MINISTRY OF EDUCATION
AND SCIENCE OF UKRAINE

NATIONAL AVIATION
UNIVERSITY

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ
УНІВЕРСИТЕТ

Abstracts of XXIII International conference of higher education students and young scientists

Тези доповідей XXIII Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених

POLIT.
CYBER SECURITY
AND SOFTWARE ENGINEERING

ПОЛІТ.
КІБЕРБЕЗПЕКА
ТА ПРОГРАМНА ІНЖЕНЕРІЯ

Faculty of cyber security
and software engineering

Факультет кібербезпеки
та програмної інженерії

Kyiv 2023

Київ 2023

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY
FACULTY OF CYBER SECURITY AND SOFTWARE ENGINEERING

Abstracts of
XXIII International
conference of higher education students
and young scientists

POLIT.
CHALLENGES OF SCIENCE TODAY

CYBER SECURITY AND SOFTWARE ENGINEERING

Kyiv 2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ

Тези доповідей
XXIII Міжнародної
науково-практичної конференції здобувачів
вищої освіти і молодих учених

ПОЛІТ.
СУЧАСНІ ПРОБЛЕМИ НАУКИ

КІБЕРБЕЗПЕКА ТА ПРОГРАМНА ІНЖЕНЕРІЯ

Київ 2023

УДК 321:341:339.9

POLIT. CHALLENGES OF SCIENCE TODAY. INTERNATIONAL RELATIONS: Abstracts of XXIII International conference of higher education students and young scientists, Kyiv, 2023, National Aviation University / Editorial board Lutskyi M. [and others]. – K.: NAU, 2023. – 93 p.

The materials of the scientific-practical conference contain a summary of the reports of research works of higher education seekers and young scientists in the field of «CYBER SECURITY AND SOFTWARE ENGINEERING».

Recommended for printing by academic council of the Faculty of cyber security and software engineering (Minutes No 4 from 25 May 2023)

УДК 004.056.5:004.738.5(043.2)
ПОЛІТ. СУЧАСНІ ПРОБЛЕМИ НАУКИ. КІБЕРБЕЗПЕКА ТА ПРОГРАМНА ІНЖЕНЕРІЯ: Тези доповідей XXIII Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених, Київ, 2023, Національний авіаційний університет / Редакційна колегія М.Луцький [та ін.]. – К.: НАУ, 2023. – 93 с.

Матеріали науково-практичної конференції містять узагальнення доповідей науково-дослідних робіт здобувачів вищої освіти та молодих учених у галузі «КІБЕРБЕЗПЕКА ТА ПРОГРАМНА ІНЖЕНЕРІЯ».

Рекомендовано до друку Вченою радою факультету кібербезпеки та програмної інженерії (Протокол № 4 від 25 травня 2023 р.)

CONTENT / ЗМІСТ

UDC 004.056.005

SYSTEM INCIDENT MANAGEMENT USING CLOUD TECHNOLOGIES

Igor Ivanchenko, Iryna Lozova, Yevhenii Pedchenko, Mari Petrovska

National aviation university, Kyiv

Supervisor – Yevheniia Ivanchenko, Candidate of Science (Engineering), professor

Keywords: information system, incident, event processing, event management, automation

Introduction

Information systems of most companies in Ukraine and beyond operate in an environment that requires fast and comprehensive information processing with the detection of information security incidents in this data stream. By the beginning of 2020, more than 90% of companies organized the work of their own employees directly using office space and a managed information space, which allowed them to collect events from information systems in a single place and detect information security incidents in this data stream, and respond to them almost instantly.

Materials and methods

At the beginning of 2020, when most companies in the world started working remotely, there was a problem with monitoring actions and tracking events that occurred on user workstations, which necessitated changing the current operating infrastructure with the transfer of critical systems to the company's territory, which has the risk of exploiting vulnerabilities and gaining illegitimate access to the company's critical business processes [1].

The main goal of this research is to develop a system that will allow companies in Ukraine and all over the world to provide visibility into events on remote workstations and servers, regardless of their geolocation.

Novelty is the system’s improvement for collecting and management incidents through the use of cloud providers (Amazon, Google, Microsoft), which will allow the processing of cyber incidents using cloud computing without the need to allocate physical and human resources in companies. In the proposed deployment option, companies do not need to allocate hardware and virtual computing resources (processor cores, RAM, hard disk memory, additional network channels) on their own infrastructure and monitoring these systems are kept up-to-date.

Operation’s principle of the developed system is illustrated schematically in Fig. 1, which is a high-level design for solving the above task of management events and incidents in the information systems of companies from anywhere in the world:

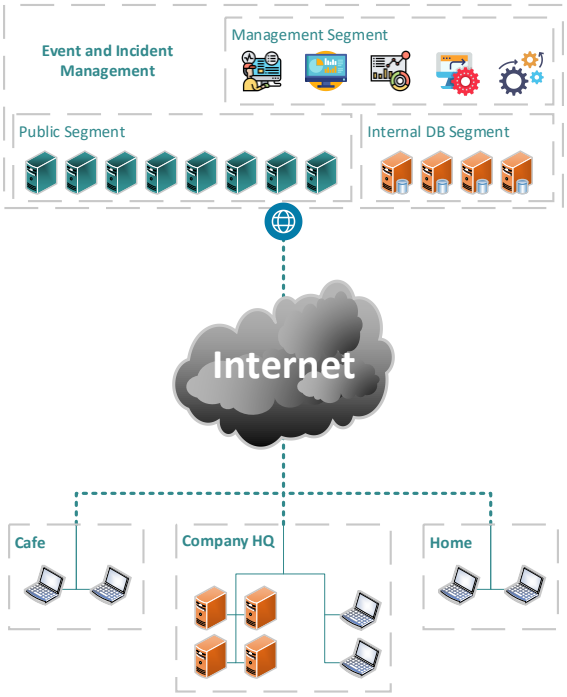

Figure 1. High-level system design of the proposed solution for management events of companies' information systems and detecting information security incidents

Result

This scheme is a system consisting of the proposed cloud-based solution and the company's headquarters and employees who perform their job responsibilities from home and cafes. The Event and Incident Management solution consists of three segments: 1) Public Segment - this infrastructure component is required to receive events from information systems and workstations of the customer's company employees. 2) Internal DB Segment - this component is necessary for storing received events from the customer's company, where a separate disk space is allocated for each company. 3) Management Segment - this component is necessary for processing the collected Security events by analysts, building information graphs based on the information received, and implementing automated processes that will allow for instant response to information security incidents.

Conclusion

The task of collecting and management security incidents has been solved with cloud deployment of an system's improvement for collecting and processing incidents, which will allow companies to send events from any country in the world at any time and will allow building a holistic picture of the functioning of workstations and information systems of companies. This approach opens up the possibility of instant and automated responses to Cyber Security incidents.

References

1. Pedchenko Y., Ivanchenko Y., Ivanchenko I., Lozova I., Jancarczyk D., Sawicki P. (2022). Analysis of modern cloud services to ensure cybersecurity. 26th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES 2022), 26 (207), 110-117. https://doi.org/10.1016/j.procs.2022.09.043

UDC 37.018.43:004.8(043.2)

USE OF ARTIFICIAL INTELLIGENCE IN ACADEMIC ASSIGNMENTS

Maliarenko Sofiia

National Aviation University, Kyiv

Scientific supervisor – Gulak Natalia Kostyantynivna, Associate Professor

Keywords: artificial intelligence, ChatGPT, plagiarism, academic work, information technologies.

Abstract*. Nowadays informational technologies are changing quickly, new technologies are creating, and old ones are improving. For instance, groundbreaking artificial intelligence is the non-human/ machine intelligence technology that enables it to perform various functions. The usage of artificial intelligence is becoming an up-to-the-meaning topic, also in the educational field, which advanced in recent years, and here is rising a question about the clarity of implementing artificial intelligence and its place in it.*

Introduction.

Recently launched ChatGPT cracked the ground on the Internet and instantly turned into the most discussed topic among people. This work aims to investigate the influence of ChatGPT on the educational process and students' academic assignments. ChatGPT is an artificial intelligence chatbot developed by OpenAI and released in November 2022 [1]. ChatGPT was launched as a prototype on November 30, 2022, and quickly drew attention for its detailed responses and articulate responses across multiple knowledge domains [2].

Main part

ChatGPT has the potential to give a major number of benefits for education and the ability to change the way of studying. Nevertheless, it has faced societal biases and caused a huge number of questions among consumers. The most popular concerns are academic honesty and plagiarism.

This paper uses theoretical, informational, and methods of analysis of the collected material.

On the positive side, students can apply ChatGPT in a different variety of tasks: translating, writing, content generation (different types of written content), searching, question answering, conversation, faster access to information, etc. Professors can implement AI-generated content into the learning process by creating faster and more personalized interactive assignments for each student with less time consumption. Also, it can cause better engagement among students, and automatize learning prosses. In fact, AI can be used for the automation of educational processes, the generation of content, and the creation of instructions, and can be useful for students' e-learning resources and tools. In addition, it can help review the student's work, and score, and provide feedback on assignments. Indeed, it is a solid source of information and a useful tool for the education field.

While employing ChatGPT in education one should consider using it with transparency and high respect for fairness. One of the most significant security threats is the risk of plagiarism, the act of plagiarizing happens when you use one's ideas and pretend that it is your ideas despite that while using ChatGPT, as an example, while writing academic work, you do not use someone's words despite the fact you do not use your text. With the usage of AI, while working on academic assignments, students can ask to create a paragraph or even a whole text, which will lead to one of the biggest challenges of presenting ChatGPT in educational prosses, inequality, and unreliability. It possibly can create a low level of academic honesty among students. There are some concerns about the reliability, has been found that in some cases ChatGPT accidentally can provide biased, incorrect, or even unethical information. If this data is distorted, the same applies to the machine. Moreover, if students rely too heavily on AI tools to complete their assignments, they may not take full responsibility for their work. This could result in a lack of accountability and a failure to develop critical thinking skills.

As we know, ChatGPT generates responses based on information entered, so everything that has been sent to will be processed. Raised some questions about the security of use, students possibly can provide their personal information, if students use AI tools to complete their assignments, they may be required to provide personal information, such as their name, email address, or other identifying information. If this information is not appropriately protected, it could be used for malicious purposes such as identity theft, cyberstalking, or other types of cybercrime. AI tools that are not appropriately secured could also be vulnerable to malware. Malware could be used to steal sensitive information, disrupt academic activities, or cause other types of damage, so here rises the problem, how can one provide the required protection of student data, and who will be responsible for it?

Likewise, there are some tactics that can help resolve part of the problems for academic assignments: put a limit on using AI, use special tools to indicate a sign of plagiarism, provide students information about basic rules for security on the internet, prevent data breaches and other security threats, it's important to implement security measures such as data encryption, firewalls, and multi-factor authentication, also, ask to do a reference list, and carefully observe students’ work.

In some counties, ChatGPT has already been banned for use in academic works due to cheating issues. Teachers and school authorities are suspicious of plagiarism, which is unavoidable if students use ChatGPT for their assignments. Plagiarism has always been a big problem in the learning process, during the performance of academic works, and now it has the potential to become much more common and less noticeable to the examiner. And now, there is no tool that can help one to accurately detect AI signs.

Conclusions

Artificial intelligence, and to be more precise, ChatGPT, has the potential to provide many new and useful learning opportunities. The question of the accuracy of its use and the order in which it is introduced into the educational process is still a matter of urgency. The same applies to the established limit on the use of artificial intelligence technologies in students' academic works.

References

1. "ChatGPT — Release Notes". Archived from the original on February 8, 2023. Retrieved February 8, 2023.

2. Lock, Samantha (December 5, 2022). "What is the AI chatbot phenomenon ChatGPT and could it replace humans?". The Guardian. Archived from the original on January 16, 2023. Retrieved December 5, 2022.

UDK УДК 004.056.5:004.738.5(043.2)

USING THE CHATGPT LANGUAGE MODEL FOR USER EXPERIENCE RESEARCH

Olexii Pidhainyi
National Aviation University, Kyiv

Research supervisor - Oleksandr Moroz, Ph.D., Associate professor

Keywords: AI, ChatGPT, User Research, UX Design, Large language model

Introduction

Large language models like ChatGPT by OpenAI have become popular for their impressive performance on various tasks, including enabling conversational communication with machines using natural language processing and machine learning algorithms [1]. ChatGPT developed by OpenAI [2] is one such implementation. This platform utilizes natural language processing and machine learning algorithms to enable users to communicate with machines in a conversational manner [3].

The use of ChatGPT in UX research is a relatively new area of research. It's conversational competency and reasoning capabilities create opportunities to explore the roles of conversational agents in design and human-AI collaboration. [4, 5, 6]. The use of ChatGPT in UX research represents a promising new avenue for researchers to better understand user needs and preferences. This thesis aims to explore the potential of ChatGPT as a tool for UX research and to identify best practices for its use in this context.

Materials and methods

A four-stage experiment was conducted to explore ChatGPT's potential and limitations. The stages included stating the project's aim and approach, researching fictional users, brainstorming, and evaluating user experience. The study was completed in a single session with the researcher serving as the designer and providing prompts for all tasks, with follow-up prompts if necessary.

Results

To design a good product, understanding competitors is essential. When ChatGPT was asked to summarize the common e-commerce app issues faced by mobile users, some of the points provided were too general, while others were specific and useful. For instance, "limited payment options" and "poor customer support" are significant sources of friction for many users, as per my experience in creating such apps. Next, ChatGPT was instructed to generate a list of direct competitors in our niche for the UA market. ChatGPT suggested Rozetka, Olx, Prom, and others. It was also able to determine each competitor's market share with data sources, although using outdated data sources as ChatGPT's training data is limited to 2021 [7].

ChatGPT can generate use cases, likes/dislikes, personas, and even simulates user sessions using AI participants [2]. However, some researchers may be hesitant about using it because ChatGPT

works by pulling existing text from the web and does not understand queries literally. Instead, it strings together sentences based on probabilities [3], similar to someone saying what they think people want to hear.

ChatGPT was requested to tell what users like about Rozetka and then ask what users like about Olx. The results are very similar overall: a wide range of products, competitive prices, user-friendly website and app, etc. The information is too vague and lacks specifics on what makes each app intuitive. There is no new knowledge coming from this information, and nothing actionable for designers to take away from it, because ChatGPT works by pulling existing text from the web and does not understand queries literally. Instead, it strings together sentences based on probabilities [2]. Additionally, it's unclear where the information is coming from, whether it's from online reviews, developer websites, or other sources.

ChatGPT can also be utilized to determine the essential key performance indicators (KPIs) and metrics for success of a specific product or service. For instance, when exploring the e-commerce app domain, ChatGPT was asked for relevant KPIs and received common but valuable metrics such as conversion rate, average order value, and customer acquisition cost.

Next I tried doing some user research on fictional users. ChatGPT successfully created 3 personas for me: Sarah, the busy mom; John, the tech-savvy millennial; Maria, the budget-conscious student. For each persona, it specified demographics, needs & wants and provided relevant contextual information. The primary persona was defined as Sarah - a good all-rounder.

After generating the personas, ChatGPT was asked to prepare ten interview questions for user research. Although there were no specifications for the aim of the interview or who will be interviewed, ChatGPT generated ten questions relevant to understanding the lives and experiences of potential users in the scope of the project, which were reasonable and useful. After obtaining the simulated interviews, ChatGPT was tasked with creating an overall summary. The simulated user feedback across all interviews was overwhelmingly positive with only a few negative points. ChatGPT also identified important features like accessibility, order tracking, and a reward program that were missed during the interviews. The next activity was ideation, where ChatGPT was asked some questions in “How might we” form. All suggestions were good, with some useful details.

Conclusion

This study aimed to evaluate ChatGPT's capabilities, limitations, and suitability to support research. While ChatGPT can assist in secondary research, as it relies on the already available. But using it for primary research raises concerns as it relies on existing data and cannot reveal unknown behavior patterns or insights. Inclusive design, which is about people who are left behind, cannot be achieved with AI alone. However, using ChatGPT and other LLMs can speed up the design process and potentially change how design services are delivered and consumed.

References

[1] Mubin Ul Haque, Mubin Ul Haque, Zarrin Tasnim Sworna, Roshan Rajapakse "I think this is the most disruptive technology": Exploring Sentiments of ChatGPT Early Adopters using Twitter Data — 2023

[2] A. Shaji George, A.s Hovan George, A S Gabrio Martin A Review of ChatGPT AI's Impact on Several Business Sectors — 2023

[3] Eeman Majumder ChatGPT-what is it and how does it work exactly? — 2022 [Digital resource]. URL: https://medium.com/geekculture/chatgpt-what-is-it-and-how-does-it-work-exactly-62e7010524d3

[4] Dominik Dellermann, Adrian Calma, Nikolaus Lipusch, Thorsten Weber, Sascha Weigel, Philipp Ebel. Year. The Future of Human-Ai Collaboration: A Taxonomy of Design Knowledge for Hybrid Intelligence Systems. In Proceedings of Hawaii International Conference on System Sciences (HICSS)

[5] Dakuo Wang, Elizabeth Churchill, Pattie Maes, Xiangmin Fan, Ben Shneiderman, Yuanchun Shi, Qianying Wang. Year. From Human-Human Collaboration to Human-Ai Collaboration: Designing Ai Systems That Can Work Together with People. In Proceedings of Extended abstracts of the 2020 CHI conference on human factors in computing systems. 1-6

[6] Qingxiao Zheng, Yiliu Tang, Yiren Liu, Weizi Liu and Yun Huang. Year. Ux Research on Conversational Human-Ai Interaction: A Literature Review of the Acm Digital Library. In Proceedings of CHI Conference on Human Factors in Computing Systems. 1-24.

[7] Joshua J. Why doesn't ChatGPT know about X? 2022 [Digital resource]. URL: https://help.openai.com/en/articles/6827058-why-doesn-t-chatgpt-know-about-x

УДК 004.053

REUSABLE COMPONENTS IN MODERN SOFTWARE DEVELOPMENT

Vladyslav Studennykov, Andrii Vynarchuk

National Aviation University, Kyiv

Scientific Advisor: PhD., associate professor Tetiana Konrad

Key words: code reuse, software development, software architecture, design patterns, object-oriented methodology.

Introduction

When developing software, reducing labor costs and development time while maintaining software quality is an urgent task. One way to achieve this is by reusing components - either partially or fully - from previously created software systems. This approach is well-known for reducing development costs. Reuse of components for prototyping software systems is given in the Demin's work. Researchers like R. Gamzayev, M. Tkachuk, and O. Tovstokorenko have proposed an approach to analyzing the degree of code reuse in dynamic software product lines (DSPL). However, despite its popularity, John Ousterhout noted that "copying and pasting code is a dangerous practice" [1]. Therefore, it is essential to analyze the advantages and disadvantages or limitations of modern methods of reusing software components. Such an analysis can help to improve the quality of the software development process. This study aims to explore the concept of component reuse in software development by identifying potential opportunities and limitations of this approach

Materials and methods.

The object of research is the process of components reuse of the software systems. The research is based on the use of methods: analysis and systematization - study of literary sources; identification of advantages and limitations of methods of software systems component reuse; systemic approach – consideration of the research object as a component of software engineering; generalization - conclusions based on research results.

Results.

Engineering reusable components is a purposeful and systematic activity that involves selecting implemented software artifacts and analyzing their functions to incorporate them into a designed system as ready-made components. The most common methods for achieving this include reusing parts of program code, organizing classes into reusable components, and utilizing design patterns.

Reuse of code within one software is called horizontal, several - vertical [2]. The advantages of the method are increased work productivity and reduced software development time. Code reuse may require modifying it to meet new requirements, in which case additional work is required to find reusable code elements, obtain the necessary components, and modify the program code [3], or use

the code elements without changes. To use the code without changes, subroutines can be used, in which the code is structured in the form of separate blocks. In modern programming languages, these blocks are called functions (or methods) with the following requirements: independence of the function from external elements; the function should not affect variables outside the scope; functions must perform one action, have a clear name (for ease of reuse); have a small number of arguments (no more than 2-3) [4]. As a rule, the general program code can be recursively decomposed into functions, each time receiving more highly specialized functions (1960, Eger Dijkstra) [5]. Within the framework of OOP methodology, a developer can add new functionality to an existing class through inheritance, to add new functionality to classes without changing the code of the parent classes and the existing architecture, but only supplementing it. If the software tool does not have a clear architecture, or the relationships between the program elements are not tested, it can be difficult to select elements for reuse. For complex software, a large number of interrelated classes may appear which will complicate the search and integration into new software [3].

Components are used in modern software engineering to organize classes for later reuse. Components organize classes into structures that make it easier to find elements for reuse and extend the functionality of existing software. Requirements for components: a component must be a set of organized classes that have the same purpose; must have the same reason for the change as the classes in the component; include all classes that will be reused together. This helps to create an independent module that can be reused, in particular for creating complex software systems [5].

In modern development, not only code can be reused, but also design ideas, specifications, etc. [1]. Design patterns can speed up the development process, because a pattern is a ready-made idea for solving a certain problem. However, the use of the same design patterns in all projects can complicate software development, so the pattern helps to make new changes and supplement the code more easily, but is not capable of significantly simplifying the development of a software tool. It is also possible to use software frameworks - structures with a certain architecture that provide components for reuse [6].

Conclusions

The analysis of methods for reusing software system components has demonstrated their usefulness for software engineering. By identifying the advantages and limitations of these methods, it is possible to reduce time costs and improve the quality of software development. Therefore, considering these factors is essential to ensure the effective use of component reuse in software development.

Materials:

[1] John K. Ousterhout (2018) A philosophy of software design. Palo-Alto: Yaknyam Press.

[2] Maria Smolarova, Pavol Navrat (1997) Software Reuse: Principles, Patterns, Prospects. Bratislava: Slovak University of technology, Journal of computing and Information Technology.

[3] Ambler S. (1998) A realistic look at object oriented reuse, from https://www.drdobbs.com/a-realistic-look-at-object-oriented-reus/184415594

[4] Martin Robert (2009) Clean Code. Boston: Pearson Education, Inc.

[5] Martin Robert (2018) Clean Architecture A CRAFTSMAN'S GUIDE TO SOFTWARE STRUCTURE AND DESIGN. Boston: Pearson Education, Inc.

