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

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Всеукраїнської науково-практичної конференції
молодих учених, студентів і курсантів

27 листопада 2020 року

Львів – 2020

ББК 32.81+78.362

*Інформаційна безпека та Інформаційні технології: з*бірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с.

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

Секція 1
КІБЕРБЕЗПЕКА

Напрям 1

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

УДК 004.056.5

INFORMATION SECURITY OF UKRAINE: MODERN ASPECTS

Близняк Д., Запотічна Р.
Львівський державний університет внутрішніх справ, м. Львів

Досліджено проблему інформаційної безпеки України та захисту національного інформаційного простору від негативних пропагандистсько-маніпулятивних інформаційних впливів. Проаналізовано теоретичні підходи до визначення сутності поняття інформаційна безпека. Розглянуто дії щодо вдосконалення державної інформаційної політики та створення ефективної системи інформаційної безпеки України.

Ключові слова: *інформаційна безпека, інформаційні загрози, інформаційний простір, кіберзлочинність, кіберпростір.*

The problem of information security of Ukraine and protection of the national information space from negative propaganda and manipulative information influences is investigated. Theoretical approaches to defining the essence of the concept of information security are analyzed. Actions to improve the state information policy and creation of an effective information security system of Ukraine are considered.

Key words: *information security, information threats, information space, cybercrime, cyberspace.*

The paper is aimed at analyzing different requirements to handle information threats, as well as exploring important security measures related to providing information security of Ukraine.

In today's global and regional information confrontation, destructive communicative influences, multi-vector collisions, national information interests, dissemination information expansion and aggression, protection of the national information space and guarantee information security is becoming a priority strategic task of modern states in the system of global information relations. Preservation information sovereignty, the formation of an effective security system in the information field is an urgent problem for Ukraine, which is often the case for external information expansion, manipulative propaganda technology and destructive information invasion [3].

In terms of the Russian-Ukrainian conflict protecting the national information space from negative information-psychological influences, operations and wars, guaranteeing information security and information sovereignty are of

particular importance and become a factor in preserving Ukraine's national identity and operating it as a sovereign and an independent state.

There are two aspects of interpreting information security in the context of national security. On the other hand, information security is regarded as an independent element of national security of any country, and on the other hand, an integrated component of any other security: military, economic, political, etc. [1, p. 23].

The most complete is the following definition: informational security is a state of vitality interests of the individual, society and the state in which minimizes the risk of damage through incomplete, untimely and unreliable information, negative information impact, negative consequences of information technology functioning [5]. This definition is optimal and reflects all aspects of interaction among subjects of information relations.

Ukraine's information sovereignty means Ukraine's exclusive power under the Constitution of Ukraine, Ukrainian legislation and the rules of international law to individually and independently identify and implement national and geopolitical information interests, domestic and foreign information policy, dispose own information resources, build an infrastructure of the national information space, pave the way for integrating it into a global information space and ensure the national information security.

Information infrastructure means organizational structures and systems in their entirety providing for the functioning and development of the information space, means of information exchange and user access to information resources. Provision of information security means the activity aimed at prevention, timely identification, removal or neutralization of real and potential threats to Ukraine's information security.

Cyber security means security of vital interests of an individual, citizen, society and the state in the cyberspace. Cyberspace means the environment, which emerges due to information (automated), telecommunication and information and telecommunication systems operating based on the unified principles and common rules.

Cybercrime means an act in the cyberspace, which is socially dangerous and punishable under applicable criminal laws of Ukraine [2, p. 45]. The level of information security of the state is largely determined by the level of its information security infrastructure. Unfortunately, as V. Petryk points out, low overall level of information infrastructure of Ukraine contributes to expansion of information services market by foreign companies, which creates favorable conditions for the redistribution of airtime in favor of foreign programs, some of which clog up the Ukrainian information space with their own vision of events, promote lifestyle and traditions, thus destructively affecting society and the state, destroying the moral and ethical fundamentals of the gene pool of the Ukrainian nation.

Insufficient professional, intellectual and creative level domestic producer of information product and services, its uncompetitiveness not only on the world

market, but also in Ukraine, leads to the situation, when the Ukrainian audience naturally prefers foreign information programs.

Therefore, the national information space unfortunately, Ukraine is facing significant threats, challenges, which endanger the functioning of the state, its political and economic development, integration into the European and Euro-Atlantic structures. Threats to the national security of Ukraine in information sphere is a set of conditions and factors that threaten the vital interests of the state, society and the individual through possibility of negative information influence on awareness and behavior of citizens as well as on information resources and information technology infrastructure [4].

The National Cybersecurity Strategy is a document that defines strategic objectives and high-level action plans for ensuring the cybersecurity of Ukraine. The main goal of the Strategy is to establish the conditions necessary for ensuring the safe use of cyberspace by individuals, society and the government. To achieve that goal, Ukraine should establish a robust national system of cybersecurity, enhance capabilities across public security and defence sectors and ensure the cybersecurity of the state government information resources and critical information infrastructure.

To conclude, in today's globalized information a society where cyberspace is turning into a field the fight against major threats to information security states (and Ukraine, in particular) are cybercrime, cyberterrorism, cyberwarfare, which imply confronting national interests in Internet usage, computer and Internet technologies to harm the enemy. Most often cyber warfare, cyberterrorism technologies are focused on the sphere of state security and defense and pose a real threat to sovereignty of the state.

Інформаційні джерела

1. Bondarenko V. 2011. Information security of the modern states: conceptual reflections [Electronic resource]. - Access mode: http://www.crime-research.iatp.org.ua/library/strateg.htm

2. Doktryna informatsiinoi bezpeky Ukrainy [Electronic resource]. - Access mode: http://www. zakon3.rada.gov.ua/laws/show/514/2009

3. Zakhyst informatsiinoi bezpeky yak funktsiia derzhavy [Electronic resource]. - Access mode: http://www.mego.info/material/23-zakhystinformatsiinoi-bezpeky-iakfunktsiia-derzhavy

4. Kontseptsiia natsionalnoi bezpeky Ukrainy [Electronic resource]. - Access mode: http://www.w1.c1. rada.gov.ua/pls/zweb2/webproc4_1

5. Kormych B. 2017. Orhanizatsiino-pravovi zasady polityky informatsiinoi bezpeky Ukrainy [Tekst]: monohrafiia. Yurydychna literatura. – 471 s.

УДК 004.056.5

CULTURAL ASPECTS OF INFORMATION SYSTEMS SECURITY

Кушнір Л., Запотічна Р.
Львівський державний університет внутрішніх справ, м. Львів

У тезах розглянуто базові теоретичні засади поняття інформаційної безпеки. Встановлено причини, які зумовили сповільнення розвитку системи захисту інформаційних систем. Зроблено висновок про важливість впливу культурних аспектів на впровадження та розвиток механізмів забезпечення інформаційної безпеки.
Ключові слова: *інформаційна безпека, інформаційні трансакції, культура.*

The basic theoretical foundations of the concept of information security are considered. The reasons that led to the slowdown in the development of information systems protection system are identified. The importance of the influence of cultural aspects on the implementation and development of mechanisms for information security is emphasized.
Key words: *information security, information transactions, culture.*

The following paper is aimed at identification of the reasons behind the lack of information systems security deployments in the developing countries. The main objective of the research is to understand the cultural factors which may impact development and implementation of information security governance.

This paper is based upon the argument that in order to achieve fully effective information security management strategy, it is essential to look at information security in a socio-technical context, i.e. the cultural, ethical, moral, legal dimensions, tools, devices and techniques.

The motivation for this study originated from the concern of social chaos, which results from ineffective information security practices in organisations in the developing nations.

Services such as registration of birth and death, issue of passport, registration of marriage, collection of tax, registration of voters, payroll, and public finance amongst others have been computerized or are under active considerations for automation. Securing these services has become a vital function within the information system governance establishments.

Information Security Culture includes all socio-cultural measures that support technical security methods, so that information security becomes a natural aspect in the daily activity of every employee. To apply these socio-cultural measures in an effective and efficient way, certain management models and tools are needed.

According to CNSS, information security is «the protection of information and information systems from unauthorized access, use, disclosure, disruption,

modification, or destruction in order to provide confidentiality, integrity, and availability» [2, p. 37].

Information security has extended to include several research directions like user authentication and authorization, network security, hardware security, software security, and data cryptography. Information security has become a crucial need for protecting almost all information transaction applications.

Public and private organizations are facing a wide range of information threats. Information security is a crucial component in their information systems. With their increasing reliance on technologies connected over open data networks, effective management of information security has become one of the most crucial success factors for public and private organizations alike [5, p. 484].

Globally information security best practices and trends are similar. When it comes to applying these best practice approaches to specific applications, however, localized variables and limitations need to be emphasized. This is the case when we consider the application of generic best practices to a specific country, particularly a country which may be considered as still developing technologically [1].

Cultural issues impact the governance of information security. This paper is based upon the argument that in order to achieve fully effective information security management strategy, it is essential to look at information security in cultural context, i.e. ethical, moral, legal dimensions, tools, devices and techniques. Developing countries are those countries which are in a process of industrialization but have limited resources. There are several unsolved issues related with efficient information security governance in the developing countries such as voter registration, voting, passport, national identity, financial records and education records.

As mentioned by H. Shaaban, many developing countries are in an early stage of adopting information systems in their government institutions. The adoption of information systems faces many challenges in many developing countries such as lack of skilled personnel, financial constraint, national culture, and inferior infrastructures among others. Training and awareness in information security is expensive, and there is a challenge in its delivery. In the literature, it has been reported that cultural aspects, management support, budgetary constraints, lack of national level information security policies and guidelines, and lack of motivation to employees are hindrances to information security awareness initiatives in organizations.

Many developing countries lack a necessary legal framework at the national level for digital information security, or they are at the development stage for legislation that protect e-commerce. There is weak law enforcement in many developing countries on crimes against information systems. This is due to lack of skills by law enforcement agencies on these types of crimes, corruption and lack of proper legislation [4, p. 12].

The Global Leadership and Organisational Behaviour Effectiveness Project defines culture as «shared motives, values, beliefs, identities, and interpretations or meanings of significant events that result from common experiences of members of collectives that are transmitted across generations». T. Schlienger and S. Teufel define information security culture as «all socio-cultural measures that support technical activity methods, so that information security becomes a natural aspect in the daily activity of every employee». In order for security culture to make a substantial contribution to the field of information security, it is necessary to have a set of methods for its study. Unfortunately, no unique toolset and method for the study of organizational and therefore security culture exists. Research is therefore still needed in this field [3, p.1]. Several studies found in the literature investigated information security culture in organizations and concluded that organizations must stress the idea that information security is the responsibility of every member [4, p. 46].

In conclusion, national culture influences the adoption of and how people in certain societies view their responsibilities, interact and convey their feelings. Many developing countries have imported information systems innovation from developed countries. Importation of information systems forces developing countries to adopt ideas that are not appropriate to their local context. In low context cultures, most of the information is contained in the message itself in an explicit and detailed way. On the other hand, in high context culture, less explicit and detailed information is carried in the message itself and inferences are drawn from implicit information. It is accepted that communication is an important facet of information security management and effective communication between IT, management and users is challenging enough to achieve in organizations even though the culture is relatively homogeneous. Consequently, in high context cultures, communication tends to be a key issue related to information security.

Інформаційні джерела

1. Alfawaz S., May L., Mohanak K. 2008. E-government security in developing countries: A managerial conceptual framework. E-government and Institutional Change Journals, 2-5

2. CNSS. 2010. National Information Assurance Glossary. URL: http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

3. Schlienger T., Teufel S. 2003. Information Security Culture – from Analysis to Change. South African Computer Journal, 31.

4. Shaaban H. 2014. Enhancing the Governance of Information Security in Developing Countries: The Case of Zanzibar. URL: https://core.ac.uk/download/pdf/29821757.pdf

5. Wang J. 2009. E-government Security Management: Key Factors and Countermeasure. Fifth International Conference on Information Assurance and Security, pp. 483-486.

УДК 65.012.8

РОЗРОБЛЕННЯ МЕТОДУ МОДЕЛЮВАННЯ Й ОЦІНКИ ОРГАНІЗАЦІЙНОЇ ПРИХИЛЬНОСТІ ПЕРСОНАЛУ

Явин Х., Кухарська Н.
Львівський державний університет безпеки життєдіяльності, м. Львів

Розроблено метод і багатофакторну адитивну модель оцінки надійності персоналу, застосування яких дасть змогу організаціям підвищити їх рівень інформаційної безпеки.

Ключові слова: *інформаційна безпека, оцінка надійності персоналу, адитивна модель.*

A method and a multifactor additive model for assessing staff reliability have been created. Their using can help the organization to increase the level of information security.

Key words: *information security, personnel reliability assessment, additive model.*

Як показують результати досліджень, що проводяться щорічно Експертно-аналітичним центром InfoWatch починаючи з 2004 року, однією з основних загроз інформаційної безпеки організацій є внутрішні порушники. Більше половини випадків (від 53 % до 73 % у різні роки) розкрадання інформації і незаконного доступу до інформаційних систем відбувалося за участю працівників організацій (включаючи керівництво) [1].

Характерними ознаками внутрішніх порушників є наявність правомірного (законного, санкціонованого) доступу до інформації, необхідність знати і дотримуватися правил обробки інформації обмеженого доступу, юридичний зв'язок (трудовий договір, угода на надання послуг) з організацією, що обробляє інформацію обмеженого доступу (тобто договірні відносини з власником або оператором інформації).

З огляду на актуальність проблеми забезпечення внутрішньої безпеки організацій та інформаційної безпеки як її складової частини, беручи до уваги недоліки існуючих методів і моделей, пропонується використовувати багатофакторну адитивну модель оцінки персоналу, яка будується на основі оцінок надійності працівників за трьома напрямками: оцінки рівня їх обізнаності щодо питань захисту інформації; оцінки рівня організаційної прихильності шляхом врахування суб'єктивно-психологічних і об'єктивних факторів і оцінки активності працівників в інформаційній системі організації. Застосування такої моделі дасть змогу підвищити ймовірність раннього виявлення потенційних і діючих інсайдерів, що позитивно позначиться на забезпеченні інформаційної безпеки, і, як наслідок, дозволить знизити збитки від шкідливого інсайда. Модель можна легко адапту-

вати під національні, етнічні, галузеві особливості, а також під специфічні особливості конкретної організації чи колективу.

Розроблену модель, складові її частини та інформацію накопичену в ході її застосування можна використовувати не тільки за прямим призначенням, а й для вирішення суміжних завдань. А саме:

1. Статистична інформація і досвід, накопичені у процесі застосування моделі, можуть бути використані для оптимізації процесів навчання працівників нормам та заходам інформаційної безпеки та атестування рівня їхньої підготовки.

2. Модель дає можливість порівнювати оцінки по суб'єктивних та об'єктивних факторах для того, аби прогнозувати зміни організаційної прихильності та надійності персоналу із зміною об'єктивних факторів.

3. Модель оцінки інформаційної активності працівників в інформаційній системі організації може бути використана не тільки для пошуку внутрішніх порушників, а й для виявлення працівників, що використовують службову техніку в особистих цілях.

Інформаційні джерела

1. Утечки данных организаций по вине или неосторожности внутреннего нарушителя. Сравнительное исследование 2013-2019 гг. Аналитический отчет Экспертно-аналитического центра InfoWatch. 2020.

ОСОБЛИВОСТІ СТАНУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ У КІБЕРПРОСТОРІ

Гончарова Д., Навитка М.
Львівський державний університет безпеки життєдіяльності, м. Львів

Вперше про зовнішні кіберзагрози в Україні заговорили після Революції гідності, позначивши новий фронт гібридної війни з російським агресором. Основу національної системи кібербезпеки становлять Міністерство оборони, Державна служба спеціального зв'язку та захисту інформації, Служба безпеки, Національна поліція, Національний банк і розвідувальні органи.

В даній статті проведено аналіз особливості стану критичної інфраструктури України у кіберпросторі. Сформульовано наслідки кібератак на об'єкти критичної інфаструктури і наведено джерела можливих кіберзагроз, які діють в інформаційному просторі.

Ключові слова: *критична інфраструктура, кібрзагрози, кібербезпека, кіберзлочинність.*

For the first time, external cyber threats in Ukraine were discussed after the Revolution of Dignity, marking a new front of the hybrid war with the Russian aggressor. The national cybersecurity system is based on the Ministry of Defense, the State Service for Special Communications and Information Protection, the Security Service, the National Police, the National Bank, and intelligence agencies.

This article analyzes the peculiarities of the critical infrastructure of Ukraine in cyberspace. The consequences of cyber attacks on critical infrastructure are formulated and the sources of possible cyber threats operating in the information space are given.

Keywords: *critical infrastructure, cyber threats, cybersecurity, cybercrime.*

Критична інфраструктура – це комплекс об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості країни. Виведення їх з ладу або руйнування може мати вплив на національну безпеку і оборону, природне середовище, навіть призвести до значних фінансових збитків та людських жертв. В перелік попадають такі галузі, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство

Критичні об'єкти національної інформаційної інфраструктури України є складовою кіберпростору. Здійснення кібернетичних загроз може призвести до настання таких наслідків:

– надзвичайна ситуація;

– блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств чи систем життєзабезпечення та об'єктів підвищеної небезпеки;

– блокування роботи державних органів, органів місцевого самоврядування;

– блокування діяльності військових формувань, органів військового управління, Збройних Сил України в цілому, або втручання в автоматизовані системи керування зброєю;

– порушення безпечного функціонування банківської та/або фінансової системи держави;

– розголошення державної таємниці;

– масові заворушення.

Рівень кіберзагроз постійно зростає у всьому світі. Хоча кіберпростір штучний, ми вже живемо в ньому. І від цілісності цього простору напряму залежить якість нашого життя. Сьогодні жодна система не захищена від проникнення і не перебуває поза досяжністю злочинців. Ми повністю інтегровані в цей простір, і атака на нього за рівнем наслідків стає рівносильною атаці в фізичному просторі. Кібербезпека – це певні технології та процеси, які створюють та підтримують безпечну життєдіяльність цього простору. Візьмемо до уваги той факт, що зловмисники, які раніше оперували у доступному їм фізичному вимірі, сьогодні все активніше діють у кіберсвіті.

Через важкість наслідків потенційних кібератак на об'єкти критичної інфраструктури їхній захист прописаний у національних стратегіях з кібезбезпеки багатьох країн. Джерелами кібернетичних загроз можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій злочинці, іноземні державні органи, терористичні та екстремістські угруповання, транснаціональні корпорації та фінансово-промислові групи.

Зростає загроза використання проти інтересів України кібернетичних засобів як з середини держави, так і її меж. Реальною є загроза використання української інформаційної інфраструктури як "транзитного майданчику", щоб приховати атаки на інформаційну інфраструктуру третьої сторони. Джерелами кібернетичних загроз можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій злочинці, іноземні державні органи, терористичні та екстремістські угруповання, транснаціональні корпорації та фінансово-промислові групи.

Тільки тепер у всьому світі почали створювати стандарти захисту об'єктів критичної інфраструктури.. Інтеграція в кіберпростір прогресуватиме й надалі, в нього переходитиме все більше систем і функцій. Таким чином, щоб побудувати ефективну систему кібербезпеки об'єктів критичної інфраструктури, потрібно впроваджувати і координувати стандарти і сервіси в цій галузі, підвищувати безпеку в кіберпросторі, розробивши ефективні рішення безпеки та заходи щодо їх покращення. Треба пройти дуже довгий та нелегкий шлях, щоб захистити в кіберпросторі повноцінну роботу критичної інфраструктури України.

Інформаційні джерела

1. https://zakon.rada.gov.ua/

2. Internet privacy and security course [Електронний ресурс] // [вебсайт]- https://book.cyberyozh.com s/

3. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: Підручник. – К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.

4. https://sites.google.com/site/infobezosob/osnovni-principi-zabezpecenna-zahistu-informaciie

5. Грайворонський М. В. Безпека інформаційно-комунікаційних систем: підруч. для студ. вищ. навч. закл., які навчаються за напрямами "Безпека інформаційних і комунікаційних систем", "Системи технічного захисту інформації", "Управління інформаційною безпекою" / М. В. Грайворонський, О. М. Новіков. – К. : Вид-во BHV, 2009. – 608 с.

УДК: 004.6

МЕТОДОЛОГІЯ ТА ІНСТРУМЕНТАРІЙ OSINT, ЯК ФОРМИ КІБЕРНЕТИЧНОЇ РОЗВІДКИ

Ориник С., Ящук В.
Львівський державний університет безпеки життєдіяльнсті, м. Львів

Розкриваються питання використання методів та засобів розвідування на основі відкритих джерел. Зокрема, актуалізується питання ефективності використання OSINT-розвідки. Описано процес пошуку та дослідження інформації. Наведено пропозиції щодо використання аналітичних функцій OSINT у кібернетичній розвідці.

Ключові слова: *OSINT-розвідка, розвідування з відкритих джерел, кібернетична розвідка.*

Opening of nutritional support methods and methods of development on the basis of Open source intelligence. The nutritional efficiency of the OSINT distribution is updated. Described the process of making a joke and receiving information. Introduced the proposition of showing the analytical functions of OSINT in cybernetic development.

Key words: *OSINT-prompting, prompting from open source intelligence, cybernetic prompting.*

Розвідування на основі відкритих джерел є важливим напрямом розвідувальної діяльності. Одним з методів ведення технічної розвідки за допомогою моніторингу інформації з відкритих джерел, її аналізу, підготовки і своєчасного надання кінцевого продукту особі, що приймає рішення з метою вирішення певних розвідувальних завдань, є OSINT (Open source intelligence) - розвідка на основі відкритих джерел [1-3]. OSINT (Open source intelligence) – розвідка відкритих джерел – це специфічна інформація, зібрана й структурована особливим чином для відповіді на конкретні запитання.

Формування даного поняття відбувалося шляхом трансформації поняття «інформація з відкритих джерел» (open source information (OSIF)). У спрощеному варіанті, даний термін стосується інформації, що не має грифу «таємно». Це інформація, яку може отримати кожен законним шляхом через запит, купівлю чи спостереження. За різними джерелами 80-90% інформації необхідної для прийняття рішень отримується з відкритих джерел [2]. У сферу інтересів OSINT входить добування та аналіз офіційних документів, проектів статутів, відстеження нових наукових розробок, баз даних, комерційних і державних сайтів, мережевих щоденників тощо.

Розвідка на основі аналізу відкритих джерел інформації є однією з головних розвідувальних дисциплін, яка застосовується ще з часів Другої світової війни. До недавнього часу така розвідка перебувала на другорядних позиціях. Нестабільна військово-політична та фінансово-економічна

обстановка, нові загрози (різного характеру кризи, тероризм), стрімке збільшення інформаційного потоку, зростання ролі та цінності інформації як такої – все це стало причиною активізації зусиль [3]. Розвиток інформаційних технологій, програмних та апаратних засобів, доступність мережі Інтернет, збільшення інформаційного потоку відкритої інформації сприяли виведенню розвідки на базі відкритих джерел на належний рівень і зробили її ще більш актуальною та необхідною. Сьогодні OSINT-техніки почали вивчати і використовувати юристи, PR-фахівці та спеціалісти в інших сферах бізнесу, у тому числі в Україні. У 2015—2016 року реалізовано освітній проект OSINT Academy. В межах проекту проведено 25 тренінгів в 19 містах України, записано 20 відкритих відеоуроків про використання методик OSINT [4].

Джерела OSINT поділяються на категорії інформаційного потоку: ЗМІ, інтернет, державні дані (Public Government Data), професійні та академічні публікації (Professional and Academic Publications), комерційні дані (Commercial Data), сіра література (Grey literature). При визначенні термінології OSINT використовуються такі визначення: відкрите джерело - персона або група, яка надає інформацію без вимоги збереження її конфіденційності - інформація або відносини незахищені від публічного розкриття; загальнодоступна інформація - дані, факти, інструкції або інші матеріали, опубліковані чи розміщені для широкого використання; доступні для громадськості; законно побачені або почуті випадковими спостерігачами; представлені на відкритих зустрічах для громадськості.

В табл. 1 наведено інструменти та сервіси OSINT, які прискорять дослідження в мережі.

Таблиця 1

Інструментарій OSINT- розвідки [4]

Назва програми, сервісу або пошукової системи	**Функції**
OneLook, Keyword Tool, Answer the Public	допомагають визначити мету пошуку
Hash At It, Social Search	знаходять згадки запиту у всіх популярних соціальних мережах і не тільки
Watson News Explorer, News Now, All You Can Read	виконують швидкий пошук у новинах, з метою отримання інформації про тренди пошукової тематики
Selection Search, Infinite Scroll for Google	розширення, які прискорюють звичайний пошук
Google Dorks Google Hacking	техніка, яка використовується ЗМІ, слідчими органами, інженерами з безпеки і будь-якими користувачами для створення запитів в різних пошукових системах для виявлення прихованої інформації та вразливості, які можна виявити на загальнодоступних серверах.

Процес пошуку і оброблення інформації складається з декількох етапів. Перший етап полягає в постановці завдання - необхідно зрозуміти завдання, деконструювати аналітичну проблему. Другим етапом є планування - етап розробки плану збору інформації, що стосується проблеми. Ухвалюється рішення щодо того, що повинно бути перевірено та проаналізовано. Необхідно чітко сформулювати цілі і завдання. З метою виконання пошукових робіт обираються методи і засоби, які допоможуть ідентифікувати і отримати необхідну інформацію. Наступний етап включає аналіз і оцінювання ключових джерел і їх змісту. Аналіз - це ключовий фактор, без якого неможливо інтерпретувати великі обсяги даних. Збір інформації повинен бути цілеспрямованим [5]. Аналітичні функції OSINT включають контент-аналіз інформаційних матеріалів, перегляд результатів тематичної добірки у вигляді цитат (результати збору інформації в мережі Інтернет, статистичний аналіз джерел інформації що висвітлюють події.

Застосування OSINT-розвідки дозволяє отримати відповідь на багато питань, які виникають в особи, що приймає рішення, а також зосередити зусилля развідувальних органів на виконання більш складних і «вузьких» завдань. Технологія OSINT є однією з важливих технологій «глибинного збору» різнорівневої різноформатної інформації, а також формування на її базі принципово нових знань. Поширення і використання перевіреної інформації з відкритих джерел дозволяє здійснювати обмін такою інформацією, оскільки при її отриманні не використовуються приховані методи і секретні джерела.

Інформаційні джерела

1. Open Source Intelligence (OSINT): Issues for Congress. - [Електронний ресурс]. – Режим доступу: https://www.fas.org/sgp/crs/intel/RL34270.pdf

2. Кожушко О.О. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США .- [Електронний ресурс]. - Режим доступу: http://jrnl.nau.edu.ua/index.php/IMV/article/viewFile/3264/3217

3. Балуев Д.Г., Новоселов А.А. Анализ разведданных из открытых источников: Учебно-наглядное пособие. — Нижний Новгород: НИИ кризисных информационных систем, 2011. — 127 с.

4. Инструменты и сервисы для OSINT .- [Електронний ресурс]. - Режим доступу: http://uplink.motd.org/2017/04/osint-tools-and-service/.

5. Распознавание информационных операций / А. Г. Додонов, Д. В. Ланде, В. В. Цыганок, О. В. Андрейчук, С. В. Каденко, А. Н. Грайворонская. -К.: Инжиниринг, 2017. — 282 с.

УДК 004.6

СПОСОБИ ЗАХИСТУ ERP-СИСТЕМ

Сениш А., Полотай О.
Львівський державний університет безпеки життєдіяльнсті, м. Львів

В даній роботі виділені основні проблеми, які виникають в плані безпеки інформації при запровадженні покращеної системи корпоративної управління підприємством. Описано особливості ERP-систем, як способу інформатизація корпоративного управління за рахунок впровадження інформаційних технологій.

***Ключові слова**: управління, класи, зовнішні порушники, внутрішні порушники, IT-інфраструктура, компоненти, клієнт-серверна архітектура, основні аспекти безпеки.*

This paper highlights the main problems that arise in terms of information security in the implementation of an improved system of corporate governance. Features of ERP-systems as a way of informatization of corporate management due to introduction of information technologies are described.

***Key words:** management, classes, external violators, internal violators, IT infrastructure, components, client-server architecture, basic security aspects.*

В даний час вдосконалення корпоративного управління стає ключовим стратегічним завданням розвитку і життєдіяльності будь-якого підприємства. В силу того, що практично всі способи вдосконалення управління вичерпані, єдиним способом виживання в конкурентній боротьбі залишаються інтенсивні способи поліпшення управління.

Одним з таких способів є інформатизація корпоративного управління за рахунок впровадження інформаційних технологій, в тому числі систем класу ERP. Зростання систем обробки, зберігання інформації, а також величезна кількість впроваджуваних нових технологій з якими доводиться стикатися при забезпеченні інформаційної безпеки породжує велику кількість проблем. У зв'язку з цим важливу роль починає відігравати інформаційна безпека, оскільки вся інформація компанії знаходиться в цифровому вигляді. Тому життєво важливо захищати інформацію компанії як від зовнішніх, так і від внутрішніх порушників.

Основну роль в IT-інфраструктурі компанії відіграє ERP-система, яка практично допомагає керувати всіма бізнес процесами компанії, оскільки містить саму важливу бізнес інформацію. Головним механізмом захисту є розмежування повноваження користувачів в ERP-системі. Даний механізм дозволяє відповідно до бізнес ролей кожного співробітника дати йому повноваження по роботі з тією чи іншою інформацією. Це необхідно, оскільки на ринку величезна кількість конкурентів і від того, як працює фірма, як налаштовані її ролі в системі буде залежати її конкурентоспроможність.

Інформаційну безпеку необхідно забезпечити для всіх компонентів ERP-системи, тому розглянемо її архітектуру. Сучасна ERP-система скла-

дається з трьох компонентів, пов'язаних через клієнт-серверну архітектури. Виділяють такі рівні ERP-системи:

– рівень бази даних (БД);

– рівень додатків;

– рівень представлення (призначений для користувача).

Забезпечення в тій чи іншій мірі захищеності інформації можливо на кожному з цих рівнів. Вибір механізмів захисту інформації на вищевказаних рівнях ERP-системи залежить від специфіки конкретного проекту. Сполучним середовищем для компонентів, що знаходяться на різних архітектурних рівнях ERP, є мережева інфраструктура.

У підсумку, можна виділити наступні основні аспекти безпеки:

– мережева безпека;

– безпека БД;

– безпека на рівні сервера додатків;

– захист інформації на клієнтському комп'ютері.

ERP-системи обробляють велику кількість різних транзакцій і реалізують складні механізми, які надають різні рівні доступу різним користувачам.

Для забезпечення надійного захисту ERP-системи на сьогодні і в подальшому, у системі інформаційної безпеки повинні бути реалізовані найпрогресивніші технології. Основними положеннями щодо безпеки є:

– аналіз і дослідження причин порушення інформаційної безпеки;

– розробка результативних моделей безпеки які будуть відповідати сучасному розвитку апаратних і програмних засобів;

– створення методів і засобів коректного впровадження моделей безпеки в існуючі обчислювальні системи, з можливістю гнучкого управління, безпекою в залежності від висунутих вимог, допустимого ризику та витрати ресурсів;

– необхідність розробки засобів аналізу безпеки комп'ютерних систем за допомогою здійснення тестових впливів (атак).

Ролі та обов'язки персоналу щодо захисту інформації є ключем до успіху в будь-якій програмі забезпечення безпеки. Чітке визначення цих ролей і обов'язків необхідно і повинно бути закріплено на етапі впровадження ERP-системи.

Практично для будь-якої ERP, крім штатних засобів захисту інформації, як правило, потрібні додаткові програмні засоби, в тому числі криптографічні, і залучення сторонніх постачальників для виконання всіх вимог з інформаційної безпеки. Саме тому дослідження можливих рішень захисту ERP-системи на сьогоднішній день є актуальним питанням.

Інформаційні джерела

1. О'Лири Д. ERP-системы. Современное планирование и управление ресурсами предприятия. Выбор, внедрение, эксплуатация. М.: Вершина, 2014. 272с.

2. Егорова Г.В., Шляпкин А.В. Информационная безопасность ERP-систем// Информационные системы и технологии: управление и безопасность. 2013. №2. С.202-211.

3. https://uk.wikipedia.org/wiki/Планування_ресурсів_підприємства

4. Катрич Д. В., Бурлаков В. М. Захист інформації в ERP-системі підприємства // Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління» № 2’ (31) 2017

АНАЛІЗ ОПОРНИХ НАПРЯМКІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Редя М.-І[1], Навитка М.[2]

[1]Лапаївський ліцей імені Героя України Георгія Кірпи Зимноводівської ОТГ

[2]Львівський державний університет безпеки життєдіяльності, м. Львів

Інтенсивне впровадження новітніх інформаційних технологій, проникнення їх в усі сфери життєво важливих інтересів держави та суспільства зумовили появу низки суттєвих проблемних питань. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем.

В даній статті проведено аналіз актуальних кіберзагроз і напрямків забезпечення кібербезпеки. Сформульовано базові вимоги і рекомендації щодо забезпечення інформаційної та кібернетичної безпеки відповідно до діючих глобальних загроз в інформаційному просторі.

Ключові слова: *загрози, ризики, кібератака, кібербезпека, кіберзлочинність*

Intensive introduction of the latest information technologies, their penetration into all spheres of vital interests of the state and society have led to the emergence of a number of significant problems. The danger of unauthorized interference in the work of computer, information and telecommunication systems is intensifying.

This article analyzes current cyber threats and areas of cybersecurity. The basic requirements and recommendations for ensuring information and cyber security in accordance with the current global threats in the information space are formulated.

Key words: *threats, risks, cyber attack, cybersecurity, cybercrime*

Проблеми інформаційної безпеки України в сучасних умовах, принципи забезпечення захисту інформації є надзвичайно актуальними і вимагають поглибленого вивчення. На даний час стало дуже важко орієнтуватися у кібербезпеці. Навіть світові компанії з великою кількістю фахівців з кібербезпеки прикладають великі зусилля, щоб оцінити рівень загроз і спланувати адекватні заходи протидії їм. Зважаючи на реальність існуючих вимог в області кібербезпеки, потрібно вкластися в обмежений бюджет та вибудувати план стратегічних дій. При цьому, поетапно реалізуючи цей план, варто пам’ятати про вектор зовнішніх і внутрішніх загроз, який постійно змінюється,

Комплекс таких факторів, як тренди цілеспрямованих кібератак дозволить прогнозувати в перспективі неабияке зростання кількості успішно реалізованих зовнішніх і внутрішніх загроз, а, отже, збільшення катастрофічних масштабів наслідків від їх успішної реалізації.

Очевидно, що для світової економіки кіберзлочинність починає представляти серйозну небезпеку. Наприклад, для бізнесу постає надзвичайно важливе питання в забезпеченні безпеки своїх даних, так і даних працівників, користувачів та третіх сторін. Тому боротьба кіберзлочинністю повинна отримати першочерговий характер.

Мішенню більшості атак є вразливі додатки і операційні системи. Використовуючи останні оновлення, можна значно зменшити кількість можливих точок входу для хакера. При оновленні програмного забезпечення (ПЗ), його обов'язково завантажувати тільки з авторизованих сайтів розробників або постачальників. При цьому використовувати тільки спеціально визначені програми і блокувати всі інші, включаючи шкідливе програмне забезпечення.

Важливо підключити систему шифрування конфіденційної інформації. Це обмежить доступ до конфіденційної інформації користувачів з привілейованими правами. Також дозволить зменшити завдану шкоду від її втрати у разі успішної атаки.

Кіберзлочинці завжди націлені на отримання контролю над законними реєстраційними даними, особливо тими, які надають доступ до особливо цінної (конфіденційної) інформації. При обмеженні права доступу до рівня, який є небхідним виключно для цього користувача, потрібно відокремити адміністраторів і визначити їх права на окремому рівні, також обмеживши доступ до інших рівнів

Все впирається в необхідність вибудовування цілісної системи управління запобіганням кіберзагрозам. Вибудовування цілісної системи управління запобігання кіберзагрозам має проводитися на сучасній матеріальній базі та з залученням високо кваліфікованих фахівців.

Інформаційні джерела

1. Укрінформ - Мультимедійна платформа іномовлення України. [Електронний ресурс] - Режим доступу: https://www.ukrinform.ru/rubric-technology/2227514-ministry-finansov-g7-obavili-vojnukiberprestupnosti.html

2. HACMAGEDON Information Security Timelines and Statistics. [Електронний ресурс] - Режим доступу:
http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/

3. Богуш В.М., Юдін О.К., Інформаційна безпека держави. – К.: «МК-Прес», 2005. – 432с.

4. Ленков С. В., Перегудов Д. А., Хорошко В. А., Методы и средства защиты информации/ под. ред. В. А.Хорошко. – К.: Арий, 2008. – Том 1. Несанкци-онированное получение информации. – 464 с.

5. Сороківська О. А., Гевко В. Л. Інформаційна безпека підприємс-тва: Нові загрози та перспективи. 14.06.2010

УДК 004.6

ВПЛИВ ЛЮДСЬКОГО ФАКТОРУ НА СИСТЕМИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Заник О., Ткачук Р.
Львівський державний університет безпеки життєдіяльнсті, м. Львів

В роботі зазначений вплив людського фактору на корпоративну безпеку. Виділені основні проблеми та ризики у збереженні інформаційної безпеки, які модуть виникати при наявності негативної мотивації, непрофесіоналізму, свідомих чи несвідомих помилок.

***Ключові слова**: людський фактор, персонал, корпоративна мережа, інформаційна безпека, захист.*

The paper mentions the impact of the human factor on corporate security. The main problems and risks in maintaining information security, which may arise in the presence of negative motivation, unprofessionalism, conscious or unconscious mistakes.

***Key words:** human factor, personnel, corporate network, information security, protection.*

За характером організації захист інформації є багатокомпонентний та має складну ієрархічну структуру. У рамках теорії організації інформаційної безпеки чітко визначено постулат, що організація інформаційної безпеки повинна враховувати не тільки складність техніко-технологічних складових системи, а й людський фактор. І відповідно, до цього вже на етапі проектування систем технічного та програмного захисту, необхідно враховувати не тільки технічний аспект а й кількісні та якісні індивідуальні характерологічні особливості персоналу, який буде брати участь у системі захисту інформації [1].

Наявність людського фактора має першорядне значення в теорії інформаційної безпеки. Головна, ключова роль у безпеці належить не машинам чи технологіям, а людині. Людський фактор, як такий залежить від багатьох, як внутрішніх так і зовнішніх, змінних а іноді може проявлятися у «ніби» нелогічних діях. Хоча при детальнішому аналізі прослідковується певна закономірність та послідовність подій.

Людський фактор завжди був і є одним із найважливіших ризиків будь-якої сфери діяльності, оскільки більшість інцидентів відбувається з вини працівників. Навмисний відтік часто важко відрізнити від ненавмисного, але це не завжди необхідно, оскільки наслідки для підприємства в будь-якому з цих варіантів можуть бути катастрофічними [2].

Люди, які контролюють і використовують корпоративну мережу, є найбільш вразливою складовою цієї системи. Захист усієї системи часто перебуває в руках системного адміністратора. Якщо адміністратор не має достатнього рівня кваліфікації або вирішить стати на шлях злочину, то така система знаходиться в серйозній небезпеці [3].

Звичайних користувачів корпоративних мереж, операторів та інший персонал також можуть підкупити або змусити вчинити протиправні дії (видати паролі, логіни, іншу конфіденційну інформацію), що створює небезпечне середовище для захисту системи.

Окремо можна виокремити так званих «ображених» працівників, які досить часто, виношують плани помсти, а іноді при певному збігу обставин її реалізують. І в результаті така категорія працівників може завдати значної шкоди, оскільки вони володіють службовою інформацією про організацію та мають певні навики [4].

Основним захистом від внутрішніх ворогів є підтримка трудової дисципліни в колективі та встановлення особистого контакту між керівником та його підлеглими для подальшого вирішення проблем, а саме особистих конфліктів.

Категорія працівників, звільнених або понижених у посаді, особливо небезпечна. В комп'ютерній інформаційній діяльності ці працівники повинні перебувати під безпосереднім наглядом керівництва, особливо якщо персонал має право доступу до активного цінного інформаційного ресурсу. А у разі звільнення слід подбати, щоб особа більше не мала доступу до корпоративної інформації.

Тобто належне адміністрування є основою безпеки організації. В інформаційній діяльності це управління відоме як політика інформаційної безпеки.

Найпоширенішими та найнебезпечнішими загрозами доступності є ненавмисні помилки звичайних користувачів, операторів, системних адміністраторів та інших, які користуються інформаційними системами чи їх обслуговують. Такі помилки зазвичай стають загрозами (неправильно введені дані або помилка в програмі, що призвела до збоїв системи), іноді вони створюють вразливості, якими можуть скористатися зловмисники. Виходячи з цього, найрадикальнішим способом боротьби з ненавмисними помилками є максимальна автоматизація та суворий контроль [1, 2].

Отже, ми можемо зробити висновок, що для зменшення навмисних та ненавмисних загроз ключовим елементом є належне управління людським фактором. В якому важливу роль відіграє політика безпеки, а також правильний підбір персоналу, логічний алгоритм доступу до інформаційних ресурсів, якісне обладнання та програмне забезпечення. А для підтримання порядку повинна бути сформована корпоративна етика, яка регулюватиме правила безпечної поведінки як в самій організації так і за її межами.

Інформаційні джерела

1. Ромака В.А. Дудикевич В.Б., Гарасим Ю.Р. Системи менеджменту інформаціної безпеки: НУ«ЛП» 2012, 256 с.

2. http://uk.wikipedia.org/wiki/Політика_інформаційної_безпеки

3. https://uk.wikipedia.org/wiki/Система_управління_інформаційною_безпекою

4. http://www.info-library.com.ua/books-text-11433.html Філософські проблеми гуманітарних наук (Збірка наукових праць)

Напрям 2

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Бойсан Д.
Відокремлений підрозділ Національного університету біоресурсів і природокористування України «Ірпінський економічний коледж», м. Ірпінь

Проблема захисту інформації не є новою. Вона з'явилася ще задовго до появи комп'ютерів. Стрімке вдосконалювання комп'ютерних технологій позначилося й на принципах побудови захисту інформації.
Ключові слова: *комп`ютерна мережа, захист, віруси, атаки, інтернет, інформація.*

The problem of information security is not new. It appeared long before the advent of computers. The rapid improvement of computer technology has affected the principles of building information security.
Keywords: *computer network, protection, viruses, attacks, internet, information.*

Судячи зі зростаючої кількості публікацій і компаній, що професійно займаються захистом інформації в комп'ютерних системах, рішенню цієї задачі надається велике значення.

Однієї з найбільш очевидних причин порушення системи захисту є навмисний несанкціонований доступ (НСД) до конфіденційної інформації з боку нелегальних користувачів і наступні небажані маніпуляції з цією інформацією

Перехід від роботи на персональних комп'ютерах до роботи в мережі ускладнює захист інформації з наступних причин:

– велика кількість користувачів у мережі і їх змінний склад. Захист на рівні імені та пароля користувача недостатній для запобігання входу в мережу сторонніх осіб;

– значна довжина мережі і наявність багатьох потенційних каналів проникнення в мережу.

Мережні атаки через мережу «Інтернет» можуть бути класифіковані в такий спосіб:

1. Відмовлення в обслуговуванні (Denial of Service – DoS). Атака DoS робить мережу недоступної для звичайного використання за рахунок перевищення припустимих меж функціонування мережі, операційної системи або додатка.

2. Парольні атаки – спроба підбора пароля легального користувача для входу в мережу.

3. Атаки типу Man-in-the-Middle – безпосередній доступ до пакетів, переданим по мережі.

4. Атаки на рівні додатків.

5. Мережна розвідка – збір інформації про мережі за допомогою загальнодоступних даних і додатків.

6. Зловживання довірою усередині мережі.

7. Несанкціонований доступ (НСД), що не може вважатися окремим типом атаки, тому що більшість мережних атак проводяться заради одержання несанкціонованого доступу. [1].

Захист інформації в мережі може бути поліпшений за рахунок використання спеціальних генераторів шуму, що маскують побічні електромагнітні випромінювання і наведення, шумо-подавляючих мережних фільтрів, пристроїв зашумлення мережі живлення, скремблерів (шифраторів телефонних переговорів), подавлювачів роботи стільникових телефонів і т.д. Кардинальним рішенням є перехід до з'єднань на основі оптоволокна, вільним від впливу електромагнітних полів, що дозволяють знайти факт несанкціонованого підключення.

У цілому засобу забезпечення захисту інформації щодо запобігання навмисних дій у залежності від способу реалізації можна розділити на групи:

1. Технічні (апаратні) засоби. Це різні по типу пристрої (механічні, електромеханічні, електронні й ін.), що апаратними засобами вирішують задачі захисту інформації. Вони або перешкоджають фізичному проникненню, або, якщо проникнення усе-таки відбулося, доступу до інформації, у тому числі за допомогою її маскування. Першу частину задачі вирішують замки, ґрати на вікнах, захисна сигналізація й ін. Другу – згадувані вище генератори шуму, мережні фільтри, скануючі радіоприймачі і безліч інших пристроїв, що перешкоджають, витоку інформації або дозволяють їх знайти.

2. Програмні засоби включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту й ін.

3. Змішані апаратно-програмні засоби реалізують ті ж функції, що апаратні і програмні засоби окремо, і мають проміжні властивості.

4. Організаційні засоби складаються з організаційно-технічних (підго-

товка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу до неї й ін.) і організаційно-правових (національні законодавства і правила роботи, установлювані керівництвом конкретного підприємства По ступені поширення і приступності виділяються програмні засоби. Інші засоби застосовуються в тих випадках, коли потрібно забезпечити додатковий рівень захисту інформації.

Комп'ютерний захист - це постійна боротьба з «дурістю» користувачів й інтелектом хакерів. Навіть хакери найчастіше використають саме некомпетентність і недбалість обслуговуючого персоналу й саме останніможна вважати головною погрозою безпеки.

Одна із проблем подібного роду - так звані слабкі паролі. Користувачі для кращого запам'ятовування вибирають паролі, що легко вгадати. Причому проконтролювати складність пароля неможливо. Інша проблема - зневага вимогами безпеки. Наприклад, небезпечно використати неперевірене програмне забезпечення [2]. Звичайно користувач сам "запрошує" у систему віруси й "троянських коней". Крім того, багато неприємностей може принести неправильно набрана команда.

Кращий захист від нападу - не допускати його. Навчання користувачів правилам безпеки мережі може запобігти нападам. Захист інформації містить у собі крім технічних мір ще й навчання або правильний підбор обслуговуючого персоналу.

Захист інформації не обмежується технічними методами. Проблема є значно ширшою. Основний недолік захисту - люди, і тому надійність системи безпеки залежить в основному від відношення до неї. Крім цього, захист повинен постійно вдосконалюватися разом з розвитком комп'ютерної мережі [3].

У цей час узагальнена теорія безпеки інформації поки не створена. Застосовувані на практиці підходи й засоби нерідко страждають істотними недоліками й не мають оголошену надійність. Тому необхідно володіти достатньою підготовкою й кваліфіковано орієнтуватися у всьому спектрі питань забезпечення інформаційної безпеки, розуміючи їх комплексний і взаємообумовлений характер.

Інформаційні джерела

1.An Introduction to Computer Security: The NIST Handbook. Draft. - National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1994

2.Захист комп'ютерної інформації від несанкціонованого доступу Щеглов А. Ю. Видавництво: Наука й техніка

3.Левин В.К. Защита информации в информационно-вычислительных системах и сетях // Программирование. – 1994

УДК 004.4

АНАЛІЗ ПРОГРАМНИХ ПРИМАНОК ЯК ЗАСОБІВ МОНІТОРИНГУ ІНФОРМАЦІЇ У КІБЕРПРОСТОРІ

Василишин С., Опірський І.
Національний університет "Львівська політехніка", м. Львів

В даній статті розглянуті основні види кіберзагроз та системи моніторингу інформації у кіберпросторі, визначається місце приманок в цій системі: проаналізована їхня ефективність в порівнянні з іншими наявними рішеннями.
Ключові слова: *кібер, простір, хакери, пастка, приманка.*

This article examines the main types of cyberthreats and information monitoring systems in cyberspace, determined by the location in this system: their effectiveness is analyzed in comparison with existing solutions.
Key words: *cyber, hackers, honeypot, honeytoken, space.*

Вступ

На сьогоднішній день Інтернет, забезпечує обмін інформацією та системи зв'язку для понад 7 мільярдів користувачів. Ця кількість різко зростає, оскільки люди стають все більш залежними від соціальних медіа/мереж, мобільних телефонів, телекомунікацій, ігор, веб-сайтів знайомств на додаток до різних хмарних послуг та засобів. Це збільшення збільшує обмін інформацією і, отже, створило термін "великі дані".

Аналіз систем моніторингу та місце програмних приманок в системі захисту кіберпросторі

Інтернет включає кілька телекомунікаційних елементів та машин, таких як сервери/клієнти, мережеву інфраструктуру, послуги та бази даних, серед багатьох інших. Одним із способів моніторингу обміну інформацією між цими пристроями є створення інструментів управління мережею на основі служб SNMP [1]. Ці методи працюють на різних мережевих рівнях, таких як фізичний, мережевий та прикладний, а також охоплюють різні сфери, такі як зберігання даних, контроль доступу тощо. Мета - зібрати статистичну інформацію про сліди атак та такі дії, як зондування/сканування вразливих служб, розповсюдження хробаків, завантаження шкідливого програмного забезпечення та інші командно-адміністративні дії, такі як виконання кібер-атак DDoS за допомогою ботнету [2].

В Інтернеті існує декілька кіберзагроз. Нижче основні загрози, які можна виявити за допомогою аналізу сенсорних систем моніторингу:

1. Сканування/зондування: Сканування, також відоме як розвідувальна діяльність, є першим кроком у життєвому циклі кібератаки.

2. Ботнет можна використовувати як платформу для супротивників. Він призначений для управління скомпрометованої машини. Отже, він

націлений надати потужний інструмент для хакерів розповсюджувати та розширювати їх атаки.

3. Відмова в обслуговуванні: атаки характеризуються явною спробою запобігти законне використання послуги. DDoS-атаки використовують кілька об'єктів, що атакують (тобто скомпрометовані Машини / боти) для досягнення цільової мети.

4. Експлойти - це програмне забезпечення або послідовність команд, що усуває помилки, збої та уразливості в комп'ютерній системі з метою здійснення шкідливих дій, таких як отримання контролю, доступ до root привілеї, компрометуючи та заражаючи відкриті машини.

5. Зловмисне програмне забезпечення - це фрагмент коду. Різні типи, такі як віруси, хробаки, трояни тощо. Кожен із цих типів має різні особливості та сім'ї.

Порівнювати вищезазначені систем моніторингу будемо на основі таких особливостей:

1. Інтерактивність - це міра рівня взаємодії між противником і системи моніторингу.

2. Складність є мірою труднощів у створенні системи моніторингу

3. Збір даних вимірює кількість даних, зібраних з датчика захоплення.

4. Безпека вимірює рівень безпеки реалізації датчика на стороні моніторингу.

Таблиця 1

Порівняння існуючих систем моніторингу

Система Моніторингу	Тип	Інтерактивність	Складність	Збір даних	Безпека
Даркнет	IP основа	-	Низька	Низька	Безпечний
Honeypot з низьким рівнем	IP основа	Низька	Низька	Низька	Вразливий
Honeypot з середнім рівнем	IP основа	Середня	Середня	Середня	Вразливий
Honeypot з високим рівнем	IP основа	Висока	Висока	Висока	Вразливий
Greynet	IP основа	Ситуативний	Ситуативний	Ситуативний	Ситуативний
HoneyToken	На цифровій основі	Висока	Висока	Ситуативний	Безпечний

У таблиці 1 наведено порівняння систем моніторингу мережі на основі кількох ознак, а саме типу датчика, інтерактивності з супротивником, складності розгортання, збору даних або збору інформації та безпеки датчика моніторингу. По-перше, у приманках інтерактивність, складність та збір даних переважно пропорційні один одному [3]. Наприклад, чим більше взаємодія з супротивником, тим складнішою є конструкція і тим більше даних збирається. Однак, що стосується аспекту безпеки, то всі «приманки», які мають інтерактивну функцію, можуть бути вразливими з точки зору безпеки. По-друге, оскільки greynet складається з darknet і honeypot, він вважається більш повною системою моніторингу, і, отже, він може мати всі можливості з точки зору інтерактивності, складності, збору даних та безпеки [4].

Висновки. Отже, обмін інформацією загалом та безпека зокрема стали викликом для мережевих операторів, постачальників послуг Інтернету, організацій, правоохоронних органів та урядів. Для того, щоб впоратися з цією проблемою, на різних рівнях IP, таких як мережі та додатки, використовується кілька систем кібермоніторингу. У цій роботі ми проаналізували, що одним з найкращих методів моніторингу кіберпростору є встановлення таких систем моніторингу, як darknet, приманки, graynet та Honeytoken та визначили місце приманок серед цих моніторингових систем. Загалом, ці системи працюють на невикористаному, але маршрутизованому адресному просторі, а отже, весь призначений для них трафік може бути підозрілим.

Інформаційні джерела

1. Gandotra, V., Singhal, A., & Bedi, P. (2012). Threat-Oriented Security Framework: A Proactive Approach in Threat Management. Procedia Technology, 4, 487-494. DOI:10.1016/j.protcy.2012.05.078

2. Khan, Z.A.; Abbasi, U. “Reputation Management Using Honeypots for Intrusion Detection in the Internet of Things”. Electronics 2020, 9, 415.

3. Akiyama, M., Yagi, T., Hariu, T., & Kadobayashi, Y. (2017). HoneyCirculator: distributing credential honeytoken for introspection of web-based attack cycle. International Journal of Information Security. DOI:10.1007/s10207-017-0361-5

4. Spitzner, L. (2003). The honeynet project: Trapping the hackers. IEEE Security & Privacy, 1(2), 15- 23.

УДК 004.77

ПРОБЛЕМИ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

Воргуль О., Білоцерківець О. Г., Сєріков А. О.
Харківський національний університет радіоелектроніки, м. Харків

Віддалений доступ є однією з найпоширеніших тенденцій у сучасних комп'ютерних середовищах. Простота доступу до внутрішніх приватних мереж через Інтернет за допомогою телекомунікаційних пристроїв породила занадто багато загроз безпеці для кінцевих пристроїв. Дані, що перебувають на кінцевій точці віддаленого доступу не мають повного захисту між шлюзом VPN та внутрішніми ресурсами.

Remote access is one of the most common trends in today's computer environment. The ease of access to internal private networks over the Internet through telecommunications devices has posed too many security threats to end devices. Data at the remote access endpoint does not have full protection between the VPN and internal resources.

Методи віддаленого доступу мають ряд проблем з безпекою, які роблять їх неефективними при розгортанні VPN. Почнемо з того, що тунельований IP-трафік може не отримати намічений рівень перевірки або застосування політики мережевими пристроями безпеки, якщо такі пристрої не підтримують тунелювання. Це знижує глибоку захист і може викликати проломи в безпеці.

Цей недолік безпеки відноситься до всіх пристроїв, розташованим в мережі, і до будь-яких міжмережевих екранів на основі кінцевих хостів, існуючі механізми перехоплення не показують їм потік IP-пакетів після того, як тунельний клієнт виконує декапсуляцію або до того, як він виконає інкапсуляцію. Крім того, IP-адреси всередині тунелів не підлягають вхідної та вихідної фільтрації в мережі, через яку вони тунелюються, і, отже, можуть пропускати шкідливий контент у внутрішні мережі.

Більш того, якщо інкапсульований IP-пакет вказує вихідну маршрутизацію за межами одержувача тунельного клієнта, хост може переслати IP-пакет на вказаний наступний перехід. Це може бути несподіваним і таким, що суперечить побажанням адміністратора, а також може обійти елементи управління маршрутизацією від джерела в мережі.

Крім того, багато підприємств дозволяють, або не регулюють використання сторонніх сервісів зберігання файлів для полегшення віддаленого доступу до даних, а коли файли потрапляють в хмарні репозиторії, підприємства втрачають контроль. Зі свого боку, прямий доступ до додатків вимагає використання IPv6 виключно для розподілу адресації між підключе-

ними кінцевими точками. Коли справа доходить до адресації і ідентифікації клієнтів, це являє собою більш серйозну проблему управління.

Для вирішення деяких з цих проблем був розроблений ряд протоколів. На жаль, ці протоколи також містять уразливості, які роблять їх небезпечними. Наприклад, протокол RFB, протокол відображення, має деякі недоліки безпеки, включаючи вразливість для атаки Man-In-The-Middle.

Незважаючи на те, що протокол RFB використовує зашифровані паролі і мережу, будь-який обмін даними по мережі вразливий і може бути атакований MITM з використанням спец. інструментів і методів. Крім того, додатки VNC, розроблені на основі протоколу RFB, зазвичай повільніші, пропонують менше функцій і варіантів безпеки, ніж віддалений робочий стіл (RD), який заснований на протоколі .

Хоча дані, що відправляються між сервером і клієнтом, зашифровані, протокол RDP може бути підданий атаці Man-In-The-Middle, оскільки під час налаштування ключів шифрування для сеансу не виконується перевірка сервера.

Інформаційні джерела

1. Шальгин В.О., Комплексний захист корпоративної інформації. Навч.пос. 2009. 404 с.

2. Биячуев Т.А. / під ред. Л.Г.Осовецкого, Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004. - 161 с.

АНАЛІЗ АТАК НА БАЗИ ДАНИХ ТА МЕТОДИКА ЗАХИСТУ

Масник С. Т., Шабатура М.М.
Національний університет «Львівська політехніка», м. Львів

У роботі розглянуто актуальну проблему на сьогоднішній день, це атаки на бази даних. Проаналізовано три найпоширеніших атаки: SQL-ін'єкції, «Meow» та атаку методом грубої сили. Запропоновано рекомендації щодо зниження шансів реалізації атак.

Ключові слова: *бази даних, атаки, захист баз даних*

In the paper was considered a major problem of our time, it is database attacks. There are three most common attacks: SQL injection, "Meow" attack and the brute force. Recommendations for reducing the chances of attack implementation are offered.

Keywords: *databases, attacks, database protection*

Цифрова трансформація суспільства спричинила неабиякий технічний прогрес у всіх сферах людського життя. Проте, окрім безумовного спрощення буденних справ та багатократного зменшення паперової тяганини, це стало каталізатором розвитку здібностей кіберзлочинців, оскільки зараз впливовість вимірюється терабайтами конфіденційної інформації.

Через невпинні темпи зростання кількості інформації, з якою доводиться працювати, з'явилась обґрунтована необхідність у належних методах обробки, структуризації та зберігання інформації. Доволі оптимальним способом вирішення цієї проблеми стало використання баз даних, що забезпечує певний рівень захищеності інформації. Однак, існують загрози, для яких базових налаштувань недостатньо. Нижче у роботі, ми розглянемо найпоширеніші атаки та наведемо рекомендації щодо їх запобігання.

SQL-ін'єкції. SQL-ін'єкції – це атака, спрямована на веб-додаток, яка полягає у вставці шкідливого коду мовою структурованих запитів через вхідні дані від клієнта. Попри те, що цей експлойт відомий давно, він є одним із найнебезпечніших, оскільки здатен нівелювати відповідність одразу трьом критеріям інформаційної безпеки: конфіденційності, цілісності та доступності [1].

Конфіденційність: зламування за допомогою SQL-ін'єкції дає змогу зловмиснику витягти вміст веб-додатку та отримати повноцінні повноваження на читання всієї інформації, що міститься у базі даних.

Цілісність: такого плану атака дає можливість порушнику маніпулювати інформацією: редагувати будь-які поля таблиць, видаляти критично важливі дані.

Доступність: подібні злами характеризуються можливістю ініціювати запити, виконання яких потребує великого об'єму серверних ресурсів. Кілька таких запитів здатні спровокувати відмову в обслуговуванні, що ускладнить доступ правомірних користувачів до веб-ресурсу [2].

Задля зменшення ризиків успішного впровадження SQL-ін'єкцій можна застосовувати хешування, параметризовані запити та обмеження привілеїв. Хешування критичної інформації, наприклад паролів, забезпечує доволі високий рівень безпеки, оскільки ймовірність відновлення початкових даних є досить низькою. Параметризовані запити всі вхідні символи, які для мови структурованих запитів є значущими, замінюють комбінацією символів так, що в кінцевому результаті вхідне значення буде стрічкою, а ймовірність загрози прямує до нуля. Що стосується прав доступу користувачів, то найкращою практикою вважається надання мінімальних прав для виконання необхідної роботи.

«Meow» атака. Цей тип атаки сколихнув інформаційне суспільство в липні поточного року. Автоматизований скрипт знищував дані або повністю перезаписував без жодних попереджень чи інших повідомлень. Дана атака спрямовувалась на незахищені бази даних та відкриті для спільного доступу в Інтернет файлові системи. Після видалення даних на серверах компаній, чимало з баз згодом опинялись у відкритому доступі, в тому числі з конфіденційною інформацією користувачів. Загалом налічується близько десяти тисяч постраждалих компаній.

Для того, аби знизити ризик злому, пропонуються наступні заходи: стійка автентифікація, чітке розмежування доступу та ідентифікація і захист конфіденційних даних [3]. Автентифікація та принцип мінімальних

повноважень позитивно вплинуть на ймовірність зовнішнього несанкціонованого підключення. Доступ до персональних даних користувачів лише з найвищими повноваженнями або, наприклад, відокремлене зберігання конфіденційної інформації мінімізує ризик неправомірної взаємодії.

Атака методом грубої сили. Цей тип атаки полягає у тому, що зловмисник заздалегідь готує певний словник, тобто набір комбінацій символів чи певних шаблонів, в якому міститься список найбільш часто використовуваних паролів користувачами, що серйозно збільшує шанси на успіхи при відносно меншій кількості спроб. Або ж більш традиційний варіант атаки – послідовний автоматизований перебір всіх можливих комбінацій символів. Найчастіше цей метод використовується для з'ясування облікових даних з ціллю подальшої автентифікації і безперешкодного доступу до бази даних [4].

Щоб захиститися від атак грубої сили достатньо виконати кілька простих кроків: застосовувати складні унікальні паролі, встановити політику блокування облікового запису, а також вести постійний аудит системи. Надійний пароль, можливо навіть згенерований випадковим чином, матиме настільки високий ступінь стійкості, що часові витрати на його пошук будуть нераціональними, оскільки поле пошуку становитиме десятки мільйонів комбінацій. Обмеження кількості спроб введення паролю з подальшим блокуванням облікового запису захистить персональну інформацію користувачів, а постійний аудит уможливить фіксацію підозрілих подій в системі.

Висновок. Будь-яка система є певною мірою вразлива, і навіть застосовуючи всі відомі засоби захисту не можна гарантувати непроникність. Бази даних потребують не менш прискіпливої конфігурації, аніж сервер, що обробляє запити від клієнта, а тому важливо знати найпоширеніші методи атак та користуватися наявними знаннями для реалізації превентивних заходів. Однак, панацеї від перелічених загроз не існує, і головним завданням спеціаліста при успішній атаці є мінімізація втрат.

Інформаційні джерела

1. SQL Injection | OWASP [Електронний ресурс] – Режим доступу: https://owasp.org/www-community/attacks/SQL_Injection, вільний;

2. Херцог Рафаэль, Горман Джим, Ахарони Мати. Kali Linux от разработчиков – СПб.: Питер, 2019. – 320 с.

3. Three Easy Ways to Avoid Meow-like Database Attacks [Електронний ресурс] – Режим доступу: https://www.darkreading.com/attacks-breaches/three-easy-ways-to-avoid-meow-like-database-attacks, вільний;

4. Brute Force Attack Software Attack | OWASP Foundation [Електронний ресурс] – Режим доступу:
https://owasp.org/www-community/attacks/Brute_force_attack, вільний.

УДК514.18:004.056

ЗАХИСТ ІНФОРМАЦІЇ В AUTOCAD

Гумен О., Селіна І., Козюк І.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

Програма комп'ютерної графіки AutoCAD, її актуальність та широке використання при створенні проектів у сучасних умовах вимагають особливої уваги до питань збереження інформації та авторства виконавців документації. При роботі з програмою потрібно здійснювати шифрування блоків креслення цифровим підписом, що забезпечує надійний захист проектної документації.

Ключові слова: захист інформації, цифровий підпис, AutoCAD.

Computer graphics program AutoCAD, its relevance and widespread use in modern conditions require special attention in matters of preserving information and authorship of documentation performers. When working with the program you need to encrypt the blocks of the drawing with a digital signature, which ensures reliable protection of project documentation.

Keywords: information protection, digital signature, AutoCAD.

Сьогодні програма Autodesk AutoCAD самий відомий і актуальний пакет для створення кресленików. Протягом багатьох років ця програма модернізується і вдосконалюється, додаються нові опції, що дозволяє прискорити процес отримання кресленика, і все більше користувачів використовують цю програму для роботи. Під час викреслювання документа можна легко внести коректування, створити резервну версію файлу чи просто скопіювати його. Але не завжди автору проекту потрібні зміни в його документах, і тут виникає питання, як захистити свою роботу, як попередити несанкціоноване копіювання чи редагування файлів. У даному випадку можна використовувати включення або відключення перевірки цифрового підпису і спеціальні позначки для файлів кресленików AutoCAD [1, 2].

Цифровий підпис – це блок зашифрованої інформації, доданої в певні файли для впізнавання творця та ідентифікації змін у файлі з моменту застосування цифрового підпису. Такі файли, в яких є цифровий підпис, мають багато переваг, а саме: разом з кресленником отримувач здобуває правдиву інформацію про особу, яка створила кресленик, а також впевненість, що кресленик доставлено адресату без змін після додавання цифрового підпису. Вивчити цифровий підпис файлу можна, прослідкувавши ланцюжок сертифікатів майже до кореневого сертифіката, який випущений довіреним центром сертифікації (ЦС) [3]. Можливо також створити самозавіряючий сертифікат за допомогою однієї з утиліт [4].

