еволюційними загрозами в кіберпросторі.

Об'єктом дослідження є процеси та методи виявлення веб-атак у реальному часі з використанням сучасних технологій штучного інтелекту, зокрема трансформерів. **Предметом дослідження** є особливості застосування трансформерних моделей для аналізу веб-трафіку, їх ефективність у виявленні складних та еволюційних загроз, а також адаптація цих моделей для швидкої обробки даних в умовах реального часу.

Переваги трансформерів у контексті виявлення веб-атак полягають у їхній здатності обробляти великі обсяги текстових даних та виявляти складні, контекстуальні залежності між елементами трафіку [1]. Завдяки цій здатності трансформери можуть розпізнавати приховані шаблони та аномалії, характерні для різних типів атак, таких як фішинг, SQL-ін'єкції або XSS, які можуть бути непомітні для традиційних алгоритмів. До того ж, вони можуть працювати в реальному часі та легко масштабуються, що дозволяє оперативно реагувати на загрози навіть у високонавантажених веб-системах.

Результати дослідження показали, що застосування трансформерів для виявлення веб-атак значно підвищує ефективність і швидкість реагування на загрози. Моделі продемонстрували точність до 99% у розпізнаванні аномалій та складних шаблонів атак, що особливо важливо для захисту в реальному часі [2]. Це робить трансформери ефективним інструментом для підсилення кібербезпеки, особливо в умовах постійно зростаючої складності веб-атак.

Список літератури

1. Y. E. Seyyar, A. G. Yavuz and H. M. Ünver, "Detection of Web Attacks Using the BERT Model," *2022 30th Signal Processing and Communications Applications Conference (SIU)*, Safranbolu, Turkey, 2022, pp. 1-4, doi: 10.1109/SIU55565.2022.9864721.

2. Кавецький М.С. Виявлення веб-атак по HTTP запитам з використанням технік NLP, Харків, ХНУРЕ, 2024

КВАНТОВО-СТІЙКИЙ ЦИФРОВИЙ ПІДПИС ДЛЯ ЗАХИСТУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА ОСНОВІ БАГАТОПАРАМЕТРИЧНИХ ГРУП

Хівренко Г.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний розвиток квантових обчислень створює нові ризики для безпеки традиційних криптографічних систем, що використовуються у захисті телекомунікаційних мереж. Квантові комп'ютери можуть ефективно розв'язувати задачі, які є основою класичних алгоритмів шифрування, ставлячи під загрозу цілісність і конфіденційність даних у таких мережах. Основною небезпекою є здатність квантових комп'ютерів до ефективного розв'язання математичних задач, які лежать в основі сучасних криптографічних алгоритмів, таких як RSA чи ECC. З огляду на це, дослідження у сфері постквантової криптографії стають дедалі актуальнішими, що вимагає розробки нових моделей, стійких до квантового криптоаналізу.

Метою доповіді є представлення архітектури цифрового підпису, яка базується на некомутативних багатопараметричних групах, для забезпечення стійкості до атак з боку квантових обчислювальних систем. У даній роботі описуються математичні структури та алгоритми, що дозволяють досягти високого рівня захисту шляхом використання складних обчислень у некомутативних просторах Така структура дозволяє досягнути криптографічної стійкості завдяки складності обчислення групових операцій у некомутативному середовищі, що на сьогодні залишається поза можливостями квантових алгоритмів, таких як алгоритм Шора.

Актуальним є застосування квантово-стійких підписів у телекомунікаційних мережах, оскільки зростання потужності квантових комп'ютерів створює ризики для безпеки даних, які передаються та обробляються у цих мережах. Особливу значущість такі підписи мають для критично важливих інфраструктур, де порушення захисту може призвести до серйозних наслідків.

Проведено аналіз існуючих моделей цифрових підписів та їх можливостей до опору квантовому криптоаналізу. Проведено моделювання обчислювальних процесів із застосуванням багатопараметричних груп та оцінено їхню ефективність у контексті телекомунікаційних систем.

Список літератури

1. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*.

2. Svaba, Pavol. (2011). Covers and Logarithmic Signatures of Finite Groups in Cryptography.

3. Wang, Y., Liu, X., & Lee, B. (2021). Quantum-resistant digital signature schemes based on non-commutative algebra. *Advances in Post-Quantum Cryptography*.