[6] Krzysztof Cwalina, Brad Abrams (2009) . Framework design guidelines: Conventions, Idioms, Patterns for reusable .NET Libraries. Boston: Pearson Education, Inc.

УДК 004.75

PROSPECTS FOR THE DEVELOPMENT OF SOFTWARE FOR RENTING AND SELLING REAL ESTATE

Tatarchyna Daryna

National Aviation University, Kyiv

Supervisor – Victoria Trofymchuk, senior lecturer

Keywords: Real estate, software, automation, artificial intelligence, machine learning, optimization, technology, prospects.

Introduction

The article studies the prospects for the development of software for renting and selling real estate. It explores the advantages of using software for real estate, including increased efficiency, improved accuracy, and better decision-making. The article also highlights the potential for future advancements in real estate technology.

The purpose of the research is describing the potential for the development of software to revolutionize the way real estate properties are managed and transactions are conducted.

The real estate industry is constantly evolving, and the use of technology has become essential for businesses to thrive in this sector. In recent years, the development of software for renting and selling real estate has become increasingly popular. The software is designed to make the process of buying, selling, and renting properties more efficient and convenient for all parties involved. In this article, we will explore the prospects for the development of software for renting and selling real estate.

Materials and methods

One of the main advantages of using software for real estate is the ability to streamline the process of listing properties. With the help of software, property managers can easily create detailed property listings that can be shared across multiple platforms. This allows for a wider reach and ensures that potential renters or buyers can easily access the necessary information about a property.

Moreover, software for real estate can also be used to automate many of the processes involved in renting or selling a property. This includes tasks such as tenant screening, lease agreements, rent payments, and property inspections. Automating these tasks not only saves time but also reduces the chances of errors, making the entire process more efficient.

Another advantage of using software for real estate is the ability to manage and track the performance of a property portfolio. This allows property managers to easily monitor occupancy rates, rent payments, maintenance schedules, and other important metrics. This information can be

used to identify areas where improvements can be made, helping to optimize the portfolio for maximum returns.

Result

In addition to these benefits, software for real estate also has the potential to revolutionize the way people search for properties. With the help of artificial intelligence and machine learning, software can analyze a user's search history and preferences to provide personalized property recommendations. This can help to streamline the search process and ensure that users are presented with properties that are most relevant to their needs.

Looking forward, the prospects for the development of software for renting and selling real estate are very promising. As technology continues to evolve, it is likely that software will become even more sophisticated and efficient. This will further streamline the processes involved in real estate transactions, making it easier for property managers, tenants, and buyers to conduct business.

Conclusion

The development of software for renting and selling real estate has the potential to revolutionize the way properties are managed and transactions are conducted. The benefits of using software for real estate include increased efficiency, improved accuracy, and better decision-making. As the real estate industry continues to evolve, it is important for businesses to embrace new technologies in order to stay ahead of the competition.

References

1. *Capozzoli, A., Rafferty, M., & White, R. (2020). Real estate technology: The future is now. Deloitte Insights.*

2. *Sardi, D. (2018). Real estate technology: Disruption and innovation. Journal of Real Estate Literature, 26(1), 139-153.*

3. *Gu, Y., & Xiao, L. (2019). The impact of artificial intelligence on the real estate industry. Journal of Real Estate Research, 41(1), 1-24.*

4. *Stojanovska, M. (2019). Digital transformation in the real estate industry. Economic Review: Journal of Economics and Business, 17(1), 53-67.*

5. *Luskin, A. (2019). PropTech: The future of real estate. Forbes.*

УДК 004.383.4:658.3.07

ОСОБЛИВОСТІ СТВОРЕННЯ СПЕЦІАЛІЗОВАНИХ AI ТА ВТІЛЕННЯ ЇХ В ДІЯЛЬНОСТІ ПІДПРИЄМСТВ

Олександр Антонюк, Олександр Єлісеєв
Національний авіаційній університет, Київ

Науковий керівник – Гращенко І. С., к.е.н., доцент.

Ключові слова: штучний інтелект, спеціалізація, ефективність, оптимізація.

Вступ

Процеси автоматизації та оптимізації діяльності підприємств станом на сьогодні є одними із ключових напрямків вивільнення частини коштів без втрати, а часто навіть з підвищення ефективності відповідних робіт, що дозволяє перенаправити їх в інші сфери функціонування та сприяє кращим кінцевим результатам. Штучний інтелект дозволяє якісно оптимізувати діяльність компанії, беручи на себе виконання великої кількості повторюваних рутинних робіт, при цьому справлячись з ними швидше, краще та дешевше людей.

Матеріали і методи

Важливо відзначити, що спеціалізація штучного інтелекту є важливим аспектом для розвитку і застосування цієї технології в різних сферах, починаючи від медичної сфери, проведення спостережень за станом здоров’я пацієнта або прогнозування можливих його захворювань, та закінчуючи банківськими операціями, логістикою. Саме спеціалізація дозволяє штучному інтелекту стати більш ефективним у виконанні конкретних завдань.

Рис.1 Порівняння зображень, які генерує AI Midjourney у своїй 1 (лівий блок картинок) версії та 5 (правий блок картинок). *Джерело: згенеровано штучним інтелектом Midjourney*

Результати

Прикладом всіх перерахованих переваг може слугувати розвиток, еволюція, різних штучних інтелектів які взаємодіють з людьми у відкритому доступі, наприклад GPT-4, Midjourney та інші. Якщо порівнювати AI Midjourney у п’ятій версії з її релізною, першою, можемо побачити суттєву різницю у якості та деталізації зображення (рис. 1). Ще одним яскравим прикладом може слугувати розвиток ChatGPT, що є чат-ботом, який створений на

основі архітектури GPT (Generative Pre-trained Transformer) та розвивається компанією OpenAI. Вона заснована на технології глибокого навчання з використанням трансформерів, яка дає можливість моделі обробляти великі обсяги тексту і генерувати відповіді з високою якістю [4]. Її можливості вражають: вона має 175 мільярдів параметрів, може генерувати тексти з різною стилістикою та мовою, і може бути використана для вирішення різноманітних задач, а також нещодавно почалось тестування версії GPT-4 [1].

Компанія Amazon використовує штучний інтелект для свої чат-ботів, де є шаблони спілкування для певних ситуацій і змінні у вигляді назв товарів, для рекомендації продуктів, шляхом аналізу місця розташування останніх покупок та відгуків щодо них, завдяки чому сьогодні система рекомендації продуктів Amazon забезпечує 35% від усього обсягу продажів. Також варто зазначити про успішний досвід використання штучного інтелекту компанією IBM, яка теж вже протягом великої кількості років концентрує свою увагу на розвитку технології ШІ, їхній Watson, що є суперкомп'ютером, який поєднує в собі штучний інтелект та складне аналітичне програмне забезпечення, і має широкий асортимент використання: від пошуку інформації до надання відповідей на питань на відкриті теми [3]. Щодо статистичних даних успішності сфери використання ШІ, то за даними Grand View Research, у 2020 році світовий ринок штучного інтелекту становив 62 мільярди доларів, і очікується, що з 2021 по 2028 рік він буде зростати на 40,2% [2].

Висновок

Отже, спеціалізація є важливою складовою розвитку штучного інтелекту, яка дозволяє покращити ефективність, зменшити складність та збільшити гнучкість використання цієї технології. Також не менш важливою складовою ефективного AI є його розвиток, навчання, що може здійснюватися у багатьох варіантах але одним з найефективніших є «спілкування» з людьми, тобто виконання завдань від них, це дозволяє розробникам знаходити помилки та доопрацьовувати програми швидше ніж у інших випадках, та знайти правильні вектори розвитку свого штучного інтелекту.

Список використаних джерел:

1. Saqib M. The Future of AI: GPT-3 vs GPT-4: A Comparative Analysis. *Medium*. URL: https://cutt.ly/L4zBV0n (date of access: 20.03.2023).

2. How Do Businesses Use Artificial Intelligence?. *Wharton Online*. URL: https://cutt.ly/94zB8Zw (date of access: 20.03.2023).

3. Marr B. The 10 Best Examples Of How Companies Use Artificial Intelligence In Practice. *Forbes*. URL: https://cutt.ly/P4zNllH (date of access: 20.03.2023).

4. Економічна правда. GPT-4 більший і кращий за ChatGPT, але OpenAI не пояснює, чому. Що відомо про нову модель?. *Економічна правда*. URL: https://cutt.ly/N4cqyst (дата звернення: 20.03.2023).

УДК 004.056.5:004.738.5(043.2)

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Зінаїда Біла

Національний авіаційній університет, Київ

Науковий керівник – Валерій Козловський, д.т.н., проф.

Ключові слова: інформація, захист, злочин, Інтернет, безпека.

Вступ

Сьогодні глобальна всесвітня мережа, що об’єднує мільйони комп’ютерів у транснаціональну єдину систему Інтернет, відкриває широкі можливості для спілкування та обміну інформацією будь-якого характеру. Кожного року кількість інформації, яка зберігається в електронному вигляді, зростає не просто в арифметичній, а саме в геометричній прогресії. Це призводить до порушення конфіденційності та безпеки інформації, також це може супроводжуватися зростанням кіберзлочинів, таких як: підробка та розкрадання комп’ютерної інформації, створення та поширення вірусів, втручання у роботу комп'ютерів, фішинг тощо. Через це, в наш час актуальним є питання захисту інформації[1].

Матеріали і методи

Основним завданням захисту інформації в інформаційних системах є забезпечення конфіденційності, цілісності та доступності інформації(КЦД), що зберігається, обробляється та передається в цих системах(Рис.1).

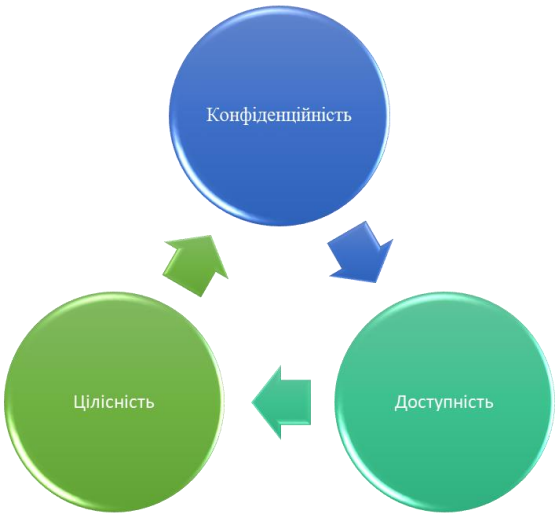

Рис.1. Тріада КЦД

Результати

З технічної точки зору, інформаційна безпека означає захист інформації під час зберігання, передачі та обробки від таких дій, як несанкціонований доступ, пошкодження та інших дій, які можуть призвести до порушення роботи інформаційних систем.

Слід зазначити, що одним з основних напрямків розвитку практичних методів захисту інформації в інформаційних системах є використання штучного інтелекту для розпізнавання поведінки користувачів і процесів, що відбуваються в системах, а також для їх аналізу.

Використання штучного інтелекту може дозволити і допомогти автоматично виявляти підозрілі дії користувачів і незвичайні ситуації, які можуть безпосередньо вказувати на можливу кібератаку або порушення безпеки даних. Це дозволяє автоматично перевіряти та аналізувати великі обсяги даних, що, в свою чергу, дозволяє швидко виявляти та реагувати на нові загрози.

Захист інформації в інформаційних системах - це процес, який потребує постійної уваги та оновлення, оскільки щодня з'являються нові загрози інформаційній безпеці. Тому для ефективного захисту інформації необхідно проводити регулярне сканування системи на наявність вразливостей і вдосконалювати захист з урахуванням нових методів і технологій.

Протягом історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми — комп'ютерні злочини стали характерною ознакою сьогодення[2].

Подане дослідження показало, що розробка нових технологій та методів захисту інформації буде продовжуватися і надалі, оскільки це необхідно для забезпечення безпеки інформації в цифрову епоху.

Висновки

Процес захисту інформації в інформаційних системах вимагає вдосконалення технологій та методів захисту від нових загроз та кібератак. Тому важливо постійно вдосконалювати системи інформаційної безпеки та використовувати новітні технології для забезпечення найвищого рівня захисту.

Список використаних джерел

1. Технології захисту інформації [Електронний ресурс]. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186

2. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник / О. А. Самойленко. Одеса : , 2020. 112 с.

УДК 004.056.5:004.738.5(043.2)

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ГОЛОСОВИХ ПОМІЧНИКІВ У СФЕРІ ТОРГІВЛІ

Владислав Бойко

Національний авіаційній університет, Київ

Ключові слова: інформація, захист, злочин, Інтернет, безпека.

Вступ

Розвиток технологій, що роблять можливим розпізнавання людської мови, привів до появи ряду практичних застосувань, таких як ідентифікація особи за звуком голосу та голосові помічники. Для двостороннього спілкування голосовий помічник повинен бути в змозі проаналізувати почуте і винести судження про сенс сказаного людиною. У найпростіших випадках таке судження зводиться до задачі розпізнавання образів з класифікацією, тобто віднесення висловлювання людини до одного з класів. Більш складний підхід передбачає можливість визначення сенсу голосових повідомлень довільної форми.

Матеріали і методи

Програмне забезпечення, що використовується для розпізнавання тих чи інших аспектів голосу, використовує технології згорткових нейронних мереж та нейромереж з довгою та короткочасною пам’яттю [1, 2].

На даний час голосові помічники впроваджуються у багатьох сферах, таких як керування окремими побутовими приладами, керування застосунками «розумного дому», керування комп’ютером, автомобілем, пошук інформації, інтерфейси різноманітних онлайн-сервісів, відправка повідомлень, і навіть вивчення іноземних мов.

Результати

Дослідження показують, що використання голосових помічників у процесі спілкування клієнта з магазином та придбання товарів чи послуг займає одне з останніх місць серед усіх застосувань голосових помічників, і ця ситуація від року у рік не покращується [3]. Небажання споживачів використовувати технологію голосових помічників у процесі добору товарів і здійснення покупок викликане цілим рядом проблем.

Перша з таких проблем – недостатні системні характеристики споживацьких пристроїв. Алгоритми штучного інтелекту для розпізнавання мови та використовувані ними бази даних мають значний обсяг. Для роботи у реальному часі вони вимагають наявності потужних обчислювальних пристроїв і пристроїв зберігання з великим обсягом і пропускною здатністю. Пристрій споживача, такий як смартфон чи ноутбук, не може забезпечити виконання таких вимог, тому програмне забезпечення, що якісно розпізнає голосові повідомлення, має

виконуватись у хмарному середовищі, а користувачу для зв'язку з ним необхідно мати швидкісний доступ до Інтернету. Звідси виникають побоювання, пов'язані з проблемами конфіденційності. Голосові помічники повинні постійно слухати звуки, що звучать у приміщенні, очікуючи на команди, надані користувачем. Інформація про почуте передається в інтернет, таким чином голосовий помічник фактично веде постійний запис приватних розмов у повсякденному житті користувача, пізніше отримані таким чином дані можуть бути використані проти користувача.

Ще одне побоювання безпеки пов'язане із можливою вразливістю технології розпізнавання голосу до кібератак. Голосові помічники можуть розпізнавати голосові команди, нечутні для людського вуха. Зловмисники можуть використовувати цю можливість для доступу до приватної інформації користувача або для виконання покупок від його імені. При цьому можуть бути використані записи оригінального голосу користувача або технології симуляції голосу, що унеможливить виявлення підробки чи суттєво знизить її імовірність.

Незважаючи на значну використовувану обчислювальну потужність, якість розпізнавання мови на даний час не ідеальна. Голосові помічники можуть неправильно інтерпретувати певні слова, не розуміти абревіатури, сленгові слова, специфічний акцент у вимові, тощо. Це може призвести до помилок у роботі системи. Якість розпізнавання голосу також може суттєво падати через наявність фонового шуму, в той час як користувач не завжди може забезпечити відсутність шумів вдома чи на роботі.

Висновки

Актуальними задачами в галузі створення голосових помічників є проведення експериментів з розпізнаванням голосу з урахуванням факторів, які можуть впливати на результати розпізнавання, тобто дослідження моделей розпізнавання мовлення, їх можливих застосувань, та у зв'язку з цим дослідження відповідних архітектур нейронних мереж.

Список використаних джерел

1. C. H. Taal, R. C. Hendriks, R. Heusdens and J. Jensen. A short-time objective intelligibility measure for time-frequency weighted noisy speech. Proceedings of 2010 IEEE International Conference on Acoustics, Speech and Signal Processing. 2010. Pp. 4214-4217. DOI: 10.1109/ICASSP.2010.5495701.

2. A. Torfi, S. M. Iranmanesh, N. Nasrabadi and J. Dawson, 3D Convolutional Neural Networks for Cross Audio-Visual Matching Recognition. IEEE Access. 2017, vol. 5, pp. 22081 – 22091. DOI: 10.1109/ACCESS.2017.2761539.

3. A. P. K. Muthukumaran, H. Vani. Optimizing the usage of voice assistants for shopping //Indian Journal of Science and Technology. – 2020, No. 13 (43). Pp. 4407 – 4416. DOI: 10.17485/IJST/v13i43.1911.

УДК 629.78

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА ОПТИМІЗАЦІЯ ПАРАМЕТРІВ РУХУ КОСМІЧНОГО АПАРАТУ

В'ячеслав Василенко

Національний авіаційній університет, Київ

Науковий керівник – Петро Жук, д-р. фіз.-мат. наук., доц.

Ключові слова: принцип максимуму Понтрягіна, крайова задача, метод стрільби.

Вступ

Оптимальне проектування траєкторії необхідне на всіх етапах космічного польоту: від траєкторії виведення супутника на робочу орбіту, подальших операцій із підтримання станції і до утилізації наприкінці терміну служби. Сучасний науковий підхід до вирішення цієї задачі полягає у використанні методів теорії оптимального керування на основі математичної моделі руху космічного апарата (див. [1]).

Матеріали і методи

Математична модель руху космічного апарата в системі координат *OXYZ*, пов'язану з центральним тілом, має вигляд [2]:

$$\frac{d\mathbf{v}}{dx} = \mathbf{g(r)} + \frac{\mathbf{F}}{m}, \qquad \frac{d\mathbf{r}}{dx} = \mathbf{v}, \tag{1}$$

де t - час, $\mathbf{r} = \left[r_x, r_y, r_z \right]^T$ і $\mathbf{v} = \left[v_x, v_y, v_z \right]^T$ - радіус-вектор і вектор швидкості космічного апарата в в системі координат *OXYZ*, $\mathbf{g(r)} = -\mu \dfrac{\mathbf{r}}{r^3}$ - вектор прискорення сили тяжіння центрального тіла, $r = |\mathbf{r}|$, μ - гравітаційний параметр тіла, $\mathbf{F}$ - сила тяги двигуна, m - маса космічного апарата, яка підраховується за формулою:

$$\frac{dm}{dt} = -\frac{F}{W_e}, \tag{2}$$

$F = |\mathbf{F}|$, W_e - ефективна швидкість витікання частинок у реактивному струмені.

Результати

Крайові умови для системи (1) подамо у вигляді:

$$\mathbf{r}_0 = \mathbf{r}(t_0), \quad \mathbf{v}_0 = \mathbf{v}(t_0) + V_\infty \mathbf{e}_v, \quad m_0 = m_0(V_\infty), \quad \mathbf{r}_T = \mathbf{r}(T), \quad \mathbf{v}_T = \mathbf{v}(T), \tag{3}$$

де t_0 і T - час початку і кінця перельоту, $\mathbf{r}_0$, $\mathbf{v}_0$, $\mathbf{r}_T$, $\mathbf{v}_T$ - положення і швидкості космічного апарата на початку t_0 і в кінці T; $\mathbf{r}(t_0)$, $\mathbf{v}(t_0)$, $\mathbf{r}(T)$, $\mathbf{v}(T)$ - фіксовані вектори положення і швидкості небесного тіла відльоту і прильоту, відповідно, на початку t_0 і в кінці

T; $|\mathbf{e}_v| = 1$, V_∞ - гіперболічний надлишок швидкості космічного апарата при відльоті від небесного тіла при t_0; $m_0(V_\infty)$ - деяка відома функція, що визначає початкову масу космічного апарата за швидкістю V_∞.

Задача оптимізації траєкторії руху космічного апарата при перельоті з одного на інше небесне тіло полягає в наступному: для фіксованих значень t_0 і T необхідно знайти величину V_∞^{opt}, вектор $\mathbf{e}_v^{opt}$ і визначену на деякій допустимій множині вектор-функцію $\mathbf{F}^{opt}(t)$, що доставляють максимум кінцевій масі $m_T = m(T)$, за умови, що рух космічного апарата описується системою диференціальних рівнянь (1), (2) і задовольняє співвідношенням (3).

Наведену вище задачу оптимізації можна розв'язати за допомогою методів теорії оптимального управління, зокрема, принципу максимуму Понтрягіна. Нелінійна двоточкова крайова задача принципу максимуму ефективно розв'язується чисельними методами, зокрема, методом стрільби.

Висновки

Побудовано математичну модель руху космічного апарата при перельоті між космічними об'єктами у вигляді крайової задачі для системи звичайних диференціальних рівнянь. На основі цієї моделі сформульована задача оптимізації траєкторії руху космічного апарата з управлінням силою тяги двигуна. Для розв'язання цієї задачі пропонується використання принципу максимуму Понтрягіна та метод стрільби для числового розв'язання крайової задачі принципу максимуму.

Список використаних джерел

1. Bernardini N., Wijayatunga M.C., Armellin R., & Baresi N. State-dependent trust region for successive convex optimization of spacecraft trajectories // In Space Flight Mechanics Meeting. 2023 (february). pp. 1-20.

2. Ivashkin V.V., Krylov I.V. Optimization of trajectories for a spacecraft with an electric rocket engine of low thrust // Preprints of the Keldysh Institute of Applied Mathematics. 2020. N 94. 32 p.

УДК 811.111 (043.2)

НОВІ ВИКЛИКИ КІБЕРБЕЗПЕЦІ В ЕПОХУ ШТУЧНОГО ІНТЕЛЕКТУ

Юрій Василюк Володимир Шлапак

Національний авіаційний університет, Київ

Науковий керівник –Олександр Туровський, д.т.н., проф.

Ключові слова: сканер, антивірус, інтерфейс, оптимізація.