Цифровий підпис можна також отримати через Інтернет. У результатах пошуку можна знайти детальну інформацію про центри сертифікації і порядок отримання цифрового посвідчення. В цифрових посвідченнях використовують два ключа – відкритий ключ, за допомогою якого будь-який користувач може перевірити цифровий підпис, і закритий ключ, відомий лише власнику цифрового посвідчення. Закритий ключ використовують для створення цифрового підпису. Цифровий підпис можна додавати до файлів форматів AutoCAD 2000 і більш сучасних версій.

Цифровий підпис файлу можна перевірити, і це має велике значення при колективній роботі над документом. Якщо ж після додавання цифрового підпису файл було змінено чи пошкоджено, то цифровий підпис стає недійсним.

Таким чином, програма AutoCAD стає незамінним помічником у забезпеченні захисту проектної документації.

Інформаційні джерела

1. Цифровые подписи для исполняемых файлов. https://knowledge.autodesk.com.
2. Защита чертежа AutoCAD паролем. https://autocad-specialist.ru.
3. Защитите себя от нелегального использования ПО AutoCAD. https://autodesk.ru.
4. Коротко о цифровых подписях. https://entercad.ru.

УДК 004:056

КІБЕРБЕЗПЕКА ВЛАСНИХ ДАНИХ

Несін С.
Львівський національний університет імені Івана Франка, м. Львів

У той час, коли наші дані є майже у всіх соціальних мережах, та навіть, щоб замовити щось онлайн, на сайтах чи додатках вимагають внести особисті дані, особливу увагу варто приділити кібербезпеці і захисту персональної інформації.
Ключові слова: *кібербезпека, соціальні мережі, особисті дані.*

While our data is available on almost all social networks, and even to order something online, sites or applications require personal data, special attention should be paid to cybersecurity and protection of personal information.
Key words: *cybersecurity, social networks, personal data.*

Поняття особистих даних в Інтернеті уже давно вийшло за рамки анкетних питань, до прикладу «як вас звати і скільки вам років?». Це питання уже включає в себе захист облікових записів користувачів соціальних мереж чи додатків, захист від вірусів та інші більш глибокі мережеві та кібер-задачі, що ускладнюють впевненість у безпеці власних даних людей усього світу.

Не відповідальність користувачів Інтернету у безпеці та введені власних даних призводить до того, що дані можуть видалити чи викрасти, якщо це стосується робочих акаунтів, то це може поставити під загрозу усю документацію фірми чи навіть вплинути на загальні настрої у роботі колективу, та призупинити роботу підприємств. Кібербезпека сьогодні відповідає за три чинники: системи, процеси, люди.

Як кажуть, хто володіє інформацією, той володіє світом. А найдорожча та найпровокативніша інформація для нас - це наші особисті дані.

Ілон Маск сказав: “Ми ВЖЕ кіборги. Люди настільки інтегровані з телефоном і комп’ютером, що навіть не усвідомлюють цього. Коли ми забуваємо десь мобільний, то здається, ніби втратили частину тіла”. І втрата цієї частини є інформація про нас, і в чиїх руках цей інструмент нашої маніпуляції, той і має усі козирі в руках.

Потреба в особистій кібербезпеці буде все зростати, тому що чим далі, тим більше ми “зростаємось” з нашими гаджетами. Кібербезпека відповідає за захист конфіденційної інформації та взаємодію з нею при користуванні будь-яким пристроєм. Наприклад, щоб до тебе не проник вірус через розумний холодильник або кавоварку [1].

У одній із своїх статей на електронному ресурсі газети «Юридична газета» юриста Ірина Вівчарик надає рекомендації щодо безпеки даних в Інтернеті:

– обмеження щодо використання електронного листування як засобу передачі -електронних документів чи будь-якої конфіденційної інформації;

– передача електронних документів через безпечні портали обміну інформацією;

– використання складних паролів та багатофакторної автентифікації для отримання доступу до електронних документів/інформації;

– шифрування;

– надання доступу до певних категорій електронних документів/інформації лише тим -учасникам арбітражу, яким така інформація необхідна для належної участі;

– обмеження доступу до паперових екземплярів документів;

– домовленість щодо обмеження відкриття документів, використовуючи публічний інтернет;

– перевірка наявності всіх учасників арбітражу брандмауерів, антишпигунських та -антивірусних програм і забезпечення ними у разі відсутності;

– попереднє погодження алгоритму спільних дій учасників арбітражного процесу на випадок порушення безпеки даних. [2]

Також спеціалісти радять у паролях використовувати ключові фрази чи слова, які розумієте лише ви, а також не використовувати одні і ті ж паролі для декількох соціальних мереж та акаунтів. Вгадати слово важче, ніж простий набір із букв та цифр.

Рекомендується теж видаляти старі дані, якщо ви забули пароль, то відновити, стерти інформацію, а не створювати нові сторінки. Коли ви видаляєте дані і вводите відразу нові, то стара інформація зникає з Інтернету, а якщо ви просто видалили інформацію чи сторінку, то ці дані залишусь я у так званому «даркнеті» чи хмарах типу цього.[3]

Пам'ятайте ваша безпека залежить лише від вас. У сучасному світі маніпуляції даними трапляються все куди частіше, і шахраї заробляють на цьому величезні кошти, в той час як ви їх втрачаєте. Тому будь свідомими користувачами Інтернету і бережіть свої дані.

Інформаційні джерела

1. Інформаційна безпека і кібербезпека - у чому різниця?[Електронний ресурс]. - 2019.- Режим доступу: https://indevlab.com/uk/blog-ua/informatsijna-bezpeka-i-kiberbezpeka-v-chomu-riznitsya/

2. Ірина Вівчарик Захист даних та кібербезпека в міжнародному арбітражі / Юридична газета [Електронний ресурс]. - 2019. - Режим диспуту: https://yur-gazeta.com/publications/practice/mizhnarodniy-arbitrazh-ta-adr/zahist-danih-ta-kiberbezpeka-v-mizhnarodnomu-arbitrazhi.html

3. 15 порад, як захистити особисту інформацію в онлайні [Електронний ресурс]. - MediaSapiens.- 2017. - Режим доступу: https://ms.detector.media/kiberbezpeka/post/18293/2017-01-28-15-porad-yak-zakhistiti-osobistu-informatsiyu-v-onlaini/

СУЧАСНИЙ ЗАХИСТ ІНФОРМАЦІЇ В КОМП`ЮТЕРНИХ МЕРЕЖАХ

Дулова О.
Відокремлений підрозділ Національного університету біоресурсів і природокористування України «Ірпінський економічний коледж», м. Ірпінь

Захист інформації є однією з вічних проблем. 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.

Ключові слова: *комп`ютерна мережа, захист, віруси, атаки, інтернет, інформація, системи, мережі, безпека.*

Information security is one of the eternal problems. Throughout human history, ways solutions to this problem were determined by the level of technological development. In the modern information society technology plays the role of activator of this problem - computer crimes have become a hallmark of today.

Keywords: *computer network, protection, viruses, attacks, internet, information, systems, networks, security.*

З самого початку свого розвитку системи інформаційної безпеки розроблялися для військових відомств. Розголошення такої інформації могло привести до величезних жертв. Тому конфіденційності (тобто нерозголошенню інформації) в перших системах безпеки приділялася особлива увага. Очевидно, що надійно захистити повідомлення й дані від розголошення і перехоплення може тільки повне їхнє шифрування.

Принципова особливість сучасної ситуації полягає в тому, що найважливішим завданням сьогодні стає захист інформації в комп'ютерних мережах.

Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їхньої обчислювальної потужності, використання комп'ютерних мереж різного масштабу привели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої діяльності.

Принцип сучасного захисту інформації можна виразити так - пошук оптимального співвідношення між доступністю й безпекою.

Повністю захищений комп'ютер - це той, який знаходиться під замком у кімнаті в сейфі, не підключений ні до якої мережі і виключений. Такий ком-

п'ютер має повноцінний захист, однак використати його не можна. У цьому прикладі не виконується вимога доступності інформації. "Повноцінності" захисту заважає не тільки необхідність користуватися захищеними даними, але й ускладнення систем, що захищають. Використання постійних, що не розвиваються механізмів захисту небезпечно, і для цього є кілька причин.

Одна з них - розвиток власної мережі. Адже захисні властивості електронних систем безпеки багато в чому залежать від конфігурації мережі й використовуваних у ній програм. Навіть якщо не міняти топологію мережі, все одно прийдеться використати нові версії раніше встановлених продуктів.

Крім того, не можна забувати про розвиток й удосконалювання засобів нападу. Техніка так швидко міняється, що важко визначити, який пристрій новий або програмне забезпечення, використане для нападу, може обдурити ваш захист.

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у такі групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зазначимо, що такий поділ є досить умовним. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту [1].

Морально-етичні засоби. До цієї групи належать норми поведінки, які традиційно склались або складаються з поширенням ЕОМ, мереж і т. ін. Ці норми здебільшого не є обов'язковими і не затверджені в законодавчому порядку, але їх невиконання часто призводить до падіння авторитету та престижу людини, групи осіб, організації або країни.

Правові засоби захисту — чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання ІТ.

Адміністративні (організаційні) засоби захисту інформації регламентують процеси функціонування 1С, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою ускладнити або не допустити порушень безпеки [2].

Засоби фізичного (технічного) захисту інформації — це різного роду механічні, електро- або електронно-механічні пристрої, а також споруджения і матеріали, призначені для захисту від несанкціонованого доступу і викрадень інформації та попередження її втрат у результаті порушення роботоздатності компонентів 1С, стихійних лих, саботажу, диверсій і т. ін.

Програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів згідно з повнова-

женнями користувачів, реєстрацію подій в комп'ютерних системах і мережах, криптографічний захист інформації, захист від комп'ютерних вірусів тощо. Розглядаючи програмні засоби захисту, доцільно спинитись на стеганографічних методах. Слово «стеганографія» означає приховане письмо, яке не дає можливості сторонній особі взнати про його існування. Одна з перших згадок про застосування тайнопису датується V століттям до н. е. Сучасним прикладом є випадок роздрукування на ЕОМ контрактів з малопомітними викривленнями обрисів окремих символів тексту — так вносилась шифрована інформація про умови складання контракту [3].

Для виявлення, знищення та попередження загроз можна використовувати загальні засоби захисту інформації (копіювання інформації, розмежовування доступу до неї) та профілактичні заходи, які зменшують імовірність зараження. Останніми роками з'являються апаратні пристрої антивірусного захисту, наприклад спеціальні антивірусні плати, які вставляються у стандартні слоти розширення комп'ютера [4]. Але найбільш поширеним методом залишається використання антивірусних програм — спеціальних програм, призначених для виявлення і знищення комп'ютерних вірусів.

Інформаційні джерела

1. An Introduction to Computer Security: The NIST Handbook. Draft. - National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1994**.**

2. Захист комп'ютерної інформації від несанкціонованого доступу Щеглов А. Ю. Видавництво: Наука й техніка

3. Столингс. В. Криптография и защита сетей. Принципы и практика /В. Столингс. – М.: «Вильямс», 2001. – 672 с

4. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В Романец., П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с.

Напрям 3

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

УДК 003.26.09

МЕТОДИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

[1]Великий В., [1]Мороз Ю., [2]Полотай О.

[1]Кафедра безпеки інформаційних технологій Національного університету «Львівська політехніка», м. Львів
[2]Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів

В даній роботі проведено детальне ознайомлення із технічним захистом інформації, а також розглянуто апаратний модуль безпеки (HSM) для зберігання, керування, генерування та використання ключів шифрування.
***Ключові слова**: технічний захист інформації, криптографічний захист інформації.*

In this paper, a detailed acquaintance with the technical protection of information, as well as a hardware security module (HSM) for storage, management, generation and use of encryption keys.
***Key words:** technical protection of information, cryptographic protection of information.*

Сучасний світ важко уявити без використання інформаційно-комунікаційних систем, які б не опрацьовували чутливу інформацію, наприклад дані медичних карток, інформацію про банківські рахунки та інші види особистої інформації. Тому питання інформаційної безпеки, відіграє значну роль у життєдіяльності кожного**.** З іншого боку роль інформаційної безпеки дуже сильно недооцінена. Багато хто розуміє її важливість, але в більшості випадків дії обмежуються встановленням базового мережевого екрану на кордоні мережі та/або звичайних антивірусних програм. В інших випадках кожен сподівається на те, що напад станеться з кимось іншим.

Зі збільшенням диджіталізації набирали обертів і зловмисники, метою яких було отримання персональних даних. Саме тому, гостро постало питання технічного захисту інформації.

Розвиток сучасних та високоефективних методів шифрування та криптографії зіграло ключову позицію в захисті інформації. Сьогодні практично будь-яка комунікація в мережах виконується із застосуванням криптографічних систем шифрування інформації та комбінації даних систем. Однією із

проблем є те, що чутлива інформація зберігається на носіях даних разом із ключами, які використовувались для шифрування цієї інформації. Зловмисники, які отримували доступ до носіїв чутливої інформації могли з легкістю отримати доступ до ключів, які використовувались для криптографічного захисту даних, що давало їм змогу без перешкод отримати чутливу інформацію. Ще однією проблемою було те, що потрібно було постійно передавати ключі по мережі, що становило загрозу перехоплення ключів методом сніфінгу. Сніфінг – процес перехоплення і аналізу мережевого трафіку. Після чого постало питання безпечного зберігання, використання ключів шифрування та захист від витоку ключів під час віддаленого злому систем.

Мета даної роботи – розглянути сучасні методи технічного захисту цінних ключів, ознайомитися із апаратними засобами для зберігання, керування, генерування ключів і обробки інформації з використанням даних ключів на прикладі апаратного модуля безпеки.

Актуальними проблемами даної теми є:

– наразі, застосування сучасних технічних засобів захисту інформації не набуло великого поширення;

– технічні засоби захисту інформації є складними у використанні;

– практично відсутня конкуренція на ринку технічних пристроїв даного типу;

– обмеження продуктивність традиційних HSM

– в більшості випадків технічні пристрої є дороговартісними.

Розроблений підхід з використанням HSM (Hardware Security Module) пропонує взагалі не давати вразливій частині системи доступ до вмісту ключа. HSM – це фізичний пристрій, підключається напряму до хоста або сервера, який зберігає чутливу інформацію.

В такому випадку перед апаратним модулем безпеки ставляться наступні завдання:

– зберігання, керування, генерування цифрових ключів або іншої секретної інформації;

– виконання криптографічних операцій з допомогою секретних ключів;

– виконання криптографічних операцій не повинно відбуватись за межами апаратного модуля безпеки, а користувач має повинен отримувати доступ тільки до результатів операцій.

Результати проведеного аналізу говорять про те, що даний продукт буде корисним для використання банківськими установами, медичними закладами, компаніями, які зберігають і обробляють дані банківських карток та персональні дані користувачів.

Інформаційні джерела

1. https://hubsecurity.io/what-is-a-hardware-security-module-hsm/

2. https://habr.com/ru/company/JetBrains-education/blog/251243/

3. https://www.advantio.com/blog/hardware-security-module-hsm-what-is-it-and-what-is-its-role-in-protecting-payment-card-data

УДК 510.57+519.27

ПРОБЛЕМИ ОХОРОНИ АВТОРСЬКИХ ПРАВ В УКРАЇНІ

Волошин В.О., Мацулевич О.Є.
Таврійський державний агротехнологічний університет ім. Дмитра Моторного, м. Мелітополь

В публікації проводиться аналіз стану охорони авторських прав в Україні в рамках беззупинного руху до світового економічного простору та пропонуються конструктивні шляхи вирішення питань охорони авторського права і суміжних прав.
Ключові слова: *авторське прево; інтелектуальна власність.*

Summary - In article the analysis state protection of copyrights in Ukraine is carried spent within the framework of unceasing movement to world economic space and constructive ways of the decision of questions of protection of the copyright are offered.
Keywords: *author's translation; Intellectual Property.*

Останнім часом навколо законодавства України про авторське право виникло більше суперечок, ніж за всі попередні роки, починаючи з 1993 р., коли було прийнято Закон України “Про авторські і суміжні права”. Нагальна необхідність ефективної правової охорони та захисту прав інтелектуальної власності для України зумовлюється обраною нею стратегією побудови цивілізованих ринкових відносин, забезпечення соціальної орієнтації економіки та інноваційного соціально-економічного розвитку, що має спиратися насамперед на активізацію власного інтелектуального потенціалу. Оцінюючи процес входження України до регіональних структур, що забезпечують правову охорону інтелектуальної власності, можна зробити висновок стосовно наявності у ньому як позитивних зрушень, так і низки невирішених проблем.

Так, у рамках виконання відповідної програми скоординованих дій правоохоронних і контролюючих органів по боротьбі з незаконним виробництвом, розповсюдженням і реалізацією аудіо - та відеопродукції, компакт-дисків та інших об’єктів права інтелектуальної власності, з метою уніфікації операцій контролю за дотриманням вимог законодавства у сфері інтелектуальної власності, за матеіалами СБУ стосовно порушення авторського права і суміжних прав слідчими органами МВС порушено 66 кримінальних справ.

Аналіз останніх досліджень та формулювання цілей статті. За результатами спільних з Державним департаментом інтелектуальної власності дій конфісковано за рішенням суду у правопорушників та знищено контрафактної продукції у кількості 168 тис. примірників на загальну суму 4,2 млн. гривень, стягнуто штрафів на суму 219 тис. гривень, складено 31 протокол про вчинення адміністративних правопорушень за нормами статті 1649 Кодексу України про адміністративні правопорушення. За результатами спільних з Державним департаментом інтелектуальної власності дій конфісковано за рішенням суду у правопорушників та знищено контрафактної продукції у кількості 168 тис. примірників на загальну суму 4,2 млн. гривень, стягнуто штрафів на суму 219 тис. гривень, складено 31 протокол

про вчинення адміністративних правопорушень за нормами статті 164 Кодексу України про адміністративні правопорушення [1].

Основна частина. На думку експертів, наявність в Україні механізму для захисту авторських та суміжних прав та його вдосконалення останніми роками зумовило зменшення кількості контрафактної продукції, однак рівень піратства в країні залишається значним, Україна є європейським лідером з виробництва та експорту неліцензійного програмного забезпечення. Експерти кажуть про те, що одним з найслабших місць України в цьому питанні є не відсутність законодавства, а насамперед слабкий урядовий контроль.

Так, Міжнародний альянс захисту інтелектуальної власності включив Україну до списку країн, за якими потрібно пильно слідкувати у плані виробництва контрафактної продукції. У 2006 році збитки від діяльності українських піратів оцінювалися в 320 мільйонів доларів. Це сума збитків лише від контрафактних програмного забезпечення та музичних дисків. З 16 країн у цій категорії Україна посіла шосте місце. Ще одна цифра: наприкінці січня 2007 року Міжнародна торгова палата назвала Україну дев'ятою країною з виробництва контрафактної продукції та піратства. [2].

Незважаючи на активізацію зусиль правоохоронних органів України із забезпечення захисту прав інтелектуальної власності, загальний рівень правопорушень у цій сфері залишається високим, що є підставою для звинувачення України в низьких стандартах забезпечення захисту прав інтелектуальної власності.

Сьогодні дуже важливим є створення ефективної системи захисту інтелектуальної власності. Ефективна кримінально-правова охорона авторського права і суміжних прав має на сьогодні особливо важливе значення. По-перше, ринкова економіка дає широкі можливості для розвитку правовідносин у сфері творчої діяльності. По-друге, можна одночасно констатувати широкий розмах посягань на авторське право і суміжні права, зокрема злочинного характеру. Останнє обумовлюється відсутністю у правоохоронних органів достатнього досвіду боротьби з цим явищем, недостатністю засобів держави для цієї боротьби, а також значною недосконалістю кримінального законодавства у даній сфері.

Зазначене і призводить до поширення в країні так званої піратської діяльності. Велика шкода завдається суб'єктам авторського права і суміжних прав, як вітчизняним, так і зарубіжним, а також економіці України, її репутації, престижу на міжнародній арені. Відповідно до даних МВС України злочинці та організовані злочинні групи за рахунок порушень авторського права і суміжних прав в Україні отримують прибуток, який вираховується десятками мільйонів доларів США на рік, при цьому уникають у переважній більшості належних мір покарання за вчинене.

Виходячи з положень ЦК України, а також Закону про авторське право, розмір завданої суб'єкту авторського права чи суміжних прав матеріальної шкоди в її цивільно-правовому розумінні має визначатись як сума коштів, яку б отримав суб'єкт авторського права чи суміжних прав на відповідні об'єкти авторського права або суміжних прав у разі, якщо б зазначені у диспозиції

ст. 176 КК України дії були вчинені з дотриманням чинного законодавства України, яке визначає їх вчинення, тобто як сума втраченої вигоди [3, 4].

З існуючої проблеми визначення матеріальної шкоди у ст. 176 КК України, можна знайти два наступні виходи: законодавець повинен внести до Примітки до ст. 176 КК України зміни і доповнення у вигляді тлумачення способу визначення розміру шкоди; Пленум ВСУ має прийняти постанову про судову практику в справах про злочини проти інтелектуальної власності, в якій надати відповідні роз'яснення по суті питання. Таке вирішення ситуації дозволить усунути неоднозначність поглядів на визначення розміру матеріальної шкоди для кваліфікації діянь винних осіб за ст. 176 КК України [5, 6].

Інформаційні джерела

1. Рекомендації парламентських слухань «Захист прав інтелектуальної власності в Україні: проблеми законодавчого забезпечення таправозастосування» (21 березня 2007 року). Схвалено Комітетом Верховної Ради з питань науки і освіти 25 травня 2007 року та Постановою Верховної Ради України від 27 червня 2007 року // Біла книга. Інтелектуальна власність в інноваційній економіці України / Г. О. Андрощук, О. В. Дем'яненко, І. Б. Жиляєв, Л. В. Сахарова, В. І. Полохало, С. В. Таран (упорядкування).- К: Парламентське вид-во, - 2008. - 448 с.

2. Асоціаціація виробників програмного забезпечення Business Software Alliance (BSA)// Пропозиції до вищих органів державної влади затвердити на законодавчому рівні програму із запобігання порушення авторських прав і використання контрафактної продукції/ Круглий стіл.- 30 жовтня 2008 року.- Київ.

3. *Ступак С.* Пиратство на Украине будет охраняться законом /Ступак С., Ступка О., Феколкин Ю. // Юрид. практика. — 2005. — 28 дек. — № 52 (158).

4. Кримінальний кодекс України (Стаття 176 в редакції Закону N850-IV від 22.05.2003, із змінами, внесеними згідно із Законом N3423-IV від 09.02.2006) *Коваль А.* Порушення авторського права і суміжних прав: кримінально-правові проблеми, які потребують свого вирішення / А.Коваль // Інтелект. власність. – 2004. – № 4.

5. *Щербина В.В., Тышковец А.А., Серёгина А.В., Щербина В.М.* Результаты анкетного опроса студентов специальности «экология» таврического государственного агротехнологического университета в области экологического образования в университетской среде / Удосконалення освітньо-виховного процесу в закладі вищої освіти: зб. наук.-метод. праць;Вип. 23, - Мелітополь: ТДАТУ, 2020, - С. 267-272.

6. *Щербина В.М., Холодняк Ю.В., Івженко О.В.* Впровадження комп'ютерної графіки в навчальний процес при підготовці фахівців інженерних спеціальностей /Удосконалення освітньо-виховного процесу в закладі вищої освіти. Випуск 24 / Збірник науково-методичних праць / ТДАТУ, - Мелітополь: ТДАТУ, 2020.

ПІСОЧНИЦІ КОМП'ЮТЕРНИХ СИСТЕМ ЯК МЕХАНІЗМ ЗАХИСТУ ВІД ВІРУСІВ

Мікуш П., Шабатура М.
Національний університет «Львівська політехніка», Львів

У роботі розглянуто рішення для перевірки підозрілих ресурсів у безпечному віртуальному середовищі. Проаналізовано види пісочниць комп'ютерних систем та механізм дії. Наведено перелік найбільш популярних пісочниць.

Ключові слова: *віруси, пісочниця, віртуалізація*

In the work described solutions for checking suspicious resources in a secure virtual environment. The types of sandboxes of computer systems and the mechanism of action are analyzed. A list of the most popular sandboxes is listed.

Keywords: *viruses, sandbox, virtualization.*

Часто бувають випадки, коли користувач завантажив програму, проте має сумніви чи підозри, що вона може бути заражена вірусами. Для того, щоб не нанести шкоду своєму комп'ютеру, щоб не потрапити на гачок шахраїв існує рішення перевірки підозрілих ресурсів у безпечному віртуальному середовищі, які називаються пісочниці (Sandbox).

Пісочниця – жорстко контрольований набір ресурсів для виконання гостьової програми. Доступ до мережі, системних ресурсів операційної системи, пряме зчитування інформації з пристроїв введення найчастіше або частково симулюються, або сильно обмежуються [1].

Підвищена безпека виконання коду в пісочниці передбачає захист системи від великих навантажень саме тому деякі види пісочниць використовують для запуску непідлагодженого або шкідливого коду.

Існують такі види «пісочниць» [1]:

1. Аплети, які виконуються у віртуальній машині або інтерпретаторі, що дає змогу запускати Java-код із будь-яких веб-сайтів без загрози операційній системі.

2. Так звані «в'язниці» (jail, chroot jail) також дають можливість вводити обмеження ресурсів для користувачів і процесів деяких ОС.

3. Віртуальні машини, які повністю симулюють стандартний комп'ютер.

Крім обмеження шкідливого й неперевіреного коду, пісочниці також використовуються в процесі розробки програмного забезпечення для запуску «сирого» коду, який може випадково пошкодити систему або зіпсувати

складну конфігурацію.

Оригінальна модель безпеки [1, 2], що надається платформою Java, відома як модель пісочниці (рис. 1), яка існувала для того, щоб забезпечити дуже обмежене середовище для запуску ненадійного коду, отриманого з відкритої мережі. Суть моделі пісочниці полягає в тому, що локальному коду довіряють повний доступ до життєво важливих системних ресурсів (наприклад, до файлової системи), тоді як завантажений віддалений код (аплет) не є надійним і може отримати доступ лише до обмежених ресурсів, наданих усередині пісочниці.

Загальна безпека забезпечується за допомогою ряду механізмів. Перш за все, мова є строго типізована та простою у використанні. Є надія, що навантаження на програміста буде така, що ймовірність здійснення незначних помилок буде менше в порівнянні з використанням інших мов програмування, таких як C або C ++. Такі мовні функції, як автоматичне керування пам'яттю, прибирання сміття та перевірка діапазону рядків і масивів, є прикладами того, як мова допомагає програмісту писати безпечний код.

По-друге, компілятори і верифікатор байт-коду забезпечують виконання тільки допустимих байт-кодів Java. Верификатор байт-коду разом з віртуальною машиною Java гарантує мовну безпеку під час виконання.

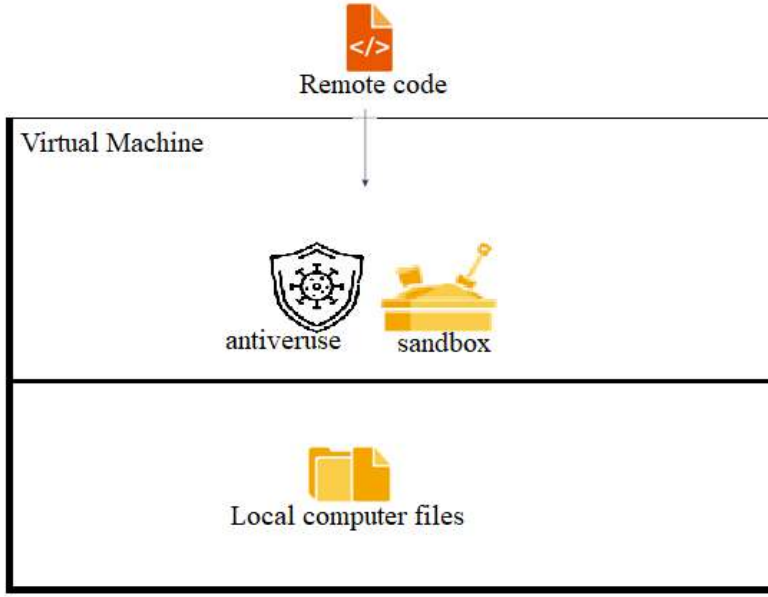


Рис. 1. Принцип дії пісочниці

Більш того, завантажувач класів визначає локальний простір імен, яке можна використовувати, щоб гарантувати, що ненадійний аплет не може втручатися в роботу інших програм.

Нарешті, доступ до критично важливих системних ресурсів забезпечується віртуальною машиною Java і заздалегідь перевіряється класом Security Manager, який обмежує дії частини ненадійного коду до мінімуму.

На сьогодні створено значне число пісочниць. До найбільш популярних для ОС Windows належать [3]: BitBox (Browser in the Box), BufferZone, Sandboxie, SHADE Sandbox, Toolwiz Time Freeze, Shadow Defender, Virtual Machine (Oracle).

Прикладом реалізації пісочниці є Qubes OS. Це операційна система, яка покликана забезпечити безпеку через ізоляцію. Віртуалізація здійснюється на базі Xen. Призначене для користувача середовище може бути засноване на Fedora, Debian, Whonix, Windows та інших операційних системах [3].

Qubes реалізує підхід «безпека в ізоляції». Передбачається, що не може бути ідеального, безпомилкового середовища робочого столу. Таке середовище налічує мільйони рядків коду, мільярди програмних / апаратних взаємодій. Одна критична помилка може призвести до того, що шкідливе програмне забезпечення візьме контроль над машиною.

У Qubes ізоляція забезпечується в двох вимірах: апаратні контролери можуть бути виділені в функціональні домени (наприклад, мережеві домени, домени контролера USB), тоді як цифрове життя користувача визначається в доменах з різним рівнем довіри. Наприклад: робоча область (найбільш довірена), домен покупок, випадковий домен (менш довірений). Кожен з цих доменів запускається на окремій віртуальній машині.

Інформаційні джерела

1. Пісочниця (комп'ютерна безпека). [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Пісочниця

2. The Original Sandbox Model [Електронний ресурс]. Режим доступу: https://docs.oracle.com/en/java/javase/11/security/java-se-platform-security-architecture.html#GUID-D6C53B30-01F9-49F1-9F61-35815558422B

3. 7 of the Best Sandbox Applications for Windows 10). [Електронний ресурс]. Режим доступу: https://www.maketecheasier.com/best-sandbox-applications-windows10

УДК 004.588

АНАЛІЗ ЗАХИЩЕНОСТІ СЕРВІСІВ ВІДЕОЗВ'ЯЗКУ

Тихолаз Д., Бумба І., Шабатура М.М.
Національний університет «Львівська політехніка», м. Львів

Розглянуто сучасні платформи забезпечення відеозв'язку. Проаналізовано стан захищеності для найбільш популярних сервісів Microsoft Teams, Zoom, Google Meet та їх недоліки. Наведено таблицю їх порівняння.
Ключові слова: *відео-конференції, передача даних, віртуальний простір.*

The modern video conferencing software is considered. Discovered security status of the most popular services, such as Microsoft Teams, Zoom, Google Meet. The comparison table is given.
Keywords: *video conferencing, data transfer, virtual space.*

Спалах коронавірусної хвороби (COVID-19) спричинив ізоляцію людей від родини, друзів та ділових партнерів. Ця ситуація сприяла різкому зростанню рівня використання відеоконференцій для різноманітних цілей у бізнесі та особистому житті людей. Пандемія змушує більшість із нас працювати і навчатися вдома, а також відвідувати віртуальні сімейні та соціальні заходи. Як результат, освітяни та споживачі звертаються до більш масштабних, більш надійних рішень для відеоконференцій корпоративного рівня.

Необхідність та корисність спричинила високе різноманіття платформ і конкуренцію на ринку. Таким чином деякі програми повністю втрачають попит, поки інші постійно вдосконалюються, спрощують інтерфейс, збільшують можливості і намагаються звести до мінімуму загрози інформаційній безпеці, які постійно оновлюються через поширеність такого виду обміну даними.

Популярними платформати для відео-конференцій є Cisco Webex Meetings, FaceTime, Google Meet, GoToMeeting, Messenger Rooms, Microsoft Teams, Slack, Webinar Meetings, WhatsApp, Zoom.

У роботі зосередимось на трьох Microsoft Teams, Zoom та Google Meet, оскільки саме ці ресурси є найбільш популярними серед освітян.

Microsoft Teams вимагає обов'язкового використання захищеного з'єднання і застосовує протокол SRTP для передачі даних. Авторизація користувачів відповідає вимогам специфікацій OAuth, а контент додатково шифрується алгоритмом AES (256-біт). Сервіс підтримує багатофакторну автентифікацію, а також використовує засоби Advanced Threat Protection (ATP) для контролю дій додатків, безпеки посилань і блокування передачі

шкідливих файлів. Функції безпеки також включають кімнати очікування, гнучкий розподіл прав учасників конференції на підставі рольової моделі, обмежений гостьовий доступ. Всі дані Teams зберігаються в розподілених дата-центрах Microsoft, і адміністратор системи бачить, в якому регіоні розташовані сервери, які опрацьовують інформацію конкретного додатка. Сервіс надає користувачеві можливість видалити накопичені дані про себе як з локальних пристроїв, так і з серверів Microsoft [1].

До недоліків безпеки Microsoft Teams можна віднести відсутність наскрізного шифрування даних. Навесні цього року в рішенні виявили баг, експлуатація якого могла призвести до злому призначеного для користувача аккаунта через шкідливий GIF-файл.

Zoom. З точки зору безпеки Zoom надає користувачеві передати дані по захищеному HTTPS-з'єднання. Шифрування переданих даних 256-бітовим алгоритмом AES GCM. Аутентифікація користувача за допомогою логіна і пароля або технології єдиного входу (SSO). Обмеження доступу до конференції по паролю. Кімнати очікування для учасників, які дозволяють організатору відеоконференції не допускати неперевірених учасників.

Проте існують недоліки, які можуть вплинути на його безпеку, а саме Zoom не забезпечує наскрізного шифрування даних. Крім того, ІБ-фахівці регулярно виявляють в Zoom уразливості, частина з яких могла стати причиною витоку даних. У квітні цього року дослідники виявили, що в ряді випадків сервіс використовує більш слабке 128-бітове шифрування контенту, а ключі безпеки передає через сервери, розташовані в Китаї. Zoom не надає користувачеві можливостей видалення даних про себе зі сховищ сервісу, проте дозволяє управляти інформацією на стороні клієнта [1, 2].

Google Meet. Компанія Google заявляє, що всі комунікації між клієнтом і хмарними серверами шифруються, сервіс підтримує стандарти безпеки IETF для Datagram Transport Layer Security і Secure Real-time Transport Protocol [3]. У рішенні доступна двухфакторная автентифікація декількох типів. У програмі реалізований ряд обмежень для зовнішніх учасників, що підключаються до конференції через код зустрічі. Вхід користувачів в конференцію повинен бути схвалений адміністратором, а саме підключення стає доступним лише за 15 хвилин до початку зборів. Управління користувальницької інформацією реалізовано в рамках стандартної політики конфіденційності для продуктів Google і допускає видалення інформації як з сервера, так і з клієнтського пристрою. Проте Google Meet не підтримує наскрізне шифрування даних, що залишає зловмисникам можливість перехоплення інформації.

У табл. 1 наведено порівняння декількох платформ.

Таблиця 1

Порівняння платформ для відео-конференцій

Назва ресурсу	Шифрування даних	Двох факторна автентифікація	Наявність кімнати очікування	Функція управління персональними даними на стороні клієнта	Функція управління персональними даними на сервері	Кількість вразливостей за MITRE
Cisco Webex Meetings	+	+	+	+	-	11
Google Meet	-	+	+	+	+	0
Microsoft Teams	-	+	+	+	+	1
Slack	-	+	-	-	-	6
Zoom	-	-	+	+	-	14

Отже, найбільш захищеним сервісом відеозв'язку є Cisco Webex Meetings, оскільки відбувається наскрізне шифрування, тобто у шифруванні беруть участь лише ті користувачі, що беруть участь в спілкуванні чи мають доступ до повідомлень і не має можливості отримати доступ до криптографічних ключів з боку третіх осіб [4].

Рішення використовувати ту чи іншу платформу для відеоконференцій справа індивідуальна, проте варто взяти до уваги недоліки кожної з платформ та зрозуміти можливі наслідки щодо втрати даних чи конфіденційності загалом.

Інформаційні джерела

1. Zoom/Microsoft Teams - Major Security Concerns Comparison Report. [Електронний ресурс]. Режим доступу: https://medium.com/@rgreenhagen/zoom-microsoft-teams-major-security-concerns-comparison-report-6ec34215e1d4

2. Privacy-and-Security. [Електронний ресурс]. Режим доступу:https://zoom.us/privacy-and-security

3. Сравнение сервисов видеоконференций с точки зрения их безопасности. [Електронний ресурс]. Режим доступу: https://www.anti-malware.ru/compare/Video-conferencing-software-security

4. Наскрізне шифрування. [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Наскрізне_шифрування

Напрям 4

БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ

УДК 004.78

ДОСЛІДЖЕННЯ ЗАГРОЗ ДЛЯ ВІРТУАЛЬНОЇ ІНФРАСТРУКТУРИ ХМАРИ ТА МЕТОДИ ЇЇ ЗАХИСТУ

Жолубак Л., Смотр О.О.
Львівський державний університет безпеки життєдіяльності, м. Львів

Роботу присвячено розгляду можливих загроз для віртуальної інфраструктури, зокрема середовища для збереження даних, так званої хмари.
Ключові слова: *віртуальна інфраструктура, хмарні технології, інфраструктура.*

The work is devoted to the consideration of possible threats to the virtual infrastructure that creates an environment for data storage, the so-called cloud.
Keywords: *virtual infrastructure, cloud technologies, infrastructure.*

На даний час дата-центри наступного покоління розмивають кордони між фізичними та віртуальними середовищами, між публічними і приватними хмарами, що призводить до розширення ряду питань щодо захисту інформації в хмарних обчисленнях і для вирішення яких потрібні постійно удосконалюючі рішення.

Забезпечення фізичної безпеки лежить на основі суворого контролю фізичного доступу до серверів та мережевої інфраструктури. Мережева безпека заснована на побудові надійної моделі загроз, що враховує захист від вторгнень і міжмережевий екран, з метою розмежування внутрішніх мереж дата-центрів на підмережі з різним рівнем довіри.

У хмарних обчисленнях технологія віртуалізації відіграє особливу роль і полягає у [1]:

– віртуалізації серверів - перенесення фізичних серверів у віртуальні машини однієї хостової системи, оснащеної гіпервізором - засобом віртуалізації;

– віртуалізації робочих користувальницьких місць - централізоване зберігання робочих місць у вигляді віртуальних машин на хостовій системі з наданням роздільного доступу по мережі з фізичних робочих місць;

– віртуалізації терміналів - для окремого користувача терміналу в операційній системі створюється власний сеанс роботи.

Концепція хмарних технологій полягає в наданні користувачам віддаленого динамічного доступу до послуг, обчислювальних ресурсів і додатків, включаючи операційні системи та інфраструктуру через різні канали доступу, в тому числі і через Інтернет. Така великомасштабна інфраструктура являє

підвищені ризики і досить обмежену можливість контролю над її ресурсами. У цьому і полягає актуальність проблем хмарних обчислень - захист інформації та довірливе ставлення користувачів до хмарних провайдерів.

Застосування спеціалізованого програмного забезпечення для віртуального середовища вимагає значної зміни у підходах до забезпечення інформаційної безпеки хмарних систем.

Вирішення задач забезпечення безпеки об'єднує в собі традиційні та специфічні рішення з особливостями, які в процесі виконання задач повинні оптимізовуватись для економії продуктивності віртуального середовища із забезпеченням захисту інформації і хмарних ресурсів.

Для забезпечення безпеки і збереження цілісності даних досліджуються актуальні загрози для віртуальної інфраструктури хмари [2, 3]:

– відсутність контролю внутрішньо мережевого трафіку, а також можливість прослуховування всього трафіку між віртуальними машинами;

– єдине сховище віртуальних машин, над якими можна отримати контроль;

– захоплення всіх ресурсів хоста віртуалізації однією віртуальною машиною, в результаті якого інші віртуальні машини можуть викликати відмову в обслуговуванні;

– незахищеність вразливих місць дискової підсистеми віртуальних машин;

– компрометація клієнтських терміналів і атака на браузери клієнтів;

– несанкціонований доступ до ресурсів віртуалізації через гіпервізор;

– перехоплення аутентифікаційних даних для доступу до хмари через хмарні API;

– несанкціонований доступ до консолі управління віртуальним середовищем;

– відсутність у віртуальній інфраструктурі розподілених комутаторів, які при міграції віртуальних машин дозволяють погоджувати політику безпеки;

– перехоплення даних при передачі по незахищених зовнішніх каналах зв'язку.

Одним з головних джерел загрози безпеки є сервер централізованого управління віртуальної інфраструктури, отримавши контроль над яким, зловмисник отримує повний доступ до всіх віртуальних машин, хостів віртуалізації, віртуальних мереж і сховищ даних. Тому необхідно, ретельно захищати сам сервер управління, звертати посилену увагу на засоби автентифікації і розмежування прав доступу, для чого має сенс використовувати додаткове програмне забезпечення, що розроблене спеціально для віртуальних інфраструктур. Доступ до сервера віртуалізації повинен здійснюватися за безпечними протоколами, а доступ адміністраторів повинен бути обмежений за IP-адресами.

Важливо також, щоб мережі управління віртуальною інфраструктурою та виробничого середовища віртуальних машин були розділені логічно і фізично для запобігання несанкціонованого втручання. Для забезпечення захисту даних у хмарі, які розміщені за межами сфери фізичного

доступу клієнта, здійснюють шифрування віртуальних жорстких дисків. При зчитуванні з диска дані розшифровуються і при записі на диск зашифровуються. При цьому ключі зберігаються на окремому сервері, який спочатку перевіряє ідентифікаційні дані і цілісність хмарного сервера, який направив запит. У разі позитивного відгуку надається ключ і хмарний сервер отримує доступ до інформації та ресурсів хмари.

Більш потужний варіант безпеки даних - це комбінування технологій шифрування даних і захищеної передачі. Тобто використовувати системи виявлення вторгнень і міжмережевого екранування з контролем зовнішніх підключень до середовища віртуалізації за допомогою апаратних рішень, а внутрішніх - за допомогою програмних рішень.

Для антивірусного захисту віртуальних машин краще використовувати безагентний підхід, що забезпечує комплексну безпеку без установки агентського модуля в захищеній системі, тобто у віртуальне середовище впроваджується віртуальний пристрій - шлюз безпеки, який бере на себе функції антивірусу для всіх віртуальних машин.

Наступними ефективними засобами захисту хмар є:

– довірене завантаження серверів віртуалізації, віртуальної машини, серверів управління віртуалізацією;

– сегментування віртуальної інфраструктури для обробки персональних даних користувачем або групою користувачів;

– ідентифікація та автентифікація доступу та об'єктів доступу у віртуальній інфраструктурі, в тому числі, адміністраторів управління засобами віртуалізації;

– управління доступом суб'єктів доступу до об'єктів доступу у віртуальній інфраструктурі, в тому числі всередині віртуальних машин;

– управління потоками інформації між компонентами віртуальної інфраструктури, а також по периметру віртуальної інфраструктури.

Підсумовуючи вищенаведене, можна стверджувати, що вірно підібрані рішення безпеки дозволяють отримати уявлення про рівень використовуваних ресурсів і своєчасно виявити атаки, які націлені на різні хмарні об'єкти.

Інформаційні джерела

1. Котяшичев И. А. Защита информации в «Облачных технологиях» как предмет национальной безопасности / И. А. Котяшичев, Е. А. Бырылова // Молодой ученый. — 2015. — №6.4. — С. 30-34.

2. Віблий В.М. Безпека інформації у хмарних сховищах / В.М. Віблий, О.О. Смотр // збірник тез доповідей ІІІ Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів "Захист інформації в інформаційно-комунікаційних системах", м. Львів, 28 листопада 2019 року. Львів, ЛДУ БЖД, 2019, – с.88-90.

3. Ладигіна О.А. Перспективи захисту інформації в хмарних обчисленнях від атак на засоби віртуалізації // Збірник тез доповідей науково-практичної конференції «Інформаційні технології та комп’ютерна інженерія».- Кіровоград: КНТУ, 2014. – 164 с.

УДК 004.056.53

АНАЛІЗ ПРИНЦИПІВ РЕАЛІЗАЦІЇ МЕТОДІВ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ В СУЧАСНИХ ПРОГРАМНИХ ДОДАТКАХ

Самара Н. М., Бурак Н. Є.
Львівський державний університет безпеки життєдіяльності, Львів

У роботі здійснено огляд сучасних методів автентифікації та проведено аналіз принципів реалізації методів двофакторної автентифікації в сучасних програмних додатках

Ключові слова: *автентифікація, захист, програмні модулі, інформація.*

The paper reviews modern methods of authentication and analyzes the principles of two-factor authentication methods implementation into modern software applications

Keywords: *authentication, protection, software modules, information.*

Інтернет є невід'ємною частиною життя сучасної людини. Безперервний стрімкий розвиток даної мережі призводить до збільшення кількості різноманітних веб-застосунків, що використовуються для будь-яких сфер діяльності. Керований доступ до наданих сервісів та персоналізація контенту – в цьому полягає сучасна тенденція створення веб-застосунків.

Поруч з великою кількістю переваг їх застосування, існує і велика кількість недоліків. Вразливості веб-застосунків є одним з найбільш поширених шляхів проникнення в інформаційні системи та витоку особистої інформації користувачів. У зв'язку з цим підвищуються вимоги до методів автентифікації та авторизації клієнтів.

Оскільки, кількість веб-застосунків зростає з кожним днем, і мати окремий логін та пароль для кожного сайту дуже важко для запам'ятовування. Це може призвести або до небезпечного зберігання такої «бази» на персональному комп'ютері користувача, або до використання для всіх сайтів однієї і тієї ж пари (логін, пароль). Існує багато методів підвищення безпеки автентифікації в наш час. Одним з найнадійніших є використання сервісів автентифікації, що розроблені згідно світових стандартів автентифікації.

Незважаючи на простоту у використанні, застосування цих додатків значно сприяє унеможливленню несанкціонованого входу до інформаційної системи.

Загалом, методи автентифікації діляться на три категорії: слабка (однофакторна), сильна (багатофакторна) та строга автентифікацію.

Слабкою називають однофакторну автентифікацію за допомогою пароля. На стійкість даного методу автентифікації значною мірою впливає людський чинник.

Сильною або багатофакторною називають автентифікацію, що використовує декілька факторів автентифікації.

Існує всього три типи факторів:

– фактор знання;

– фактор володіння;

– фактор властивості.

Строга автентифікація є різновидом багатофакторної автентифікації. Ідея строгої автентифікації, що реалізується в криптографічних протоколах, полягає в наступному. Користувач доводить свою автентичність інформаційній системі демонструючи знання будь-якого секрету, який, наприклад, може бути попередньо розподілений безпечним способом між сторонами автентифікаційного обміну. На даний момент строга автентифікація є найбільш стійкою, однак, незважаючи на це, вона не є стійкою до атак, які направлені на мережу чи власне апаратне забезпечення.

Для впровадження строгої автентифікації використовують сервіси автентифікації. Реалізації представлені компаніями-гігантами, наприклад, як Google та Microsoft надають впевненість в їх коректності та стійкості обраних ними факторів автентифікації. Далі розглянемо дані сервіси автентифікації.

Google Authenticator – мобільний застосунок, що використовується для виконання двофакторної автентифікації, в облікових записах Google та сторонніх сервісах. Реалізований для декількох мобільних платформ, не має можливості ініціалізації на декількох пристроях. Секретний ключ можна інтегрувати в застосунок як QR-код, або ввести вручну. Налаштування в застосунку представлені лише засобами синхронізації часу з серверами Google. Автентифікатор генерує 6-ти або 8-мизначний одноразовий пароль, з використанням відкритих стандартів алгоритмів HOTP та TOTP. Дані паролі використовуються в якості другого фактору автентифікації і вводяться після коректного введення логіну та паролю. Пароль дійсний протягом 30 секунд, що запобігає використанню його кілька разів.

Microsoft Authenticator – мобільний застосунок, який допомагає входити в облікові записи, виконуючи двофакторну автентифікацію. Працює з будь-яким обліковим записом, який використовує двофакторну автентифікацію та підтримує одноразові паролі (TOTP).

Даний додаток можна використовувати кількома способами, включаючи:

1. Після входу з іменем користувача та паролем в застосунок надходить запит на автентифікацію.

2. Вхід без введення пароля, використовуючи ім'я користувача, застосунок автентифікації та мобільний пристрій, використовуючи відбиток пальця, обличчя або PIN-код.

3. Як генератор коду для будь-яких облікових записів, які підтримують програми автентифікації.

В якості генератора кодів Microsoft Authenticator генерує шестизначний пароль, який відображається під кожним доданим обліковим записом. Пароль дійсний протягом 30 секунд, що запобігає використанню коду кілька разів. Ініціалізація облікового запису проходить шляхом сканування QR-коду, або введення коду вручну. Не має можливості ініціалізувати один обліковий запис в декількох застосунках на різних пристроях одночасно.

Отже, у загальних принципах, Google Authenticator і Microsoft Authenticator виконують однакову роботу і працюють подібними способами. Однак необхідно відзначити, що Microsoft пропонує більш комплексний продукт. Це не тільки можливість синхронізації декількох пристроїв, але і можливість створення резервної копії, яка буде важливою, якщо користувачеві коли-небудь потрібно буде отримати новий телефон. Крім того, якщо користувач щодня користується продуктами Microsoft, використання автентифікатора від того самого розробника полегшує підключення до відповідних облікових записів - користувачам просто потрібно натиснути сповіщення.

Інформаційні джерела

1. Чунарьова А. В. Аналіз існуючих шаблонів систем автентифікації в інформаційно-комунікаційних системах та мережах / А. В. Чунарьова, А. В. Чунарьов // Безпека інформації: наук.-практ. журнал. – 2012. – № 2 (18). – С. 65–70.

2. Ляшенко, Г.Є & Астраханцев, А.А. (2017). Дослідження ефективності методів біометричної автентифікації. Системи обробки інформації. 2(148). 111-114. https://doi.org/10.30748/soi.2017.148.20

3. Иванов Вадим Вадимович, Лубова Елена Сергеевна, and Черкасов Денис Юрьевич. "Аутентификация и авторизация" Проблемы современной науки и образования, no. 2 (84), 2017, pp. 31-33.

4. Мушинський А.О. Інформаційна безпека пристроїв IoT // Проблеми та перспективи розвитку системи безпеки життєдіяльності: Зб. наук. праць XV Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів. – Львів: ЛДУ БЖД, 2020. – С. 214-216.

УДК 004.4

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ СИСТЕМИ AZURE LOG ANALYTICS ДЛЯ АНАЛІЗУ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ХМАРНИХ РІШЕННЯХ

Сусукайло В., Опірський І.
Національний університет "Львівська політехніка", м. Львів

В даній статті досліджено особливості та можливості рішення Azure Log Analytics, який дозволяє аналізувати інциденти та події інформаційної безпеки у хмарному середовищі Azure. Дане дослідження дає змогу проаналізувати проблему моніторингу хмарних рішень Azure.

Ключові слова: *Azure, Log Analytics, хмарне середовище, API, SDK.*

This article explores the features and capabilities of the Azure Log Analytics solution, which allows cybersecurity professional to analyze information security incidents and events in the Azure cloud environment. This research analyzes the problem of monitoring Azure cloud environment.

Keywords: *Azure, Log Analytics, cloud environment, API, SDK.*

Вступ

Хмарні технології все більше використовуються з кожним днем для побудови комплексних застосунків. Хоча хмара має гнучкість, яка надає розробникам та організаціям свободу розпочати експерименти та масштабування, вона також несе велику відповідальність за вирішення підвищеної площі загрози безпеці.

У умовах пандемії все більше організацій почали використовувати хмарні рішення для забезпечення неперервності процесів. Це зумовило те, що забезпечення належного рівня безпеки інформації у хмарних рішенням стало пріоритетним завданням експертів з кібербезпеки.

Хмарна безпека є спільною відповідальністю хмарного постачальника та замовника. У міру зростання хмарних технологій потрібно застосовувати заходи безпеки, що забезпечать конфіденційність, цілісність та доступність інформації що ними обробляється тому вендори хмарних рішень розробляють власні сканери вразливостей та системи моніторингу подій [1]. Одним з таких застосунків є Azure Log Analytics – технологія дослідження подій у хмарному середовищі Azure та частина Центру Безпеки Azure.

Аналіз можливостей Azure Log Analytics для дослідження кіберзлочинів у хмарному середовищі Azure

Log Analytics є частиною загального рішення для моніторингу Microsoft Azure. Log Analytics контролює хмарні та локальні середовища, щоб підтримувати доступність та продуктивність як кінцевих точок так і корпоративних сервісів [2]. Azure Log Analytics, як інструмент дослідження подій у хмарному середовищі Azure може виконувати наступні функції:

1. Збір інформації- деталізовані сучасні показники та журнали - із ресурсів Azure та локальної інфраструктури.

2. Візуалізація - вбудовані інформаційні панелі для візуалізації, які допоможуть швидко зрозуміти що сталось.

3. Аналіз - аналітика програм та інфраструктури.

4. Реагування- автоматичне реагування на інциденти.

5. Інтеграція - використання 20+ партнерських інтеграцій та відкриту структуру з API та SDK.

Дані функції дають змогу зрозуміти, що за допомогою Log Analytics експерти з кібербезпеки здатні не лише досліджувати події але й реагувати на них. Тому Log Analytics можна віднести до SIEM подібних систем моніторингу інфраструктури організації яка знаходиться в хмарі. Також однією з переваг Azure Log Analytics для використання як центральної системи моніторингу подій є те, що застосунок доступний для управління використовуючи загальний менеджмент центр Azure, що забезпечує можливість безпечного доступу до нього з будь якої ділянки світу, та й відповідно мінімізує ризик втрати доступності сервісу.

В умовах забезпечення безперервності процесів в організації однією з вагомих потреб є можливість використання агентного підходу. Це дає змогу забезпечити безперервний монтіторинг подій для організації. У випадку з Azure, програмний застосунок – агент встановлюється на кінцеву точку для збору інформації та передання її до центрального сервісу моніторингу подій [3]. Для дослідження зібраної інформації у Azure Log Analytics використовується мова побудови запитів Azure. Комбінуючи різні запити в один, можна виявити підозрілу активність. Для прикладу в даному дослідженні ми вказуємо запит, який визначає потенційну атаку типу Bruteforce для бази даних:

```
search *
| where Type == "SQLAuditLog" and TimeGenerated > ago(3m)
| where ActionName_s == "DATABASE AUTHENTICATION FAILED"
| summarize FailedAuth=count() by ServerPrincipalName_s
| where FailedAuth > 5
```

На основі запиту експерти з кібербезпеки можуть створити нотифікацію про атаку будь якого типу типу та відповідно вчасно зреагувати на загрозу.

Висновок. Враховуючи даний аналіз можна зробити висновок, що функціонал Azure Log Analytics є досить широкий та може стати зручним інструментом дослідження кіберзлочинів. Для фахівця з кібербезпеки завжди було досить важливим моментом в роботі бути завжди в змозі зреагувати на потенційно шкідливі події, знати що відбувається на серверах і отримувати своєчасно повідомлення і звіти. Так як в сервісі консолідуються дані зі всіх підключених активів, вказуються запити пошуку шкідливих подій та статистика відображається у вигляді графіків, експерти з кібербезпеки бачать повну картину кібератак.

Інформаційні джерела

1. Rich Mogull, James Arlen, Francoise Gilbert, Adrian Lane, David Mortman, Gunnar Peterson, Mike Rothman,The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, 2017 Cloud Security Alliance, p.31.

2. Tender P. De., Rendon D., Erskine S., “Optimizing IT Operations Using Azure Monitor and Log Analytics” Pro **Azure** Governance and Security, 2019 – Springer.

3. Веб ресурс: https://docs.microsoft.com/en-us/azure/azure-monitor/

Напрям 5

КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056:061.68

ПОРІВНЯЛЬНИЙ АНАЛІЗ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ В БЕЗПРОВІДНИХ МЕРЕЖАХ

Дудикевич В. Б., Микитин Г. В., Ленник М. В.
Національний університет «Львівська політехніка», Львів

Вступ. Процеси передавання/приймання інформації, зокрема безпровідними мережами (БМ), займають один з головних сегментів в стратегії інтелектуалізації суспільства. Безпеку безпровідних мереж визначають основні профілі – конфіденційність, цілісність, достовірність інформації. Однією з основних технологій захисту інформації в БМ є криптографічні алгоритми шифрування. Розглянемо їх порівняльний аналіз.

Безпровідні мережі. В табл. 1 наведено класифікацію безпровідних мереж залежно від радіуса дії [1].

Таблиця 1

Безпровідні мережі залежно від радіусу дії

Клас	Приклади стандартів	Радіус дії
Безпровідна глобальна мережа (WWAN)	супутникові; стільникові: UMTS, GSM, LTE;	десятки і тисячі км
Безпровідна міська мережа (WMAN)	IEEE 802.16 (Wi-MAX)	декілька км
Безпровідна локальна мережа (WLAN)	IEEE 802.11 (Wi-Fi)	~100м – 1км
Безпровідна персональна мережа (WPAN)	802.15.1(Bluetooth); 802.15.4a (ZigBee)	~10м

Криптографічні протоколи та алгоритми. Для захисту інформації в мережах *GSM/GPRS* використовується криптографічний протокол

TCP/IP, алгоритми шифрування A5/1, A5/3, довжина ключа 64 біт. Призначення: шифрування набору триплетів, що передаються між модулем і базовою станцією, обчислення сеансового ключа. A5/3 реалізований на апаратному рівні і враховує особливості обробки сигналів в мобільних телефонах, причому шифрується не лише голосовий трафік, але і дані, що передаються по безпровідному каналу.

Для захисту інформації в мережах *3G/UMTS* та *LTE/*4G використовується криптографічний протокол AKA, алгоритм шифрування A5/3, довжина ключа 64 біт. Призначення: шифрування набору триплетів, що передаються між модулем і базовою станцією, обчислення сеансового ключа.

В мережі *WiMAX* стандарт IEEE 802.16 використовує алгоритм DES в режимі зчеплення блоку шифрів для шифрування даних, згодом DES3(Triple DES). В даний час DES вважається небезпечним, тому у додатку до стандарту IEEE 802.16 е для шифрування даних був доданий алгоритм AES. Алгоритм захисту виконується на фізичному рівні.

В *Wi-Fi* мережах використовувались криптографічний протокол WEP, алгоритм шифрування RC4, довжина ключа 64-128 біт; криптографічні протоколи WPA, TKIP алгоритм шифрування AES, довжина ключа 128 біт, алгоритм шифрування SHA, довжина ключа 128 біт. Призначення: шифрування переданої інформації.

Зараз ці протоколи замінені на WPA2. Варто зауважити, що в WPA2 підтримується шифрування відповідно до стандарту. Також розробляється WPA3 де буде відбуватись шифрування без автентифікації за допомогою використання Opportunistic Wireless Encryption (OWE).

В *Bluetooth* мережі використовуються протоколи SSP, Shared Secret, LMP, алгоритм шифрування AES-CCM, довжина ключа 8-128 біт, алгоритм E0, довжина ключа 128 біт. Призначення: шифрування переданої інформації.

В *ZigBee* – всі пакети з даними передаються тільки в зашифрованому вигляді за допомогою 128-біт алгоритму AES**.**

Порівняльний аналіз алгоритмів шифрування. Для порівняльного аналізу криптографічних алгоритмів вибрано симетричні алгоритми блокового шифрування. За порівняльні параметри обрано: розмір блоку, довжина ключа, швидкодія, мінімальна кількість циклів, для якої шифр є стійким, число раундів, обчислювальну складність відновлення ключа шифрування під час здійснення успішної атаки, а також назву найменш витратного способу успішного криптоаналізу/атаки (табл. 2) [2].

Таблиця 2

Порівняння характеристик алгоритмів симетричного шифрування

Назва алгоритму	Розмір блоку (біт)	Довжина ключа (біт)	Швидкодія (Мбіт/с)	Мін. кільк. циклів, для якої шифр є стійким	Показники атак		Назва найменш витратного способу криптоаналізу/атаки	Число раундів
					Макс. кільк. циклів	Обчисл. складність відновлення ключа шифр.		
AES (Rijndael)	128	128	2525.89	9	8	2^{32}	Диференційний	10
		256	1993.53					14
DES	64	56	Висока			2^{56}	Лінійний	16
Triple DES	64	168	88.67			2^{112}		48
Kalyna	128	128	2611.77	5	3	$2^{52.8}$	Лінійний	10
		256	1779.52					14
	256	256	2017.97	7	5	$2^{220.8}$	Лінійний	14
		512	1560.89					18
	512	512	1386.46	9	7	$2^{470.4}$	Лінійний	18
GOST 28147-89	64	256	639.18					32/16
Kuznye-chik	128	256	1081.08	6	5	$2^{140.3}$	Зустріч посередині	10
TWO-FISH	128	192	2600					16
		256	5200					
RC6	128	128	1300	13	12	2^{119}	Статистичні відмінності	20
		192		15	14	2^{122}		
		256		16	15	2^{215}		
		Від 256 - 2040						
RC5	32	40 - 2040		6	5	2^{24}	Диференційний	12
	64			11	10	2^{45}		
	128				12	2^{53}		
Blow-fish	64	32- 448	Висока	16	7	2^{24}	Атака з відомою функцію F(x)	16

Висновки. Порівняльний аналіз алгоритмів симетричного блокового шифрування в безпровідних мережах показує, що ефективно забезпечують конфіденційність, цілісність, доступність інформації тільки AES, Kalyna і TWOFISH, оскільки саме їм властивий високий ступінь криптостійкості при великій швидкодії.

Інформаційні джерела

1. Превентивні та реактивні механізми безпеки в бездротових традиційних та AD-HOC мережах / Гладиш С. В. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2009. – Вип. 1(18). – С. 111-112. – Режим доступу: https://ela.kpi.ua/handle/123456789/9794.

2. Ефективна реалізація алгоритму блокового симетричного шифрування ДСТУ 7624:2014 («Калина») для 8/16/32-бітових вбудованих систем / Я. Р. Совин, В. І. Отенко, Є. Ф. Штефанюк / Сучасний захист інформації. 2017. № 3. С. 6-16. Режим доступу: http://nbuv.gov.ua/UJRN/szi_2017_3_3.

РОЛЬ СТЕГАНОГРАФІЇ У СУЧАСНОМУ ЗАХИСТІ ІНФОРМАЦІЇ

Мальцева Н., Полотай О.
[1]Кафедра безпеки інформаційних технологій Національного університету «Львівська політехніка», м. Львів
[2]Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів

У роботі наведено практичне використання стеганографії, роль даного напряму в захисті інформації, приведено результати виконаного дослідження із приховування файлів у стегоконтейнері.

Ключові слова: *стеганографія, секретний ключ, стегоконтейнер, приховування інформації.*

This work presents the practical use of steganography, the purpose and objectives of this area in the information security and also contains results of the research based on hiding files in the stegocontainer.

Key words: *steganography, secret key, stegocontainer, information hiding.*

В першу чергу, визначимо поняття стеганографії. Стеганографія — наука, предметом якої є приховування факту присутності секретної інформації. Саме в цьому і полягає відмінність даної науки від не менш поширеного напрямку захисту інформації — криптографії, при використанні якого читання вмісту повідомлення стає неможливим.

Сучасну стеганографію прийнято розділяти на класичну, комп'ютерну і цифрову [1, ст. 65], також виділяють мережеву. Класична пов`язана із приховуванням текстових даних, використовуючи властивості самого тексту або ж навколишнього середовища. З іншого боку — комп'ютерна і цифрова стеганографія, які розглядають методи приховування будь-якої електронної інформації (текст, звуковий файл, зображення, відео, програма) з використанням можливостей інформаційних систем. Мережева стеганографія використовує можливості протоколу передачі даних транспортного рівню – TCP.

В нашій роботі зосередимось на можливостях цифрової стеганографії, спираючись на розповсюдженність цифрового середовища і розвиток кібернетичного простору [2, ст. 97]. Підґрунтям розвитку стеганографії в останньому десятиріччі можна вважати величезні об'єми графічної інформації, що поширюються у мережі. Тим часом, кожен цифровий об'єкт потенційно може містити приховані дані.

Отже, розглянемо напрями цифрової стеганографії [3]:

– вбудовування інформації з метою її прихованої передачі або ж прихованого зберігання;

– вбудовування цифрових водяних знаків для захисту авторських прав;

– вбудовування ідентифікаційних номерів з метою відстежування наступних дії з даними або контентом і також підтвердження достовірності переданої інформації.

Серед актуальних та практичних застосувань стеганографії слід виділити: можливість вкладення більш таємного файлу у менш таємний, який у свою чергу вкладений у файл-контейнер; шифрування прихованого файлу за допомогою одного з криптографічних алгоритмів (наприклад, потрійний DES, MDC або IDEA); можливість приховування аудіофайлу в іншому звуковому файлі. Тож, стеганографія реалізує захист даних у два кроки: приховує факт наявності даних, а при їх виявленні вимагає проведення автентифікації – введення секретного ключа.