ЗАСТОСУВАННЯ ГОМОМОРФНОГО ШИФРУВАННЯ ДЛЯ ЗАХИСТУ ХМАРНИХ ОБЧИСЛЕНЬ

Гущин Б.-Д.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Одним із основних сучасних застосувань гомоморфного шифрування є безпечні хмарні обчислення. На даний час організації все частіше переміщують свої дані та обчислення в хмару, забезпечення конфіденційності даних стає критичною проблемою. Гомоморфне шифрування дозволяє користувачам зберігати й обробляти свої дані на хмарних серверах, не розкриваючи фактичні дані постачальнику послуг. Гомоморфне шифрування - це форма шифрування, що дозволяє здійснювати певні типи обчислень на зашифрованому тексті та отримувати зашифровані результати обчислень, які при розшифруванні відповідають результатам операцій, що виконуються на відкритому тексті [1-3].

Метою доповіді є аналіз застосування гомоморфного шифрування для захисту хмарних обчислень.

Користувач, який розміщує у сховищі свої конфіденційні дані та не довіряє хмарі, має вживати відповідних заходів та пред'являти вимоги щодо забезпечення їх безпеки. Тому дані необхідно шифрувати користувачем, щоб вони надходили на сервер у шифрованому вигляді. Також необхідно опрацьовувати ці дані без розшифрування. У зв'язку з цим гомоморфне шифрування відкриває нові можливості збереження цілісності, доступності та конфіденційності даних при їх обробці в хмарних системах [1-3].

У хмарних обчисленнях, де продуктивність є головним пріоритетом, для практичного застосування повністю гомоморфної системи шифрування слід обмежувати кількість операцій, які можна здійснювати над даними.

Проведений аналіз показав, що найближчим часом методи гомоморфного шифрування істотно впливатимуть на ринок хмарних послуг. Однак поки що не створено ефективних алгоритмів повністю гомоморфного шифрування, що забезпечують рівень продуктивності, придатний для практичного застосування у хмарних сховищах [1-3]. Усі пропоновані схеми не реалізовані практично, оскільки призводять до накопичення помилок і швидкого збільшення шифрованих текстів. При цьому частково гомоморфні системи успішно застосовуються у хмарних обчисленнях, електронному голосуванні, захищеному пошуку інформації, системах із зворотним зв'язком тощо.

Список літератури

1. Halevi, S., & Shoup, V. (A Full Introduction to Homomorphic Encryption). 2013. IBM Research. 92 pages.
2. Yi, X., Paulet, R., Bertino, E., Yi, X., Paulet, R., & Bertino, E. (2014). Homomorphic encryption (pp. 27-46). Springer International Publishing
3. Coron, J.-S., Naccache, D., & Tibouchi, M. (Homomorphic Encryption). 2011. Springer. 142 pages.

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ВІРТУАЛІЗАЦІЇ INTEL ДЛЯ СТВОРЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ OPEN PORTABLE TRUSTED EXECUTION ENVIRONMENT (OP-TEE)

Шулік П.В.
Харківський національний університет радіоелектроніки, Харків, Україна

OP-TEE фреймворк являється поширеним в системах захисту інформації на базі ARM SoC та використовується в сучасних смартфонах, системах інтернету речей та інших хмарних системах [1]. OP-TEE базується на технології захисту інформації ARM TrustZone. Суть даної технології складається в тому, що вводиться додатковий режим роботи ARM ядра – захищений режим у якому виконується робота з секретною інформацією, яка не повинна бути доступною для основної операційної системи та її додатків. Таким чином система поділяється на два світа: звичайний (non secure world) – де працює звичайне програмне забезпечення та захищений світ (secure world), в якому ведеться робота з секретною інформацією.

Метою даного дослідження є розгляд одного із підходів інтеграції OP-TEE фреймворка с Intel-X86 платформами, які не підтримують технологію ARM Trust Zone. **Предметом дослідження** є програмні засоби інтеграції OP-TEE фреймворка с Intel-X86.