Вступ

У сучасному світі штучний інтелект є неодмінною складовою технологічного прогресу, який має значний вплив на розвиток бізнесу та суспільства в цілому. Однак, разом з перевагами, які принесли інновації в галузі штучного інтелекту, з'явилися і нові виклики для кібербезпеки.

Матеріали і методи

До нових викликів кібербезпеки віднесемо.

По-перше, створення алгоритмів штучного інтелекту вимагає значної кількості даних. Це ставить питання про захист цих даних від несанкціонованого доступу, викрадення чи втрати. Крім того, інформація, що збирається для навчання систем штучного інтелекту може містити конфіденційні дані про користувачів, що може призвести до порушення їх прав на приватність.

По-друге, з'явилися нові загрози для кібербезпеки, пов'язані з використанням штучного інтелекту в злочинних діях. Наприклад, кіберзлочинці можуть використовувати штучний інтелект для створення нових видів шкідливих програм, які можуть обходити захист від класичних антивірусів.

По-третє, штучний інтелект може бути використаний для відправки фішингових повідомлень, що є серйозною загрозою для кібербезпеки. Інтелектуальні системи можуть аналізувати стилі письма та поведінку користувачів в Інтернеті, що може бути використано для створення реалістичних фішингових повідомлень.

По-четверте, штучний інтелект може бути використаний для створення додаткових каналів атак на комп'ютерні системи, кільки він може здійснювати атаки в реальному часі та адаптуватися до захисту системи. Наприклад, атаки, засновані на штучному інтелекті, можуть здійснюватися шляхом швидкого розпізнавання вразливостей в системах безпеки та швидкого підбору оптимальних варіантів атаки на основі зібраних даних.

По-п'яте, штучний інтелект може бути використаний для підробки та маніпулювання інформацією в Інтернеті. Наприклад, інтелектуальні системи можуть бути використані для створення ботів, які можуть поширювати дезінформацію або відстежувати дії користувачів.

Для того, щоб забезпечити кібербезпеку в епоху штучного інтелекту, необхідно приділяти більшу увагу захисту даних та захисту від нових видів кіберзлочинів, пов'язаних з штучним інтелектом.

Результати

Деякі приклади таких кіберзлочинів зі штучним інтелектом включають:

Атаки на системи розпізнавання обличь: Системи розпізнавання обличь на основі штучного інтелекту використовуються в багатьох сферах, включаючи банківський сектор та системи безпеки. Проте, злочинці можуть використовувати штучний інтелект, щоб обійти систему розпізнавання обличь та отримати доступ до захищених об'єктів.

Атаки на системи глибокого навчання: Системи глибокого навчання на основі штучного інтелекту використовуються в багатьох сферах, включаючи медицину, автомобільну промисловість та банківський сектор. Проте, злочинці можуть використовувати штучний інтелект, щоб зламати систему глибокого навчання та впливати на результати.

Атаки на системи автономних транспортних засобів: Застосування штучного інтелекту в автономних транспортних засобах може призвести до нових видів кіберзлочинів. Наприклад, злочинці можуть використовувати штучний інтелект, щоб зламати систему управління автономним транспортним засобом та вплинути на його рух.

Атаки на системи шифрування: Штучний інтелект може використовуватись для зламування систем шифрування. Злочинці можуть використовувати штучний інтелект, щоб знайти вразливості в системах шифрування та отримати доступ до захищених даних.

Фішинг-атаки на основі штучного інтелекту: Фішинг-атаки - це спроби здійснити шахрайство, використовуючи соціальну інженерію для отримання конфіденційної інформації. Штучний інтелект може бути використаний для створення більш переконливих та складніших фішинг-атак, які можуть бути складніше виявити та запобігти.

Атаки на системи управління енергопостачанням: Штучний інтелект може бути використаний для зламу систем управління енергопостачанням, що може призвести до відключення енергопостачання в окремих районах або країнах, а також до кібертерористичних атак на критичну інфраструктуру.

Також варто розглядати можливість використання самого штучного інтелекту для забезпечення кібербезпеки, наприклад, для виявлення загроз та захисту від атак.

Висновки

Загалом, розвиток технологій повинен супроводжуватися вдосконаленням заходів кібербезпеки, щоб мінімізувати ризики та забезпечити безпеку користувачів та компаній.

Також варто розглядати можливість використання самого штучного інтелекту для забезпечення кібербезпеки, наприклад, для виявлення загроз та захисту від атак.

Використані джерела інформації:

1. Blockchain Facts: What It Is How It Works, and How It Can Be Used. URL: https://www.investopedia.com/terms/b/blockchain.asp#toc-what-is-a-blockchain

2. Blockchain security: What keeps your transaction data safe? URL: https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/

3. Blockchain Security Mechanisms. URL: https://towardsdatascience.com/mechanisms-securing-blockchain-data-9e762513ae28

4. Yadav, S.P. (2022). Blockchain Security. In: Baalamurugan, K., Kumar, S.R., Kumar, A., Kumar, V., Padmanaban, S. (eds) Blockchain Security in Cloud Computing. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-70501-5_1.

УДК 004.056.56:342(043.2)

БЕЗПАРОЛЬНА АВТЕНТИФІКАЦІЯ

Олександр Веклич

Національний авіаційний університет, Київ

Науковий керівник – Валерій Козловський, д.т.н., проф.

Ключові слова: інформація, автентифікація, злочин, Інтернет, безпека.

Вступ

Паролі – є головною ціллю злочинців. Прості методи автентифікації, які вимагають лише комбінації імені користувача та пароля, за своєю суттю вразливі. З використанням слабких паролів пов’язано 81% зломів. Саме тому все більшого поширення набирає безпарольна автентифікація - Passwordless authentication.

Матеріали і методи

Автентифікація без пароля — це засіб перевірки особи користувача без використання пароля. Натомість без пароля використовуються більш безпечні альтернативи, такі як [1]:

- *Біометрія*: фізичні ознаки, як-от сканування відбитків пальців або сітківки ока, і особливості поведінки, як-от набір тексту та динаміка сенсорного екрана, використовуються для унікальної ідентифікації людини. Незважаючи на те, що сучасний штучний інтелект дозволяє хакерам підробити певні фізичні риси, поведінкові характеристики все ще надзвичайно важко підробити.
- *Фактори володіння*: автентифікація через те, що користувач має або носить із собою. Наприклад, код, згенерований програмою автентифікації смартфона, одноразові паролі, отримані через SMS, або апаратний маркер.
- *Чарівні посилання*: користувач вводить свою електронну адресу, і система надсилає йому електронний лист. Електронний лист містить посилання, натискання на яке надає доступ користувачеві.

Результати

Безпарольна автентифікація посилює безпеку, усуваючи ризиковані практики керування паролями та зменшуючи вектори атак. Це також покращує взаємодію з користувачем, усуваючи втому від паролів і секретів.

Автентифікація без пароля працює шляхом заміни паролів іншими факторами автентифікації, які за своєю суттю є безпечнішими. При автентифікації на основі пароля наданий користувачем пароль зіставляється з тим, що зберігається в базі даних [2].

У деяких безпарольних системах (наприклад, біометрії) порівняння відбувається подібним чином, але замість паролів порівнюються відмінні характеристики користувача.

Наприклад, система фіксує обличчя користувача, витягує з нього числові дані, а потім порівнює їх із перевіреними даними, наявними в базі даних.

В інших реалізаціях систем без пароля порівняння можуть відбуватися інакше. Наприклад, система надсилає одноразовий пароль на мобільний телефон користувача за допомогою SMS. Користувач отримує його та вводить у вікно входу. Потім система порівнює введений користувачем пароль із тим, який він надіслав.

Автентифікація без пароля базується на тих же принципах, що й цифрові сертифікати: пара криптографічних ключів із закритим і відкритим ключами. Хоча вони обидва називаються ключами, розглядайте відкритий ключ як навісний замок, а закритий ключ — як фактичний ключ, який його розблоковує. Цифрові сертифікати працюють таким чином, що існує лише один ключ для замка та лише один замок для ключа. Користувач, який бажає створити захищений обліковий запис, використовує інструмент (мобільний додаток, розширення браузера), щоб створити пару відкритий-приватний ключ.

Закритий ключ зберігається на локальному пристрої користувача, і доступ до нього можливий лише за допомогою фактору автентифікації, наприклад, відбитка пальця, PIN-коду або одноразового пароля. Відкритий ключ надається системі, у якій користувач хоче мати безпечний обліковий запис.

Чи є автентифікація без пароля безпечною, залежить від визначення безпеки. Якщо безпечний означає «той, що важче зламати та менш схильний до найпоширеніших кібератак», тоді так, автентифікація без пароля безпечна.

Якщо під безпечним мати на увазі, що він непроникний для злому, то ні, це небезпечно. Немає жодної системи автентифікації, яку не можна було б зламати. Можливо, немає очевидного способу зламати його, але це не означає, що найдосвідченіші хакери не можуть обійти його захист.

Зважаючи на це, безпарольні методи за своєю суттю безпечніші, ніж паролі. Наприклад, щоб зламати систему, засновану на паролях, зловмисник може використати словникову атаку, яка часто вважається найбільш елементарною технікою злому (продовжуйте пробувати різні паролі, доки не знайдете збіг).

Навіть хакери-любителі можуть здійснити атаку за словником. І навпаки, щоб проникнути в систему без пароля, потрібен значно вищий рівень хакерського досвіду та витонченості.

Автентифікація без пароля просто замінює паролі на більш відповідний фактор автентифікації. З іншого боку, MFA (multi-factor authentication – багатофакторна автентифікація) використовує більше одного фактора автентифікації для перевірки особи користувача.

Наприклад, система MFA може використовувати сканування відбитків пальців як основний фактор автентифікації, а одноразові паролі SMS як вторинний.

Висновки

Люди іноді плутають безпарольний режим із MFA або використовують обидва як взаємозамінні. Це тому, що багато традиційних систем входу на основі пароля почали використовувати безпарольну техніку як вторинний фактор автентифікації.

Список використаних джерел

3. Технології захисту інформації [Електронний ресурс]. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186

4. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник / О. А. Самойленко. Одеса : , 2020. 112 с.

УДК 629.7.014-519(043.2)

ВИКОРИСТАННЯ АНАЛІЗУ ДАНИХ ДЛЯ ОПТИМІЗАЦІЇ РОБОТИ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ТА ПІДВИЩЕННЯ ЇХ ПРОДУКТИВНОСТІ

Сергій Вишневський

Національний авіаційній університет, Київ

Науковий керівник – Радішевський М. Ф., к.т.н., доцент

Ключові слова: аналіз даних, безпілотний літальний апарат, машинне навчання

Вступ

Безпілотна авіація все більше охоплює різноманітні сфери та галузі нашого життя, починаючи від моніторингу врожаїв на полях до розвідувально-ударних операцій на полі бою. Їх використання надає великі об’єми даних, які потрібно ефективно та оперативно аналізувати, для досягнення максимальних результатів. Аналіз даних може бути використаний не тільки для обробки вже відзнятих даних, а і, наприклад, для оптимізації роботи безпілотних літальних апаратів безпосередньо під час польоту, що в свою чергу збільшує коефіцієнт ефективності одиниці та підвищує її продуктивність.

Матеріали і методи

Аналіз даних може допомогти підвищити продуктивність безпілотного літального апарату, виявивши недоліки у роботі безпілотного апарату, для прикладу, оптимізувавши маршрут з урахування зовнішніх та внутрішніх факторів, таких як погодні умови, локація польоту, геологія місцевості, технічні характеристики апарату тощо. Це дає змогу зменшити втрати часу та енергії, збільшити час польоту, оптимізувати маршрут та покращити якість відзнятої інформації, яку в подальшому можна використати для машинного навчання програмного забезпечення, яке може автоматизовано аналізувати дані. Прорахування та точний аналіз зовнішніх факторів допоможе знизити ризики втрати безпілотного апарату та в цілому підвищить безпеку польотів, що продовжить життя комплексу.

Результати

Використовуючи машинне навчання, можна вийти на новий рівень використання безпілотних апаратів. Навчивши апарат автоматично розпізнавати техніку, їх класифікацію та стан під час польоту, прямопропорційно зменшує час обробки даних, їх передачі та відпрацювання по цілі. Такий метод прискорює роботу, зменшує навантаження пілота та кількість людей в екіпажі, адже сам аналіз та виявлення цілі проводить штучний інтелект і повідомляє ці дані на екран. Цей метод також можна використати в цивільних операціях, таких як рятувальні чи пошукові, оперативність та ефективність таких завдань зросла з впровадженням безпілотної авіації. Тепер вона виходить на новий рівень завдяки аналізу

даних та автоматизації цього процесу, використовуючи машинне навчання, що допоможе врятувати багато життів.

Аналіз даних допомагає в підвищенні ефективності та точності роботи безпілотних літальних апаратів. Перші методи аналізу використовували звичайний перегляд відео та фото, що займало багато часу, людських ресурсів та збільшувало вплив людського фактору, адже не завжди все можна помітити чи відслідкувати. Тому з часом запроваджуються нове програмне забезпечення, яке навчається на вже відзнятому матеріалі та отримує ті ж самі навички, але за більш короткий термін з більшою ефективністю виконання завдання. Одночасно машинне навчання є викликом в обробці та аналізі великих об’ємів даних, що теж потребує уваги та часу.

Окрім обробки відзнятих даних або аналізу обстановки в реальному часі, аналіз даних відкриває можливості в аналітиці та прогнозуванні поведінки літального апарату, уникненні аварійних ситуацій та підвищенні безпеки. Аналітика по виявленню проблем та недоліків може забезпечити не тільки безпеку та ефективність апарату, а і надати інформацію по можливим оновленням та покращенням БЛА. В свою чергу це призводить до нових ускладнень, але в перспективі – повна автоматизація процесу аналізу та оброки даних, яка надає структурований масив інформації, аналіз відзнятого матеріалу, прокладанню оптимального маршруту, заміри та аналіз даних по польоту апарату, аналітика та багато інших функцій.

Висновки

В сучасному світі безпілотні літальні апарати відіграють одну з найважливіших ролей, адже не тільки підвищують ефективність роботи, а і допомагають рятувати більше життів, що є найважливішим фактором. Одну з провідних ролей для БЛА займає аналіз даних, машинне навчання та спеціалізоване програмне забезпечення, яке дозволяє аналізувати великі об’єми відзнятих даних, точно прогнозувати та надавати аналітику по самому апарату, його маршруту та майбутнім діям. Даний сектор є провідним та стратегічно важливим не тільки для безпілотної авіації, а і для науки в цілому.

Список використаних джерел

1. Технології захисту інформації [Електронний ресурс]. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186

2. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник / О. А. Самойленко. Одеса : , 2020. 112 с.

УДК 004.056.5-048.66(043.2)

ПРОБЛЕМАТИКА НОВІТНІХ ЗАГРОЗ РЕСУРСАМ ІНФОРМАЦІЙНИХ СИСТЕМ

Євгенія Галич, Владислав Павленко

Національний авіаційній університет, Київ

Науковий керівник – Олена Дубчак, ст. викладач.

Ключові слова: інформаційні системи, захист інформації, загрози ресурсам інформаційних систем, методи протидії загрозам.

Вступ

Проблема загроз ресурсам інформаційних систем (ІС) та способів боротьби з ними є дуже актуальною на сьогоднішній день. ІС відіграють провідну роль в багатьох сферах життя сучасного суспільства. Захист ІС стає складнішим через зростаючу складність програмного забезпечення (ПЗ) та обладнання, що використовуються в системах.

Матеріали і методи

Основним завданням розкриття проблеми є проведення аналітичних досліджень сучасних загроз та ризиків для ІС. Важливо забезпечити розуміння значення щодо їх належного захисту для підтримання безпеки багатьох галузей та сфер життя, формування свідомого підходу до гарантій їхньої безпеки. Віруси та інше зловмисне ПЗ, таке як хробаки, троянські програми, є одними з найбільш відомих та задокументованих загроз для ресурсів ІС. Проте, існують зовсім інші, нові небезпечні ризики, поява яких в інформаційному просторі загострює проблеми захисту ІС.

Результати

З розвитком ІС розпочалось створення перших квантових комп’ютерів (КК) з новим принципом роботи, використовуючи кубіти, що можуть мати значення 0, 1 або комбінацію обох значень одночасно. В результаті КК можуть вирішувати складні завдання, такі як пошук криптографічних ключів, швидше, ніж звичайні комп'ютери. [1] Однією з найсерйозніших загроз від КК є злам криптографічних систем, що використовуються для захисту даних. Більшість сучасних криптографічних протоколів, що застосовуються від нападу на важливі дані, будуть неефективними проти КК. Одним із способів боротьби з цією загрозою є розробка криптографічних алгоритмів, стійких до КК. Система McEliece була спроєктована як одностороння (OW-CPA, One-Wayness Against Chosen-Plaintext Attack) - це означає, що зловмисники не можуть швидко знайти кодове слово із зашифрованого тексту та відкритого ключа, під час випадкової генерації кодового слова. Алгоритм використовує квантові властивості для генерації ключів і шифрування даних. Це є способом захисту від КК. [2]

Децентралізація є наступним етапом розвитку ІС через зміну підходу до управління та розподілу даних в ІС і, таким чином, підвищенням рівня безпеки ІС. Повсюдне впровадження

блокчейн - технологій є основою децентралізації. Блокчейн – технологія - створення розподільних ІС, де дані зберігаються в безпечному та недоступному для зміни форматі, а також створюється структура, за допомогою якої всі учасники цієї ІС можуть взаємодіяти між собою без посередництва централізованих організацій. Управління ІС в блокчейні здійснюється за допомогою децентралізованих баз даних, протоколів і механізмів голосування, які забезпечують безпеку і цілісність мережі. Однак, як і будь-яка інша технологія, блокчейн - технологія не є повністю захищеною від загроз та вразливостей. Серед наявних ризиків основними, зокрема, є:

1) Атака 51%. Відбувається, коли зловмисники контролюють більшість обчислювальної потужності, а саме 51 % мережі блокчейн. Таким чином отримується повний контроль над блокчейном. Заходи для захисту від цього типу атаки включають: збільшення мережі; підвищення складності алгоритму консенсусу, який використовується для змін у блокчейні. [3]
2) Вразливості у ПЗ. Блокчейн, як і інший програмний продукт, створений людиною, може містити вразливості, що потенційно можуть бути використані зловмисниками з метою атакувати мережу. Для протидії потрібно використовувати надійне ПЗ, регулярно його оновлюючи.

Висновки

З розвитком технологій, зумовленим попитом і суспільними тенденціями, ризики кібератак та інших загроз для ІС зростає зі збільшенням кількості підключених пристроїв та обсягу інформації, що циркулює в мережі Інтернет. Тому для зниження загроз квантових комп'ютерів необхідно розробляти та впроваджувати нові криптографічні методи, які були б стійкими до квантових атак. Крім того, необхідно розвивати децентралізовані системи, такі як блокчейн, задля зменшення загроз, пов'язаних із децентралізацією ІС.

Список використаних джерел

1. Quantum Computation. How D-Wave Systems Work. URL: https://www.dwavesys.com/learn/quantum-computing/

2. Bernstein D. J. Attacking and defending the McEliece cryptosystem //International Workshop on Post-Quantum Cryptography/ D. J. Bernstein //Berlin:2008. – 31 p. URL: https://link.springer.com/chapter/10.1007/978-3-540-88403-3_3

3. Jake Frankenfield. 51% Attack: Definition, Who Is At Risk, Example, and Cost. URL: https://www.investopedia.com/terms/1/51-attack.asp.

УДК 359(0477):004.056.53:355.422(043.2)

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ ПІД ЧАС ВІЙНИ

Галущак Єлизавета Василівна

Національний авіаційній університет, Київ

Науковий керівник – Козловський Валерій Валерійович ,

доктор технічних наук, професор.

Ключові слова: кібербезпека, ЗСУ, захист інформації, інформація, доступ, кадри, захищеність.

Вступ

Кіберзагрози входять до переліку основних загроз національній безпеці усіх країн Європи, в тому числі і України. На жаль, поки що в Україні ключові питання координації кібербезпеки національного рівня залишаються невирішеними. Гостро стоїть питання з безпекою державних реєстрів та баз даних. Відсутня ефективна система підготовки кіберкадрів, навіть для приватного сектору. З державного сектору нікуди не ділася низька кваліфікація та корупція. Немає повноцінного та працюючого Закону про кібербезпеку. Більшість кіберфахівців об’єдналися у окремі групи та намагаються завдати локальних контрударів по ворогу на кібер-фронті. Але навіть якщо напад ефективний та скоординований — він не вирішує проблем власної «тилової» кібер-захищеності критичної інфраструктури України та загалом як держави.

Проблема : проблема створення кібервійськ, їх фактична відсутність, надзвичайно низька ефективність держави у сфері захищеності органів влади , низький рівень підготовки спеціалістів, питання безпеки державних реєстрів та баз даних.

Матеріали і методи

Росія розпочала кібервійну проти нашої країни. Саме тоді проросійські хакери здійснили масовану атаку на органи влади. Внаслідок атаки постраждали 22 сайти органів державної влади, але стратегічної мети – завдати критичної шкоди нашій інфраструктурі – хакерам досягти не вдалося. За цією атакою слідувала низка потужних DDoS-атак у середині лютого та кібератаки напередодні вторгнення.

Метою цих атак було як руйнування інфраструктури, так і сіяння паніки та недовіри серед населення країни. Втім, навіть під час війни російські хакери не досягли успіху. На діаграмі ми можемо спостерігати кількість виконаних кібератак на українську критичну інформаційну інфраструктуру протягом місяця війни. Було зафіксовано 198 кібератак з боку російських та білоруських хакерів на державний сектор України.