Для досліження ми обрали стеганографічний програмний засіб S-Tools. В ході роботи було виконано приховування у файлі-контейнері різнотипних файлів: аудіофайлу (із розширенням .wav), виконуваної програми (exe), зображення (.bmp), текстового файлу (.txt). Після того ми переглянули оригінальне зображення та модифіковане у двійковому вигляді і визначили, що приховані файли рівномірно розподіляються по бітах файлу-контейнеру з метою приховування самого факту існування таємної інформації.

Під час виконання цього завдання було встановлено, що у файлі зображення (1920×1080 пікселів) обсягом 6 220 854 байт можна приховати 777 584 байт інформації, що становить більше 10% об'єму початкового

файлу. Співвідношення між розміром файлу із зображенням і розміром файлу, який можна приховати, залежить від конкретного випадку, однак при правильному виборі файлу-контейнера, факт використання стеганографічних засобів (не знаючи секретний ключ) встановити і довести практично неможливо. Якщо ж скористатись компресією зображення і приховувати не сам файл, а його архів, то у зображенні меншого розміру можна приховати зображення більшого розміру.

Ми зробили висновок, що для більшої надійності приховування слід використовувати зображення з великою кількістю півтонів та відтінків і не рекомендується – зображення з великими зонами одного кольору.

У випадку аудіофайлу наведемо елементарні розрахунки: нехай перетворення аналогового сигналу у цифровий відбувається із частотою дискретизації 44,1 кГц. Це дозволяє кожну секунду зберігати 44100 біт інформації для монофонічного сигналу та 88200 біт – відповідно для стереофонічного. Отже, у звуці, який триває всього 1 секунду, можна вмістити текст обсягом більш ніж 10 Кбайт. При цьому, в результаті приховування отримується аудіофайл без помітних для слуху втручань, що містить інший закодований прихований файл.

Ми переконались, що при застосуванні стеганографії програми використовують певні алгоритми, які приховують секретні дані серед вмісту контейнера: біти початкового файлу у випадкових позиціях замінюються на біти приховуваного файлу. Таким чином, розмір початкового файлу і файлу-контейнеру (що містить вкладену інформацію) є однаковим, навіть за умови приховуванні різної кількості файлів або різного обсягу даних.

Таким чином, для людини не є можливим визначити, чи були використані засоби стеганографії під час створення певного файлу. Для цього необхідне застосування спеціалізованого програмного забезпечення, проте з причини низької швидкодії воно не може бути використане в промислових об’ємах, а антивірусні програми не виявляють файли-контейнери.

Інформаційні джерела

1. Мельник С. Методи цифрової стеганографії: стан та напрями розвитку // С. Мельник, В. Кащук. // Information Security of the Person, Society and State. – 2013. – №3. – С. 65–70.

2. Шелест М. Комп’ютерна стеганографія та її можливості // М. Шелест, В. Андреев. // Сучасна спеціальна техніка. – 2011. – №24. – С. 97–104.

3. Конахович Г., Прогонов Д., Пузиренко О. Комп’ютерна стеганографічна обробка й аналіз мультимедійних даних [підручник]. — К. : «Центр навчальної літератури», 2018. — 558 с.

УДК 003.26

АЛГОРИТМИ АСИМІТРИЧНОГО ШИФРУВАННЯ

Самсонова М.
Харківський національний університет радіоелектроніки, м. Харків

В цій доповіді розповідається про основи криптографії. Збереження переданої інформації методом асиметричного шифрування. Алгоритм електронного підпису

This report describes the basics of cryptography. Saving the transmitted information by asymmetric encryption. Algorithm of electronic signature.

Люди постійно обмінюємося інформацією, але ми не можемо передбачити що трапиться з об'єктами які ми передаємо по дорозі до адресата. Навіть зараз, коли ми майже миттєво обмінюємся повідомленнями, інформація повинна пройти фізичний шлях з умовної точки А в точку Б. Так, зараз це не паперові листи, але навіть хвилі пересувається в просторі. Та за той невеликий проміжок часу інформацію все рівно можна перехопити. Постає питання як зберегти інформацію у безпеці, та надати їй повну конфіденційність. Цим питанням і займається криптографія.

Нам необхідно передавати інформацію таким чином щоб її міг прочитати лише той кому ми цю інформацію надсилаємо. Перше що спадає на думку це зашифрувати інформацію і передати інструкцію щодо її розшифрування, але потрібно пам'ятати що ці інструкції пройдуть по відкритому каналу зв'язку, та їх також можуть перехопити. Для рішення цієї проблеми використовують асиметричні алгоритми шифрування.

Отримувач повинен розробити шифр та два ключі до нього, один з них – ключ шифровки, а інший – розшифрування. У такому випадку, якщо шифр буде унікальним, отримувач може відправити його та шифрувальний ключ нам. Тоді інформація шифрується за допомогою цього ключа, та нарешті відправляється адресату. У такому випадку, так як шифр унікальний та іншого ключа розшифрування просто немає, перехоплювачі не зможуть розшифрувати інформацію, а адресат розшифровує її ключем що залишився в нього.

Але що якщо зловмисник піде іншим шляхом і вирішить підробити повідомлення? Він перехопить шифр та ключ шифрування і зможе зашифрувати вже інше повідомлення. Тобто хоча інформація не вдасться прочитати, але її можна зіпсувати. Щоб цього не сталося можна використати алгоритм електронного підпису. Принцип буде таким самим, але тепер ми шифруємо електронний підпис в основному шифру. Сенс у тому що потрібно переслати ключ розшифрування адресату, одночасно з тим як він відп-

равляє основний шифр, та код його шифровки. Тепер у отримувача два ключа розшифрування, а у нас два шифру та їх ключи шифрування. Ми шифруємо підпис, а потім шифруємо інформацію разом із цим підписом основним шифром, тож якщо не розшифрувати основний шифр то і зашифрований підпис не отримати. Тепер злочинці не зможуть підробити підпис, тож адресат точно буде знати, чи підроблено повідомлення.

Інформаційні джерела

1. Вильям Столлингс. Криптография и защита сетей: принципы и практика. М.: Вильямс, 2001. ISBN 5-8459-0185-5.
2. Основы криптозащиты АСУ. Под ред. Б. П. Козлова. М.: МО, 1996.
3. J. Menezes, P. C. van Oorschot, S. A. Vanstone. Handbook of Applied Cryptography. — 1997. — ISBN 0-8493-8523-7.
4. Рябко Б. Я., Фионов А. Н. Основы современной криптографии для специалистов в информационных технологиях — Научный мир, 2004. — 173 с. — ISBN 978-5-89176-233-6

WINRAR CRYPTO-PROTECTOR

Ткаченко А.
Львівський державний університет безпеки життєдіяльності, м. Львів

Ключові слова: *криптограма, WinRAR, AES, C#, вихідний файл, криптографічний засіб, стеноґрафічний засіб, Microsoft Visual Studio.*

Проблеми безпеки інформації за останні кілька років набули виключної актуальності. Серед різних методів захисту інформації провідне місце займають криптографічні та стеноґрафічні методи. Знання основних понять криптології, володіння криптографічними методами захисту інформації за сучасних умов вкрай необхідні будь-якому фахівцю, що займається створенням систем захисту інформації.

Я розробив новий тип захисту WinRAR Crypto-protector на мові програмування C#. В цьому захисті поєднуються криптографічні та стеноґрафічні засоби захисту інформації. Суть цього захисту полягає в тому, що створюється звичайний WinRAR-архів з файлами, але в цей архів добавляється зашифрований шифром AES файл, що не відображається у списку файлів архіву. Тепер розглянемо схему побудови цього захисту:

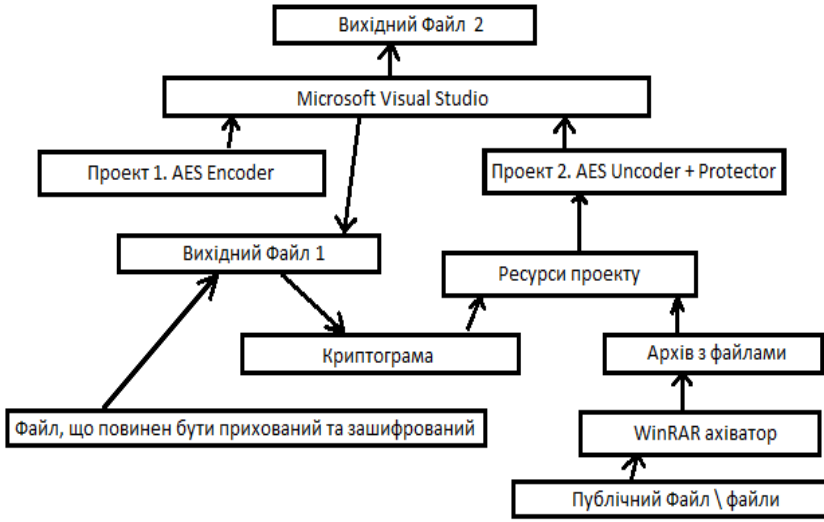


Схема побудови WinRAR Crypto-protector

На схемі видно, що спочатку створюється звичайний WinRAR архів з файлів. Далі створюється “проект 1” в Microsoft Visual Studio, результатом якого буде “вихідний файл 1”, що зчитує будь-який файл і за допомогою шифру AES створює криптограму. Потім створюється “проект 2”. В цей проект компілюється в ресурси криптограма і архів. Вихідний файл якого є ціллю всіх попередніх маніпуляцій. Далі вихідному файлу змінюється розширення з *.exe на *.rar. Відкривши такий архів, можна побачити тільки звичайні файли, компроментація яких не принесе жодної шкоди. Розшифрувати прихований файл можна за допомогою командного рядка, що виконає rar-архів як програму windows з параметрами, в одному з яких міститься пароль для розшифрування криптограми.

Висновок. Отже, ми ознайомились з новим типом захисту інформації, який можна комбінувати з будь-якими іншими криптографічними та стенографічними засобами захисту інформації.

Інформаційні джерела

1. https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography.aes?view=netframework-4.6.2

2. https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography?view=netframework-4.6.2

УДК 004.7

ІНФОРМАЦІЙНА БЕЗПЕКА І СОЦІАЛЬНІ МЕРЕЖІ

Васів Д., Навитка М.
Львівський державний університет безпеки життєдіяльності, м .Львів

В наслідок інтенсивного розвитку інформаційних технологій у світі та Україні соціальні мережі стали дієвим інструментом впливу на суспільні й політичні процеси у державі. Стало очевидним, що під впливом інформації зростає потенційна вразливість суспільних процесів від інформаційного впливу. Інформація стала чинником, здатним призвести до великомасштабних аварій, військових конфліктів, дезорганізації державного управління тощо.

В даній статті проведено аналіз інформаційної безпеки в соціальних мережах. Рекомендовано більше уваги приділяти проблемам захисту інформації та пошуків шляхів її вирішення.

Ключові слова: *інформаційна безпека, соціальні мережі, інформаційний простір, «фейкова» інформація, соціальний бот.*

As a result of the intensive development of information technologies in the world and in Ukraine, social networks have become an effective tool for influencing social and political processes in the country. It became obvious that under the influence of information the potential vulnerability of social processes to informational influence increases. Information has become a factor that can lead to large-scale accidents, military conflicts, disorganization of public administration and more.

This article analyzes the information security in social networks. It is recommended to pay more attention to the problems of information protection and finding ways to solve it.

Keywords: *information security, social networks, information space, "fake" information, social bot.*

Сучасні соціальні мережі стали ефективним інструментом суспільного розвитку і міждержавних відносин. В сучасному інформаційному суспільстві вони об’єднали всі сфери людської діяльності. Соціальні мережі неперервно взаємодіють з національним та глобальним інформаційними просторами. Будучи частиною національного інформаційного простору держави, забезпечують створення контенту у мережі Інтернет. Його зберігання, поширення та інформаційна взаємодія користувачів задовільняє їх інформаційні потреби та впливає на ефективність суспільної діяльності.

Соціальна мережа - це віртуальне об'єднання людей, де обмінюються певною інформацією. Причини її існування очевидні: сьогодні люди проводять величезну кількість часу за комп'ютером і звикли обмінюватися інформацією одне з одним насамперед в електронному вигляді.

Нас турбують соціальні мережі як інструмент маніпуляції та провокації задля впливу на масову свідомість. Їх зростаюча суспільна важливість зумовлює вразливість елементів інформаційної інфраструктури до негати-

вних впливів. Інформаційна інфраструктура стала об'єктом інформаційної агресії та інформаційних воєн. Інформаційну війну ведуть усі держави як суб'єкти світової політики.

Деякі соціальні мережі майже ідеально створені для прикриття розвідувально-пошукової діяльності спецслужб щодо збору різнопланової, придатної для наступного аналітичного дослідження інформації. У системі національної оборони дедалі більшого значення набуває інформація, яка заповнює вільний час і формує настрій громадян. Сучасні соціальні мережі вщент заповнені користувачами-професіоналами. Їхньою функцією є вкидання «фейкової» інформації в коло користувачів соціальних мереж. Формуються серед певної частини населення бачення громадської думки, настроїв і чуток. Дальше йде трансляція з їх допомогою максимально широкому загалу користувачів соцмереж.

Соціальні мережі перетворилися на джерело загроз інформаційній безпеці держави. Адже поширення недостовірного, неповного чи упередженого контенту у поєднанні з технологіями інформаційно-психологічного впливу на індивідуальну, колективну і масову свідомість може мати наслідком прояв у суспільстві соціальної напруженості, міжнаціональної ворожнечі, протестних настроїв, незадоволення існуючою системою управління в державі. Без забезпечення ефективного захисту інформаційної безпеки, виникають чи корегуються певні судження, вчинки чи організовуються соціальні протести, які використовуються внутрішніми і зовнішніми агресорами для вирішення різного роду цілей. Соціальні мережі можуть бути складовим елементом, як у локальних так і у військових конфліктах.

Одним з найпоширеніших явищ соцмережах є використання соціальних ботів для формування суспільної думки з актуальних питань, активного обговорення у віртуальних спільнотах другорядних подій, блокування акаунтів окремих користувачів. Загрози в мережах носять комплексний характер, а їх кількість постійно збільшується. Встановлено, що загрози інформаційній безпеці відрізняються за масштабністю, способом впливу на користувачів, частотою повторюваності тощо. Забезпечення інформаційної безпеки в соціальних мережах – це складний процес, який потребує постійного контролю і вдосконалення.

Отже, інформаційна безпека відіграє важливу роль у забезпеченні інтересів будь-якої держави. Діюча на сьогодні в Україні система захисту особи не спроможна забезпечити ефективний захист наших співгромадян від протиправних дій з використанням інформаційно-маніпулятивних технологій в соціальних мережах. Забезпечення інформаційної безпеки у соціальних мережах залишається однією із гострих проблем, які потребують свого вирішення. Більше уваги потрібно приділяти проблемам захисту інформації та пошуків шляхів її вирішення. Проблема виявлення ознак загроз інформаційної безпеки у соцмережах та змога оцінити їх рівень зво-

диться до розроблення нових методів і технологій, виявлення складових ознак загроз та оцінювання їх рівня.

Інформаційні джерела

1. Засоби і методи захисту інформації [Електронний ресурс]. – Режим доступу: http://kiev-security.org.ua/

2. http://www.binom.net.ua

3. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: Підручник. – К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.

УДК 004.7

ХАРАКТЕРИСТИКИ БАЗОВИХ АТРИБУТІВ ТЕХНІЧНОГО ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ

Франчук А., Навитка М.

Львівський державний університет безпеки життєдіяльності, м .Львів

В даній статті проведено аналіз характеристик базових атрибутів технічного захисту акустичної інформації. Доцільність модернізації комплексу технічного захисту для забезпечення захисту приміщень, які використовуються для проведення засідань, переговорів, нарад і конфіденційних бесід.

Ключові слова: *телефони, телефаксні лінії зв'язку, мобільні та радіотелефони, радіостанції.*

This article analyzes the characteristics of the basic attributes of technical protection of acoustic information. The expediency of modernizing the technical protection complex to ensure the protection of the premises used for meetings, negotiations, meetings and confidential conversations.

Keywords: *telephones, fax lines, mobile and radio telephones, radio stations.*

На сьогодні одним з основних джерел загроз інформаційної безпеки будь-якого підприємства є діяльність розвідувальних і спеціальних служб, злочинних співтовариств, організацій і груп, протизаконна діяльність окремих осіб. Їх діяльність спрямована на збір і розкрадання цінної інформації – службової, комерційної і особистої, що закрита для доступу сторонніх осіб. Для збору інформації вони активно в даний час використовуються наступні можливості:

– прослуховування розмов в приміщенні або автомобілі за допомогою попередньо встановлених радіозакладок або диктофонів;

– зняття акустичної (мовної) інформації за допомогою контактних мікрофонів з елементів конструкцій приміщення, а також з використанням спеціальних лазерних стетоскопів, що дозволяють знімати інформацію з скла;

– контроль телефонів, телефаксних ліній зв'язку, мобільних та радіотелефонів, радіостанцій;

– дистанційне зняття інформації з різних технічних засобів.

Технічний захист інформації представляється як комплекс організаційно-технічних заходів. Його кінцевою метою є виключення витоку конфіденційної інформації. Тому роботи по виявленню каналів витоку мовної та видової інформації через закладні пристрої необхідно розглядати як один з етапів виконання робіт з технічного захисту інформації.

Суттєвою перепоною на шляху від витоку акустичної інформації є створення на об'єктах особливих, захищених приміщень для проведення засідань, переговорів, нарад і конфіденційних бесід.

У захищених приміщеннях створюється комплекс технічного захисту інформації. Він включає в себе ряд організаційно-технічних заходів. Це дозволить виключити витік акустичної інформації технічними каналами.

Інформація, що становить комерційну таємницю, може бути присутня в розмовах, що проходять в кабінетах або в документах, які обробляються засобами оргтехніки та комп'ютерами. Важливим елементом діяльності будь-якого виду комерційних об'єктів є телефонний зв'язок.

Захист каналів зв'язку, що виходять з об'єкту включає в себе:

– використання апаратури електронного шифрування для телефонного зв'язку при обміні конфіденційною інформацією з партнерами;

– скорочення або виключення обговорень за телефонами важливих комерційних питань, особливо при використанні бездротових телефонних апаратів.

Захист внутрішніх комунікацій включає в себе:

– екранування комунікацій;

– використання електронного зашумлення комунікацій та мереж електроживлення, що забезпечують роботу технічних засобів обробки важливої інформації;

– установка датчиків сигналізації в місцях можливих сторонніх підключень до комунікацій;

– періодичний контроль внутрішніх комунікацій фахівцем служби технічного захисту інформації.

З метою захисту інформації, переданої по каналах зв'язку всередині об'єкта, не рекомендується використовувати радіотелефонні апарати, незважаючи на їх видимі зручності. Це особливо важливо для співробітників служби охорони, які використовують радіостанції при несенні служби всередині об'єкта і при супроводі людей і цінних вантажів. Переговори по «відкритому» радіоканалу можуть стати надбанням сторонніх осіб, які мають відповідну радіоприймальну апаратуру.

Необхідно відзначити, що використання всіх перерахованих вище засобів і методів захисту вимагає певних матеріальних витрат, відповідної професійної підготовки та досвіду роботи персоналу служби безпеки в цій галузі.

Інформаційні джерела

1. Засоби і методи захисту інформації [Електронний ресурс]. – Режим доступу: http://kiev-security.org.ua/

2. http://www.binom.net.ua

3. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: Підручник. – К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.

4. Um.co.ua [Електронний ресурс] : [Веб-сайт]. – Способи та засоби енергетичного приховування акустичного сигналу. – режим доступа : http://um.co.ua/6/6-6/6-65546.html

УДК 004.056.53

ПРОЕКТ OWASP, ЯК ФРЕЙМВОРК ПРОВЕДЕННЯ ТЕСТУВАННЯ НА ВРАЗЛИВОСТІ

Странатко М., Косиєв О.

Львівський державний університет безпеки життєдіяльності, м. Львів

OWASP - це структура, яка включає документацію, інструкції, найкращі практики та інструменти для тестування та підвищення безпеки додатків.

Ключові слова: *етичний хакінг, owasp, тестування на вразливості.*

OWASP is a framework that includes documentation, instructions, best practices, and tools for testing and improving application security.

Keywords: *ethical hacking, owasp, vulnerability testing.*

Open Web Application Security Project (OWASP) - це всесвітня благодійна організація 501c3 not-for-profit [1], що займається підвищенням безпеки прикладного програмного забезпечення. Їхнє програмування включає:

– проекти програмного забезпечення з відкритим кодом під керівництвом громади;

– понад 275 місцевих глав у всьому світі;

– десятки тисяч членів;

– провідні освітні та навчальні конференції в галузі.

Позначенням "501c3" - це US юридичний термін, який означає, що пожертвування в організацію підлягають оподаткуванню.

Проект Open Web Application Security Project (OWASP) - це відкрите співтовариство, призначене для надання організаціям можливості ство-

рювати, розробляти, здобувати, експлуатувати і підтримувати додатки, яким можна довіряти. Всі інструменти OWASP, документи, форуми, статті безкоштовні і відкриті для всіх, хто зацікавлений в підвищенні безпеки додатків. Вони виступають за те, щоб розглядати безпеку додатків як проблему людей, процесів і технологій, оскільки найбільш ефективні підходи до безпеки додатків включають поліпшення у всіх цих областях.

OWASP - це новий вид організації. Їхня свобода від комерційного тиску дозволяє їм надавати об'єктивну, практичну і економічно ефективну інформацію про безпеку додатків. OWASP не є афілійованою особою жодної технологічної компанії. Подібно до багатьох проектів з відкритим вихідним кодом, OWASP виробляє багато типів матеріалів в спільній, відкритій формі.

Деякі види діяльності фонду включають в себе [2]:

1. Громадські тренінги, пов'язані з безпекою.

2. Періодична публікація рейтингів вразливостей, щоб команда розробників додатків могла враховувати ці фактори при створенні безпечних додатків - OWASP Top 10.

3. Створення інструментів з відкритим вихідним кодом, які можна було б використовувати для поліпшення безпеки програми. Наприклад, OWASP Dependency Check-це інструмент аналізу складу програмного забезпечення, який може бути включений в ваш проект.

4. Розроблення і надання документацію, зокрема перевіряльні листи, контрольні списки, інструкції пов'язані з безпекою.

Крім цього це організація, яка займається розробкою безпечного програмного забезпечення.

В рамках цього вони розробляють керівні принципи і програмне забезпечення тестування і забезпечення безпеки програмного забезпечення. Одна частина програмного забезпечення є Live CD - мета цієї частини проекту "to make application security tools and documentation easily available".

Вони в першу чергу пов'язані з безпечною веб-розробкою.

Сукупність практик і методологій OWASP, а також програмне забезпечення, покрокові інструкції з виявлення та експлуатації вразливостей у додатках – один з кращих і абсолютно безкоштовних методів для якісного і ефективного підвищення рівня додатків та всієї інфраструктури організації загалом.

Інформаційні джерела

1. OWASP testing guide. Посібник для тестування на вразливості. Режим доступу: https://owasp.org/www-pdf-archive/OWASP_Top_10-2017-ru.pdf

2. Вимоги до захисту інформації веб-додатків OWASP. Режим доступу: https://owasp.org/index.php/SAMM_-_Security_Requirements_-_1

УДК 004.056

МОДЕЛЬ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Глянцева С., Максимів О.
Львівський державний університет безпеки життєдіяльності, м .Львів

В даній роботі розглянуто проблему побудови системи захисту інформаці з оптимальним рівнем ризику для об'єкта. Наведено модель системи інформаційної безпеки яка дозволяє оцінити або переоцінити сучасний стан інформаційної безпеки об'єкта та розробити рекомендації щодо зменшення потенційних втрат.
Ключові слова: *система, захист, інформація, модель, ризик.*

This paper considers the problem of building an information security system with the optimal level of risk for the object. A model of the information security system is presented, which allows to assess or re-evaluate the current state of information security of the object and to develop recommendations for reducing potential losses.
Keywords: *system, protection, information, model, risk.*

Щоб побудувати збалансовану систему захисту інформації, спочатку потрібно провести аналіз ризиків інформаційної безпеки. Потім визначають оптимальний рівень ризику для об'єкта на основі заданого критерію. Система захисту інформації повинна бути побудована таким чином, щоб досягти заданого рівня ризику [1].

При побудові такої системи слід враховувати взаємозв'язок між ресурсами. Такі відносини визначають основу побудови моделі організації з точки зору інформаційної безпеки.

Загалом, система захисту інформації має забезпечувати:

– уточнення захисних функцій;

– вибір архітектурних принципів побудови системи захисту інформації;

– розробка логічної структури системи захисту інформації (чіткий опис інтерфейсів);

– роз'яснення вимог функцій забезпечення безпеки системи захисту інформації;

– розробка алгоритму випробувань на відповідність сформульованим вимогам.

При реалізації даної задачі можна використовувати модель системи захисту інформації представлену на рисунку 1, яка побудована, відповідно, до стандарту (ISO 15408) та даних аналізу ризиків (ISO 17799). Ця модель відповідає спеціальним положенням про інформаційну безпеку, прийнятим в Україні, міжнародному стандарту ISO / IEC 15408 "Інформаційні технології - методи захисту, критерії оцінки інформаційної безпеки", ISO / IEC

17799 "Управління інформаційною безпекою" та враховує тенденції у вітчизняних нормативних актах баз даних про інформаційну безпеку [2].

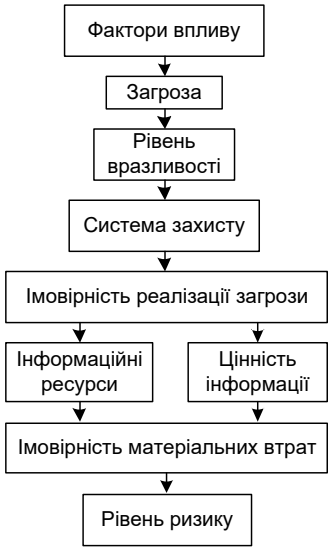


Рис. 1. Блок схема моделі системи інформаційної безпеки

Ця модель, будується наступним чином: для виділених ресурсів визначають їх вартість з огляду на пов'язані з цим можливі фінансові втрати та зниження репутації організації, дезорганізацію її діяльності, моральні втрати від розголошення конфіденційних даних інформація тощо. Описують взаємозв'язок ресурсів, виявляють загрози безпеці та оцінюють ймовірність їх реалізації.

Об'єктивні фактори моделі:

– загрози інформаційній безпеці, що характеризуються ймовірністю реалізації;

– вразливості інформаційної системи або системи контрзаходів (системи захисту інформації);

– ризик – фактор, який відображає можливу шкоду організації в результаті загрози інформаційної безпеки: витік інформації та її неправильне використання (ризик відображає ймовірні фінансові втрати - прямі чи непрямі).

На основі наведеної моделі можна обґрунтовано вибрати систему контрзаходів, що знижує ризики до прийнятних рівнів та є ефективною. Частиною системи контрзаходів є рекомендації щодо регулярних перевірок ефективності системи захисту.

Підвищені вимоги до інформаційної безпеки передбачають відповідні заходи. Ці заходи плануються після закінчення фази аналізу ризику та вибору контрзаходів. Обов'язковою частиною цих планів є періодична перевірка відповідності існуючого режиму інформаційної безпеки політиці безпеки, сертифікація інформаційної системи на відповідність вимогам певного стандарту безпеки [1].

На етапі оцінки досягнутого рівня гарантування безпеки інформаційного середовища об’єкта автоматизації, після реалізації рекомендованих заходів, робиться висновок чи можна довіряти інформаційному середовищу об’єкта чи потрібно вводити додаткові заходи безпеки.

Загалом, вищезазначена модель дозволяє оцінити або переоцінити сучасний стан інформаційної безпеки об’єкта, розробити рекомендації щодо

зменшення потенційних втрат за рахунок підвищення стабільності корпоративної мережі, розробити концепцію та політику конфіденційної інформації, що передається через відкриті канали зв'язку, захисту корпоративної інформації від навмисного спотворення знищення чи несанкціонованого доступу до неї, її копіювання або використання не за первинним призначенням.

Інформаційні джерела

1. Засоби і методи захисту інформації [Електронний ресурс]. – Режим доступу: http://kiev-security.org.ua/

2. Захист критичної інфраструктури. Проблеми та перспективи впровадження. Режим доступу: https://niss.gov.ua/sites/default/files/2012-09/zah_ynfrastr-b98c0.pdf

УДК 004.056.53

ПОШИРЕНІСТЬ DOS-АТАК ТА ЗАХИСТ ВІД НИХ

Стефанів Т., Косиєв О.
Львівський державний університет безпеки життєдіяльності, м .Львів

Атаки DOS і DDOS - один з найпростіших, але найпоширеніших типів атак, який може завдати значної шкоди організації, порушуючи доступність даних, спричиняючи зупинку безпеки і, таким чином, завдаючи організації ще більших втрат.

Ключові слова: *доступність, кібератаки, DOS, DDOS.*

DOS and DDOS attacks are one of the simplest but most common types of attacks, which can cause significant damage to the organization, disrupting the availability of data, causing security to stop, and thus causing even greater losses to the organization.

Keywords: *availability, cyberattacks, DOS, DDOS.*

DoS-атака - атака на сервер з метою вивести його з ладу, тобто створення таких умов, при яких легітимні (правомірні) користувачі системи не можуть отримати доступ до наданих системою ресурсам, або цей доступ ускладнений. Відмова системи може бути як самоціллю (наприклад, зробити недоступним популярний сайт), так і одним із кроків контролю над системою.

Якщо атака виконується одночасно великої кількості комп’ютерів, говорять DDoS-атака [1] (від англ. Distributed Denial of Service, розподілена атака типу «відмова в обслуговуванні»).

DoS-атаки поділяються на локальні та віддалені. До локальних відносяться різні експлойти: форк-бомби і програми, що відкривають по мільйону файлів або запускають якийсь циклічний алгоритм, який «з'їдає» пам'ять та процесорні ресурси. Для локальної DoS атаки необхідно мати, або якимось чином отримати доступ до атакованої машини на рівні, що буде достатнім для захоплення ресурсів.

Далі розглянемо найпоширеніші способи атаки [2].

HTTP flood – відправка на вебсайт кілька десятків тисяч запитів GET, POST, HTTP 1.1 по 80 порту веб-сервера.

UDP flood – відправка на адресу системи безлічі пакетів UDP. Цей метод використовувався в ранніх атаках і в даний час вважається найменш небезпечним.

TCP flood – відправка на адресу сервера безлічі TCP-пакетів, що також призводить до перевантаження мережевих ресурсів.

Небезпека більшості DDoS-атак — в їх абсолютній прозорості і «нормальності». Адже якщо помилка в ПЗ завжди може бути виправлена, то повна витрата ресурсів — явище майже буденне. З ними стикаються багато адміністраторів, коли ресурсів машини (ширини каналу) стає недостатньо, або web-сайт піддається слешдот-ефекту. І, якщо різати трафік і ресурси для всіх підряд, то можна врятуватися від DDoS, у той же час, втративши велику частину клієнтів.

У 2019 році одна з німецьких компаній провела аналітичне дослідження на предмет схильності DDoS-атакам. Виявилося, більше половини з 250 осіб, що приймають рішення в області IT, і консультантів, опитаних для дослідження, вже стали жертвами DDoS-атаки.

Але що вони могли зробити, щоб захистити системи? Багато IT-відділів безпорадні проти такої атаки, оскільки навіть спеціальні брандмауери перевантажуються і падають. Природно, найпростіший спосіб запобігти атаку на сервери - закрити порти і відрізати будь-який зовнішній веб-трафік, але це також призведе і вашої власної ізоляції.

Якщо компанія зауважує DDoS-атаку, їй слід якомога швидше зв'язатися з провайдером, щоб можна було негайно вжити контрзаходів, і щоб негативний ефект виявився мінімальним. Експерти з кібербезпеки стежать за з'єднанням на час атаки, яка може тривати кілька тижнів.

Інформаційні джерела

1. Інструменти та методи атак, захист від них. Режим доступу: https://cryptoworld.su/ddos-ataka-na-sajt-instrumenty-i-texnolog/

2. Захист критичної інфраструктури. Проблеми та перспективи впровадження. Режим доступу: https://niss.gov.ua/sites/default/files/2012-09/zah_ynfrastr-b98c0.pdf

Напрям 6

ІНФОРМАЦІЙНІ ВІЙНИ

УДК: 004.6

ДЕЗІНФОРМАЦІЯ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ ДЕРЖАВИ ЯК ОСНОВНИЙ ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ ВІЙНИ

Довганич М., Ящук В.
Львівський державний університет безпеки життєдіяльності, м .Львів

Розкриваються питання ведення інформаційної війни в інформаційному просторі країни. Піднімається питання пріоритетності вирішення проблеми пропаганди в новинних каналах та соціальних мережах. Описано проект "Fnews", який частково вирішуватиме проблему розповсюдження фейкових новин для припинення маніпуляцій настроями суспільства.
Ключові слова: *Fake News, Fnews, дезінформація, інформаційна війна.*

The issues of information warfare in the information space of the country are revealed. The question of the priority of solving the problem of propaganda in news channels and social networks is raised. Describes the Fnews project, which will partially solve the problem of spreading fake news to stop manipulating public sentiment.
Keywords*: Fake News, Fnews, misinformation, infowar.*

Інформаційні війни сьогодні є одним з найбільш недооцінених напрямів ведення військових дій. В цьому векторі мішенню стають не тільки військовослужбовці, а й цивільні громадяни, адже основною ціллю є вплив на свідомість та ідеологію населення країни - суперника. Наслідки ведення інформаційних війн у суспільній психології за масштабами і значенням цілком співмірні, а часом і перевищують наслідки збройних війн.

Інформаційна війна [information warfare] розглядається як комплекс підходів і операцій, спрямованих на забезпечення інформаційної переваги по підношенню до потенційного або реального противника [1]. Також поняття "Інформаційна війна" визначається як "дії, початі для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що базуються на інформації і інформаційних системах супротивника при одночасному захисті власної інформації. "А основним методом є блокування та спотворення інформаційних потоків та процесів прийняття рішень суперника.

Інформаційна війна ведеться не тільки у фізичному просторі, де знаходяться фізичні інформаційні системи і засоби, але і у деякій віртуальній зоні (віртуальному або кібернетичному просторі). Інформаційна війна розширює простір ведення війн, який раніше обмежувався великими висотами в атмосфері (стратосфері) і великими глибинами у Світовому океані. До особливостей

інформаційної війни відноситься те, що вона ведеться як під час фактичних бойових дій, так і у мирний час і у кризових ситуаціях. Початок війни інформаційної неможливо визначити однозначно. Будь-які міжнародні юридичні і моральні норми ведення інформаційної війни відсутні [1].

Враховуючи, що в основі ідеології інформаційної війни лежить макіавеллізм, часто інформаційна війна ведеться в обидві сторони, тобто і на населення держави-мішені, і на населення атакуючої держави. Наслідком ведення таких інформаційних атак часто є збройні конфлікти. Наприклад приводом для бомбардування Багдаду США стала поширена через світові ЗМІ інформація, що режим Хусейна нібито має зброю масового знищення. Війна в Іраку триває й досі, але такої зброї так і не знайшли. Насправді ж, головною метою збройної атаки на Ірак була не ЗМЗ, а велика кількість нафти, яку прагнув взяти під контроль американський уряд, але це не могло стати причиною нападу, тому довелося створити фіктивний привід для нападу на цю державу, який б не підірвав легітимність американського держапарату.

Дослідження Центру з досліджень безпеки при Федеральній вищій технічній школі Цюриха випустили “Кібернетична та інформаційна війна в українському конфлікті”, в якому автори Марі Безнер та Патріс Робін вивчають природу інформаційної війни, яку Росія веде проти України та описують наслідки цієї війни для України, та описують рекомендації щодо обмеження впливу російської агресії:

– широка обізнаність проблеми пропаганди. Суспільство повинне бути проінформоване про такі види атак і приймати інформацію критично.

– заборона використання російських платформ та соціальних мереж - адже більшість з них передає інформацію про користувачів третім особам, які й займаються аналізом інформації і готують наступні атаки на основі попереднього аналізу.

– міжнародне відстеження кіберактивності Росії в Україні, щоб оцінити пов'язані ризики та розробити план протидії інформаційній агресії Кремля.

В свою чергу проект “FNews” є спробою відповіді на вищеописану загрозу національній безпеці. Метою проекту є розроблення інформаційного порталу, який перевіряє найпопулярніші джерела інформації на предмет «фейковості». З цією метою моделюєтьсямо нейронна мережа, яка, отримуючи інформацію, спершу перевіряє заголовки новин на предмет “сенсаційності”, текст новини на слова - маніпулятори, після чого досліджує прикріплені посилання до новини та виводить співвідношення однакових слів, таким чином перевіряючи маніпуляцію контекстом джерела. На основі цих показників виводиться оцінка новини, після чого вона перевіряється людиною. Таким чином нейронна мережа й навчається. Сьогодні проект “FNews” знаходиться на етапі формування логіки нейронної мережі, але щойно я описав ключові аспекти.

Отже, результатом реалізації проекту буде підвищення рівня інформаційної безпеки держави та демонстрація суспільству кількість та масштабність інформаційних атак з боку Росії.

Інформаційні джерела

1. Богуш В. М.Інформаційна безпека держави. / В. М. Богуш, О. К. Юдін — К. : "МК-Прес", 2005. — 432с.

2. Cyber and Information warfare in the Ukrainian conflict - [Електронний ресурс] - https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-01.pdf

3. imi - [Електронний ресурс] https://imi.org.ua/monitorings/krymchany-vtratyly-ostannij-zv-yazok-z-ukrayinoyu-informatsijnyj-i36113

Informnapalm - [Електронний ресурс] - http://informnapalm.rocks

УДК: 004.6

ІНФОРМАЦІЙНІ ВІЙНИ НОВОГО ПОКОЛІННЯ

[1]Антіпенко А., [2]Бабаджанова О.

[1]Національний університет "Львівська політехніка", м. Львів

[2]Львівський державний університет безпеки життєдіяльності, м. Львів

Розглядається інформаційна війна не як допоміжний механізм реальної війни, а як механізм впливу на громадську думку. Наведено чотири основні чинники, які визначають ефективність інформаційного впливу. Розглянуто методи та цілі кібервійни та інформаційно-мережевої війни, як інформаційних війн нового покоління.

Ключові слова: *інформаційна війна, кібервійна, інформаційний вплив.*

We review the information war not as an auxiliary mechanism for real war, but as a mechanism of affecting the public opinion. There are the four main factors that determine the effectiveness of the impact of information. Methods and aims of cyberwar and informational network war also considered, as the information wars of new generation.

Keywords: *information war, cyberwar, information impact.*

Інформаційна війна – це якісно новий рівень міждержавного протиборства. Активне та агресивне нав'язування чужих цілей – це те, що робить інформаційну війну війною і відрізняє її від звичайної реклами. Інформаційні війни розглядаються як важливий засіб досягнення національних цілей тієї чи іншої держави за допомогою інформації, причому складовими інформаційних війн виступають війни психологічні, кібервійни, мережеві тощо.

Кібервійни спрямовані передусім на дестабілізацію комп'ютерних систем і доступу до інтернету державних установ, фінансових та ділових центрів і створення безладу та хаосу в житті країн, які покладаються на інтернет у повсякденному житті. Інше визначення кібервійни – це чітко скоординована цифрова атака однієї держави, спрямована на проникнення у комп'ютери та мережі іншої держави, з метою завдання шкоди або руй-

нування. За визнанням спеціалістів, лідерами у веденні кібервійни зараз є Китай та Росія.

В кібервійні неможливо ідентифікувати «агресора», навіть коли причетність до кібератаки державних структур певних країн багатьом здається очевидною. Крім того, географічним джерелом кібератаки є, як правило, зовсім не та держава, якій така атака може бути об'єктивно вигідною.

На рубежі XX–XXI століть у західному суспільстві були розроблені численні технології прихованого руйнівного впливу, які з часом оформилися в новий тип воєн – інформаційно-мережевих, метою яких є міцне закріплення більшої частини стратегічно важливих ресурсів країни-жертви за агресором. Основним їх завданням є ускладнення доступу людей до об'єктивної і достовірної інформації.

Інформаційна війна може бути спрямована як на населення супротивника, так і на власне населення, або населення держав усього світу, що оточують держави-конкуренти, які пов'язані із протистоянням. Варто виділити чотири групи чинників, які визначають ефективність інформаційного впливу на населення:

– суб'єкти інформаційних війн, інформаційного протиборства (безпосередньо держави, міжнародні організації, медіа-корпорації тощо);

– використовувані канали впливу, так звана зброя інформаційної війни (Інтернет, засоби масової інформації, зокрема телебачення);

– сам контент, зміст інформації, що транслюється у ході інформаційної війни;

– специфіка масової свідомості населення у тих чи інших країнах, формування та функціонування у них громадської думки.

В інформаційній війні, війні нового типу, використовуються канали безпосереднього впливу на суспільну свідомість, на душі людей. Завдання полягає в тому, щоб змусити маси діяти в потрібному напрямку, навіть проти своїх інтересів.

Інформаційні джерела

1. Інформаційні війни: тенденції та шляхи розвитку. https://ms.detector.media/manipulyatsii/post/6479/2012-08-12-informatsiini-viini-tendentsii-ta-shlyakhi-rozvitku/

2. Богуш В. М.Інформаційна безпека держави. / В. М. Богуш, О. К. Юдін – К. : "МК-Прес", 2005. – 432с.

3. Російсько-українська інформаційна війна. https://uk.wikipedia.org/wiki

УДК: 004.6

ДІПФЕЙКИ. ПРИЧИНИ, ПРОБЛЕМИ ТА ВИРІШЕННЯ

Малець О.-С. І.
Львівський національний університет ім. Івана Франка, м. Львів

Цей допис описує основну ідею діп фейків. Причини для їхнього створення, проблеми які вони завдають, можливі вирішення цієї проблеми на сьогодні та майбутнє яке нас очікує.

Ключові слова: *Захист інформації, діпфейк, діпфейк розробки, інформаційні війни.*

The article outlines main ideas about deep fakes. The reason they are made, problems they are creating, possible handling of the deep fakes for today and the future that waits for us.

Keywords: *information security, deep fake, deep fake software, information wars.*

Інформація завжди була “на вагу золота”. Та чи інша новина може врятувати, або ж погубити тисячі життів за лічені секунди, принести мільйони, або ж загубити все ваше майно. Ні для кого не секрет, що світ давно перебуває в величезному інформаційному потоці. Важко залишитися в стороні від гучних подій, коли смартфон зранку присилає про неї сповіщення, всі радіохвилі обговорюють її, а по телеканалах транслюють обговорення та репортажі. І ковтаючи ці галони інформацію, було б непогано мати можливість “відфільтрувати” її, тим більше якщо фільтр не пропускатиме брехню.

Почнемо з декількох визначень для чіткості. Фейк - неправдива інформація сфабрикована з тої чи іншої причини, зазвичай для великої аудиторії. Діп фейк - зазвичай аудіо або відео матеріал, який дуже вміло сфабриковує, змінює ті чи інші події, знову ж таки, зазвичай зв’язані з відомими, популярними або впливовими людьми.

Тепер можемо розібратися з причинами для створення подібного роду матеріалу. Спочатку діпфейки використовувалися як свого роду хобі, спосіб розважити себе та своїх друзів. З тодішнім програмним забезпеченням, діпфейки можна було розпізнати неозброєним оком. Так як в основному діпфейки продукують над відеозаписами з людським обличчям, то зауважити “підробку” не потребувало багато зусиль: можливо жестикуляція не відповідала виразу обличчя, можливо нове обличчя було накладено не ідеально, погано підібраний тон шкіри. Зважаючи на аматорський підхід, можна було спокійно знайти неправдивий матеріал.

Проте діпфейки почали використовувати не лише для розваги. Для порушення роботи тої чи іншої компанії, можна було записати аудіозапис ніколи не сказаних слів верхівок, або ж зруйнувати чийсь шлюб за допомогою підставленого обличчя в відеоматеріал порнографічного характеру, підставити кандидата на виборах поширивши аудіо/відео матеріал з неіснуючими репліками та діями. Тобто принести реальну шкоду, нереальною інформацією.

Беручи до уваги швидкість, з якою розвивається ця галузь, стає все страшніше уявляти наслідки та майбутні проблеми спричинені діпфейками. Марко Рубіо, один з кандидатів в президенти США від республіканців у 2016 році, назвав діпфейки еквівалентом ядерної зброї сучасності. "Раніше, якщо хтось хотів завдати шкоди США, їм було потрібно 10 авіаносців, ядерну зброю та міжконтинентальні ракети. Сьогодні, можна мати доступ до інтернету, зробити дуже реалістичний діпфейк та послабити країну зсередини зірвавши вибори або розпаливши внутрішні конфлікти". Крім того, так як програми з заміною лиця зараз стали дуже популярними у молоді, для розваги, індустрія на місці не стоїть. Поки звичайні користувачі розважаються та дають оцінку програмам, розробники коригують алгоритм заміни обличчя, підтягують ваги в нейронних мережах та постійно показують все кращі та й кращі результати.

Одні з представників діпфекових продуктів:

– https://thispersondoesnotexist.com/

– https://reflect.tech/

– https://faceswap.dev/

Як з цим боротися. Ну тут насправді все досить просто. Поки існують розробники що пишуть діпфейк алгоритми, існують і ті розробники, які пишуть алгоритми для розпізнавання діпфейків. Так як зацікавлених в обох видав матеріалу є достатньо, то і фінансування буде в обох сторін. Та поки на діпфейки не будуть врегульовані на законодавчому рівні, боротьба буде беззмістовною. Люди вірять у те що хочуть. Без базових знань про діпфейки, суспільство з часом перетвориться на дитсадок, у якому ніхто нічого не розуміє, а лише кричить що знає.

Інформаційні джерела

1. How and why deepfake videos work — and what is at risk By J.M. Porup, CSO USA, 2019

2. Deepfakes: What are they and why would I make one? - BBC UK, 2020

3. What are deepfakes – and how can you spot them? - The Guardian, 2020

4. Deepfake technologies: What they are, what they do, and how they're made by Sally Adee, Spectrum IEEE, April 2020.

УДК 004.738.5

ОГЛЯД АКТУАЛЬНИХ АЛГОРИТМІВ РОЗПІЗНАВАННЯ ФЕЙКОВИХ НОВИН У СОЦІАЛЬНИХ МЕРЕЖАХ

Штефанюк Є., Опірський І., Колбасинський І.
Національний університет "Львівська політехніка", м. Львів

В даній статті розглянуто проблему виявлення неправдивих новин у засобах медіа; наведено класифікацію алгоритмів для розпізнавання фейкових новин у соціальних мережах; розглянуто деякі найпоширеніші алгоритми та проаналізовано їхні особливості.

Ключові слова: *фейкові новини, нейронні мережі, соціальні мережі, Fakedetector, UFD, HC-CB-3.*

This article examines the problem of detecting false news in the media; the classification of algorithms for recognizing fake news in social networks is given; some of the most common algorithms are considered and their features are analyzed.

Keywords: *fake news, neural networks, social networks, Fakedetector, UFD, HC-CB-3.*

Вступ

Останніми роками можна спостерігати збільшення ролі соціальних медіа у створенні та поширенні інформації між людьми. Вони використовуються як для обміну особистою інформацією, так і для поширення публічних думок відомих діячів політики та культури. Внаслідок цього, актуальним стає завдання визначення достовірності інформації, що поширюється соціальними мережами.

Все більшого поширення набувають фейкові новини –статті та дописи в соціальних мережах, що містять неправдиву інформацію і створені навмисно, щоб ввести користувачів в оману. Це стає потужним інструментом інформаційного впливу на соціум. Яскравим прикладом можуть слугувати дослідження, що виявили наявність впливу фейкових новин на вибори президента в США в 2016 році. [1]. Спеціально створені фейкові дописи, що поширюються в соцмережах, можуть стати підґрунтям до зміни соціальної думки щодо певних питань, зростання напруження в суспільстві чи дискредитації окремих людей через їхні погляди.

Таким чином, завдання розробки та застосування ефективних засобів виявлення таких фейкових новин є надзвичайно актуальним сьогодні.

Огляд актуальних алгоритмів

Згідно з [2], алгоритми для виявлення фейкових новин можна поділити на дві групи: з навчанням з учителем та з самонавчанням. На основі

особливостей даних, які враховуються алгоритмами, вони поділяються на наступні категорії:

– content-based: беруть до уваги зміст новини, опис профілю її автора;

– social-based: враховують реакції користувачів соцмережі на допис;

– combined: використовують обидва вищезазначені методи.

Прикладом алгоритму, що реалізує перший підхід є фреймворк Fakedetector [3]. Він використовує модуль HFLU (Hybrid feature learning unit) для виявлення так званих зовнішніх та внутрішніх маркерів (features) допису в соцмережі, аналізуючи його контент. Для цього він застосовує рекурентну нейронну мережу (Recurrent Neural Network, RNN). Далі фреймворк використовує глибинну нейронну мережу (Deep diffusive neural network), яка обробляє ці маркери, представлені у вигляді векторів. Для тренування нейронної мережі застосовують метод зворотного поширення помилки (backpropagation training). В результаті роботи фреймворку, автору допису, темі та його контенту допису присвоюється певний рейтинг правдивості.

Таким чином, Fakedetector являє собою фреймворк з навчанням з учителем, що здійснює визначення рівня довіри до самого інформаційного контенту, його автора та його теми.

Іншим підходом до розпізнавання фейкових дописів, який комбінує алгоритми для врахування як змісту допису так і реакцій користувачів на них, є метод описаний в [2]. Він аналізує специфіку поширення фейкових новин в соціальних мережах. Для досягнення кращих результатів застосовується комбінація з двох окремих алгоритмів. Перший алгоритм базується на гіпотезі, що фейкові новини відрізняються від справжніх кількістю та особливостями реакцій користувачів соцмережі. Для аналізу цієї інформації використовується підхід “Harmonic boolean label crowdsourcing on social signals” (HC-CB-3). Проте, він є ефективним лише при наявності достатньої кількості інформації про реакції користувачів на дописи. Щойно створений допис може не зібрати достатню кількість коментарів чи реакцій, що різко знижує ефективність застосування даного алгоритму. У такому випадку пропонується використовувати другий алгоритм - алгоритм аналізу контенту дописів для виявлення особливостей, які є характерними для фейків.

Варто підкреслити, що великий вплив на якість кінцевого результату має вибір порогового значення кількості реакцій користувачів на допис – якщо кількість реакцій менша за порогову – застосовується перший алгоритм, якщо більша – другий.

Третій актуальний зараз підхід, який об’єднує в собі аналіз як контенту так і соціальної складової в одному алгоритмі, описаний в [4] – Unsupervised framework, або UFD. Він базується на оцінці реакцій користувачів соцмережі на конкретний допис. В основі застосування UFD лежить гіпотеза, що користувач висловлює свою власну думку про допис через

коментар або відповідну реакцію, що може слугувати маркером правдивості інформації в дописі. Зібравши достатню кількість реакцій користувачів, можна з достатньою точністю виявити фейковий допис. Автори використовують метод Collapsed Gibbs Sampling, правило оновлення якого враховується на основі кількості реакцій користувачів з групи довірених та недовірених. Користувачі, реакції яких на допис в більшості збігаються з рішенням системи про його правдивість, заносяться до групи довірених; інші користувачі складають групу недовірених. Відповідно до групи, до якої належить користувач, його реакція враховується в алгоритмі з певним коефіцієнтом, допомагаючи, таким чином, зменшувати вплив заангажованих користувачів або акаунтів-ботів на кінцевий результат передбачення.

Висновки. На тлі поширення соціальних мереж як засобу отримання на поширення новин, на перший план виходить завдання визначення правдивості інформації, що поширюється у формі дописів в цих мережах.

Існує багато підходів та алгоритмів для розпізнавання фейкового контенту в соціальних мережах. Вони базуються як на конкретних математичних моделях, так і на алгоритмах машинного навчання та нейронних мережах.

На даний момент, методи для виявлення фейкового контенту в дописах можна поділити на три групи: content-based методи, social-based методи та combined методи. Прикладом content-based методу є фреймворк Fakedetector, що враховує контент допису та профіль його автора. Social-based підхід застосовує алгоритм UFD, що базується на аналізі оцінок допису користувачами в коментарях і реакціях. Алгоритм HC-CB-3 застосовує комбінований підхід, використовуючи два алгоритми, рішення про застосування конкретного з яких приймається відповідно до кількості реакцій користувачів на допис.

Інформаційні джерела

1. Allcott H. Gentzkow M. Social media and fake news in the 2016 election. Journal of Eco-nomic Perspectives, 2017.

2. Vedova M. L. Della, Tacchini E., Moret S., Ballarin G., DiPierro M., de Alfaro L. "Automatic Online Fake News Detection Combining Content and Social Signals," 2018 22nd Conference of Open Innovations Association (FRUCT), Jyvaskyla, 2018, pp. 272-279, doi: 10.23919/FRUCT.2018.8468301.

3. Zhang J., Dong B.,Yu P. S. , "Fakedetector: Effective Fake News Detection with Deep Diffusive Neural Network," 2020 IEEE 36th International Conference on Data Engineering (ICDE), Dallas, TX, USA, 2020, pp. 1826-1829, doi: 10.1109/ICDE48307.2020.00180.

4. Yang, Shuo & Shu, Kai & Wang, Suhang & Gu, Renjie & Wu, Fan & Liu, Huan. (2019). Unsupervised Fake News Detection on Social Media: A Generative Approach. Proceedings of the AAAI Conference on Artificial Intelligence. 33. 5644-5651. 10.1609/aaai.v33i01.33015644.

УДК: 316.101

ІНФОРМАЦІЙНІ ВІЙНИ В СУЧАСНОМУ СВІТІ

Яковчук В. С.[1], Малець Б. І.[2], Борзов Ю. О.[1]
[1] Львівський державний університет безпеки життєдіяльності, м. Львів
[2] Львівський національний університет ім. Івана Франка, м. Львів

Розглянуто поняття інформаційної війни та процеси інформаційного впливу на суспільство. Виділено особливості інформаційної війни між Україною та Російською федерацією.

Ключові слова: *інформаційна війна, інформація, технологія, пропаганда, інформаційний простір.*

Інформаційні війни супроводжують всю історію людства. Спочатку вони були релігійними та ідеологічними, причому для боротьби з носіями чужих поглядів застосовувалися всі види репресій. В далекому минулому інквізиція чи репресивні апарати тоталітарних держав двадцятого сторіччя вели активну боротьбу з носіями чужих ідей.

Кожен з нас пов'язаний з терміном «інформаційна війна», адже як ніколи на сьогоднішній день, ми надто тісно прив'язані до цього, світом керує інформація. Зважаючи на роль інформації у сучасному світі, американський дослідник Маклюен виводить цікаву тезу, яка звучить так: "Істинно тотальна війна - це війна за допомогою інформації". Війна інформації на сьогодні стала одним з найнебезпечніших видів зброї. Користуватися компроматами, виливанням бруду, підкиданням неправдивої інформації, намагання за допомогою інформації ввести в оману стало для багатьох тоталітарних систем основою існування.

Після розвитку новітніх технологій, вплив інформації на прогрес людства зріс в тисячі разів. Інформація має вплив на маси, тобто за умови вдалого маніпулювання свідомістю мас можна досягти практично будь-якої мети: знищити опонента, прибрати з дороги конкурентів чи розпалити війну.

Завдяки розсиланням маси інформації, влада чи керуюча процесом особа, формує у суспільстві чи групі людей потрібну точку зору, громадську думку, хід взаємодоповнюючих логічних думок, вичерпну систему поглядів щодо окремих питань на користь організатора інформаційної пропаганди. Як наслідок, відбувається усвідомлення окремих фактів чи подій у потрібному для маніпулятора світлі, формування потрібного світогляду чи життєвої позиції стосовно питань, у яких раніше були

протиріччя чи нерозуміння. У випадку відсутності протиріч і наявної сталої системи поглядів, завданням інформаційної війни є породження сумнівів, насівання протиріч та домислів в існуючі переконання. Розвиток людини влаштований так, що людина завжди шукає відповіді про турбуючі її питання, спірні питання, що є невід'ємною рисою безперервних процесів пізнання.

Очевидно, що інформаційна війна - складова частина ідеологічної боротьби. Такі війни не призводять безпосередньо до кровопролиття, руйнувань, при їх веденні немає жертв, ніхто не позбавляється їжі, даху над головою.

І це породжує небезпечну безпечність у ставленні до них. Тим часом, руйнування, яких завдають інформаційні війни у суспільній психології, психології особи, за масштабами і за значенням цілком співмірні, а часом і перевищують наслідки збройних війн.

Що ж таке інформаційна війна, як саме науковці пояснюють таке явище в сучасному світі [1].

У книзі Прокофьєва "Інформаційна війна і інформаційна злочинність" дано визначення: інформаційна війна – це дії, початі для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що базуються на інформації і інформаційних системах супротивника при одночасному захисті власної інформації, процесів, що базуються на інформації і інформаційних системах.

Найбільш вразливим місцем сучасних складних систем стають процеси прийняття рішень. Саме тому інформація як така поступово почала змінювати свій статус. Вона стала переходити від сили, що допомагала в бою, до сили основної, яка й вирішує результат війни.

Першим варіантом інформаційної війни можна визнати пропаганду. Вся холодна війна базувалася на механізмах пропаганди, бо механізми гарячої війни не застосовувалися. До речі, потреба пропаганди в холодній війні надала суттєвий поштовх розробці теорії комунікації, бо виникла велика кількість суто прикладних завдань у галузі комунікації.

Французький соціолог ***Жак Еллюль*** запропонував розрізняти вертикальну та горизонтальну пропаганди (***Ellul J. Propaganda. The formation of men's attitudes. – New York, 1965***). Вертикальна – це класичний варіант пропаганди, як ми всі собі її уявляємо, інформаційний потік згори до низу з пасивним реагуванням аудиторії.

Горизонтальну пропаганду Еллюль називає новим винаходом. Вона зветься горизонтальною, бо реалізується в групі, а не йде згори. У цій ситуації всі учасники є рівними, серед них немає лідера.

Ж. Еллюль уводить також поняття політичної та соціологічної пропаганди. Знову ж таки політична – те, що ми звикли звати пропагандою. Це техніки впливу держави, партії, адміністрації. Соціологічна ж працює на об'єднання групи. Це стиль життя й типи поведінки, які є нормою в цьому суспільстві. Соціологічну пропаганду він вважає важчою для розуміння, бо вона є більш непомітною. Якщо політична пропаганда є розповсюдженням ідеології, то соціологічна – її проникненням завдяки існуючим економічним, політичним і соціологічним факторам. В першому випадку мас-медіа є провідником, у другому – економічні та політичні структури.

Розрізнення вертикальної/горизонтальної пропаганди та політичної/соціологічної на перший погляд можуть здаватися тотожними. Але в них акцентуються різні базові параметри. Вертикальна/горизонтальна стосуються напряму комунікації, що породжує ієрархічність. Саме тому йдеться й про лідера. У випадку розрізнення політичної/соціологічної пропаганди акцентується тип медіа, коли за нього беруться й інститути суспільства [2].

Яскравим прикладом інформаційної війни може стати міждержавний конфлікт між Україною та Росією, в якому використовується політична та соціологічна пропаганда, комплекс заходів, постійно здійснюваних урядовими та неурядовими організаціями Росії та України в інформаційному просторі України, Росії, інших країн та міжнародних організацій, спрямованих на отримання стратегічно-політичних переваг шляхом деморалізації або введення в оману противника та протидії заходам іншої сторони у глобальному протистоянні Росії і України, а також протистоянні Росії та «Західного світу» [3].

Інформаційні джерела

1. Інформаційна війна – зброя масового знищення. https://www.pravda.com.ua/rus/articles/2006/04/20/4399050/

2. Інформаційні війни: тенденції та шляхи розвитку. https://ms.detector.media/manipulyatsii/post/6479/2012-08-12-informatsiini-viini-tendentsii-ta-shlyakhi-rozvitku/

3. Російсько-українська інформаційна війна. https://uk.wikipedia.org/wiki

Секція 2
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Напрям 7

ПРИКЛАДНЕ ТА СИСТЕМНЕ ПРОГРАМУВАННЯ

УДК 004.652.3

ОСНОВНІ ЗАДАЧІ МЕТОДОЛОГІЇ ПРОГРАМУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

Гоєнко Д.С., Дмитрієв Ю.О.
Таврійський державний агротехнологічний університет ім. Дмитра Моторного, м. Мелітополь

Розглянуті основні задачі методології програмування інформаційних систем, подана класифікація методологій та виділено головні вимоги до технології створення програмного продукту.

Ключові слова: *інформаційна система, технологія программування, проектування, методологія.*

The primary goals of methodology of programming of information systems are considered, classification методологий is given and the main requirements to technology of creation of software product are allocated.

Key words: *information system, programming technology, design, methodology.*

Метою даної роботи є аналіз існуючих методологій програмування інформаційних систем, їх класифікація та виділення головних вимог до технології створення програмного продукту.

Слід зазначити, що інформаційна система – це організаційно впорядкована сукупність документів (масивів документів) і інформаційних технологій, у тому числі і з використанням засобів обчислювальної техніки й зв'язку, що реалізують інформаційні процеси.

Інформаційна система в програмуванні - це прикладна програмна підсистема, яка орієнтована на збір, зберігання, пошук і обробку інформації та працює в режимі діалогу з користувачем [1].

Залежно від предметної області інформаційні системи можуть дуже сильно різнитися за своїми функціями, архітектурою та реалізацією. Однак, можна виділити ряд властивостей, які є загальними:

1. Інформаційні системи, що призначені для збору, зберігання й обробки інформації. В основі кожної з них лежить середовище зберігання й доступу до даних.

2. нформаційні системи, що орієнтовані на кінцевого користувача, який не володіє високою кваліфікацією в області застосування обчислювальної техніки. Клієнтські додатки таких інформаційних систем повинні

мати простий, зручний, легко освоюваний інтерфейс, який надає кінцевому користувачеві всі необхідні для роботи функції, але в той же час не дає йому можливості виконувати будь-які зайві дії.

Будь-яка теоретична або практична сфера діяльності використовує властиві тільки їй методи рішення поставлених задач. Метод - це спосіб досягнення якої-небудь мети, вирішення конкретної задачі, сукупність прийомів або операцій практичного або теоретичного освоєння дійсності. Методологія - сукупність методів, які застосовуються у будь-якій області людської діяльності [2].

Методологія науки дає характеристику компонентів наукового дослідження - його об'єкта, предмета аналізу, завдання дослідження, сукупності дослідницьких засобів, необхідних для вирішення завдання даного типу, а також формує представлення про послідовність руху дослідника в процесі вирішення завдання [3].

Методологія створення інформаційних систем полягає в організації процесу побудови інформаційної системи й забезпеченні керування цим процесом для того, щоб гарантувати виконання вимог як до самої системи, так і до характеристик процесу розробки.

На сьогоднішній день існує не так багато методологій, особливо повних, тобто враховуючих усі стадії життєвого циклу програмного забезпечення. Методології створення інформаційних систем можна класифікувати по декільком відмітним ознакам.

Основними задачами, рішення яких повинна забезпечувати методологія створення інформаційних систем, є наступні:

– забезпечення створення інформаційних систем, що відповідають цілям і завданням підприємства та відповідним пропонованим ними вимогам;

– гарантія створення системи із заданими параметрами протягом заданого часу в рамках певного бюджету;

– простота супроводження, модифікації й розширення системи з метою забезпечення її відповідності мінливим умовам роботи підприємства;

– забезпечення створення інформаційних систем, що відповідають вимогам відкритості, мобільності й масштабованості;

– можливість використання в створюваній системі розроблених раніше засобів інформаційних технологій (програмного забезпечення, баз даних, засобів обчислювальної техніки, телекомунікацій).

Саме методологія визначає, які мови й системи будуть застосовуватися для розробки програмного забезпечення й, багато в чому, рекомендує, який технологічний підхід буде при цьому використаний.

Виділяють наступні загальні вимоги, яким повинні задовольняти технології програмування і супроводження інформаційних систем [5-9]:

– підтримувати повний життєвий цикл інформаційної системи;

– забезпечувати гарантоване досягнення цілей розробки системи із заданою якістю та у встановлений час;

– забезпечувати можливість розділення великих проектів на ряд підсистем, а саме ділити композицію проекту на складові частини, які розробляються групами виконавців обмеженої чисельності, з наступною інтеграцією складових частин;

– технологія повинна забезпечувати можливість ведення робіт із програмування окремих підсистем невеликими групами;

– забезпечувати мінімальний час одержання працездатної системи;

– передбачати можливість керування конфігурацією проекту, ведення версій проекту і його складових, можливість автоматичного випуску проектної документації й синхронізацію її версій з версіями проекту;

– забезпечувати незалежність виконуваних проектних рішень від засобів реалізації системи - системи керування базами даних, операційної системи, мови й системи програмування.

Висновки. У статті було розглянуто основні задачі методології програмування інформаційних систем, подана класифікація методологій та виділено головні вимоги до технології створення програмного продукту.

Інформаційні джерела

1. Петров В.Н. Информационные системы: учеб. пособие - СПб.: Питер, 2002. - 588 с.

2. Краткий философский словарь / под ред.А.П. Алексеева. - 2-е изд., перераб. и доп. - М.: ТК Велби, Изд-во Проспект, 2006. - 496 с.

3. Юдин Э.Г. Методология науки. Системность. Деятельность. - М.: Эдиториал УРСС, 1997. - 246 с.

4. Информационные системы: учеб пособие / под ред. В.Н. Волковой, Б.И. Кузина. - 2-е изд., перераб и доп. - СПб.: Изд-во СПбГПУ, 2004. - 224 с.

5. Брауде Э. Технология разработки программного обеспечения. - СПб,: Питер, 2004. - 655 с.