Суть інтеграції OP-TEE складається в заміщенні технології TrustZone віртуальними технологіями процесорів Intel-x86 VT-d/VT-x, де апаратні ресурси розподіляються між віртуальними операційними системами, і забезпечують ізоляцію ресурсів та інформації між операційними системами. У якості орбітра, який керує переключенням роботи процесора та доступу до ресурсів може виступати гіпервайзор першого типу. У якості такого гіпервайзора в запропонованому рішенні виступає гіпервайзор компанії Intel Kernel Guard Technology (iKGT). Основний підхід закладений в iKGT називається Intel Supervisor Mode Execution Prevention (SMEP) - запобігання виконання коду в режимі супервізора. Технологія полягає в запобіганні виконання коду, розташованого на сторінці користувача (тобто звичайний світ, який не повинен мати доступу до захищеної інформації), при поточному рівні привілеїв рівному 0 (рівень доступу до захищеної інформації).

Таким чином, практично технологія Intel SMEP виконує дуже схожу функціональність з ARM TrustZone може використовуватися сумісно з OP-TEE фрейворком.

Список літератури

1. Arshad Nehal, Priyanka Ahlawat Securing IoT applications with OP-TEE from hardware level OS: 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA) 10.1109/ICECA.2019.8822040

ВАЖЛИВІСТЬ МАГНІТНОЇ СКЛАДОВОЇ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ЗАСОБІВ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ ДЛЯ КОНТРОЛЮ НОРМ ЗАХИЩЕННОСТІ В ТЗІ

Гапіченко А.М., Заболотний В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Майже всі сфери людської діяльності на сьогоднішній день не функціонують без використання інформаційних технологій. Розповсюдженість персональних комп'ютерів та інших засобів обробки, зчитування, а також озвучування даних впливає на збільшення кількості інформації, що циркулює з використанням електронних компонентів навколо яких завжди присутні поля випромінювання. Оскільки ці випромінювання небажані та носять паразитний характер, їх називають побічними електромагнітними випромінюваннями (ПЕМВ) [1]. Саме тому даний технічний канал витоку інформації (ТКВІ) потребує детального аналізу.

Метою доповіді є дослідження впливу магнітної складової ПЕМВ при створенні комплексів технічного захисту інформації. В доповіді наводяться результати експериментальних розрахунків магнітної складової для типового діапазону небезпечних для розвідки відстаней.

Згідно з [2] електромагнітне поле — особливий вид матерії, яку визначають векторними величинами, що характеризують змінні у часі електричне та магнітне поля, і є носієм інформації, магнітне поле — це один з двох складників ЕМП, обумовлений рухомими електричними зарядами (електричним струмом) та змінним електричним полем.

Для оцінки магнітної складової в ході експериментів використовується друге рівняння Максвела, яке описано в [3].

В ході виконання роботи отримано результати, необхідні для подальших досліджень можливостей ТКВІ ПЕМВ відеотракту засобів обчислювальної техніки.

Список літератури

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. / С.О. Іванченко, О.В. Гавриленко , О.А. Липський, А.С. Шевцов – Київ : НТУУ «КПІ», 2016. – 101 с.

2. Технічна електродинаміка та поширення радіохвиль: навч. посіб. для студентів напряму підготовки 6.050903 «Телекомунікації» / В. В. Пілінський. –К.: Національний технічний університет України «КПІ», 2014. – 336 с.

3. Заболотний, В. І. Дослідження зміни форми сигналу у каналі побічних електромагнітних випромінювань монітору / В. І. Заболотний, Є. В. Герасименко, В. І. Перепадя // Радіотехніка: Всеукр. межвід. наук.-техн. зб. – Харків, 2014. – Вип. 176. – С. 116– 121.

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ПОХИБКИ ЛОКАЛІЗАЦІЇ РАДІОАКУСТИЧНИХ ЗАКЛАДНИХ ПРИСТРОЇВ

Школьник В.А., Олейніков А.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Радіовиявлювачі - це технічні засоби виявлення, ідентифікації та локалізації джерел електромагнітного випромінювання в галузі технічного захисту інформації.[1] Цей термін визначений у нормативному документі НД ТЗІ 1.5-001-2000.

Метою доповіді є дослідження похибок локалізації радіоакустичних закладних пристроїв, що виникають при використанні акустичного далекоміра (АД) апаратно-програмного комплексу (АПК) «VOSTOK» [2-5].

У рамках дослідження, було проведено комп'ютерне моделювання двох методів для фіксації положення імпульсу: порогового та кореляційного. У першому випадку було змішано нормальний шум з сигналом, в той час як для другого - використали два імпульси від радіоакустичного закладного пристрою і еталона.