Рис.1 кібератаки на критичну інформаційну інфраструктуру протягом місяця війни

Результати

Асиметричну відсіч країні-агресору можуть дати кібервійська, які слід було створити ще на початку гібридної агресії. Головна проблема для створення кібервійськ - відсутність кадрів у кожному органі, який відповідає за цю сферу, створення кадрового резерву з числа молодих і талановитих ІТ – спеціалістів . В ЗСУ фактично не існує "кібервійськ" чи "кіберсил". Існують кілька підрозділів, які виконують різні "кіберзавдання" або навіть мають у назві слово "кібер". Але завдання ці виконують, скажімо м'яко, не досить ефективно, не досить скоординовано та і взагалі не факт, що виконують. Нині склалася така ситуація, коли переважна більшість людей, залучених до захисту держави, включаючи працівників і старших офіцерів, елементарно не усвідомлюють небезпеки і можливих наслідків протистояння, що стрімко набирає обертів у площині кіберпростору. Це питання слід вирішити шляхом побудови кіберрезерву фахівців - молодих хлопців і дівчат, які проходитимуть, у тому числі, строкову службу. Зараз в державному секторі є проблеми як з професіоналізмом, так і з фінансуванням. Я сумніваюся, що такі державні підрозділи зможуть діяти швидко, ефективно і якісно. Причини: корупція, надзвичайно низька ефективність держави у цій сфері, низький рівень підготовки спеціалістів. Найкращі фахівці – масово переходять у приватний сектор. Адже однією з причин є неготовність держави гідно платити за роботу цифрових професіоналів. Вони не повинні працювати на голому патріотизмі. Треба платити за роботу стільки, скільки вона коштує.

Висновок

Без технологічної переваги сучасні війни не виграють. Виграє той, у кого точніші розвіддані, у кого безпілотники більш захищені, у кого захищені канали передачі даних, у кого сучасніше військове устаткування. Але, якщо усі ці технології не є достатньо безпечними — вони не можуть бути ефективними у військовому сенсі. Тобто без кібербезпеки у ЗСУ все це нівелює технологічну перевагу та, відповідно, втрачає сенс. Зробити технології небезпечними та, відповідно, позбавити сенсу їх застосування ворогом — це вже завдання для кібервійськ. Кібербезпека є єдиним засобом переконатися, що використання сучасних технологій є безпечним для їхніх користувачів. Якщо користувач не впевнений у безпеці технології — користуватися не буде, а нема користувачів — це означає смерть технології. Отак і виходить, що без технологій та кібербезпеки сучасна армія не може перемагати. Нам необхідно побороти корупцію і побудувати потужне кібервійсько, з яким країна буде захищена і технологічно на високому рівні .

Список використаної літератури

1. Стаття ЗСУ «Військова кібербезпека». URL: https://www.mil.gov.ua/ukbs/
2. Стаття мультимедійної платформи іномовлення України.
3. Інтерв’ю керівниці служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталії Ткачук.

УДК 004.89

СТВОРЕННЯ NPC В КОМП'ЮТЕРНИХ ІГРАХ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

Олександр Гузо

Національний авіаційний університет, Київ

Науковий керівник – Глазок О. М. к. т. н., доц.

Ключові слова: NPC, штучний інтелект, комп’ютерні ігри, гравець, алгоритм

Вступ

Підходи та засоби штучного інтелекту (ШІ) можуть бути дуже корисними інструментами для розробників ігор. Штучний інтелект дозволяє дозволяє створювати в іграх більш реалістичний та динамічний ігровий світ, розширити можливості та покращити якість геймплею, роблячи його більш складним та цікавим для гравців. Одним із ключових елементів розробки ігор є створення неігрових персонажів, які повинні бути життєвими, реалістичними та наділені відповідними рисами характеру. («Неігровий персонаж» – усталений термін, що позначає персонажів комп’ютерної гри або відеогри, поведінка яких не контролюється гравцем-людиною.)

Методи та матеріали

Штучний інтелект може бути використаний для керування рухом персонажів, їх поведінкою та взаємодією з гравцями. Використання ШІ також дозволяє створювати більш складні ігрові ситуації та випробування для гравців, що збільшує рівень складності гри.

Застосування штучного інтелекту в створенні неігрових персонажів в іграх має безліч переваг, які роблять його незамінним інструментом для розробки сучасних ігор. Ось деякі з цих переваг:

1. Реалістичність: засоби штучного інтелекту допомагають створити персонажів, які поводяться і реагують на події, як люди. Вони можуть рухатись, взаємодіяти з ігровим світом та гравцем, і навіть розуміти складні інструкції.

2. Адаптивність: персонажі можуть змінювати свої дії залежно від ситуації, пристосовуватись в реальному часі до змін в ігровому середовищі. Вони можуть навчитись новим вмінням, які зроблять гру більш складною та цікавою, та взаємодіяти з новими предметами, які з'являються у грі. Якщо гравець починає втручатися в діяльність персонажу, той може перейти до іншої поведінки.

3. Економія робочого часу: замість створення персонажів з нуля розробники ігор можуть використовувати готові алгоритми та інструменти ШІ, що зменшує час, потрібний для розробки гри.

Результати

Розглянемо декілька популярних моделей ШІ для створення NPC в іграх.

1. Finite State Machines (FSM) – це одна з найпростіших моделей ШІ, яка забезпечує персонажа обмеженою кількістю станів та переходів між ними. Кожен стан визначає, як персонаж повинен поводитися в певних обставинах.

2. Behaviour Trees (BT) – дерева поведінки, більш складна модель ШІ, яка дозволяє створювати неігрових персонажів з більшою кількістю дій та варіантів поведінкки. Кожен вузол дерева відповідає певній дії персонажу чи шаблону його поведінки, а гілки відповідають умовам, при яких ця дія має бути виконана [1].

3. Goal Oriented Action Planning (GOAP) – це модель ШІ, яка дозволяє NPC самостійно вирішувати, які дії виконувати, щоб досягти поставленої мети. GOAP забезпечує NPC гнучкість та можливість адаптуватися до змінних умов гри.

4. Neural Networks (NN) – це модель ШІ, яка дозволяє персонажу навчатися на основі досвіду та самостійно приймати рішення. Нейромережі забезпечують персонажу можливість вирішувати складні задачі та динамічно адаптуватися до умов гри.

Розробники платформ програмування усвідомлюють актуальність застосування підходів штучного інтелекту і впроваджують технології їх підтримки [2].

Застосування методів та засобів ШІ для створення персонажів може бути дуже ресурсо- та часозатратним завданням. Навіть при використанні готових бібліотек та фреймворків для реалізації ШІ в іграх розробникам доводиться витрачати багато часу на тонке налаштування та підгонку параметрів, щоб забезпечити оптимальну продуктивність та якість дій персонажа.

Висновок

Штучний інтелект в створенні NPC в комп’ютерних іграх є ключовим елементом, що визначає рівень реалістичності та іммерсивності геймплею. NPC, або некеровані персонажі, відіграють важливу роль у створенні атмосфери гри та взаємодії з гравцем.

Список використаних джерел:

1. Yannakakis G., Togelius J. Artificial Intelligence and Games. – Springer Cham, 2018. – 337 p. DOI: 10.1007/978-3-319-63519-4.

2. Unity: A General Platform for Intelligent Agents [Preprint]. /Juliani A., Berges, V., Vckay E., Gao Yuan, Henry H., Mattar M., Lange D. – Unity Technologies, 2020. – 19 p.

УДК 004.056

ДОСЛІДЖЕННЯ РОБОТИ АНТИВІРУСУ «NORTON»

Станіслав Давидюк

Національний авіаційній університет, Київ

Науковий керівник – Валерій Козловський, д.т.н., проф.

Ключові слова: Norton, антивірус, захист

Вступ

Norton — це потужне антивірусне програмне забезпечення, яке забезпечує розширений захист від широкого спектру онлайн-загроз, включаючи віруси, зловмисне програмне забезпечення, шпигунське програмне забезпечення, програми-вимагачі та фішингові атаки. Norton використовує багаторівневий підхід до безпеки, включаючи виявлення на основі сигнатур, виявлення на основі поведінки та алгоритми машинного навчання, які аналізують мільйони файлів, щоб ідентифікувати та блокувати нові та нові загрози.

Матеріали і методи

Захист Norton у режимі реального часу розроблений для тихої роботи у фоновому режимі, відстежуючи весь вхідний і вихідний трафік, щоб виявити та заблокувати зловмисну активність, перш ніж вона може завдати шкоди пристрою користувача. Norton також має потужний брандмауер, який блокує несанкціонований доступ до мережі користувача, а також ряд інших функцій, таких як захист від спаму, фішингу та шпигунського програмного забезпечення.

Захист кількох пристроїв Norton є однією з його видатних функцій, що дозволяє користувачам захищати всі свої пристрої, включаючи Windows, Mac, Android та iOS, за допомогою однієї підписки. Norton також пропонує хмарне резервне копіювання та зберігання, що дозволяє користувачам безпечно зберігати та отримувати доступ до своїх файлів і документів з будь-якого місця, а також відновлювати їх у разі збою пристрою або втрати даних.

Norton має зручний інтерфейс, який полегшує навігацію та налаштування параметрів відповідно до вподобань користувача. Інтерфейс Norton інтуїтивно зрозумілий і зручний, усі основні функції та налаштування доступні з однієї інформаційної панелі. У Norton також є ряд параметрів налаштування, що дозволяє користувачам регулювати рівень захисту та налаштовувати програмне забезпечення для запуску сканування та оновлення в певний час.

Часті оновлення та виправлення Norton мають вирішальне значення для підтримки актуальності програмного забезпечення та захисту від останніх загроз. Оновлення Norton є автоматичними та працюють у фоновому режимі, гарантуючи, що програмне забезпечення

завжди оновлене та захищене від останніх вразливостей і експлойтів. Norton також має ряд інших функцій, які допомагають користувачам залишатися в безпеці в Інтернеті, наприклад менеджер паролів, який дозволяє користувачам безпечно зберігати свої паролі та керувати ними, і VPN, який шифрує інтернет-трафік користувача та захищає його конфіденційність в Інтернеті.

Служба підтримки клієнтів Norton чудова, завдяки повній базі знань, форумам спільноти та цілодобовій підтримці по телефону та в чаті. Команда підтримки У Norton також є низка ресурсів та інструментів, які допомагають користувачам бути в курсі останніх загроз і передових методів безпеки в Інтернеті.

Результати

Norton пропонує низку тарифних планів, які відповідають різним бюджетам і потребам, включаючи річну та місячну підписку, а також багаторічні плани для більшої економії. Ціни Norton конкурентоспроможні та пропонують хороше співвідношення ціни та якості, враховуючи набір функцій і рівень захисту, які забезпечує програмне забезпечення. Norton також пропонує 60-денну гарантію повернення грошей, що дозволяє користувачам випробувати програмне забезпечення без ризику та отримати повне відшкодування, якщо вони не задоволені продуктом.

Висновок

Підсумовуючи, зазначу, що антивірус Norton — це потужне та комплексне програмне забезпечення безпеки, яке пропонує розширений захист від широкого спектру онлайн-загроз.

Його багаторівневий підхід до безпеки, захист у режимі реального часу та розширені функції, такі як захист кількох пристроїв, резервне копіювання в хмарі та підтримка клієнтів, роблять його чудовим вибором для користувачів, яким потрібна надійна та надійна онлайн-безпека.

Список використаних джерел:

1. https://en.wikipedia.org/wiki/Norton_AntiVirus
2. https://us.norton.com/
3. https://cybernews.com/best-antivirus-software/norton-antivirus-review/

УДК 004.056.53(043.2)

ЗАХИСТ МЕРЕЖЕВИХ СЕРВІСІВ ВІД DDoS-АТАК З ДОПОМОГОЮ НЕЙРОМЕРЕЖЕВИХ ТЕХНОЛОГІЙ

Тетяна Драч

Національний авіаційній університет, Київ

Науковий керівник – Валерій Козловський, д.т.н., проф.

Ключові слова: DDoS-атака, кібервійна, нейронні мережі, трафік.

Вступ

Сьогодні для проведення війни агресори обирають не лише певні території, а й цифровий простір, де розпочинають кібервійну. Ще у перші години повномаштабного вторгнення росії Україна та її кібервійсько зіткнулися із блокуванням урядових сайтів, сайтів державних структур, банків, ЗМІ та ін., що продовжується і нині. Це власне і є DDoS-атаки – простіше кажучи, створення великої кількості запитів, який система атакованого ресурсу нездатна обробити. Паралельно із цим у світі розвиваються нейронні мережі – це один із напрямків штучного інтелекту, мета якого змоделювати аналітичні механізми, що здійснюються людським мозком [1]. Нейромережі здатні самостійно навчатися і розвиватися, будуючи свій досвід на помилках.

Матеріали і методи

Основою даної ідеї - використання нейронної мережі для виявлення аномального трафіку. Аномальний трафік і сигналізує про DDoS-атаку. Після вивчення великої кількості даних нейронна мережа може встановити зв'язки між параметрами трафіку, такими як тип пакету, його довжина, швидкість передачі даних, інше. Після цього у разі виявлення нейронною мережею атипового трафіку, можна вжити заходів для зниження його впливу на систему. Наприклад, системи маршрутизації трафіку можна використовувати для перенаправлення атакуючого трафіку на певні сервери, які можуть більш ретельно перевіряти трафік і відфільтровувати зловмисний [4].

1. Аналіз наукових джерел та літератури з питань захисту від DDoS-атак та застосування нейронних мереж.
2. Аналіз результатів тестування та порівняння ефективності розробленої системи з іншими методами захисту від DDoS-атак.

Результати

Отже, в результаті дослідження було показано, що застосування нейронних мереж для захисту від DDoS-атак може бути ефективним підходом [4]. Розроблена система дозволяє виявляти та блокувати DDoS-атаки, зменшуючи їхній вплив на комп'ютерну мережу.

Враховуючи зростання кількості DDoS-атак у сучасному Інтернеті, застосування нейронних мереж може бути цінним інструментом для захисту від цих атак.

Хоча використання нейронних мереж для захисту від DDoS-атак є перспективним напрямком, цей спосіб не є абсолютним рішенням проблеми. Зловмисники можуть «обманути» нейронні мережі. Наприклад, створити атаку, що імітуватиме нормальний трафік. Отже, для досягнення найкращих результатів, потрібно використовувати нейронні мережі у комбінації з іншими методами захисту. Прикладом можуть бути: попереднє виявлення інцидентів, фільтрація трафіку, інше [5].

Висновок

Отже, застосування нейронних мереж для захисту від DDoS-атак може бути ефективним та має потенційну цінність для подальшого розвитку та вдосконалення систем захисту від DDoS-атак.

Список використаних джерел:

1. Що таке нейронні мережі. URL: https://livingfo.com/shcho-take-nejronni-merezhi-ta-iak-vony-pratsiuiut/

2. Роз’яснення Держвної служби спеціального зв’язку та захисту інформації України що таке DDoS-атака. URL: https://cip.gov.ua/ua/faqs/sho-take-ddos-ataka.

3. Засоби захисту від DDoS-атак. URL: https://iitd.com.ua/zashchita-ot-ddos-atak/

4. Mihoub A. et al. Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques //Computers & Electrical Engineering. – 2022. – Т. 98. – С. 107716.

5. Vishwakarma R., Jain A. K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network //Telecommunication systems. – 2020. – Т. 73. – №. 1. – С. 3-25.

УДК 070.16:355.271(043.2)

ПОШИРЕННЯ ДЕЗІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

Катерина Дячук

Національний авіаційній університет, Київ

Науковий керівник – Валерій Козловський, д.т.н., проф.

Ключові слова: дезінформація, інформаційний фронт, маніпулятивний вплив.

Вступ

Сучасність приносить свої зміни не лише у технології, науку чи мистецтво, а й в умови проведення війни, додаючи людям не лише нові можливості для допомоги, а й новий не менш важливий фронт – інформаційний. З сучасними технологіями ми практично є необмеженими у виборі джерела інформації, що і робить пересічного користувача вразливим до впливу замаскованої дезінформації від ворога.

Матеріали та методи.

Об’єктом дослідження є дезінформація, оскільки її поширення зараз набуло більшого рівня небезпеки ніж раніше. При дослідженні використовувались аналітичний та статистичний методи дослідження.

Зрозуміти що таке дезінформація не важко, адже дезінформація – це спотворена чи навіть вигадана інформація. Поки що це визначення не надто відрізняється від звичайної помилкової інформації, але ці два визначення мають значну відмінність – мету. Помилкова інформація розповсюджується ненавмисно, її власник не мав за мету заподіяти комусь шкоди. Використання ж дезінформації має мету дестабілізувати населення, дискредитувати владу у його очах та заподіяти іншу шкоду людині та суспільству загалом.

Результати

В умовах війни поширення дезінформації набуває нового рівня небезпеки, адже зараз довіра до помилкового джерела може коштувати нам волі, або й життя. Як і до повномасштабної війни, дезінформація поширюється проти влади країн, які є неугодними для джерела дезінформації, проте варто зауважити, що зараз потік дезінформації значно збільшився, про це може свідчити графік рис. 1 [1] та додались нові вигадки, щоб якось виправдати свої злочинні дії. У змісті такої дезінформації використовують демонстрування медіа із знущаннями над простими громадянами, демонстрування буцімто низького рівня життя, одночасно показуючи яке «чудове» життя чекає на громадян, що оберуть для себе майбутнє у країні-окупант та інші речі, які потенційно можуть довести свою «правоту» чи просто звабити на проживання у країні з їхньою владою. Як наслідок, ми бачимо

маніпулятивний вплив з боку ворожої влади на власний народ та на інших людей зі всього світу, що й додає їм сил вже не на інформаційному фронті, а на фізичному.

Рис. 1 – графік виявлених повідомлень із дезінформацією за 2019, 2020, 2021 та 2022 роки [1]

Основними джерелами дезінформації є телебачення, соціальні мережі, месенджери з можливістю створення груп та газетні чи інтернет-видання, ці платформи є всього лише ресурсом для розповсюдження. Зазвичай дезінформація, що поширюється, спонсорується владою та є однотипною. Дезінформація має характерні ознаки [2]. По-перше, сенсаційна «новина» та надемоційність тексту, наприклад «У штабі військових знайшли ознаки використання чорної магії». По-друге, посилання на неіснуючі джерела інформації, наприклад «Британські вчені встановили, що…». По-третє, дезінформація має примітивний зміст, через що користується більшим попитом серед споживачів. Та по-четверте, дезінформація зазвичай не має продовження, її метою є створити маніпулятивний вплив на думку суспільства на сьогоднішній день, а завтра вигадується «новина» з такою ж метою.

На сьогоднішній день в Україні немає юридичного визначення дезінформація [3], є лише зазначення у законах «Про інформацію», Про друковані засоби масової інформації (пресу) в Україні» і «Про телебачення та радіомовлення», що інформація має бути повною та достовірною. Рішенням Ради національної безпеки і оборони України було створено Центр протидії дезінформації, основна увага якого зосереджена на протидію поширення дезінформації у інтернеті та медіапросторі.

Висновок.

Під час проведення будь-якої війни не менш важливим фактором є інформаційний фронт, адже він забезпечує населення важливою інформацією та може впливати на основну думку людей про ту чи іншу подію. Тому вкрай важливо захистити людей від споживання дезінформації.

Список використаних джерел:

1. https://zmina.info/articles/rik-povnomasshtabnoyi-brehni-shho-peredrikaye-rosijska-dezinformacziya/
2. https://oduvs.edu.ua/news/інформаційна-гігієна-як-засіб-протид/
3. https://cedem.org.ua/analytics/epidemiya-dezinformatsiyi/

УДК 004.056.53(043.2)

КІБЕРБЕЗПЕКА ІНТЕЛЕКТУАЛЬНИХ МІКРОМЕРЕЖ

Тетяна Іващенко, Аліна Іващенко

Національний авіаційний університет, Київ

Науковий керівник - Олександр Туровський, д.т.н., професор

Ключові слова: кібербезпека, інтелектуальні мікромережі, кібератаки.

Вступ

В останні роки розвиток розумних мереж стрімко зростає. Інтелектуальні мережі - це взаємопов'язані кластери мікромереж змінного і постійного струму, в яких інтелектуальні силові електронні перетворювачі широко використовуються для взаємодії між розподіленою генерацією (РГ) і накопичувачами енергії, а також навантаженнями. У таких мікромережах інформаційно-комунікаційні технології відіграють вирішальну роль в їх експлуатації та управлінні. Будь-яка затримка або пошкодження даних може вплинути на безперебійну роботу фізичної системи і поставити під загрозу ефективність, стабільність і безпеку інтелектуальних мереж [1,2].

Матеріали та методи

Щоб вивчити структуру кібератак у інтелектуальних мікромережах, які інтенсивно використовують силову електроніку, спочатку розглядається система керування такими мікромережами. В інтелектуальних мікромережах зазвичай використовується багатошарова структура управління, в якій зовнішній і внутрішній шари називаються наглядовим і первинним рівнями управління відповідно [3].

Результати

Кіберсистема в розумних мікромережах збирає, передає та обробляє дані для контролю фізичної роботи системи. Потік даних кіберсистеми має бути ефективним, надійним і своєчасним, щоб керувати роботою фізичного процесу. У свою чергу кібератаки порушують функціонування мікромереж. Можливо визначити наступні кібератаки на потік даних інтелектуальної мікромережі:

1. Атаки на доступність даних (кіберсистема повинна гарантувати, що дані є своєчасними та доступними, що має вирішальне значення для керування перетворювачами силової електроніки в інтелектуальних мікромережах, особливо в острівному режимі та перехідних процесах). Атаки, основною метою яких є блокування або затримка передачі даних, називаються атаками на доступність даних. Відмова в обслуговуванні (DoS) і розподілена відмова в обслуговуванні (DDoS) є прикладами атак на доступність даних.

2. Атаки на цілісність даних (будь-яка атака, що надходить у кіберсистему, і порушує цілісність даних, змінює інформацію). Ці атаки можуть бути здійснені шляхом пошкодження вимірювань або командних сигналів у мережі зв’язку та можуть призвести до збоїв у роботі мікромережі та вплинути на її керування, включаючи регулювання частоти та напруги, управління живленням та енергією, виявлення острівців та повторну синхронізацію. Типовим прикладом атак, що порушують цілісність даних, є кібератаки FDI (False Data Injection, FDI) [4, 5].

3. Атаки на конфіденційність даних (кібератаки, що порушують конфіденційність, дозволяють хакерам шпигувати за комунікаційною мережею, щоб отримати інформацію про клієнтів, а також роботу мікромережі та стратегії контролю). Хоча, ці атаки можуть не мати сильного впливу на роботу мікромереж, виявлену інформацію можуть використати хакери для ефективних атак на доступність і цілісність даних.

Традиційні енергосистеми еволюціонують в інтелектуальні мережі, які об'єднують взаємопов'язані мікромережі.

Слід підкреслити, що мікромережі більш схильні до проблем зі стабільністю в разі кібератаки через свою низьку інерційність. Через тісний зв'язок підсистем змінного та постійного струму в гібридних мікромережах змінного/постійного струму будь-який кіберінцидент в одній підсистемі може мати руйнівний вплив на іншу сторону.