6. Мацулевич О.Є., Щербина В.М. Використання пакету прикладних програм NETCRACKER // Фундаментальна підготовка фахівців у природничо-математичній, технічній, агротехнологічній та економічній галузях : матеріали Всеукраїнської наук.-практ. конференції з міжнар. участю (Мелітополь, 11-13 вересня 2017 р.) : присвяченої 85-річчю кафедри вищої математики і фізики ТДАТУ.

7. Мацулевич О.Є., Щербина В.М., Коломієць С.М. Геометричне моделювання складних тривимірних поверхонь із застосуванням матричного рівняння еліптичного повороту // / Праці Таврійського державного агротехнологічного університету, Вип. 19(2), С. 294-300

8. Мацулевич О.Є., Зінов'єва О.Г. Розв’язання задач аналізу тренд-сезонних часових рядів / Праці Таврійського державного агротехнологічного університету, Вип. 19(2), С. 264-270

9. Корчинський В.М., Свинаренко Д.М., Мацулевич О.Є. Методи підвищення інформаційних показників багатоспектральних зображень на основі ортогоналізації даних / Праці Таврійського державного агротехнологічного університету, Вип. 14(2), 2014, С. 264-270.

УДК [004.42+005.6]:378.1

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ВИБОРУ ОСВІТНЬОЇ ПРОГРАМИ

Гулковський М., Придатко О.
Львівський державний університет безпеки життєдіяльності, Львів

У роботі досліджено проблематику щодо вдалого вибору освітньої програми для подальшого навчання у Львівському державному університеті безпеки життєдіяльності. Запропоновано вирішення проблеми вдалого вибору шляхом розроблення та інтеграції в освітнє середовище відповідної системи підтримки прийняття рішень.

Ключові слова: *прийняття рішень, система, абітурієнт, освітня програма*

The problem of choosing a future profession for the entrant of Lviv State University of Life Safety is investigated in the work. The solution of the problem of successful choice by development and integration into the educational environment of the corresponding decision support system is offered.

Key words: *decision making, system, entrant, educational program*

На завершальних етапах здобуття середньої освіти, будь-який абітурієнт задається запитанням вибору майбутньої професії. І не завжди вдається зробити вірний вибір. Не одноразові випадки, коли студенти керуючись інтуїцією батьків, підказками друзів або просто обираючи майбутню професію шляхом підбору сертифікатів ЗНО, вже на перший курсах усвідомлює про невірний вибір. Власне такий стан справ зумовив до глибшого розкриття означеної проблеми та розроблення рішень для ефективного вибору освітньої програми із використанням інформаційних технологій.

Для досягнення поставленої мети в роботі окреслені такі завдання:

– провести оцінку наявних у Львівському державному університеті безпеки життєдіяльності освітніх програм на предмет їх відносності до певних категорій;

– на основі проведеної оцінки спеціальностей розробити тестове завдання, що надаватиме ґрунтовні підстави для вибору певної освітньої програми;

– із використанням технології Java програмно реалізувати описану технологію тестування із автоматичним опрацюванням результату (розробити систему підтримки прийняття рішень).

– провести емпіричні дослідження та порівняти їх з результатами натурних спостережень.

Перше питання, яке постало в ході реалізації задуму, це визначення основних результатів навчання освітніх програм. Для цього за основу взято стандарти вищої освіти відповідних спеціальностей та проведено опитування студентів старших курсів. В результаті детального аналізу стандартів та отриманих даних опитування визначені основні характеристики (труднощі, переваги тощо) навчання на освітніх програмах Університету. Зроблено висновок, що деякі освітні програми тісто пов'язані між собою, що надало можливість сформувати певні групи освітніх програм (наприклад Комп'ютерні науки та Кібербезпека; Пожежна безпека та Цивільна безпека тощо).

Формування тестового опитування базувалось на основних принципах психодіагностики. В основу тестування закладено три рівні опитування:

– 1-ший відповідає за розподіл за загальними вподобаннями та ділить респондентів на три категорії (технічний, гуманітарний та нейтральний).

– 2-гий, включає в себе чіткіші запитання, які стосуються певної групи освітніх програм, та орієнтує вподобання користувача до певної освітньої програми.

– 3-й етап визначає до якої із суміжних спеціальностей, абітурієнт має найбільшу схильність (наприклад Комп'ютерні науки або Кібербезпека; Пожежна безпека або Цивільна безпека тощо).

За результатами тестування користувач отримує від системи повідомлення про освітню програму, яка найбільш підходитиме абітурієнту, зважаючи на аналіз даних психодіагностики та особистих еподобань.

Здійснивши побудову основних елементів системи постало питання у зручності подання відповідної інформації до користувача та проведення анонсованого тестування. Інтерфейс ситеми вирішено реалізувати у вигляді аплікація для мобільного застосунку під операційну систему Android з використанням мови програмування Java. Програмний код реалізовано у 4-х класах, які швидко та без зайвих обрахунків зчитують, та аналізують вхідні дані. Задля наочності структури програмного коду подано UML-діаграму аплікації (рис. 1).

В подальшому планується реалізація descktop-інтерфейсу з використанням JavaFX, який дозволятиме швидке проходження тестування.

І завершальним етапом роботи, який буде реалізовано після повної розробки застосунку, це емпіричні дослідження ефективності роботи додатку та його удосконалення за необхідності. За результатами емпіричних досліджень буде визначено відсоткову похибку правильності вибору освітніх програм студентами Університету. Підставою для проведення подібних досліджень є неодноразові відгуки здобувачів освіти про важкість навчання та незадоволення вибором обраної освітньої програми. Попередня орієнтація на визначену освітню програму, на наше переконання, значно зменшить кількість незадоволених студентів та підвищить якість навчання.

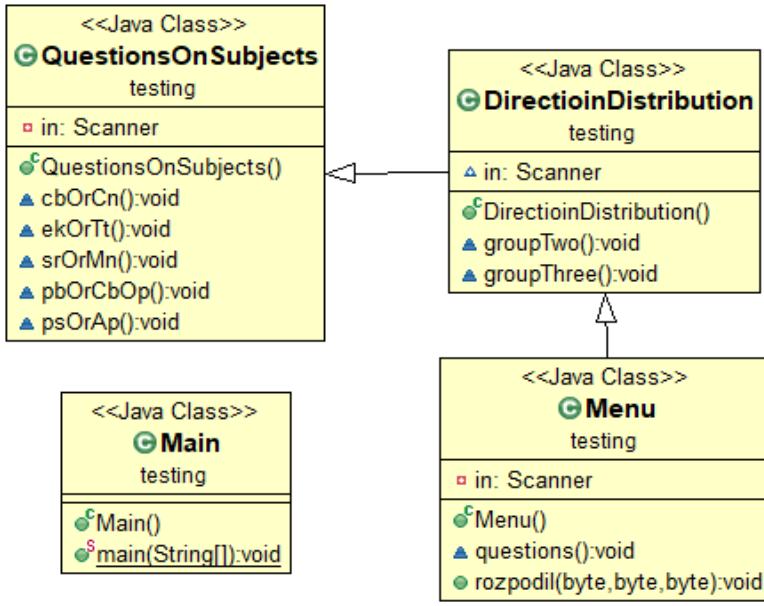


Рис 1. UML-діаграма

Інформаційні джерела

1. Різун Н. О. Розробка методів та моделей мінімізації похибок машино-людської взаємодії в автоматизованих системах діагностики рівня професійної підготовки / Н. О. Різун // Науковий вісник НГУ : науковий журнал. – Дніпропетровськ : НГУ, 2013. – № 2. – С. 90-97.

2. Prydatko, O., Prydatko, V., Borzov, Yu., & Dzen V. (2018). Integration of the new method of mobile education in educational projects of programmer training. Bulletin of Lviv State University of Life Safety, 18, 71-80. https://doi.org/0.32447/20784643.18.2018.07

3. Придатко О. В. Інтеграція 3D-інтерактивних технологій навчання в освітні проекти безпеко-орієнтованих спеціальностей / О. В. Придатко, А. Г. Ренкас, Н. Є. Бурак, М. В. Лемішко // Вісник ЛДУБЖД: Зб. наук. праць. Львів: ЛДУ БЖД, 2017. – №15. – С.46-54.

4. Козяр М. М. Інтерактивні методики навчання у ВНЗ / М. М. Козяр // Проблеми та перспективи формування національної гуманітарно-технічної еліти : зб. наук. праць. – Харків : НТУ «ХПІ», 2015. - №42(46). – С. 285-292.

5. Head First Java (изучаем Java) : пер. с англ. / Kathy Sierra, Bert Bates. – Москва : «Эксмо», 2012. – 718 с.

ГЕНЕРАЦІЯ РОЗМІТКИ З ВИКОРИСТАННЯМ КОМП'ЮТЕРНОГО ЗОРУ

Матюшенко М., Сліпченко В.
каф. ГМКГ Національний технічний університет «Харківський політехнічний інститут», м. Харкыв

Автоматизація генерації UI розмітки за допомогою Computer Vision бібліотек з використанням мови програмування Python.

Ключові слова: *Computer Vision, CV, ML, Python, UI, Automation, Generation, User Interface, WEB, IT, Веб-розробка, Комп'ютерний зір, Алгоритм розпізнавання, Графічні об'єкти.*

Комп'ютерний зір – теорія та технологія створення програмного забезпечення або машин, які можуть бачити шляхом обробки зображення, яке надходить з відео-пристроїв. Як наукова дисципліна, комп'ютерний зір відноситься до методології створення штучних систем, які отримують інформацію з зображень. Відео дані можуть бути представлені безліччю форм, таких як звичайні зображення, відеопослідовність, зображення з різних камер або тривимірні дані з медичного сканера. Розробки подібного роду можуть бути використані у різних галузях та сферах людської діяльності з метою покращення за рахунок більш точного аналізу та використання інформації.

Оскільки розробка програмних продуктів продовжує розвиватися, ми все більше відчуваємо потребу в продуманій, конструктивній, системній розробці, продукт якої повинен мати можливість перевикористання і має відповідати сучасним стандартам за такими критеріями як: гнучкість в інтеграції, масштабуванні, та легкість підтримки.

Багато чого було сказано на рахунок створення систем дизайну, і найбільший акцент робиться, в основному, на встановлення кольорів, розмітки, графічних об'єктів, текстур і т.п. Такий підхід до вирішення проблеми, безсумнівно, важливий, проте дані аспекти дизайну, по великому рахунку, вони завжди суб'єктивні. Останнім часом розробникам не давав спокою питання про те, з чого складаються наші інтерфейси, і як ми можемо проектувати їх більш осмислено і систематично, економлячи при цьому ресурси – як на проектування, так і на реалізацію.

За прикладом для реалізації концепту можно звернутися то основ хімії. Всі речовини (такі як тверді тіла, рідини, гази, прості, складні і т.д) складаються з атомів. Атоми зв'язуються між собою і утворюють молекули, які, в свою чергу, комбінуються і формують більш комплексні системи - організми.

Схожим шляхом інтерфейси складаються з менших компонентів. Це означає, що ми можемо розбити інтерфейси на логічні, фундаментальні блоки і комбінувати їх, поступово нарощуючи їх складність. Це суть сучасного атомного веб дизайну та розробки в цілому.

Використовуючи такий елементарний та розподілений підхід, ми маємо можливість автоматизувати створення розмітки інтерфейсу користувача, що значно спростить життя як розробнику, так і користувачеві та прискорить процес розробкил; мінімізує кількість використовуваних ресурсів .

Досягненути даної мети допоможе Python з розвиненою технологією комп'ютерного зору. Суть даної технології полягає в аналізі графічного файлу, розбиті на логічні елементи і генерацію розмітки.

Основна ідея така: зображення-зразок має бути структуровано, тобто інформація в ньому повинна бути зменшена до необхідного мінімуму, але так щоб не втрачався сенс. Наприклад, художники малюють скетчі - всього в кілька точних ліній художник може зобразити обличчя людини або якийсь предмет і глядачеві буде зрозуміло що зображено. Зображення містить матрицю M * N пікселів. Кожен піксель містить певну кількість біт інформації про колір, а якщо уявити це все у вигляді параметрів ліній, то обсяг інформації різко зменшується і обробка такої інформації набагато спрощується. Приблизно те ж саме повинен робити алгоритм. Він повинен виділити головні деталі в кадрі - то що несе в собі основну інформацію і відкинути все зайве.

Для цього варто лише залучитися підтримкою відповідної бібліотеки та налаштувати параметри, які дозволять направити програму на пошук необхідних елементів виходячи з поданого зображення. Проте варто пам’ятати, чим краще графічне зображення – тим кращий і більш передбачуваний результат мі отримаємо.

У результаті розпізнавання буде згенеровано відповідну html розмітку у текстовому форматі та збережено на обраний носій. Отриману розмітку можна використовувати при побудові веб сторінок, інтерфейсів та багато чого іншого.

Інформаційні джерела

1. Pcmag.com – What Is Computer Vision?, 2020р. – [Електронний ресурс]: https://www.pcmag.com/news/what-is-computer-vision

2. Tryolabs.com – An Introductory Guide to Computer Vision, 2020р. – [Електронний ресурс]: https://tryolabs.com/resources/introductory-guide-computer-vision/

3. Sciencedirect.com – Computer Vision Algorithms, 2019р. – [Електронний ресурс]: https://www.sciencedirect.com/topics/computer-science/computer-vision-algorithms

4. Medium.com – Object Detection Techniques in Computer Vision, 2020р. – [Електронний ресурс]: https://medium.com/swlh/object-detection-techniques-in-computer-vision-7c169771fb15

5. Frontiersin.org – Object Detection: Current and Future Directions, 2015р. – [Електронний ресурс]: https://www.frontiersin.org/articles/10.3389/frobt.2015.00029/full

УДК: 004.03

РОЗВ'ЯЗАННЯ ЗАДАЧ КЛАСИФІКАЦІЇ І РЕГРЕСІЇ ІЗ ЗАСТОСУВАННЯМ СПЕЦІАЛІЗОВАНИХ БІБЛІОТЕК

Новіков А.В., Холодняк Ю.В.
Таврійський державний агротехнологічний університет ім. Дмитра Моторного, м. Мелітополь

Пропонуються нові можливості застосування комп'ютерних технологій для розв'язання задач класифікації і регресії.
Ключові слова: *комп'ютерні технології, класифікація, регресія, аналіз даних.*

New opportunities of employment of computer technologies for decision of problems of classification and regression are offered.
Keywords: *computer technology, classification, regression, data analysis.*

З появою перших комп'ютерів настав етап інформатизації різних сторін людської діяльності. В даний час сучасні обчислювальні системи і комп'ютерні мережі дозволяють зберігати великі масиви даних для розв'язання задач обробки і аналізу. На жаль, сама по собі машинна форма представлення даних містить інформацію, необхідну людині, в прихованому вигляді, і для її отримання потрібно використовувати спеціальні методи аналізу даних.

Технологія Data Mining (інтелектуальний аналіз даних) вивчає процес знаходження нових і корисних знань в базах даних. При аналізі накопичених даних часто потрібно визначити, до якого з відомих класів відносяться досліджувані об'єкти, тобто розв'язати задачу класифікації. Наприклад, коли людина звертається в банк за наданням йому кредиту, банківський службовець повинен прийняти рішення: чи кредитоспроможний потенційний клієнт чи ні. Очевидно, що таке рішення приймається на підставі даних про досліджуваний об'єкт (в даному випадку - про людину): його місце роботи, розмір заробітної плати, вік, склад сім'ї і тому подібне. В результаті аналізу цієї інформації банківський службовець повинен віднести людину до одного з двох відомих класів: "кредитоспроможний" і "некредитоспроможний".

В даній роботі пропонуються нові можливості застосування комп'ютерних технологій для розв'язання задач класифікації і регресії**.** У Data Mining задачу класифікації розглядають як задачу визначення значення одного з параметрів аналізованого об'єкту на підставі значень інших параметрів. Параметр, значення якого треба визначити, часто називають залежною змінною, а параметри, що беруть участь в його визначенні, - незалежними змінними. У

розглянутому прикладі незалежними змінними є зарплата, вік, кількість дітей. Залежною змінною в цьому прикладі є кредитоспроможність клієнта. Якщо значеннями незалежних і залежної змінних є дійсні числа, то задача називається задачею регресії. Прикладом задачі регресії може бути задача визначення суми кредиту, яка може бути видана клієнту.

Задачі класифікації і регресії розв'язуються в два етапи. На першому виділяється навчальна вибірка. У неї входять об'єкти, для яких відомі значення як незалежних, так і залежних змінних. У описаному раніше прикладі такою навчальною вибіркою може бути інформація про клієнтів, яким раніше видавалися кредити на різні суми, і інформація про їх повернення.

На підставі навчальної вибірки будується модель дерева рішень для отримання правил класифікації або регресії. Цю модель часто називають функцією класифікації або регресії. Для отримання максимально точної функції до навчальної вибірки пред'являються наступні основні вимоги:

– кількість об'єктів, що входять у вибірку, має бути достатнє великим, чим більше об'єктів, тим точніше буде побудована на її основі функція класифікації або регресії;

– у вибірку повинні входити об'єкти, що представляють всі можливі класи в разі задачі класифікації або всю область значень в разі задачі регресії.

На другому етапі побудовану модель дерева рішень застосовують до аналізованих об'єктів для визначення значення залежної змінної.

При, наприклад, розв'язанні задачі класифікації даних про клієнтів телекомунікаційної компанії, з метою визначення чи покине клієнт компанію після двох років співпраці, вихідні дані представлені в таблиці 1.

Таблиця 1

Стать	Вік	Поточний тариф	Витрачена сума	Покинув
f	23	Normal	345	No
m	18	Power	9455	No
m	36	Power	456	No
m	34	Normal	3854	Yes
f	52	Economy	2445	No
f	19	Economy	14 326	No
f	45	Normal	347	No
m	42	Economy	5 698	Yes
m	21	Power	267	No
m	48	Normal	4 711	Yes

В результаті побудови моделі дерева рішень отримуємо наступні правила класифікації:

Rules:

1. IF вік equals below20 THEN 'покинув' = 'no'

2. IF вік equals 20to30 THEN 'покинув' = 'no'

3. IF вік equals 31to40 AND поточний_тариф equals normal THEN 'покинув' = 'yes'

4. IF вік equals 31to40 AND поточний_тариф equals power THEN 'покинув' = 'no'

5. IF вік equals 31to40 AND поточний_тариф equals econoty THEN 'покинув' = 'yes'

6. IF вік equals 41to50 AND стать equals f THEN 'покинув' = 'no'

7. IF вік equals 41to50 AND стать equals m THEN 'покинув' = 'yes'

8. IF вік equals 51to60 THEN 'покинув' = 'no'

9. IF вік equals above61 THEN 'покинув' = 'no'

Аналізуючи результати, можна зробити висновок, що з 4 аналізованих клієнтів 2 клієнти покинуть компанію.

Висновки. Запропоновано нові можливості для розв'язання задач класифікації і регресії з використанням бібліотеки Xelopes алгоритмів data mining.

Інформаційні джерела

1. Барсегян А.А., Куприянов М.С., Степаненко В.В., Холод И.И. Методы и модели анализа данных: OLAP и Data Mining – СПб.: БХВ-Петербург, 2004. – 336 с.

2. Гайдышев И. Анализ и обработка данных: специальный справочник– СПб.: Питер, 2001. – 752 с.

3. Мандель И.Д. Кластерный аналіз : Финансы и статистика, 1988. – 176 с.

4. Мацулевич О.Є., Щербина В.М. Використання пакету прикладних програм NETCRACKER // Фундаментальна підготовка фахівців у природничо-математичній, технічній, агротехнологічній та економічній галузях : матеріали Всеукраїнської наук.-практ. конференції з міжнар. участю (Мелітополь, 11-13 вересня 2017 р.) : присвяченої 85-річчю кафедри вищої математики і фізики ТДАТУ.

5. Мацулевич О.Є., Щербина В.М., Коломієць С.М. Геометричне моделювання складних тривимірних поверхонь із застосуванням матричного рівняння еліптичного повороту // / Праці Таврійського державного агротехнологічного університету, Вип. 19(2), С. 294-300.

ПОШУК КОРЕЛЯЦІЇ ОЗНАК КОРИСТУВАЧІВ ТА ЧАТ-БОТУ ОНЛАЙН-ТЕРАПІЇ

Погребняк Т., Заволодько Г.
Національний технічний університет «ХПІ»,

Анотація. *У даній статті проведено аналіз шляхів пошуку залежності швидкості відповіді системи миттєвого обміну повідомленнями в залежності з повідомленнями користувача. Розглянуті залежності ймовірності відповіді системи від очікування користувача та ймовірності виходу з чат-боту.*

Ключові слова: *чат-бот, система миттєвого обміну повідомленнями, кореляція даних, онлайн-терапія.*

Abstract. *This article analyzes the ways to find the response rate of the instant messaging system depending on the user's messages. The dependences of the probability of the system response on the user's expectation and the probability of leaving the chatbot are considered.*

Keywords*: chatbot, instant messaging system, data correlation, online therapy.*

Системи миттєвого обміну повідомленнями використовуються сотнями мільйонів людей по всьому світу. Вони перетворилися із засобів для спілкування між людьми у засоби для отримання інформації та у неймовірно потужний маркетинговий інструмент. Онлайн-терапія (психотерапія онлайн, e-therapy, віртуальна психотерапія, телетерапія або веб-консультування) - відносно нова форма психологічних послуг, в якій терапевт або консультант надає психологічну допомогу через інтернет.[1] Ключовою частиною, при використанні чат- ботів в онлайн-терапії, є можливість спілкуватися клієнтам із ботами. Це дозволяє автоматизувати процес консультування, та оптимізувати роботу фахівців. Брак часу, мала кількість співробітників, слабо розвинені технічні потужності – все це позначається на якості і ефективності взаємодії з клієнтами. Боти дозволяють уникнути цих проблем.

За останні 10 років чат-боти почали широко застосовуватись для пошуку та передачі інформації, ринок чат-ботів оцінюється в $1,5 мільярда доларів та зростає на ~20% щорічно [2].

При цьому найбільше на якість окремого чат-боту в цілому впливає якість інформації та швидкість відповіді: якщо користувач не задоволений якістю або швидкістю, він виходить з чат-боту [3]. Виходом вважається момент, після якого користувач не відповідає на відповіді чат-боту. [4]

При початковому аналізі залежності ймовірності виходу користувача від часу очікування одної відповіді не було виявлено кореляції. При цьому людська поведінка повинна відповідати нормальному розподілу [5], але розподіл ймовірностей після кожної окремої відповіді не відповідає будь-якому відомому розподілу і схожий на нестабільне плато після 2 хвилин очікування. У процесі зміни від нульової до першої хвилини очікування відповіді, з боту виходить менше 5% користувачів, однак починаючи з 2 хвилини, кількість змінюється до 8%.

Було виявлено, що кореляція між часом очікування та ймовірністю виходу з боту існує лише за умови, що час очікування не зменшується 3 відповіді підряд. Це означає, що вплив на ймовірність має лише швидкість послідовності відповідей, а кожна окрема відповідь такого впливу не має.

Ймовірність виходу починає змінюватись й стабільно зростати якщо час очікування складає понад 2 хвили на протязі 3 відповідей. При таких умовах розподіл ймовірностей ідеально відповідає розподілу Гаусса.

На основі цього аналізу можемо зробити висновок, що швидкість чат-боту не впливає на якого якість, якщо хоча б кожна друга відповідь надається менше ніж за 2 хвилини. Таким чином на якість онлайн-терапії не впливає затримка у часі при відповіді чат-бота.

Інформаційні джерела

1. Провотар, А. И. Особенности и проблемы виртуального общения с помощью чат-ботов / Провотар, А. И., Клочко К. А.. // Наукові труди Винницького національного технічного університету. – 2013. – №3.

2. Chatbot Market Research [Електронний ресурс] // Allied Market Research. – 2020. – Режим доступу до ресурсу: https://www.alliedmarketresearch.com/chatbot-market.

3. Chatbots: History, technology, and applications [Електронний ресурс] // Eleni Adamopoulou. – 2020. – Режим доступу до ресурсу: https://www.researchgate.net/publication/345815999_Chatbots_History_technology_and_applications.

4. Drpaul P Mathai. Customer Churn Prediction: A Survey [Електронний ресурс] / Drpaul P Mathai // International Journal of Advanced Research in Computer Science. – 2020. – Режим доступу до ресурсу: https://www.researchgate.net/publication/343787983_Customer_Churn_PredictionA_Survey.

5. Craig P. Speelman. How Mean is the Mean? [Електронний ресурс] / Craig P. Speelman, Marek McGann // Frontiers in Psychology. – 2016. – Режим доступу до ресурсу: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3719041/.

УДК 004

ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМІВ КОЛЕКТИВНОГО ОБЧИСЛЮВАЛЬНОГО ІНТЕЛЕКТУ

Попроцька Д.І., Рудніченко М.Д., Бут Н.В.
Одеський національний політехнічний університет, м. Одеса

Метою даної роботи є огляд основних алгоритмів колективного інтелекту обчислювальних систем, шляхом опису принципів роботи, а також виявлення їх переваг та недоліків. Порівняльний аналіз алгоритмів проводився за такими критеріями: швидкість виконання, галузі застосування, простота реалізації та інші.

Ключові слова: *колективний інтелект, обчислювальний інтелект, алгоритми, бджолиний алгоритм, алгоритм кажанів, алгоритм зозулі, порівняльна характеристика.*

The purpose of this work is to review the basic algorithms of collective intelligence of computer systems, by describing the principles of operation, as well as identifying their advantages and disadvantages. The comparative analysis was conducted according to the following criteria: speed of implementation, areas of application, ease of implementation and others.

Keywords: *collective intelligence, numerical intelligence, algorithms, bjolin algorithm, Kazan algorithm, zozuly algorithm, individual characteristic.*

З стрімким розвитком сучасних технологій обчислювальний інтелект стає все більш розповсюдженим у більшості галузей науки. Це, здебільшого, зумовлено, необхідністю обробки великих обсягів даних для спрощення їх аналізу та пошуку оптимальних параметрів моделей для підвищення ефективності вирішення відповідних прикладних завдань.

При розробці великих технологічних, енергетичних, аерокосмічних, інформаційних та інших складних комплексів виникають питання, пов'язані з вибором оптимальної організації взаємодії елементів, режимів їх функціонування, як наслідок, з необхідністю вирішення завдань оптимізації [1].

Одним з перспективних напрямків обчислювального інтелекту, який вирішує ряд питань оптимізації, є колективний інтелект.

На даний момент алгоритми колективного інтелекту широко застосовуються в різних галузях, наприклад, у медицині, робототехніці, в оптимізаційних задачах і так далі.

Системи колективного інтелекту, як правило, складаються із множини агентів, що локально взаємодіють як між собою так із навколишнім середовищем.

Самі агенти зазвичай досить прості, але всі разом, вони створюють так званий колективний інтелект. Прикладом у природі може служити колонія мурах, рій бджіл, зграя птахів, косяк риб.

Для аналізу було обрано три алгоритми колективного інтелекту: бджолиний алгоритм, алгоритм зозулі та алгоритм кажанів. Кожний з алгоритмів має свої переваги та недоліки. Для їх виділення необхідно проаналізувати кожний з них, та виділити основні характеристики.

Першим алгоритмом є алгоритм кажанів, який застосовується для вирішення завдань оптимізації, проектування, планування, класифікації, вирішення проблеми ергономіки робочого місця та ін.

Однією з основних переваг алгоритму є швидкість його виконання. Цей алгоритм потенційно більш потужний, ніж алгоритм рою часток і генетичний алгоритм.

Алгоритм може здатися трохи складніше, ніж більшість інших алгоритмів ройового інтелекту, а також еволюційних алгоритмів, проте він може бути досить ефективно застосований до проблем оптимізації і давати хороші результати, витрачаючи меншу кількість часу [2].

Наступним є бджолиний алгоритм, який використовується для вирішення різних завдань, що виникають при плануванні виробництва, складанні графіків огляду, зберігання і транспортування товарів та інше, які часто можуть бути представлені як завдання теорії графів.

Дані завдання відносять до класу NP-важких завдань, точне рішення яких не можна знайти за розумний час, тому що простір пошуку рішень збільшується в експоненційної залежності від вхідних даних [2].

Останнім алгоритмом є алгоритм зозулі, який являє собою оптимізований алгоритм. Натхненням для його створення послужив гніздовий паразитизм деяких видів зозуль, що підкладають свої яйця до гнізд інших птахів.

У алгоритмі зозулі такий спосіб поведінки був ідеалізований і таким чином може бути пристосованим для розв'язування різноманітних задач оптимізації.

Можливо, він зможе перевершити інші метаевристичні алгоритми у прикладних програмах. Іншою сферою застосування, здавалось би зовсім не пов’язаною з алгоритмом, є алгоритм хешування [3].

Повну порівняльну характеристику приведено в таблиці 1. Таким чином, можна побачити, що ефективність використання відповідного алгоритму може відрізнятися для різних типів завдань, що вказує на необхідність проведення ретельного попереднього аналізу вихідних даних.

Таблиця 1

Порівняльна характеристика

Назва алгоритму	Бджолиний	Кажанів	Зозулі
Швидкість виконання алгоритму	–	+	+ –
Виділення підсистем	+	+	+
Ефективність вирішення задач	+	+	+
Простота реалізації	+	–	–
Зручність в застосуванні до різного спектру завдань (масштабованість)	+	+	+
Використання додаткових методів для реалізації	–	+	+
Вплив параметрів, що настроюються на результати роботи алгоритму	+	+	+
Точність виконання	+	+	+

Висновки. Таким чином використання того чи іншого алгоритму залежить від типу завдання, яке необхідно вирішити. В даній роботі був проведений аналіз алгоритмів колективного інтелекту, були виявлені їх переваги та недоліки. Отримані результати будуть використані у подальшій роботі над даною тематикою.

Інформаційні джерела

1. Системное описание алгоритмов роевого интеллекта. - [Електронний ресурс]. - Режим доступу: https://www.researchgate.net/publication/281065239_Sistemnoe_opisanie_algoritmov_roevogo_intellekta

2. Алгоритми колективного інтелекту - [Електронний ресурс]. - Режим доступу: https://lektsii.org/4-17736.html

3. Алгоритм зозулі. Вікіпедія. - [Електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%B7%D0%BE%D0%B7%D1%83%D0%BB%D1%96

УДК 004

РОЗРОБКА ПРОЕКТУ МОБІЛЬНОГО ЗАСТОСУВАННЯ ПІДТРИМКИ РОБОТИ КАСОВОЇ СИСТЕМИ

Рудніченко М. Д., Голопотилюк Є. А., Плотніков М. С.
Одеський національний політехнічний університет, м. Одеса

В роботі наведено опис проекту мобільного застосування для ведення облікових дій з управління фінансовими транзакціями у малому бізнесі.
Ключові слова: *мобільні застосування, Android, платіжні системи, касові рішення.*

The paper describes the project of mobile application for accounting operations for financial transaction management in small business.
Keywords: *mobile applications, Android, payment systems, cash solutions.*

У наш час дуже розвинута система безготівкового розрахунку та касового обліку. Кожен день мільйони транзакцій проходять через наші банківські рахунки. Підприємці намагаються бути конкурентоспроможними та йти з ногою в тренд, але інколи обмеження не дають змоги реалізувати подібні системи. Для того, щоб встановити касовий апарат потрібно мати цілий список техніки та додаткових умов – стабільний інтернет, комп'ютер, сканер, принтер та інше, що іноді не можливо встановити на локації котрій працює підприємець. Така проблема розповсюджується на ФОП першої та другої групи котрі ведуть торгівлю на ринку, в ларьках та займаються сезонним бізнесом, де придбання техніки на малий період не є рентабельним [1]. Окремою проблемою є встановлення та підтримування системи безготівкового розрахунку. Відсутність електроживлення та висока плата за техніку, відштовхує підприємців. По статистичним даним приблизно 30 відсотків доходу приходиться на безготівковий розрахунок, це відображається на конкурентоспроможності та доходах підприємця. Розвиток мобільних технологій має актуальне рішення для даних проблем. Кожен має мобільний телефон на операційній системі Android та IOS, даний момент показує, що населення пристосувалось та використовує телефон постійно [2].

Основні задачі для вирішення проблем и створення продукту – створення мобільного додатку на Android, що дозволить створювати бази продуктів, приймати оплату, створювати електроні чеки, зберігати інформацію у хмарі.

Для створення зрозумілого інтерфейсу та роутину, створюється макет переходів та сцен, що доступні користувачу при відповідних умовах. Логічний ланцюг починається з завантаження мобільного додатку, потім реєст-

рації, авторизації та переходу до приватного кабінету. Обмеження користувача у відповідних сценах, дає можливість уникнути системних помилок та зробити зрозумілі переходи. Для цього моменту, будується свого роду макет, через котрий можна подивиться переходи, що відображено на рисунку 1. Початкова точка – завантаження, а кінцева закриття мобільного додатку. Це допомагає відслідкувати статистку та проводити аналітику про дії користувача.

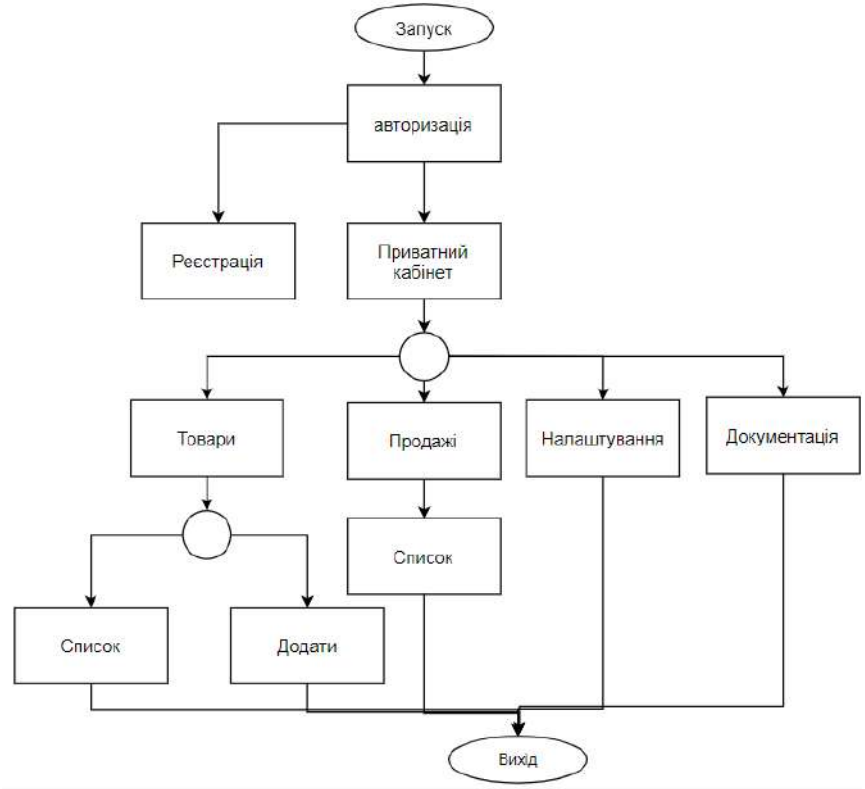


Рис. 1. Структурна схема життевого циклу роботи мобільного застосування

Коли клієнт завантажує мобільний додаток, або заходить в персональну панель, він звертається до серверу «CosmoPay» на якому виконуються певні функції – звернення до СУБД MongoDB, API E-Receipt, API LiqPAy. У відповідь з серверу клієнт отримує відповідь, що містить в собі інформа-

цію для продовження роботи. Структура відповіді базується на відповіді «помилка» та «успішно» з під'єднаною інформацією, якщо це потрібно.

Для захисту передачі даних використовується так звані публічні та приватні ключі. За допомогою них, сервер та клієнт може зашифровувати та розшифровувати дані.

Для обміну інформацією використовується JSON-файл, що відображається на сервері з певним переданим ключем захист. Наприклад: cosmopay.com.ua/transaction/? act = guser&dk=f3vg2r4fDf3gbvb2G3423f, де, атрибут «act» відповідає за функцію, котру потрібно використати на сервері, а атрибут «dk» містить в собі ключ сесії для доступ зчитування json-файлу.Проект створений для проведення транзакцій, створення РРО та POS. Існує два типи користувача – користувач, що використовує мобільний гаманець та підприємець, що користується мобільним терміналом. Алгоритм продажу за допомогою системи "CosmoPay" реалізовано наступним чином.

Покупець вибирає товари, продавець формує замовлення та QR-code через мобільний додаток, покупець сканує код та провірівши інформацію про оплату згоджується Уся інформація проходить через сервер проекту та повертає відповідні результати. Для точного розуміння працездатності та функціонування проекту, потрібно розуміти її архітектури та зв'язки класів.

За допомогою класу «DataBase» ми можем з'єднатись з сервером та отримати дані з таблиці. Для запиту на сервер використовується url з GET даними у шифрованому виді. Після отримання даних, ми можемо відображати елементи – список карток та транзакцій. За допомогою класу «Private» додаток шифрує, або дешифрує дані. У виді «private_key+data+public_key»

Висновки. Розроблений проект мобільного застосування може бути використаний фізичними та юридичними особами для контролю і управління виконаних фінансових операцій, зменшуючи витрати на додаткове обладнання.

Інформаційні джерела

1. Уланова К.С. Сучасні платіжні системи: поняття, вимоги, тенденції / К.С. Уланова // Азимут наукових досліджень: економіка і управління. – 2018. – №. 3 (28). – С. 382-384.

2. Балашев Н.Б. Динаміка розвитку електронних платіжних технологій / Н.Б. Балашев, Д.В. Пономарьов // Міжнародний журнал гуманітарних та природничих наук. – 2019. – №13. – С. 119-123.

УДК 004

РОЗРОБКА КОНЦЕПЦІЇ ПРОГРАМНОГО ЗАСТОСУВАННЯ СПРЯМОВАНОГО НА ОТРИМАННЯ ПОБУТОВИХ ПОСЛУГ

Рудніченко М.Д., Медяник Є.І., Кобець М.О., Березовський В.О.
Одеський національний політехнічний університет, Одеса

У роботі розглянуто концепцію поетапної розробки мобільного додатку для надання та отримання побутових послуг, зокрема наведено результати аналізу інструментів, за допомогою яких, реалізація відповідного програмного забезпечення стане більш ефективною.

***Ключові слова**: REST, Android, Java, Kotlin, JavaScript.*

The paper considers the concept of step-by-step development of a mobile application for the provision and receipt of household services, in particular, the results of the analysis of tools with which the implementation of relevant software will be more effective.

***Keywords:** REST, Android, Java, Kotlin, Javascript.*

Вступ. Одними з затребуваних послуг у світі мають побутовий характер, з метою спрощення цього процесу є розробка програмного застосування (ПЗ), яке дозволить за мінімальний проміжок часу отримати відповідні послуги [1]. З цієї причини, концепція мобільного веб-застосування, яке здатне виповнювати всі відповідні функції є досить актуальною. Можливість охопити велику кількість користувачів є найвищим пріоритетом у розробці веб-застосування орієнтованого на надання можливості отримання побутових послуг. Серед додаткових переваг розробки ПЗ можна виділити можливість розгортання нових функцій у середовищі та швидкість виправлення помилок, що є одним із головних факторів у заощадженні часу. Діаграмам основних варіантів використання ПЗ наведена на рис. 1.

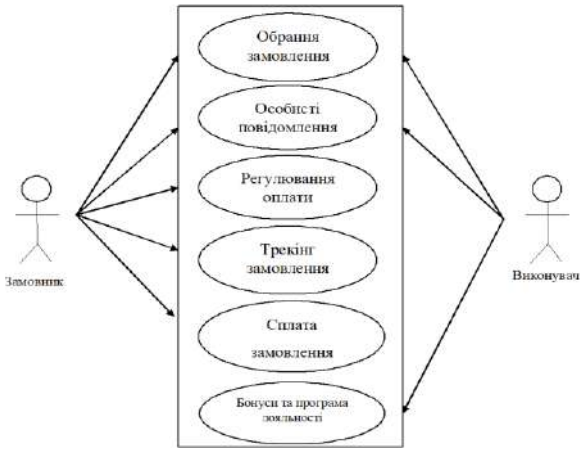


Рис. 1. Use-case діаграма системи

Висновки. У розробці мобільного веб-додатку одними з найефективніших засобів реалізації є JavaScript та Kotlin для розробки візуальної частини, Java – для роботи із серверною частиною та PostgreSQL і MongoDB для роботи зберігання та обробки даних, які обрано в рамках розробки проекту програмного застосування.

Інформаційні джерела

1. Back.F.Back-end development of mobile application for the collection of dietary data. – Umea: Department of Applied Physics and Electronics, 2012. – 96 с.

УДК 004

АНАЛІЗ СПЕЦИФІКИ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ

Рудніченко М.Д., Гежа Н.І., Тищенко С.Є., Шибаєв Д.С.
Одеський національний політехнічний університет, м. Одеса

У роботі наведено результати огляду та аналізу ключових аспектів та складнощів здійснення інтелектуального аналізу даних.

Ключові слова: *штучний інтелект, машинне навчання, інтелектуальний аналіз даних*

The paper presents the results of a review and analysis of key aspects and difficulties of data mining.

Keywords: *artificial intelligence, machine learning, data mining*

Останнім часом процедура вилучення знань з даних застосовується для багатьох цілей, наприклад, для створення рекомендацій на підставі ситуації, прогнозування, а також виявлення аномалій. До результатів аналізу застосовуються такі вимоги, як достовірність, здатність до інтерпретації і корисність. Даний аналіз набув широкого поширення в сфері бізнесу (наприклад, для передбачення кількості покупців, розбиття покупців на групи за інтересами), фінансах (визначення фальшивих транзакцій, оцінка надійності клієнта банку), науці, медицині (постанова діагнозу, прогнозування стану пацієнта і рекомендація ходу лікування), а також в інших областях [1].

У зв'язку з тим, що при аналізі великої кількості даних експерт неспроможний знайти всі можливі залежності, в даній сфері широке застосування отримала наука про машинне навчання (МН) [2]. Ця наука полягає в

створенні алгоритмів (також названих моделями), здатних навчатися залежностям у великих наборах даних і моделювати їх. Дані алгоритми навчають на тренувальній вибірці з даних, перевіряють на тестовій вибірці й застосовують для моделювання взаємозв'язків на практиці. Прикладами деяких із завдань, для яких використовують моделі МН, є класифікація, регресія, кластеризація, і зменшення просторовості. Існує велика кількість моделей МН, і, згідно NFL теоремі, не існує алгоритму, що перевершує всі інші в усіх задачах. Причини цього в тому, що, в залежності від характеристик задачі і вхідних даних, моделі відрізняються за якістю результату, і на одній задачі алгоритми досягають різних результатів в різних метриках. Також, алгоритми мають різні обчислювальні і просторові труднощі. Отже, так як для деяких завдань може бути критично важлива та чи інша метрика (наприклад, алгоритм повинен завжди класифікувати хвору людину як хворого, але допустимо, що здорового вважатиме за хворого), то для знаходження найкращого для поставленого завдання алгоритму, необхідно виконувати порівняння якості і часу роботи різних моделей.

Висновки. Чим більше обсяг даних, тим більше часу і пам'яті необхідно приділити порівнянню алгоритмів. Також, чим більше різних алгоритмів або їх варіацій бере участь в порівнянні, тим більша необхідна кількість обчислювальних ресурсів. Дані умови створюють проблему, яка полягає в великих витратах часу і пам'яті, необхідних для знаходження найбільш відповідної моделі. Для вирішення цієї проблеми доцільним є розробка проекту рекомендаційною системи, що дозволить за короткий час отримати перелік рейтинг алгоритмів з урахуванням поставленої задачі та вхідних даних.

Інформаційні джерела

1. Рудніченко М.Д. Розробка концепції модуля інтелектуального аналізу великих обсягів даних в транспортних системах на базі методів машинного навчання / М.Д. Рудніченко, В.В. Вичужанін, Н.О. Шибаєва, Д.С. Шибаєв, Н.І. Гежа // Міжвузівський збірник наукових статей (з міжнародною участю) «Актуальні проблеми автотранспортного комплексу» [відп. ред. О.М. Батищева]. - Самара: Самар. держ. техн. ун-т, 2020. - С. 85-92.

2.Рудніченко М. Застосування методів машинного навчання для автоматизації процесів класифікації масивів текстових даних великого обсягу / М. Рудніченко, В. Вичужанін, Н. Шибаєва, Д. Шибаєв, Т. Отрадская, І. Петров // Інформаційні управляючі системи та технології. Проблеми і рішення .: монографія. - Одеса, 2019. - С.31-46.

УДК 004

АНАЛІЗ РИНКУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ГАЛУЗІ НАДАННЯ ПОСЛУГ

Шибаєва Н.О., Березоруцька О.В., Краковський В.О., Рокитенко В.М.
Одеський національний політехнічний університет, м. Одеса

Метою даної роботи є аналіз ринку програмного забезпечення в галузі надання послуг. Проаналізовано роботу чотирьох діючих програм і нашого проєкту, виявлено їх переваги та недоліки. Порівняльний аналіз проводився за такими критеріями: наявність мобільного додатку, можливість "безпечної" оплати замовлення, використання геолокації для визначення місця розташування клієнтів і виконавців тощо.

Ключові слова: *ринок надання послуг, сервіс замовлення послуг, порівняльна характеристика, "безпечна" оплата.*

The purpose of the work is to analyze the software market in the field of services. The work of four existing applications and our project has been analyzed, their advantages and disadvantages have been revealed. The comparative analysis was carried out according to the following criteria: the presence of a mobile application, the possibility of "secure" payment for orders, the use of geolocation to determine the location of customers and performers, etc.

Keywords: *service rendering market, application of ordering services, comparative characteristics, "safe" payment.*

Часто в житті людей виникають ситуації, під час яких необхідно викликати фахівця для надання деяких послуг (клінінгових, кур'єрських, ремонтних, ділових тощо).

Тоді доводиться розглядати безліч оголошень з різних джерел для вирішення проблеми, що виникла.

Концепція нашого додатку "BeWorky" полягає в тому, що він містить в собі інформацію про розташування найближчих фахівців, що готові виконати відповідну роботу.

Не завжди певна послуга присутня на ринку якоїсь території, вона має локальну специфіку. Ця програма вирішує проблему ускладненого пошуку потрібного працівника і робить життя споживача зручнішим.

У сучасному світі час є найціннішим ресурсом, і програмне забезпечення, яке дозволяє зменшити його витрати, сьогодні має велику актуальность.

На ринку додатків неодноразово робилися спроби реалізувати таку ідею, але у кожного з уже представлених на ринку продуктів є як переваги, так і недоліки. Ми ставимо за мету реалізацію максимально зручного додатку, який має свої особливості і виправляє більшість недоліків в аналогах. Для досягнення поставленої мети необхідно розглянути і проаналізувати ринок праці і програмного забезпечення, виділивши основні моменти, і зробити відповідні висновки.

Ринок додатків, які надають сервіс замовлення послуг (в будь-який час і в будь-якому місці), не великий. Основними аналогами є такі мобільні додатки, як Help&Job і HelpFi. Також серед web-аналогів можна виділити сервіси YouDo і "Кабанчик". Критерії, за якими буде проводитися порівняльна характеристика:

– наявність веб-сайту;

– наявність мобільного додатку (а також наявність єдиного додатку з поділом на замовників і виконавців або двох окремих для кожної категорії):

– єдиний додаток легше реалізувати і в подальшому підтримувати;

– два додатки - безпечніше;

– багатомовність сервісу;

– можливість застрахувати замовлення;

– можливість "безпечної" оплати (з резервуванням коштів замовника на транзитному рахунку в банку, поки робота буде в процесі виконання);

– перегляд найближчих до споживача виконавців за допомогою геолокації;

– та ін. [1, 2].

Повну порівняльну характеристику приведено в таблиці 1.

Таблиця 1.

Порівняльна характеристика

Назва сервісу	***Help&Job***	***HelpFi***	***YouDo***	***Кабанчик***	***BeWorky***
веб-сайт	-	-	+	+	+
мобільний додаток (1 чи 2)	+ (1)	+(1)	+(1)	+(2)	+ (1)
багатомовність сервісу	+ (рос., укр.)	-	-	-	+ (рос., укр., англ.)
можливість застрахувати замовлення	+	-	+	+	+
можливість “безпечної” оплати	+	-	+	+	+
перегляд найближчих до користувача виконавців за допомогою геолокації	+	+	+	-	+
вибір користувачем радіуса дії	+	+	+	-	+
пошук користувачем замовлень поблизу	+	+	+	-	+
система рекомендацій замовлень виконавцям за геопозицією	+	-	-	-	+
гейміфікація	+-	-	+	-	+
рейтинг виконавців і замовників	-	-	+	-	+

перевірка професійної інформації виконавців (дипломи, сертифікати, рекомендаційні листи)	-	-	-	-	+
зручний інтерфейс	+	-	+	+	+

Існують певні плюси нашого додатку, які було важко перевірити у аналогів, так як довелося б створювати фіктивні замовлення, а це могло б перешкодити роботі цих додатків. Наприклад, можливість нарахування авансу виконавцю і заохочень після завершення замовлення [3].

Зручний у використанні додаток, що включає в себе всі найнеобхідніші функції для ПЗ в галузі надання послуг, є сьогодні необхідним і затребуваним. Це зробить нашу роботу конкурентоспроможною.

Інформаційні джерела

1. Основные критерии качества приложений. - [Електронний ресурс]. - Режим доступу: https://developer.android.com/docs/quality-guidelines/core-app-quality?hl=ru

2. Smale, Thomas. How to Value a Mobile App? - [Електронний ресурс]. - Режим доступу: https://buildfire.com/mobile-app-value/

3. Ricketts, Ben. How To Value An App. - [Електронний ресурс]. - Режим доступу: https://sellmysite.com/how-to-value-an-app/

СТРУКТУРА CMS СИСТЕМ

Прохоренко В. А., Заволодько Г. Е.
Кафедра систем інформації Харківський національний університет «ХПІ», м. Харків

У даній статті проведено аналіз структури систем керування вмістом. Порівняно три найбільш популярні CMS та виділено найбільш оптимізоване програмне забезпечення. Всі розглянуті системи мають відкритий вихідний код та є повністю безкоштовними.

Ключові слова: *система керування вмістом, контент, система, CMS, структура.*

This paper analyzes the structure of the content management system. All systems are free and have open source code.

Keywords: *content management system, CMS, structure.*

Сучасні системи керування контентом мають відповідати наступним критеріям, щоб бути конкурентоспроможними:

1. Швидке та ефективне маніпулювання інформацією. Програмне забезпечення має надавати можливість делегувати наповнення сайту редактору, web-мастеру або іншому співробітнику без попереднього формування технічного завдання.

2. Зменшення вартості підтримки системи. CMS повинно надавати власнику простий та зрозумілий інструмент для встановлення додаткових функційних можливстей та додавання, редагування або видалення контенту.

3. Розмежування прав та доступу. Кожен користувач повинен мати власну роль, яка дозволяє йому виконувати тільки певний спектр задач, не впливаючи на роботу інших компонентів [1].

4. SEO-оптимізація. Просування сайту у пошукових системах за змістовими критеріями – це одна з головних задач власника сайту. Тому у вебресурсі повинні бути інструменти для кастомізації метаданих та налаштування URL-адреси.

5. Можливість змінювати дизайн, не впливаючи на роботу функціональних елементів.

Що стосується архітектури системи керування контентом, то популярні сьогодні варіанти (WordPress, OpenCart та Joomla) схожі за своєю внутрішньою структурою. Вони створені з використанням розподілених сервісів. Завдяки цьому CMS стає гнучкою, простою для взаємодії, як для користувача, так і для розробника, та надає можливість розширювати спектр дій одного сервісу за допомогою встановлення іншого [2].

WordPress - це повністю безкоштовна система керування вмістом з відкритим вихідним кодом з вбудованою системою керування плагінами та темами. На сьогоднішній день вона є найбільш популярною у світі. WordPress реалізована на платформі PHP, у якості бази даних використовується MySQL [3].

У даному програмному забезпеченню є вбудована система керування плагінами та темами. До того ж його розробники Ryan Boren, Mark Jaquith, Matt Mullenweg, Andrew Ozz, Peter Westwood дозволяють розширювати функціональне наповнення за допомогою своїх модулів.

Адміністративна панель WordPress має доволі простий та інтуїтивно зрозумілий інтерфейс. Тому навіть користувач без технічних навичок розбереться, як створити сторінку, пост, рубрику або як встановити плагін.

Цільовою аудиторією даної системи керування вмістом можна вважати власників сайтів-візиток, блогів та корпоративних сайтів. Також WordPress використовують підприємці, бізнесом котрих є невеликі та середні інтернет-магазини.

OpenCart представляє собою безкоштовну систему керування вмістом. Вона розроблена Дениэлем Керром та Джоном Хелфишом для створення інтернет-магазинів. У якості платформи використана мова програмування PHP, система керування базою даних (СКБД) – MySQL [4].

За швидкістю OpenCart значно повільніший, ніж WordPress, більше ніж у 6 разів.

Joomla займає 11% ринку в странах СНГ. Також вона входить до п'ятірки лідируючих систем для створення сайтів у світі. Вона створена командою незалежною командою розробників із CMS Mambo і розповсюджується повністю безкоштовно [5].

Написана Joomla із використанням об'єктно-орієнтованої технології та за допомогою мови програмування PHP, СКБД – MySQL.

За зручністю користування Joomla є аналогом WordPress. Встановлення та налаштування системи займає не більше 5 хвилин. До того ж, інтерфейс панелі керування досить простий і дозволяє обрати комфортну для роботи мову (російську, англійську або українську).

Найбільш швидкою, зручною та універсальною системою керування контентом є WordPress. Ця CMS відрізняється більш продуманою архітектурою, що відобразилося на продуктивності, інтуїтивно зрозумілою панеллю адміністратора і в підсумковому аналізі має більше переваг над своїми аналогами.

Сьогодні рішення для створення сучасних веб-сторінок та веб-ресурсів базуються на активній інтеграції різноманітних патернів, підходів, засобів розробки та інструментів. За останні три десятиліття сайти перетворилися із звичайного способу передачі гіпертексту на багатокомпонентне програмне забезпечення, яке обслуговує тисячі користувачів одночасно. Для зручного маніпулювання даними у такому випадку використовуються системи керування контентом.

Інформаційні джерела

1. Преимущества и недостатки сайта на CMS [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://sdvv.ru/articles/testovyy-razdel/preimushchestva-i-nedostatki-sayta-na-cms.

2. Иванов А. В. Архитектура и программная инфраструктура систем управления контентом и модели описания их функционирования : дис. канд. : 05.13.11 / Иванов Алексей Владимирович – Москва, 2018. – 160 с.

3. WordPress [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://wordpress.com/

4. OpenCart [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://opencart.ua/

5. Joomla [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.joomla.org/

УДК 004.438

REST-СЕРВЕР ІНТЕРНЕТ-МАГАЗИНУ НА БАЗІ ФРЕЙМВОРКУ RUBY ON RAILS

Созанський М., Пархоменко В.-П., Головатий Р.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі проведений узагальнений аналіз основних переваг розробки інтернет-магазину за допомогою фреймворку Ruby on Rails.
Ключові слова: *REST, Ruby on Rails.*

The paper presents a generalized analysis of the main advantages of developing an online store using the Ruby on Rails framework.
Keywords: *REST, Ruby on Rails.*

RESTful API − це інтерфейс прикладної програми (API), який використовує HTTP-запити GET, PUT, POST та DELETE даних.

API для веб-сайту − це код, який дозволяє двом програмним програмам взаємодіяти між собою. API визначає належний спосіб розробнику написати програму, яка вимагає надання послуг з операційної системи або іншої програми.

Технологія REST, як правило, віддається перевазі більш надійній технології простого протоколу доступу до об'єктів (SOAP), оскільки REST використовує меншу пропускну здатність, що робить її більш придатною для ефективного використання інтернету.

Об'єктно-орієнтована − це означає, що мова використовує об'єкти в своїх процесах, які дозволяють або окремі частини програми або всієї програми в цілому, для повторного використання в інших проектах. Крім того, об'єктно-орієнтоване програмування забезпечує чітку модульну структуру проектів програміста.

Ruby має репутацію дуже зручної для інновацій − вона не тільки має безліч функцій, які можна вибрати за замовчуванням, але також легко приймає більшість нових реалізацій та оновлень.

За допомогою менеджерів пакетів або сторонніх інструментів є безліч варіантів встановлення та управління Ruby.

У наш час магазини трансформуються та переходять в онлайн. За допомогою онлайн-магазинів знайти вподобану річ набагато простіше, ніж шукати її в звичайних магазинах. Можна вибрати і купити потрібний товар сидячи вдома, а сам процес займає мінімум часу. Сьогодні онлайн магазини є невід'ємною частиною електронної комерції, яка відкриває широкі

можливості для тих, хто зацікавлений в успішному розвитку бізнесу. Тому в перспективі очікується тільки зростання затребуваності подібних систем.

Ruby on Rails, також відомий як RoR, або просто «Rails» – це структура з відкритим кодом, побудована на мові Ruby, яка може використовуватися з декількома іншими мовами, такими як XML та JavaScript. Фреймворк був випущений в грудні 2005 року. Хоча в галузі існує безліч інших досить популярних і широко використовуваних технологій, ROR залишається популярним серед розробників у всіх областях.

Інформаційні джерела

1. Борзов Ю. Особливості застосування комп'ютерного моделювання для покращення навчального процесу / Ю. Борзов, Р. Головатий, Я. Магеровський. // Інформаційні технології розвитку змісту освіти. – 2019. – С. 80–81.

2. Зачко О.Б., Головатий О.Р. Мультиагентна модель управління безпекою при плануванні проектів створення об'єктів з масовим перебуванням людей. Стратегічне управління, управління портфелями, програмами та проектами. 2017. № 2 (1224). С. 46–51.

3. Лущ В.І. Аналіз тренувальних комплексів для підготовки газодимозахисників країн європейського союзу / Лущ В.І., Лущ І.В., Пархоменко В.О., Шпак Р.М. // Збірник наукових праць: «Пожежна безпека» Львів. 2015. – №27

Напрям 8

МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.7.056.5

ПРОЄКТУВАННЯ ТА РОЗРОБЛЕННЯ ВІДКРИТИХ WIFI-МЕРЕЖ З ФУНКЦІЄЮ ЗБИРАННЯ ІНФОРМАЦІЇ ПРО ПРИСТРОЇ

Бурнашов С., Ящук В.
Львівський державний університет безпеки життєдіяльності, м. Львів

Розкриваються проблеми поширення кіберзлочинності з використанням відкритих WiFi-мереж. Актуалізується питання ідентифікації пристроїв, які використовують користувачі відкритих WiFi-мереж. Наведено пропозиції щодо використання WiFi-маршрутизаторів та технології цифрового відбитка пристрою для збирання інформації про пристрої які отримують доступ до відкритих WiFi-мереж та їх подальшу ідентифікацію.

Ключові слова: *відкрита WiFi-мережа, ідентифікація пристроїв, цифровий відбиток пристрою.*

Problems are being raised about the expansion of cyber-breakdowns from victories to critical WiFi networks. Up-to-date food identification of annexes, such as corystoids on a WiFi net. Proposals have been made to show Wi-Fi routers and digital video bit technology to an attachment for collecting information about attachments, which will provide access to a Wi-Fi network and a further identification.

Key words: *WiFi-network, attachment identification, cross-browser fingerprinting.*

Сьогодні стрімкий розвиток інформаційних технологій спричинив існування великої кількості WiFi-мереж, доступ до яких відкритий або надається приватними організаціями в якості сервісу. Це дає підгрунтя для скоєння кіберзлочинів через отримання доступу до мережі інтернет та уникнення повної або часткової ідентифікації пристроїв, які використовуються. Неможливість ідентифікації полягає в тому, що WiFi-маршрутизатор не передає дані про мережеве ім'я та MAC-адресу підключеного пристрою. За таких умов можливо лише визначити фізичне розташування маршрутизатору, зареєстроване за IP-адресою, яка надана інтернет-провайдером. З метою забезпечення ідентифікації пристроїв пропонується створення відкритих WiFi-мереж з використанням модифікованих маршрутизаторів, які надають доступ до мережі інтернет лише після визначення цифрового відби-

тку пристрою, відправлення його на сервер для оброблення та подальшого зберігання. Відтак, розглядається можливість заміни звичайних маршрутизаторів, які надаються приватними організаціями в якості сервісу, на модифіковані. Наявності цифрового відбитка пристрою надає можливість визначати пристрої які знаходяться у розшуку, або власникам яких можна оголосити підозру в незаконній діяльності в мережі інтернет.

Основні дані, які можна отримати з маршрутизатора про його клієнта: ім'я пристрою, локальна адреса, MAC-адреса, час підключення. Дані, які можна отримати через WEB-браузер за допомогою Java Script: інформація про плагіни, версія браузера та операційної системи, роздільна здатність дисплея, шрифти, кількість ядер процесора тощо. Існує складніша, але більш точна технологія зняття цифрового відбитку пристрою - cross-browser fingerprinting - яка використовує характеристики комп'ютера, сформовані незалежно від версії браузера при обробленні та рендерингу графіки.

Принцип роботи модифікованого WiFi-маршрутизатора полягає в перенаправленні запитів мережі 172.24.1.1/24 отриманих на WiFi-пристрій з ім'ям wlan0 за допомогою правил доданих в утиліту Iptables на стартову сторінку за локальною IP-адресою172.24.1.1 порт 80 вбудовану в маршрутизатор: iptables -t nat -A PREROUTING -i wlan0 -p tcp -s 172.24.1.1/24 -j DNAT --to 172.24.1.1:80, сторінка містить в собі Java Script - код для зчитування відбитку та публічну оферту згідно діючого законодавства України, де користувач погоджується з передачею цифрового відбитка пристрою для оброблення та зберігання на сервері. Базові данні про пристрій користувача можна отримати з ARP-таблиці за допомогою скрипта командного інтерпретатора Bourne SHell (sh) підключеного до коду на Java Script: "script.sh", на який як аргумент передається IP-адреса користувача визначена при підключені до WEB-сторінки за локальною IP-адресою 172.24.1.1: "sh script.sh ip-адреса", а як значення повертається MAC-адреса користувача: arp 172.24.1.100 -n | grep 172.24.1.100 | tr -s ' ' | cut -d ' ' -f 3. Та записуються в зміні Java Script коду: var ip_ = 172.24.1.100, var mac_ = 00:00:00:00:00:00, var time_ = час (програма ntpd) і очікує на передачу до сервера бази даних (рис. 1).

Після згоди куристувача з умовами публічної оферти, програма додає нове правило до утиліти Iptables, яке дозволяє пристрою, з визначеною MAC-адресою, доступ до мережі інтернет на визначений час, після закінчення якого процедура повторюється: iptables -t nat --insert PREROUTING -s 172.24.1.100 -j ACCEPT, iptables -t nat -D PREROUTING -s 172.24.1.100 -j ACCEPT " | at -m now + 60 minutes. Водночас передає цифровий відбиток пристрою на сервер бази даних.

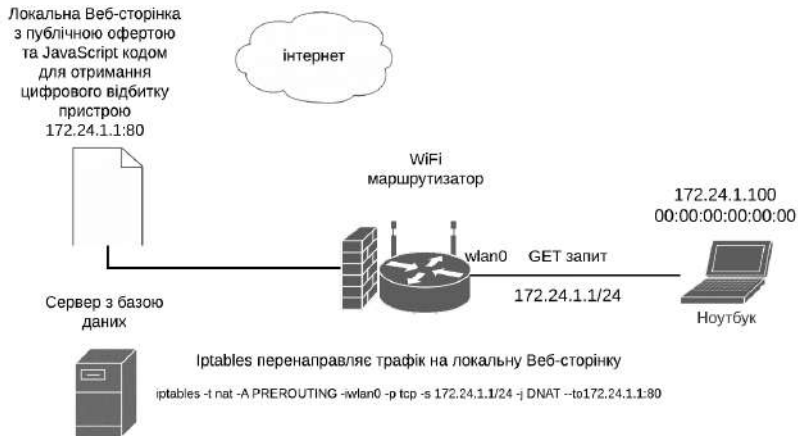


Рис. 1. Структурна схема перенаправлення запитів

Рис. 2. Структурна схема дозволу доступу до мережі інтернет

Таким чином, запропонована технологія надає можливість отримання цифрових відбитків пристроїв користувачів WiFi-мереж, з яких отримано доступ до мережі інтернет та формування бази даних з метою моніторингу та накопичення інформації.

Інформаційні джерела

1. Iptables Tutorial [Електронний ресурс]. – Режим доступу: https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html

2. Bash Reference Manual [Електронний ресурс]. – Режим доступу: https://www.gnu.org/software/bash/manual/html_node/index.html

УДК 004.057.4

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ВИКОРИСТАННЯ ПРОТОКОЛУ IPV6

Іванчук Б.І., Бурак Н.Є.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі здійснено огляд нової версії протоколу мережевого рівня IPv6. Проведено короткий аналіз його призначення ,особливостей роботи в мережі та історії розробки.
Ключові слова: *протокол, адресація, взаємодія, мережа.*

The paper reviews the new version of the IPv6 network layer protocol. A brief analysis of its purpose, features of networking and history of development.
Keywords: *protocol, addressing, interaction, network.*

Сучасна взаємодія через середовище комп'ютерних мереж передбачає використання певних, наперед заданих, правил узгодження як апаратного забезпечення так і програмного. Таким набором правил є – протоколи міжмережної взаємодії.

При реалізації надсилання та отримання повідомлень та пакетів даних застосовують два найпопулярніші протоколи – TCP (Transport Communication Protocol) – протокол передачі інформації з підтвердження та гаратнтією отримання даних; та UDP (User Datagram Protocol) – протокол передачі датаграм, один з найпростіших протоколів транспортного рівня моделі OSI, котрий виконує обмін повідомленнями без підтвердження та гарантії доставки. Проте, одного тільки протоколу для реалізації обміну даних не достатньо. Необхідно також знати мережеву адресу джерела та одержування цього процесу. За виконання даної функції відповідає протокол IP (Internet Protocol) – протокол мережевого рівня, який використовується для ідентифікації хостів у мережі. Сьогодні відомі дві версії даного протоколу IPv4 та IPv6.