В доповіді наведені результати проведеного дослідження, зокрема те, що кореляційний метод має меншу похибку у діапазоні співвідношення сигнал/шум від 2 до ~20, оскільки він аналізує енергію всього сигналу, тоді як пороговий метод покладається на передній фронт імпульсу. З підвищенням співвідношення с/ш кожен з методів демонструє схожі результати.

Також, отримані дані вказують, на те, що кореляційний метод ефективніший при локалізації закладних пристроїв з амплітудною або частотною модуляцією. Він не лише, знижує похибку локалізації на 15% порівняно з пороговим методом, а й забезпечує високу стабільність результатів і має низьку чутливість до змін амплітуди сигналу.

Список літератури

1. НД ТЗІ 1.5-001-2000. Радіовиявлювачі. Класифікація. Загальні технічні вимоги.[Чинний від 2000-06-13]. Вид. офіц. Київ, 2000.

2. Олейніков А.М., Коваль В.П. Особливості застосування апаратно-програмних комплексів для виявлення та локалізації закладних пристроїв//Захист інформації.- Київ: 2002- N 3. С.28-36.

3. Пошук та локалізація радіозакладних пристроїв/ В.О.Хорошко, О.Д.Азаров, Г.О.Максименко, Ю.Є.Яремчук - Вінниця: ВНТУ, 2007. - 333 с

4. Засоби та системи технічного захисту інформації./І.Є. Антіпов, А.М. Олейніков, Ю.В. Ликов, В.Д. Кукуш, І.О. Милютченко. Харків: ХНУРЕ, 2019. 216 с.

5. D. Sathyamoorthy , M. Jalis, Md Jelas, Shalini Shafii /Wireless spy devices: A review of technologies and detection methods/November Defence S and T Technical Bulletin 7(2), 2014,:130-139 p.

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД КОМПЛЕКСІВ РАДІОРОЗВІДКИ

Голобородько Ю.М., Наконечний М.В.
Харківський національний університет радіоелектроніки, Харків, Україна

При побудові систем захисту інформації одним з елементів є забезпечення захисту об'єктів від систем радіорозвідки. Методи захисту від радіорозвідки спрямовані на виключення чи утруднення виявлення випромінювання радіоелектронних засобів об'єкту захисту, а також утруднення вимірювання параметрів їх сигналів та координат. Комплекси радіорозвідки використовується для виявлення, розпізнавання об'єктів (визначення класу, типу, держналежності), визначення їх місця розташування, характеру діяльності та інше щодо випромінювання їх засобів зв'язку.

Метою доповіді є аналіз завдань систем захисту інформації для протидії системам радіорозвідки.

Радіорозвідка передбачає послідовне виконання трьох основних задач:

– виявлення факту роботи системи (засобу) радіозв'язку (виявлення сигналу);

– визначення структури виявленого сигналу і його основних параметрів;

– розкриття інформації, яка міститься в сигналі.

Сучасні засоби радіорозвідки передбачають залучення штучного інтелекту з можливістю самонавчання. Вважається, що так можна забезпечити швидкий та ефективний аналіз великих масивів інформації, що надходять, з одночасним відпрацюванням можливих сценаріїв реагування. Також передбачається, що штучний інтелект дозволить краще виявляти важливі дані, що містяться у перехоплених сигналах, проводити відповідний аналіз і дистрибуцію результатів. Для захисту від сучасних систем радіорозвідки необхідно застосування комплексу організаційних та технічних заходів. Для захисту застосовуються всі спільні організаційні заходи, що включають територіальні, просторові, енергетичні та тимчасові обмеження на випромінювання у вільний простір, здійснення радіообміну за раціональними маршрутами з низькою розвідувальною доступністю.

Список літератури

1. Вавpічен О., Городиський Р., Площик А. Методи захисту інформації в сучасних засобах радіозв'язку. *Наука і техніка сьогодні*, 2023, №13 (27).
2. Opirskyy I., Bybyk R. Дослідження сучасних методів РЕБ та методів і засобів її протидії. *Ukrainian Scientific Journal of Information Security*, 2023, №*29*(2), С. 88-97.
3. Яковлев М., Волобуєв А., Прібилєв Ю. Математичне моделювання процесів функціонування автоматизованих систем військового радіозв'язку в умовах їх захисту від радіорозвідки. *Збірник наукових праць Національної академії Національної гвардії України*, 2024. №1(43), С. 130-144.