Висновки

Розумні мікромережі відіграватимуть важливу роль у наступному поколінні енергосистеми.

Гібридні мікромережі змінного/постійного струму вважаються найбільш вірогідною структурою майбутньої мікромережі, в якій високе проникнення силових електронних перетворювачів забезпечує взаємодію між розподіленою генерацією, накопичувачами енергії та навантаженнями, а також взаємозв'язок між підмережами змінного та постійного струму.

Інтелектуальні гібридні мікромережі змінного/постійного струму потребують надійної та безпечної кіберсистеми та мережі зв'язку для оптимальної, безперебійної та плавної роботи, а будь-які кібератаки можуть призвести до непередбачуваних інцидентів у роботі цих мереж.

Список використаних джерел:

1. Li, Z.; Shahidehpour, M.; Aminifar, F. Cybersecurity in Distributed Power Systems. *Proc. IEEE* **2017**, *105*, 1367–1388. [**Google Scholar**] [**CrossRef**].

2. Singh, S.K.; Khanna, K.; Bose, R.; Panigrahi, B.K.; Joshi, A. Joint-Transformation-Based Detection of False Data Injection Attacks in Smart Grid. *IEEE Trans. Ind. Inf.* **2018**, *14*, 89–97. [**Google Scholar**] [**CrossRef**].

3. Nejabatkhah, F.; Li, Y.W.; Tian, H. Power Quality Control of Smart Hybrid AC/DC Microgrids: An Overview. *IEEE Access* **2019**, *7*, 52295–52318. [**Google Scholar**] [**CrossRef**].

4. Deng, R.; Xiao, G.; Lu, R.; Liang, H.; Vasilakos, A.V. False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey. *IEEE Trans. Ind. Inf.* **2017**, *13*, 411–423. [**Google Scholar**] [**CrossRef**].

5. Liu, Y.; Reiter, M.K.; Ning, P. False data injection attacks against state estimation in electric power grids. In Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009; pp. 21–32. [**Google Scholar**].

УДК 004.021

МОДУЛЬ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ КОРИСТУВАЧА СОЦІАЛЬНИХ МЕРЕЖ

Поліна Котирло

Національний авіаційній університет, Київ

Науковий керівник – Дубчак Олена, старший викладач

Ключові слова: інформаційна безпека, соціальні мережі, метод найближчого сусіда, алгоритм машинного навчання

Вступ

Зворотною стороною використання новітніх систем збереження, обробки та поширення інформації є загострення проблем інформаційної безпеки. Розвиток сучасних інформаційно-комунікаційних технологій розширив можливості агресивного психологічного впливу на особистість у віртуальному світі.

Метою роботи є дослідження методу найближчого сусіда (МНС) як алгоритму машинного навчання задля підвищення рівня безпеки користувачів соціальних мереж.

Матеріали і методи

Алгоритм МНС, який є одним з багатьох алгоритмів машинного навчання, заснований на порівнянні елементів множини та їх класифікації на основі порівняння подібності різних об’єктів: починаючи від початкової точки перевіряється кожний найближчий об’єкт, поступово перебираючи їх усіх.

МНС широко використовується для обрання найоптимальнішого варіанту вирішення завдання: в медицині - для обрання найоптимальнішого діагнозу; в плануваннях будівництва - для вибору найоптимальнішого місця розміщення будівлі громадського використання тощо.

Як відомо [1], геометричне рішення методу найближчого сусіда запропонував український вчений Георгій Вороний, побудувавши діаграму з виділеною областю близькості.

Для вибору кількості найближчих сусідів пропонується використовувати значення k, На цьому кроці варто зважати, щоб не обрати занадто велику або малу кількість об’єктів.

Якщо прийняти k = 1, то алгоритм втратить узагальнюючу здатність - видавати правильний результат для даних, що не зустрічалися раніше в алгоритмі, оскільки новому запису буде присвоєний клас, близький до нього [2]. Якщо обрати k парним числом, то при прийнятті рішення з’являється можливість «нічиєї», що уповільнює та зменшує ефективність алгоритму.

Наступний крок - вибірка найближчих до визначеної початкової точки об’єктів та їх впорядкування, після чого для впорядкованих значень атрибутів обчислюється Евклідова

відстань. Коли впорядковані класи знайдено, необхідно визначити, як вони впливають на класи для їх оптимального розподілення, задля чого можна використати функцію поєднання.

Далі відбувається зважене голосування для визначення та розподілення класів. Зважене голосування означає, що найближчий до визначеного об’єкта атрибут матиме найбільшу вагу.

Результати

Таким чином, за допомогою алгоритму МНС достатньо просто можна класифікувати набори даних, маючи мінімальну кількість інформації про них. Він нескладно піддається інтерпретації, а можливість модифікування алгоритму дозволяє широко застосовувати його для вирішення прикладних задач [3].

За результатами проведених досліджень, МНС обрано для вирішення завдання виявлення потенційно небезпечних користувачів в соціальних мережах та використано у створеному програмному модулі. Для випробування точності МНС було проведено експеримент - фільтрування проросійських коментарів у соціальній мережі Facebook.

Визначено, що запропоноване рішення дозволяє виявити близько 73% коментарів, які містять ворожі риторики. Це значення можна збільшити за рахунок швидкості прийняття рішення, проте отриманий варіант рішення прийнято як оптимальний.

Висновок

Перевага використання алгоритму МНС полягає в простоті його реалізації з відносно точними результатами щодо класифікації потрібних даних. Ефективність алгоритму за результатами проведеного експерименту вкладає 73%.

Список використаних джерел:

1. Метод k найближчих сусідів. URL: http://om.univ.kiev.ua/users_upload/15/upload/file.pdf (Last accessed: 23.03.2023).

2. Актуальні проблеми Data Mining URL: http://csc.knu.ua/media/filer_public/38/03/3803002b-e068-4a08-8a6c-a4edc183892a/datamining20170917.pdf (Last accessed: 23.03.2023).

3. Дослідження ймовірності помилки при класифікації методом найближчого сусіда. URL: https://matan.kpi.ua/public/files/2017/dis/Chubyk.pdf (Last accessed: 23.03.2023).

УДК 351.746.1:004.8(043.2)

НАЦІОНАЛЬНА БЕЗПЕКА В УМОВАХ РОЗВИТКУ ІНДУСТРІЇ ШТУЧНОГО ІНТЕЛЕКТУ

Рут Кузьмінська

Національний авіаційній університет, Київ

Науковий керівник – *Ігор Дерев'янко, к.і.н., доц.*

Ключові слова: національна безпека, інформаційна безпека, штучний інтелект, кіберзагрози, кібератаки.

Вступ

Стрімкий розвиток індустрії штучного інтелекту має великий потенціал для зміни багатьох аспектів життя людей і впливу на суспільство в цілому. Застосування штучного інтелекту в різних галузях, таких як: медицина, транспорт, фінанси, енергетика та інші, може зробити їх більш безпечними та ефективними. Однак, також потрібно враховувати можливі наслідки незаконного використання цієї технології.

Матеріали і методи

Для отримання даних про поточний стан розвитку індустрії штучного інтелекту були проаналізовані наукові статті, звіти, статистичні дані, законодавчі акти та інші джерела. Для аналізу впливу розвитку штучного інтелекту на національну безпеку було проведено:

- соціологічні дослідження і експертний аналіз щодо застосування штучного інтелекту в різних галузях;

- моделювання ризиків які можуть виникнути при застосуванні штучного інтелекту в різних галузях.

Результати

Штучний інтелект (далі ШІ) - технологія яка здатна відтворювати дії подібні людським. На даний момент відомо що ШІ має потенціал до вирішення найактуальніших проблем, з якими сьогодні стикається світ, такими як зміна клімату, охорона здоров’я та транспорт. Проте швидкий розвиток ШІ створює значні виклики та ризики для національної безпеки, оскільки країни та корпорації поспішають розробляти та використовувати його.

Національна безпека є одним з найголовніших чинників забезпечення умов реалізації національних інтересів. Застосування штучного інтелекту може спричинити виток даних та привести до порушення конфіденційності. Крім того, невірна робота систем ШІ може привести до виникнення аварій та катастроф, які можуть стати загрозою для національної безпеки. У разі використання технології військовими структурами, його неконтрольоване використання може призвести до ситуації, коли збройний конфлікт стане безкінечним. Крім

того, існує ризик, що деякі країни та корпорації зможуть скористатися перевагами штучного інтелекту для здійснення кібератак та шпигунської діяльності, що становить значні загрози для національної безпеки.

Ескалація кіберзагроз національним інтересам вимагає ефективних заходів для захисту національних інформаційних ресурсів і забезпечення цілісності та безпеки інформації. Одним з найбільш ефективних способів захисту національної безпеки є використання інтелектуальних систем виявлення загроз, що дозволяє автоматично виявляти підозрілу активність в мережі та запобігати атакам. Крім того, можуть бути застосовані технології шифрування та аутентифікації, що забезпечують захист від несанкціонованого доступу до даних та систем. Важливим є також постійний моніторинг та аналіз мережевої активності для виявлення нових загроз та вчасної реакції на них.

Застосування ШІ державними органами інформаційної сфери допомагає виявляти загрози для національної безпеки та боротися з ними. Людині важко конкурувати з ШІ в управлінні складними системами, які вимагають миттєвого прийняття рішень. Аналізуючи великі маштаби інформації, поведіку користувачів та мережевий трафік, технології швидко виявляють кіберзагрози. Системи з використанням штучного інтелекту можуть ефективно реагувати на кібератаки автоматично розробляючи стратегії захисту.

Висновки

Розвиток нових методів та технологій в області національної безпеки, що базуються на застосуванні ШІ, може значно покращити безпеку та ефективність систем оборони. Однак, успіх залежить від того, наскільки добре будуть збалансовані інновації та безпека. Тому необхідно знайти оптимальну стратегію розвитку індустрії штучного інтелекту, що враховує інтереси національної безпеки та етичні принципи використання новітніх технологій.

Список використаних джерел:

1. How Artificial Intelligence Is Transforming National Security. [Electronic recourse]. URL: https://www.gao.gov/blog/how-artificial-intelligence-transforming-national-security

2. Artificial Intelligence and National Security. [Electronic recourse]. URL: https://webcache.googleusercontent.com/search?q=cache:rPUR7H3ib9cJ:https://sgp.fas.org/crs/natsec/R45178.pdf&cd=13&hl=uk&ct=clnk&gl=ua

3. The Evolution of War: How AI has Changed Military Weaponry and Technology. [Electronic recourse]. URL: https://montrealethics.ai/the-evolution-of-war-how-ai-has-changed-military-weaponry-and-technology/

УДК 004.056.56:342(043.2)

КІБЕРБЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Іван Лічковаха, Олександр Калашник

Національний авіаційний університет, Київ

Науковий керівник – Олександр Туровський, д.т.н., проф.

Ключові слова: інформація, захист, злочин, Інтернет, безпека.

Вступ

Із початком військової агресії росії на території України наша держава отримала велику кількість кібератак, яка вплинула на державні органи, приватні компанії та громадян.

Кожна сучасна соціально активна людина в Україні зараз має смартфон, комп'ютер, користується соціальними мережами або іншими засобами доступу у віртуальному просторі (мережі Інтернет). Державні органи переходять на електронний документообіг. Стабільна діяльність банківського сектору, залізниці й авіатранспорту, великих підприємств залежить від стабільності кіберпростору, із яким вони працюють, та базується на комунікації за допомогою електронних засобів зв'язку.

Матеріали і методи

На початку XXI століття злодій – це не обов'язково холоднокровно озброєна людина. Злодієм може виявитися звичайна людина з ноутбуком у руках та доступом до інтернету. І дізнатися, хто саме ця людина, дуже важко. В умовах війни така людина стає бойовою одиницею, як солдат, який вбиває людей, тільки ціль такого бійця – кібератаки та злами.

Під час воєнного стану атаки можуть бути не тільки з боку ворога, але й серед звичайних людей, які вирішили скористатися скрутним становищем, коли правоохоронні органи перевантажені, та наживатися на довірі громадян та вкрасти їхню приватну інформацію або кошти. За рік війни темпи росту кібератак стрімко зросли.

Мета таких дій – розкрадання або руйнування інформації в інформаційних системах і мережах. В умовах війни кіберзлочини можуть здійснюватися з метою дестабілізації ситуації в країні, крадіжки необхідних (конфіденційних) даних, виведення з ладу державних інституцій, техніки, завдання іншої матеріальної шкоди.

Результати

Від початку війни стало відомо про велику кількість кібератак на Україну. Варто згадати невдалу спробу атаки хакерського угруповання Strontium, яке намагалося отримати доступ до комп'ютерних мереж в Україні, США та ЄС, щоб забезпечити тактичну підтримку фізичного вторгнення росії в Україну та викрасти конфіденційну інформацію.

Нещодавно Держспецзв'язок повідомив про отримання українськими користувачами нових небезпечних електронних листів із темою «№ 1275 від 07.04.2022», відкриття яких призводить до отримання хакерами повного контролю над персональним комп'ютером та загрожує крадіжкою та пошкодженням комп'ютерних даних.

Раніше, 4 квітня, Держспецзв'язку попереджувало про розповсюдження електронних листів із назвою «Військові злочинці РФ.htm», відкриття яких призводить до того, що зловмисники отримують віддалений доступ до комп'ютера жертви.

Під прицілом перебувають також об'єкти критичної інфраструктури. Український провайдер Укртелеком зазнав потужної атаки 28 березня 2022 року, під час якої хакери намагалися проаналізувати, як влаштована IT-інфраструктура, вивести з ладу обладнання та сервіси, а також отримати контроль над мережею та обладнанням компанії.

Проблематика руйнівних та нищівних кібератак росії перед вторгненням у нашу країну доводить, що кібератаки відіграють важливу та стратегічну роль у сучасному світі та війні, попри те, чи відомо про це громадськості. Ця загроза є постійною, і вона не стоїть на місці та розвивається. Кібератаки завдають чималих проблем нашій системі та інфраструктурі з парадоксальними наслідками.

Висновки

Безпека України суттєво залежить від поліпшення кібербезпеки. На це варто не тільки звернути увагу, а й навіть докласти максимальних зусиль. Технічний прогрес зростатиме, а за нею і ця залежність у кіберпросторі.

Вберегти себе від кібератак можливо лише дотримуватися безпеки в інтернеті, а саме перевіряти оновлення антивірусу та оновлень операційної системи. Використовувати лише ліцензійне програмне забезпечення, та налаштування двофакторної аутентифікації на електронних адресах або в програмах де така функція присутня.

Також не слід відкривати листи від незнайомих осіб, тому що в таких листах, бо такий лист може містити в собі віруси. Перевіряйте свої акаунти у соціальних мережах чи не підключені інші пристрої, зловмисники можуть місяцями й навіть роками слідкувати за жертвою.

Тільки дотримання правил «цифрової гігієни» можуть вберегти від кібератак.

Поточна ситуація залишається непередбачуваною – компаніям та організаціям важливо постійно аналізувати, як ситуація може розвиватися далі, та які сценарії можуть виникнути.

Список використаних джерел

1. C. H. Taal, R. C. Hendriks, R. Heusdens and J. Jensen. A short-time objective intelligibility measure for time-frequency weighted noisy speech. Proceedings of 2010 IEEE

International Conference on Acoustics, Speech and Signal Processing. 2010. Pp. 4214-4217. DOI: 10.1109/ICASSP.2010.5495701.

2. A. Torfi, S. M. Iranmanesh, N. Nasrabadi and J. Dawson, 3D Convolutional Neural Networks for Cross Audio-Visual Matching Recognition. IEEE Access. 2017, vol. 5, pp. 22081 – 22091. DOI: 10.1109/ACCESS.2017.2761539.

3. A. P. K. Muthukumaran, H. Vani. Optimizing the usage of voice assistants for shopping //Indian Journal of Science and Technology. – 2020, No. 13 (43). Pp. 4407 – 4416. DOI: 10.17485/IJST/v13i43.1911.

УДК 004.8:004.056

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ: ПЕРЕВАГИ ТА НЕДОЛІКИ

Світлана Лучай
Національний авіаційній університет, Київ

Науковий керівник – Олена Прокопенко

Ключові слова: штучний інтелект, кібербезпека, кіберзлочинність, кібератака.

Вступ

З появою все більшої кількості цифрових даних та збільшенням кількості кібератак, штучний інтелект зіграв важливу роль в забезпеченні кібербезпеки. Наша сучасна технологічна ера, безумовно, надає нам набагато більше можливостей і зручностей, але також вона створює нові загрози безпеці. Кіберзлочинці використовують різні методи та техніки для того, щоб зламати систему безпеки та здійснити кібератаку з метою отримання доступу до конфіденційної інформації, або ж навіть знищення даних. У таких ситуаціях, штучний інтелект може стати надзвичайно корисним інструментом, який допоможе виявити та запобігти кібератакам, а також забезпечити безпеку в режимі реального часу. Проте, з використанням ШІ в кібербезпеці пов'язані як переваги, так і недоліки.

Матеріали і методи

Об'єктом цього дослідження є застосування штучного інтелекту (ШІ) в кібербезпеці. Методика дослідження передбачає проведення аналізу наукової літератури, аналіз статистичних даних про кібератаки та їхні наслідки при застосуванні штучного інтелекту, вивчення відкритих даних та інформаційних ресурсів.

Результати

Щодо переваг застосування ШІ в кібербезпеці, варто зазначити, що він може допомогти виявляти загрози та атаки на ранніх стадіях, коли вони ще не завдали значної шкоди. Завдяки здатності штучного інтелекту аналізувати величезні обсяги даних в реальному часі, він може виявляти вразливості та атаки на систему, перш ніж вони стануть серйозними проблемами. Також, ШІ може допомогти виявити зловмисників та запобігти кібератакам. При цьому, він здатний виявляти загрози, які можуть бути пропущені людиною через втому, недосвідченість або відсутність необхідної інформації [1].

Окрім того, штучний інтелект має здатність до самонавчання - на основі даних з попередніх кібератак він може навчатися та вдосконалювати свої алгоритми з часом, що забезпечує більш ефективний захист від нових загроз. Наприклад, ШІ може використовувати еволюційні алгоритми, щоб створювати нові методи захисту, які можуть бути більш ефективними, ніж ті, що використовуються в даний час.

Але необхідно пам'ятати, що застосування штучного інтелекту має свої недоліки. Перш за все, ШІ може бути запрограмований некоректно, що призведе до помилкових рішень та погіршення захисту системи. Наприклад, він може використовувати неправильні моделі у випадку, коли недостатньо враховується контекст аналізу. Зловмисники можуть використовувати штучний інтелект для навчання своїх програм атакувати системи більш ефективно. Наприклад, зловмисники можуть створювати власні алгоритми, щоб обійти системи захисту, що використовують ШІ. Це може призвести до появи нових загроз та атак, які можуть виявитися більш складними для виявлення та запобігання. Також одним з найбільших недоліків застосування штучного інтелекту в кібербезпеці є висока ціна. Його використання може бути дуже дорогим, оскільки вимагає наявності спеціалізованого обладнання та програмного забезпечення [2, 3].

Важливо розвивати та вдосконалювати штучний інтелект в кібербезпеці, але з великою обережністю та контролем, тому рекомендовано: забезпечити коректні налаштування та належний контроль алгоритмів захисту та моніторингу системи, щоб уникнути помилок та недоліків; забезпечити відповідний рівень захисту системи ШІ від атак; забезпечити навчання на даних які відображають всі можливі сценарії атак; регулярно оновлювати та вдосконалювати алгоритми, щоб захист відповідав новим викликам та загрозам.

Висновки

Застосування ШІ в кібербезпеці має свої позитивні та негативні сторони: з одного боку, це може бути ефективним інструментом для прогнозування, моделювання, виявлення та запобігання кібератак, проте з іншого боку, за умови неналежного навчання, несанкціонованого впливу на алгоритми, неналежного контролю - це може стати загрозою. Для зменшення ризиків варто розробляти та впроваджувати ефективні технології захисту, проводити тестування та навчання персоналу, який працює з цими системами.

Список використаних джерел

1. Kabbas A., Alharthi A, Munshi A. Застосування штучного інтелекту в кібербезпеці. IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.2, Fabruary 2020. 120-124.

2. Документація про використання штучного інтелекту в кібербезпеці - https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity

3. Платформа Balbix «Використання штучного інтелекту в кібербезпеці» - https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

УДК 004.657

ПОБУДОВА ЗАПИТІВ ПРИРОДНЬОЮ МОВОЮ НА БАЗІ ТЕОРІЇ НЕЧІТКИХ МНОЖИН

Манжула Ксенія

Національний авіаційний університет, Київ

Науковий керівник – Наталія Шибицька, к.т.н., доц.

Ключові слова: Бази даних, нечітка множина, SQL запити, нечіткі запити

Вступ

На сьогоднішній день одним із ключових компонентів сучасних інформаційних систем є бази даних. Бази даних використовуються у кожному аспекті нашої повсякденної діяльності, що пов’язана з інформаційним простором – при перегляді ранкових/вечірніх новин, при пошуку книг, фільмів, ігор, музики, при спілкуванні із друзями та колегами через різні месенджери. Таким чином, кількість запитів до баз даних різних інформаційних систем може досягати якщо не сотень, то тисяч запитів у день.

Матеріали і методи

Основним інструментом здійснення запитів користувачами до різних баз даних є пошукові системи, які приймають від користувача запит, та транслюють його у відповідну базу даних у форматі SQL або NoSQL коду.

Результати

Однак, практичний досвід користувачів різних категорій показує єдину тенденцію – частина тих результатів, що були повернені пошуковими системами як відповідь на запит, або є некоректною, або не може у повній мірі задовольнити сам запит користувача [1-3].

Дослідження показують [1-3], що причиною некоректної відповіді баз даних на прості для людини запити є “нечіткість” самих запитів. Людині притаманне «нечітке мислення», і все своє життя вона використовує такі нечіткі поняття як “малий”, “великий”, “дешевий” та інші нечіткі значення, в той час як програма оперує конкретними значеннями, і не може опанувати сенс нечіткого поняття. Така тенденція невідповідності між запитом та результатом є серйозною проблемою, оскільки інформаційне суспільство базується не тільки на самих даних, але і на їх коректності.