На початку 2012 року, у зв'язку із стрімким ростом кількості пристроїв, які підключаються до мережі і, відповідно, потребують присвоєння ідентифікатора з адресного простору протоколу IP, діапазон допустимих адрес приблизився до свого максимуму. Ще в кінці 90-х років минулого століття експерти були впевнені, що адресації цього протоколу має вистачити, принаймні, ще років на 30. Але такого стрімкого розвитку мережевих ресурсів передбачити не міг ніхто, ще призвело до виникнення загрозу неможливості розвитку IT сфери. Тому почалося впровадження нового джерела розвитку мережевої інфраструктури. Цим джерелом послужив протокол IPv6. По суті, протокол IP шостої версії є повноцінною заміною IPv4, що належить до сімейства протоколів TCP / IP.

IPv6 (англ. Internet Protocol version 6) — нова версія IP-протоколу — IP версії 6. Розробку протоколу IPv6 почали в 1992 році, а з 2003 р. його підтримує більшість телекомунікаційного обладнання корпоративного рівня. IPv6 – було розроблено з урахуванням того, що глобальна мережа постійно і дуже великими темпами зростає.

Найбільш суттєва різниця між IPv4 та IPv6 полягає в тому, що раніше на інтернет-адресу виділяли 4 байти (32 біти), що відповідає стандартній на сьогодні чотириблоковій адресі IP, а протокол IPv6 виділяє на адресу 16 байтів (128 бітів) (Рис. 1.), яка містить вісім рядків, кожен з яких складається з чотирьох цифр, що розділяються двокрапкою. Це відповідає 340 секстильйонам адрес (3,4x1038) або по 5x1028 адрес на кожну людину. Типова адреса виглядає приблизно так:

2018:0ab6:84a2:0000:0000:7a2b:0271:7435.

Після закінчення IPv4 діапазону, паралельне використання протоколів, дасть можливість повного впровадження протоколу, за допомогою поступового збільшення трафіку в IPv6 мережах. Але при цьому, повне виведення IPv4 діапазону буде доступний ще не скоро, адже існує величезна кількість пристроїв, що не підтримують інноваційну технологію.

Рис. 1. Кількість унікальних адрес протоколів IPv4 та IPv6

Протокол четвертої версії підтримував два варіанти реалізації для користувача IP-адрес:

– статистичний адреса, який був незмінним ідентифікатором;

– динамічний, змінювався при кожному новому підключенні до мережі.

На відміну від IPv4, IPv6 підтримує тільки варіант статичної адресації. Таке рішення було обумовлено тим, що, в перспективі кожному пристрою в підмережі будь-якого рівня буде доступний свій унікальний ідентифікатор – IP-адреса. Відповідно до стандарту нового протоколу, усі адреси розділені на три категорії:

1. Unicast. Стандартні адреси з одиничною прив'язкою до мережевого інтерфейсу.

2. Anycast. Адреси, передбачені для груп мережевих оболонок, і призначаються тільки маршрутизаторам. Такі адреси розраховані на створення внутрішніх мережевих груп з кількох комп'ютерів.

3. Multicast. Адреси для групового обміну даними, в основному виділяються регіональним серверам.

У порівнянні протоколів IPv4 та IPv6, виділяють наступні переваги 6-ї версії:

– більша кількість доступних адрес;

– вища швидкість;

– авто-конфігурація;

– підвищена ефективність маршрутизації;

– надійний рівень безпеки;

– вищий показник переходів.

Незважаючи на досконаліть протоколу IPv6, у ньому все таки присутні деякі недоліки, зокрема:

– протокол IPv4 є більш популярним;

– протоколи IPv6 та IPv4 не є безпосередньо сумісними і вимагають використання сервера;

– VPN-служби не реагують на потребу оновлення серверів для підтримки протоколу IPv6.

Отже, завдяки своїм перевагам, більшість сучасних мережевих інженерів, дата-центрів, технологічних компаній та мобільних операторів переходять на використання протоколу IPv6 оскільки він є пріоритетним вибором серед професіоналів.

Інформаційні джерела

1. Робачевский А. IPv6: вчера, сегодня, завтра [Электронный ресурс] / А. Робачевский. – Режим доступа к ресурсу: http://www.ripn.net/articles/IPv6_today/.

2. Рубан И. В. Взаимодействие протоколов IPv4 и IPv6 в телекоммуникационных сетях / И.В. Рубан, И.В. Карпова // Системи обробки інформації. – 2012. – № 2(100). – С. 208-210.

3. Cisco IPv6 Lab: IPv6 Deployment.
URL: http://6lab.cisco.com/stats/index.php

4. Google statistics IPv6 Режим доступа:
http://www.google.com/intl/en/ipv6/statistics.html

5. Главацкий С.П. Исследование количества свободных IP адресов V4 / С.П. Главацкий // Сучасна наука: теорія і практика : матеріали міжнар. наук. практ. конф. 27-28 листопада 2015 р., м. Запоріжжя / ГО «Інститут освітньої та молодіжної політики»; Науково-навчальний центр прикладної інформатики НАН України. – Запоріжжя : ГО «ІОМП», 2015. – С. 147–149.

СИСТЕМА ОПЕРАТИВНО-ДИСПЕТЧЕРСЬКОГО УПРАВЛІННЯ

Олійник А.І., Леськів С.В., Малець І.О.
Львівський державний університет безпеки життєдіяльності м. Львів

У роботі проведено аналіз роботи системи оперативно-диспетчерського управління, її будова та функціонування в Україні.

Ключові слова: *ДСНС, ліквідація, СОДУ, надзвичайна ситуація, ОКЦ, диспетчер.*

The analysis of the operational and dispatching management system, its structure and functioning in Ukraine is carried out in the work.

Key words: *SES, liquidation, SODU, emergency situation, OCC, dispatcher.*

Система оперативно-диспетчерського управління є територіальною підсистемою Урядової інформаційно-аналітичної системи ліквідації надзвичайних ситуацій (УІАНС).

Метою провадження СОДУ є максимальна автоматизація диспетчерських функцій, скорочення термінів обробки викликів та висилки техніки, що є вирішальним фактором при ліквідації НС, рятуванні людей.

В останні роки зафіксована тенденція до зростання кількості пожеж в Україні. З ростом кількості пожеж зростає відповідно і кількість викликів. Враховуючи це, збільшилося навантаження на чергових диспетчерів оперативно-диспетчерської служби оперативно-координаційного центру тому, що фактично збільшився обсяг оброблюваної ними інформації. Негативним наслідком цього явища згідно досліджень, може бути збільшення імовірності виконання помилкових дій черговими диспетчерами, що може призвести до зростання часу оброки повідомлень та зростання часу вільного розвитку пожежі.

Отже, основним призначенням систем є автоматизація оперативно-диспетчерського управління ПРП та забезпечення інформаційної підтримки в процесі:

1) оперативної висилки сил та засобів на виклик;

2) прийняття рішень при управлінні ПРП під час проведення ними оперативних дій під час ліквідації НС;

3) збору оперативної інформації про стан ПРА;

4) ведення баз даних і формування інформаційних і статистичних звітів.

Будова та функціонування СОДУ

В ОДС ОКЦ обладнані робочі місця, на кожному з яких встановлена двомоніторна система на базі персонального комп'ютера та системного апарату відомчої автоматичної телефонної станції (АТС). Один з моніторів призначений для роботи з оперативною задачею, а другий для відображення картографічних даних.

Дзвінок від абонента приймається вільним черговим диспетчером, номер телефону визначається відомчою АТС і передається автоматизовано

через програмний інтерфейс в програмно-апаратний комплекс «СОДУ». За визначеним номером телефону та при наявності інформації в базі даних визначається місце розташування стаціонарних абонентів телефонної мережі загального користування.

Диспетчер:

– вводить дані (зі слів заявника) про адресу НС та її особливості;

– реєструє подію, після чого система пропонує на виїзд перелік сил та засобів для ліквідації НС з врахуванням мінімального часу прибуття;

– підтверджує запропонований варіант, або при необхідності вносить зміни в перелік техніки, що висилається на виклик та передає команду на виїзд у відповідні ПРП.

Надалі в ці підрозділи надходить бланк дорожнього листа (в якому також відображена карта з маршрутом прямування та переліком найближчих вододжерел, які знаходяться поблизу місця виклику) та вмикається сигнал «Тривога», що супроводжується автоматичним озвученням синтезатором мови текстової інформації, яка записана в полі «зміст повідомлення».

Інформація, яка надходить з місця події за допомогою радіо та телефонного зв'язку в тому числі про прибуття оперативних розрахунків, розвиток, локалізацію та ліквідацію НС вводиться диспетчером ПРП в поле «оперативна задача».

Система надає також змогу формувати зведені стройові записки по особовому складу гарнізону, ПРА з відображенням в реальному часі інформації про стан техніки, а також сформувати добове зведення та інші звіти згідно табелю донесень.

Недоліком даної системи є формування маршруту прямування ПРП на місце виклику без врахування дорожніх заторів, що є актуальною проблемою у великих містах.

Практика використання автоматизованої системи СОДУ у структурних підрозділах МНС України дає змогу зробити такі висновки.

1. Інформатизація такої галузі діяльності, як забезпечення безпеки людини, приводить до істотної зміни та удосконалення методів збирання, опрацювання, зберігання інформації та дає змогу проводити такий її аналіз, який є принципово неможливим при використанні традиційних методів.

2. Застосування комп'ютерних систем у процесі підготовки та прийняття управлінських рішень викликає істотні зміни як у сутності змістової характеристики його організаційно-правових елементів, так і в правовому регулюванні суспільних відносин, що виникають при цьому.

Багато елементів процесу підготовки та прийняття рішень (зокрема, правовий стан та функції учасників даного виду управлінської діяльності, характер та зміст розв'язуваних ними управлінських задач, засоби збирання та опрацювання управлінської інформації тощо) істотно модифікуються.

3. В умовах функціонування СОДУ істотно збільшується склад "учасників" в процесі прийняття управлінських рішень. Змінюється технологія та засоби їх реалізації. Саме тому ці зміни потребують відповідної системи правової регламентації для забезпечення їх законності.

У вимогах, що ставляться до підготовки, прийняття та організації виконання управлінських рішень, доцільно закріпити положення щодо:

а) системного аналізу управлінських ситуацій, змістовного і всебічного вивчення проблем, які потрібно вирішити;

б) організаційних форм і методів на різних етапах формування управлінських рішень: підготовки, прийняття та забезпечення реалізації

в)форм залучення кваліфікованих фахівців і технічних працівників до участі у формуванні рішень;

г) встановлення обов'язкових правил документування рішень і надання їм юридичного статусу;

д) правового регулювання прийняття усних рішень уповноваженим на те суб'єктом тощо.

Наведена вище інформація свідчить про те, що процес прийняття управлінських рішень в умовах використання СОДУ повинен базуватись на чітко оформленій системі правових приписів, які визначають цілі діяльності відповідно до заздалегідь встановлених критеріїв та засобів їх досягнення.

Таким чином, дослідження особливостей впровадження нових комп’ютерних інформаційних технологій в органах управління МНС України свідчать про те, що кардинальна проблема удосконалення їх організаційної структури та здійснюваних там процесів управління зводиться в основному до таких чинників: підвищення місткості та пропускної здатності приймачів інформації; оптимізації каналів зв'язку між елементами системи і системою та зовнішнім середовищем.

Отже, інформатизація структурних підрозділів МНС України вимагає широкого використання системного підходу при розмежуванні компетенції між органами управління, більш чіткого її визначення, виявлення специфіки виконання однотипних управлінських функцій на тому чи іншому рівні управлінської системи та стандартизації термінології через закріплення її у відповідних юридичних документах.

Інформаційні джерела

1. Авер'янов В.Б. Державне управління в Україні : навч. посібн. / В.Б. Авер'янов. - К.Вид-во "Юрінком-Інтер", 1998. - 432 с.

2. Сікора Л.С. Системологія прийняття рішень на управління в складних технологічних структурах / Л.С. Сікора. - Львів : Каменяр, 1998. - 453 с.

3. Моргун ОМ. Комп'ютерна. система оптимізації вибору маршрутів слідування аварійно-рятувальної техніки / О.М. Моргун, Л.О. Моргун // Пожежна безпека: теорія і практика

СИСТЕМА 112

Частило А.О., Жолубак Л.І., Малець І.О.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі проведено аналіз роботи системи 112 та її впровадження в Україні.
Ключові слова: *система 112, екстрена допомога, надзвичайна ситуація.*

The paper analyzes the operation of the 112 system and its implementation in Ukraine.
Key words: *112 system, emergency aid, emergency situation.*

Вперше питання про створення такої служби постало ще у 1976 році, коли Європейська конференція адміністрацій пошти та телекомунікацій запропонувала використовувати номер 112 як єдиний загальноєвропейський телефонний номер екстреного виклику. Але минуло 15 років, перш ніж Рада Європи ухвалила відповідне рішення, і до 1996 року безкоштовна Система 112 почала діяти у всіх країнах-членах ЄС.

112 — чергово-диспетчерська система екстреної допомоги населенню за єдиним безкоштовним телефонним номером виклику екстрених служб 112, який запроваджено в усіх країнах-членах Європейського Союзу. Унікальність номеру 112 у тому, що його можна набрати з будь-якого телефонного апарата навіть мобільного без SIM-карти, без введення PIN-коду та при заблокованій клавіатурі.

Головна мета створення системи екстреної допомоги населенню за єдиним телефонним номером 112 (Система 112) в Україні – забезпечити дотримання конституційних прав громадян на особисту безпеку, охорону здоров'я та майна, надати державні послуги європейського рівня, забезпечити єдиний номер виклику «112» для всіх екстрених ситуацій, безкоштовне з'єднання з кожної точки держави з будь-якого доступного телефону (комунікатора), високу швидкість з'єднання з оператором Системи 112, оперативне отримання кваліфікованої допомоги, можливість спілкування іноземними мовами.

Створення Системи 112 несе в собі не заміну служб екстреного виклику (101,102,103, 104), не їх об'єднання в єдину службу, а побудову комплексного ефективного та дієздатного механізму координації дій (забезпечення інформаційної підтримки) всіх екстрених служб, що дозволить вчасно надавати екстрену допомогу населенню і реагувати на екстрені та надзвичайні ситуації.

Система 112 включає утворені у складі територіальних органів спеціально уповноваженого центрального органу виконавчої влади з питань цивільного захисту центри екстреної допомоги населенню за єдиним телефонним номером 112 (центри 112), оперативно-диспетчерські служби аварійно-рятувальних та аварійних служб, правоохоронних органів, центрів

екстреної медичної допомоги та медицини катастроф (ОДС), підрозділи екстреної допомоги населенню.

Хронологія створення системи 112:

В Україні вперше про екстрену службу порятунку 112 заговорили в 2008 році, відповідальним за створення та впровадження системи уряд визначив Міністерство надзвичайних ситуацій. За рік з'явилося державне підприємство «Центр громадської безпеки 112». На розробку технічного проєкту Системи 112 планувалося виділити 2,2 млн грн;

Наприкінці 2011 року при головних територіальних управліннях МНС у Донецькій, Харківській, Львівській областей та в Києві були створені центри для роботи Системи 112;

З травня 2012 року Міністерство запевняло, що Система 112 нарешті почне діяти в Києві, Донецькій, Харківській, Львівській та Київській областях. На проєкт реалізації Системи 112 у 2012 році було виділено 452 млн грн, які не освоєні;

На початку 2013 року голова Держслужби з надзвичайних ситуацій Михайло Болотських пообіцяв, що проєкт зі створення Системи 112 «буде реалізовано». За рік пресслужба ДСНС повідомила, що протягом року не планується здійснювати жодних практичних заходів щодо впровадження Системи 112;

З березня 2015 року у Львівській області запрацював пілотний проєкт «Єдина служба допомоги населенню 112», до якого були залучені Львівська ОДА, облрада, ГУ ДСНС тощо. Незважаючи на це, Андрій Садовий у своїй передвиборчій програмі пообіцяв після перемоги на виборах створити таку службу;

У вересні 2019 року в Білій Церкві Київської області почали тестувати систему екстреного реагування 101 як частини загальної системи екстреної допомоги населенню за єдиним номером 112;

Зрештою 5 січня 2020 року радниця міністра цифрової трансформації Яніка Мерило повідомила про створення пілотного проєкту єдиного номера екстреної допомоги 112 у Києві, Київській та Дніпропетровській областях.

Отже, Система 112 може виступати основним постачальником достовірної інформації про наявну обстановку для функціонування єдиної державної системи цивільного захисту, а створення сучасної кваліфікованої послуги населенню передбачає розвиток на новому якісному рівні функціонування єдиної державної системи цивільного захисту на всій території країни, що суттєво наблизить Україну до європейських стандартів безпеки.

Інформаційні джерела

1. Закон України «Про систему екстреної допомоги населенню за єдиним телефонним номером 112» (№ 4499-VI від 13.03.2012).

2. Наказ України №594 «Про виконання робіт із впровадження СОДУ»(від 07.06.2011).

УДК 0048:681.3

ШТУЧНИЙ ІНТЕЛЕКТ В НОВІТНІХ ТЕХНОЛОГІЯХ ВИЯВЛЕННЯ ПОЖЕЖ

Гембара Т., Ковальчук Т.
Львівський державний університет безпеки життєдіяльності, м. Львів

Новітня технологія виявлення пожежі за зображенням відіграє вирішальну роль у зменшенні втрат від пожежі за рахунок давачів сигналізації на ранніх стадіях, завдяки ранньому виявленню пожежі. Виявлення пожежі базується на алгоритмічному аналізі зображень. Однак у типових алгоритмах виявлення є низька точність, затримка виявлення та велика кількість обчислень, включаючи автоматичне вилучення функцій зображення вручну та програмно. Тому пропонуються нові підходи в алгоритмах виявлення пожежі за зображенням, засновані на вдосконалених моделях CNN.

Ключові слова: *штучний інтелект, нейронна мережа, зображення, модель, пожежа.*

As a new fire detection technology, image fire detection has recently played a crucial role in reducing fire losses by alarming users early through early fire detection. Image fire detection is based on an algorithmic analysis of images. However, there is a lower accuracy, delayed detection, and a large amount of computation in common detection algorithms, including manually and machine automatically extracting image features. Therefore, novel image fire detection algorithms based on the advanced object detection CNN models are proposed.

Key words: *artificial intelligence, neural network, image, model, fire.*

У наші дні ми спостерігаємо бурхливий розвиток інформаційних технологій, серед яких одним із пріоритетних напрямків є розробка та удосконалення систем штучного інтелекту, які використовуються вже навіть в більшості сфер людської діяльності, від побутової до наукових досягнень і відкриттів. В останнє десятиріччя отримано важливі наукові результати в галузі їх застосування для виявлення, ідентифікації, оцінки джерел загорання та пожеж [1-8], особливі успіхи були отримані у розробках алгоритмів згорткових нейронних мереж, навіть для систем відеоспостереження (рис. 1).

На сьогодні згорткова нейронна мережа, CNN – один з основних інструментів штучного інтелекту для класифікації та розпізнавання об'єктів, облич на фотографіях, розпізнавання мови. Є багато алгоритмічних методик CNN, такі як Deep Convolutional Neural Network (DCNN), Region-CNN (R-CNN), Fully Convolutional Neural Networks (FCNN), Mask R-CNN тощо. Для нас представляє інтерес в першу чергу CNN для зображень, де використовуєтья "згортка" – відома універсальна математична

операція. Її можна застосувати для будь-якого сигналу, чи то дані з давачів, чи аудіосигнал, чи зображення.

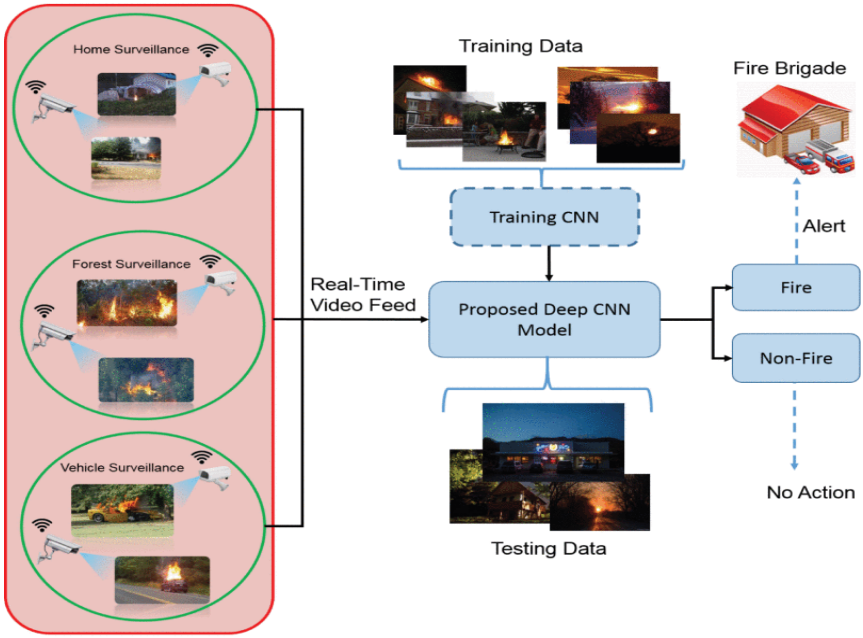


Рис 1. Схема виявлення вогнища системою відеоспостереження за допомогою системи штучного інтелекту глибокого навчання CNN [1].

Отже, у нас завдання виділити на зображенні об'єкт, наприклад, джерело загорання, чи пожежу (для масштабної пожежі, зрозуміло що мова може йти про зображення, отримане з супутника). Експерт легко зрозуміє, що перед ним початкове загорання, чи пожежа і розпізнає їх за багатьма ознаками. Але як навчити обчислювальну машину що "цей набір точок на зображенні –пожежа"? Відповідь на це питання лежить не в понятті нейронної мережі - з цим завданням може впоратися і одна з простих нейронних мереж на персептроні. Згорткова ж нейронна мережа за рахунок застосування спеціальної операції, власне згортки, дозволяє водночас зменшити кількість інформації, що зберігається в машинній пам'яті, за рахунок чого краще впорається з зображеннями більш високої роздільної здатності. Також дозволяє виділити опорні ознаки зображення, такі як ребра, контури або грані. На наступному рівні обробки з цих ребер і граней можна розпізнати повторювані фрагменти текстур, які далі можуть скластися в фрагменти зображення. По суті кожен шар нейронної мережі використовує

власне перетворення. Якщо на перших шарах мережа оперує такими поняттями як "ребра", "грані" тощо то далі використовуються поняття "текстура", "частини об'єктів". У результаті такого опрацювання ми можемо правильно класифікувати зображення або виділити на кінцевому етапі потрібний об'єкт на зображенні. Простір кольорів RGB не ізолює інформацію про колір від іншої інформації, наприклад, освітлення. Якщо використовувати RGB для представлення зображення, в розрахунках потрібно враховувати всі 3 канали. Для того, щоб зменшити величезний розмір даних в ітераціях алгоритму, для зображень пропонуємо використовувати колірний простір HSV, який ізолює інформацію про колір в єдиний канал. У такому випадку за колір відповідає канал hue (H), відтінок. Зображення генерували в програмі (FDS) Fire Dynamic Simulator з використанням розробленого програмного коду NumPy Python, отримано гістограми представлення відтінкового каналу. Аналіз діаграм показав ефективну придатність використання каналу hue, де помилка ідентифікації не перевищувала 10%, що підвищує продуктивність системи штучного інтелекту (рис. 1).

Інформаційні джерела

1. K. Muhammad, J. Ahmad, I. Mehmood. Convolutional neural networks based fire detection in surveillance videos.IEEE Access, 6 (2018), pp. 18174-18183.

2. C. Tao, J. Zhang, P. Wang Smoke detection based on deep convolutional neural networks. 2016 International Conference on Industrial Informatics - Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICII) (2016), pp. 150-153.

3. A. Filonenko, L. Kurnianggoro, K. Jo. Comparative study of modern convolutional neural networks for smoke detection on image data. 2017 10th International Conference on Human System Interactions (HSI) (2017), pp. 64-68.

4. Z. Yin, B. Wan, F. Yuan, *et al.* A deep normalization and convolutional neural network for image smoke detectionIEEE ACCESS, 5 (2017), pp. 18429-18438.

5. A.J. Dunnings, T.P. Breckon. Experimentally defined convolutional neural network architecture variants for non-temporal real-time fire detectionю 2018 25th IEEE International Conference on Image Processing (ICIP) (2018), pp. 1558-1562.

6. A. Namozov, Y. Cho. An efficient deep learning algorithm for fire and smoke detection with limited data Adv. Electr. Comput. Eng., 18 (2018), pp. 121-128.

7. W. Mao, W. Wang, Z. Dou, Y. Li. Fire recognition based on multichannel convolutional neural network Fire Technol., 54 (2018), pp. 531-554.

8. K. Muhammad, J. Ahmad, S.W. Baik. Early fire detection using convolutional neural networks during surveillance for effective disaster management Neurocomputing, 288 (2018), pp. 30-42.

Напрям 9

3D МОДЕЛЮВАННЯ ТА 3D ДРУК

УДК 514.182.7

МОДЕРНІЗАЦІЯ ТЕХНОЛОГІЧНОЇ ПІДГОТОВКИ ВИРОБНИЦТВА ДЛЯ ВИГОТОВЛЕННЯ ДЕТАЛІ «ВАЛ-ШЕСТЕРНЯ»

Бохан О.Д., Пихтєєва І.В.
Таврійський державний агротехнологічний університет ім. Дмитра Моторного, м. Мелітополь

Пропонується проект документів для технологічної підготовки виробництва деталі «Вал-шестерня», яка включає проектування нової продукції, модифікацію раніше створеної, зміну геометричних параметрів деталі, розробку проекту реконструкції підприємства та його підрозділів.
Ключові слова: *API – технологія , геометрична модель, модуль розрахунку, коефіцієнт запасу міцності.*

The draft documents for technological preparation of production of a detail «Shaft gear wheel» which includes design of new production, updating earlier created, replacement of geometrichny parasubway вдетали, development of the project of reconstruction of the enterprise and its divisions are offered.
Keywords: *API - technology, geometric model, calculation module, safety margin.*

Сучасний етап розвитку ЕОМ вимагає автоматизації виробництва - потрібне створення інженерних розрахунків, які необхідні для вирішення проектних завдань. Вихідними даними для створення нових виробів є технічне завдання, яке надає замовник. Основним завданням розробки технічного завдання є обгрунтування технічної можливості створення виробу з високими технічними параметрами якості при максимальної економічної ефективності виробництвата. Технічне завдання включає в себе: назву, призначення деталі, її область застосування, технічні характеристики деталі, обсяг виробництвадеталіітерміни виготовлення.

На підставі технічного завдання складається технічна пропозиція. При розробці технічної пропозиції обгрунтовується доцільність створення виробу в цілому. Уточнюються і розраховуються собівартість, показники експлуатаційної надійності, техніко - економічні дані і загальний технічний рівень виробу. Технічна пропозиція виконується з метою виявлення додаткових і уточнених вимог до виробу, які не можуть бути зазначені в технічному завданні і включає в себе:

– виявлення та конструкторське пророблення можливих варіантів рішень;

– перевірку варіантів на конкурентоспроможність ;

– порівняльна оцінка розглянутих варіантів за показниками якості та технологічності ;

– вибір оптимального варіанту вироби і встановлення остаточних вимог до нього.

В роботі пропонується методика модернізації технічної підготовки виробництва на прикладі деталі «Вал-шестерня».

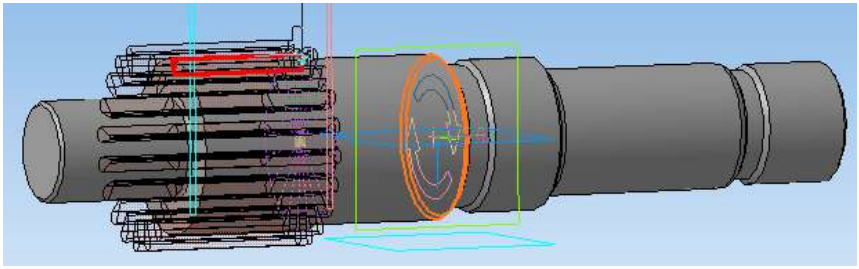


Рис. 1. Створення деталі «Вал-шестерня»

У першу чергу була створена тривимірна модель деталі в системі автоматизованого проектування КОМПАС V17. Приведений на рисунку 1 етап - є першим у створенні деталі. Другий етап – обґрунтування вибору програми для кінематичного аналізу деталі за допомогою методу аналізу ієрархії [2].

Кінематичний аналіз деталі було проведено в програмі COSMOS Works. Інструменти COSMOS Works дозволяють без зайвих часових і матеріальних витрат прораховувати багатопланові параметри конструкції, забезпечуючи максимальний запас міцності. Програма виявляє переміщення в напрямках X, Y, Z у кожному вузлі, таким чином вона розраховує навантаження, що діють у різних напрямках. Застосовуються способи обмежень (рисунок 2) в різних областях деталі.

Проаналізувавши отримані результати можна зробити висновок, що для збільшення коефіцієнту запасу міцності необхідно внести зміни до конструкції деталі.

Наступний етап – створення програмного модуля API. Більшість застосовуваних у промисловості тривимірних САПР можуть бути використані як основа для побудови спеціалізованої САПР, і є вирішальними для вирішення завдання розрахунку і проектування конкретного класу виробів. Прицьому необхідно об'єднати розрахунковий модуль, що визначає розмірні та інші параметри проектованого об'єкта, з наявним в САПР тривимірним геометричним ядром.

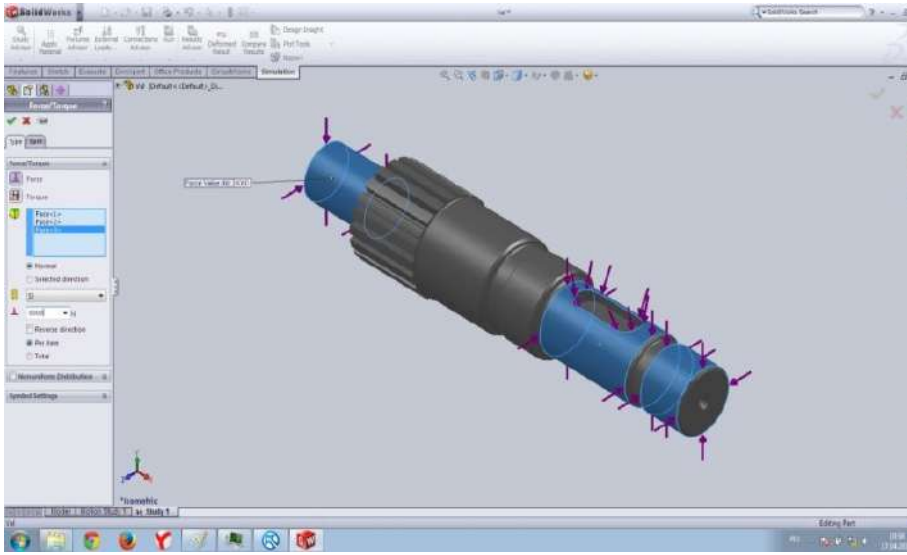


Рис. 2. Накладання обмежень на деталь

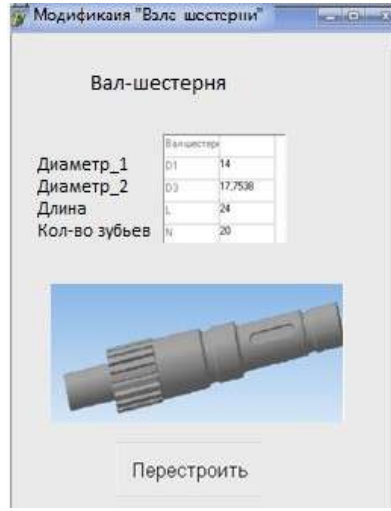


Рис. 3. Інтерфейс головного вікна

Розрахунковий модуль може розрахувати необхідні значення змінних моделі і автоматично змінити їх, в результаті чого буде отримано новий варіант 3D збірки. Таким чином, відразу ж після розрахунку буде отримана нова геометрія виробу.

В процесі роботи було створено програмний модуль API програми, який дозволяє змінити чотири основні параметри деталі: діаметри валів, довжину шпонкового пазу та кількість зубів у шестерні (Рисунок 3)

Висновки. В процесі проектування технологічної документації була визначена конструкція деталі «Вал-шестерня» , її зовнішній вигляд. Було створено тривимірну модель та кресленик деталі в системі автоматизованого проектування КОМПАС V17.

Був розроблен API- додаток при взаємодії КОМПАС та Delphi. Створення API буде невід'ємною частиною при проектуванні деталі. Завдяки створеннюAPI – програми можна буде надалі підлаштовувати деталь під необхідні параметри, змінюючи діаметри, радіуси, довжини складових.

Інформаційні джерела

1. Аверченков В.И., Каштальян И.А., Пархутик А.П. САПР технологических процессов, приспособлений и режущих инструментов: Учебное пособие для вузов //-Мн.: Выш. шк.,1993.-288 с.: ил.

2. Громов Ю.Ю. Системный анализ в информационных технологиях /ИЗДАТЕЛЬСТВО ТГТУ, 2007.

3. Норенков И.П. Основы автоматизированного проектирования // . М.: МГТУ имени Н.Э.Баумана, 2002

4. Потемкин А. Трехмерное твердотельное моделирование – М.: Компьютер//Пресс, 2002. – 296 с.: ил.

5. Мацулевич О.Є., Щербина В.М. Використання пакету прикладних програм NETCRACKER // Фундаментальна підготовка фахівців у природничо-математичній, технічній, агротехнологічній та економічній галузях : матеріали Всеукраїнської наук.-практ. конференції з міжнар. участю (Мелітополь, 11-13 вересня 2017 р.) : присвяченої 85-річчю кафедри вищої математики і фізики ТДАТУ.

6. Мацулевич О.Є., Щербина В.М., Коломієць С.М. Геометричне моделювання складних тривимірних поверхонь із застосуванням матричного рівняння еліптичного повороту // / Праці Таврійського державного агротехнологічного університету, Вип. 19(2), С. 294-300

УДК 004.92

КОНЦЕПТ СУЧАСНОГО ТА БЕЗПЕЧНОГО ДИТЯЧОГО МАЙДАНЧИКА

Брусов І., Павленко Д., Ніцин Д.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Щорічне зростання кількості нещасних випадків у зонах дитячого відпочинку визначило проблему необхідності розробки проекту дитячого майданчика з екологічно чистих та безпечних матеріалів. Дане дослідження є демонстрацією засобів дизайн-проектування для промислових виробів і визначення ролі об'єктного дизайну, як одного з найбільш актуальних сучасних проектно-художніх напрямків.

Ключові слова: *зонований дитячий майданчик, дитячі майданчики, благоустрій, інклюзивність, 3D-моделювання.*

The annual increase in the number of accidents in children's recreation areas has identified the problem of the need to develop a playground project of environmentally friendly and safe materials. This study is a demonstration of design tools for industrial products and defines the role of object design as one of the most relevant modern design and artistic trends.

Keywords: *zoned playground, playground, landscaping, inclusiveness, 3D-modeling.*

Для дитини перебування на відкритому повітрі - єдиний шанс досліджувати навколишній світ. Відкрите повітря - це місце, де діти можуть вільно покращувати свої навички, такі як біг, стрибки, лазання і так далі. Також це найбільш відповідна область для розвитку маніпулятивних навичок, таких як підйом і балансування. У більшості випадків перебування на відкритому повітрі має фізичні переваги. Гра на відкритому повітрі дозволяє дітям дізнатися про світ щось нове. Завдання полягає в тому, щоб знайти баланс між розробкою безпечного ігрового майданчика, який надасть дітям можливості для активних і пасивних ігор і діленням майданчика на зони для дітей різної вікової категорії, а також для дітей з обмеженими можливостями (рис. 1).

Поверхня майданчика покрита прогумованим матеріалом, що дозволяє дітям на інвалідних колясках або з милицями вільно переміщатися, без страху застрягти в землі. При цьому поверхня досить м'яка, щоб захистити дітей від серйозних травм у разі падіння. Замість сходинок або сходів використовуються широкі пандуси і широкі проходи, які дозволяють легко переміщатися ігровим комплексом, як для бігаючих дітей, так і для тих, хто користується інвалідними колясками. Висота устаткування розрахована для дітей на інвалідних колясках, а також для самих юних користувачів дитячого майданчика.

Рис. 1 Примірник зонованого дитячого майданчику

При проектуванні ігрового майданчика, дизайнер повинен думати про розвиток і навички, які кожна дитина отримує в процесі розвитку. Якщо на ігровому майданчику багато устаткування, що вимагає більш, ніж одного користувача, дітям рекомендується грати разом, тим самим вони можуть поліпшити свої соціальні навички, а також навчитися співпрацювати в групі. В той же час вони відкривають нові здібності, розширюють свою уяву і вчаться шукати нові рішення.

Так, Groves & Mason (1993) виявили, що діти віддають перевагу ігровим майданчикам, які вміщують в себе різні види діяльності і які дозволяють їм змінювати, адаптувати і управляти приладдям, що наявне в майданчику.

Дослідження Тітмана (1994) показало, що дітям подобаються ігрові майданчики з деревами, листям, тінистими і трав'янистими ділянками, а також з різними місцями, куди вони могли б піднятися.

Було проведено порівняння продукції сучасних українських виробників дитячих майданчиків з запропонованим проектом (рис. 2).

У порівнянні з іншими українськими компаніями наша розробка ігрового майданчика ”Child space” має найбільшу кількість переваг, зокрема: наявність зонування, використання еко-матеріалів та інклюзивний підхід.

Властивості/ Виробники	БІМБОКА	BiLand	Child space
Зонування	—	—	✓
Благоустрій	✓	✓	✓
Ігрові комплекси	✓	✓	✓
Еко-матеріали	—	—	✓
Безпечність	✓	✓	✓
Інклюзивність	—	—	✓

Рис. 2 Порівняння дитячих майданчиків українських виробників

Для реалізації поставленого завдання використовуються методи 3D-моделювання. В залежності від потреб кінцевого користувача на тривимірній моделі ландшафту задаються потрібні зони. Створюється бібліотека устаткування майданчика, яка дозволяє динамічно моделювати розташовування об'єктів по зонам. Бібліотеку можливо структурувати розподілив її на групи по віковим ознакам, динаміки дитячих ігор, потребам інклюзивних відвідувачів та інші. Також це дозволяє швидко змінювати колір як одної моделі, так і будь якої групи моделей, що потрібно для більш зрозумілого поділення простору на зони. Як подальший розвиток проекту розглядаєтеся можливість додавати до моделей та спроектованих зон дитячих майданчиків набори властивостей, таких як: фізичні властивості, стійкість до впливу зовнішнього середовища, вартість використаних матеріалів та інше. Це дозволить розширити можливості виконання замовлень на розробку дитячих майданчиків під потреби дітей та автоматизувати економічні розрахунки.

Інформаційні джерела

1. http://togetherweplay.playlsi.com/category/autism
2. https://www.playlsi.com/en/commercial-playground-equipment/playgrounds/signal-butte-park/
3. Titman W., "Special Places, Special People: The Hidden Curriculum of School Grounds", Learning Through Landscapes, England 1994.
4. Strickling C., "Impact Of Visual Impairment On Development", Texas School for the Blind and Visually Impaired. Retrieved from: http://www.tsbvi.edu/infants/134-infants/3293-theimpact-of-visual-impairment-on-development [Accessed 25 February 2015]
5. Depass D., "Multisensory Playgrounds Accessible to Kids with Disabilities" SpecialEdPost, News for the special education community. February 2013. Retrived from: http://specialedpost.org/?p=23441 [Accessed 4 January 2015]. Evans J., "In Search of Peaceful Playgrounds"

УДК: 004.72

ОСОБЛИВОСТІ РОЗРОБКИ ПЕРСОНАЖА-ТАЛІСМАНА ВІДОМОГО БРЕНДА

Вдович А. О., Сидоренко О.С.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Мета роботи полягає в тому щоб розкрити поняття маскот, дати рекомендації по створенню та інтегруванню його в існуючу стилістику відомого бренду засобом реалізації 3D-моделі персонажа.
Ключові слова: *Маскот, персонаж-талісман, 3D--модель*

The purpose of the work is to reveal the concept of mascots, to give recommendations for its creation and integration into the existing style of a well-known brand by means of implementing a 3D character model.
Keywords: *Mascot, character, 3D model*

Персонаж талісман, маскот (фр. Mascotte — «людина, тварина або об'єкт, який приносить удачу») - практично будь-який відомий персонаж, антропоморфний і не дуже, що втілює собою якийсь колектив: школу, спортивну команду, спільноту, військовий підрозділ, захід або бренд [1]. Таким персонажем можуть виступати предмети, люди, тварини або вигадані істоти. Спектр застосування маскотів дуже широкий: логотипи, сувеніри, іконки на сайтах і в мобільних додатках, реклама, розвага глядачів на заходах і багато іншого.

Розробка фірмового персонажа починається з виявлення його призначення і ключових особливостей. Йдеться про образ самої організації, отже, враховуються якості, які підприємство прагне відобразити в своєму посилі. Головна ідея персонажа народжується у керівника кожної організації та знаходить своє місце і свій відбиток у фірмовому стилі.

Талісмани в рекламі - один з найефективніших способів зв'язку бренду зі своїми клієнтами і створення любові до бренду.

Серед українських широко відомих компаній, які використовують персонажів-талісманів, можна привести в приклад Rozetka і Foxtrot. Остання не так давно зробила ребрендинг "оживив" логотип лисиці, котра вдихнула в бренд новизну і не може не виділяти його серед конкурентів

Переваги використання персонажів-талісманів:

1. Емоційний зв'язок з брендом

Протягом століть люди наділяли людськими якостями предмети, рослини, тварин. Дослідники прийшли до висновку [2], що «талісмани бренду відображають глибоко вкорінену тенденцію людини розуміти світ через

антропоморфні об'єкти». Людина починає асоціювати себе з брендом, який використовує маскота в комунікації, тому що бачить подібність.

2. Ефективна комунікація

«Живому» талісману простіше доносити повідомлення компанії до споживачів. Їх можна застосовувати в будь-який комунікації бренду з клієнтами - від реєстрації на сайті до пояснення складної послуги. Маскот працює на довготривалу перспективу і зміцнює зв'язок з покупцями.

3. Впізнаваність

Завдяки деталям і звичним людським рисам мозок споживача швидко зчитує характер маскота (а значить - і бренду) і розпізнає його в подальшому. Персонажі стають впізнаваними навіть без інших атрибутів фірмового стилю. Наприклад, лого McDonnald's - це золоті арки, а талісман - Рональд Макдональд.

4. Вірусний потенціал

Персонажі-талісмани часто народжують жарти, пародії, обговорення і нові версії користувачів. Все це працює на популярність бренду. Аналіз [3] показав, що використання маскотів в Facebook в більшості випадків збільшує залученість користувачів. Рекордний показник встановила компанія Charmin: її ведмеді підвищили залученість на 585 відсотків.

Реалізація 3D-моделі:

Щоб продумати маскота слід уважно дослідити фірмовий стиль, філософію, цільову і вже набуту аудиторію відомого бренда. Фірмовий герой повинен бути простим, щоб користувачі могли легко ідентифікувати його, навіть, якщо побачать тільки силует. Почати слід з ідеї, яку нам необхідно висловити в концептах. Це важливий етап, який буде фундаментом для всієї подальшої роботи. Маючи ескіз, ви будете чітко уявляти фінальний результат і кроки, які необхідні для його реалізації.

На етапі, коли характер і зовнішність персонажа-талісмана для бренду визначені можна приступити до реалізації його 3д моделі. Зробити це можна за допомогою таких програмних пакетів як Autodesk 3ds Max, Autodesk Maya, Blender, Cinema 4D та інших.

Вам буде потрібно задіяти всі наявні знання і навички, щоб виліпити вашого персонажа, не шкодуючи полігонів. Головне завдання - створити максимально деталізовану модель. Тому що, на наступних етапах, внести якусь деталізацію буде проблематично. Завершивши роботу над high poly моделлю, можна сміливо приступати до її оптимізації, тому що в тому вигляді, в якому знаходиться модель зараз, її використання вкрай не раціонально. Виконуємо процес ретопології, основною суттю якого є зменшення кількість полігонів до оптимального і побудови правильної сітки придатною для анімації.

Приступаємо до текстурування нашої моделі персонажа. Для текстурінга можна використовувати як готові матеріали, так і створені власноруч

для будь-яких нестандартних потреб, але найчастіше стандартного набору матеріалів буде достатньо.

Щоб вдихнути життя в нашого персонажа, нам потрібно створити йому кістки. Скінінг - (від англійського слова skin - шкіра, skinning - процес створення шкіри, зустрічається також написання скіннінг) - це один з етапів створення 3D-персонажа, коли готовий скелет прив'язується до самої 3D-моделі.

Тільки пройшовши через всі ці етапи, модель ставати придатною для створення анімації.

Готові рендери 3D-моделі простіше використовувати в подальшому для виготовлення різноманітної рекламної продукції бренду, що не тільки скоротить витрати, але і час на разробку різних варіацій.

Фірмовий стиль - це інструмент, який ідентифікує компанію і її продукцію в очах споживача. Створений один раз, він буде «працювати» на вас протягом багатьох років. Ось чому розробка фірмового стилю так важлива для фірми.

Один з найбільш ефективних методів реклами є нанесення фірмового стилю компанії на сувенірну продукцію.

Це результативний і, в той же час, один з найбільш недорогих способів донести інформацію про свою фірму до контрагентів або споживачів. Сувенірна продукція з нанесенням фірмового стилю діє на підсвідомість людини набагато тонше, але не менш ефективно, ніж пряма реклама.

Інформаційні джерела

1. Маскот [Електроний ресурс]: Вікіпедія. Вільна енциклопедія. – URL: https://uk.wikipedia.org/wiki/%D0%9C%D0%B0%D1%81%D0%BA%D0%BE%D1%82 (дата звернення: 03.11.2020).

2. Rick Enrico. How a Brand Mascot Can Make Your Business More Personable [сайт]. – URL: https://medium.com/@rick.enrico/how-a-brand-mascot-can-make-your-business-more-personable-24320364a635 (дата звернення: 04.11.2020).

3. Mark Kelley. Do Brand Characters Help or Hurt Visual Content Marketing on Facebook? [сайт]. – URL: https://www.convinceandconvert.com/social-media-case-studies/do-brand-characters-help-or-hurt-visual-content-marketing-on-facebook/ (дата звернення: 04.11.2020).

4. Корпоративная идентичность [Електроний ресурс]: Вікіпедія. Вільна енциклопедія. – URL: https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%B0%D1%8F_%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%87%D0%BD%D0%BE%D1%81%D1%82%D1%8C (дата звернення: 05.11.2020).

УДК 514.18

COMPUTER 3D MODELING IN THE LEARNING PROCESS

Herhovskyi O.I., Martyn E.V.
Lviv State University of Life Safety, Lviv

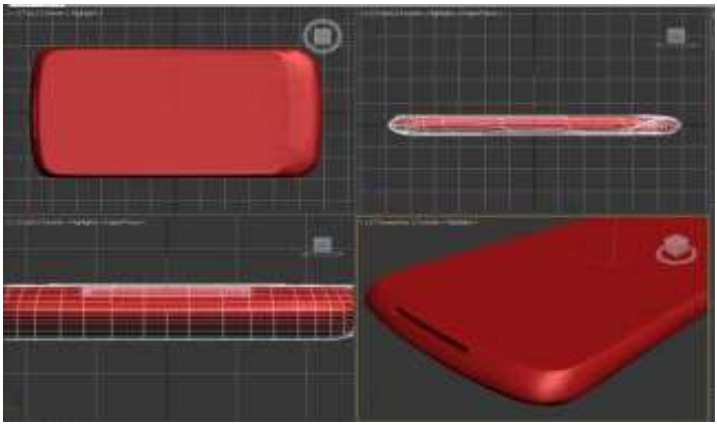
The study contains information on improving the effectiveness of the educational process for solving visual demonstrations created by computer 3D-modeling.

A similar approach to the construction of the educational process is implemented using information systems distributed in America and Europe. Peculiarities of technologies of solving technical problems based on construction and analysis with the help of computer technology of mathematical model of the studied object are investigated. Given the significant practical use, the actual problem arises comprehensive study features practical use of computer 3D modeling.

Keywords: *software, 3D modeling, analysis of educational process.*

Computer modeling is a method of solving the problem of analysis or synthesis of a technical system based on the use of a computer model. The essence of computer modeling is to find quantitative and qualitative results with its involvement. Qualitative conclusions made on the basis of such a study allow to reveal the hitherto unknown properties of the studied system: structure, dynamics of development, stability, integrity, etc. Quantitative conclusions are mainly in the nature of forecasting future or explaining past values of variables that characterize the system. Computer modeling, which emerged as one of the areas of mathematical modeling, with the development of computer information technology has become an independent and important area of application of information technology. Computer modeling in scientific and practical research is one of the main methods of cognition. Without computer simulation, it is now impossible to solve scientific, technical and economic problems. The technology of solving technical problems based on the construction and analysis with the help of computer technology of the mathematical model of the studied object is developed. In these cases, computer simulation is used. Computer modeling is also widely used for educational purposes [1, 2, 3]. The study of computer modeling opens wide opportunities for understanding the connection between computer science and mathematics and other natural and social sciences. In the educational process, you can use computer models to demonstrate the phenomenon under study, whether it is the movement of astronomical objects or atoms, a model of a molecule or the growth of microbes, etc. Modeling a specific phenomenon, process or object (fig. 1), it is possible not only to master the material, but also to acquire the ability to pose problems and tasks, predict research results, give estimates, identify major and minor factors to build models, choose analogies and mathematical formulations, use a computer to solve problems, analyze computational experiments [4]. The object model can be implemented in one (fig. 1, a) or four (fig. 1, b) planes of projections.

a)



b)

Figure1. Example of using 3D modeling

Thus, the use of computer 3D modeling allows to bring the methodology of educational activities with the methodology of research.

Інформаційні джерела

1. Гумен О. М. Графічні інформаційні технології у підготовці фахівців технологічних спеціальностей / О. М. Гумен, С. Є. Лясковська, Є. В. Мартин // Теорія і методика електронного навчання: зб. наук. пр. – Кривий Ріг: Криворізький національний університет, 2013.– Вип. IV. – С. 65-68.

2. Лясковська С. Є. Комп'ютерне графічне забезпечення технічних проектів / С. Є. Лясковська, Є.В. Мартин, Ю. Р. Оленюк.- Л.: ЛДУБЖД, 2017. – 330 с.

3. Скиба О. П. Комп'ютерна графіка / О.П. Скиба. - Т.:ТНТУ, 2019. - С. 61 – 75.

4. Герговський О.І. Розроблення твердотільної моделі вогнегасника / О.І. Герговський, Є.В.Мартин, О.В. Придатко // Проблеми та перспективи розвитку системи безпеки життєдіяльності: Зб. праць XV Міжн. наук. – практ. конф. молодих вчених, курсантів та студентів. – Л.: ЛДУБЖД, 2020.- С. 227-229.

УДК 004.92

ОСОБЛИВОСТІ ВІЗУАЛІЗАЦІЇ ДАНИХ

Герилів В., Полотай О.
Національний університет «Львівська політехніка», Львівський державний університет безпеки життєдіяльності

В даній роботі виділені основні проблеми, які постають через брак візуалізації даних та досліджено як із ними боротися. Проведено детальне ознайомлення із принципами, техніками та способами обробки та подання великих масивів інформації кінцевим користувачам.

Ключові слова: візуалізація, масиви даних, інструментарій оброблення даних.

This paper highlights the main problems that arise due to lack of data visualization and explores how to deal with them. A detailed acquaintance with the principles, techniques and methods of processing and presenting large arrays of information to end users.

Key words: visualization, data arrays, data processing tools.

Сучасний користувач щоденно споживає десятки гігабайтів контенту. Існувати в умовах постійного перенавантаження дуже складно: енергія та сили не безкінечні. Тому, аудиторії в інтернеті потрібен легкий спосіб сприйняття великих масивів даних.

Візуалізація даних допомагає сприймати та запам'ятовувати інформацію. Наш мозок влаштований таким чином, що візуальні образи він сприймає набагато краще, ніж текстовий, цифровий або табличний контент. Тому, часто ми можемо не помічати важливу інформацію у масивних об'ємах тексту. Візуалізація покликана донести до користувача те, що він зазвичай не бачить. Веб-дизайнери та контент-мейкери можуть влучно використовувати цю природну особливість людини, щоб передавати їй велику кількість даних. А добре продумані візуалізації, особливо персоналізовані, можуть не тільки донести інформацію, а ще й закарбуватися в пам'яті. Це спричинено тим, що користувач реагує на дизайн візуалізації так само, як і на самий контент. Якщо загальне оформлення або певні елементи звертаються до його досвіду, особливих якостей, переживань тощо, то реакція користувача на них і їхній візуальний вплив будуть сильнішими. В його пам'яті залишиться певний досвід.

Візуальна інформація краще сприймається і дозволяє швидко й ефективно донести доглядача власні думки та ідеї. Численні дослідження підтверджують, що:

- 90 % інформації людина сприймає через зір;
- 70 % сенсорних рецепторів знаходяться в очах;
- близько половини нейронів головного мозку людини задіяні в обробці візуальної інформації;

Унікальність візуалізації як інформаційно-інтелектуального феномену та обґрунтування її особливого статусу не лише в контексті технологічних інновацій, але й з точки зору нагальних потреб зі створення принципово нового логічного базису та, в цілому, якісно відмінної методології. Автори, базуючись на нових науково-технічних підходах, формулюють гіпотезу, де стверджують про те, що:

1) Інформаційно-символьні системи (якої б доскональності вони не досягли) не є достатніми в контексті реалізації можливостей сучасних систем штучного інтелекту;

2) Більш евристично потужними та інформаційно ємними є інформаційно-образні структури (в тому числі візуалізація), а тому саме за ними майбутнє;

3) жодна із вказаних інтелектуальних структур не може сама по собі реалізуватися повною мірою, адже лише шлях інтеграції та взаємодоповнення – істинне розуміння в цілому перспектив розвитку сучасних інтелектуально-інформаційних технологій та досліджень проблеми штучного інтелекту взагалі

Візуалізація – це метод подання інформації у вигляді оптичного зображення (наприклад, у вигляді рисунків, фотографій, графіків, структурних схем, діаграм, таблиць, карт тощо).

Зображення, отримані в результаті аналізу даних, повинні бути доступні для користувача за рахунок різноманітних засобів: границь, пропорцій, масштабу, кольору і т.д. Від цього залежить ефективність комунікації між користувачем і творцем проекту.

Основні принципи комбінації візуальних засобів подання інформації:

- принцип акценту на основних смислових елементах,
- принцип лаконічності, узагальнення та уніфікації, автономності, структурності, стадійності,
- принцип автономності, принцип використання звичних асоціацій і стереотипів.

Крім цього, засіб візуалізації бути надійним і мати швидкість, яка влаштує користувача, що приймає на основі цих даних рішення. Оскільки ми говоримо про сферу інформаційної безпеки, то швидкість обробки та подання даних є чи не найголовнішим фактором подання інформації кінцевому користувачу. Також варте уваги порівняння між пакетною обробкою даних та потоковою. Пакетна обробка може бути використана для обчислення довільних запитів щодо різних наборів даних. Зазвичай даний спосіб обчислює результати, які надіслали великим масивом, і дає змогу глибоко це все аналізувати. На відміну від цього, обробка потоку вимагає послідовну роботу над даними та поступове оновлення метрик, звітів та зведених статистичних звітів. Другий спосіб краще підходить для функцій моніторингу та реагування в режимі реального часу.

До сучасних інструментів обробки великого масиву даних та їх візуалізації відносять Splunk, ELK, Grafana, Qlik-sense, Tableau, PowerBI, Jupyter, BiqQuery + Data Studio, FineReport. За допомогою даних сервісів, фахівці можуть швидко та легко обробляти чималі потоки даних, які будуть представлені в різноманітних формах:

- графіки відношень – встановлення чи доведення зв'язку між двома чи більше змінними(точкова та бульбашкова діаграма)
- порівнянь – дослідження того, як дані змінюються протягом часу(гістограма, таблиці, стовпчаста та лінійна діаграма)
- розподілу – показ того, як ця ж інформація розподіляється на певні чітко виділені групи протягом визначених часових інтервалів - мова йде про потокові дані в реальному часі(стовпчаста гістограма та точкова діаграма)
- композицій – виділення різних елементів з яких складаються ваші дані, тут вже йдеться більше про статичні дані(кругова діаграма, деревовидна та накопичувальна діаграма)

Отже, напрошується висновок, що швидка візуалізація великих масивів даних в сучасному світі є невід'ємною складовою. Вона в сотні разів пришвидшує та покращує роботу фахівців різних сфер.

Інформаційні джерела:

1. http://yellowarrow.design/index.php/ua/blog-article/98-data-visualisation-web
2. http://eidos.org.ua/novyny/yak-i-dlya-choho-vykorystovuvaty-vizualizatsiyu-danyh/
3. https://nauchkor.ru/pubs/sposoby-vizualizatsii-big-data-v-sovremennoy-zhurnalistike-5a6f88357966e12684eea318

УДК 004.94

РОЗВИТОК ТА ЗАСТОСУВАННЯ 3D ДРУКУ

Гулковський М.М., Амс Ю.І.,Малець І.О.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі здійснено огляд сучасних систем 3D - друку, які використовують в різних сферах діяльності.
Ключові слова: *3D – друк, винаходи.*

During the work, an overview of modern 3D printing systems was performed, which provides various areas of activity.
Keywords: *3D - printing, inventions.*

Якщо ви вважаєте, що 3D-друк це новітня технологія, то ваше твердження помилкове. Насправді їй вже понад 30 років. Все почалося в 1981 році, коли доктор Хідео Кодама з Нагойського інституту, що в Японії, продемонстрував систему швидкого прототипування з використанням фотополімерів. Модель створювалась накладання шарів один за одним.

А вже у 1984, відбувся справжній прорив в цій галузі. Чарльз Халл показав світу стереолітографічний апарат, завдяки якому можна було друкувати 3D-об'єкти, моделювання яких виконувалось на комп'ютері. В якості матеріалу для друку використовувався рідкий полімер на основі акрилу, який під дією ультрафіолету моментально застигав в необхідній формі.

Незабаром, компанія Stratasys, вигадала кращу технологію - моделювання методом наплавлення . Одним словом це метод накладання шарів, які повторюють контури цифрової моделі. Як матеріал найчастіше вибирають термопластики, які подаються в принтер у вигляді спеціальних котушок ниток.

Цей метод 3D друку і використовується на даному етапі

Сам термін "3D-друк" вигадали не так давно – у 1995 році. І з того часу всі машини, що надають нам 3D-друк, прийнято називати 3D-принтерами.

А де ж саме застосовують це 3D-друк? Якщо коротко то - всюди, проте найцікавіші та найбільш перспективні сфери:

– модна індустрія;
– дизайн, мистецтво та архітектура;
– будівництво;
– авіабудування;
– ракетобудування;

– медицина.

Про останню детальніше. Нема нічого важливішого за здоров'я і саме в цій сфері завдяки 3D-друку медики здатні творити неймовірні речі. Завдяки індивідуальному підходу можна створювати найскладніші імпланти з неймовірною точністю, шини, які значно комфортніші ніж гіпси, або ж біонічні протези за доступною ціною.

В ортодонтії на зміну жахливим брекетам прийшли елайнери - пристрої які виправляють прикус. Вони дешевші, завдають менше незручностей у використанні та виглядають значно естетичніше та майже непомітно.

Але найдивовижніше - це біодрук, в якому замість штучних матеріалів використовують живі клітини. І хоча наразі цей вид 3D-друку знаходиться на зародковому етапі, йому пророкують велике майбутнє. Уявіть, що скоро можна буде друкувати потрібні органи з власних клітин, які не будуть відторгатися організмом. За допомогою 3D-принтерів друкують копії пухлин, щоб лікарі чітко розуміли: з чим мають справу в процесі операції. Для немовлят, які через генетичні дефекти народилися без вух, на 3D-принтері створюють протези. Американські вчені витратили 24 млн. доларів на принтер, що друкує людські органи, щоб потім на них тестувати віруси. Таким чином планують спостерігати за реакцією «організму» на ту чи іншу недугу.

У 2013 році в Університеті Уейк Форест у США дослідники успішно взяли клітини з хворого сечового міхура пацієнта, культивували їх додавши додаткові корисні речовини. Потім була надрукована трьохвимірна форма сечового міхура пацієнта. Форма була поміщена в інкубатор та коли вона досягла потрібної кондиції її пересадили у тіло пацієнта. Форма з часом зруйнується, залишивши лише органічний матеріал. Та ж команда успішно створила життєздатну уретру.

В 2018р. дослідники з Ньюкаслського університету у Великій Британії створили рогівку на 3D – принтері. Вчені використовували для друку біочорнила зі стовбурових клітин. Вчені створили біочорнила, які складаються зі стовбурових клітин строми — основного шару рогівки живого донора, альгінатів (полісахаридів) і колагену — білку, що становить основу сполучної тканини організму. На основі цієї речовини звичайний 3D-принтер сформував здорову рогівку за десять хвилин.

В 2019р. вчені із університету Тель-Авіва здійснили справжній прорив в 3D друці. Надрукувавши живе серце з людських тканин. Воно розміром із ягоду і може підійти кролю. Матеріалом для серця стали жирові людські тканини, які перетворили на стовбурові клітини серцево – судинного м’яза

та поєднали зі сполучною тканиною. Розмір серця усього близько 2,5 сантиметрів.

Деякі елементи із 3D – друку ми виготовляли та використовували у власному житті на нашому принтері.

Рис 1. 3D – принтер.

Інформаційні джерела

1. https://hromadske.ua/posts/ucheni-vpershe-nadrukuvaly-rohivku-na-3d-prynteri

2. http://thefuture.news/3d-printing

3. https://3d4u.com.ua/uk/blog/post/64-kak-3d-printery-ispolzuyutsya-v-avtomobilestroenii

4. https://acc.cv.ua/news/storystorynka/tehnologichno/3d-druk-v-medicini-neymovirni-fakti-65122

5. 3D ДРУК. РОЗВИТОК ТА ЗАСТОСУВАННЯ (Гулковський М.М., Борзов Ю.О.) ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНОКОМУНІКАЦІЙНИХ СИСТЕМАХ ст.233

6. https://www.imena.ua/blog/3d-bioprint-part-1/

УДК 514.182.7

ВИКОРИСТАННЯ МЕТОДІВ АВТОМАТИЗОВАНОГО ПРОЕКТУВАННЯ ПРИ ВИГОТОВЛЕННІ ДИЗАЙНЕРСЬКИХ ВИРОБІВ СКЛАДНОЇ КОНФІГУРАЦІЇ

Дуков В.О., Мацулевич О.Є.
Таврійський державний агротехнологічний університет ім. Дмитра Моторного, м. Мелітополь

У роботі розроблено технологію створення прес-форми на виготовлення декоративної рамки зі складною поверхнею, призначену для реалізації дизайнерського проекту.

Ключові слова: *низькополігональна 3D-модель, симуляція обробки деталі, дизайнерський проект.*

In this workwere describeddevelop the technology to create molds for the manufacture of a decorative frame has a complicated surface, for the implementation of the design project.

Keywords: *low-polylogy 3D-model, part processing simulation, design project.*

При проектуванні технологічного процесу для розроблення технологічного оснащення використовуються різні методи. В їх основу покладений принцип застосування верстатів з числовим програмним керуванням (ЧПК) на всіх етапах виготовлення елементів такого оснащення.

Основною метою досліджень, результати яких подано у статті, є розробка технологічного процесу виготовлення декоративних елементів, що дозволить мінімізувати використання дорого вартісного обладнання на кожному з етапів виготовлення декоративних елементів.

В процесі досліджень використані досягнення програмного забезпечення систем автоматизованого проектування та верстатів з числовим програмним управлінням для створення нового підходу для розробки дизайнерської задумки, тому що в наш час великим попитом користуються елементи декору (дизайнерські вироби), які відповідають високим естетичним вимогам сучасних споживачів.

Подібні вироби важко виготовити звичними методами через складність форми утворюючої поверхні. Застосування систем автоматизованого проектування і виробництва дає можливість отримати якісно нові результати для складних рельєфних поверхонь.

В рамках реалізації наукового проекту була поставлена мета створення об'єктів декору, а саме — декоративної рамки складної конфігурації. Реалізація проекту виконувалася на верстатах з ЧПК тільки на етапі виготовлення технологічної оснастки, що дозволяє істотно скоротити витрати на виробництво.

Реалізація поставленої задачі полягає у проектуванні складних прес-форм з двокомпонентного пластику для масового виготовлення виробів.

Процес виконання задачі подано на прикладі дизайнерського проекту декоративної рамки. На початковому етапі розроблялася 3D-модель засобами програми ***3Ds MAX***.

Надалі у системі ***PowerMill*** створювалась керуюча програма для верстата з ЧПК. Це один із найкращих програмних продуктів для швидкого і точного оброблення деталей без зарізів інструменту, оснащений інтегрованими засобами візуального контролю траєкторії ***ViewMill*** [1, 2]. Важливою перевагою ***PowerMill*** є наявність в університеті ліцензії на такий програмний продукт.

До оболонки програми завантажується 3D-модель, на основі якої створюється формат заготовки, траєкторії обробки і необхідний для них різальний інструмент. Далі в автоматичному режимі формується керуюча програма, на основі якої здійснюється обробка моделі деталі з твердої породи дерева.