УЧАСНИКИ КОНФЕРЕНЦІЇ (секції 1, 2, 3)

ОРГАНІЗАЦІЇ, ЯКІ ПРИЙНЯЛИ УЧАСТЬ У КОНФЕРЕНЦІЇ

Азербайджанська національна авіаційна академія, Баку, Азербайджан
Азербайджанський державний аграрний університет; Гянджа, Азербайджан
Азербайджанський державний педагогічний університет, Баку, Азербайджан
Азербайджанський державний університет нафти та промисловості, Баку, Азербайджан
Азербайджанський економічний університет UNEC, Баку, Азербайджан
Азербайджанський технічний університет, Баку, Азербайджан
Азербайджанський технологічний університет, Баку, Азербайджан
Азербайджанський університет будівництва та архітектури, Баку, Азербайджан
Бакинський державний університет, Баку, Азербайджан
Бакинський інженерний університет, Баку, Азербайджан
Бакинський слов'янський університет, Баку, Азербайджан
Військовий науково-дослідний інститут, Баку, Азербайджан
Військовий інститут імені Гейдара Алієва, Баку, Азербайджан
Військовий інститут зв'язку та інформаційних технологій імені Героїв Крут Київ, Україна
Головне управління ДСНС України в Полтавській області, Полтава, Україна
Головне управління ДСНС України в Херсонській області, Херсон, Україна
Гуманітарна міжнародна організація The Halo Trust, Київ, Україна
Державна служба спеціального зв'язку та захисту інформації України, Київ, Україна
Державний біотехнологічний університет, Харків, Україна
Інститут військового управління Національного університету оборони, Баку, Азербайджан
Інститут освіти Азербайджанської Республіки, Баку, Азербайджан
Інститут радіаційних проблем, Баку, Азербайджан
Інститут систем управління Азербайджанської Національної академії наук, Баку, Азербайджан
Національна авіаційна академія, Баку, Азербайджан
Національна академія Національної гвардії України, Харків, Україна
Національне аерокосмічне агентство, Баку, Азербайджан
Національний авіаційний університет, Київ, Україна
Національний аерокосмічний університет імені М. Є. Жуковського "Харківський авіаційний інститут", Харків, Україна
Національний технічний університет "Харківський політехнічний інститут", Харків, Україна
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна
Національний університет оборони Азербайджанської республіки, Баку, Азербайджан
Національний університет "Одеська політехніка", Одеса, Україна
Національний університет цивільного захисту України, Харків, Україна
Придніпровська державна академія будівництва та архітектури, Дніпро, Україна
Республіканський центр сейсморозвідки, Баку, Азербайджан
Сумгаїтський державний університет, Сумгаїт, Азербайджан
Університет технології і гуманітарних наук, Бельсько-Бяла, Польща
Харківський національний університет внутрішніх справ, Харків, Україна
Харківський національний економічний університет ім. Саймона Кузнеця, Харків, Україна
Харківський національний університет імені В.Н. Каразіна, Харків, Україна
Харківський національний університет міського господарства імені О.М. Бекетова, Харків, Україна
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна
Харківський національний університет радіоелектроніки, Харків, Україна
Харківський радіотехнічний фаховий коледж, Харків, Україна

ЗМІСТ

НАУКОВЕ ВИДАННЯ

ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ

Тези доповідей
одинадцятої міжнародної науково-технічної конференції
(21 – 22 листопада 2024 року)
Том 1: секції 1, 2, 3

Відповідальна за випуск *Н. Г. Кучук*
Технічний редактор *І. А. Лєбедева*
Коректор *В. В. Богомаз*
Комп'ютерне складання та верстання *Н. Г. Кучук, І. Ю. Петровська*

Адреса оргкомітету: вул. Кирпичова, 2, Харків, 61002, Україна
НТУ «ХПІ», Вечірній корпус, кімната 314
тел. +38 (057) 707 61 65

Підписано до друку 14.11.2024 Формат 60 × 84/16
Ум.-вид. арк. 9,5. Тираж 100 пр. Зам. 1114-24/1

Віддруковано з готових оригінал-макетів у цифровій друкарні Impress
61002, м. Харків, вул. Пушкінська, 56, тел. **+ 38 (057) 714-52-11**
e-mail: **irina@impress.biz.ua**