Часткове рішення даної проблеми полягає у так званих “нечітких запитах”. Хоча дане рішення було запропоновано досить давно, воно активно розвивається і сьогодні, результатом чого є те, що пошукові системи та бази даних обробляють “природню” мову людини краще, ніж 5 – 10 років тому. Алгоритм роботи даних запитів наступний:

1. Формується деяке нечітке поняття (наприклад, “Досвід роботи”) – це лінгвістична змінна;

2. Для даної змінної задається область визначення – числовий інтервал. У випадку досвіду роботи це може бути інтервал від 1 до 15 років.

3. Для визначеної раніше лінгвістичної змінної виділяється три лінгвістичні терми. Відповідно до змінної “Досвід роботи” лінгвістичними термами будуть: “Малий досвід”, “Середній досвід” та “Великий досвід”.

4. Обирається функція приналежності. Частіше всього, обирається трапецеїдальна функція приналежності із параметрами [a, b, c, d] для кожного лінгвістичного терму. Параметри [a, b, c, d] визначаються спеціалістами, та йдуть за зростанням.

$$MF_C(x)=\begin{cases}1-\dfrac{b-x}{b-a}, a\le x\le b\\ 1, b\le x\le c\\ 1-\dfrac{x-c}{d-c}, c\le x\le d\\ 0, x\notin(a,d)\end{cases}$$

5. За трапецеїдальною функцією приналежності визначається відповідність деякого значення до однієї з визначених раніше груп (лінгвістичних термів).

В результаті дослідження було розроблено нечіткі запити та проаналізовано можливість їх застосування з метою збільшення рівню відповідності людських запитів нечіткого характеру та результатів, що повертають бази даних.

Висновки

Таким чином, застосування нечітких запитів у базах даних дозволяє вирішити проблему невідповідності та уточнити діапазон значень, що повертається у порівнянні із звичайними запитами з урахуванням суб’єктивної оцінки користувача.

Список використаних джерел:

1. Александрова Ю. С. Нечітка логіка та нечіткі запити запити до бази даних. // Збірник наукових праць з актуальних проблем економічних наук 2018. – С.77-80. [Електронний ресурс] – Режим доступу до ресурсу: http://molodyvcheny.in.ua/files/conf/other/28july2018/26.pdf.

2. Капустинський Р.І, Щирба З.В. Аналіз застосування нечітких систем для управління доступом до ресурсів. // Збірник публікацій ІІІ науково-практичної конференції. «Інтелектуальні комп’ютерні системи та мережі» 2020 – С.16.

3. Клічук О. Обробка реляційних баз даних засобами функціонального програмування. // Штучний інтелект №2 2009 – С. 57-62. [Електронний ресурс] – Режим доступу до ресурсу: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/7896/07-Klichuk.pdf?sequence=1.

УДК 004.056

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ КІБЕРБЕЗПЕКИ

Ірина Маришева

Національний авіаційній університет, Київ

Науковий керівник – Олена Прокопенко

Ключові слова: кібербезпека, тенденції, загрози

Вступ

В сучасному світі, коли технології зайняли важливе місце у нашому житті, постійне зростання рівня загроз кібернетичного простору стало однією з найбільш актуальних проблем. За останні кілька років технологічний прогрес був неабияким, що викликає значний ризик для безпеки усіх верст населення. Різке збільшення кількості кібератак, розширення меж їх реалізації вимагають адекватної відповіді перед поставленими викликами, які можливо досягти шляхом впровадження новітніх технологій, підходів, методів, засобів та заходів захисту, тому варто розглянути основні тенденції розвитку кібербезпеки.

Матеріали та методи

Об'єкт дослідження - це використання та впровадження сучасних підходів у кібербезпеці. Для здійснення даного дослідження використовується метод теоретичного узагальнення та порівняльного аналізу статичних даних про стан кібербезпеки, що знаходяться у вільному доступі та дослідження інформаційних ресурсів із мережі Інтернет. Основними властивостями досліджуваних явищ є зростання кількості та складності кібератак, розширення сфери їх застосування та збільшення втрат внаслідок кіберзлочинності.

Результати

Однією з найбільш важливих тенденцій у кібербезпеці є зростаюча кількість кібератак[1]. З метою отримання несанкціонованого доступу до даних та збору інформації[8], порушення доступності вебресурсів[7] здебільшого використовуються "старі відомі вразливості"[1] для проведення атак, що свідчить про необхідність оновлення систем з урахуванням потенційних поточних загроз, так і впровадженням удосконалених технологій кібербезпеки, адаптованих до нових загроз.

Ще однією тенденцією є збільшення ролі штучного інтелекту та машинного навчання у кібербезпеці[2,6]. Ці технології можуть допомогти виявляти та запобігати кібератакам, а також забезпечити більш точний та ефективний аналіз даних. Однак, також важливо враховувати етичні та правові аспекти використання штучного інтелекту та машинного навчання в кібербезпеці.

Крім того, збільшується увага до кібербезпеки від індивідуальних користувачів та підприємств[2]. Реалізовуються програми інформування користувачів щодо можливих загроз, методів їх усунення, акцентується увага на зменшенні «доступності своїх цифрових даних в Мережі» - свідомового ставлення до власної кібербезпеки[1].

Наступною тенденцією є поширення Інтернету речей (IoT)[2,3], яка передбачає підключення до мережі Інтернет різних пристроїв, від домашніх електроприладів до автомобілів та медичного обладнання, що створює нові ризики для кібербезпеки, оскільки багато з цих пристроїв можуть бути уразливими до кібератак.

З урахуванням поточних викликів спостерігається тенденція посилення рівня безпеки постачальниками хмарних сервісів, які звертають увагу на забезпечення високого рівня захисту даних, використовуючи передові технології шифрування та захисту мережі - провідні компанії світу, такі як Amazon, Google, Microsoft і Oracle «червоні команди» NSA перевіряють на стійкість захисту власні хмарні середовища, за принципом "нульової довіри"[1], застосовують більш стійкі криптоалгоритми для шифрування інформації в хмарних середовищах, тощо.

Також варто згадати про міжнародне співробітництво у сфері кібербезпеки[4]. У зв'язку з географією кіберзлочинів важливо мати програми, міжнародні стандарти та домовленості[1] для боротьби з кіберзлочинністю.

Висновки

Спостерігається окреслений чіткий напрям на посилення рівня захищеності в кібернетичному просторі задля протидії атакам та зменшення рівня загроз. Внаслідок реалізованої значної кількості атак, як глобальних, так і локальних, та тлі усунення наслідків відбувається консолідація сил протидії, створення та впровадження стратегій, концепцій кібербезпеки та проєктів для посилення захисту та інформування користувачів з метою підтримки кібергігієни, впровадження нових практик кіберзахисту на основі удосконалених технологій з урахуванням досвіду.

Список використаних джерел:

1. Syber digest. Огляд подій в сфері кібербезпеки на січень 2023 - https://www.rnbo.gov.ua/files/2023/NKCK/Cyber%20digest_january_2023_fin.pdf

2. Cyber Security Trends to Watch Out For in 2023 - https://www.glocomms.com/blog/2023/03/cyber-security-trends

3. 10 трендів кібербезпеки у 2023році - https://hub.kyivstar.ua/news/10-trendiv-kiberbezpeky-u-2023-roczi/

4. Top 10 Cybersecurity Predictions and Statistics For 2023 - https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

5. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review - https://www.mdpi.com/2079-9292/11/2/198

6. The future of Artificial Intelligence in Cybersecurity: Comprehensive Survey - https://www.researchgate.net/publication/353046785_The_future_of_Artificial_Intelligence_in_Cybersecurity_A_Comprehensive_Survey

7. Що таке DDoS-атака? - https://cip.gov.ua/ua/faqs/sho-take-ddos-ataka

8. Що таке вразливості програмних продуктів, та якої шкоди через це може зазнати пристрій? - https://cip.gov.ua/ua/faqs/sho-take-vrazlivosti-programnikh-produktiv-ta-yakoyi-shkodi-cherez-ce-mozhe-zaznati-pristrii

УДК 004.056.5:004.738.5(043.2)

CODEWARS ЧИ LEETCODE: ЯКА ПЛАТФОРМА КРАЩА ДЛЯ НАБУТТЯ ПРАКТИЧНИХ НАВИЧОК З ПРОГРАМУВАННЯ

Тарас Мельник

Національний авіаційний університет, Київ

Ключові слова: навчання, практика, програмування, задача, рішення, платформа.

Вступ

Нині спостерігається значний прогрес інформаційних технологій, що тягне за собою збільшення попиту на фахівців даної галузі. Чи не найбільшу частину IT займає сфера програмування. Існує чимало способів отримання навичок для роботи програмістом. Один із них - практика. CodeWars та LeetCode - це дві популярні онлайн-платформи для вивчення та практикування програмування. Хоч вони і мають спільну ціль, проте між ними існують відмінності, які можуть вплинути на швидкість та якість набуття необхідного досвіду.

Матеріали і методи

CodeWars представлений у вигляді веб-сайту, що надає користувачеві можливість вирішувати різноманітні задачі з програмування, які мають назву «ката» (англ. «kata»). При успішному вирішенні ката підвищується ранг. Чим вище ранг, тим складніші задачі. CodeWars пропонує більше 20 мов програмування для практикування, а якщо включати і ті мови, що знаходяться у бета-тестуванні, то більше 50. Особливістю даної платформи є те, що вона створена «суспільством для суспільства», тобто мається на увазі, що ті завдання, які пропонуються користувачам для розв’язання, створюються цими ж користувачами.

LeetCode являє собою веб-сайт, який пропонує вирішити так звані «проблеми», тобто задачі з програмування. На відмінну від CodeWars, тут можна самому обирати рівень складності завдання: легкі, середні або важкі. Задачі на платформу додають її розробники. Вони (розробники) у свою чергу беруть ці завдання із технічних співбесід у IT-компаніях. Це великий плюс, оскільки вирішення таких задач допоможе у майбутньому при влаштуванні на роботу. Також необхідно зазначити те, що LeetCode акцентує увагу на ефективності рішення: під час розв’язання завдання платформа повідомляє скільки часу та яку кількість ресурсів комп’ютера використає згенерований код.

Результати

Порівнюючи між собою CodeWars та LeetCode потрібно враховувати ціль, яку ставить перед собою людина, що зібралась використовувати один з цих ресурсів. Якщо головною метою є працевлаштування, то явним лідером виступає LeetCode, оскільки дана платформа сфокусована на вирішенні задач, які пропонуються під час проходження технічної співбесіди

на позицію програміста, а також містить додаткові ресурси для навчання, такі як статті, практичні поради тощо. Явною перевагою являється той факт, що LeetCode робить аспект на найефективнішому рішенні задачі і має для цього відповідні інструменти. Якщо ж користувач має на меті тільки удосконалення навичок з програмування та поглиблення знань алгоритмів і структур даних, то для цього чудово підходять обидві платформи. Слід зазначити, що CodeWars краще підлаштований для спілкування з іншими програмістами, оскільки він надає більше можливостей для співпраці та обміну думками.

Висновки

Якщо вам подобається ідея навчання у середовищі, яке ґрунтується на комунікації між людьми, то кращим вибором є CodeWars. Ви повинні обрати LeetCode, якщо ваша головна мета - це успішно пройти технічне інтерв'ю при працевлаштуванні та вивчити алгоритми і структури даних у найбільш спрощений та швидкий спосіб.

Список використаних джерел

1. Cyber Security Trends to Watch Out For in 2023 - https://www.glocomms.com/blog/2023/03/cyber-security-trends

2. 10 трендів кібербезпеки у 2023році - https://hub.kyivstar.ua/news/10-trendiv-kiberbezpeky-u-2023-roczi/

3. Top 10 Cybersecurity Predictions and Statistics For 2023 - https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

4. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review - https://www.mdpi.com/2079-9292/11/2/198

5. The future of Artificial Intelligence in Cybersecurity: Comprehensive Survey - https://www.researchgate.net/publication/353046785_The_future_of_Artificial_Intelligence_in_Cybersecurity_A_Comprehensive_Survey

6. Що таке DDoS-атака? - https://cip.gov.ua/ua/faqs/sho-take-ddos-ataka

УДК 004.056.55

АНАЛІЗ ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ТА ЗАХИСТУ ВІД КІБЕРАТАК НА СИСТЕМИ УПРАВЛІННЯ ЕНЕРГЕТИЧНИМИ МЕРЕЖАМИ.

Діана Москаленко

Національний авіаційний університет, Київ

Науковий керівник – Валерій Козловський, д.т.н, проф.

Ключові слова: сканер, антивірус, інтерфейс, оптимізація

Вступ

У зв'язку зі зростанням кількості кібератак на системи управління енергетичними мережами, виникає необхідність у розробці нових методів виявлення та захисту від таких загроз. Використання методів машинного навчання є одним з потенційно ефективних способів боротьби з цими загрозами [1-3]. Метою цього дослідження є аналіз застосування таких методів для забезпечення кібербезпеки систем управління енергетичними мережами.

Матеріали і методи

У даному дослідженні я аналізувала застосування методів машинного навчання для виявлення та захисту від кібератак на системи управління енергетичними мережами. Об'єктом дослідження є системи управління енергетичними мережами. В досліджені використано методи аналізу даних та машинного навчання, проведено аналіз різних алгоритмів машинного навчання, таких як нейронні мережі, дерева рішень, ансамблеві методи тощо. Також використано методи візуалізації даних та статистичного аналізу та дані з реальних систем управління енергетичними мережами.

Окрім того, було проведено порівняльний аналіз різних підходів до захисту систем управління енергетичними мережами від кібератак. Усі етапи дослідження були проведені з використанням програмного забезпечення Python та відповідних бібліотек для машинного навчання та обробки даних.

Результати

Результати цього дослідження показали, що застосування методів машинного навчання є потенційно ефективним способом боротьби з кібератаками на системи управління енергетичними мережами. Я дослідила різні підходи до застосування машинного навчання, такі як навчання з вчителем, навчання без вчителя та підсилене навчання, і порівняли їх ефективність в забезпеченні кібербезпеки.

Зокрема, було виявлено, що навчання з вчителем дозволяє досягати високої точності виявлення кібератак, однак воно вимагає великої кількості позначених даних для навчання

моделей. Навчання без вчителя, яке базується на аналізі властивостей даних, може працювати з меншою кількістю позначених даних, але його ефективність залежить від якості вихідних даних та вибору алгоритмів кластеризації. Підсилене навчання, яке базується на навчанні агента взаємодіяти з середовищем та отримувати нагороду за правильні дії, може бути ефективним способом виявлення кібератак, якщо він використовується зі спеціалізованими середовищами та розробленими алгоритмами.

Тому це дослідження підтверджує, що застосування методів машинного навчання є потенційно ефективним інструментом в боротьбі з кібератаками на системи управління енергетичними мережами. При цьому важливо враховувати особливості кожного підходу та добирати його в залежності від конкретної задачі та наявної кількості даних.

Висновки

Аналіз застосування методів машинного навчання для виявлення та захисту від кібератак на системи управління енергетичними мережами показав, що використання таких методів є ефективним і дозволяє підвищити рівень безпеки в енергетичній сфері. Отримані результати можуть бути використані для розробки нових систем захисту від кібератак та покращення існуючих. Наукова новизна полягає у застосуванні сучасних методів машинного навчання до проблем безпеки в енергетиці.

Список використаних джерел

1. T. Kuzlu, "The Importance of Cybersecurity in the Energy Sector," Energy and Power Engineering, vol. 10, no. 4, pp. 168-174, 2018.

2. S. Wang, S. Zhang, and J. Zou, "Application of Machine Learning in Cybersecurity of Critical Infrastructure," in Advances in Computer Science and Ubiquitous Computing, Springer, 2018, pp. 103-110.

3. Al-Mousawi, M. Al-Khalid, and M. Al-Kandari, "Cybersecurity of Critical Energy Infrastructure: Challenges and Opportunities," in Cyber Security and Privacy, Springer

4. Кан Ю., Гао Дж. та Лю К. (2021). Кібербезпека енергосистем: огляд. Renewable and Sustainable Energy Reviews, 145, 111032. doi: 10.1016/j.rser.2021.111032

5. NIST Cybersecurity Framework. https://www.nist.gov/cyberframework

6. Модель зрілості потенціалу кібербезпеки Міністерства енергетики США (C2M2), версія 2.0. https://www.energy.gov/sites/prod/files/2015/10/f27/C2M2-v2-0_final_10-22-15.pdf.

УДК 004.056.5-048.66(043.2)

ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ КОМП'ЮТЕРА ЗА ДОПОМОГОЮ BIOS

Максим Омельченко

Національний авіаційній університет, Київ

Науковий керівник –Валерій Козловський, д.т.н., проф.

Ключові слова: сканер, антивірус, BIOS, захист, комп'ютер..

Вступ

Технологій проблема захисту інформації є актуальною повсякчас. Програми, що мають доступ до персональної інформації користувачів, повинні відповідати високим вимогам безпеки та запобігти зловмисному використанню особистих даних користувача.

Матеріали і методи

BIOS (Basic Input/Output System) - це програмне забезпечення, яке запускається на комп'ютері при його включенні і контролює його основні функції. Включаючи налаштування інтерфейсу, перевірку обладнання, запуск операційної системи та багато іншого.

Результати

Система захисту комп'ютера за допомогою BIOS може бути реалізована за допомогою різноманітних методів. Один з найбільш поширених методів полягає в використанні пароля на рівні BIOS. Це означає, що перед тим, як користувач зможе запустити операційну систему, йому потрібно буде ввести пароль на екрані BIOS. Це запобігає несанкціонованому доступу до комп'ютера та забезпечує його безпеку.

Інший метод захисту комп'ютера за допомогою BIOS полягає в обмеженні доступу до дискових пристроїв. За допомогою налаштувань BIOS можна заблокувати доступ до дисків або встановити обмеження на запис та відтворення інформації на них. Це може бути корисно для захисту конфіденційних даних від несанкціонованого доступу.

Додатково, за допомогою BIOS можна встановити правила для завантаження комп'ютера, такі як встановлення перевірки на наявність вірусів під час завантаження операційної системи. Це може допомогти запобігти розповсюдженню шкідливих програм та вірусів на комп'ютері.

Висновки

Система BIOS також може відключати певні пристрої, які можуть бути використані для зламу або несанкціонованого доступу до комп'ютера. Наприклад, заблокувати USB-порти або слоти для карт пам'яті.

Список використаних джерел

1. Blockchain Facts: What It Is How It Works, and How It Can Be Used. URL: https://www.investopedia.com/terms/b/blockchain.asp#toc-what-is-a-blockchain

2. Blockchain security: What keeps your transaction data safe? URL: https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/

3. Blockchain Security Mechanisms. URL: https://towardsdatascience.com/mechanisms-securing-blockchain-data-9e762513ae28

4. Yadav, S.P. (2022). Blockchain Security. In: Baalamurugan, K., Kumar, S.R., Kumar, A., Kumar, V., Padmanaban, S. (eds) Blockchain Security in Cloud Computing. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-70501-5_1.

УДК 004.056.56:342(043.2)

КІБЕРБЕЗПЕКА ЯК ВАЖЛИВА СКЛАДОВА ВСІЄЇ СИСТЕМИ ЗАХИСТУ ДЕРЖАВИ

Владислав Панасюк, Юрій Нестеров

Національний авіаційній університет, Київ

Науковий керівник – Володимир Темніков, д.т.н., доц.

Ключові слова: кібербезпека, кібератаки, кіберзагрози, захист, загроза.

Висновки

Кібербезпека є невід'ємною складовою захисту держави від кібератак та кіберзлочинності, оскільки сучасний світ все більше цифровізується, а кіберзлочинці шукають нові способи злому систем та крадіжки важливої інформації. Відсутність належного рівня кібербезпеки може призвести до серйозних наслідків для національної безпеки та економіки країни, тому захист від кібератак є важливим завданням для будь-якої держави.

Матеріали і методи

Кібератаки можуть спричинити порушення роботи критичних інфраструктурних об'єктів, крадіжку персональних даних та інформації, а також завдати інші види шкоди. Це може мати серйозні наслідки для держави, такі як втрата довіри до влади, порушення економічної стабільності тощо. Тому важливо забезпечувати належний рівень кібербезпеки для захисту національної безпеки та економіки країни.

Результати

Кіберзлочинці постійно розвивають нові технології та методики для злому систем та крадіжки інформації. Тому, для ефективного захисту від кібератак, потрібні постійні зусилля та постійне оновлення заходів кібербезпеки. Це включає в себе впровадження нових технологій та інструментів, постійне навчання та підвищення кваліфікації персоналу, розробку стратегій та політик кібербезпеки, а також співпрацю з іншими державами та секторами для обміну досвідом та взаємної допомоги.

Система захисту держави від кібератак повинна бути цілісною та включати в себе відповідні технічні, правові та організаційні заходи. Технічні заходи повинні включати захист мереж та систем, захист даних та інформації, виявлення та відповідь на кібератаки. Правові заходи повинні встановлювати законодавство, яке регулює використання технологій та інформації в державній сфері, а також кримінальну відповідальність за кіберзлочини. Організаційні заходи повинні включати розробку та впровадження стратегій та політик кібербезпеки, а також підготовку та навчання персоналу, що працює з технологіями та

інформацією, з метою запобігання кібератакам та виявлення їх вчасно. Тільки комплексний підхід до кібербезпеки забезпечить ефективний захист держави від кібератак.

Висновок

Таким чином, кібербезпека є невід'ємною складовою захисту держави від кібератак та кіберзлочинності, і недостатній рівень кібербезпеки може призвести до серйозних наслідків для національної безпеки та економіки країни. Оновлення та вдосконалення заходів з кібербезпеки є необхідним для ефективного захисту від сучасних загроз.

Список використаних джерел

3. Костова Н.І., Косарь У.С. Актуальні проблеми кібербезпеки в Україні та шляхи їх вирішення. URI: https://hdl.handle.net/11300/19839

4. Янковський О. Україні потрібна нова кіберстратегія. URL: https://www.pravda.com.ua/columns/2019/09/14/7226291

5. Актуальні проблеми кібербезпеки в Україні. URL: https://interfax.com.ua/news/press-release/845965.html.

УДК 004.056.5:004.738.5(043.2)

СТВОРЕННЯ ПРОТОКОЛІВ БЕЗПЕКИ

Олег Пелих

Національний авіаційній університет, Київ

Ключові слова: інформація, захист, злочин, Інтернет, безпека.