Наступним кроком є формування прес-форми з двокомпонентного силікону, що має високий коефіцієнт розтягування. Завершальним етапом є безпосередньо виготовлення декоративних рамок шляхом заливання до форми необхідного матеріалу (в нашому випадку – гіпс).

На рисунках 1-4 представлено етапи створення прес-форми для виготовлення декоративної рамки.

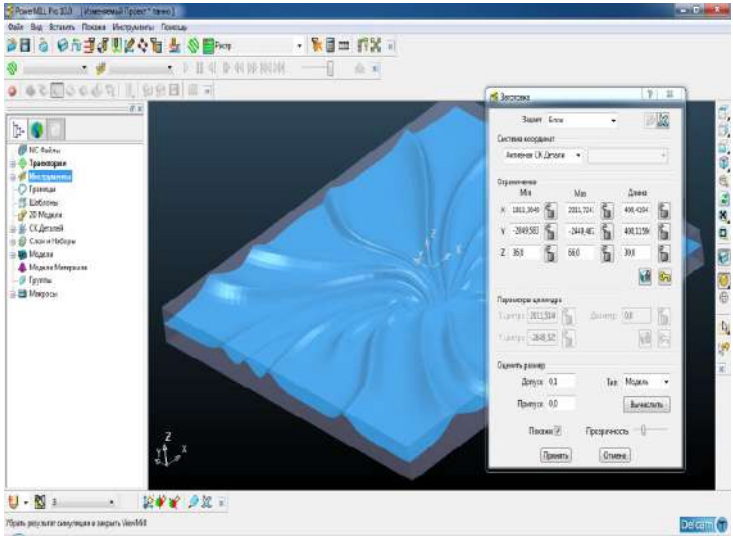


Рис. 1. Створення систем координат для обробки на верстаті

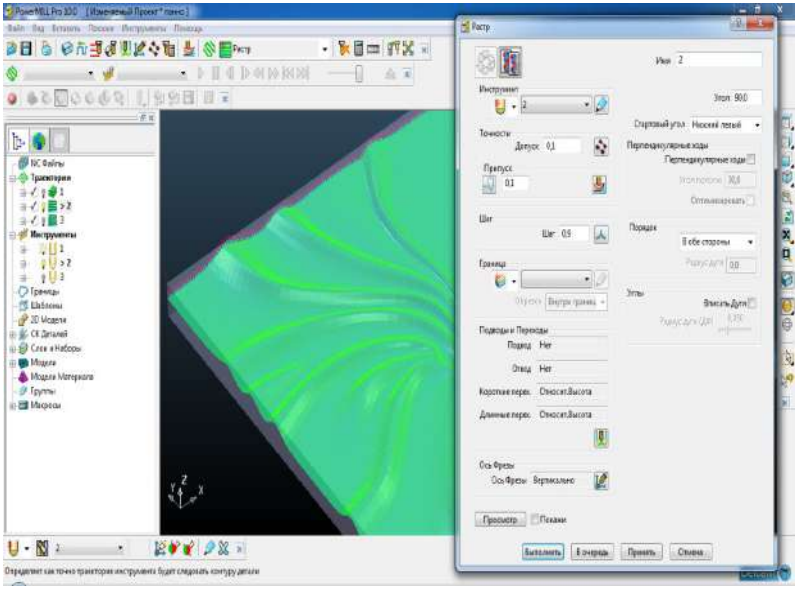


Рис. 2. Формування стратегії чистової обробки

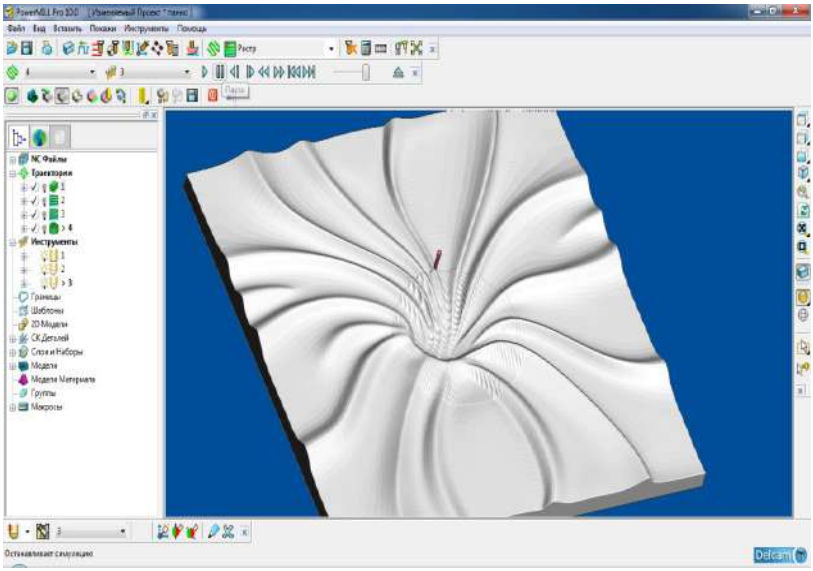


Рис. 3. Симуляція чистової обробки

Рис. 4. Готова декоративна плита

Висновки. Для реалізації дизайнерського проекту розроблена технологія створення прес-форми на виготовлення декоративної рамки, що має складну поверхню. Проектування об'ємної моделі здійснювалося в середовищі ***3Ds MAX***. Створення керуючої програми виконувалася засобами програми ***PowerMill***. Практична реалізація проекту дозволила виготовити необхідну кількість декоративної рамки для втілення дизайнерського проекту. Запропонований алгоритм дозволяє створювати велике розмаїття дизайнерських елементів високої складності, які задовольняють належним умовам якості та зниження собівартості виготовлення за рахунок застосування складного обладнання тільки на етапі виготовлення технологічного оснащення.

Інформаційні джерела

1. Щербина В.М., Холодняк Ю.В., Івженко О.В. Впровадження комп'ютерної графіки в навчальний процес при підготовці фахівців інженерних спеціальностей /Удосконалення освітньо-виховного процесу в закладі вищої освіти. Випуск 24 / Збірник науково-методичних праць / ТДАТУ, - Мелітополь: ТДАТУ, 2020.

2. Пихтєєва І.В., Антонова, Г.В. Алгоритм до знаходження верхньої граничної траєкторії на лемішно-відвальній поверхні / Праці Таврійського державного агротехнологічного університету, Вип. 19(3), С. 308-315.

3. Холодняк Ю.В., Гавриленко Є.А., Івженко О.В., Найдиш А.В. Технологія моделювання поверхонь складних технічних виробів за заданими умовами / Праці Таврійського державного агротехнологічного університету, Вип. 19(2), С. 257-263

УДК 004.946

ПРИНЦИПИ СТВОРЕННЯ 3D ОБ'ЄКТІВ ТА ПЕРСОНАЖІВ

Лубенець А.В., Сімонова О. Г.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Розглянуто деякі з сфер застосування тривимірної графіки у повсякденному житті, етапи та технології розробки 3d моделі та всього проекту.

Ключові слова: *тривимірна графіка, моделювання, етапи розробки проекту, сфери застосування.*

Складно заперечувати актуальність теми в часи розвитку інформаційних технологій. Тривимірна графіка сильно переплетена у багатьох сферах нашого життя, наприклад: під час створення макету будівлі, деталі чи будь-яких речей, які використовуються у побуті та потребують проектування, що значно зменшує час виконання поставленої задачі у порівнянні з паперовими кресленнями, а також надає можливість оперативно вносити зміні у проект. Іншою сферою використання виступає кіно, яке не може обійтись без комп'ютерної графіки, теж саме відноситься і до комп'ютерних ігор. Не можна забувати і про створення рекламних роликів чи плакатів, що значно зменшує затрати на їх створення.

Під час проектування було розглянуто технології, принципи та методи моделювання, побудови сцени, які включали в собі етапи та вимоги для побудови сцени, отримано нові навички роботи з середовищем розробки тривимірної графіки та моделювання 3d персонажів, що у подальшому покращить та пришвидшить створення робіт.

При моделюванні потрібно обрати за яким принципом це буде відбуватися, оскільки є декілька видів моделювання [1], таблиця 1.

Таблиця 1

Види моделювання

Назва	Види моделювання		
	Поверхневе моделювання	Каркасне моделювання	Твердотільне моделювання
1	2	3	4
Сфера застосування	Сфера розваг та послуг (кіно, ігри, реклама).	Програмне забезпечення з високою продуктивністю.	Інженерія, машинобудування, архітектура.

Продовження

Назва	Види моделювання		
	Поверхневе моделювання	Каркасне моделювання	Твердотільне моделювання
1	2	3	4
Приклади використання	Будь-який 3d редактор (Zbrush, 3d max, Cinema 4D тощо). Використавши модель можна: створити 3d об'єкт на принторі, станку.	UV mapping в 3d max, для створення розгортки текстури і відображення результату використовується каркасне моделювання .	Спеціалізовані промислові вироби (деталі верстаків, складові конструкції, ювелірні вироби тощо).
Технічне обладнання	Обладнання (ПК, планшет тощо) високої, середньої потужності.	Обладнання (ПК, планшет тощо) низького, середнього потужності.	Обладнання (ПК, планшет тощо) високої, середньої потужності.
Технічні навички, простота у використанні	Низький - високий рівень знань та навичок (залежить від поставленої задачі).	Високий та середній рівень знань та навичок.	Середній рівень знань та навичок.
Переваги	Можливість розпізнавати і зображати складні криволінійні грані, особливі побудови на поверхнях(отвори тощо), якісне зображення та зручний інтерфейс. Здатність розпізнавати межі, що допомагає при відображенні світла, тіні.	Каркасна модель вимагає набагато менше комп'ютерної пам'яті та ресурсів, тому вона призначена для вирішення простих завдань, відображення простих форм.	Визначення об'ємної форми, розмежування зовнішньої, внутрішньої областей об'єкта. Аналіз параметрів моделі. Імітація динаміки механізмів, процедурної генерації траєкторії руху інструменту.
Недоліки	Виникнення неоднозначності при моделювання твердого тіла. Недостатня точність представлення поверхневих моделей (правильність даних про тривимірні об'ємні тіла. Складність процедур видалення прихованих ліній і відображення внутрішніх областей.	Неоднозначність відображення орієнтації і видимості граней каркасного зображення. Неможливість відрізнити криволінійні грані, видимі межі від прихованих. Труднощі в обчисленні фізичних характеристик(маса, площа, центр ваги тощо).	Високі вимоги до продуктивності апаратних засобів, високі вимоги до кваліфікації персоналу і значна вартість таких систем.

Використовувалось поверхневе моделювання, а саме – полігональне, за допомогою програми для створення тривимірної графіки 3d max(студентська версія).

3d моделі створювались поетапно, якщо розглядати персонажів, то спочатку моделюються голова, пізніше руки та ноги, потім – тулуб, після чого відбувається «зшивання» частин тіла, останніми кроками залишаються: створення волосся та рисування текстур. Якщо розглядати оточення персонажу, то спочатку створюються локації, пізніше відбувається заповнення інтер'єром та екстер'єром саме місце дії.

Якщо розглядати розробку проекту, то можна його поділити на етапи:

1) Поява ідеї – потрібне розуміння подальшого розвитку проекту.

2) Розробка концепт-артів та дизайну.

3) Моделювання персонажів та їх оточення.

4) Підготовка моделі для накладання текстур, після – текстурінг.

5) Створюється скелет, який «прикріплюється» до моделі, створюється анімація.

6) Одяг(якщо не є частиною персонажа) та волосся анімується окремо від персонажа.

7) На останньому етапі налаштовується сцена та світло в ній, після – рендер (процес отримання зображення або відео моделі за допомогою комп'ютерної програми) [2].

Підводячи підсумки, можна сказати, що у подальшому проект може бути використаний в інших роботах, а саме: можуть запозичуватися моделі чи локації, налаштування рендеру, скелету чи текстур.

Інформаційні джерела

1. Каркасные, поверхностные, твердотельные модели, их преимущества и недостатки [Електронний ресурс] – http://wap.ism-06-2.ru/shpora.php?razdel=5&id=398&

2. 3D-моделирование и визуализация от компании KOLORO [Електронний ресурс] – https://koloro.ua/3d-modelirovanie-i-vizualizaciya.html

УДК 004.72

РОЗРОБКА ЕЛЕМЕНТІВ ДОДАТКУ ДЛЯ МАНДРІВКИ ГЛИБИНАМИ ОКЕАНУ

Белевщук С.О., Сидоренко О.С.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

У рамках розробки проекту було створено інформаційне середовище з використанням 3D-графіки для більш реалістичного занурення у підводний світ. У роботі зустрічаються різноманітні організми флори та фауни, зовнішній вигляд та коротка характеристика їхнього існування.

Ключові слова: *підводний світ, океан.*

Within the framework of the project, an information center was created using 3D-graphics for more realistic immersion in the underwater light. The robots develop the versatile organisms of the flora and fauna, their appearance and a short characteristic of their sensation.

Keywords: *underwater light, ocean.*

Актуальність теми та постановка проблеми. Вода займає 71% земної поверхні, де 97% складають океани. Оскільки океан займає велику площу на нашій планеті в його середовищі існує багато живих та неживих організмів. Людина обстежила лише 5% океану, а інші так і залишаються невідомими. Багато матеріалу ми можемо побачити з приводу підводного світу, але немає деталізованої інформації у вигляді 3D. Дана тема є важливою, оскільки набувається не тільки наукове пізнання, а й розвивається уявлення щодо життя в океані.

Розробки 3D-моделі складається з окреміх етапів, а саме:

1. Створення геометричних моделей. Планування та моделювання середовища океану та його жителів.

2. Текстурування об’єкту. Від текстур залежить наскільки точно та реалістично буде піднесено реальний об’єкт, який представлений перед нами.

3. Налаштування світла і місця спостереження. Важливий етап від якого залежить ракурс сприйняття візуалізації. Потрібно налаштувати не тільки місце, де буде розглядатися сам об’єкт, а й тон світла, рівень яскравості, глибина тіні і т.і.

4. 3D-візуалізація або рендерінг. Завершальний етап за допомогою якого доповнюються відсутні ресурси, редагуються або виправляються помилки, а також налаштовуються характеристики самого проекту (підбирається формат зображення, кількість кадрів в секунду та ін.).

Інформаційні джерела

1. Підводний світ [Текст] : для дітей серед. шк. віку / авт.-упоряд. М. О. Панкова, І. Ю. Романенко. - Х. : Фоліо, 2008. - 319 с.: іл. - (Серія "Дитяча енциклопедія").

2. Тварини водного світу: сайт.

URL: https://www.sites.google.com/site/svittwarin/tvarini-vodnogo-svitu (дата звернення: 10.11.2020). – Текст: електронний.

3. 3D-моделювання та візуалізація: сайт. - URL: https://koloro.ua/ua/3d-modelirovanie-i-vizualizaciya.html (дата звернення: 10.11.2020). – Текст: електронний.

Напрям 10

МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ СИСТЕМ

УДК 550.34:621.039.58

ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ПЛАНУВАННЯ ЕВАКУАЦІЇ НАСЕЛЕННЯ ВНАСЛІДОК ХІМІЧНОЇ АВАРІЇ

Гаврись А., Данилевський Д.
Львівський державний університет безпеки життєдіяльності, м. Львів

Проаналізовано методики розрахунків здійснення та планування евакуації населення при виникненні надзвичайних ситуацій техногенного характеру в Україні і зроблено висновок, що жодна з методик не застосовує гнучкого підходу розрахунку параметрів небезпечних факторів за допомогою програмного забезпечення. Запропоновано метод використання програм ALOHA разом із програмою ArcGIS для ефективнішого планування евакуації.

Ключові слова: *хімічно-небезпечний об'єкт, небезпечна хімічна речовина, план евакуації.*

The methods of calculating the implementation and planning of population evacuation in case of man-made emergencies in Ukraine were analyzed and concluded that none of the methods a flexible approach to calculating the parameters of hazardous factors using software wasn't use. A method of using ALOHA programs together with ArcGIS program for more efficient evacuation planning was proposed.

Key words: *chemical-hazardous object, hazardous chemical substance, evacuation plan.*

На основі аналізу стану техногенної та природної безпеки в Україні, діючих методик розрахунків наслідків виливу (викиду) небезпечних хімічних речовин у разі аварії на хімічно небезпечних об'єктах (ХНО) та транспорті, переваг сучасних світових програмних комплексів, таких як ALOHA та WISER, та недоліків національних методів розрахунку, обґрунтовано необхідність та запропоновано створення веб-сервісу для проведення аварійної оцінки обстановки при аваріях на хімічно небезпечних об'єктах та транспорті. Розроблений веб-сервіс буде використано в роботі підрозділів ДСНС України та інших зацікавлених служб для підготовки пропозицій щодо прийняття управлінських рішень, плануванні евакуації населення або при проведенні різного роду навчань, які пов'язані з обігом небезпечних хімічних речовин.

Головним завданням держави загалом та ДСНС України, як органа виконавчої влади, є забезпечення безпеки життєдіяльності населення країни. Згідно з даними Аналітичного огляду стану техногенної та природної безпеки в Україні за 2019 рік [1], на території країни існує високий рівень ризику виникнення надзвичайних ситуацій (НС), пов'язаних із аваріями з викидом або загрозою викиду небезпечних хімічних речовин. В Україні на об'єктах різного призначення зберігається, використовується, транспортується більше 285 тис. т небезпечних хімічних речовин [2].

Серед таких об'єктів: підприємства виробництва вибухових речовин та боєприпасів, виробництва неорганічних речовин, нафто- й газопереробні заводи, підприємства виробництва продуктів органічного синтезу, склади і бази із запасами отрутохімікатів для сільського господарства, магістральні аміако- та етиленопроводи тощо.

Саме з метою підвищення ефективності роботи аварійно-рятувальних підрозділів в напрямку підтримки прийняття управлінських рішень, щодо локалізації та ліквідації техногенних аварій, які пов'язані з обігом небезпечних хімічних речовин в усьому світі широко використовуються різного роду оперативні програмні комплекси та сервіси.

В США для цих цілей використовується програмний комплекс ALOHA (Areal Locations of Hazardous Atmospheres). Комплекс ALOHA призначений для використання при проведенні розрахунків під час розливу небезпечних хімічних речовин, в допомогу аварійно-рятувальним службам в ліквідації аварій пов'язаний з небезпекою поширення токсичних повітряних мас, теплового випромінювання від пожеж та ефектів вибуху.

ALOHA використовує графічний інтерфейс для введення даних та відображення результатів. Вплив токсичних хімічних парів, надлишкового тиску, теплового випромінювання або областей, де присутні легкозаймисті гази, представлені графічно та у вигляді текстового матеріалу. Комплекс ALOHA був розроблений та підтримується Відділенням реагування на надзвичайні ситуації, департаментом Національної агенції океану та атмосфери у співпраці з Управлінням надзвичайних ситуацій Агентства з охорони довкілля [3].

Основою методології ALOHA є моделі дисперсії повітря для оцінки ризику інгаляції, пов'язаної з токсичними хімічними речовинами в повітрі, та ступенем займистої хмари. Ці моделі дисперсії повітря використовуються для прогнозування того, як концентрація забруднювача, коли викидається в атмосферу, коливається залежно від часу та положення. ALOHA включає в себе дві напівемпіричні моделі дисперсії повітря: Гаусова модель використовується для прогнозування напрямку поширення хмари, яка легше повітря; модель Heavy Gas використовується для забруднюючих хмар, які важчі за повітря [3].

Після проведення розрахунків в програмі ALOHA, результати експортуються в середовище ArcGIS, де накладаються на карту території в

режимі реального часу [4], як показано на рисунку 1. За допомогою програми ArcMap виділяються будівлі та споруди, які потрапляють в зону ураження і з яких необхідно зробити евакуацію населення. Адресний список будівель необхідних для евакуації передаватиметься аварійно-рятувальним службам для оперативнішого реагування на НС. При зміні метеорологічних умов карта коригуватиметься і перелік будівель в яких необхідна евакуація змінюватиметься відповідно до обставин.

Рисунок 1 – Результат розрахунку викиду аміаку на ТОВ «Львівхолод»

Даний веб-сервіс допоможе підвищити ефективність реагування оперативно-рятувальних підрозділів ДСНС України на надзвичайні ситуації техногенного характеру, тим самим врятувати людські життя.

Література

1. Офіційний сайт ДСНС України. Режим доступу – https://www.dsns.gov.ua/ua/Dovidka-za-kvartal/103179.html.

2. Стародуб Ю.П., Гаврись А.П., Федюк Я.І. (2014). Структура та методологія управління ризиками надзвичайних ситуацій природного та техногенного характеру. Збірник наукових праць «Вісник ЛДУ БЖД», №10, С. 118-123.

3. Офіційний сайт Агентства США з охорони навколишнього середовища. Режим доступу – https://www.epa.gov/cameo/aloha-software .

4. Havrys, A. P., Moreniuk, R. Ya., & Harasymiuk, I. M. (2019). Method of fire areas localization on the basis of remote sensing data. Scientific Bulletin of UNFU, 29(8), 36–42. https://doi.org/10.15421/40290804

УДК 550.34:621.039.58

СТВОРЕННЯ ТОЧКОВОЇ КАРТИ ЗАГОРЯНЬ НА ОСНОВІ ДАНИХ ДИСТАНЦІЙНОГО ЗОНДУВАННЯ ЗЕМЛІ

Гаврись А., Гарасимюк І.
Львівський державний університет безпеки життєдіяльності, м. Львів

Щодня, з супутників отримують велику кількість інформації і лише 5% з неї реально використовують. Запропоновано використання інформації супутників для оперативного дистанційного моніторингу лісових пожеж, що дасть можливість ліквідовувати їх на ранніх стадіях. Одним із способів їх використання є створення точкових карт загорянь території.

Ключові слова: *програмне забезпечення, пожежа, комп'ютерне моделювання.*

Every day, a large amount of information is received from satellites and only 5% of it is actually used. The use of satellite information for operational remote monitoring of forest fires, which will make it possible to eliminate them at an early stage was proposed. One of the ways to use them is to create point maps of fires in the area.

Key words: *software, fire, computer modelling.*

Лісові пожежі становлять постійну загрозу екологічним системам, інфраструктурі та людським життям. Окремо від профілактичних заходів, раннє виявлення та точний моніторинг залишаються найбільш ефективними способами мінімізації наслідків загорянь. Зменшення часу реагування на пожежу призведе до зменшення заподіяної шкоди населенню та матеріальним цінностям, а також зменшення витрат держави на відшкодування. Хоча в останні кілька років розроблено та випробувано багато нових технологій. Одним з таких методів є локалізації пожежонебезпечних ділянок на основі дистанційного зондування землі [1].

Як приклад реалізації такого методу може бути точкова карта впливу небезпек, яку можна виконати в програмному забезпеченні ArcGIS. У зв'язку з останніми подіями у світі розробимо таку карту для Австралії, де відбулась наймасштабніша лісова пожежа за останнє століття.

Точки пожежі в межах території сліду пожежі - це зразок температури вогню в цьому місці пожежі. Оцінимо температуру кожного місця пожежі, обчисливши середнє значення точок, що складають кожен полігон місця пожежі. Просторово приєднуємо точки пожежі до полігонів місць пожежі і розраховуємо кількість, середнє та стандартне відхилення для кожної ділянки пожежі.

Австралія дуже велика в порівнянні з розміром слідів пожеж, тому перегляд таких місць пожеж як полігону в континентальному масштабі не є практичним [2]. Враховуючи велику різницю в масштабах між полігонами і континентом, краще моделювати місця пожеж як точки, а не полігони, як зображено на рисунку 1.

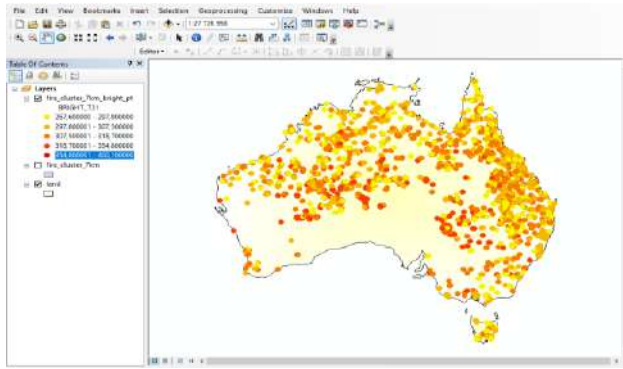


Рисунок 1 – Просторове розподілення температури на ділянках пожежі [1]

Перетворення в точки має три переваги:

1. Всі місця пожеж відображаються однаково незалежно від розміру (символи точок можуть бути визначені за площею полігону).

2. Полігони потребують більшого запам'ятовування, а це означає, що все відбувається повільніше, включаючи час коли зображення з'являється на екрані.

3. Точки – це формат просторових даних, необхідний для деяких інших аналітичних інструментів, які можна буде використати для подальших досліджень.

Мета такої карти полягає в тому, щоб показати, де виникла небезпека і в якій мірі. Карта з зображенням точок пожеж дає нам повний огляд виникнення лісових пожеж на материку, але точки, що знаходяться близько, закривають одні одних, затуляючи рисунок. Використовуючи менші точки нам доведеться візуально шукати карту, щоб визначити регіони з високою щільністю пожеж. Проте, це все ж буде простіше ніж на карті з полігонами пожеж.

На прикладі цієї карти можна зробити висновок, що за допомогою подібних карт можна локалізувати пожежу ще на початкових стадій, що суттєво зменшить збитки і не призведе до таких катастрофічних наслідків як це відбулось в Австралії в кінці 2019 та на початку 2020 років, оскільки не завжди в лісі чи поблизу знаходяться люди для вчасного повідомлення про пожежу аварійно-рятувальним підрозділам.

Література

1. Havrys, A. P., Moreniuk, R. Ya., & Harasymiuk, I. M. (2019). Method of fire areas localization on the basis of remote sensing data. Scientific Bulletin of UNFU, 29(8), 36–42. https://doi.org/10.15421/40290804.

2. Стародуб Ю.П., Купльовський Б.Є., Шелюх Ю.Є., Гаврись А.П. (2013) Локалізація пожежонебезпечних ділянок з використанням супутникових даних для сейсмоактивних зон України. Пожежна безпека: Зб. наук. пр. – №23, 151-158.

УДК [004.42+005.6]:378.1

АРХІТЕКТУРА ІНФОРМАЦІЙНО-ДОВІДКОВОЇ СИСТЕМИ "UNIBELL"

Дзень В., Кунинець М., Придатко О.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі висвітлені особливості архітектури та роботи інформаційно-довідкової системи швидкого доступу до бази даних навчального розкладу. Подано модель клієнтської та серверної частин системи. Описано особливості взаємодії клієнтської та серверної частин системи.

***Ключові слова**: база даних, розклад, мобільний додаток, архітектура застосунку.*

The paper describes the architecture of the information and reference system of access to the curriculum database. The model of client and server part of the system is given. Features of interaction of client and server part of system are described.

***Keywords**: database, schedule, mobile application, application architecture.*

Модернізація освітнього середовища в сучасних умовах потребує постійного удосконалення існуючих та розроблення нових сервісів, які націлені на забезпечення якості здобуття освіти. Не виключенням стало створення інформаційно-довідкової системи «UniBell» на базі Львівського державного університету безпеки життєдіяльності. Інформаційно-довідкова система орієнтована на швидкий доступ до бази навчального розкладу за допомогою мобільних технологій. Зважаючи на те, що система реалізує складні алгоритми, для її створення використано декілька мов та технологій програмування, то в означеній роботі ми поставили мету розглянути лише архітектуру системи.

Інформаційно-довідкова система побудована за клієнт-серверною архітектурою. Користувацький інтерфейс реалізовано у вигляді мобільного додатку під операційну систему Android. Серверна частина призначена для завантаження, зберігання, пошуку та обробки даних, а також підтримки працездатності системи.

Розглянемо концептуальну модель програмного забезпечення шляхом візуалізації архітектури клієнтської частин застосунку (рис. 1).

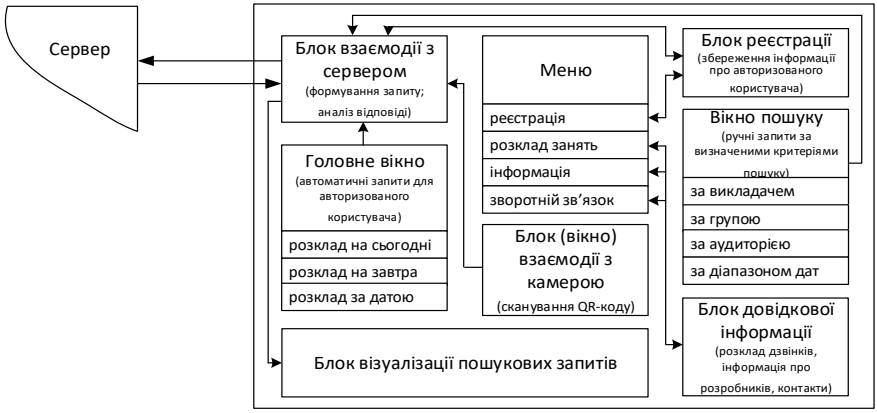


Рис. 1. Архітектура клієнтської частини системи «UniBell»

Архітектура цієї частини застосунку відповідає за реакцію дій користувача та її взаємодію із сервером. За умови авторизації користувача його дані заносяться до реєстру та зберігаються там до моменту нової авторизації на мобільному пристрої. Збереження даних про авторизованого користувача потрібне для формування та надсилання миттєвих автоматичних запитів через «Головне вікно» при повсякденному вході у додаток залежно від обраного фільтру (запит на сьогодні, на завтра, на визначену дату). Для формування спеціалізованих (індивідуальних) запитів за певними критеріями пошуку (викладач, група, аудиторія) інформація про авторизованого користувача не приймається до уваги, а пошукове розпорядження формується за допомогою передбачених фільтрів у «Вікні пошуку». Ще один варіант пошукових розпоряджень може готуватись на стороні клієнта за допомогою вбудованої опції QR-сканування, в результаті чого формується запит на отримання інформації про заняття у визначеній аудиторії в режимі реального часу.

Основне призначення роботи серверної частини (рис. 2) в автоматичному режимі – це опрацювання запитів, що надходять з клієнтської частини та зворотне надсилання результатів їх обробки через блок взаємодії з клієнтом.

Залежно від того, який запит було сформовано на клієнтській стороні, його опрацювання передається на відповідний блок обробки (автоматичних запитів, стандартних запитів або індивідуальних пошукових запитів). Після порівняння пошукових образів у базі даних отримана інформація у структурованому вигляді надсилається до клієнтської частини.

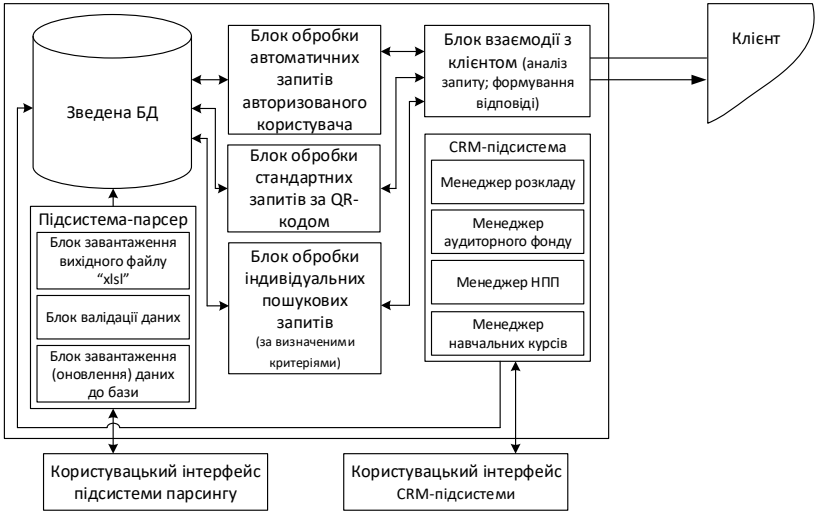


Рис. 2. Архітектура серверної частина системи «UniBell»

Висновки. Шляхом розроблення специфікації та проєктування архітектури інформаційно-довідкової системи стає можливим подальша побудова алгоритму та його реалізація з використанням програмних технологій .Net, Java, SQL у вигляді системи організації віддаленого доступу до бази даних навчального розкладу (із використанням мобільних технологій).

Інформаційні джерела

1. Burak, N., & Rak, Yu. (2014). Модель проектно-інформаційного середовища покращення підготовки рятувальника в ментальному просторі IT-технологій. Вісник Львівського державного університету безпеки життєдіяльності. 10, 24–32.

2. Malets, I., Popovych, V., Prydatko, O., Dominik, A. (2018). Interactive Computer Simulators in Rescuer Training and Research of their Optimal Use Indicator. 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP), 2, 558-562. https://doi.org/10.1109/DSMP.2018.8478486

3. Prydatko, O., Prydatko, V., Borzov, Yu., & Dzen V. (2018). Integration of the new method of mobile education in educational projects of programmer training. Bulletin of Lviv State University of Life Safety, 18, 71-80. https://doi.org/0.32447/20784643.18.2018.07

ОБЧИСЛЕННЯ ЕКСПОНЕНТИ МЕТОДОМ CORDIC

Горжієвська О., Самотий В.
Львівський державний університет безпеки життєдіяльності, м. Львів

Алгоритми CORDIC (Coordinate Rotation in a Digital Compute) розроблені досить давно. Але донині вони цікавлять багатьох вчених. Ці методи можуть бути легко використані для обчислення швидкого перетворення Фур'є, перетворення Housholdera, цифрової фільтрації сигналів, розпізнавання зображення. Ідея цього алгоритму полягає у використанні ітераційного процесу обертання векторів на площині на будь-який кут. Тут ми використовуємо лише операції зсуву та додавання. Було опубліковано багато праць, в яких алгоритми CORDIC реалізовані у вигляді електронних пристроїв. Але лише в одному з них представлені реалізації електронних експоненціальних функцій [Kantabutra V., Apparatus For Computing Exponential And Trigonometric Functions, United States Patent, US006055553A, Apr. 25, 2000]. Цей підхід передбачає велику кількість обчислень і вимагає електронного виконання двох ітераційних рівнянь, що в свою чергу є трудомістким процесом.

Алгоритм призначений для обчислення функції:

$$x = \exp(\pm\varphi), \tag{1}$$

аргумент φ перетворюємо до двійкового коду (m - число бітів),

$$\varphi = \sum_{i=1}^{m} a_i 2^{-i} \ , \qquad a_i = \{0,1\} \qquad \varphi \in [0,1) \tag{2}$$

Відомі алгоритми обчислення експоненти [1-3] використовують ітераційні цикли CORDIC:

$$x_{i+1} = x_i + \sigma_i y_i 2^{-i}, \qquad y_{i+1} = y_i + \sigma_i x_i 2^{-i} \ , \ z_{i+1} = z_i - \sigma_i \alpha_i \ ;$$

$$\alpha_i = \arctan h\left(2^{-i}\right) \ ; \ i = 1,2,3,4,4,5..12,13,13,14..,m \ ;$$

$$\sigma_i = \begin{cases} -1 \, if \ z_i < 0 \\ +1 \, if \ z_i \geq 0 \end{cases} ;$$

$$x_1 = P^{'} \ , y_1 = 0 \quad , z_1 = \varphi \ , \ x_{m+1} \approx \cosh(\varphi), \quad y_{m+1} \approx \sinh(\varphi) \quad \varphi \in [0, \ 1.118]$$

$$P^{'}_{m1} = \prod_{i=1}^{m} \cosh(\alpha_i) = \prod_{i=1}^{m} \frac{1}{\sqrt{1-2^{-2i}}} \ ; P^{'}_{m2} = \frac{1}{\sqrt{1-2^{-8}}} \frac{1}{\sqrt{1-2^{-26}}} \frac{1}{\sqrt{1-2^{-80}}} \ ; P^{'} = P^{'}_{m1} \ P^{'}_{m2}$$

Після закінчення ітераційного процесу обчислення функції $y_{m+1} \approx \sinh(\varphi)$ і $x_{m+1} \approx \cosh(\varphi)$ можна обчислити функції експонент

$$x_{m+1} + y_{m+1} \approx \exp(\varphi) \, , \ x_{m+1} - y_{m+1} \approx \exp(-\varphi) \, .$$

Недоліком таких алгоритмів є велика кількість електронних елементів при реалізації трьох ітераційних рівнянь для змінних x_{i+1} , y_{i+1} , z_{i+1} і як

результат довгий час обчислень. Спрощений алгоритм обчислення експоненти описано в [4]

$$w_{i+1} = w_i + \sigma_i w_i 2^{-i},\ z_{i+1} = z_i - \sigma_i \alpha_i,\ w_1 = P^{'}\ ,\ z_1 = \varphi\ ,\ w_{m+1} \approx \exp(\varphi)$$

$$w_{i+1} = w_i - \sigma_i w_i 2^{-i},\ z_{i+1} = z_i - \sigma_i \alpha_i,\ w_1 = P^{'}\ ,\ z_1 = \varphi\ ,\ w_{m+1} \approx \exp(-\varphi)\ ,$$

$\varphi \in [0,\ 1.118]$.

Тут реалізовано лише два ітераційні рівняння для w_{i+1} і z_{i+1}, що спрощує структуру пристрою. Але це не зменшує число операцій. Кінцевою метою нашого алгоритму є спрощення електронної реалізації пристрою і зменшення числа арифметичних операцій. Розглянемо обчислення функції $x = \exp(+\varphi)$.

Пропонуємо поділити аргумент φ на три частини φ_1, φ_2, φ_3

$$\varphi = \varphi_1 + \varphi_2 + \varphi_3\ , \tag{3}$$

Перша частина φ_1 займає m_1 старших бітів аргументу φ. Вони подаються на таблиці LUT (Look Up Table)

$$\varphi_1 = \sum_{i=1}^{m1} a_i 2^{-i} \tag{4}$$

Друга частина φ_2 аргументу φ обчислюється методом CORDIC, який реалізовуємо у вигляді одного ітераційного рівняння. Друга частина φ_2 аргументу φ займає наступних m_2 - m_1 бітів

$$\varphi_2 = \sum_{i=m1+1}^{m2} a_i 2^{-i} \tag{5}$$

В кінці третій обчислювальний блок передбачає множення на кут φ_3, який займає m - m_2 бітів

$$\varphi_3 = \sum_{i=m2+1}^{m} a_i 2^{-i} \tag{6}$$

Тут $m1$ – число старших бітів аргументу φ, що подаються до таблиці LUT, яка виконує функцію

$$x_{m1} = P \cdot \exp(\varphi_1 + D_c) \tag{7}$$

де D_c і P – сталі, які обчислюємо згідно

$$D_c = \sum_{i=m1+2}^{m2+1} \arctan h(2^{-i})\ , \tag{8}$$

$$P = 1/(\prod_{i=m1+1}^{m2} \sqrt{1 - 2^{-2i-2}})\ ; \tag{9}$$

Значення x_{m1}, які отримуємо з виходів LUT, мають m бітів. Мінімальне значення $m1$ вибираємо з умови

$$m1_{\min} = \left\lceil \frac{m - 10 - 2 \cdot \log_2 3}{6} \right\rceil . \tag{10}$$

Саме таке значення числа старших бітів $m1_{\min}$ дає можливість тримати точність обчислень в m бітів. Верхня межа $m1$ обмежена значенням $m2$ і залежить від обсягу пам'яті LUT.

Біти частини φ_2, з номерами $m1+1...m2$ обробляються методом CORDIC. Значення $m2$ вибираємо згідно умови

$$m2 = \left\lceil \frac{m}{2} \right\rceil \tag{11}$$

На практиці рівняння CORDIC

$$b_i = 2 \cdot a_i - 1 \tag{13}$$

$$x_i = x_{i-1} + b_i \cdot x_{i-1} \cdot 2^{-i-1} \tag{14}$$

реалізовані таким чином

якщо $a_i = 1$, то $b_i = 1$ і: $x_i = x_{i-1} + x_{i-1} \cdot 2^{-i-1}$,

якщо $a_i = 0$, то $b_i = -1$ і: $x_i = x_{i-1} - x_{i-1} \cdot 2^{-i-1}$.

З цього виникає що CORDIC має лише одне ітераційне рівняння (14). На виході CORDIC маємо код x_{m2}. На останньому етапі використовуємо значення z скоригованого на D_v складової φ_3, яку обчислюємо згідно рівняння

$$z = \varphi_3 + D_v, \tag{15}$$

де

$$D_v = (\sum_{i=m1+1}^{m3} a_i [2^{-i} - 2 \cdot \arctan h(2^{-i-1})] \tag{16}$$

$$m3 = \left\lceil \frac{m - 5 - \log_2 3}{3} \right\rceil. \tag{17}$$

$$x_r = x_{m2} + z \cdot x_{m2}. \tag{18}$$

Запропонований алгоритм можна використати для обчислення функції активації в нейронних мережах, що дає можливість значного зменшення числа обчислень в процесі навчання мережі.

Інформаційні джерела

1. Walther J.S. "A unified algorithm for elementary functions", in Proc. Spring Joint Comput. Conf., 1971, pp. 379-385.

2. Walther J.S. "Elementary floating-point Cordic function processor and shifter". US Patent 3766370, 1973.

3. Muller J. M. Elementary functions : algorithms and implementation. – Birkhauser Boston, 2006. -2nd edition, – 265 pp.

4. Pottathuparambil R. and R. Sass. Implementation of a CORDIC based double-precision exponential core on an FPGA. Proceedings of RSSI. – 2008, pp. 1–4.

УДК 519.85

ЗАСТОСУВАННЯ РЕДАКТОРА EXCEL ПРИ РОЗВ'ЯЗАННІ ЗАДАЧ ТЕОРІЇ ІГОР

Величко С. Д., Мелешко О. Д., Зінов'єва О.Г.
Таврійський державний агротехнологічний університет ім. Дмитра Моторного, м. Мелітополь

Зведення кінцевої матричної гри до подвійної задачі лінійного програмування, розв'язання якої знаходиться симплекс-методом засобами табличного редактора Excel.

Ключові слова: *антагоністична гра, платіжна матриця, верхня і нижня ціна гри, сідлова точка, змішана стратегія, подвійна задача лінійного програмування, симплекс-метод.*

Reduction of the final matrix game to a double linear programming problem, the solution of which is a simplex method by means of Excel spreadsheet editor.

Keywords: *antagonistic game, payment matrix, upper and lower game price, saddle point, mixed strategy, double linear programming problem, simplex method.*

Метою статті є обґрунтування доцільності розв'язання теоретико-ігрової моделі симплекс-методом в табличному редакторі Excel за допомогою засобу "Поиск решения".

Пропонується розглянути розв'язок кінцевої антагоністичної матричної гри подвійним симплекс-методом за допомогою засобу "Поиск решения" на прикладі задачі по розподіл посівних площ.

Фермер, що має певну земельну ділянку, може засівати її різними культурами, урожайність яких залежить головним чином від погоди. Необхідно визначити пропорції, в яких фермер повинен засівати наявну ділянку землі, щоб максимізувати свій дохід, незалежно від погодних умов.

Таблиця 1

Врожайність культур

Види культур	Погодні умови			Ціни на 1 ц
	Засуха	Помірні опади	Надмірні опади	
Перша	20	5	15	2
Друга	7,5	12,5	5	4
Третя	0	7,5	10	8

Задача може бути зведена до антагоністичної гри: перший гравець – фермер, другий – природа. Перший гравець може припустити, що ситуація для нього буде найбільш несприятливою в тому випадку, якщо другий гравець поводитиметься по відношенню до нього як антагоніст. В цьому випадку фермеру слід визначати свою оптимальну стратегію так само, як і в антагоністичній грі двох осіб.

Можливі доходи фермера від продажу кожної з культур при різному погодних умовах складуть матрицю гри:

$$\begin{pmatrix} 40 & 10 & 30 \\ 30 & 50 & 20 \\ 0 & 60 & 80 \end{pmatrix}.$$

Нижня ціна гри, як найбільше значення доходу з можливих найменших його значень при різних погодних умовах, складе:

$$V_{нижн}\left(0; 10; 20\right) = 20 .$$

Верхня ціна гри, як найменше значення доходу з можливих найбільших його значень для різних культур, складе:

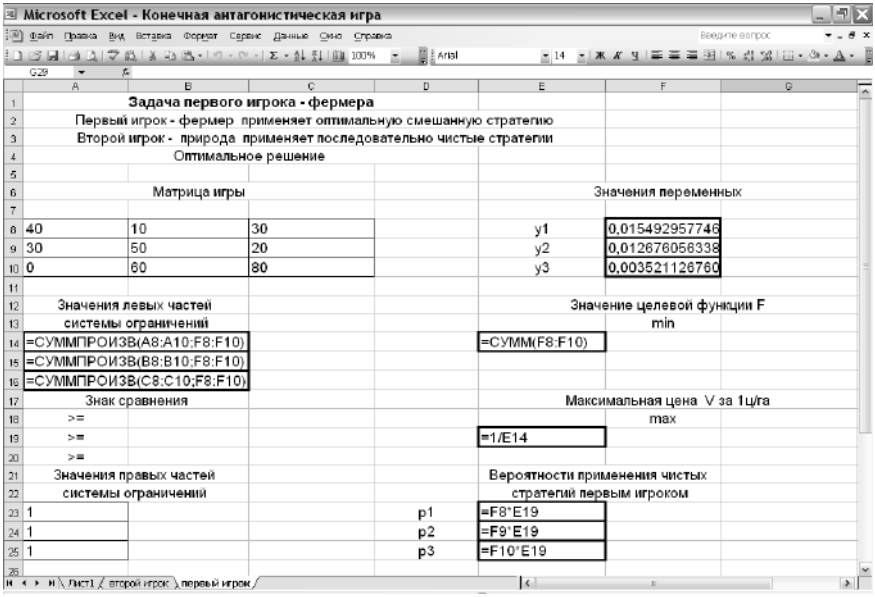
$$V_{верхн}\left(40; 50; 80\right) = 40 .$$

Кінцева антагоністична гра не має сідлової точки, тому її розв'язок необхідно шукати в змішаних стратегіях.

Вірогідність застосування чистих стратегій першим і другим гравцями позначимо p_i та g_j відповідно. Математичне очікування доходу, який може одержати фермер з своєї ділянки, буде не менше ціни гри V, а математичне очікування програшу другого гравця буде не більше ціни гри.

Завдання обох гравців можна привести до подвійної задачі лінійного програмування, ввівши нові змінні $y_i = p_i / V$ і $x_i = g_i / V$. Оскільки метою першого гравця – фермера – є максимізація його виграшу, а математичне очікування його виграшу не менше ціни гри, то перший гравець прагнутиме максимізувати ціну гри, яка, у свою чергу, еквівалентна мінімізації величини $1/V$. Метою другого гравця – природи – є мінімізація його програшу, математичне очікування його програшу не більше ціни гри, тому другий гравець прагнутиме мінімізувати ціну гри, яка, у свою чергу, еквівалентна максимізації величини $1/V$.

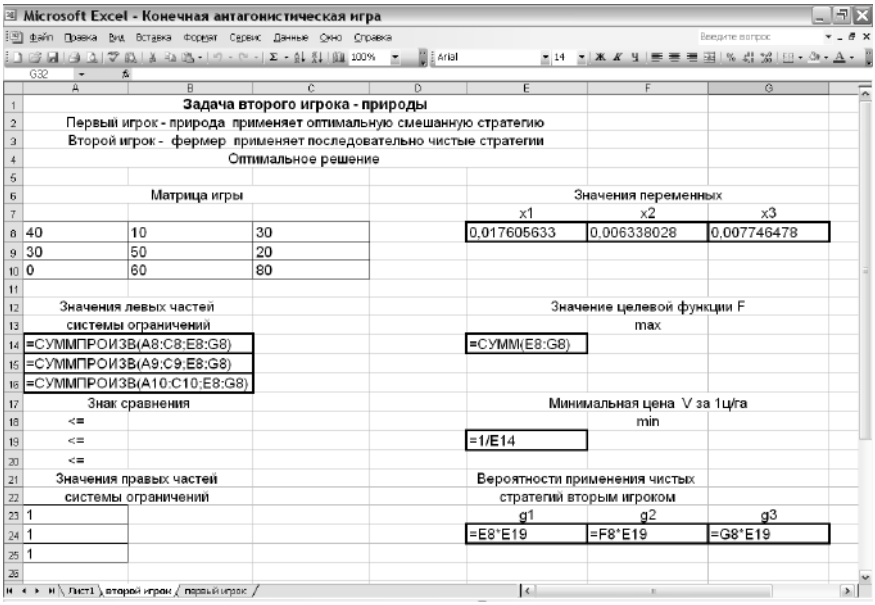
Застосовуючи надбудову "Поиск решения" табличного редактора Excel, знайдемо оптимальні стратегії першого і другого гравців і ціну гри.



Microsoft Excel - Конечная антагонистическая игра

	A	B	C	D	E	F	G
1	Задача первого игрока - фермера						
2	Первый игрок - фермер применяет оптимальную смешанную стратегию						
3	Второй игрок - природа применяет последовательно чистые стратегии						
4	Оптимальное решение						
5							
6	Матрица игры				Значения переменных		
7							
8	40	10	30		y1	0,015492957746	
9	30	50	20		y2	0,012676056338	
10	0	60	80		y3	0,003521126760	
11							
12	Значения левых частей				Значение целевой функции F		
13	системы ограничений				min		
14	=СУММПРОИЗВ(A8:A10;F8:F10)				=СУММ(F8:F10)		
15	=СУММПРОИЗВ(B8:B10;F8:F10)						
16	=СУММПРОИЗВ(C8:C10;F8:F10)						
17	Знак сравнения				Максимальная цена V за 1ц/га		
18	>=				max		
19	>=				=1/E14		
20	>=						
21	Значения правых частей				Вероятности применения чистых		
22	системы ограничений				стратегий первым игроком		
23	1			p1	=F8*E19		
24	1			p2	=F9*E19		
25	1			p3	=F10*E19		
26							

Лист1 / второй игрок / первый игрок /



Microsoft Excel - Конечная антагонистическая игра

	A	B	C	D	E	F	G
1	Задача второго игрока - природы						
2	Первый игрок - природа применяет оптимальную смешанную стратегию						
3	Второй игрок - фермер применяет последовательно чистые стратегии						
4	Оптимальное решение						
5							
6	Матрица игры				Значения переменных		
7					x1	x2	x3
8	40	10	30		0,017605633	0,006338028	0,007746478
9	30	50	20				
10	0	60	80				
11							
12	Значения левых частей				Значение целевой функции F		
13	системы ограничений				max		
14	=СУММПРОИЗВ(A8:C8;E8:G8)				=СУММ(E8:G8)		
15	=СУММПРОИЗВ(A9:C9;E8:G8)						
16	=СУММПРОИЗВ(A10:C10;E8:G8)						
17	Знак сравнения				Минимальная цена V за 1ц/га		
18	<=				min		
19	<=				=1/E14		
20	<=						
21	Значения правых частей				Вероятности применения чистых		
22	системы ограничений				стратегий вторым игроком		
23	1				g1	g2	g3
24	1				=E8*E19	=F8*E19	=G8*E19
25	1						
26							

Лист1 / второй игрок / первый игрок /

Рис. 1. Оптимальні стратегії гравців – фермера та природи

В результаті розв'язку визначено пропорції, в яких фермер повинен засівати наявну ділянку землі, щоб максимізувати свій дохід, незалежно від погодних умов.З отриманих розв'язків випливає, що найбільш несприятлива для фермера поведінка природи:

– у 0,56 випадках створювати засуху;
– у 0,20 випадках – помірні опади;
– у 0,24 випадках – надмірні опади.

Оптимальна стратегія фермера складається у тому, щоб засівати:

– 0,49 частину ділянки першою культурою;
– 0,40 частину ділянки другою культурою;
– 0,11 частину ділянки третьою культурою.

Оптимальну стратегію фермера необхідно використовувати як планове рішення.

Інформаційні джерела

1. Крушевский А.В., Швецов К.И. Математическое программирование и моделирование в экономике: Учеб. пособие для вузов. – Киев: Вища школа. Головное изд-во, 1979.

2. Акулич И.Л. Математическое программирование в примерах и задачах: Учеб. пособие для студентов эконом. спец. вузов. – М. Высш. шк., 1986.

3. Хачатрян С.Р., Пинегина М.В., Буянов В.П. Методы и модели решения экономических задач: Учебное пособие. – М.: Экзамен, 2002.

4. Красс М.С., Чупрынов Б.П Математические методы и модели для магистрантов экономики: Учебное пособие. – СПб: Питер, 2006.

УДК 519.83

МЕТОДИКА РОЗВ'ЯЗАННЯ ЗАДАЧІ ТЕОРІЇ ІГОР ІЗ ЗАСТОСУВАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Величко С. Д., Мелешко О. Д., Зінов'єва О.Г.
Таврійський державний агротехнологічний університет ім. Дмитра Моторного, м. Мелітополь

Анотація – *Уроботі пропонується методика розв'язання задачі теорії ігор за допомогою програми MatrixGames.*

Ключові слова *–прийняття рішень, теорія ігор, комп'ютерні технології.*

Summary *– The paper offers a method for solving the problem of game theory using the program MatrixGames.*

Keywords *- decision making, game theory, computer technology***.**

Алгоритми для розв'язання задач прийняття рішень вимагають велику кількість перерахунків і графічних побудов, що суттєво ускладнює отримання результату. Але при використанні програмних засобів багато задач теорії прийняття рішень, в тому числі і задачі теорії ігор, розв'язуються наваго швидше.

Задача теорії ігор може бути реалізована засобами Excel або Maple [3]. Але іноді достатньо підібрати готовий програмний продукт, який надасть можливість реалізувати певний алгоритм і суттєво спростити розрахунки. Таким програмним продуктом є програма MatrixGames.

При розв'язанні багатьох практичних задач приходиться аналізувати ситуації, де приймають участь дві або більше сторони, які переслідують різну мету, при цьому результат кожної залежить від того, який вибір зробить інша сторона. Рішенням таких проблем і займається теорія ігор.

На промислових підприємствах теорія ігор може застосовуватися для вибору оптимальних рішень, наприклад, при створенні раціональних запасів сировини, матеріалів, коли протиборствують дві тенденції: збільшення запасів, що гарантують безперебійну роботу підприємства, скорочення запасів з метою мінімізації затрат на їх зберігання. При розробці програмного забезпечення теорія ігор може застосовуватися як оцінка ризиків, пов'язаних із конкретними вразливостями в програмному забезпеченні.

В даній роботі пропонується методика розв'язання цих задач за допомогою програмного продукту MatrixGames. Дана програма призначена для розв'язання матричних ігор методами Лагранжа, Брауна-Робінсона або із використанням симплекс-методу.

Задача полягає в розв'язанні матричної гри

$$p = \begin{pmatrix} 40 & -10 & 30 \\ 30 & 50 & -20 \\ 0 & 60 & 80 \end{pmatrix}$$

При проведенні перетворень приходимо до наступної задачі лінійного програмування.

Знайти таке рішення $X = (x_1, x_2, x_3)$, при якому $F = x_1 + x_2 + x_3 \to \min$

при умовах

$$\begin{cases} 40x_1 + 30x_2 \geq 1, \\ 10x_1 + 50x_2 + 60x_3 \geq 1, \\ 30x_1 + 20x_2 + 80x_3 \geq 1, \\ x_j \geq 0, \ (j = \overline{1,3}). \end{cases}$$

Головне вікно програми MatrixGames містить наступні компоненти:

1) Вибір методу пошуку оптимальної стратегії
2) Параметри обраного методу
3) Вікно вводу та відображення платіжної матриці

4) Вибір кількості стратегій гравців
5) Вікно відображення ходу розв'язання та знайдених рішень

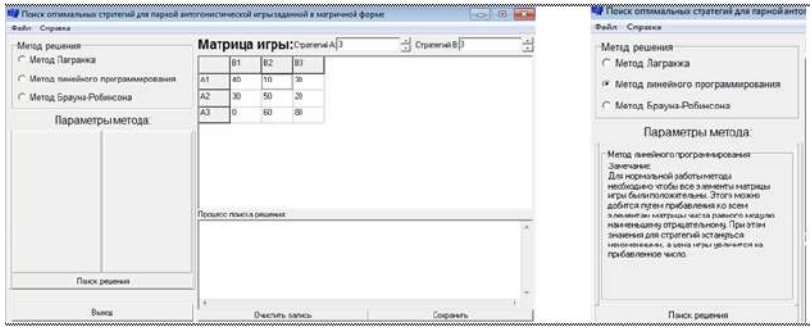


Рисунок 1 – Введення вихідних даних та вибір параметрів лінійного програмування

Для встановлення розмірності матриці необхідно вибрати кількість стратегій гравця А та гравця В.

Пошук рішення задачі теорії ігор можна вести методом лінійного програмування, або методом Лагранжа.

В результаті отримуємо оптимальні стратегії гравців $S_a = (0,49; 0,4; 0,11)$, $S_b = (0,56; 0,2; 0,24)$ та значення ціни гри $v = 31,56$.

Запропонована методика розв'язання задачі про максимальний потік є ефективним способом отримання оптимального розв'язку, який не потребує громіздких обчислень, дозволяє сконцентрувати увагу не на алгоритмі обчислення, а безпосередньо на аналізі результатів моделювання, збільшує час для обмірковування алгоритму задач.

Інформаційні джерела

1. *Протасов И.Д.* Теория игр и исследование операций : Учеб.пособие / И.Д.Протасов. – М.: Гелиос АРВ, 2003 – 368с.
2. *Оуэн Г.* Теория игр. – М.: Вузовская книга, 2004.
3. *Зінов'єва О.Г.* Розв'язання матричної гри за допомогою пакету Maple. Інформаційні технології в прикладної геометрії. Праці/Таврійський державний агротехнологічний університет. - Вип. 5, т. 6. – Мелітополь: ТДАТУ, 2011

УДК 614.8

ВИЗНАЧЕННЯ ПЛОЩІ ГОРИЗОНТАЛЬНОЇ ПРОЕКЦІЇ ЛЮДИНИ ІЗ ЗАСТОСУВАННЯМ ГРАФІЧНОГО РЕДАКТОРА

Луканді С., Хлевной О.
Львівський державний університет безпеки життєдіяльності

При проведенні розрахунків часу евакуації із закладів освіти собливої уваги заслуговує такий параметр, як середня площа горизонтальної проекції дітей та підлітків, оскільки ця категорія населення характеризується значною варіативністю антропометричних параметрів і точності розрахунку площі горизонтальної проекції в такому випадку досягнути найважче. Для визначення середніх значень потрібно провести заміри великої кількості дітей та підлітків, щоб забезпечити репрезентативність вибіркової сукупності.

Вирішити цю проблему можна, застосовуючи графічні редактори у поєднанні з фотозйомкою із глибинним масштабом. В такому випадку заміри потрібно поділити на кілька етапів.

Перший етап передбачає планову фотозйомку з глибинним масштабом кожного учасника за допомогою фотокамери, встановленої на висоті 3 м. Всіх учасників потрібно фотографувати на білому листі площею 1 м^2. Під час фотозйомки оптична вісь об'єктива має співпадати з горизонтальною віссю симетрії людини, а фокальну площину фотокамери слід встановити паралельно до підлоги. Одночасно із фотографуванням слід вимірювати значення ширини горизонтальної проекції учасника (на рівні плечей).

Подальші обрахунки потрібно виконувати у графічному редакторі, наприклад, Corel Draw 12, для якого створено скрипт для підрахунку площі GetArea. Усі фотографії слід імпортувати до редактора, обрізати та масштабувати (саме для цього і потрібен квадратний аркуш розміром 1 х 1 м).

Варто зазначити, що отримані зображення не дозволять точно визначити площу геометричної проекції учасника експерименту через перспективне спотворення. Щоб позбутися спотворення потрібно використати результати замірів ширини горизонтальної проекції. Для цього відбувається трасування фотографії з метою отримання криволінійної фігури та повторне її масштабування відповідно до замірів. В результаті можна отримати криволінійну фігуру, придатну для подальшого визначення площі.

На завершальному етапі за допомогою скрипта GetArea можна обчислити досить точне значення площі фігури (рис. 1).

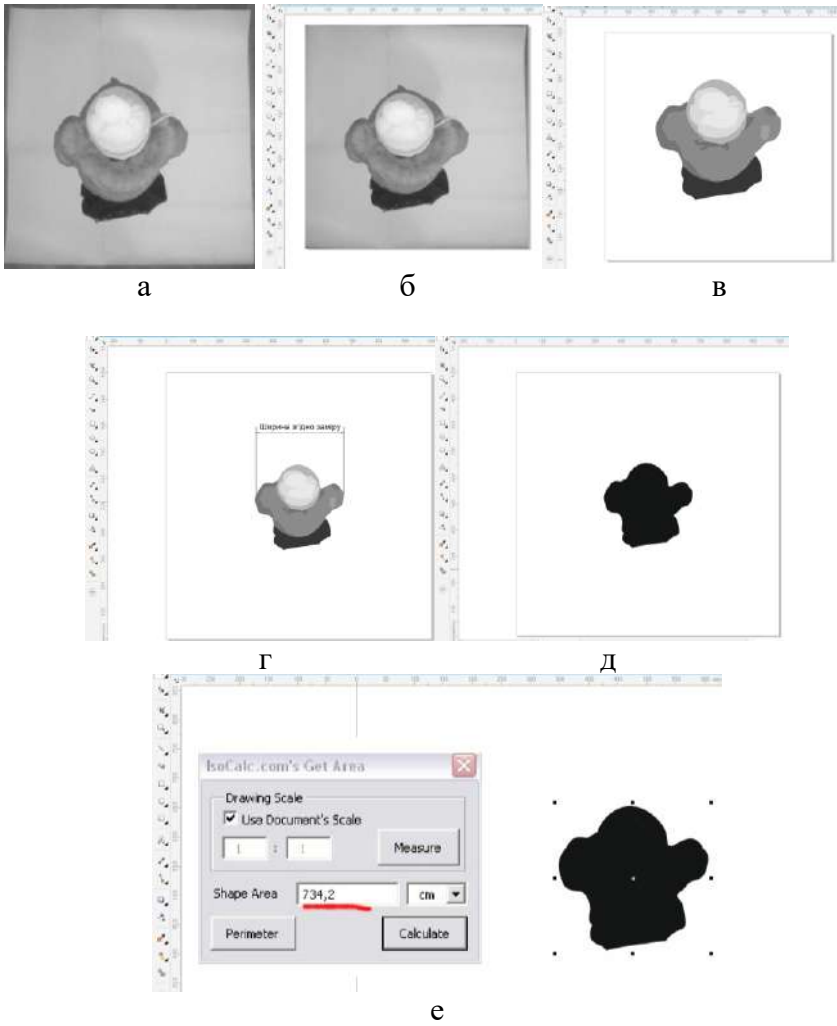


Рисунок 1 – Послідовність етапів обчислення площі горизонтальної проекції:
а – фотографування; б – масштабування; в – трасування; г – усунення перспективного спотворення; д – визначення криволінійної фігури;
д - розрахунок площі

Запропонований спосіб дає змогу легко і оперативно отримувати велику кількість експериментальних даних.

УДК 614.8

МОДЕЛЮВАННЯ ПАРАМЕТРІВ РУХУ ДІТЕЙ З ОСОБЛИВИМИ ПОТРЕБАМИ ІЗ ЗАСТОСУВАННЯМ ПРИКЛАДНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Могильний Я., Хлевной О.
Львівський державний університет безпеки життєдіяльності

Здійснено порівняльний аналіз можливостей використання сучасного прикладного програмного забезпечення для розрахунку часу евакуації при пожежах у закладах дошкільної та середньої освіти з інклюзивними групами.

Ключові слова: *евакуація при пожежі, інклюзивна група, програмний комплекс.*

A comparative analysis of the possibilities of using modern application software to calculate the time of evacuation in case of fire in preschool and secondary education institutions with inclusive groups has been done.

Key words: *fire evacuation, inclusive group, software package.*

За 2015-2020 роки кількість інклюзивних груп в закладах дошкільної освіти та класів у загальноосвітніх школах України збільшилася майже у 7 разів. Для нашої держави інклюзивна освіта є інноваційним явищем, тому при її впровадженні виникає немало проблем. Однією із найсуттєвіших проблем є низький рівень заходів із забезпечення пожежної безпеки. В Україні смертність дітей на пожежах перевищує показники Європейського союзу більше, ніж в 4 рази. Оскільки діти з особливими потребами під час виникнення пожеж є більш вразливими, дослідження питань пожежної безпеки в закладах з інклюзивними групами, особливо евакуації при пожежі, є актуальним завданням.

Серед усіх моделей, що використовуються для розрахунку часу евакуації з будівель різного призначення, найточнішою та найфункціональнішою є модель індивідуально-потокового руху людей, яка лягла в основу значної кількості прикладних комп'ютерних програм, серед яких варто відзначити Pathfinder, FDS+Evac, Fenix+, Citis Evatec, SIMULEX, тощо. Усі вони оснащені вбудованими анімаційними графічними редакторами, які дають змогу імпортувати проектну документацію, створювати 3D-моделі приміщень, розміщувати та налаштовувати індивідуальні параметри кожної людини, що евакуюється. Вихідними даними для налаштування параметрів людини є такі показники, як площа горизонтальної проекції та мобільність.

Ми провели порівняльний аналіз можливостей моделювання евакуаційних процесів за участю дітей з особливими потребами серед найпопу-

лярніших комп'ютерних програм, у роботі яких використовується індивідуально-потокова модель (таблиця 1).

Таблиця 2 – Можливості розрахунку параметрів руху дітей з особливими потребами для прикладних програм розрахунку евакуації

Категорія дітей з обмеженими можливостями	Pathfinder	Fenix+	СИТИС Evatec	SIMULEX
Діти з порушеннями опорно-рухового апарату	–	–	–	–
Діти із затримкою психічного розвитку	+*	+*	–	–
Діти із зниженим зором чи слухом	+*	+*	+*	+*

Примітка. Можливість реалізована частково.