Вступ

Технологій проблема захисту інформації є актуальною повсякчас. Програми, що мають доступ до персональної інформації користувачів, повинні відповідати високим вимогам безпеки та запобігти зловмисному використанню особистих даних користувача.

Матеріали і методи

Створення протоколів безпеки є важливим завданням в сфері кібербезпеки, яке дозволяє забезпечити надійний захист від різних видів кіберзагроз. Процес створення протоколу безпеки включає декілька важливих кроків, які дозволяють розробити ефективний та надійний захист.

Результати

Першим кроком у створенні протоколу безпеки є докладний аналіз можливих кіберзагроз та вразливостей, що можуть бути використані для злому системи. Цей аналіз дозволяє визначити потенційні точки входу для зловмисників та визначити можливі способи атаки на систему.

Другим кроком є розробка ефективних методів захисту від різних видів кіберзагроз. Це може включати розробку нових алгоритмів шифрування, автентифікації та контролю доступу, які забезпечують високий рівень захисту від несанкціонованого доступу.

Третім кроком є розробка протоколу безпеки, що включає в себе детальне визначення правил та процедур для обміну даними та забезпечення безпеки в процесі цього обміну. Це може включати розробку спеціальних алгоритмів для шифрування, автентифікації та контролю доступу.

Четвертим кроком є реалізація протоколу безпеки, що включає в себе розробку програмного забезпечення, яке дозволяє виконувати створений протокол. Під час реалізації необхідно враховувати всі розроблені раніше методи захисту та правила протоколу.

Останнім кроком у процесі створення нового протоколу безпеки є тестування його ефективності та надійності в різних умовах. Це дозволить переконатись у тому, що протокол забезпечує достатній рівень захисту від різних видів кіберзагроз та може бути успішно використаний в реальних умовах.

Отже, створення нових протоколів безпеки є важливим завданням, яке вимагає високої кваліфікації, експертизи та докладних досліджень у галузі кібербезпеки.

Висновки

Протоколи створення нових протоколів безпеки мають достатню кількість ефективних вбудованих принципів захисту інформації від зловмисного втручання та використання даних як на рівні самих ланцюгів, так і на рівні користувачів. Використання технології дозволить суттєво прискорити різні конфіденційні користувальницькі операції та зробити їх більш прозорими, скоротити витрати на надання та зберігання паперових документів, а також зменшити ризики фальсифікації та втрати документів. Проте, досить велика роль у безпеці транзакцій все ще покладається на користувачів, що призводить до потреби кращого ознайомлення користувачів із більш поглибленими правилами безпеки.

Використані джерела інформації:

1. Blockchain Facts: What It Is How It Works, and How It Can Be Used. URL: https://www.investopedia.com/terms/b/blockchain.asp#toc-what-is-a-blockchain

2. Blockchain security: What keeps your transaction data safe? URL: https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/

3. Blockchain Security Mechanisms. URL: https://towardsdatascience.com/mechanisms-securing-blockchain-data-9e762513ae28

4. Yadav, S.P. (2022). Blockchain Security. In: Baalamurugan, K., Kumar, S.R., Kumar, A., Kumar, V., Padmanaban, S. (eds) Blockchain Security in Cloud Computing. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-70501-5_1

УДК 004.056.5

ПРИХОВУВАННЯ ДАНИХ В МЕДІАФАЙЛАХ МЕТОДАМИ СТЕГАНОГРАФІЇ.

к.т.н, доц. Андрій Петренко, Валентина Телющенко

Національний авіаційний університет, м. Київ

Ключові слова: захист інформації, стеганографія, фазове кодування, найменший значущий біт, медіафайли, вбудовування інформації

Вступ

Надійний захист інформації від несанкціонованого доступу є одним із завдань, що потребує вирішення. У зв'язку швидким розвитком і поширенням інформаційний технологій, які дозволяють використовувати засоби автоматизованої обробки та синхронного відтворення різноманітних типів сигналів, питання захисту інформації, представленої в цифровому вигляді, є актуальним. Доступність численних даних в цифровій формі, таких як аудіо, відео в мережі Інтернет спричиняє неконтрольоване та несанкціоноване їх розповсюдження і копіювання, що в свою чергу приводить до потреб захисту інтелектуальної власності.

Матеріали та методи

Методи стеганографії полягають у приховуванні самого факту передачі конфіденційних даних чи факту наявності секретного повідомлення в стеганоконтейнері. В якості стеганоконтейнера використовуються зображення, медіафайли, тощо [1].

Проте методи стеганографіі використовують не тільки для передачі секретної інформації, а також для захисту даних від крадіжок, а саме від нелегального їх розповсюдження, чи копіювання, чи розміщення в різних джерелах, пошуку інформації в мультимедійних базах даних, тощо. Тобто завдяки даним методам можна захистити свої авторські права шляхом вбудовування відповідних міток чи цифрових водяних знаків, які служать для ідентифікації автора твору, наприклад таких як аудіо чи відеофайли, зображення [2].

В матеріалі розглянемо два основних метода вбудовування даних в медіафайли – метод LSB (метод найменшого значущого біту**)** та фазового кодування.

Результати

Зазначені методи стеганографії забезпечують пересилання повідомлень достатньо великого об'єму у медіа файлах за рахунок їх модифікації. Однак вносити зміни в звукові файли потрібно так, щоб зловмиснику не вдалося усунути їх, не спотворивши вихідний сигнал. Враховуючи особливості слухового сприйняття звукових файлів людиною можливо змінювати фазу сигналу таким чином, що при подальшому прослуховуванні даних звукових

файлів, людина ніяких змін не відчує. Передача інформації в медіафайлах можлива за рахунок властивостей слухової системи людини, яка не чутлива до зміни абсолютної фази сигнала.

Суть методу LSB полягає в заміні останніх значущих бітів у медіафайлах. Використовуючи звуковий сигнал шляхом заміни найменшого значущого біта кожної точки реалізації вибірки, яка представлена у вигляді двійкової послідовності можна вкласти достатній об'єм інформації. Головний недолік даного метода є його чутливість до сторонніх впливів, наприклад вбудована інформація може бути зруйнована через наявність шумів в каналі. Проте, його перевага заключається в простоті реалізації приховування інформацію з високою швидкістю передачі даних.

Метод фазового кодування використовує модифікацію фази початкового сегмента аудіо сигналу, куди вбудовується інформація, а фаза наступних сегментів узгоджується, щоб зберегти різницю фаз. Це потрібно для збереження різниці фаз, до якої людських слух нечутливий. Значення вбудованого повідомлення перетворюється у значення фаз $\frac{\pi}{2}$ і $\left(-\frac{\pi}{2}\right)$, що представляють собою одиниці і нулі відповідно. При вбудовуванні даних на основі даного методу зміни вносяться в область високих частот, що дає змогу досягти стійкості до різних видів атак. Також, у порівнянні з іншими стеганографічними методами, метод фазового кодування є одним із методів, який стійкий до стиснення і впливу шумів. Недоліком даного методу являється низька пропускна здатність, яка складає від 8 до 32 біт/с в залежності від звукового контексту [1].

Висновок

Вбудовування інформації представленими стеганографічними методами базується на внесенні незначних змін в параметри медіафайлів, які слухова система людини не здатна відрізнити. При використанні методу LSB можна приховати значний об'єм інформації у відносно невеликих файлах, що не приводить до спотворення вихідного аудіофайла, а це в свою чергу зменшує ймовірність виявлення факту вбудовування інформації. Фазове кодування є одним із найбільш ефективних методів по критерію відношення сигнал/шум, але має низьку пропускну здатність.

Список використаних джерел

1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика // Конахович Г.Ф., Пузыренко А.Ю – К: «МК-Пресс», 2006. – 288с.

2 Хорошко В.О., Яремчук Ю.Є., Карпінець В.В. Комп'ютерна стеганографія : навчальний посібник– В. : Вид. ВНТУ, 2017. – 86 с.

3. Петренко А.Б, Телющенко В.А., Приховування даних в аудіофайлах методом LSB, ITSec-2019: IX ,Міжнародна науково-технічна конференція, 22–27 березня 2019 р.: тези доп. – К., 2019. – С. 40.

УДК 004.946.5056(043.2)

КІБЕРРОЗВІДКА ЯК СУЧАСНИЙ МЕТОД ПРОВЕДЕННЯ ОПЕРАТИВНИХ РОЗСЛІДУВАНЬ

Лілія Погорецька, Тетяна Яськова

Національний авіаційній університет, Київ

Науковий керівник – Олександр Туровський, д.т.н., професор.

Ключові слова: інформація, кіберрозвідка, кіберпростір, комп'ютерні технології.

Вступ

Активне застосування комп'ютерних технологій в усіх сферах життя, а також перехід значної частини злочинності з реального світу у кіберпростір, який став як місцем і засобом вчинення кримінальних правопорушень, так і джерелом інформації, яка становить оперативний інтерес, вважаємо за доцільне виділити вид кримінальної розвідки – кіберрозвідку.

Матеріали та методи

Виділимо три окремі рівні кіберрозвідки:

- Стратегічний – рівень де оброблюється інформація високого рівня
- Оперативний – рівень, на якому добувається інформація про ймовірні атаки на організацію
- Тактичний – на основі даних від систем виявлення та запобігання вторгнень, мережевих сенсорів, кінцевих пристроїв, спеціалізованих засобів захисту виявляються мережеві артефакти та ідентифікатори компрометації комп'ютерної мережі й може бути висунута гіпотеза щодо інструментів здійснення атаки [1].

У теорії оперативних розслідувань на даний час відсутнє усталене визначення кіберрозвідки. Разом з тим, в юридичній літературі досить часто використовуються такі поняття, як:

– комп'ютерна розвідка – оперативно-розшуковий захід, який полягає у цілеспрямованому пошуку та отриманні інформації з комп'ютерних систем та мереж, доступ до яких не обмежується їх власником, володільцем чи розпорядником або не пов'язаний з подоланням системи логічного захисту, що здійснюється працівниками оперативних та оперативно-технічних підрозділів з метою виявлення відомостей криміногенного та кримінального характеру [2];

– аналітична розвідка – розвідувальний пошук, технічна розвідка, комплексне вивчення матеріалів прихованого спостереження та оперативної установки, а також аналіз повідомлень,

публікацій та виступів у засобах масової інформації, статистичних даних, відомостей автоматизованих банків даних [3];

– «віртуальна» розвідка – комплекс заходів щодо здобуття, обробки й аналізу розвідувальної інформації в кібернетичному (телекомунікаційному, віртуальному) просторі за допомогою різних видів програмно-математичного впливу. При цьому «віртуальна розвідка» включає в себе кіберрозвідку, радіорозвідку, розвідку систем. Науковий процес та наукові підходи: методика та реалізація досліджень супутникового зв'язку [4].

Результати

Ми можемо проаналізувати і запропонувати визначення кіберрозвідки як напряму оперативних розслідувань, що реалізовується з дотриманням принципів законності та верховенства права уповноваженими на те суб'єктами, та полягає збиранні, аналізі, оцінці та використанні інформації, яка розміщена у кіберпросторі, з метою виявлення, припинення, розкриття та розслідування кримінальних правопорушень, розшуку осіб, які переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування кримінального покарання та безвісно відсутніх осіб. При проведенні кіберрозвідки під час оперативний розслідувань та в ході розслідування злочинів використовуються наступні засоби та методи: аналіз відкритих джерел інформації (OSINT – Open source intelligence), соціальна інженерія, зняття інформації з транспортних телекомунікаційних мереж та з електронних інформаційних систем, отримання та аналіз інформації, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання. Під час кіберрозвідки можливо використовувати ще такі засоби, як комп'ютерні віруси, «троянські коні», логічні бомби та засоби віддаленого доступу [4]. Разом з тим, зауважимо, що використання вказаних засобів повинно відбуватися лише за умови чіткого та неухильного дотримання вимог чинного законодавства та виключати будь-які прояви порушення прав людини та громадянина.

Висновок

Кіберрозвідка є важливим методом проведення оперативних розслідувань у сучасних умовах, що дозволяє збирати та аналізувати інформацію швидко та ефективно. Дослідження пов'язано з розробкою новітніх методів, засобів пошуку, збору та аналізу інформації з урахуванням науково-технічного прогресу.

Список використаних джерел:

1. Жилін А., Ніколаєнко Б., Баклинський О. Підвищення захищеності державних інформаційних ресурсів за рахунок застосування платформи THREAT INTELLIGENCE. 2021. С. 136-146.

2. Мовчан, А. В. Окремі аспекти застосування комп'ютерної розвідки в оперативно-розшуковій діяльності. Проблеми правоохоронної діяльності. 2014. С. 107-122.

3. Білоглазов Є. Р. Методологія аналітичної розвідки кримінальних процесів та явищ. 2007.

4. Сідченко, С. О., Бєлімов, В. В. & Хударковський К. І. Можлива організаційна структура підрозділу розвідки у кібернетичному просторі. Системи озброєння і військова техніка. 2006. С. 47-50.

5. Сідченко С. А., Петров, В. Л., Бєлімов В.В. & Залкін С. В. Основні характеристики розвідки інформації у кібернетичному просторі. Радіоелектронні та комп'ютерні системи. 2026. С. 90-95.

УДК 004.051

СКОРОЧЕННЯ ЦИКЛУ ПОГОДЖЕННЯ ДОКУМЕНТІВ З ВИКОРИСТАННЯМ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Людмила Рибак

Національний авіаційний університет, Київ

Науковий керівник – Тетяна Конрад, к.т.н.

Ключові слова: СЕД, електронний документообіг, візування.

Вступ

Діяльність кожної юридичної особи пов’язана зі створенням та обміном великою кількістю документів для реалізації виробничих процесів, таких як: обробка звернень, документування відряджень, доведення інформації про накази, управлінські рішення тощо. Проте, досі обробка значного обсягу документів проводиться у ручному режимі традиційними методами паперового документообігу. Цей метод демонструє свою нерентабельність та невідповідність сучасним вимогам до обробки та збереження даних, а також потребує більшого часу на погодження та переадресацію документів. Для впорядкування цих процесів динамічним і надійним способом пропонується використання систем електронного документообігу (СЕД). Призначенням СЕД є створення та ведення електронних документів замість паперових версій. Перспективи впровадження СЕД наведені в працях вчених Подворнюк О. О., Поліщук Н. В. Переваги та надоліки експлуатації СЕД наведено в працях Гаркуші С. А., Шепель І. В., Конрад Т. І., Савчука В. С. [1]. Аналіз публікацій показав, що не достаньо уваги з боку вчених приділено питанню впливу СЕД на перебіг циклу погодження документів. Тому, доцільним є аналіз залучення СЕД для реалізації потреби в скороченні циклу погодження документів.

Мета роботи: скорочення циклу погодження документів за рахунок використання СЕД.

Матеріали та методи

Об’єктом дослідження є процес погодження документів. Дослідження ґрунтуються на використанні методів: *аналізу* – порівняльний аналіз циклів погодження документів у ручному та автоматизованому режимі; *системний підхід* – розгляд об'єкту дослідження як складової СЕД; *узагальнення* – висновки за результатами дослідження.

Результати

Погодження проектів документів зацікавленими установами, структурними підрозділами, окремими посадовими особами здійснюється з метою підвищення якості ділових паперів шляхом компетентної оцінки їх змісту, редакції, відповідними службовими особами. Постановою Кабінету Міністрів України від 17 січня 2018 р. № 55 затверджено

регламент організації взаємодії органів виконавчої влади в електронній формі із залученням системи електронної взаємодії органів виконавчої влади, яка призначена для автоматизації основних процесів життєвого циклу документів та визнається пріоритетною формою взаємодії органів влади з іншими державними органами [2].

Життєвий цикл документа передбачає етапи: створення → надсилання → передачу → одержання → оброблення (візування) → використання → зберігання → знищення.

Цикл погодження паперової версії документу у ручному режимі (без використання СЕД) передбачає фізичне переміщення документа від одного до іншого співробітника для реалізації візування [3]. У цьому випадку цикл є більш складним та тривалим, за рахунок впливу: людського фактору – способу мислення, стилю поведінки, відповідальності осіб; територіального розміщення об'єктів – особи можуть знаходитися в різних офісах / містах тощо; можливості фальсифікації документів. Це, в свою чергу, збільшує часову тривалість циклу погодження, ризики в умовах невизначеності, та зменшує стійкість підприємства. У той самий час електронний документообіг (ЕД) скорочує цикл перегляду та затвердження документів в межах їх життєвого циклу за рахунок рівномірного розподілу навантаження підрозділів та посадових осіб; зменшує трудомісткість на етапах створення, візування та архівування документів; знижує ризики помилок та можливості несанкціонованого доступу до документів. Держава сприяє активному розвитку ЕД, затвердивши єдиний інформаційний простір для реєстрації, приймання, аналізу та зберігання організаційно-розпорядчих документів органів виконавчої влади в електронному вигляді із застосуванням кваліфікованого електронного підпису. Таким чином ЕД відбувається швидко, без витрат на друк та доставку, що дозволяє значно прискорити процес погодження умов та підписання і, відповідно, забезпечити стрімкий початок робіт, надання послуг, здійснення розрахунків, отримання актів виконаних робіт тощо. Беззаперечною перевагою СЕД є ведення електронного архіву, що надає структуроване зберігання електронних документів із забезпеченням надійності, конфіденційності, розмежування прав доступу та зручний пошук.

Висновок

СЕД сприяє підвищенню продуктивності працівників організації, спрощує умови створення та скорочує цикл погодження документів, зменшуючи трудомісткість на всіх етапах життєвого циклу електронного документа, що сприяє підвищенню ефективності та оперативності прийняття управлінських рішень.

Список використаних джерел

1. Конрад Т.І., Савчук В.С. Аналіз потреб в системах електронного документування держустановами та підприємствами / ТІ. Конрад, В.С. Савчук // Інтелектуальні технології

лінгвістичного аналізу: тези Міжнародної науково-технічної конференції, м. Київ, 18-19 жовтня 2022р. – К.: НАУ, 2022. – С. 9.

2. Деякі питання документування управлінської діяльності. URL: https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF#n1251 (Last accessed: 12.03.2023).

3. Процедури візування (погодження) документів та їх різновиди. URL: https://instaco.com.ua/news/protseduri-vizuvannya-pogodzhennya-dokumentiv-ta-yih-riznovidi (Last accessed: 12.03.2023).

УДК 771.429(043.2)

AVIRA ANTIVIRUS, ВИКОРИСТАННЯ ТА ОСОБЛИВОСТІ

Данило Соколов

Національний авіаційній університет, Київ

Науковий керівник –Валерій Козловський, д.т.н., проф.

Ключові слова: сканер, антивірус, інтерфейс, оптимізація.

Вступ

Технологій проблема захисту інформації є актуальною повсякчас. Програми, що мають доступ до персональної інформації користувачів, повинні відповідати високим вимогам безпеки та запобігти зловмисному використанню особистих даних користувача.

Матеріали і методи

AVIRA ANTIVIRUS - це не одна програма, а ціла їх серія, з кожним новим оновленням змінювалися можливості цього антивірусу, його функціональні можливості і т.д.. Головною метою цього і будь-якого іншого антивірусу є захист вашої інформації, браузеру, електронної пошти.

Результати

Найбільше у мене викликало позитивних вражень від використання цього антивірусу— сканер Avira. У нього дуже чутливе налаштування, що дає змогу зробити пошук шкідливих файлів легшим. Є можливість задати конкретні параметри пошуку, вказати тільки потрібні каталоги. Також перевагою цього сканеру є швидкість. Не дивлячись на обсяг перевірки (сканування жорстких дисків та інших, процесору, програм системи Windows та інших ОС), вона виконується доволі швидко. Також певною перевагою є інтерфейс. Функції антивірусу знаходяться у своїх розділах, що полегшує інтуїтивний пошук для користувача. Також існує можливість кастомізувати інтерфейс під ваші потреби у налаштуваннях.

Після певного часу використання цього антивірусу, я для себе виділив низку висновків. Насамперед, браузерне розширення AVIRA має гарну систему блокування фішингових сайтів, спаму у почті, реклами в інтернеті.

У порівняні з багатьма іншими, або звичайними, що є у CHROME і т.д., розширення AVIRA виконує свої функції найкраще. Будучими фанатом відеоігор, я був приємно здивований, що AVIRA надає можливість прискорити відеокарту, що значно поліпшило враження. Ще гарним «бонусом» є розширена вибірка можливостей оптимізації роботи пристрою: від видалення кешу файлів, до сканування програм и виявлення тих, що найбільше впливають на роботу пристрою у негативному напряму.

Висновки

AVIRA можливо має свої недоліки, як наприклад безліч платних версій, у яких не важко заплутатись. Та попри все, користувач отримує зручний інтерфейс, широкі можливості щодо оптимізації пристроїв та систему сканування, яка збереже особисту інформацію від загроз у інтернеті.

Використані джерела інформації

1. Blockchain Facts: What It Is How It Works, and How It Can Be Used. URL: https://www.investopedia.com/terms/b/blockchain.asp#toc-what-is-a-blockchain

2. Blockchain security: What keeps your transaction data safe? URL: https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/

3. Blockchain Security Mechanisms. URL: https://towardsdatascience.com/mechanisms-securing-blockchain-data-9e762513ae28

4. Yadav, S.P. (2022). Blockchain Security. In: Baalamurugan, K., Kumar, S.R., Kumar, A., Kumar, V., Padmanaban, S. (eds) Blockchain Security in Cloud Computing. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-70501-5_1.

УДК 004.056

СПОСОБИ ЗАХИСТУ ДАНИХ В БЛОКЧЕЙНІ

Єлизавета Соколова

Національний авіаційний університет, Київ

Науковий керівник – Яна Бєлозьорова, к.т.н., доцент

Ключові слова: блокчейн, смарт-контракт, захист інформації.

Вступ

Технологій проблема захисту інформації є актуальною повсякчас. Програми, що мають доступ до персональної інформації користувачів, повинні відповідати високим вимогам безпеки та запобігти зловмисному використанню особистих даних користувача.