Результати аналізу вказують на те, що можливості використання сучасних комп'ютерних програм для моделювання евакуаційних процесів за участю дітей з особливими потребами досить обмежені. Як правило для моделювання застосовуються значення площ горизонтальних проекцій дітей та значення швидкостей, розрахованих для різних груп мобільності у дорослого населення.

Інформаційні джерела

1. Ніжник В., Тесленко О., Цимбалістий С., Кравченко Н. Щодо розрахунку часу евакуації дітей з шкільних і дошкільних закладів у разі пожежі. Науковий вісник: Цивільний захист та пожежна безпека. Київ, 2016. № 1 (1). С. 81-87.

Напрям 11

ОРГАНІЗАЦІЯ БАЗ ДАНИХ І ЗНАНЬ

АКТУАЛЬНІ ПРОБЛЕМИ ТА ПЕРЕВАГИ ЗАСТОСУВАННЯ ДИСТАНЦІЙНОГО ГОЛОСУВАННЯ В УМОВАХ ПАНДЕМІЇ: ЗАРУБІЖНИЙ ДОСВІД

Герасимов А., Рижков Е.
Факультет підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ, м. Дніпропетровськ

У наш час проведення виборів є невід'ємним процесом будь-якої сучасної розвиненої держави. Він є способом формування органів державної влади, органів місцевого самоврядування або наділення їх певними повноваженнями. Вибори стали необхідним атрибутом життя держави та суспільства, вони характеризують рівень державного режиму в розрізі демократії, реалізують народний суверенітет. Міжнародне право закріплює стандарти щодо проведення й організації виборів у органи публічної влади, які формуються та доповнюються різними конституційно-правовими системами країн, зокрема України [1, с. 145-147].

Стаття 71 Конституції України встановлює основоположні принципи проведення виборів депутатів місцевих рад, сільських, селищних та міських голів та старост, а саме: вони мають відбуватися на основі загального, рівного і прямого виборчого права шляхом таємного голосування [2].

Згідно статті 12 пункту 5 Виборчого кодексу України процес проведення виборів здійснюється, перш за все, на засадах рівноправного та вільного висування кандидатів, відкритості та гласності, рівних можливостей усіх кандидатів у проведенні виборчої компанії. Дотримання цих принципів є найголовнішим фактором впливу на точність, справедливість та виправданість проведення виборів [3].

До найактуальнішої проблеми організації та проведення виборів депутатів місцевих рад, сільських, селищних та міських голів та старост в Україні є розповсюдження захворюваності на COVID-19. Можна помітити, що десятками країн світу було прийнято рішення про перенесення виборів різного значення: президентські (Ісландія, Польща, Молдова); парламент-

ські (Чорногорія, Грузія, Румунія, Хорватія, Австрія) та місцеві (Велика Британія, Франція, Австрія, Іспанія). Ці країни перенесли вибори, що мали відбутися найближчим часом, у той час, як до українських виборів залишається цілий місяць, за який може відбутися багато змін по кількості та періодичності захворюваності на COVID-19 [4].

Досвід такої держави як Канада показує, що електронні вибори не проводяться на федеральному рівні. Ще у 2000 році почалися перемови щодо можливості застосування електронних машин для відмови від паперу. Кіберзагроза демократичному процесу в Канаді – головна причина невикористання механізму дистанційного голосування. Хоча нещодавно місцеві, муніціпльні вибори, а також референдум з питання виборчої системи проводився як онлайн, так і за телефоном (хоча і були свої збої). Канада на своєму прикладі показує всьому світу, що суспільство позитивно ставиться до можливості голосувати дистанційно (за допомогою телефону та комп'ютеру), але втручання в результати голосування та збої під час їх підрахування ставлять під сумнів чесність цього процесу [5].

Сполучені штати Америки мають свої особливості: кожен штат має своє законодавство, яке діє на вибори усіх рівнів. Отже, в різних штатах по різному відбувається процес голосування: поштою, через додаток у смартфоні, за допомогою технології блокчейн (можливість голосувати громадянам, які на момент виборів знаходяться за кордоном). Практика США показує, що наразі відбувається збільшення виборців, які надають перевагу дистанційному голосуванню. Так, в 2004 році таких виборців було 24,9 млн. (20.5%), в 2016 – 57,2 млн. (40.8%), на виборах 2016 року в 16 штатах більше 50% виборців проголосували завчасно або дистанційно. Якщо тенденція буде збережена, то цілком можливо, що на виборах президента в 2020 році більше половини голосів виборців будуть віддані не на виборчих дільницях та достроково [6].

Така країна як Мексика також з 2006 року використовує голосування через пошту, але лише для тих виборців, які мають посвідчення з фотокарткою (посвідчення виборця, що видається тим, хто пройшов спеціальну перевірку та реєстрацію). Оформити таке посвідчення можна через консульство, але повноваження видавати їх може лише Національний виборчий інститут, що знаходиться безпосередньо всередині країни. Така процедура схожа на італійську: вищезгаданий орган розсилає пакети з бюлетенями та зворотними конвертами усім виборцям, що мають посвідчення. Відмінність лише в тому, що зворотний конверт відсилається лише за допомогою посольств або консульств [7].

Не треба виключати те, що пандемія COVID-19 не дасть провести в Україні парламентські вибори 25 жовтня так, як це буває зазвичай. Директор українського інституту політики Руслан Бортник заявив, що команда Президента України Володимира Зеленського планує проводити дистанційне голосування під час місцевих виборів. Для цього виборцям треба буде авторизуватися в системі через паспортні дані та віддати свій голос за певну політичну партію [8].

Позитивними факторами введення такого виду голосування є те, що усі результати будуть надсилатися до єдиної інформаційної бази даних, яка буде рахувати кількість голосів, що, по-перше, полегшить роботу ЦВК (Центральної виборчої комісії) , по-друге, зменшить об'єм витрат на фінансування дільниць, що включає в себе витрати електроенергії, антибактеріальних засобів (антисептику, марлевих пов'язок, рукавиць), видачі заробітної плати особам, що будуть допомагати при їх проведенні.

Серед негативних факторів слід відзначити те, що для функціонування такої системи голосування нелегко знайти справжніх фахівців у сфері інформаційного простору, які спроможні створити та контролювати її роботу. Відсутність спеціального професійного обладнання, яке б контролювало та захищало систему від перевантаження та збоїв, теж є серйозним питанням. Вирішити його можна складанням спеціального графіку голосування, за яким виборці з певних областей в конкретний період часу зможуть заходити в систему позачергово, коли ж виборцям з інших областей не буде надано доступу до авторизації у цій системі.

Не треба виключати той факт, що знайдеться багато фахівців, які захочуть зірвати процес голосування або внести зміни в його результати, унаслідок свого втручання в систему, тому треба задіяти найрозумніших та найдосвідченіших працівників у сфері інформаційної безпеки, які в разі потреби зможуть захистити систему та блокувати спроби втрутитися в неї. Але ж 16.8% виборців відносяться до осіб похилого віку, які не настільки обізнані в користуванні смартфонами та сучасними комп'ютерами. Отже, саме для них повинно бути придумане вирішення цієї проблеми: спеціальні особи будуть їздити за місцем їх проживання та збирати результати або ж дозволяти їм відвідувати дільниці по паспорту, де вказаний їх вік [9].

Отже, актуальною проблемою проведення та організації виборів є збільшення захворюваності на COVID-19. Цей чинник може дуже сильно вплинути на швидкість розповсюдження коронавірусу, а недооцінка його може призвести до другої хвилі захворюваності. Влада повинна знайти раціональний та найбільш грамотний вихід із цієї важкої ситуації. Проблема стосується самої організації виборів у дистанційному форматі: налагодження обладнання, створення системи голосування, доведення інформації

громадянам про порядок голосування, винайдення системи захисту та шифрування результатів та ще багато нюансів. Беручи до уваги те, що до виборів залишився один місяць, можна зробити висновок: вже зараз треба починати роботу над їх організацією та ретельно все підготувати.

Інформаційні джерела

1. Кравченко В.В.Конституційне право України: навчальний посібник. Атіка, 2004. 512 с. (дата звернення 15.09.2020).

2. Конституція: Закон України від 28.06.1996. №254к/96-ВР. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 16.09.2020).

3. Виборчий кодекс: Закон України від 19.12.2019. №396-IX.. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/396-20 (дата звернення: 16.09.2020).

4. Тарасенко Н.А. Особливості підготовки та проведення місцевих виборів-2020 в оцінках експертів. Центр досліджень соціальних комунікацій НБУВ.
URL: http://www.nbuviap.gov.ua/index.php?option=com_content&view=article&id=4905:mistsevi-vibori-2020-problemni-pitannya-pidgotovki&catid=8&Itemid=350 (дата звернення: 17.09.2020).

5. Канада вирішила відмовитися від електронного голосування: стаття / Мультимедійна платформа іномовлення, УКРІНФОРМ. 08.04.2017. URL: https://www.ukrinform.ua/rubric-world/2208338-kanada-virisila-vidmovitisa-vid-elektronnogo-golosuvanna.html (дата звернення 03.10.2020)

6. Трамп радить виборцям спробувати проголосувати за нього двічі: стаття / BBC NEWS. 03.10.2020.
URL: https://www.bbc.com/ukrainian/news-54012970 (дата звернення 03.10.2020)

7. Раннє та дистанційне голосування: досвід країн Північної Америки: стаття / Громадянська мережа ОПОРА. 04.03.2020.
URL: https://www.oporaua.org/article/vybory/19691-rannie-ta-distantsiine-golosuvannia-dosvid-krayin-pivnichnoyi-ameriki (дата звернення: 02.10.2020).

8. Р.О. Бортнік: Команда Зеленського на місцевих виборах хоче використовувати дистанційне голосування. Український інститут політики. 24.06.2020р. URL: https://nash.live/news/politics/bortnik-komanda-zelenskohona-mistsevikh-viborakh-khoche-vikoristati-distantsijne-holosuvannja.html (дата звернення: 19.09.2020).

9. Население Украины составляет 37 млн 289 тыс. человек, - Кабмин: 112.ua. URL: https://112.ua/glavnye-novosti/naselenie-ukrainy-sostavlyaet-37-mln-289-tys-chelovek-kabmin-523050.html

УДК 004.65

СУЧАСНІ СИСТЕМИ УПРАВЛІННЯ БАЗАМИ ДАНИХ

Гулковський М. М., Бурак Н. Є.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі здійснено огляд сучасних систем управління базами даних, які використовують в діяльності провідні ІТ компанії України та світу. Проведено аналіз поточних популярних програм.
Ключові слова: *систем управління базами даних, SQL, сучасні додатки.*

The paper reviews modern database management systems used in the activities of leading IT companies in Ukraine and around the world. The study analysis popular programs for database management.
Keywords: *database management system, structured query language, modern applications.*

У сучасному світі інформація є одним із найважливіших елементів життєдіяльності, які здійснюють вплив на суспільство. Збір, обробка, зберігання та подальше використання даних неможливе без застосування новітніх засобів обчислювальної техніки. З кожним роком кількість інформації збільшується стрімкими темпами, що призводить до необхідності пошуку нових методів її збереження, структуризації та групування. Таким середовищем, яке задовольняє зазначені умови є сучасні бази даних, які автоматизують процес введення, розміщення, структурування та виведення необхідної інформації. Оскільки середовище баз даних є лише місцем, яке дає змогу розмістити дані, то для управління їх роботою необхідне спеціальне програмне рішення системи управління базами даних (далі – СУБД)

Сучасні СУБД здебільшого є додатками Windows, так як дане середовище дозволяє в більшій мірі використовувати можливості персональної комп'ютерів (далі – ПК), ніж середовище DOS(дискова операційна система). Зниження вартості потужних ПК зумовив не тільки широкий перехід до середовища Windows, де розробник програмного забезпечення може в меншій мірі піклуватися про розподіл ресурсів, але також зробив програмне забезпечення ПК в цілому і СУБД зокрема, менш критичними до апаратних ресурсів.

Серед найбільш яскравих представників систем управління базами даних можна відзначити:

Borland dBase;
PostgreSQL;
Microsoft SQL Server;
Oracle Databas;

Microsoft Access.

На даний час не має істотного значення, на якій мові і на основі якого пакету написано конкретний додаток, і який формат даних в ньому використовується. Тому, за сучасних темпів розвитку інформаційних технологій в плані програмування, в одному ряді з «класичними» СУБД все частіше згадуються і мови програмування Visual Basic і Visual C ++, які дозволяють швидко створювати необхідні компоненти додатків, критичні за швидкістю роботи, які важко, а іноді неможливо, розробити засобами «класичних» СУБД. Сучасний підхід до управління базами даних передбачає також широке використання технології «клієнт-серверної» взаємодії.

Розберемо детальніше програмні продукти.

Borland dBase **–** сімейство широко розповсюджених СУБД, а також мова програмування, яка використовується в базі. Перша версія ***dBase II*** була випущена в 1980 році компанією Ashton-Tate під DOS. Версії для ПК прийшли вже із ***dBase III*** *та* ***dBase IV*****,** та декілька років були одними із найпопулярнішим середовище роботи з даними. Тривалий час ***dBase*** не підтримувала операційну систему Windows і, як результат, з'явились сильні конкуренти.

PostgreSQL — сучасна система управління базами даних з відкритим початковим кодом. Функції даної системи дозволяють виконувати деякий код безпосередньо сервером бази даних. Ці функції можуть бути написані на мові SQL. СУБД поширюється із інтегрованою базою даних, яка підтримує об'єктно-орієнтованість та сумісність із сучасними мовами програмування, зокрема:

- Вбудована мова, яка зветься PL/pgSQL, подібна до процедурної мови PL/SQL компанії Oracle.
- Підтримка мов розробки сценаріїв: PL/Perl, PL/Python, PL/Tcl, PL/Ruby, PL/sh.
- Можливість використання мови програмування C, C++, Java (за допомогою PL/Java).

Microsoft SQL Server — система управління базами даних, яка розробляється корпорацією Microsoft. Сервер даних виконує головну функцію по збереженню та наданню даних у відповідь на запити інших застосунків, які можуть виконуватися як на тому ж самому сервері, так і через мережу.

Microsoft SQL Server як мову запитів використовує версію SQL, що отримала назву Transact-SQL (скорочено T-SQL), яка є реалізацією SQL-92 (стандарт ISO для SQL) з багатьма розширеннями. T-SQL дозволяє використовувати додатковий синтаксис процедур, що зберігаються і забезпечує підтримку транзакцій (взаємодія бази даних з керуючим застосунком). Microsoft SQL Server та Sybase ASE для взаємодії з мережею використовують протокол рівня застосунка під назвою Tabular Data Stream (TDS, протокол передачі табличних даних).

База даних Oracle - це багатомодельна система управління базами даних, що виробляється корпорацією Oracle. Це база даних, яка зазвичай використовується для запуску обробки онлайн-транзакцій, зберігання даних та змішаних навантажень баз даних. Особливістю СУБД є можливість розміщення бази даних Oracle як локально на власному ПК, так і в хмарі, або як гібридна хмарна установка. Ексклюзивно для хмарних клієнтів Oracle пропонує автономну базу даних Oracle, що забезпечує повністю автоматизовані процедури роботи.

Microsoft Access входить до складу популярного пакету Microsoft Office та забезпечує повноцінна роботу щодо організації невеликих та елементарних баз даних користувачами. Основні переваги цієї СУБД: схожий інтерфейс із іншими додатками пакету Microsoft Office , що робить її зручною у користуванні, має високу стійкість даних, може використовуватися звичайними користувачами, дозволяє готувати звіти з баз даних різних форматів. Вагомою перевагою є також широкий інструментарій, який призначений для створення звітів довільної форми на підставі різних даних і розробки некомерційних додатків.

Зазначені програмні продукти мають можливості візуального проектування інтерфейсу користувача, тобто розробник з готових фрагментів створює елементи інтерфейсу, програмує тільки їх зміни у відповідь на будь-які події.

Таким чином, провівши аналіз популярних систем управління базами даних, які сьогодні пропонують IT-компанії та спільнота, можна зробити висновок, що виокремити якусь одну та зазначити, що вона є найзручніша та найефективніша не можливо. Кожна із СУБД має свої особливості, які виділяють її серед інших. Тому рішення про вибір тієї чи іншої системи управління базою покладається на майбутнього її адміністратора, а також залежить від специфіки її використання.

Інформаційні джерела

1. Тарасов О. В. Особливості використання мови визначення даних SQL у сучасних СКБД / О. В. Тарасов // Системи обробки інформації. - 2012. - Вип. 8. - С. 50-53. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2012_8_14.

2. Aung, Zeyar. (2013). Database Systems for the Smart Grid. Green Energy and Technology. 132. 151-168. DOI:10.1007/978-1-4471-5210-1-7

3. Чмир П.О. Аналіз проблем безпеки даних в серверах на базі SQL Server / П.О. Чмир, Н.Є. Бурак // Проблеми та перспективи забезпечення цивільного захисту: матеріали міжнар. наук.-практ. конф. молодих учених. – Харків: НУЦЗ України, 2018. – С. 157

4. John Hammink The Types of Modern Databases. [Електронний ресурс]. – Режим доступу: https://dzone.com/articles/the-types-of-modern-databases

УДК 004.65

ПРАВИЛА КОДДА В БАЗАХ ДАНИХ

Жолубак Л.І., Бурак Н.Є.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі проведено огляд методів теоретичної ідентифікації реляційних баз даних на основі застосування правил Кодда. Виконано детальний аналіз класифікаційних умов відповідності структур баз даних.

Ключові слова: *систем управління базами даних, реляційна база даних, відношення.*

Based on Codd rules, in study were reviewed methods of relational databases theoretical identification. Were made detailed analysis of classification conditions for database structures compliance to relation type.

Keywords: *database management system, relational database, relation.*

Завдання тривалого зберігання й обробки інформації з'явилося практично одразу з появою перших комп'ютерів. Для рішення цього завдання наприкінці 60-х років були розроблені спеціалізовані програми, що одержали назву систем управління базами даних (далі - СУБД). СУБД пройшли тривалий шлях еволюції від системи керування файлами, через ієрархічні й мережні бази даних. У сучасних умовах, виникла складнощі організації зберігання даних у моделях структури, які були розроблені раніше, було запропоновано новий тип бази даних – реляційна, яка наприкінці 80-х років стала домінуючою, оскільки буда зручною та легкою у розумінні та реалізації. Із того часу такі СУБД стали стандартом де-факто, і для того, щоб уніфікувати роботу з ними, була розроблена структурована мова запитів (SQL), що являє собою мову керування саме реляційними базами даних на основі звернень.

Реляційна база даних – база даних, заснована на реляційній моделі. Термін "реляційний" походить від англійського "relation" (відношення). Для роботи з реляційними базами застосовують реляційні СУБД.

Теорія реляційних баз даних була розроблена британським доктором Едгаром Коддом з компанії IBM в 1970 році. У реляційних базах даних всі дані представлені у вигляді простих таблиць, розбитих на рядки й стовпці, на перетинанні яких розташовані дані.

Після проведення грунтовного дослідження реляційної моделі систем баз даних, Е. Коддом було написано правила, за допомогою яких можна дізнатись чи є СУБД реляційною. 12 правил Кодда — набір 13 правил

(пронумерованих від нуля до дванадцяти). Правила передбачають досить чіткі умови відповідності, а саме:

0. Фундаментальне правило (Foundation Rule): Реляційна СУБД має бути здатною повністю керувати базою даних, використовуючи зв'язки між даними.

1. Інформаційне правило (Information Rule): Інформація має бути представлена у вигляді даних, що зберігаються в осередках. Дані, що зберігаються у комірках, мають бути атомарними. Порядок рядків у реляційній таблиці не повинен впливати на зміст даних.

2. Правило гарантованого доступу (Guaranteed Access Rule): Доступ до даних має бути вільним від двозначності. До кожного елементу даних має бути гарантований доступ за допомогою комбінації імені таблиці, первинного ключа рядку й імені стовпця.

3. Систематична обробка Null-значень (Systematic Treatment of Null Values): Невідомі значення NULL, відмінні від будь-якого відомого значення, мають підтримуватись для всіх типів даних при виконанні будь-яких операцій. Наприклад, для числових даних невідомі значення не повинні розглядатись як нулі, а для символьних даних — як порожні рядки.

4. Правило доступу до системного каталогу на основі реляційної моделі (Dynamic On-line Catalog Based on the Relational Model): Словник даних має зберігатись у формі реляційних таблиць, і СУБД повинна підтримувати доступ до нього за допомогою стандартних мовних засобів, тих самих, що використовуються для роботи з реляційними таблицями, які містять дані користувача.

5. Правило повноти підмови маніпулювання даними (Comprehensive Data Sublanguage Rule): Система управління реляційними базами даних має підтримувати хоча б одну реляційну мову, яка а) має лінійний синтаксис, б) може використовуватись інтерактивно і в прикладних програмах, в) підтримує операції визначення даних, визначення уявлень, маніпулювання даними (інтерактивні та програмні), обмежувачі цілісності, управління доступом та операції управління транзакціями (begin, commit і rollback).

6. Правило модифікації поглядів (View Updating Rule): Кожне подання має підтримувати усі операції маніпулювання даними, які підтримують реляційні таблиці: операції вибірки, вставки, модифікації і видалення даних.

7. Правило високорівневих операцій модифікації даних (High-level Insert, Update, and Delete): Операції вставки, модифікації і видалення даних мають підтримуватись не тільки щодо одного рядку реляційної таблиці, але й щодо будь-якої безлічі рядків.

8. Правило фізичної незалежності даних (Physical Data Independence): Додатки не повинні залежати від використовуваних способів зберігання

даних на носіях, від апаратного забезпечення комп'ютерів, на яких знаходиться реляційна база даних.

9. Правило логічної незалежності даних (Logical Data Independence): Представлення даних в додатку не повинно залежати від структури реляційних таблиць. Якщо в процесі нормалізації одна реляційна таблиця розділяється на дві, подання має забезпечити об'єднання цих даних, щоб зміна структури реляційних таблиць не позначалась на роботі додатків.

10. Правило незалежності контролю цілісності (Integrity Independence): Вся інформація, необхідна для підтримки цілісності, має бути у словнику даних. Мова для роботи з даними має виконувати перевірку вхідних даних і автоматично підтримувати цілісність даних.

11. Правило незалежності від розміщення (Distribution Independence): База даних може бути розподіленою, може перебувати на кількох комп'ютерах, і це не повинно впливати на додатки. Перенесення бази даних на інший комп'ютер не повинне впливати на додатки.

12. Правило узгодженості мовних рівнів (The Nonsubversion Rule): Якщо використовується низькорівнева мова доступу до даних, вона не повинна ігнорувати правила безпеки і правила цілісності, які підтримуються мовою більш високого рівня.

Ці правила можуть застосовуватися в будь-якій системі баз даних, яка управляє збереженими даними, використовуючи тільки свої реляційні можливості.

Аналізуючи зазначені правила та структуру і функціональність популярних сьогодні «реляційних» СУБД, можна зробити висновок про неповну їх відповідність стандартам реляційних баз. Таким чином, сучасні системи управління базами даних є синтезом декількох моделей організації внутрішньої структури розміщення даних.

Інформаційні джерела

1. Harrington, Jan. (2009). Codd's Rules for Relational Database Design. DOI: 10.1016/B978-0-12-374730-3.00010-3.

2. Компан С. В. Типізація сучасних баз даних (огляд) / С. В. Компан // Вісник Київського національного університету імені Тараса Шевченка. Серія : Фізико-математичні науки. - 2014. - Вип. 3. - С. 144-153. - Режим доступу: http://nbuv.gov.ua/UJRN/VKNU_fiz_mat_2014_3_31.

3. Головчинер М.Н Базы данных: Основные понятия, модели данных, процесс проектирования: учебное пособие. / М.Н.Головчинер. – Томск.: ТГУ , 2009. – 126 с.

4. Тереник, Дмитро & Анатолійович, Георгій. (2020). Порівняння SQL і NOSQL баз даних на прикладі проектування аффілейт репорт систем. Radioelectronic And Computer Systems. 83-89. DOI: 10.32620/reks.2020.1.08.

Напрям 12

ОПЕРАЦІЙНІ СИСТЕМИ

ОПЕРАЦІЙНІ СИСТЕМИ

Мечус Х.В., Карабин О.О.
Львівський державний університет безпеки життєдіяльності, м. Львів

Виконано порівняльний аналіз та наведено відсотковий рейтинг популярності операційних систем, які використовуються в роботі десктопів, мобільних телефонів, планшетів, ігрових приставок.

Ключові слова: *операційна система, програмні ресурси, інформаційні технології.*

Comparative analysis and percentage rating of the popularity of operating systems used in desktops, mobile phones, tablets, game consoles performed.

Keywords: *operating system, software resources, information technologies.*

Важко назвати іншу сферу людської діяльності, яка розвивалася б так стрімко і породжувала б таке розмаїття проблем, як інформатизація та комп'ютеризація суспільства. Історія розвитку інформаційних технологій характеризується швидкою зміною концептуальних уявлень, технічних засобів, методів та сфер їх застосування.

У сучасних реаліях вельми актуальним для більшості людей стало вміння користуватися промисловими інформаційними технологіями. Проникнення комп'ютерів в усі сфери життя суспільства переконує в тому, що культура спілкування з комп'ютером стає частиною загальної культури людини.

Під час вмикання комп'ютера операційна система завантажується в пам'ять раніше, ніж інші програми і потім служить платформою і середовищем для їх роботи. Без операційної системи неможливо уявити роботу з комп'ютером. Знання операційної системи є необхідним для успішного користування сучасними комп'ютерами.

Операційна система (ОС) – це системне програмне забезпечення, яке управляє комп’ютерними апаратними та програмними ресурсами і надає

загальні служби для комп'ютерних програм. Всі комп'ютерні програми, за винятком прошивки, вимагають роботи операційної системи.

Операційні системи з поділом часу планують завдання для ефективного використання системи і можуть також включати в себе програмне забезпечення обліку для розподілу витрат часу процесора, масового зберігання, друку та інших ресурсів.

Загальний рейтинг операційних систем в Україні, включаючи десктопи, мобільні, планшети та ігрові приставки показує, що лідером є Windows, який встановлено на 59,81% пристроїв.

Якщо брати окремо операційні системи встановлені на комп'ютерах, лідером в Україні є також Windows – 83,73%, OS X – 13,1% і Linux – 1,82%.

Серед мобільних телефонів перше місце посідає система Android – 82,09%, операційна система iOS посідає друге місце 17,46% – практично кожен шостий смартфон. В планшетах також лідирує Android (54,93%), а у iOS використовується у 44,85% всіх планшетів.

Серед ігрових приставок в Україні найбільше люблять Playstation (71,52%) та Xbox (28,42%).

Топ 5 операційних систем світу в 2020 році

Андроїд. Це визнана домінуюча ОС згідно з даними статистики. Андроїд запрограмований в 39,77% всіх пристроїв. Затятими прибічниками мобільної платформи Android можна назвати жителів Китаю. Тут частка цієї ОС складає 46,9%. У порівнянні з квітнем 2019 популярність Андроїда в Китаї збільшилася з 40,11% до 46,9%, внаслідок чого Windows знизив показники з 39,53% до 34,81%.

Windows. З огляду на сукупні статистичні дані настільних і мобільних платформ у всьому світі за квітень 2020 року, друге місце займає Windows з показником 32,31% всіх пристроїв. Це монополіст, створений компанією Microsoft, якому належить право на модифікацію і копіювання. Статистика за квітень 2018-2019 підтверджувала зростання популярності цієї операційної системи серед користувачів – в квітні 2018 року її рейтинг становив 36,74%, тоді як в квітні 2019 року він піднявся до 38,05%.

iOS. У мобільному секторі за даними квітня 2019 року операційна система виробництва Apple займала третє місце з показником 13,75%. Прямий конкурент Android зміг завоювати значну частку на світовому ринку в цьому році вже з показником 17,66%. Операційна система займає почесне третє місце в світі.

MacOs. Її перша назва Mac Os X, до 2016 року система була відома як OS X. Сьогодні Mac Os -популярна операційна система виробництва Apple, яка знаходиться на четвертій позиції в рейтингу згідно з даними Світової статистики – 7,98%. В Америці ця десктопна платформа з часткою ринку 12,05% також займає четверте місце, тоді як в Україні (9,35%) знаходиться на третій позиції.

LinUx. Операційна система з відкритою ліцензією, завдяки чому використовується на будь-якому обчислювальному пристрої. Різновиди Linux перебувають на п'ятій позиції в Китаї, Росії та Україні. У США це програмне забезпечення втратило популярність і здало позиції. Якщо в квітні 2018 року його рейтинг становив 0,9%, то в квітні 2019 року Linux став використовуватися на 0,74% пристроїв в Америці.

Операційна система, це комплекс програм, за допомогою яких здійснюється управління ресурсами комп'ютера, ноутбука або будь-якого іншого гаджета. З огляду на статистичні дані, лідируючою в мобільному секторі по використанню операційною системою є Android, тоді як домінуючою настільною платформою визнана Windows.

Інформаційні джерела

1. https://marketer.ua/ua/stats-operating-system-2017/
2. https://marketer.ua/ua/stats-operating-system-2020/

Напрям 13

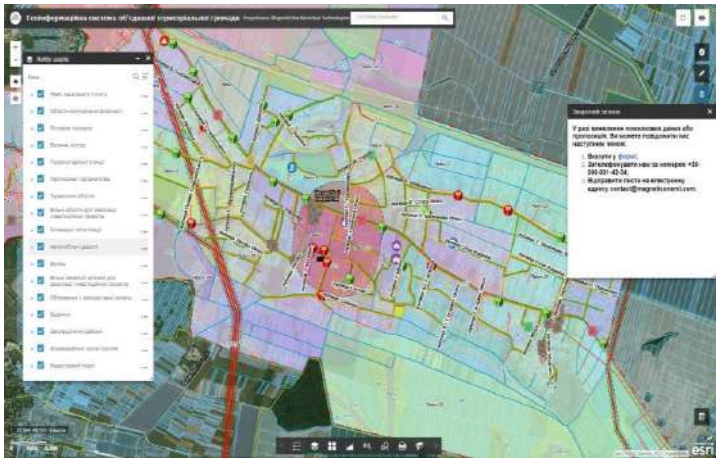
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ ПРОЕКТАМИ

УДК 004.03

MAGNETICONE MUNICIPAL TECHNOLOGIES

Богданов О.С,Семеренко Д.І., Малець І.О.
Львівський державний університет безпеки життєдіяльності, Львів

Діяльність **компанії MagneticOne Municipal Technologies** спрямована на підвищення ефективності роботи органів державної влади та місцевого самоврядування, галузевих господарств та звичайних громадян шляхом впровадження сучасних геоінформаційних технологій. **Стратегічна мета компанії** – широке впровадження геоінформаційних систем (ГІС) в усі сфери життя суспільства, господарства, бізнесу та влади з метою науково та економічно обґрунтованих управлінських рішень.



Основним принципом роботи компанії є відкритість співпраці та взаємодії з організаціями, які спеціалізуються на геоінформаційному моделюванні та веб-картографії. Виходячи з цього принципу компанія MagneticOne Municipal Technologies реалізує партнерську програму, за-

прошуючи до співпраці передові колективи та організації, зацікавлені у використанні даних геоінформаційного моделювання, реалізації спільних взаємовигідних проектів.

Пріоритетні напрямки діяльності MagneticOne Municipal Technologies:

– розробка та комплексне впровадження муніципальних геоінформаційних систем та геопорталів відкритих даних для забезпечення публічності та прозорості влади;

– створення спеціалізованих ГІС та мобільних картографічних додатків для забезпечення комфортності управління природними ресурсами та оперативності у прийнятті рішень щодо їх раціонального використання;

– надання інформаційної підтримки прийняття рішень в області екологічної безпеки населення та попередження надзвичайних ситуацій через впровадження муніципальних ситуаційних центрів на базі ГІС;

– розробка інструментів інвентаризації проблемних ділянок муніципалітету, ядром якої слугує потужна геоінформаційна платформа.

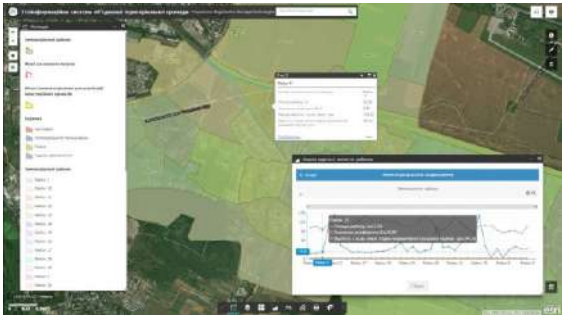
Продуктова лінійка компанії MagneticOne Municipal Technologies спрямована на вирішення завдань:

1. Позитивного результату у сфері стратегічного містобудівного планування досягайте шляхом використання муніципальних ГІС, спеціалізовані рішення яких чітко відповідають потребам міст, залежно від їх розміру.Впроваджуйте муніципальну ГІС та синхронізований з нею мобільний картографічний додаток для отримання регламентованого доступу до достовірних та актуальних даних міста, при цьому витрачаючи набагато менше часу на їх пошук, ана- ліз та узагальнення.

2.Подолання проблем, пов'язаних із прогнозуванням напрямків розвитку міської інженерної інфраструктури, ефективним менеджментом комунального господарства та управлінням інвестиційними проектами через впровадження відповідних картографічних веб-ресурсів. Такі ГІС-продукти сприятимуть автоматизації повсякденної роботи фахівців, якості наданих ними послуг, знижуватимуть ризики, в тому числі пов'язані з безпекою працівників комунальних служб.

3.Вирішення питання нераціонального управління природними ресурсами. Впровадження ГІС для водного та лісового кадастру дозволяє полегшити та автоматизувати роботу, істотно розширити можливість обробки великих об'ємів даних, отримувати кількісну та якісну інформацію про природні ресурси чи явища, недоступні під час польових досліджень.

4.Забезпечуйте функцію інформаційної підтримки прийняття рішень в області екологічної безпеки життєдіяльності населення, запобігайте виникненню надзвичайних ситуацій природного і техногенного характеру. Розроблені ГІС-продукти акумулюють в собі найсучасніші технологічні рішення і слугують інноваційною стратегією цивільного захисту, де акцент робиться на ранньому попередженні надзвичайних ситуацій та миттєвому реагуванні на них на основі моніторингу та картографічній візуалізації просторових даних через муніципальний ситуаційний центр.



5.Система спеціально розроблених для аудиту міського середовища мобільних картографічних додатків оснащених потужною ГІС-платформою покликані інвентаризувати проблемні ділянки муніципалітету (ями на дорогах, відсутність пішохідних переходів і люків оглядових колодязів, місця несанкціонованого складування сміття та вирубки дерев тощо). Система опитування мобільного додатку дозволяє місцевій владі у зручній для користувачів (аудиторів та громадян) формі оприлюднювати інформацію про діяльність міських комунальних служб та отримувати зворотній зв'язок від населення про якість наданих послуг.

Інформаційні джерела

1.uk.wikipedia.org
2.https://www.dsns.gov.ua/
3.https://zakon.rada.gov.ua/
4.https://czu.dsns.gov.ua/

УДК: 004.03

ДОСЛІДЖЕННЯ НЕОБХІДНОСТІ ПРОЕКТУВАННЯ ДОВІДКОВО-АНАЛІТИЧНОЇ СИСТЕМИ ОПТИМІЗАЦІЇ ГОСПОДАРСЬКИХ ОПЕРАЦІЙ ДЛЯ ВИРОБНИКІВ СІЛЬСЬКОГОСПОДАРСЬКОЇ ПРОДУКЦІЇ

Гончарук А.Г., Дереза О.О.
Таврійський державний агротехнологічний університет ім. Дмитра Моторного, м. Мелітополь

В роботі розглядаються питання присвячені аналізу існуючих проблем у галузі сільського господарства. Надано обґрунтування актуальності проектування сучасної довідково-аналітичної системи оптимізації господарських операцій для виробників сільськогосподарської продукції.

Ключові слова: *агропромисловий комплекс (АПК), автоматизована система, система автоматизації, програмний продукт, електронно-обчислювальна машина (ЕОМ).*

This paper considers the issue devoted to the analysis of the existing problems in agriculture. Courtesy justify the relevance of modern design reference and analysis system for optimization of business operations of agricultural producers.

Key words: *agro-industrial complex (AIC), automated system, automation system, software product, electronic computer.*

Однією з проблемних ситуацій в АПК є невисока оперативність та, в деякій мірі, мала ефективність схвалюваних управлінських рішень щодо розрахунків собівартості виконання певних робіт – в тому числі і розрахунку затрат на оптимізацію господарських операцій. Доволі часто загально прийняті норми щодо виробництва сільськогосподарської продукції, недостатнього відповідають вимогам, ухваленим законодавством України в ДСТУ. Основою цього в більшості є людський фактор, що виражається в допущенні певних помилок в процесі діяльності. Через це виникає пряма необхідність до створення автоматизованих систем, які забезпечать певну відповідність вимогам розрахунку та виконання робіт установлених законодавством, що полегшить діяльність людей в цій сфері.

На основі досліджень, які стосувались вивчення існуючих в нашій країні систем для автоматизованої оптимізації розрахунку витрат на сільськогосподарські операції, потрібно зазначити, що інформаційні системи цього типу постійно зазнають динамічних змін і мають свої вузькогалузеву направленість, а тому дуже часто лише частково задовольняють можливість розра-хунку оптимізації господарських операцій для виробників сільсько-господарської продукції.

Розглянемо існуючі українські системи оптимізації витрат на сільськогосподарські операції.

1. Програма «Dixi - рослинництво 3.02». Є потужним засобом, що дозволяє за короткий час розробити технологічні карти для господарства, підібрати машинно-тракторний парк, спланувати витрати і прибуток, порівняти різні варіанти і вибрати рішення, близькі до оптимального. В даний час реалізовані завдання розробки технологічних карт, аналіз машинно-тракторного парку та аналіз економічної ефективності.

2. Комплекс «АГРО». Створений для підтримки прийняття рішень щодо застосування контрзаходів при веденні сільськогоспо-дарського виробництва на забрудненій території. Програмний комплекс «АГРО» вирішує такі проблеми:

– визначення оптимального комплексу контрзаходів, спрямованих на виробництво екологічно чистої продукції в господарствах, які постраждали в результаті аварії на ЧАЕС;

– прогнозування забруднення товарної сільськогосподарської продукції;

– прогнозування врожаю;

– оцінки рентабельності виробництва.

Для побудови відповідних систем необхідно заздалегідь перед-бачити технологію та середовище програмування, щоб в подальшому саме з цього боку не було певних обмежень щодо вирішення питань автоматизації сільськогосподарського виробництва.

Технології для розробки систем потребують певних ресурсів, а також може виникати складність щодо інсталяції готового прикладного рішення на комп'ютери користувачів, оснащених різним технічним та програмним забезпеченням. Виникає необхідність використовувати технологію та середовище програмування, яка б забезпечила технічну підтримку від виробника та якість самої технології. Однією із таких технологій є «Microsoft Visual Studio» - одне з найпоширеніших сучасних середовищ розробки, яке доцільно розглядати в якості платформи для розробки системи розрахунку.

На основі аналізу існуючих проблем обґрунтувати необхідність створення програмного забезпечення, що дає можливість автоматизувати оптимізацію господарських операцій для сільськогосподарських підприємств. Метою статті є також викладення та аналіз технічних аспектів при створенні подібної системи розрахунку та її впровадження.

Автоматизовані системи дозволяють фахівцям виконувати основні функції з високою надійністю та мінімумом(або без) проміжних документів. Наприклад, довідково-аналітична система оптимізації господарських операцій для виробників сільськогосподарської продукції забезпечує оперативний вибір найбільш оптимального варіанту сівозміни, виходячи з затрат до наявних площ, їх розмірів, агрономічних властивостей ґрунту, планових завдань по виробництву різних видів сільськогосподарської продукції, використання добрив, пестицидів та інших чинників [3].

Аналізуючи сутність систем автоматизування, фахівці визначають їх як професіонально-орієнтовані малі обчислювальні системи, розташовані безпосередньо на робочих місцях фахівців і призначені для автоматизації їх робіт.

Слід передбачити відповідні особливості систем автоматизації в залежності від області застосування. Але принципи створення для такого програмного забезпечення повинні бути загальними: надійність, наявність певної візуальної структури, гнучкість, ефективність. Згідно із приведених у літературі вимог щодо систем розрахунку, програмні продукти, що класифікують як системи автоматизації (або автоматизовані системи) в цій галузі повинні відповідати наступним основним вимогам [2]:

– своєчасне виконання інформаційної і обчислювальної задачі.
– простота роботи, надійність і легкість в обслуговуванні.
– можливість роботи у складі обчислювальної мережі.
– швидка робота і в суворій відповідності до Держстандарту.
– врахування специфіки, створення галузевих версій.

Висновки. Перед початком проектування системи виконується ознайомлення та аналіз технічного завдання на проектування та існуючих систем автоматизації роботи сільськогосподарських організацій; визначення пріоритетів та можливих складностей. Розглянуті вище вимоги охоплюють усі можливі напрямки використання та створення автоматизованих систем

в сільсько-господарській промисловості. Опис базових вимог для вітчизняних систем автоматизації сільськогосподарської діяльності доводять, що незалежно від професійної спеціалізації подібна система буде доречна практично в кожному із напрямків діяльності сільського господарства, в тому числі й під час оптимізації сільськогосподарських операцій.

Інформаційні джерела

1. ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення.
2. Інтернет ресурс http:// uk.wikipedia.org/
3. Інформаційні технології управління: Навч. посібник / Під ред. Тіторенко Г. А. - М.: ЮНИТИ-ДАНА, 2002. - 280 с.

УДК 004.002

ОСОБЛИВОСТІ РОЗРОБКИ АВТОМАТИЗОВАНИХ СИСТЕМ ПРОЕКТУВАННЯ НА ОСНОВІ СИСТЕМОТЕХНІЧНОЇ ДІЯЛЬНОСТІ

Мацулевич Ю.О., Антонова Г.В.
Таврійський державний агротехнологічний університет ім. Дмитра Моторного, м. Мелітополь

В роботі розглядається питання вирішення системотехнічних задач при розробці автоматизованих систем проектування.
Ключові слова: *системотехніка, складні технічні системи (СТС), системотехнічна діяльність (СТД), система автоматизованого проектування (САПР), оптимізація, метасистема.*

The paper considers the issue of solving system problems in the development of automated design systems.
Key words: *system engineering, complex technical systems (STS), system technical activity (STD), computer - aided design (CAD) system, optimization, metasystem.*

В розвитку теорії і практики автоматизованого проектування можна виділити дві взаємозв'язані тенденції:

1. Зростання числа об'єктів проектування, що є складними технічними виробами;

2. Перехід від автоматизації окремих процедур або етапів проектування до створення інтегрованих САПР, що охоплює весь процес проектування виробів або навіть всю діяльність проектно- конструкторського підрозділу.

У зв'язку з цим виникає необхідність розглядати автоматизовану систему проектування як складну технічну систему, що включає в свій склад різнорідні, але взаємозв'язані компоненти. В створенні таких систем бере участь декілька колективів розробників, чия діяльність повинна бути скоординована на користь розробки ефективної системи. Але досягнення високого рівня ефективності і якості неможливе без цілеспрямованої і добре організованої діяльності за рішенням виникаючих в процесі проектування системотехнических задач.

В даний час ведуться роботи по трьох взаємозв'язаних напрямах:

1. Розвиток системного підходу – конкретно-методологічної позиції, пов'язаної з цілісним розглядом складної технічної системи і принципів її створення і функціонування.

2. Розробка комплексної науково-технічної дисципліни, частиною системного аналізу, та частиною, що об'єднує принципи, методи і засоби аналізу і організації процедури дослідження і проектування складних технічних систем.

3. Системотехнічна діяльність, направлена на організацію створення, використовування і розвиток конкретної складної технічної системи, забезпечення інтеграції частин системи в єдине ціле.

В роботі розглядаються задачі системотехнічної діяльності при розробці автоматизованих систем проектування.

В процесі створення автоматизованих систем проектування залежно від стадії життєвого циклу об'єкту дослідження можна виділити різні види системотехнічної діяльності, які направлено на розробку методології і організацію процесу створення САПР. До них можна віднести:

1. Проектування складного технічного виробу.

2. Отримання оптимальних рішень в рамках окремої підсистеми.

3. Забезпечення створення САПР з необхідним рівнем ефективності і якості за рахунок координації із загальносистемних позицій процесів розробки підсистем.

Процес проектування САПР має структуру, обумовлену структурою об'єкту проектування.

Для його реалізації необхідна проектна організація, що володіє рисами складної системи, яку по відношенню до проектованої САПР назвемо *метасистемой.* Метасистема повинна забезпечувати здійснення всього життєвого циклу САПР, включаючи не тільки її проектування, але і виготовлення, настройку експлуатацію, модернізацію. У зв'язку з цим для забезпечення ефективності створюваної САПР системотехнічна діяльність охоплює як питання оптимальної інтеграції частин САПР в єдине ціле, так і питання, пов'язані з введенням в процес проектування єдиного організуючого початку. Воно необхідне для дозволу суперечності між необхідністю створення єдиного злагодженого проекту САПР і участю в проектуванні великого числа фахівців - проектувальників. В загальному виді його можна сформулювати як суперечність між цілісністю САПР і складністю її метасистеми. Дозвіл цієї суперечності здійснюється в рамках системотехнічної діяльності, основним призначенням якої є забезпечення функціонування метасистеми як єдиного цілого на користь створення і експлуатації ефективної САПР.

Для забезпечення функціонування метасистеми в рамках системотехнічної діяльності необхідно вирішити дві комплексні задачі:

1. Представлення результатів попередніх етапів процесу проектування, одержаних іншими проектувальниками, у вигляді, достатньому для продовження процесу проектування.

2. Забезпечення взаємодії колективів проектувальників на користь створення єдиного злагодженого проекту САПР.

Єство системотехнічної діяльності при розробці автоматизованих систем проектування визначається наявністю суперечності між необхідністю створення працездатної і ефективної системи і участю в цьому процесі різних розробників, що спеціалізуються у відповідних наочних областях.

В основі системотехнічної діяльності лежить концепція цілісності створюваної системи, що вимагає її цілісного опису. Він забезпечується сукупністю певних видів і форм представлень системи, віддзеркалення різних груп її властивостей з різним ступенем конкретизації і формалізації.

Інформаційні джерела

1. Норенков И.П. Основы автоматизированного проектирования. М. Издательство МГТУ им. Баумана, 2002 – 334с.

2. Разработка САПР. В 10 книгах под редакцией Петрова А.В. – М. Высшая школа 1990 – 143с.

3. Щербина В.М., Холодняк Ю.В., Івженко О.В. Впровадження комп'ютерної графіки в навчальний процес при підготовці фахівців інженерних спеціальностей /Удосконалення освітньо-виховного процесу в закладі вищої освіти. Випуск 24 / Збірник науково-методичних праць / ТДАТУ, - Мелітополь: ТДАТУ, 2020.

4. Холодняк Ю.В., Гавриленко Є.А., Івженко О.В., Найдиш А.В. Технологія моделювання поверхонь складних технічних виробів за заданими умовами / Праці Таврійського державного агротехнологічного університету, Вип. 19(2), С. 257-263

5. Мацулевич О.Є., Щербина В.М. Використання пакету прикладних програм NETCRACKER // Фундаментальна підготовка фахівців у природничо-математичній, технічній, агротехнологічній та економічній галузях : матеріали Всеукраїнської наук.-практ. конференції з міжнар. участю (Мелітополь, 11-13 вересня 2017 р.) : присвяченої 85-річчю кафедри вищої математики і фізики ТДАТУ.

6. Мацулевич О.Є., Щербина В.М., Коломієць С.М. Геометричне моделювання складних тривимірних поверхонь із застосуванням матричного рівняння еліптичного повороту // / Праці Таврійського державного агротехнологічного університету, Вип. 19(2), С. 294-303

7. Мацулевич О.Є., Зінов'єва О.Г. Розв'язання задач аналізу трендсезонних часових рядів / Праці Таврійського державного агротехнологічного університету, Вип. 19(2), С. 264-270

8. Корчинський В.М., Свинаренко Д.М., Мацулевич О.Є. Методи підвищення інформаційних показників багатоспектральних зображень на основі ортогоналізації даних / Праці Таврійського державного агротехнологічного університету, Вип. 14(2), 2014, С. 264-270.

9. Мацулевич О.Є., Зінов'єва О.Г. Розв'язання задач аналізу трендсезонних часових рядів / Праці Таврійського державного агротехнологічного університету, Вип. 19(2), С. 264-270

10. Мацулевич О.Є., Щербина В.М. Функції та принципи тестового контролю знань студентів /Праці Таврійського державного агротехнологічного університету// Збірник науково-методичних праць/ Таврійський державний агротехнологічний університет – Мелітополь, 2014 - С.160-164

УДК 004.413

ПЕРЕВАГИ ВИКОРИСТАННЯ AGILE-МЕТОДОЛІГОЇ ПІД ЧАС РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В УМОВАХ СУЧАСНОГО РИНКУ

Кордунова Ю.С., Придатко О.В., Смотр О.О.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі проведений узагальнений аналіз основних методологій розробки програмного забезпечення на підставі чого розроблені рекомендації щодо їх використання в умовах сучасного ринку.
Ключові слова: *каскадна модель управління проєктами, Agile-методологія.*

The paper describes the main methodologies of software development, according to this developed recommendations for their use in today's market.
Keywords: *waterfall model, Agile- methodology.*

Одним із ключових моментів у досягненні успіху в процесах створення нового продукту є правильний вибір методології управління. Не виключенням стали і проєкти розробки програмного забезпечення. До недавнього часу більшості компаніям були доступні інструменти та активно використовувались каскадні моделі управління проєктами [1, 2], які, на перший погляд, здавались ідеальними. Ідеальність в першу чергу досягалась за рахунок їх простоти як у розумінні так і у інтеграції у виробничі процеси. Даний спосіб управління передбачає чітке планування, яке супроводжується суворою документацією. Проте, проєкти, реалізація яких заснована на використанні традиційних моделей, сьогодні є не найоптимальнішими, особливо, коли річ іде про управління змінами, довготривалу реалізацію проєкту та швидку зміну потреб ринку. Велика кількість проєктів зазнала краху через суворі вимоги, неефективне планування, нездатність команди адаптуватися до змін, що зумовлене використанням каскадних моделей.

На зміну традиційним моделям управління проєктами у 2001 році прийшла Agile-методологія. Свій початок вона бере саме з IT-сфери, хоча сьогодні активно використовується у більшості галузей із використанням проєктного підходу. Основною Agile-підходу є гнучка методологія розробки програмного забезпечення, яка базується на ітеративному виконанні проєкту. Увесь процес розробки виконується серією коротких ітерацій, які складаються із планування, реалізації, перевірки та оцінки. За умови ітеративного підходу замовник після кожної ітерації має можливість ознайомитись із певною частиною функціоналу програмного продукту, за бажання внести корективи або зміни у наступну ітерацію. В цьому закладена основна цінність гнучких методологій розробки програмного забезпечення – готовність до змін, можливість швидко реагувати на виклики ринку та розбиття ризиків на окремі ітерації. Agile-підхід робить акцент на людській співпраці та комунікації, готовності до змін

та роботі на результат. У Agile-проєктах немає місця надлишковій документації та довгостроковому плануванню [3–5].

Таким чином можна зробити висновок, що вибір методології управління є дуже важливим для реалізації успішного проєкту. В сучасному світі технології та бажання замовника змінюються настільки швидко, що гнучкість – це основна перевага розробки на основі Agile-підходу. Лише ті команди, які можуть іти в ногу з часом, які працюють на результат та на задоволення потреб замовника залишатимуться конкурентно-спроможними на сучасному ринку.

Інформаційні джерела

1. Пятенко С. В. Методы анализа наиболее типичных проблем управления проектом / С. В. Пятенко [Електронний ресурс]. – Режим доступу: https://iteam.ru/publications/project/section 35/article 2808

2. A guide to the Project Management Body of Knowledge. PMBOK guide SIXTH EDITION – USA: Project Management Institute, 2017.

3. Agile-маніфест розробки програмного забезпечення [Електронний ресурс] – Режим доступу до ресурсу: https://agilemanifesto.org/iso/uk/manifesto.html.

4. Постигая Agile. Ценности, принципы, методологии – Москва: Манн, Иванов и Фербер, 2017.

5. Analyzing Agile Development – from Waterfall Style to Scrumban. // Informatica Economică. – 2016. – №4. – С. 5–14.

УДК 004.032.8

ПОБУДОВА БАГАТОШАРОВОГО ДОКУМЕНТУ З ВИКОРИСТАННЯМ МУЛЬТИМЕДІЙНИХ ТЕХНОЛОГІЙ

Носань С.В., Антонова Г.В.
Таврійський державний агротехнологічний університет ім. Дмитра Моторного, м. Мелітополь

У статті розглядається побудова багатошарового документу, розміщення порядку шарів, статистичних зображень, футожів фільмів, роликів та переходів, рендерінг результату.

Ключові слова: *багатошаровий документ, рендерінг, футаж, статистичні зображення.*

The article considers the construction of a multilayer document, placement of the order of layers, statistical images, footage of films, videos and transitions, rendering the result.

Keywords: *multilayer document, rendering, footage, statistical images.*

В сучасному суспільстві потік інформації зростає що митті. Психологи відкрили, що найбільш ефективно запам'ятовується інформація у вигляду фільму, подвижна динамічна. До розробки посібників користувача, відео курсів, інструкції налаштування програмного продукту, презентації нового виробу необхідно залучати мультимедійні технології.

Мультимедійні технології включають в себе усі технології роботи зі звуком, формування статичних зображень, програми перетворення звуку до цифрового вигляду, програми обробки відеофайлів, програми захопленя екрану. Сьогодні за рахунок мультимедійних технологій є можливість виготовити фільм за яким завгодно сценарієм. Єдине обмеження це потужність комп'ютерних систем. За рахунок комп'ютерних систем студенти які пройшли даний курс зможуть виготовити рекламний ролик підприємства, чи мультимедійне керівництво користувача.

Пропонується розвинути ідеї викладання предмету «Мультимедійні технології» через розробку багатошарового документу- невеликого відео курсу на задану тему.

Самостійна робота це найбільш важлива частина учбового курсу. Студент на основі навичок які получив за час виконання лабораторних робіт розробляє кінцевий продукт, який має цінність.

Найбільш трудомістка частина, це підготовка состав них частин відеокурсу. Він складається з статичних зображень, відеороликів, та музикального супроводження.

У програмі Adobe PhotoShop будуть розроблені статичні зображення, файли у форматі jpg.:

– заставка студії – zastavka;

– логотип студії – logotip;

– прикраса екрану – ukrach;

– фамілія та посада диктора – familia_diktor.

За допомогою технічних заходів получаємо файли:

– диктор знятий на синьому чи зеленому фоні, розповідаючи про предмет, та про виконання лабораторної роботи – diktor.avi;

– взятий з архіву файл з водоспадами, лісом, та інше – priroda.avi;

– файл, який получили за рахунок захоплення екрану при виконані лабораторної роботи – zachop.avi.

Мета самостійного завдання: при запуску avi-файлу з'являється заставка студії, після цього диктор розповідає про предмет, потім з'являється вікно з роботою програми і диктор розповідає про роботу програми.

Методика зборки відеокурса в програмі Adobe Preimire Pro. У цій програмі ми встановлюємо потрібну ієрархію файлів, справа в тому, що самий нижний файл являється базовим і не має ключів прозорості. Можлива установка 98 шарів в одному файлі проекту.

Виходячи з цього робимо наступне:

1. Беремо файл логотипу, розтягуємо, або встановлюємо час 10 секунд

2. Ставимо файл priroda.avi на перший рівень між логотипом і файлом з природою ставимо ефект взаємне проникнення.

3. На другий доріжці встановимо diktor.avi, застосовуючи ефекти з ключами прозорості для синього або зеленого кольору.

4. На третій доріжці встановлюємо logotip, додаємо позиціонування і розтягуємо картинку на весь ролик

5. На четвертій доріжці встановлюємо прикраса(ukrac), приміром із запчастин.

6. Файл відео захоплення розміщуємо на п'ятій доріжці, визначаємо розмір для даного зображення і позиціонування поруч з диктором.

Даний файл розміщуємо на три хвилини після початку роботи файлу з диктором. Для нього встановлюємо файл посилення на шостий доріжці встановлюємо рядок з заставкою імені, прізвища диктора, ключами посилення й ослаблення ми періодично домагаємося появи підпису з ім'ям диктатора, проводимо рендеринг, оцифровку файлу і отримуємо результуючий фільм.

Рис. 1. Загальний вигляд кадру відео курсу

Інформаційні джерела

1. Кузнецов И. Создание фильма на компьютере. Технология и творчество. / Кузнецов И., Познин В. //- Мн.: Харвест, 2007.- 512 с.

2. Днепров А. Видеосамоучитель – монтаж домашнего видео в Adobe Premiere Pro CS3./ Днепров А. //.- Мн.: Харвест, 2002.- 416 с.

3. Борзенко А.Е., Федоров А.Г. Мультимедиа для всех. / Борзенко А.Е., Федоров А.Г //– М.: КомпьютерПресс, 2007.

4. Кречман Д., Мультимедиа своими руками. / Кречман Д., Пушков А. //– СПб.: БХВ – Санкт-Петербург, 1999.

5. Рош Уинн Л. Библия мультимедиа./ Рош Уинн Л. // – К.: ДиаСофт, 1998.

УДК 514.18

РОЗРОБКА КОНЦЕПЦІЇ НАВЧАЛЬНОГО ОНЛАЙН РЕСУРСУ ДЛЯ КУРСУ «ОСНОВИ 3Д МОДЕЛЮВАННЯ»

Ризавський К. Є., Мартин Є. В.
Львівський державний університет безпеки життєдіяльності

У сучасних реаліях світу усе більшого поширення набувають онлайн курси та дистанційні заняття. В першу чергу, звісно, таке поширення завдячується вимушеному карантину, у зв'язку з яким більшість навчальних закладів різного рівня акредитації змушені зачинити свої двері для усіх, хто має відношення до навчального процесу (як студентів, так і викладачів). Саме у зв'язку із цим нами були розроблені методичні матеріали з тривимірного моделювання на базі Autodesk 3Ds Max [1,2,3,4]. Розглянемо основні положення пропонованого концепту навчального онлайн ресурсу, в якому ці матеріали знайдуть практичне втілення.

Перш за все слід відмітити, що концепт має спрощений візуальний вигляд для демонстративності та зручності користування – кольорова гамма та фактичний вигляд вікон спрощений, а функціонал та інші можливості в процесі розроблення можуть дещо змінюватись та доповнюватись.

Розглянемо основний функціонал навчального онлайн ресурсу для курсу «Основи 3 д моделювання», виходячи з аналізу сучасних графічних редакторів для реалізації можливостей ілюстративної комп'ютерної графіки.

Досвід вивчення навчальної дисципліни «Основи 3 д моделювання» показує, що найкращий спосіб навчити теорії - це дати якісну практику, саме тому в основі навчальних матеріалів лежать:

1) лекційні матеріали, що заточені на практику, тобто при поясненні тих чи інших інструментів наводиться приклад їх фактичного застосування;

2) практичні матеріали, що викладені у покроковій формі;

3) відео матеріали, що в демонстраційній покроковій манері роз'яснюють методичні матеріали для тих, хто краще сприймає звукову інформацію, ніж текстову;

4) демонстрація в базовому курсі саме тих графічних інструментів та функцій, які необхідні для подальшого вивчення дисципліни та одержання практичних навичок роботи у середовищі Autodesk 3Ds Max.

Навчальний курс пропонуємо розділити на два **рівні,** а саме - **базовий** та **розширений**. У базовому рівні будуть розглянуті власне ті матеріали, які описані вище. У свою чергу розширений рівень буде ознайомлювати користувачів зі складнішими функціями, як от наприклад робота з розгортками та V-ray текстурами.

Пропонуємо ознайомитись з концептом робочого вікна ресурсу відповідно до рис.1. Зазначимо, що пропонований концепт поданий у викляді Web сторінки. А, отже. користування з ним не повинно викликати жодних ускладнень.

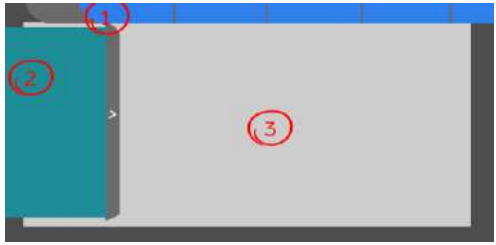


Рис. 1.Зовнішній вигляд концепту навчального ресурсу.

Розроблюваний ресурс буде мати темну тему як основну, щоб менше навантажувати очі користувача, а число меню пропонується мінімальним.

Розглянемо функціонал (див. рис.1):

1) у верхній стрічці буде розміщуватись головне меню з кнопками
-“головна”,
- “зворотній зв’язок”,
-“курси”,
-“пошук”,
- форма реєстрації, щоб користувач міг легко запам’ятовувати свій навчальний прогрес;

2) ліворуч знаходиться випадне меню, яке дозволить зручно переміщатись між різними курсами;

3) тут знаходиться основне робоче поле, де і пропонується розташування усіх навчальних матеріалів.

Інформаційні джерела

1. Рижавський К. Є. Комп'ютерні графічні технології у підготовці фахівців технічного спрямування/ К. Є. Рижавський, Є. Є. Мартин, О. В. Придатко // Сучасні проблеми моделювання. Наук. фах. видання. – Мелітополь.: Видавництво Мелітопольського державного педагогічного університету імені Богдана Хмельницького, 2016. – С.130-137.

2. Рижавський К. Є. Використання анімації у просторовому моделюванні пожежної техніки / К. Є. Рижавський, Є. Є. Мартин, О. В. Придатко // Зб. доп. VI Всеукр. наук.-практ.конф. студентів, аспір-антів та молодих вчених».-К.: НТУУ «КПІ», 2017. – С. .228-231.

3. Рижавський К. Є. Розроблення твердо тільної моделі пожежного автомобіля/ К. Є. Рижавський ,Є. Є. В. Мартин, О. В. Придатко // Проблеми та перспективи розвитку забезпечення безпеки життєдіяльності. Зб. м-лів Міжн. наук.– практ. конф. курсантів і студентів.- Л.:ЛДУБЖД,2017. – С.61-62.

4. Рижавський К. Є. Дослідження характеристик та принципів роботи інформаційного програмного забеспечення / К. Є. Рижавський, Є. Є. Мартин // Захист інформації в інформаційно-комунікаційних системах. Зб. М-лів Міжвуз. наук.-практ. конф. студентів і курсантів.– Л.:ЛДУБЖД,2017.

Напрям 14

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

УДК 37.01

МЕТОДИ ВИКЛАДАННЯ ІНОЗЕМНОЇ МОВИ В НЕМОВНИХ ЗВО ІЗ ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УМОВАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

Лупаца С., Мельник В.
Львівський державний університет внутрішніх справ, м. Львів

У статті розглядаються сучасні методи навчання іноземної мови в немовних закладах вищої освіти із застосуванням інформаційних технологій як ефективного засобу їх впровадження. Комп'ютерне тестування, аудіомовний та аудіолінгвістичний методи не є їх повним переліком, але можуть ефективно доповнити традиційні методи викладання іноземних мов в немовних ЗВО в умовах дистанційного навчання.

Ключові слова: *інформативні технології, комп'ютерне тестування, методи викладання, дистанційне навчання.*

The article deals with modern methods of teaching a foreign language in non-language institutions of higher education with the use of information technology as an effective means of their implementation. Computer-based testing, audio-language and audio-linguistic methods are not a complete list of them, but they can effectively complement traditional methods of teaching foreign languages in the conditions of distance learning.

Keywords*: information technologies, computer testing, teaching methods, distance learning.*

Основною метою викладання іноземної мови в професійних цілях в немовних закладах вищої освіти є формування комунікативних компетентностей у галузі майбутньої спеціалізації - навичок та вмінь висловлюватися усно та письмово як частина професійного предмету, опановуючи необхідну термінологію. При цьому питання використання інформаційних технологій залишається не достатньо розкритим та визначеним в сучасній лінгвістичній науці.

Одним із завдань викладача іноземної мови в немовних закладах вищої освіти є знайти шляхи вдосконалення методології застосування нових методів навчання. Слід зазначити, що інформаційні технології виступають ефективним засобом впровадження сучасних методів навчання іноземної мови в немовних закладах вищої освіти [2].

Зокрема, це стосується комп'ютеризованих тестів, застосування яких у викладанні мови в немовних ЗВО може допомогти організувати процедуру скринінгу та оцінювання та покращити процес навчання.

Варто відзначити, що основні переваги комп'ютерного тестування є наступними:

– відсутність фактора суб'єктивності при перевірці тестів;

– можливість швидкого редагування та поповнення банку тестових завдань;

– скорочення часу, проведеного під час тестування;

– широке коло завдань, що дає студентам можливість навчатися самостійно (система доступу до мережі).

Провідні напрями сучасних досліджень проблем комп'ютерних методів тестування в немовних закладах вищої освіти полягають у розробці комп'ютерного дистанційного тестування; створенні банків тестових завдань і програм; інтерпретація результатів комп'ютерних тестів у системі моніторингу навчального процесу; проблематика дидактики ІТ-мови і застосування комп'ютерних тестів при викладанні іноземних мов; алгоритми і методи підготовки до комп'ютерних тестів.

Комп'ютерні тести можна вважати одним із сучасних методів навчання іноземної мови. Цей метод не скасовує індивідуальний внесок викладача в організацію та контроль навчального процесу, але допомагає вдосконалити його, автоматизувати систему оцінки та контролю знань та підвищити її якість.

Ефективність у використанні комп'ютерного тестування ставить перед викладачем проблему розробки та наукового обґрунтування теоретичної моделі тестування, яка є її основним елементом. Однак, існують певні проблеми з ефективним застосуванням та впровадженням комп'ютерних тестів в університетах, зумовлені різними факторами: матеріальна база університету, розробка прозорої системи застосування цього методу тощо [1].

Комп'ютерні технології можна використовувати не тільки для контролю знань, але і задля їх поглиблення. Створення спеціальних програм, що формують мовні компетенції студентів у професійній галузі, використання Інтернету в навчальному процесі, розробка проєктів, презентації з використанням комп'ютерних технологій та Інтернет-ресурсів допоможуть мотивувати та зацікавити студентів у вивченні іноземних мов. Обговорення

матеріалу, підготовленого студентом із використанням Інтернету, дискусії та рольові ігри сприятимуть ефективному розвитку навичок монологічного та діалогічного мовлення в немовних закладах вищої освіти.

Аудіомовний метод можна використовувати одночасно з іншими методами викладання іноземної мови в професійних цілях. Цей метод можна ефективно вдосконалити за допомогою комп'ютерних технологій (розробка комп'ютерних програм для вивчення іноземної мови на основі аудіомовного методу). Мова повсякденного спілкування - основа аудіомовного методу. Рівень складності мовлення підбирається таким чином, щоб учні почали вивчати мову з простих форм.

Основними елементами аудіомовного методу є ситуативні діалоги, мова повсякденного спілкування, акцент на мовленні, акцент на запам'ятовуванні, рольові ігри, створення діалогів, хорові та індивідуальні повтори, читання та письмо для кращого запам'ятовування тощо.

Аудіолінгвістичний метод спонукає студентів до комунікативної мови. Нова лексика та структури представлені через діалоги та тексти, наслідування та повторення. Навчання базується на зразках, представлених у діалогах та текстах. Граматика стимулюється прикладами, чіткі граматичні правила не рекомендуються. Культурна інформація контекстуалізується в діалогах та текстах або подається викладачем. Читання та письмо спирається на попередні усні роботи.

Важливо урізноманітнити викладання іноземних мов, моделюючи ситуації, близькі до реальних, в яких студенти змогли б використовувати набуті знання та вміння в закладах вищої освіти. Для досягнення позитивного результату, використання різних методів навчання іноземної мови повинно супроводжуватися індивідуальним психолого-педагогічним підходом з урахуванням індивідуальних особливостей кожного учня та всієї групи.

Отже, зазначені вище методи викладання іноземної мови із застосуванням сучасних інформаційних технологій не є їх повним переліком, але можуть ефективно доповнити традиційні методи викладання іноземних мов в немовних закладах вищої освіти в умовах сьогодення [3].

Інформаційні джерела

1. Зубов А.В., Зубова И.И. Информационные технологии в лингвистике. М.: Академия, 2019. 144 с.

2. Подопригорова Л.А. Использование Интернета в обучении иностранным языкам /Иностранные языки в школе. 2013. № 5. С. 25-31.

3. Інформаційні технології сьогодення. Режим доступу: http://uk.wikipedia.org/wiki/Інформаційні_технології.

УДК 004.932.72

АВТОМАТИЗАЦІЯ РОБОТИ НАВЧАЛЬНОГО ЗАКЛАДУ ПРИ ДИСТАЦІЙНОМУ НАВЧАННІ

Валієва К.Р., Івженко О.В.
Таврійський державний агротехнологічний університет ім. Дмитра Моторного, м. Мелітополь

Робота присвячена розробці комплексу програм для автоматизації робочого та навчального процесу навчальних закладів. Розроблено та реалізовано програмне забезпечення для роботи з документацією, розписом занять та ведення обліку при дистанційному навчанні.

Ключові слова: *інформаційні технології, навчальні програми, мережа, оперативна документація, освіта.*

The work is dedicated to the development of complex software to automate the process of training and educational institution. Develop and implement software to work with the documentations , schedule and record keeping.

Key words: *information technologies, educational programs, network, operative documentation, education.*

У структуру змісту комп'ютерної технології (комп'ютерної грамотності) входять:

– знання основних понять інформатики й обчислювальної техніки;

– знання принципового обладнання й функціональних можливостей комп'ютерної техніки;

– знання сучасних операційних систем і володіння їх основними командами;

– знання сучасних програмних оболонок і операційних засобів загального призначення і володіння їх функціями;

– володіння хоча б одним текстовим редактором;

– первісні вистави про алгоритми, мови й пакетах програмування;

– первісний досвід використання прикладних програм утилітарного призначення.

Зовсім унікальні можливості для діалогу студента з наукою й культурою представляє всесвітня комп'ютерна мережа Internet:

– переписка-розмова з однолітками із усіх частин миру;

– залучення наукової й культурної інформації із усіх музеїв, сховищ миру;

– інтерактивне спілкування.

Одним з напрямків інформаційно-комунікаційних технологій є використання аудіо-відеозасобів [1-3]. Тому поряд з комп'ютерними технологіями говоримо про технології навчання, у яких значна частина керування

пізнавальною діяльністю студентів здійснюється за допомогою спеціально розроблених аудіовізуальних навчальних матеріалів.

Комбінація комп'ютерних навчальних програм з телекомунікаційною мережею є різновидом дистанційного навчання (навчання на відстані).

Є декілька програмних систем, які використовуються для автоматизації управління навчальним закладом. Більша частина таких систем підтримує тільки певний набір функцій, пов’язаних з управлінням навчальним закладом, має певну структуру даних, яка не дозволяє забезпечити горизонтальний (від одного закладу до іншого) та вертикальний (інформація для органів управління освітою на рівні міста, області, держави) обмін даними.

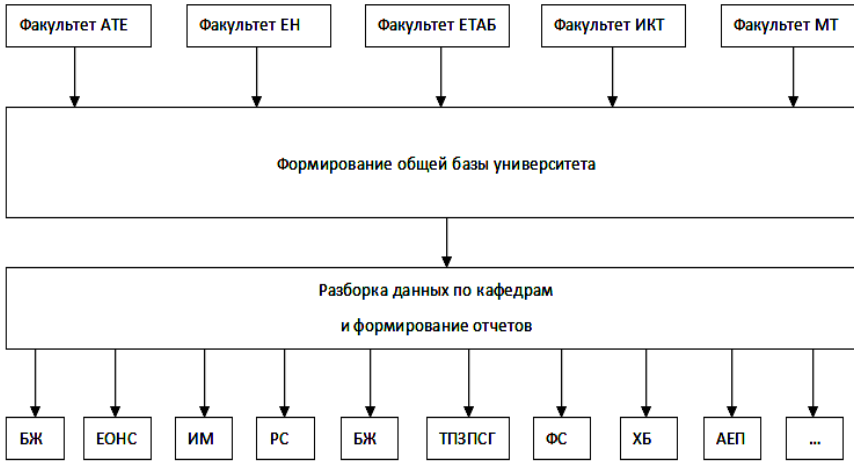


Рис. 1. Структурна схема автоматизації роботи
навчального відділу ТДАТУ

Використання засобів ІКТ в організації та плануванні діяльності навчального закладу [4, 5] має певні переваги, а саме:

– підвищення ефективності навчального процесу;

– можливість управління з використанням результатів попередньої діяльності;

– прийняття більш ефективних управлінських рішень;

– підвищення об’єктивності в оцінці діяльності педагогів та студентів;

– більш ефективне управління пізнавальною діяльністюстудентів;

– можливість прийняття більш виважених рішень, які стосуються підвищення результативності навчання;

– оперативний доступ до організаційної інформації стосовно діяльності освітнього закладу;

– економія як матеріальних, так і людських ресурсів;

– вільний час на вирішення важливих питань;

– скорочення обсягу рутинної роботи.

Значним кроком у розвитку засобів автоматизації роботи навчального закладу є об'єднання розрізнених інформаційно-комунікаційних систем у єдину систему документообігу.

Як приклад, представлено пропоновану систему автоматизації роботи навчального відділу ТДАТУ (рисунок 1). Системний підхід до формування єдиного електронного документообігу навчального закладу дозволить значно підвищити швидкість обробки даних, спростити доступ до різноманітної інформації та, в цілому, сприяти росту ефективності праці всіх структурних елементів навчального закладу [6].

Висновки. В роботі наведено приклад ймовірного розвитку систем автоматизації робочого та навчального процесу навчальних закладів України на прикладі розвитку системи автоматизації навчального відділу Таврійського державного агротехнологічного університету імені Дмитра Моторного.

Інформаційні джерела

1. Дік Н. Ф. Працюєм по новому.— К.: «Світ», 2005. — 282 с.

2. Єрмолова А.І. Методологія роботи— К.: «Світ», 1999. — 135с.

3. Мацулевич О.Є., Зінов'єва О.Г. Розв'язання задач аналізу тренд-сезонних часових рядів / Праці Таврійського державного агротехнологічного університету, Вип. 19(2), С. 264-270

4. Мацулевич О.Є., Щербина В.М. Використання пакету прикладних програм NETCRACKER/ Фундаментальна підготовка фахівців у природничо-математичній, технічній, агротехнологічній та економічній галузях : матеріали Всеукраїнської наук.-практ. конференції з міжнар. участю (Мелітополь, 11-13 вересня 2017 р.) : присвяченої 85-річчю кафедри вищої математики і фізики ТДАТУ

5. Мацулевич О.Є., Щербина В.М. Функції та принципи тестового контролю знань студентів /Праці Таврійського державного агротехнологічного університету// Збірник науково-методичних праць/ Таврійський державний агротехнологічний університет – Мелітополь, 2014 - С.160-164

6. Корчинський В.М., Свинаренко Д.М., Мацулевич О.Є. Методи підвищення інформаційних показників багатоспектральних зображень на основі ортогоналізації даних / Праці Таврійського державного агротехнологічного університету, Вип. 14(2), 2014, С. 264-270.

УДК 519.85

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ РОЗВ'ЯЗАННІ ТРАНСПОРТНИХ ЗАДАЧ

Валієва К.Р., Бондаренко Л.Ю.
Таврійський державний агротехнологічний університет ім. Дмитра Моторного, м. Мелітополь

В статті пропонується методика розв'язання транспортної задачі за допомогою пакету Maple.
Ключові слова: *прикладні програми, транспортна задача, комп'ютерні технології.*

The article offers a method of solving a transport problem using the Maple package.
Keywords: *applications, transport task, computer technology.*

В наш час персональні ЕОМ широко впроваджуються в науку, техніку, економіку, і, звісно, в процес освіти. Багато професій, також і в економіці, потребують знань, вмінь та навичок, пов'язаних з задачами оптимізації. А вміння розв'язувати ці задачі із застосуванням комп'ютера робить їх більш ефективним. Майбутні фахівці повинні вміти користуватися готовими пакетами прикладних програм, застосовувати їх до розв'язання оптимізаційних задач. До таких пакетів відноситься пакет символьної математики Maple, який не потребує знання складних алгоритмічних мов, не передбачених для студентів економічних спеціальностей, та дозволяє реалізовувати складні алгоритми розв'язків. Пакет Maple містить необхідний набір функцій, що спрощує розв'язок задачі оптимізації.

Для розв'язання оптимізаційних задач можна використовувати табличний процесор Microsoft Excel, а саме програмну надбудову «Поиск решения» [3, 4].

Програмний пакет Maple можна використовувати для перевірки вже отриманих студентами результатів розв'язку задач оптимізації.

Транспортна задача є важливою частиною загальної задачі лінійного програмування.

Постановка задачі: визначення оптимального плану перевезень деякого однорідного вантажу з m пунктів відправлення $A_1, A_2, ..., A_m$ в n пунктів призначення $B_1, B_2, ..., B_n$. При цьому, у якості критерію оптимальності виступає або мінімальна вартість перевезень усього вантажу, або мінімальний час його доставки.

Математична постановка задачі:

$$F = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} x_{ij} \to \min \qquad (1)$$

при умовах $\sum_{i=1}^{m} x_{ij} = b_j \ \left(j = \overline{1,n}\right)$, $\sum_{j=1}^{n} x_{ij} = a_i \ \left(i = \overline{1,m}\right)$, $x_{ij} \geq 0 \ \left(i = \overline{1,m}; j = \overline{1,n}\right)$, де c_{ij} – тарифи перевезення одиниці вантажу з *i*-го пункту відправлення до *j*-го пункту призначення; a_i – запаси вантажу в *i*-ому пункті; b_j – потреби вантажу в *j*-ому пункті; x_{ij} – кількість одиниць вантажу, перевезеного з *i*-го пункту відправлення до *j*-го пункту призначення.

На практичному занятті пропонується розв'язати наступну задачу.

На трьох складах оптової бази зосереджений однорідний вантаж в кількості 450, 300 та 400 одиниць ($a_i = (450, 300, 400)$), цей вантаж необхідно перевезти до чотирьох пунктів призначення. Кожний з пунктів призначення повинен отримати відповідно 240, 300, 295, 245 одиниць вантажу ($b_j = (240, 300, 295, 245)$). Тарифи перевезень з кожного з складів до всіх пунктів призначення задані матрицею:

$$C = \begin{pmatrix} 5 & 4 & 6 & 7 \\ 3 & 8 & 9 & 10 \\ 8 & 11 & 7 & 12 \end{pmatrix}$$

Необхідно знайти план перевезень з найменшими транспортними витратами.

За допомогою пакету Maple розв'язуємо задачу лінійного програмування:

```
> with(simplex);
Warning, new definition for maximize
Warning, new definition for minimize
```

[basis, convexhull, cterm, define_zero, display, dual, feasible,maximize, minimize, pivot, pivoteqn, pivotvar, ratio, setup,standardize]

```
> minimize(F,{sum(x[1,j],j=1..5)=450,sum(x[2,j],
j=1..5)=300,sum(x[3,j],j=1..5)=400,sum(x[i,1],i=1..3)=240,sum(x[i,2],i=1..
3)=300,sum(x[i,3],i=1..3)=295,sum(x[i,4],i=1..3)=245,sum(x[i,5],i=1..3)=70},N
ONNEGATIVE);
```

{*x*[1, 1] = 0, *x*[3, 1] = 0, *x*[2, 2] = 0, *x*[1, 3] = 0, *x*[2, 3] = 0, *x*[3, 2] = 0, *x*[2, 1] = 240, *x*[1, 4] = 150, *x*[3, 3] = 295, *x*[2, 5] = 0, *x*[3, 5] = 70, *x*[3, 4] = 35, *x*[1, 2] = 300, *x*[2, 4] = 60, *x*[1, 5] = 0}

Матричний вигляд отриманого розв'язку:

```
> v:=matrix([[0,300,0,150,0],[240,0,0,60,0],
[0,0,295,35,70]]);
```

$$v := \begin{bmatrix} 0 & 300 & 0 & 150 & 0 \\ 240 & 0 & 0 & 60 & 0 \\ 0 & 0 & 295 & 35 & 70 \end{bmatrix}$$

Мінімальна вартість перевезень:
> sum(sum(C[i,j]*v[i,j],i=1..3),j=1..5);
6055

Висновки. Запропонована методика розв'язання транспортної задачі лінійного програмування є ефективним способом отримання оптимального розв'язку, який не потребує громіздких обчислень. Застосування пакету Maple підвищує у студентів цікавість до вивчаємого предмету та зменшує час на засвоєння матеріалу.

Інформаційні джерела

1. Манзон Б.М. Maple V Power Edition – М.: Информационно-издательский дом «Филинъ», 1998. – 240 с.
2. Прохоров Г.В., Колбеев В.В., Желнов К.И., Леденев М.А. Математический пакет Maple V Release 4, - 1998
3. Гельман В. Я. Решение математических задач средствами Excel. СПб.: Питер, 2003. - 240 с.
4. Дубіна А., Орлова С., Шубіна І., Хромова А. Excel для экономистов и менеджеров. - СПб.: Питер, 2004. - 295 с.
5. Акулич И.Л. Математическое программирование в примерах и задачах: Учеб. Пособие для студентов эконом. Спец. Вузов. - М.: Высш. шк., 1986. - 319 с.

УДК 004.92:001.893.54:629.783.085

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ МОДЕЛЮВАННЯ ПРОЦЕСУ ВИВЕДЕННЯ РАКЕТОЮ-НОСІЄМ СУПУТНИКА НА ЗАДАНУ ОРБІТУ

Бублій В. Е.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Розглянуто основні моменти моделювання процесу виведення ракетою-носієм супутника на задану орбіту та труднощі їх програмування.
Ключові слова: *ракета-носій, моделювання, програмування, орбіта.*

The main points of modeling the process of launching a satellite into a given orbit and the difficulties of their programming are considered.
Key words: *lander, modeling, programming, orbit.*

Програмне забезпечення для моделювання польоту ракет в свій час дало можливість не тільки моделювати різні ситуації без самого запуску носія, що істотно прискорило прогрес ракетобудування, але і суттєво зни-

зило вартість польоту не в останню чергу через економію палива. В наш час моделювання стає все точнішим та достовірнішим завдяки зростанню обчислювальних потужностей, що відкриває все нові і нові можливості.

Здешевлення польотів стало можливим за рахунок знаходження близької до ідеальної траєкторії за рахунок моделювання. В сучасних моделях обов'язково враховуються усі фізичні параметри, які діють на ракету [1] (прискорення земного тяжіння, щільність атмосфери та ін.) та їх зміна моделюється через функцію часу, також модель повинна враховувати і обертання навколо центра мас самої ракети.

Данна наукова робота була зосереджена на найважчих для моделювання так званих управляючих параметрах(ті що використовуються для корування ракетою), тобто нахил рулів, кут сопла маршового двигуна, потужність тяги маневрових двигунів та ін. Складність полягає як в дуже точному заданні параметрів, наприклад, для введення тіла на орбіту йому треба задати швидкість близько 7,91 км/с. Тобто, мінімальне відхилення моделі від реальних параметрів може призвести до похибки в кілька тисяч кілометрів [2], що може призвести до тяжких наслідків(наприклад, сходження в щільні шари атмосфери з подальшим руйнуванням конструкції). Інша складність полягає в можливості зміни цих параметрів не лінійно, наприклад, після завершення подачі палива на двигун він не одразу ж перестає давати тягу, що доволі важко розрахувати, потрібні реальні стендові випробування для отримання даних параметрів, лише після цього їх можна буде коректно запрограмувати.

Саме програмування відбувалося на мові C# [3] - це сучасна і доволі швидка мова програмування, яка була обрана за сукупністю параметрів, що дозолило зробити програму доволі точною, швидкою та легкою до змін та розширення функціоналу(був використаний об'єктно-орієнтований підхід та принципи SOLID).

Інформаційні джерела

1. Вопросы построения программной траектории выведения ракеты-носителя с космическим аппаратом [Електронний ресурс] – https://elar.urfu.ru/bitstream/10995/4645/2/urgu1170s.pdf

2. Управление вектором тяги жидкостного ракетного двигателя Космической ступени ракеты-носителя при возникновении массовой асимметрии [Електронний ресурс] – https://core.ac.uk/download/pdf/87400035.pdf

3. Документация по C# [Електронний ресурс] – https://docs.microsoft.com/ru-ru/dotnet/csharp/

УДК 004.421

АНАЛІЗ АМПЛІТУДНО-ЧАСТОТНИХ ХАРАКТЕРИСТИК ЗА ДОПОМОГОЮ ПРОГРАМИ SPECTROID

Варениця А., Лясковська С. Є.
Національний університет «Львівська політехніка», м. Львів

Перевірка і налагоджування багатьох радіотехнічних пристроїв, їх окремих трактів і вузлів прискорюється та полегшується при можливості спостереження на екрані приладу амплітудно-частотних характеристик. Щоб проаналізувати якість звуку динаміка розглянемо наступні його характеристики. Підсилювач звукових частот – це пристрій що підсилює малопотужні електричні сигнали звукового діапазону (від 20 Гц до 20 кГц, що відповідає діапазону чутих людиною акустичних коливань) до рівня, необхідного для роботи акустичної системи. Основні параметри підсилювачів звуку:

– амплітудно-частотна характеристика;
– відношення сигналу до шуму;
– рівень нелінійних спотворень;
– рівень інтермодуляції спотворень;
– номінальна потужність;
– максимальна потужність;
– опір акустичних систем (зазвичай 4 або 8 Ом).

Основним елементом підсилювача є транзистор (рис. 1).

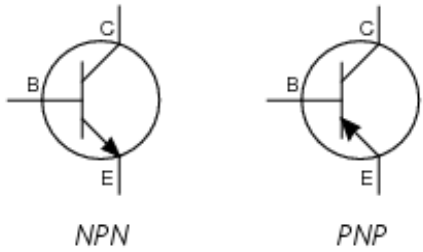
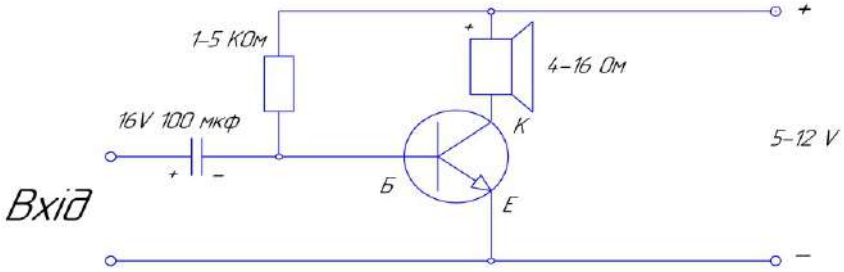


Рис.1. Схематичне позначення транзистора

Транзистор — напівпровідниковий елемент, який дозволяє керувати струмом, що протікає крізь нього, за допомогою зміни вхідної напруги або струму, поданих на базу,або інший електрод. На рис. 2. представлено найпростіший підсилювач на транзисторі КТ 805 БМ.

Одним із важливих параметрів для підсилювачів звуку є амплітудно-частотні характеристики. Автоматичне формування амплітудно-частотних характеристик (АЧХ) забезпечується за допомогою ЧМ-генераторів спеціального типу – генераторів коливної частоти (ГКЧ), що працюють парале-

льно з осцилографічними індикаторами. ГКЧ являє собою джерело напруги постійної амплітуди, частота якої періодично і плавно змінюється в заданій смузі частот. В даній роботі досліджено амплітудно частотні характеристики динаміка (8 Ом, 35 ГДН) з використанням сервісу Spectroid і виконано дослід вимірювання АЧХ для динаміків. Даний сервіс допомагає аналізувати звуковий спектр в реальному часі з роздільною здатністю частоти по всьому спектру частот.



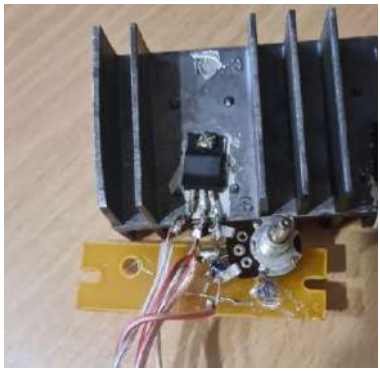


Рис. 2. Найпростіший підсилювач на транзисторі КТ 805 БМ

Послідовність виконання даного досліду:

1. Завантажити програму Spectroid на телефон.
2. Підключити звуковідтворювальний динамік до комп'ютера через підсилювач звуку.
3. Увімкнути на пристрої білий шум.
4. Увімкнути на телефоні програму Spectroid.
5. Отриманий графік зберегти за допомогою скріншота.

На рис. 3 продемонстровано зображення АЧХ (червона лінія на графіку) для трьох видів динаміків (*а* -низькочастотний динамік, *б* - середньочастотний динамік, *в* - високочастотний динамік), зображення отримані з використанням програми Spectroid.

Spectroid реагує на звук і відображає криву АЧХ, результатом якої є характер звучання колонок. Варто відзначити, що чим далі телефон знаходиться від джерела відтворення, тим більше коригувань в звук вносять резонанси кімнати. Працюючи з цими даними, можливо знайти оптимальне місце для установки акустики і точки прослуховування, орієнтуючись на отримання, більш прямої червоної лінії в програмі. Чим рівніше результат вимірів АЧХ, тим більш лінійний звук.

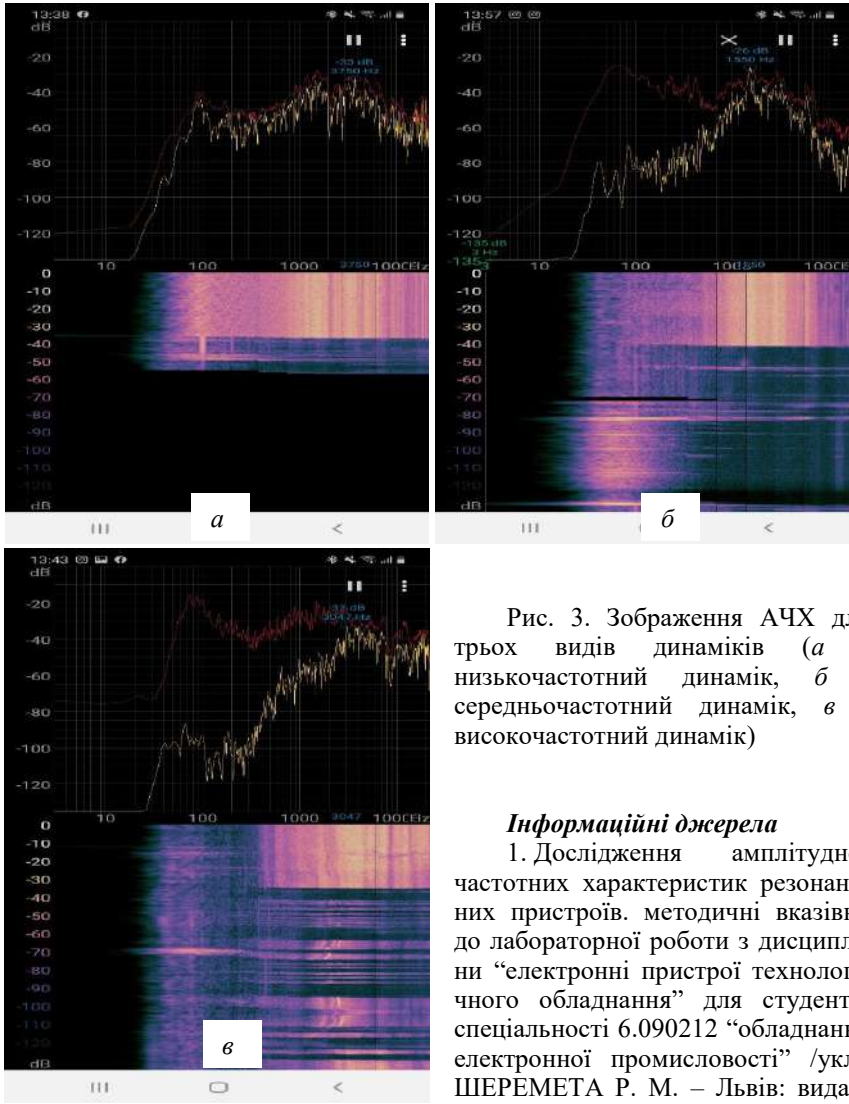


Рис. 3. Зображення АЧХ для трьох видів динаміків (*а* - низькочастотний динамік, *б* - середньочастотний динамік, *в* - високочастотний динамік)

Інформаційні джерела

1. Дослідження амплітудно-частотних характеристик резонансних пристроїв. методичні вказівки до лабораторної роботи з дисципліни “електронні пристрої технологічного обладнання” для студентів спеціальності 6.090212 “обладнання електронної промисловості” /укл.: ШЕРЕМЕТА Р. М. – Львів: видавництво національного університету “Львівська політехніка”, 2002. – 10 с.

2. https://www.youtube.com/watch?v=X40eKEIDaHA

УДК: 378.02

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТНЬОМУ ПРОЦЕСІ

Мечус Х.В.[1], Малець О.-С. І.,[2] Борзов Ю.О.
[1]Львівський державний університет безпеки життєдіяльності
[2]Львівський національний університет ім. Івана Франка

Розглянуто роль та застосування інформаційних технологій у сучасній освіті. Проведено аналіз переваг та недоліків використання дистанційного навчання для підготовки та здобуття відповідного фаху.

Ключові слова: *інформаційні технології, освіта, дистанційне навчання, on-line, off-line, заняття.*

Інформаційні технології все більше захоплюють наше життя. Замовлення їжі, таксі, побутових товарів та навіть питної води – міцно осіли в наших смартфонах. Завдяки інформаційним технологіям зараз працюють цілі заводи, літають гелікоптери та проектуються будинки.

Не оминула інформатизація й освіту. Використання мультимедійних дошок, планшетів, комп'ютерних класів безперечно вплинули на освітній процес. Однак на це потрібно дивитись значно глибше.

Якщо говорити про Україну, часто ми бачимо як навчальні заклади обладнують мультимедійним обладнанням, новими комп'ютерними класами, планшетами.

Але чи дає це можливість максимально ефективно використовувати технології в освіті та отримувати необхідні для сучасного розвинутого світу навички та уміння?

У сучасному світі активно розвивається система дистанційного навчання в самих різних галузях освіти. Тепер вже не є проблемою отримання повноцінної освіти практично в будь-якій галузі, дистанційно в умовах браку часу. Але, як будь-яке інше навчання, воно має як позитивні, так і негативні сторони.

Зручність і переваги дистанційного навчання перед іншими формами навчання.

Можливість навчатися в будь-який час. Студент, який навчається дистанційно, може самостійно вирішувати, коли і скільки часу протягом семестру йому приділяти на вивчення матеріалу. Він будує для себе індивідуальний графік навчання. Деякі освітні установи надають своїм студентам можливість відкладати навчання на тривалий термін і повертатися до нього без необхідності знову оплачувати освітні послуги.

Можливість навчатися в своєму темпі. Студентам при дистанційному навчанні не потрібно турбуватися про те, що вони відстануть від своїх однокурсників. Завжди можна повернутися до вивчення більш складних

питань, кілька разів подивитися відео-лекції, перечитати переписку з викладачем для успішного проходження проміжних і підсумкових атестацій.

Можливість навчатися в будь-якому місці. Студенти можуть вчитися, не виходячи з дому чи офісу, перебуваючи в будь-якій точці світу. Щоб приступити до навчання, необхідно мати комп'ютер з доступом в Інтернет. Відсутність необхідності щодня відвідувати навчальний заклад – безсумнівний плюс для людей з обмеженими можливостями здоров'я, для проживаючих в важкодоступних місцевостях, які відбувають покарання в місцях позбавлення волі, батьків з маленькими дітьми.

Мобільність. Зв'язок з викладачами, репетиторами здійснюється різними способами: як on-line, так і off-line. Проконсультуватися за допомогою електронної пошти іноді ефективніше і швидше, ніж призначити особисту зустріч при очному або заочному навчанні.

Навчання в спокійній обстановці. Проміжна атестація студентів дистанційних курсів проходить в формі on-line тестів. Тому у студентів менше приводів для хвилювання перед зустріччю з викладачами на заліках та іспитах. Виключається можливість суб'єктивної оцінки: на систему, яка перевіряє правильність відповідей на питання тесту, не вплине успішність студента з інших предметів, його суспільний статус і інші фактори.

Зручність для викладача. Вчителі, репетитори, викладачі, що займаються педагогічною діяльністю дистанційно, можуть приділяти увагу більшій кількості учнів і працювати, перебуваючи, наприклад, в декретній відпустці.

Індивідуальний підхід. При традиційному навчанні викладачеві досить важко приділити необхідну кількість уваги всім студентам групи, підлаштуватися під темп роботи кожного. Використання дистанційних технологій підходить для організації індивідуального підходу. Студент сам вибирає собі темп навчання, він може оперативно отримати у тьютора відповіді на всі запитання.

Але, зрозуміло, поряд з перевагами дистанційне навчання має і недоліки.

Необхідна сильна мотивація. Практично весь навчальний матеріал студент-дистанційник освоює самостійно. Це вимагає достатньої сили волі, відповідальності і самоконтролю. Швидше за все, ніхто його підганяти чи заохочувати до навчання не стане. Підтримувати потрібний темп навчання без контролю з боку вдається не всім.

Нестача практичних вмінь та навичок. Досить проблемно якісно організувати дистанційне навчання за напрямами підготовки та спеціальностями, на яких передбачена велика кількість практичних занять.

Дистанційна освіта не підходить для розвитку комунікабельності. При дистанційному навчанні особистий контакт студентів один з одним і з викладачами мінімальний, а то і цілком відсутній. Тому така форма на-

вчання не підходить для розвитку комунікабельності, впевненості, навичок роботи у команді.

У зв'язку із теперішньою ситуацією у країні дистанційне навчання має великі перспективи, тому що виправдовує себе і є дійсно зручним. Дана форма навчання інноваційна, але вже зараз дистанційне навчання набуває своїх послідовників. Система дистанційного навчання побудована з урахуванням всіх тонкощів і нюансів, щоб забезпечити максимальну ефективність і користь навчання і в той же час, забезпечити зручність її використання.

Інформаційні джерела

1. Биков В. Ю. Дистанційне навчання в країнах Європи та США і перспективи для України
2. https://www.dli.donetsk.ua/news/2020-06-04-3
3. https://works.doklad.ru/view/aB103dgV6x8.html

УДК 004.891.2

ЗАСТОСУВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В ОСВІТІ

Мічурін І.
Харківський національний університет радіоелектроніки, м. Харків

Проаналізовано практичне застосування штучного інтелекту у галузі освіти.
Ключові слова: *штучний інтелект, освіта, навчання.*

Analyzed the practical application of artificial intelligence in education.
Keywords: *artificial intelligence, education, study.*

Вступ. У наш час технології штучного інтелекту застосовуються практично в кожній галузі. Вони дозволяють підвищувати продуктивність праці людини, швидко та ефективно аналізувати великі обсяги інформації. Крім цього, системи штучного інтелекту здатні виконувати значну кількість дій для збільшення ефективності процесу навчання, що дозволяє покращити рівень підготовки учнів та студентів під час здобуття ними освіти.

Застосування систем штучного інтелекту в освіті. Системи штучного інтелекту в освіті вже застосовуються у Сполучених Штатах Америки, Китайській Народній Республіці, Австралії тощо. У США однією з найбільш популярних систем штучного інтелекту є McGraw Hill's ALEKS, що використовується для навчання й оцінювання учнів під час виконання шкільних і домашніх завдань. Учні починають з оцінювання в системі ALEKS для вимірювання їх рівня знань за рядом предметів. Далі, коли учень переходить в режим навчання, система використовує отримане оці-

нювання для коригування програми навчання з метою усунення прогалин в знаннях [1]. У Китаї після кількох років активних інвестицій у галузь штучного інтелекту було досягнуто стану, коли десятки мільйонів учнів в процесі свого навчання використовують його у тій чи іншій формі. Одним з прикладів такого застосування є Squirrel AI, що дозволяє виявляти слабкі сторони учнів і складати індивідуальний навчальний план таким чином, щоб заповнити виявлені прогалини. Учні можуть пройти тест, який допомагає виявити, які з підтем при вивченні дисципліни даються їм найбільш важко. Технології штучного інтелекту використовуються для виявлення зв'язків між різними темами і використанням цих зв'язків при побудові індивідуальної програми навчання. Наприклад, програма виявляє пов'язані теми, які так само можуть потребувати додаткової уваги та визначає, в якому порядку та за допомогою яких практичних завдань тому чи іншому учню буде легше освоїти потрібний матеріал. Перш за все ця система застосовується у позашкільному репетиторстві [2]. В Австралії було створено Deakin Genie – розумного персоналізованого цифрового асистента, що відповідає на будь-яке питання щодо навчального процесу в університеті. Він дозволяє підвищити інформованість студентів про їх оцінки, список завдань й проектів та їх терміни виконання тощо [3].

Висновки. Штучний інтелект може ефективно застосовуватися для вирішення завдань сучасної освіти, його ефективність у цій діяльності є високою. Варто сподіватися на те, що в майбутньому можна очікувати суттєве збільшення рівня знань випускників шкіл та університетів завдяки застосуванню штучному інтелекту.

Інформаційні джерела

1. Штучний інтелект та освіта. Сьогодні і завтра. / Портал видавничої групи Основа. URL: http://osnova.com.ua/news/1916-Штучний_інтелект_та_освіта._Сьогоді_і_завтра (дата звернення: 11.11.2020).

2. Шкільна освіта в добу штучного інтелекту / Український тиждень. URL: https://tyzhden.ua/Science/233609 (дата звернення: 11.11.2020).

3. Віртуальні школи й Siri для студентів: як штучний інтелект змінює освіту. / Inspired. URL: https://inspired.com.ua/creative/technology/virtualni-shkoly-j-siri-dlya-studentiv-yak-shtuchnyj-intelekt-zminyuye-osvitu/ (дата звернення: 11.11.2020).

УДК 004

ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В КОНТЕКСТІ ДИСТАНЦІЙНОГО НАВЧАННЯ СТУДЕНТІВ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Пранничук О., Шаповал Д., Кордунова Ю.
Львівський державний університет безпеки життєдіяльності, м. Львів

В сучасному суспільстві інформаційно-комунікаційні технології (ІКТ) займають важливу ланку у життєдіяльності людей. Вони роблять товари і послуги більш доступними, а процес обміну інформацією - більш швидким. ІКТ торкається всіх сфер життєдіяльності людини, але, мабуть, найбільший вплив вони мають на освітній процес, адже відкривають нові можливості методів викладання та навчання. Зміна освітньої системи, на основі ІКТ призвела до появи відкритої системи освіти, віртуальних університетів та, відповідно, нової форми навчання - дистанційної. У роботі розглянуто особливості дистанційної форми навчання, проаналізовано основні переваги і недоліки та застосування її у сучасних реаліях.

Під дистанційним навчанням розуміється індивідуалізований процес набуття знань, умінь, навичок і способів пізнавальної діяльності людини, який відбувається в основному за опосередкованої взаємодії віддалених один від одного учасників навчального процесу у спеціалізованому середовищі, яке функціонує на базі сучасних психолого-педагогічних та інформаційно-комунікаційних технологій [1]. Відповідно, його метою є надання освітніх послуг шляхом використання у навчанні сучасних ІКТ. Це, в свою чергу, передбачає доступ до інтернету, відповідне апаратне та програмне забезпечення в усіх учасників освітнього процесу. Також, не варто забувати, про відповідний рівень знань та навичок у користуванні цими інформаційно-комунікаційними технологіями у викладачів та студентів.

Зрозуміло, що для того, щоб вивести дистанційне навчання на належний рівень потрібен час, досвід та матеріальні ресурси. На відміну від зарубіжних країн, де дистанційна освіта стоїть поряд із традиційною, в Україні така форма навчання лише розвивається, проте вже й активно застосовується. До переваг дистанційної форми навчання можна віднести: вільний вибір закладу вищої освіти (як на території держави, так і за її межами); не перешкоджає основному типу діяльності студента; надає можливість самостійно планувати час навчання; забезпечує студентів з обмеженими можливостями гідними умовами, для отримання повноцінної освіти; доступ до програм найкращих університетів і викладачів світу, найновіша інформація та технології.

Проте, ця форма освіти має і свої недоліки. Зокрема, це: брак досвіду викладачів та студентів у роботі в режимі онлайн; відсутність належного

фінансування, апаратного та програмного забезпечення для дистанційної роботи, забезпечення доступу до Internet мережі у викладачів та студентів; відсутність комунікації, візуального контакту викладача і студента; неможливість відпрацювання практичних занять у спеціалізованих навчальних лабораторіях/центрах.

Таким чином, можна зробити висновок, що інформаційно-телекомунікаційні технології відкривають перед викладачами та студентами цілого світу велику кількість можливостей. Дистанційне навчання, не зважаючи на ряд недоліків – це майбутнє нашої освіти, комунікації із світом та неперервний розвиток.

Інформаційні джерела

1. Положення про дистанційне навчання (Затверджено наказом Міністерства освіти і науки України 21.01.2004 № 40) [Електронний ресурс] Режим доступу до ресурсу: http://zakon4.rada.gov.ua/laws/show/z0703-13#n18

2. Токарук Н. С. Сучасні аспекти дистанційного навчання/ Н. С. Токарук, Р. З. Ган, О. Г. Попадинець, М. І. грищук, Т. Л. Котик // Актуальні питання піжвищення якості освітнього процесу : Науково-методична конференція з міжнародною участю, 18 вересня 2020 р., м. Івано-Франківськ, Україна : зб. Наук. Праць. – Івано-Франківськ, 2020. – С. 64.

УДК 004.003

АВТОМАТИЗАЦІЯ УПРАВЛІННЯ ОРГАНІЗАЦІЇ НАВЧАЛЬНОГО ПРОЦЕСУ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

Райта Д., Борзов Ю.
Львівський державний університет безпеки життєдіяльності, м. Львів

В роботі проведений узагальнений аналіз інформаційних систем, що використовуються у закладах вищої освіти, та розроблені рекомендації щодо автоматизації управління організації навчального процесу в навчальних закладах.
Ключові слова: *організація навчального процесу, SRM.*

The paper provides a generalized analysis of information systems used in higher education institutions, and developed recommendations for automating the management of the educational process in educational institutions.
Keywords: *Organization of the educational process, SRM.*

В даний час істотний вплив в сфері освіти є здатність ефективно управляти навчальним процесом, ресурсами та даними закладу вищої освіти (далі ЗВО) в умовах дистанційного навчання.

У цьому полягають особливості управління організації навчального процесу в постійно мінливих та нестабільних умовах змішаної системи навчання.

Актуальним є автоматизація навчання ЗВО з використанням інноваційних інструментів. Проводиться огляд особливостей управління з використанням системи Student Relationship Management (далі SRM): огляд можливостей, переваг і можливих ризиків, пов'язаних з його використанням.

Інформаційні системи, що використовуються у закладах вищої освіти, підтримують, по суті, процеси академічного управління, такі як реєстрація студентів, управління студентами, оцінки студентів тощо. Ці системи не дозволяють ретельно контролювати навчальну діяльність студентів, оцінювати їх академічний успіх та підтримувати навчальну діяльність, пов’язану з викладанням та проведенням консультацій. З іншого боку, загальновизнано, що існує сильний взаємозв'язок між пильним моніторингом діяльності студентів та ефективності їхнього навчання. Для підтримки процесів навчання та навчання важливим є набуття узагальнених знань про студентів та стану перебігу їхнього навчання. Ці знання дозволять прийняти адекватні та ефективні дії / рішення для пильного відстеження навчальної діяльності студентів. Для того, щоб такі процедури були можливими, нами пропонується використовувати систему управління взаємовідносинами зі студентами SRM.

Дана система підтримуватиме концепцію SRM та практику SRM і буде впроваджена з використанням концепцій та технологічної інфраструктури, що підтримує системи бізнес-аналітики. Основною метою є забезпечення технологічного інструменту, що підтримує студентів закладу вищої освіти у отриманні знань, що мають важливе значення для процесу прийняття рішень.

Інформаційні джерела

1. Борзов Ю. Особливості застосування комп'ютерного моделювання для покращення навчального процесу / Ю. Борзов, Р. Головатий, Я. Магеровський. // Інформаційні технології розвитку змісту освіти. – 2019. – С. 80–81.

2. Зачко О.Б., Головатий О.Р. Мультиагентна модель управління безпекою при плануванні проектів створення об'єктів з масовим перебуванням людей. Стратегічне управління, управління портфелями, програмами та проектами. 2017. № 2 (1224). С. 46–51.

3. Придатко О.В., Ренкас А.Г. Дослідження ефективності та аспекти впровадження інтерактивних засобів навчання в організацію навчального процесу ЛДУБЖД. Збірник наукових праць Львівського державного університету безпеки життєдіяльності. Львів – 2010

4. Головатий Р.Р. Управління зацікавленими сторонами проекту безпечної експлуатації торгово-розважальних центрів // Р.Р. Головатий // III Міжнародна науково-практична конференції «Інформаційні технології та взаємодії» (IT & I) // Київ: НУ ім. Т.Г. Шевченка, 2016 – С.55 – 57

УДК 004.422.81

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ КОМП'ЮТЕРНИХ ТРЕНАЖЕРІВ У НАВЧАЛЬНОМУ ПРОЦЕСІ ПРИ ВИВЧЕННІ ТЕХНІЧНИХ ДИСЦИПЛІН

Чернобильський Д. Ю., Щербина В.М.
Таврійський державний агротехнологічний університет ім. Дмитра Моторного, м. Мелітополь

Сучасні процеси інформатизації освіти вимагають більш широкого використання інформаційних технологій у навчальному процесі. Одним із засобів практичної реалізації інформатизації є використання електронних засобів навчального призначення, зокрема комп'ютерних тренажерів. У статті розглядаються окремі теоретичні питання щодо визначення та призначення комп'ютерних навчальних тренажерів та висуваються вимоги до їх використання.

Ключові слова: *вища освіта, програмно-педагогічні засоби, комп'ютерні тренажери.*

Modern processes of informatization of education require a wider use of information technology in the educational process. One of the means of practical implementation of informatization is the use of electronic teaching aids, including computer simulators. The article considers some theoretical issues regarding the definition and purpose of computer training simulators and sets requirements for their use.

Keywords: *higher education, software and pedagogical tools, computer simulators.*

Одним з головних напрямів процесу інформатизації сучасного суспільства стає інформатизація освіти, що забезпечує широке впровадження у навчальну практику програмно-педагогічних розробок та інформаційних технологій, направлених на поліпшення процесу навчання, вдосконалення форм і методів організації навчального процесу. Одним з напрямів інформатизації освіти є використанні електронних навчальних тренажерів, які забезпечують більш якісну підготовку фахівців до майбутньої професійної діяльності.

Тренажер (від англ. train – виховувати, навчати, тренувати) – навчально-тренувальний пристрій, який імітує обставини, дії, створюючи ситуацію, наближену до реальної. У більш вузькому значенні це комп'ютерна навчальна програма для вироблення у студентів умінь і навичок певної діяльності, а також розвитку пов'язаних з нею здібностей.

Архітектура та зміст будь-якого комп'ютерного тренажеру, як і класифікація цих програмних засобів, визначається його призначенням, переліком завдань та функціональними можливостями:

1. Тренажери для розвитку моторних навичок.

2. Тренажери, які навчають розпізнаванню образів.

3. Тренажери для розвитку навичок роботи за певним алгоритмом.,

4. Тренувальні тренажери для розвинення навичок поведінки в нештатних (аварійних).

5. Тренажери, призначені для вирішення завдань з необхідністю прийняття конкретних рішень.

Комп'ютерний тренажер має забезпечувати виконання наступних функцій:

– послідовне виведення на екран завдань заданої складності з вибраної теми;

– контроль за діями користувача з розв'язання запропонованого завдання;

– миттєва реакція на неправильні дії користувача;

– виправлення помилок користувача;

– демонстрація правильного розв'язання завдання;

– виведення підсумкового повідомлення про результати роботи користувача [1].

Потреба у комп'ютерних тренажерах стрімко зростає. Комп'ютерні тренажери є необхідними у галузях людської життєдіяльності, де помилки під час навчання на реальних об'єктах можуть призвести до надзвичайних наслідків, а їх усунення – до великих фінансових витрат. Тому, використання навчальних тренажерів покращує якість та ефективність навчання; значно знижує його вартість; дає користувачам практичні навички до початку їх роботи в реальних умовах. Це, на наш погляд, забезпечить безпомилкове застосування набутих навичок при виконанні поставлених завдань.

Використання комп'ютерних тренажерів у навчальному процесі забезпечує наступні позитивні моменти:

– враховується індивідуальний темп роботи студента, який сам управляє навчальним процесом;

– скорочується час розвитку необхідних навичок;

– збільшується кількість тренувальних завдань;

– легко досягається рівнева диференціація у навчанні;

– підвищується мотивація навчальної діяльності.

Застосування сучасних інформаційних технологій, зокрема комп'ютерних тренажерів, у навчальному процесі дозволить об'єднати різні підходи для отримання найкращих результатів у навчанні. При виборі програмних засобів навчального призначення слід методично оцінити програму з погляду можливості їх використання у навчальному процесі.

До програмно-навчальних засобів висувається перелік вимог, які можна застосовувати і до навчальних тренажерів:

1. Згідно вимозі стійкості система повинна виявляти і коректувати помилки введення, що людині здаються очевидними.

2. Вимога корисності передбачає, що система повинна вміти надавати допомогу користувачеві, відображаючи на моніторі документацію, що описує її власну структуру або інструкцію користувача.

3. Вимога простоти. Система повинна звести до мінімуму введення з клавіатури команд, які необхідні для досягнення визначеної мети (тобто рішення стандартних або простих задач повинно досягатися натисканням декількох ключових клавіш).

4. Вимога зрозумілості. Система не повинна ускладнювати роботу користувачу необхідністю вибору з декількох кнопок.

5. Вимога керованості. При роботі з системою користувач завжди повинен мати можливість визначити своє місце на шляху до досягнення мети.

6. Вимога узгодженості. З погляду користувача система повинна діяти зрозуміло послідовно та логічно.

7. Вимога очевидності. Результати дій користувача завжди повинні демонструватися

8. Вимога гнучкості. Досвідчені користувачі повинні знати всі можливості системи. Всі користувачі, навіть початкового рівня, повинні мати можливість відхилятися від стандартних засобів рішення.

9. Вимога слухняності. Система повинна завжди знаходитися під керуванням користувача.

Під комп'ютерний тренажером розуміється програмний засіб для вироблення умінь і навичок з певної діяльності, а також розвитку пов'язаних з нею здібностей. Це поняття входить до більш загальних понять програмно-педагогічного засобу та електронного засобу навчального призначення, які відрізняються як за функціональними можливостями, так і за сферою застосування. Якісний тренажер повинен відповідати певним вимогам, які висуваються до програмно-педагогічних засобів та враховувати особливості навчання у певній цільовій аудиторії.

Інформаційні джерела

1. Грибова В. Концепция разработки диагностических компьютерных тренажеров на основе знаний / Валерия Грибова, Григорий Осипенков, Сергей Сова // Information science & computing. – Bulgaria. – SOFIA, 2009. – С. 27 – 33.

2. Филатова Н.Н. Мультимедиа тренажерные комплексы для технического образования / Н.Н. Филатова, Н.И. Вавилова, О.Л. Ахремчик // Educational Technology & Society. – № 6(3), 2003. – pp. 164-186.

3. Мацулевич О.Є. Методика створення імітації роботи промислових технічних виробів та систем /О.Є. Мацулевич, О.А. Ніконенко //Матеріли Всеукраїнської науково-технічної конференції магістрантів і студентів ТДАТУ (присвячується 80-річчю Запорізької області за підсумками наукових досліджень 2018 року). Факультет інженерії та комп'ютерних технологій: збірник тез доповідей (Мелітополь, 19-23 листопада 2018 р.); С. 32

УДК 519.87

РОЗВ'ЯЗАННЯ ТРАНСПОРТНИХ ЗАДАЧ ЗАСОБАМИ ПРОГРАМИ ОПТИМАЛ

Притула І.І., Вершков О.О.
Таврійський державний агротехнологічний університет ім. Дмитра Моторного, м. Мелітополь

Пропонуються нові можливості розв'язання транспортних задач засобами програми Оптимал.

Ключові слова: *транспортна задача, комп'ютерні технології, оптимальний план.*

Offers new possibilities for solving transport problems by means of the Optimal program.

Keywords: *transport problem, computer technology, optimal plan.*

Безперервно збільшується об'єм і змінюється зміст знань, умінь і навиків, якими повинні володіти сучасні фахівці. У всіх сферах освіти ведуться пошуки способів швидкої модернізації системи підготовки, підвищення якості навчання з використанням комп'ютерних технологій. Можливості комп'ютерних технологій як інструменту людської діяльності і принципово нового засобу навчання привело до появи нових методів і організаційних форм навчання і швидшого їх впровадження в учбовий процес. Майбутні фахівці повинні володіти системою знань і умінь, що дозволяють грамотно використовувати комп'ютерні технології в майбутній професійній діяльності.

Таким чином, постає проблема застосування в навчальному процесі прикладних програм, які дозволять студентам краще зрозуміти навчальний матеріал.

Пропонується використовувати програму *Оптимал* при вивченні студентами 3-го курсу спеціальності "Обладнання переробних та харчових виробництв" матеріалу за темою "Розв'язання транспортних задач" з дисципліни "Прикладна математика".

Для розв'язання транспортних задач на практиці часто використовують засоби табличного процесору Excel [1]. Проте Excel не дає можливості побачити внутрішній механізм розв'язання задачі. Програма *Оптимал* не тільки має можливості для виводу проміжних обчислень, що може бути використано для навчання студентів розв'язанню транспортних задач, а також може застосовуватися викладачами для контролю знань студентів.

В даній роботі пропонуються нові можливості розв'язання транспортних задач з використанням програми *Оптимал.*

Загальна постановка транспортної задачі полягає у визначенні оптимального плану перевезень деякого однорідного вантажу з m пунктів відправлення $A_1, A_2, ..., A_m$ в n пунктів призначення $B_1, B_2, ..., B_n$. При цьому критерієм оптимальності зазвичай є мінімальна вартість перевезень всього вантажу, або мінімальний час його доставки. Процес розв'язання транспортної задачі включає велику кількість однотипних операцій, на виконання яких потрібно багато часу. Тому рекомендується використовувати прикладну комп'ютерну програму *Оптимал*, яка здатна за дуже короткий час виконати всі необхідні обчислення.

Математична постановка транспортної задачі полягає у визначенні мінімального значення функції:

$$F = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} x_{ij} ,$$

при заданих обмеженнях:

$$\sum_{i=1}^{m} x_{ij} = b_j \quad \left(j = \overline{1,n}\right), \quad \sum_{j=1}^{n} x_{ij} = a_i \quad \left(i = \overline{1,m}\right), \quad x_{ij} \geq 0 \quad \left(i = \overline{1,m};\ j = \overline{1,n}\right),$$

де F – цільова функція, a_{ij}, b_i, c_j – задані постійні величини.

На практичному занятті пропонується розв'язати наступну задачу.

Задача. На трьох складах оптової бази зосереджений однорідний вантаж. Цей вантаж необхідно перевезти в чотири магазини. Кожен з магазинів повинен отримати певну кількість вантажу. Тарифи перевезень одиниці вантажу з кожного склада у всі магазини відомі. Визначити оптимальний план перевезень вантажу, при якому загальна вартість перевезень буде мінімальною [2].

Пропонується наступний алгоритм розв'язку задачі:

1. Встановити розмір таблиці вихідних даних за допомогою меню *Таблица*.

2. Вибрати метод знаходження опорного плану, метод і режим розв'язання транспортної задачі за допомогою команди *Задача* $\Rightarrow$ *Настройки*.

3. Ввести вихідні дані.

4. Щоб розв'язати транспортну задачу, натиснути на кнопку *Решить*.

На рис. 1 наведені результати роботи програми *Оптимал*: мінімальне значення функції і оптимальний план.

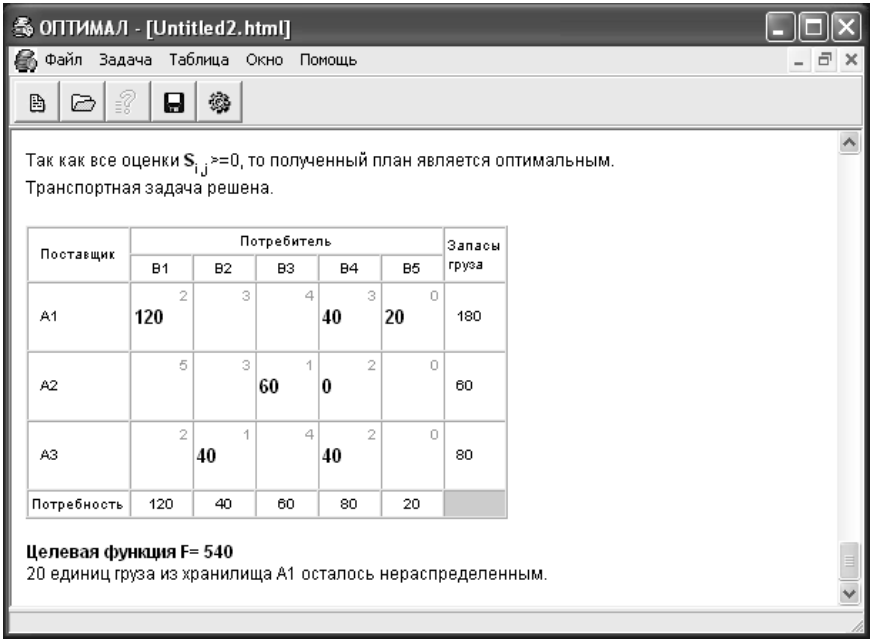


Рис. 1 Результати роботи програми *Оптимат*

Висновки. Запропоновано нові можливості розв'язання транспортних задач з використанням програми *Оптимал* для проведення лабораторної роботи за темою "Розв'язання транспортних задач" в рамках курсу "Прикладна математика". Результати проведеної лабораторної роботи показали, що при використанні даної навчальної програми студенти продемонстрували рівень знань вищий, ніж студенти, які вивчали цей матеріал звичайним способом.

Інформаційні джерела

1. Орлова И.В. Экономико-математические методы и модели. Выполнение расчетов в среде Excel. – М.: ЗАО Финстатинформ, 2000. – 136 с.

2. Акулич И.Л. Математическое программирование в примерах и задачах. – М.: Высш. школа, 1986. – 319 с.

3. Ашманов С.А. Линейное программирование. – М.: Наука, 1981. – 340 с.

УДК 004.9:378

РОЛЬ СУЧАСНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТІ

Яковчук В., Смотр О.
Львівський державний університет безпеки життєдіяльності, м. Львів

Роботу присвячено розгляду ролі сучасних інформаційних та телекомунікаційних технологій в трансформації розвитку суспільства загалом та зокрема, освітнього процесу.

Ключові слова: *інформаційна технологія, інформаційне суспільство, освіта.*

The work is devoted to the role of modern information and telecommunication technologies in the transformation of the development of society in general and in particular, the educational process.

Key words*: information technology, information society, education.*

Сьогодні інформаційні технології стали невід'ємною частиною сучасного світу, вони значною мірою визначають подальший економічний та суспільний розвиток людства. Очевидно, що у таких умовах і система навчання вимагає революційних змін. Безумовно, неймовірно актуальним є на сьогодні вивчення питання впровадження інформаційних технології у сучасне освітнє середовище. Адже нині якісне викладання дисциплін не може здійснюватися без використання засобів і можливостей, які надають інформаційні технології та всесвітня мережева павутина Інтернет [1].

Впровадження в освітній процес інформаційних технологій, пов'язаних з використанням мережі та Інтернету, надає можливість зреалізувати принцип безперервної освіти – «навчання впродовж усього життя», перейти від догматичного заучування до діяльнісного та компетентного підходу - підготовки фахівців, здатних в умовах сучасного виробництва вирішувати наявні проблеми в нетривіальних умовах. Інформаційно-комунікаційні технології мають великі можливості для особистісного розвитку людини, розкриття її потенціалу, тому на сучасному етапі, особливо в період карантинних обмежень, пов'язаних із поширенням COVID 19, невід'ємною частиною освітнього процесу стають дистанційні форми та технології навчання й виховання.

Сучасна інформаційна технологія (СІТ) в освіті – це комплекс навчальних і навчально-методичних матеріалів, технічних та інструментальних засобів техніки навчального призначення, а також система наукових знань про роль і місце обчислювальної техніки в навчальному процесі, про форми і методи їх застосування для вдосконалення праці викладачів та студентів [1,2].

Завдяки інформаційним технологіям, змінюється рівень кваліфікації викладачів, велика кількість інформації опублікована на публічних інформаційних сайтах-бібліотеках. Основним джерелом цієї всієї інформації являється «Інтернет». Кожен викладач має можливість не лише навчити, а й сам почерпнути важливої інформації. Це полегшує та робить навчання більш інтегрованим в навчальний процес.

У багатьох розвинених країнах світу сьогодні активно йде процес переходу від індустріального до інформаційного суспільства. У цих умовах засоби створення і використання інформаційних ресурсів в будь-якій розвиненій країні мають бути на рівні сучасних вимог. Такими засобами є:

• наукова методологія, використовувана в інформаційній сфері суспільства;

• програмно-апаратні засоби інформатизації;

• сучасні інформаційні технології.

Одним із сучасних шляхів інтенсифікації та оптимізації навчального процесу є інформатизація освіти, і зокрема, використання комп'ютерних технологій. Як показує аналіз, більшість учнів та студентів уже на ранніх стадіях навчання прекрасно усвідомлюють необхідність застосування новітніх інформаційних технологій у своїй професійній діяльності.

До хорошого швидко звикаєш. Сьогодні ділова людина вже не уявляє своє життя без мобільного телефону і персонального комп'ютера, а будь-яка сучасна установа немислима без власної автоматизованої інформаційної системи, електронної копіювальної техніки і виходу в міжнародну інформаційно-телекомунікаційну мережу. Нікого не здивує і персональна ЕОМ з процесором Core i7 чи AMD Ryzen на столі у звичайного студента і навіть школяра, з такими функціональними можливості, якими всього 10—15 років тому могли володіти тільки системи, що відносилися в цей період до розряду СУПЕРЕОМ та були на балансі лише у незначної кількості державних структур.

Завдяки стрімкому розвитку засобів інформатики, що відбувається останніми роками, інформаційна сфера суспільства нестримно змінюється, роблячи тим самим сильний вплив на всі інші сторони життя і діяльності людей. Умови життя і діяльності людей в розвинених країнах вже в середині XXI століття будуть так само сильно відрізнятися від сучасних, як умови життя нашого часу відрізняються від умов життя в Росії за часів правління царя Петра Першого.

У новому високоавтоматизованому інформаційному суспільстві у людей з'являться не тільки абсолютно нові можливості, але і нові проблеми - це проблема інформаційної нерівності людей в новому інформаційному середовищі і забезпечення інформаційної безпеки людини і суспільства, а також всієї біосфери нашої планети.

Цілком можливо, що в тому новому високоавтоматизованому інформаційному середовищі, яке вже формується в розвинених країнах світової спільноти, виникнуть і інші принципово нові глобальні проблеми, про зміст яких сьогодні можна тільки здогадуватися. На одну з таких проблем вказав в своїй оглядовій лекції з фізики відомий англійський учений С. Хокинг. Сьогодні він очолює в Кембриджі ту саму кафедру, якою свого часу завідував Ісаак Ньютон. У цій лекції, яка була прочитана в 1998 р. у Вашингтоні для президента США Біла Клінтона і його найближчого оточення, С. Хокинг відзначив ще одну нову небезпеку, яку може породити ніким сьогодні не контрольований процес розвитку інтелектуальних можливостей кібернетичних пристроїв і автоматизованих роботів. Він вважає, що якщо цей процес і далі продовжуватиметься такими ж темпами, як це має місце сьогодні (а ніякі реальні обмеження в розвитку цього процесу поки не є видимими), то вже в XXI столітті цілком вірогідною може опинитися ситуація, коли людству доведеться боротися за своє місце під сонцем вже не тільки з грізними силами Природи, але і з новою високоорганізованою штучною цивілізацією. Основу цієї цивілізації, на думку ученого, складатимуть біороботи і системи штучного розуму на базі надпотужних комп'ютерних мереж [3]. Звісно все це жарти, фантастика геніальної людини, але все ж, сама система розвитку не аби як важлива для піднесення людства на новий рівень розумової здатності.

Підсумовуючи вищенаведене, та зважаючи на надзвичайні умови, пов’язані з карантинними обмеженнями, через поширення пандемії COVID 19, в яких на сьогодні вчиться жити та здобувати освіту по новому увесь світ, можемо стверджувати, що використання СІТ є невід’ємною частино нашого життя загалом, та освітнього процесу, зокрема. Дистанційне навчання на сьогодні - це одна з найефективніших систем підготовки і безперервної підтримки високого кваліфікаційного рівня фахівців. Лише використання сучасних інформаційно-телекомунікаційних технологій в освітньому процесу надасть можливість найбільш ефективно забезпечувати реалізацію конституційного права на освіту усіх громадян нашої країни.

Література

1. Любович А.А. Сучасні інформаційні технології в освіті / А.А. Любович, О.Г. Єсіна // Інформатика та інформаційні технології : студ.наук.конф., 20 квітня 2015 р.: матер. Конф. – Одеса, ОНЕУ. – С. 118-120.

2. Купчак М.І. Тенденції та проблеми впровадження інформаційних технологій в управління університетом / М.І. Купчак, О.О. Смотр, М.Я. Купчак // Вісник Львівського державного університету безпеки життєдіяльності : зб. наук. праць. – Львів : Вид-во ЛДУ БЖД. – 2013. – № 7. – С. 28-32

3. Сучасні технології освіти дорослих : посіб. / авт. кол. : Л. Б. Лук’янова, О. В. Аніщенко, Л. Є. Сігаєва, С. В. Зінченко, О. В. Баніт, Н. І. Дорошенко. — Кіровоград : Імекс-ЛТД, 2013. — 182 с.

З М І С Т

Секція 1

КІБЕРБЕЗПЕКА

Напрям 1. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Напрям 2. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Напрям 3. ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Напрям 4. БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ

Напрям 5. КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Напрям 6. ІНФОРМАЦІЙНІ ВІЙНИ

Секція 2

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Напрям 7. ПРИКЛАДНЕ ТА СИСТЕМНЕ ПРОГРАМУВАННЯ

ПРОЄКТАМИ

Напрям 14. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Всеукраїнської науково-практичної конференції
молодих учених, студентів і курсантів

Відповідальні за випуск **Олександр Придатко**
Ростислав Ткачук

Оригінал-макет **Ростислав Ткачук**

Друк на різографі **Маріанна Климус**

Підписано до друку 12.11.2020 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різографі. Папір офсетний.
Ум. друк. арк. 15,7.

Друк ЛДУ БЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.
e- mail: mail@ubgd.lviv.ua, ndr@ ubgd.lviv.ua