Матеріали і методи

Блокчейн це розподілена база даних, що поширюється між вузлами комп'ютерної мережі [1]. Найбільш відомою сферою використання блокчейну є галузь криптовалют, використання якого дозволяє досягти захищеності та децентралізації запису транзакцій у криптовалютних системах. Таким чином, інформація від кожної транзакції структуровано зберігається у блоках, що пов'язуються із попереднім та наступними блоками, утворюючи ланцюг.

Тому, в блокчейн технологіях передбачено декілька механізмів та засобів захисту даних від зловмисного використання. Ці механізми покладено в сам принцип блокчейну, далі описані деякі з них.

Результати

Незмінна база[2]. Однією із ключових особливостей блокчейну є відсутність можливості змінювати або видаляти вже записані у ланцюг вузли, що впроваджує високий рівень захищеності. Таким чином, кожна спроба змінити транзакції буде заборонена мережею, що робить дані захищеними від несанкціонованого доступу.

Криптографія[2]. Записи в блокчейні захищені за допомогою криптографії. Учасники мережі мають власні закриті ключі, які призначаються транзакціям, які вони здійснюють, і діють як персональний цифровий підпис. Якщо запис змінюється, підпис стає недійсним, і однорангова мережа відразу дізнається, що щось трапилося. Раннє сповіщення має вирішальне значення для запобігання подальшій шкоді.

Використання хеш-функцій[3]. Дані будь-якої довжини, що містяться у блоках, зазвичай приводяться до унікальної строки із визначеною кількістю символів. Існує багато алгоритмів хешування, наприклад MD5, SHA1, SHA-256, Keccak-256 та інші, кожен з яких відрізняється послідовністю та складністю, через що одні алгоритми є більш підтвердженими до зламу, ніж інші.

Механізм консенсусу[4]. Щоб транзакція була додана до блокчейну, учасники мережі повинні погодитися, що це єдина версія істини. Це робиться через консенсус, що означає згоду. Наприклад у Біткоїні, що є публічним блокчейном, консенсус досягається за допомогою «майнінгу» – вирішення складної криптографічної задачі. У приватних блокчейнах консенсус досягається за допомогою вибіркового схвалення – процес, коли користувачі із відповідними доступами та дозволами перевіряють транзакції.

Мнемонічні фрази. Для захисту доступу до особистих даних користувачів у блокчейні активно використовуються мнемонічні фрази, які є приватними ключами учасників ланцюгів. Такі ключі генеруються на основі двійкового коду, і щоб зробити запам'ятовування простішим та безпечнішими для всіх користувачів, була розроблена стандартна система BIP39, із врахуванням безпеки.

Висновки

Блокчейн технології мають достатню кількість ефективних вбудованих принципів захисту інформації від зловмисного втручання та використання даних як на рівні самих ланцюгів, так і на рівні користувачів. Використання технології дозволить суттєво прискорити різні конфіденційні користувальницькі операції та зробити їх більш прозорими, скоротити витрати на надання та зберігання паперових документів, а також зменшити ризики фальсифікації та втрати документів. Проте, досить велика роль у безпеці транзакцій все ще покладається на користувачів, що призводить до потреби кращого ознайомлення користувачів із більш поглибленими правилами безпеки у блокчейнах.

Список використаних джерел

1. Blockchain Facts: What It Is How It Works, and How It Can Be Used. URL: https://www.investopedia.com/terms/b/blockchain.asp#toc-what-is-a-blockchain

2. Blockchain security: What keeps your transaction data safe? URL: https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/

3. Blockchain Security Mechanisms. URL: https://towardsdatascience.com/mechanisms-securing-blockchain-data-9e762513ae28

4. Yadav, S.P. (2022). Blockchain Security. In: Baalamurugan, K., Kumar, S.R., Kumar, A., Kumar, V., Padmanaban, S. (eds) Blockchain Security in Cloud Computing. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-70501-5_1

УДК 004.9

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Хлищиборщ П.О.
Національний авіаційній університет, Київ

Науковий керівник –Артамонов Є.Б., д.т.н., доц.

Ключові слова: штучний інтелект, розробка, програмне забезпечення.

Вступ

Використання штучного інтелекту як інструменту розробки програмного забезпечення є актуальною з багатьох причин. Використання штучного інтелекту може допомогти покращити швидкість та якість розробки, зменшити витрати та знизити ризик помилок в програмному забезпеченні. Зростає попит на інноваційні технології в програмному забезпеченні, які можуть забезпечувати більш ефективні, автоматизовані та інтелектуальні процеси розробки. Штучний інтелект вже успішно використовується в багатьох інших сферах, таких як медицина, фінанси та індустрія. Тому дослідження та розробка нових методів та технологій використання штучного інтелекту в розробці програмного забезпечення може допомогти зробити цей процес ще більш ефективним та інноваційним.

Матеріали і методи

Для досягнення наукового обґрунтування користі використання штучного інтелекту як інструменту розробки було обрано декілька методів дослідження, а саме спостереження: для спостереження за розробкою програмного забезпечення, щоб оцінити ефективність використання штучного інтелекту та виявити можливі проблеми, моделювання: моделювання процесу розробки програмного забезпечення з використанням штучного інтелекту для оцінки ефективності та можливостей використання штучного інтелекту у різних умовах, та контент-аналіз: контент-аналіз документації та програмного коду, щоб визначити, як саме використовується штучний інтелект в розробці програмного забезпечення, які інструменти використовуються та які результати досягаються.

Результати

Однією з головних переваг використання штучного інтелекту в розробці програмного забезпечення є зменшення витрат на розробку та тестування програмного забезпечення. Завдяки використанню штучного інтелекту можливо автоматизувати багато процесів розробки, що дозволяє знизити кількість ручної роботи та скоротити час, потрібний на розробку програмного забезпечення. За допомогою штучного інтелекту можливо забезпечити більш точне та швидке тестування програмного забезпечення, а також покращити процес відлагодження та оптимізації коду.[1] Це дозволяє збільшити якість програмного забезпечення

та зменшити ризик виявлення помилок після його релізу. ШІ може використовуватися для автоматичної генерації коду, створення тестових наборів або навіть для розпізнавання образів, що дозволяє прискорити процес розробки та збільшити продуктивність розробників. Через використання штучного інтелекту може бути досягнуто покращення управління процесом розробки програмного забезпечення, інструменти штучного інтелекту можуть допомогти управляти складністю та ризиками проекту, забезпечуючи оптимальне розподілення ресурсів, визначення завдань та контроль за їх виконанням. Це дозволяє розробникам більш ефективно управляти розробкою проекту, скоротити строк розробки та забезпечити високу якість програмного забезпечення. Ще однією перевагою є можливість використання розумних алгоритмів, які можуть допомогти забезпечити оптимальну проектну архітектуру, забезпечити більш точну оцінку ризиків та прогнозування можливих проблем. ШІ може використовуватися для аналізу даних про роботу програмного забезпечення та розпізнавання проблем в режимі реального часу. Це дозволяє розробникам швидко виявляти та усувати проблеми, зменшувати час, потрібний на підтримку програмного забезпечення та забезпечувати більш високу задоволеність користувачів. Однак, варто зауважити, що використання штучного інтелекту також може мати свої обмеження та проблеми. Однією з таких проблем є необхідність висококваліфікованих фахівців для розробки та впровадження штучного інтелекту в процес розробки ПЗ. Крім того, забезпечення безпеки та захисту даних може бути складною задачею у разі використання штучного інтелекту в розробки ПЗ. Також слід зазначити, що використання штучного інтелекту в розробці програмного забезпечення є досить новим підходом, тому може виникати необхідність у додаткових дослідженнях та розробці нових методів для ефективного впровадження штучного інтелекту в процес розробки ПЗ.

Висновки

Отже, використання штучного інтелекту як інструменту розробки програмного забезпечення дозволяє забезпечити ряд переваг, таких як зменшення витрат на розробку та тестування, покращення якості та ефективності процесу розробки, автоматизація деяких процесів розробки, більш гнучкий та адаптивний процес розробки, покращення управління процесом розробки та підтримки програмного забезпечення, використання розумних алгоритмів та забезпечення більш ефективної підтримки ПЗ.

Список використаних джерел

1. How Artificial Intelligence and Machine Learning are Revolutionizing Software Development. URL: https://www.computer.org/publications/technews/trends/ai-is-changing-software-development (Last accessed:20.03.2023).

УДК 004.056

ПІДСИСТЕМА ДЛЯ ОРГАНІЗАЦІЇ НАУКОВИХ ОНЛАЙН-КОНФЕРЕНЦІЙ

Ангеліна Цезар

Національний авіаційній університет, Київ

Науковий керівник – Олександр Мороз, д.т.н., доц.

Ключові слова: конференція, веб-застосунок, розробка

Вступ

В даний час наукові онлайн-конференції стали основним способом спілкування та обміну інформацією в науковому співтоваристві [1]. Ці конференції дозволяють людям з різних куточків світу спілкуватися та обмінюватися ідеями, що має вирішальне значення для прогресу науки. Варто зазначити, що через нинішню ситуацію в Україні, а раніше через обмеження щодо COVID-19 науковці з України та інших країн можуть брати участь лише в онлайн-конференціях [2]. Для багатьох людей вкрай важливо продовжувати свою наукову діяльність в безпечних і комфортних умовах, що спонукає до переведення офлайн-конференцій в онлайн формат.

Матеріали та методи

Проаналізувавши сайти із подібною специфікою, можна побачити наступні проблеми: вони зосереджені виключно на наданні інформації про конкретну конференцію, через що потенційним доповідачам важко відшукати конференції, які відповідають їх інтересам; відсутність інтерактивних елементів, тобто вони несуть лише лише інформативний характер.

Методологією розробки програмного забезпечення, яка використовується в цьому проекті, є модель прототипування. Це методологія, за якою прототип створюється, тестується, а потім переробляється за необхідності, доки нарешті не буде досягнуто прийнятний прототип, на основі якого можна розробити повну систему або продукт [3].

Результати

Розробка веб-застосунку проведена на основі мови програмування JavaScript разом із фреймворком React та наступними бібліотеками: firebase для керування базою даних, react-loading-skeleton для відображення візуальної індикації про завантаження вмісту сторінки, react-router-dom для навігації між сторінками.

Пропоноване рішення для вирішення вищезазначених проблем включає впровадження таких заходів:

- Включення інтерактивних елементів: форми реєстрації та входу з перевіркою коректності введених даних, а також модальне вікно, яке дозволяє користувачам надсилати заявки електронною поштою з попередньо заповненими полями одержувачів і темою.

- Відображення карток конференції зі стислою інформацією, такою як тема, короткий опис, дата та мова проведення.

- Надання більш детальної інформації про конференції на окремих сторінках, як-от дати розміщення матеріалів конференції на веб-сайті, терміни подання тез, вартість організаційного внеску, тематика конференції, описи та контактна інформація організаторів, включаючи їх ПІБ, електронну адресу і веб-сайт.

- Додати на кожну сторінку модальне вікно з інструкціями щодо подання та оформлення тез, зразком їх оформлення та прикладом сертифікату, який можна отримати за участь у конференції.

- Щоб збільшити залучення доповідачів і викликати інтерес до інших конференцій, додати відповідні рекомендації у кінці кожної сторінки.

Висновки

Запропонований підхід робить веб-застосунок більш зручним та інформативним для відвідувачів шляхом додавання інтерактивних елементів, надання детальних відомостей та рекомендії інших конференцій, що призводять до зростання інтересу до участі у них.

Список використаних джерел:

1. Maria sá Virtual and Face-To-Face Academic Conferences: Comparison and Potentials – 2019

2. Agata Kopacz, Anna Knapińska, Adam Müller, Grzegorz Banerski, Zbigniew Bohdanowicz Remote Scientific Conferences After the COVID-19 Pandemic: The Need for Socialization Drives Preferences for Virtual Reality Meetings – 2022

3. F. Cheng, “Basic App Structure,” Build Mobile Apps with Ionic 2 and Firebase, с. 47–55 – 2017 [Електронний ресурс]. URL: https://doi.org/10.1007/978-1-4842-2737-4_3.

УДК 004.056.5

КІБЕРБЕЗПЕКА ЯК КРИТИЧНИЙ ФАКТОР У ПРОТИДІЇ ЗАГРОЗАМ В ОНЛАЙН СЕРЕДОВИЩІ ПІД ЧАС ВІЙНИ В УКРАЇНІ

Владислав Швець, Альона Цапенко

Національний авіаційній університет, Київ

Науковий керівник – Бурбела О. О., асистент

Ключові слова: кібербезпека, загрози, онлайн середовище, дизінформація.

Вступ

У сучасних умовах кібербезпека стала надзвичайно актуальною, особливо у контексті ведення війни в онлайн середовищі. Кібербезпека є критичним фактором в протидії загрозам, які можуть виникнути в онлайн просторі України в період війни. Отож, визначення можливих загроз, методів їх усунення та шляхів покращення сервісу кібербезпеки в Україні є першочерговою умовою створення та підтримання безпечного онлайн середовища.

Матеріали та методи

Об’єктом дослідження став рівень забезпечення кібербезпеки онлайн простору України під час війни. Метою даної статті є дослідження стану та перспектив розвитку даної галузі. Для наукового обґрунтування результатів дослідження було використано метод аналізу ринку та метод узагальнення.

Результати

Загрози кібербезпеці під час війни:

У період війни в онлайн середовищі в Україні можуть виникати різноманітні загрози. Одна з таких загроз - це кібератаки. Кібератаки можуть бути спрямовані на критичну інфраструктуру, таку як електростанції, водні ресурси, телекомунікаційні системи та інші системи, які є ключовими для функціонування держави. Інша загроза полягає в поширенні дезінформації. Дезінформація може бути використана для маніпулювання громадською думкою та підірвання довіри до державних інституцій. Це може призвести до порушення стабільності країни та зростання соціальних напружень.

Методи усунення загроз:

Для протидії загрозам в онлайн середовищі України у період війни необхідно вживати заходів щодо кібербезпеки. Серед цих заходів можна відзначити:

1. Впровадження міцних заходів безпеки для критичних систем. Ці заходи можуть включати в себе встановлення брандмауерів, шифрування даних та систем аутентифікації, що допоможуть захистити системи від несанкціонованого доступу.

2. Підвищення освіти та усвідомлення важливості кібербезпеки серед користувачів. У багатьох випадках, найбільшу загрозу для безпеки систем становлять самі користувачі, які не дотримуються основних правил кібербезпеки, наприклад, використовують слабкі паролі або не оновлюють своє програмне забезпечення. Тому, підвищення рівня кібербезпеки включає в себе популяризацію основних правил безпеки та надання користувачам наочних прикладів.

3. Розроблення та впровадження стратегії кібербезпеки на державному рівні. Відповідальними за кібербезпеку є не тільки кожен окремий користувач, але й держава. Українська держава вже прийняла законодавчі акти та стратегії з кібербезпеки, однак, необхідно продовжувати розвивати та вдосконалювати ці стратегії відповідно до сучасних викликів.

4. Для забезпечення кібербезпеки у період війни, важливо підтримувати резервне копіювання даних та захист важливих інформаційних ресурсів. Це допоможе у разі втрати даних чи знищення систем, відновити роботу та уникнути серйозних наслідків для безпеки та ефективності діяльності.

Усі ці методи є лише декількома з численних шляхів удосконалення кібербезпеки у період війни. Важливо зрозуміти, що кібербезпека є невід'ємною складовою військової стратегії та потребує постійного вдосконалення та оновлення. Крім того, важливо пам'ятати про значення освіти та підвищення кваліфікації фахівців з кібербезпеки, а також про важливість взаємодії між усіма сторонами, які займаються кібербезпекою в Україні, включаючи військові, правоохоронні та громадські структури.

Висновок

Зважаючи на те, що загрози у онлайн середовищі надзвичайно швидко змінюються та зростають у розмірах та складності, важливо постійно оновлювати знання та вміння у цій галузі. Організації повинні постійно моніторити свої кіберзаходи та забезпечувати своєчасну реакцію на будь-які нові загрози. У цьому контексті важливо відзначити, що кібербезпека має стати однією з найважливіших тем у військовому та громадському дискурсі в Україні.

Список використаних джерел

1. Концепція національної стратегії кібербезпеки України на період до 2022 року. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21. Дата доступу: 20.03.2023

2. Національний центр кібербезпеки. URL:https://www.rnbo.gov.ua/ua/Diialnist/4658.html. Дата доступу: 22.03.2023

3. Закон про кібербезпеку та стратегія кібербезпеки України URL:https://uz.ligazakon.ua/ua/magazine_article/EA010553. Дата доступу: 21.03.2023.

УДК 004.056.53(043.2)

ПОШУК НАЙКРАЩОЇ ПРОТИДІЇ ЗАГРОЗАМ У ПРОСТОРІ ІНТЕРНЕТУ.

Олександр Шумбар

Національний авіаційній університет, Київ

Науковий керівник – Валерій Козловський, д.т.н., доц.

Ключові слова: антивірус, сканування, загрози.

Вступ

Темою даної роботи є створення сайту для швидкого пошуку виду і видалення вірусу, для людей, які не мають певного досвіду щодо користування комп’ютером.

Матеріали та методи

Актуальність даної теми пов’язана зі зростанням кількості різновидів вірусів в Інтернеті. Кожен день дуже велике число ПК починає ”глючити”, ”тормозити”. Користувачі починають нервувати: ”Як зробити так, щоб персональний комп'ютер почав плавно працювати”, ”Там же стільки потрібної інформації”. Саме для них і був створений даний сайт.

Покоління Х потребує більш детального роз’яснення щодо користування персональним комп’ютером, одним з яких – є захист ПК від вірусів.

Суспільство на теперішньому етапі розвитку потребує прийняття комплексних (з урахуванням багатьох критеріїв) рішень для розв’язання складних проблем, які щоденно виникають при роботі з різними сайтами інтернету. Рішення, що ґрунтуються на виклику майстра по обслуговуванню комп’ютера в багатьох випадках вже не влаштовують практику. Люди часто застосовують методи автоматизації наведення порядку на персональному комп’ютері, використовуючи при цьому різне програмне забезпечення.

Результати

Завданням і результатом даної роботи є сайт створений за допомогою тегів HTML, який легко та швидко допомагає знаходити, розрізняти та приймати рішення про знешкодження різних видів вірусів в пам’яті комп’ютера.

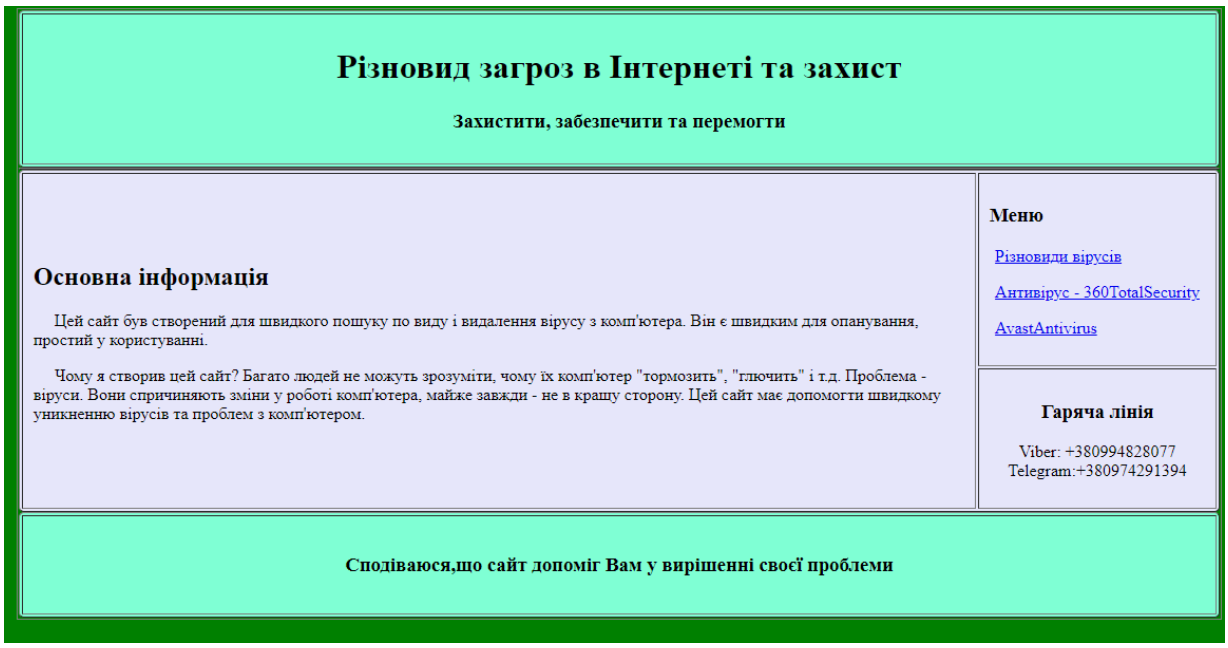

Рис 1. Зовнішній вигляд сайту.

Висновок

Створений сайт «Різновиди загроз в інтернеті» можна використовувати як для обслуговування власного комп’ютера так і для проведення занять з інформатики при вивченні теми «Основи інформаційної безпеки».

Список використаних джерел

1. Концепція національної стратегії кібербезпеки України на період до 2022 року. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21. Дата доступу: 20.03.2023
2. Національний центр кібербезпеки. URL:https://www.rnbo.gov.ua/ua/Diialnist/4658.html. Дата доступу: 22.03.2023
3. Закон про кібербезпеку та стратегія кібербезпеки України URL:https://uz.ligazakon.ua/ua/magazine_article/EA010553. Дата доступу: 21.03.2023.

Scientific publication

POLIT.
Challenges of science today
CYBER SECURITY AND SOFTWARE ENGINEERING

Abstracts of
XXIII International
conference of higher education students
and young scientists

Kyiv, 4-7 April 2023
Published in the author's edition

Наукова публікація

ПОЛІТ.
СУЧАСНІ ПРОБЛЕМИ НАУКИ
КІБЕРБЕЗПЕКА ТА ПРОГРАМНА ІНЖЕНЕРІЯ

Тези доповідей
XXIII Міжнародної
науково-практичної конференції здобувачів
вищої освіти і молодих учених

Київ, 4-7 квітня 2023
Публікується у авторській редакції

Підп. до друку 10.06.2023. Електронне видання.
Формат 60x84/16. Видавець і виготівник
Національний авіаційний університет 03058. Київ – 58, проспект Любомира Гузара, 1
Свідоцтво про внесення до Державного реєстру України суб'єктів видавничої справи ДК № 977 від 05.07.2002